CIS Center for Internet Security®

CIS Benchmarks™

# CIS Microsoft 365 Foundations Benchmark

v6.0.0 - 10-31-2025

# Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

**NOTE**: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

# Table of Contents


*Terms of Use* ..... *1*

*Table of Contents* ..... *2*

*Overview* ..... *8*

**Important Usage Information** ..... **8**

**Key Stakeholders** ..... **8**

**Apply the Correct Version of a Benchmark** ..... **9**

**Exceptions** ..... **9**

**Remediation** ..... **10**

**Summary** ..... **10**

**Target Technology Details** ..... **11**

**Intended Audience** ..... **11**

**Consensus Guidance** ..... **12**

**Typographical Conventions** ..... **13**

*Recommendation Definitions* ..... *14*

**Title** ..... **14**

**Assessment Status** ..... **14**

**Automated** ..... **14**

**Manual** ..... **14**

**Profile** ..... **14**

**Description** ..... **14**

**Rationale Statement** ..... **14**

**Impact Statement** ..... **15**

**Audit Procedure** ..... **15**

**Remediation Procedure** ..... **15**

**Default Value** ..... **15**

**References** ..... **15**

**CIS Critical Security Controls® (CIS Controls®)** ..... **15**

**Additional Information** ..... **15**

**Profile Definitions** ..... **16**

**Acknowledgements** ..... **17**

*Recommendations* ..... *18*

**1 Microsoft 365 admin center** ..... **18**

**1.1 Users** ..... **19**

1.1.1 (L1) Ensure Administrative accounts are cloud-only (Automated) ..... 20

1.1.2 (L1) Ensure two emergency access accounts have been defined (Manual) ..... 23

1.1.3 (L1) Ensure that between two and four global admins are designated (Automated) ..... 27

1.1.4 (L1) Ensure administrative accounts use licenses with a reduced application footprint (Automated) ..... 30
**1.2 Teams & groups ..... 35**
1.2.1 (L2) Ensure that only organizationally managed/approved public groups exist (Automated) ..... 36
1.2.2 (L1) Ensure sign-in to shared mailboxes is blocked (Automated) ..... 39
**1.3 Settings ..... 42**
1.3.1 (L1) Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)' (Automated) ..... 43
1.3.2 (L2) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices (Automated) ..... 46
1.3.3 (L2) Ensure 'External sharing' of calendars is not available (Automated) ..... 52
1.3.4 (L1) Ensure 'User owned apps and services' is restricted (Automated) ..... 55
1.3.5 (L1) Ensure internal phishing protection for Forms is enabled (Automated) ..... 59
1.3.6 (L2) Ensure the customer lockbox feature is enabled (Automated) ..... 61
1.3.7 (L2) Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web' (Automated) ..... 63
1.3.8 (L2) Ensure that Sways cannot be shared with people outside of your organization (Manual) ..... 67
1.3.9 (L1) Ensure shared bookings paged are restricted to select users (Automated) ..... 69
**2 Microsoft 365 Defender ..... 72**
**2.1 Email & collaboration ..... 73**
2.1.1 (L2) Ensure Safe Links for Office Applications is Enabled (Automated) ..... 74
2.1.2 (L1) Ensure the Common Attachment Types Filter is enabled (Automated) ..... 79
2.1.3 (L1) Ensure notifications for internal users sending malware is Enabled (Automated) ..... 82
2.1.4 (L2) Ensure Safe Attachments policy is enabled (Automated) ..... 85
2.1.5 (L2) Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled (Automated) ..... 89
2.1.6 (L1) Ensure Exchange Online Spam Policies are set to notify administrators (Automated) ..... 92
2.1.7 (L2) Ensure that an anti-phishing policy has been created (Automated) ..... 95
2.1.8 (L1) Ensure that SPF records are published for all Exchange Domains (Automated) ..... 101
2.1.9 (L1) Ensure that DKIM is enabled for all Exchange Online Domains (Automated) ..... 103
2.1.10 (L1) Ensure DMARC Records for all Exchange Online domains are published (Automated) ..... 107
2.1.11 (L2) Ensure comprehensive attachment filtering is applied (Automated) ..... 111
2.1.12 (L1) Ensure the connection filter IP allow list is not used (Automated) ..... 118
2.1.13 (L1) Ensure the connection filter safe list is off (Automated) ..... 121
2.1.14 (L1) Ensure inbound anti-spam policies do not contain allowed domains (Automated) ..... 124
2.1.15 (L1) Ensure outbound anti-spam message limits are in place (Automated) ..... 127
**2.2 Cloud apps ..... 132**
2.2.1 (L1) Ensure emergency access account activity is monitored (Manual) ..... 133
**2.3 Audit ..... 136**
**2.4 System ..... 136**
2.4.1 (L1) Ensure Priority account protection is enabled and configured (Automated) ..... 137
2.4.2 (L1) Ensure Priority accounts have 'Strict protection' presets applied (Automated) ..... 141
2.4.3 (L2) Ensure Microsoft Defender for Cloud Apps is enabled and configured (Manual) ..... 144
2.4.4 (L1) Ensure Zero-hour auto purge for Microsoft Teams is on (Automated) ..... 147
**3 Microsoft Purview ..... 149**
**3.1 Audit ..... 150**
3.1.1 (L1) Ensure Microsoft 365 audit log search is Enabled (Automated) ..... 151
**3.2 Data loss protection ..... 153**
3.2.1 (L1) Ensure DLP policies are enabled (Automated) ..... 154
3.2.2 (L1) Ensure DLP policies are enabled for Microsoft Teams (Automated) ..... 156

**3.3 Information Protection ..... 160**
3.3.1 (L1) Ensure Information Protection sensitivity label policies are published (Automated) ..... 161
**4 Microsoft Intune admin center ..... 164**
4.1 (L2) Ensure devices without a compliance policy are marked 'not compliant' (Automated) ..... 165
4.2 (L2) Ensure device enrollment for personally owned devices is blocked by default (Automated) ..... 168
**5 Microsoft Entra admin center ..... 173**
**5.1 Entra ID ..... 173**
**5.1.1 Overview ..... 173**
**5.1.2 Users ..... 174**
5.1.2.1 (L1) Ensure 'Per-user MFA' is disabled (Automated) ..... 175
5.1.2.2 (L2) Ensure third party integrated applications are not allowed (Automated) ..... 177
5.1.2.3 (L1) Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated) ..... 179
5.1.2.4 (L1) Ensure access to the Entra admin center is restricted (Manual) ..... 182
5.1.2.5 (L2) Ensure the option to remain signed in is hidden (Manual) ..... 184
5.1.2.6 (L2) Ensure 'LinkedIn account connections' is disabled (Manual) ..... 186
**5.1.3 Groups ..... 188**
5.1.3.1 (L1) Ensure a dynamic group for guest users is created (Automated) ..... 189
5.1.3.2 (L1) Ensure users cannot create security groups (Automated) ..... 193
**5.1.4 Devices ..... 196**
5.1.4.1 (L2) Ensure the ability to join devices to Entra is restricted (Automated) ..... 197
5.1.4.2 (L1) Ensure the maximum number of devices per user is limited (Automated) ..... 200
5.1.4.3 (L1) Ensure the GA role is not added as a local administrator during Entra join (Automated) ..... 203
5.1.4.4 (L1) Ensure local administrator assignment is limited during Entra join (Automated) 206
5.1.4.5 (L1) Ensure Local Administrator Password Solution is enabled (Automated) ..... 209
5.1.4.6 (L2) Ensure users are restricted from recovering BitLocker keys (Automated) ..... 212
**5.1.5 Applications ..... 215**
5.1.5.1 (L2) Ensure user consent to apps accessing company data on their behalf is not allowed (Automated) ..... 216
5.1.5.2 (L1) Ensure the admin consent workflow is enabled (Automated) ..... 219
**5.1.6 External Identities ..... 222**
5.1.6.1 (L2) Ensure that collaboration invitations are sent to allowed domains only (Automated) ..... 223
5.1.6.2 (L1) Ensure that guest user access is restricted (Automated) ..... 226
5.1.6.3 (L2) Ensure guest user invitations are limited to the Guest Inviter role (Automated) ..... 229
**5.1.7 User experiences ..... 231**
**5.1.8 Hybrid management ..... 232**
5.1.8.1 (L1) Ensure that password hash sync is enabled for hybrid deployments (Manual) ..... 233
**5.2 ID Protection ..... 236**
**5.2.1 Identity Protection ..... 236**
**5.2.2 Risk-based Conditional Access ..... 237**
5.2.2.1 (L1) Ensure multifactor authentication is enabled for all users in administrative roles (Automated) ..... 238
5.2.2.2 (L1) Ensure multifactor authentication is enabled for all users (Automated) ..... 242
5.2.2.3 (L1) Enable Conditional Access policies to block legacy authentication (Automated) 245
5.2.2.4 (L1) Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users (Automated) ..... 248
5.2.2.5 (L2) Ensure 'Phishing-resistant MFA strength' is required for Administrators (Automated) ..... 252
5.2.2.6 (L1) Enable Identity Protection user risk policies (Automated) ..... 256
5.2.2.7 (L1) Enable Identity Protection sign-in risk policies (Automated) ..... 259

5.2.2.8 (L2) Ensure 'sign-in risk' is blocked for medium and high risk (Automated) ..... 262
5.2.2.9 (L1) Ensure a managed device is required for authentication (Automated) ..... 265
5.2.2.10 (L1) Ensure a managed device is required to register security information (Automated) ..... 268
5.2.2.11 (L1) Ensure sign-in frequency for Intune Enrollment is set to 'Every time' (Automated) ..... 271
5.2.2.12 (L1) Ensure the device code sign-in flow is blocked (Automated) ..... 274
**5.2.3 Authentication Methods ..... 277**
5.2.3.1 (L1) Ensure Microsoft Authenticator is configured to protect against MFA fatigue (Automated) ..... 278
5.2.3.2 (L1) Ensure custom banned passwords lists are used (Automated) ..... 281
5.2.3.3 (L1) Ensure password protection is enabled for on-prem Active Directory (Automated) ..... 284
5.2.3.4 (L1) Ensure all member users are 'MFA capable' (Automated) ..... 287
5.2.3.5 (L1) Ensure weak authentication methods are disabled (Automated) ..... 291
5.2.3.6 (L1) Ensure system-preferred multifactor authentication is enabled (Automated) ..... 294
5.2.3.7 (L2) Ensure the email OTP authentication method is disabled (Automated) ..... 297
**5.2.4 Password reset ..... 300**
5.2.4.1 (L1) Ensure 'Self service password reset enabled' is set to 'All' (Manual) ..... 301
**5.3 ID Governance ..... 303**
5.3.1 (L2) Ensure 'Privileged Identity Management' is used to manage roles (Automated) ..... 304
5.3.2 (L1) Ensure 'Access reviews' for Guest Users are configured (Automated) ..... 308
5.3.3 (L1) Ensure 'Access reviews' for privileged roles are configured (Automated) ..... 313
5.3.4 (L1) Ensure approval is required for Global Administrator role activation (Automated) 317
5.3.5 (L1) Ensure approval is required for Privileged Role Administrator activation (Automated) ..... 320

**6 Exchange admin center ..... 323**
**6.1 Audit ..... 324**
6.1.1 (L1) Ensure 'AuditDisabled' organizationally is set to 'False' (Automated) ..... 325
6.1.2 (L1) Ensure mailbox audit actions are configured (Automated) ..... 327
6.1.3 (L1) Ensure 'AuditBypassEnabled' is not enabled on mailboxes (Automated) ..... 334
**6.2 Mail flow ..... 337**
6.2.1 (L1) Ensure all forms of mail forwarding are blocked and/or disabled (Automated) ..... 338
6.2.2 (L1) Ensure mail transport rules do not whitelist specific domains (Automated) ..... 343
6.2.3 (L1) Ensure email from external senders is identified (Automated) ..... 346
**6.3 Roles ..... 348**
6.3.1 (L2) Ensure users installing Outlook add-ins is not allowed (Automated) ..... 349
**6.4 Reports ..... 353**
**6.5 Settings ..... 354**
6.5.1 (L1) Ensure modern authentication for Exchange Online is enabled (Automated) ..... 355
6.5.2 (L1) Ensure MailTips are enabled for end users (Automated) ..... 358
6.5.3 (L2) Ensure additional storage providers are restricted in Outlook on the web (Automated) ..... 361
6.5.4 (L1) Ensure SMTP AUTH is disabled (Automated) ..... 363
6.5.5 (L2) Ensure Direct Send submissions are rejected (Automated) ..... 366

**7 SharePoint admin center ..... 369**
**7.1 Sites ..... 369**
**7.2 Policies ..... 370**
7.2.1 (L1) Ensure modern authentication for SharePoint applications is required (Automated) ..... 371
7.2.2 (L1) Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled (Automated) ..... 374
7.2.3 (L1) Ensure external content sharing is restricted (Automated) ..... 376
7.2.4 (L2) Ensure OneDrive content sharing is restricted (Automated) ..... 379

7.2.5 (L2) Ensure that SharePoint guest users cannot share items they don't own (Automated) ..... 382
7.2.6 (L2) Ensure SharePoint external sharing is restricted (Automated) ..... 385
7.2.7 (L1) Ensure link sharing is restricted in SharePoint and OneDrive (Automated) ..... 388
7.2.8 (L2) Ensure external sharing is restricted by security group (Manual) ..... 390
7.2.9 (L1) Ensure guest access to a site or OneDrive will expire automatically (Automated) 392
7.2.10 (L1) Ensure reauthentication with verification code is restricted (Automated) ..... 395
7.2.11 (L1) Ensure the SharePoint default sharing link permission is set (Automated) ..... 398
**7.3 Settings ..... 400**
7.3.1 (L2) Ensure Office 365 SharePoint infected files are disallowed for download (Automated) ..... 401
7.3.2 (L2) Ensure OneDrive sync is restricted for unmanaged devices (Automated) ..... 403
**8 Microsoft Teams admin center ..... 406**
**8.1 Teams ..... 407**
8.1.1 (L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services (Automated) ..... 408
8.1.2 (L1) Ensure users can't send emails to a channel email address (Automated) ..... 412
**8.2 Users ..... 415**
8.2.1 (L2) Ensure external domains are restricted in the Teams admin center (Automated) . 416
8.2.2 (L1) Ensure communication with unmanaged Teams users is disabled (Automated) .. 420
8.2.3 (L1) Ensure external Teams users cannot initiate conversations (Automated) ..... 423
8.2.4 (L1) Ensure the organization cannot communicate with accounts in trial Teams tenants (Automated) ..... 427
**8.3 Teams devices ..... 430**
**8.4 Teams apps ..... 431**
8.4.1 (L1) Ensure app permission policies are configured (Manual) ..... 432
**8.5 Meetings ..... 434**
8.5.1 (L2) Ensure anonymous users can't join a meeting (Automated) ..... 435
8.5.2 (L1) Ensure anonymous users and dial-in callers can't start a meeting (Automated) ... 438
8.5.3 (L1) Ensure only people in my org can bypass the lobby (Automated) ..... 441
8.5.4 (L1) Ensure users dialing in can't bypass the lobby (Automated) ..... 444
8.5.5 (L2) Ensure meeting chat does not allow anonymous users (Automated) ..... 446
8.5.6 (L2) Ensure only organizers and co-organizers can present (Automated) ..... 448
8.5.7 (L1) Ensure external participants can't give or request control (Automated) ..... 450
8.5.8 (L2) Ensure external meeting chat is off (Automated) ..... 453
8.5.9 (L2) Ensure meeting recording is off by default (Automated) ..... 455
**8.6 Messaging ..... 457**
8.6.1 (L1) Ensure users can report security concerns in Teams (Automated) ..... 458
**9 Microsoft Fabric ..... 463**
**9.1 Tenant settings ..... 464**
9.1.1 (L1) Ensure guest user access is restricted (Manual) ..... 465
9.1.2 (L1) Ensure external user invitations are restricted (Manual) ..... 467
9.1.3 (L1) Ensure guest access to content is restricted (Manual) ..... 469
9.1.4 (L1) Ensure 'Publish to web' is restricted (Manual) ..... 471
9.1.5 (L2) Ensure 'Interact with and share R and Python' visuals is 'Disabled' (Manual) ..... 473
9.1.6 (L1) Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled' (Manual) .. 475
9.1.7 (L1) Ensure shareable links are restricted (Manual) ..... 478
9.1.8 (L1) Ensure enabling of external data sharing is restricted (Manual) ..... 481
9.1.9 (L1) Ensure 'Block ResourceKey Authentication' is 'Enabled' (Manual) ..... 483
9.1.10 (L1) Ensure access to APIs by service principals is restricted (Manual) ..... 485
9.1.11 (L1) Ensure service principals cannot create and use profiles (Manual) ..... 487
9.1.12 (L1) Ensure service principals ability to create workspaces, connections and deployment pipelines is restricted (Manual) ..... 489
***Appendix: Summary Table ..... 491***

*Appendix: Change History ..... 504*

# Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

## Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

**NOTE**: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

### Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

## Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

## Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

## Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

**When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.**

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completes successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

## Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

**NOTE**: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

## Target Technology Details

This document, Security Configuration Benchmark for Microsoft 365, provides prescriptive guidance for establishing a secure configuration posture for Microsoft 365 Cloud offerings running on any OS. This guide was tested against Microsoft 365, and includes recommendations for Exchange Online, SharePoint Online, OneDrive for Business, Teams, Power BI (Fabric) and Microsoft Entra ID.

To ensure all PowerShell cmdlets work in your tenant please download the latest versions of the PowerShell modules. Scripts and cmdlets referenced in this benchmark were tested using the following module versions.

- MicrosoftTeams `7.1.0`
- ExchangeOnlineManagement `3.8.0`
- PnP.PowerShell `3.1.0`
- Microsoft.Graph.Applications `2.30.0`
- Microsoft.Graph.Authentication `2.30.0`
- Microsoft.Graph.DeviceManagement `2.30.0`
- Microsoft.Graph.Groups `2.30.0`
- Microsoft.Graph.Identity.DirectoryManagement `2.30.0`
- Microsoft.Graph.Identity.Governance `2.30.0`
- Microsoft.Graph.Identity.SignIns `2.30.0`
- Microsoft.Graph.Reports `2.30.0`
- Microsoft.Graph.Users `2.30.0`
- Microsoft.Online.SharePoint.PowerShell `16.0.26510.12000`

Note that the individual software applications installed on the end user device: Word, Excel, etc. are covered in separate benchmarks that compliment this guide. See the CIS Microsoft Office Enterprise Benchmark for details, available at https://workbench.cisecurity.org/communities/39

To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

## Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft 365. Where possible audit and remediation guidance is provided using both PowerShell and relevant Admin Centers, using either method is acceptable when attempting to determine a Pass or Fail for a particular recommendation.

## Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

## Typographical Conventions

The following typographical conventions are used throughout this guide:

| Convention | Meaning |
| --- | --- |
| `Stylized Monospace font` | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented. |
| `Monospace font` | Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented. |
| `<Monospace font in brackets>` | Text set in angle brackets denote a variable requiring substitution for a real value. |
| *Italic font* | Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication. |
| **Bold font** | Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal). |

# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable.  If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

## Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

## Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## References

Additional documentation relative to the recommendation.

## CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

## Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **E3 Level 1**

  Items in this profile apply to customer deployments of Microsoft M365 with an E3 license and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **E3 Level 2**

  This profile extends the "E3 Level 1" profile. Items in this profile exhibit one or more of the following characteristics and is focused on customer deployments of Microsoft M365 E3:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

- **E5 Level 1**

  Items in this profile extend what is provided by the "E3 Level 1" profile for customer deployments of Microsoft M365 with an E5 license and intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **E5 Level 2**

  This profile extends the "E3 Level 1" and "E5 Level 1" profiles and will effectively include all E3 and E5 recommendations at both levels. Items in this profile exhibit one or more of the following characteristics and is focused on customer deployments of Microsoft M365 E5:

  - are intended for environments or use cases where security is paramount
  - acts as defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

# Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

**Contributor**
Dan Menicucci
Brandon Cox
Richard Handley
Jennifer Jarose
Mack Bodie
Jason Inks
Samuel Emangard
Kyle Cira
Oleksii Burchynskyi
Havard Overas
Talbert Houle
Casey Hennings
Kaua Pickett
Jon Milner
Rex Farabee
Michael Smith
Steven Los

**Editor**
Caleb Eifert
Cody McLees

# Recommendations

## 1 Microsoft 365 admin center

The Microsoft 365 admin center is the primary landing page for everything 365 related and contains navigational links to all the other admin centers.

https://admin.microsoft.com/

## 1.1 Users

### *1.1.1 (L1) Ensure Administrative accounts are cloud-only (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Administrative accounts are special privileged accounts that could have varying levels of access to data, users, and settings. Regular user accounts should never be utilized for administrative tasks and care should be taken, in the case of a hybrid environment, to keep administrative accounts separate from on-prem accounts. Administrative accounts should not have applications assigned so that they have no access to potentially vulnerable services (EX. email, Teams, SharePoint, etc.) and only access to perform tasks as needed for administrative purposes.

Ensure administrative accounts are not `On-premises sync enabled`.

**Rationale:**

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

**Impact:**

Administrative users will need to utilize login/logout functionality to switch accounts when performing administrative tasks, which means they will not benefit from SSO. This will require a migration process from the 'daily driver' account to a dedicated admin account.

Once the new admin account is created, permission sets should be migrated from the 'daily driver' account to the new admin account. This includes both M365 and Azure RBAC roles. Failure to migrate Azure RBAC roles could prevent an admin from seeing their subscriptions/resources while using their admin account.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Users` and select `All users`.
3. To the right of the search box click the `Add filter` button.
4. Add the `On-premises sync enabled` filter with the value set to `Yes` and click `Apply.`
5. Verify that no user accounts in administrative roles are present in the filtered list.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "RoleManagement.Read.Directory","User.Read.All"`
2. Run the following PowerShell script:

```
$DirectoryRoles = Get-MgDirectoryRole

# Get privileged role IDs
$PrivilegedRoles = $DirectoryRoles | Where-Object {
    $_.DisplayName -like "*Administrator*" -or $_.DisplayName -eq "Global
Reader"
}

# Get the members of these various roles
$RoleMembers = $PrivilegedRoles | ForEach-Object { Get-MgDirectoryRoleMember
-DirectoryRoleId $_.Id } |
    Select-Object Id -Unique

# Retrieve details about the members in these roles
$PrivilegedUsers = $RoleMembers | ForEach-Object {
    Get-MgUser -UserId $_.Id -Property UserPrincipalName, DisplayName, Id,
OnPremisesSyncEnabled
}

$PrivilegedUsers | Where-Object { $_.OnPremisesSyncEnabled -eq $true } |
    ft DisplayName,UserPrincipalName,OnPremisesSyncEnabled
```

3. The script will output any hybrid users that are also members of privileged roles. If nothing returns, then no users with that criteria exist.

**Remediation:**

Remediation will require first identifying the privileged accounts that are synced from on-premises and then creating a new cloud-only account for that user. Once a replacement account is established, the hybrid account should have its role reduced to that of a non-privileged user or removed depending on the need.

**Default Value:**

N/A

**References:**

1. https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/add-users?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/enterprise/protect-your-global-administrator-accounts?view=o365-worldwide
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices#9-use-cloud-native-accounts-for-microsoft-entra-roles
4. https://learn.microsoft.com/en-us/entra/fundamentals/whatis
5. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts<br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. | ● | ● | ● |
| v7 | 4.1 Maintain Inventory of Administrative Accounts<br>Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. | | ● | ● |

## *1.1.2 (L1) Ensure two emergency access accounts have been defined (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Emergency access or "break glass" accounts are limited for emergency scenarios where normal administrative accounts are unavailable. They are not assigned to a specific user and will have a combination of physical and technical controls to prevent them from being accessed outside a true emergency. These emergencies could be due to several things, including:

- Technical failures of a cellular provider or Microsoft related service such as MFA.
- The last remaining Global Administrator account is inaccessible.

Ensure two `Emergency Access` accounts have been defined.

**Note:** Microsoft provides several recommendations for these accounts and how to configure them. For more information on this, please refer to the references section. The CIS Benchmark outlines the more critical things to consider.

**Rationale:**

In various situations, an organization may require the use of a break glass account to gain emergency access. In the event of losing access to administrative functions, an organization may experience a significant loss in its ability to provide support, lose insight into its security posture, and potentially suffer financial losses.

**Impact:**

Failure to properly implement emergency access accounts can weaken the security posture. Microsoft recommends excluding at least one of the two emergency access accounts from all conditional access rules, necessitating passwords with sufficient entropy and length to protect against random guesses. For a secure passwordless solution, FIDO2 security keys may be used instead of passwords.

**Audit:**

**To audit using the UI:**

**Step 1 - Ensure a policy and procedure is in place at the organization:**

- In order for accounts to be effectively used in a break-glass situation the proper policies and procedures must be authorized and distributed by senior management.
- FIDO2 Security Keys should be locked in a secure separate fireproof location.
- Passwords should be at least 16 characters, randomly generated and MAY be separated in multiple pieces to be joined on emergency.

**Step 2 - Ensure two emergency access accounts are defined:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com
2. Expand `Users` > `Active Users`
3. Inspect the designated emergency access accounts and ensure the following:
    - The accounts are named correctly, and do NOT identify with a particular person.
    - The accounts use the default `.onmicrosoft.com` domain and not the organization's.
    - The accounts are cloud-only.
    - The accounts are unlicensed.
    - The accounts are assigned the `Global Administrator` directory role.

**Step 3 - Ensure at least one account is excluded from all conditional access rules:**

1. Navigate `Microsoft Entra admin center` https://entra.microsoft.com/
2. Expand `Protection` > `Conditional Access`.
3. Inspect the conditional access rules.
4. Ensure one of the emergency access accounts is excluded from all rules.

**Warning:** As of 10/15/2024 MFA is required for all users including Break Glass Accounts. It is recommended to update these accounts to use passkey (FIDO2) or configure certificate-based authentication for MFA. Both methods satisfy the MFA requirement.

**Remediation:**

**To remediate using the UI:**

**Step 1 - Create two emergency access accounts:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com
2. Expand `Users` > `Active Users`
3. Click `Add user` and create a new user with this criteria:
    - Name the account in a way that does NOT identify it with a particular person.
    - Assign the account to the default `.onmicrosoft.com` domain and not the organization's.
    - The password must be at least 16 characters and generated randomly.
    - Do not assign a license.
    - Assign the user the `Global Administrator` role.
4. Repeat the above steps for the second account.

**Step 2 - Exclude at least one account from conditional access policies:**

1. Navigate `Microsoft Entra admin center` https://entra.microsoft.com/
2. Expand `Protection` > `Conditional Access`.
3. Inspect the conditional access policies.
4. For each rule add an exclusion for at least one of the emergency access accounts.
5. `Users` > `Exclude` > `Users and groups` and select one emergency access account.

**Step 3 - Ensure the necessary procedures and policies are in place:**

- In order for accounts to be effectively used in a break glass situation the proper policies and procedures must be authorized and distributed by senior management.
- FIDO2 Security Keys should be locked in a secure separate fireproof location.
- Passwords should be at least 16 characters, randomly generated and MAY be separated in multiple pieces to be joined on emergency.

**Warning:** As of 10/15/2024 MFA is required for all users including Break Glass Accounts. It is recommended to update these accounts to use passkey (FIDO2) or configure certificate-based authentication for MFA. Both methods satisfy the MFA requirement.

**Additional suggestions for emergency account management:**

- Create access reviews for these users.
- Exclude users from conditional access rules.
- Add the account to a restricted management administrative unit.

**Warning**: If CA (conditional access) exclusion is managed by a group, this group should be added to PIM for groups (licensing required) or be created as a role-assignable group. If it is a regular security group, then users with the Group Administrators role are able to bypass CA entirely.

**Default Value:**

Not defined.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-planning#stage-1-critical-items-to-do-right-now
2. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-restricted-management
4. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mandatory-multifactor-authentication#accounts

**Additional Information:**

Microsoft has additional instructions regarding using Azure Monitor to capture events in the Log Analytics workspace, and then generate alerts for Emergency Access accounts. This requires an Azure subscription but should be strongly considered as a method of monitoring activity on these accounts:

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access#monitor-sign-in-and-audit-logs

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.1 Establish and Maintain an Inventory of Accounts<br>Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | ● | ● | ● |

## *1.1.3 (L1) Ensure that between two and four global admins are designated (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Between two and four global administrators should be designated in the tenant. Ideally, these accounts will not have licenses assigned to them which supports additional controls found in this benchmark.

**Rationale:**

If there is only one global administrator, they could perform malicious activities without being detected by another admin. Designating multiple global administrators eliminates this risk and ensures redundancy if the sole remaining global administrator leaves the organization.

However, to minimize the attack surface, there should be no more than four global admins set for any tenant. A large number of global admins increases the likelihood of a successful account breach by an external attacker.

**Impact:**

The potential impact associated with ensuring compliance with this requirement is dependent upon the current number of global administrators configured in the tenant. If there is only one global administrator in a tenant, an additional global administrator will need to be identified and configured. If there are more than four global administrators, a review of role requirements for current global administrators will be required to identify which of the users require global administrator access.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft 365 admin center` https://admin.microsoft.com
2. Select `Roles` > `Role assignments`.
3. Select the `Global Administrator` role from the list and click on `Assigned`.
4. Review the list of Global Administrators.
    - If there are groups present, then inspect each group and its members.
    - Take note of the total number of Global Administrators in and outside of groups.
5. Ensure the number of Global Administrators is between two and four.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes Directory.Read.All`
2. Run the following PowerShell script:

```
# Determine Id of GA role using the immutable RoleTemplateId value.
$GlobalAdminRole = Get-MgDirectoryRole -Filter "RoleTemplateId eq '62e90394-
69f5-4237-9190-012177145e10'"
$RoleMembers = Get-MgDirectoryRoleMember -DirectoryRoleId $GlobalAdminRole.Id

$GlobalAdmins = [System.Collections.Generic.List[Object]]::new()
foreach ($object in $RoleMembers) {
    $Type = $object.AdditionalProperties.'@odata.type'
    # Check for and process role assigned groups
    if ($Type -eq '#microsoft.graph.group') {
        $GroupId = $object.Id
        $GroupMembers = (Get-MgGroupMember -GroupId
$GroupId).AdditionalProperties

        foreach ($member in $GroupMembers) {
            if ($member.'@odata.type' -eq '#microsoft.graph.user') {
                $GlobalAdmins.Add([PSCustomObject][Ordered]@{
                        DisplayName       = $member.displayName
                        UserPrincipalName = $member.userPrincipalName
                    })
            }
        }
    } elseif ($Type -eq '#microsoft.graph.user') {
        $DisplayName = $object.AdditionalProperties.displayName
        $UPN = $object.AdditionalProperties.userPrincipalName
        $GlobalAdmins.Add([PSCustomObject][Ordered]@{
                DisplayName       = $DisplayName
                UserPrincipalName = $UPN
            })
    }
}

$GlobalAdmins = $GlobalAdmins | select DisplayName,UserPrincipalName -Unique
Write-Host "*** There are" $GlobalAdmins.Count "Global Administrators in the
organization."
```

3. Review the output and ensure there are between 2 and 4 Global Administrators.

**Note:** When tallying the number of Global Administrators, the above does not account for Partner relationships. Those are located under `Settings` > `Partner Relationships` and should be reviewed on a reoccurring basis.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft 365 admin center` https://admin.microsoft.com
2. Select `Users` > `Active Users`.
3. In the `Search` field enter the name of the user to be made a Global Administrator.
4. To create a new Global Admin:
    1. Select the user's name.
    2. A window will appear to the right.
    3. Select `Manage roles`.
    4. Select `Admin center access`.
    5. Check `Global Administrator`.
    6. Click `Save changes`.
5. To remove Global Admins:
    1. Select User.
    2. Under `Roles` select `Manage roles`
    3. De-Select the appropriate role.
    4. Click `Save changes`.

**References:**

1. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.directorymanagement/get-mgdirectoryrole?view=graph-powershell-1.0
2. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#all-roles
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices#5-limit-the-number-of-global-administrators-to-less-than-5

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.1 Establish and Maintain an Inventory of Accounts<br>Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | ● | ● | ● |
| v7 | 4.1 Maintain Inventory of Administrative Accounts<br>Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. | | ● | ● |

### *1.1.4 (L1) Ensure administrative accounts use licenses with a reduced application footprint (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Administrative accounts are special privileged accounts that could have varying levels of access to data, users, and settings. A license can enable an account to gain access to a variety of different applications, depending on the license assigned.

The recommended state is to not license a privileged account or use licenses without associated applications such as `Microsoft Entra ID P1` or `Microsoft Entra ID P2`.

**Rationale:**

Ensuring administrative accounts do not use licenses with applications assigned to them will reduce the attack surface of high privileged identities in the organization's environment. Granting access to a mailbox or other collaborative tools increases the likelihood that privileged users might interact with these applications, raising the risk of exposure to social engineering attacks or malicious content. These activities should be restricted to an unprivileged 'daily driver' account.

**Note:** In order to participate in Microsoft 365 security services such as Identity Protection, PIM and Conditional Access an administrative account will need a license attached to it. Ensure that the license used does not include any applications with potentially vulnerable services by using either **Microsoft Entra ID P1** or **Microsoft Entra ID P2** for the cloud-only account with administrator roles.

**Impact:**

Administrative users will be required to switch accounts and use manual login/logout procedures when performing privileged tasks. This change also means they will not benefit from Single Sign-On (SSO), potentially impacting workflow efficiency and user experience.

**Note:** Alerts will be sent to **TenantAdmins**, including Global Administrators, by default. To ensure proper receipt, configure alerts to be sent to security or operations staff with valid email addresses or a security operations center. Otherwise, after adoption of this recommendation, alerts sent to **TenantAdmins** may go unreceived due to the lack of an application-based license assigned to the Global Administrator accounts.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com.
2. Click to expand `Users` select `Active users`.
3. Sort by the `Licenses` column.
4. For each user account in an administrative role verify the account is assigned a license that is not associated with applications i.e. (Microsoft Entra ID P1, Microsoft Entra ID P2).
    - If an organization uses PIM to elevate a daily driver account to privileged levels, this control and licensing requirement can be considered satisfied.

**Note:** The final step assumes PIM is properly configured to best practices. Accounts eligible for the Global Administrator role should require approval to activate. Using the PIM blade to permanently assign accounts to privileged roles would not satisfy this audit procedure.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "RoleManagement.Read.Directory","User.Read.All"`
2. Run the following PowerShell script:

```
$DirectoryRoles = Get-MgDirectoryRole

# Get privileged role IDs
$PrivilegedRoles = $DirectoryRoles | Where-Object {
    $_.DisplayName -like "*Administrator*" -or $_.DisplayName -eq "Global
Reader"
}

# Get the members of these various roles
$RoleMembers = $PrivilegedRoles | ForEach-Object { Get-MgDirectoryRoleMember
-DirectoryRoleId $_.Id } |
    Select-Object Id -Unique

# Retrieve details about the members in these roles
$PrivilegedUsers = $RoleMembers | ForEach-Object {
    Get-MgUser -UserId $_.Id -Property UserPrincipalName, DisplayName, Id
}

$Report = [System.Collections.Generic.List[Object]]::new()

foreach ($Admin in $PrivilegedUsers) {
    $License = $null
    $License = (Get-MgUserLicenseDetail -UserId $Admin.id).SkuPartNumber -
join ", "
    $Object = [pscustomobject][ordered]@{
        DisplayName           = $Admin.DisplayName
        UserPrincipalName     = $Admin.UserPrincipalName
        License               = $License
    }
    $Report.Add($Object)
}

$Report
```

3. The output will display users assigned privileged roles alongside their assigned licenses. Additional manual assessment is required to determine if the licensing is appropriate for the user.

**Remediation:**

**To remediate using the UI:**

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

**Note:** Utilizing PIM to best practices will satisfy this control. CIS and Microsoft recommend an organization keep zero permanently active assignments for roles other than emergency access accounts.

**Default Value:**

N/A

**References:**

1. https://learn.microsoft.com/en-us/microsoft-365/enterprise/protect-your-global-administrator-accounts?view=o365-worldwide
2. https://learn.microsoft.com/en-us/entra/fundamentals/whatis#what-are-the-microsoft-entra-id-licenses
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference
4. https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-protect-admin-accounts?view=o365-worldwide
5. https://learn.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings?view=o365-worldwide#licenses
6. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-deployment-plan#principle-of-least-privilege

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts<br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. | ● | ● | ● |
| v7 | 4.1 Maintain Inventory of Administrative Accounts<br>Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. | | ● | ● |

## 1.2 Teams & groups

### *1.2.1 (L2) Ensure that only organizationally managed/approved public groups exist (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Microsoft 365 Groups is the foundational membership service that drives all teamwork across Microsoft 365. With Microsoft 365 Groups, you can give a group of people access to a collection of shared resources. When a new group is created in the Administration panel, the default privacy value of the group is "Public". (In this case, ‘public’ means accessible to the identities within the organization without requiring group owner authorization to join.)

Ensure that Microsoft 365 Groups are set to `Private` in the Administration panel.

**Note:** Although there are several different group types, this recommendation concerns Microsoft 365 Groups specifically.

**Rationale:**

If group privacy is not controlled, any user may access sensitive information, depending on the group they try to access.

When the privacy value of a group is set to "Public," users may access data related to this group (e.g. SharePoint) via three methods:

1. The Azure Portal: Users can add themselves to the public group via the Azure Portal; however, administrators are notified when users access the Portal.
2. Access Requests: Users can request to join the group via the Groups application in the Access Panel. This provides the user with immediate access to the group, even though they are required to send a message to the group owner when requesting to join.
3. SharePoint URL: Users can directly access a group via its SharePoint URL, which is usually guessable and can be found in the Groups application within the Access Panel.

**Impact:**

If the recommendation is applied, group owners could receive more access requests than usual, especially regarding groups originally meant to be public.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com.
2. Click to expand `Teams & groups` select `Active teams & groups`.
3. On the **Active teams and groups page**, check that no groups have the status 'Public' in the privacy column.

**To audit using PowerShell:**

1. Connect to the Microsoft Graph service using `Connect-MgGraph -Scopes "Group.Read.All"`.
2. Run the following Microsoft Graph PowerShell command:

```
Get-MgGroup -All | where {$_.Visibility -eq "Public"} | select
DisplayName,Visibility
```

3. Ensure `Visibility` is `Private` for each group.

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

Public when created from the Administration portal; private otherwise.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management
2. https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v7 | 13.1 Maintain an Inventory Sensitive Information<br>Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider. | ● | ● | ● |

### *1.2.2 (L1) Ensure sign-in to shared mailboxes is blocked (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Shared mailboxes are used when multiple people need access to the same mailbox, such as a company information or support email address, reception desk, or other function that might be shared by multiple people.

Users with permissions to the group mailbox can send as or send on behalf of the mailbox email address if the administrator has given that user permissions to do that. This is particularly useful for help and support mailboxes because users can send emails from "Contoso Support" or "Building A Reception Desk."

Shared mailboxes are created with a corresponding user account using a system generated password that is unknown at the time of creation.

The recommended state is `Sign in blocked` for `Shared mailboxes`.

**Rationale:**

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

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com/
2. Click to expand `Teams & groups` and select `Shared mailboxes`.
3. Take note of all shared mailboxes.
4. Click to expand `Users` and select `Active users`.
5. Select a shared mailbox account to open its properties pane, and review.
6. Ensure the text under the name reads `Sign-in blocked`.
7. Repeat for any additional shared mailboxes.

**Note:** If sign-in is not blocked there will be an option to `Block sign-in`. This means the shared mailbox is out of compliance with this recommendation.

**To audit using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`
2. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "User.Read.All"`
3. Run the following PowerShell commands:

```
$MBX = Get-EXOMailbox -RecipientTypeDetails SharedMailbox -ResultSize
Unlimited
$MBX | ForEach-Object { Get-MgUser -UserId $_.ExternalDirectoryObjectId `
    -Property DisplayName, UserPrincipalName, AccountEnabled } |
    Format-Table DisplayName, UserPrincipalName, AccountEnabled
```

4. Ensure `AccountEnabled` is set to `False` for all Shared Mailboxes.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "User.ReadWrite.All"`
2. Connect to Exchange Online using `Connect-ExchangeOnline`.
3. To disable sign-in for a single account:

```
$MBX = Get-EXOMailbox -Identity TestUser@example.com
Update-MgUser -UserId $MBX.ExternalDirectoryObjectId -AccountEnabled:$false
```

3. The following will block sign-in to all Shared Mailboxes.

```
$MBX = Get-EXOMailbox -RecipientTypeDetails SharedMailbox
$MBX | ForEach-Object { Update-MgUser -UserId $_.ExternalDirectoryObjectId -
AccountEnabled:$false }
```

**Default Value:**

AccountEnabled: `True`

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## 1.3 Settings

### *1.3.1 (L1) Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)' (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Rationale:**

Organizations such as NIST and Microsoft have updated their password policy recommendations to not arbitrarily require users to change their passwords after a specific amount of time, unless there is evidence that the password is compromised, or the user forgot it. They suggest this even for single factor (Password Only) use cases, with a reasoning that forcing arbitrary password changes on users actually make the passwords less secure. Other recommendations within this Benchmark suggest the use of MFA authentication for at least critical accounts (at minimum), which makes password expiration even less useful as well as password protection for Entra ID.

**Impact:**

When setting passwords not to expire it is important to have other controls in place to supplement this setting. See below for related recommendations and user guidance.

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

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand Settings select Org Settings.
3. Click on Security & privacy.
4. Select Password expiration policy ensure that Set passwords to never expire (recommended) has been checked.

**To audit using PowerShell:**

1. Connect to the Microsoft Graph service using Connect-MgGraph -Scopes "Domain.Read.All".
2. Run the following Microsoft Online PowerShell command:

```
Get-MgDomain | ft id,PasswordValidityPeriodInDays
```

3. Verify the value returned for valid domains is 2147483647

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand Settings select Org Settings.
3. Click on Security & privacy.
4. Check the Set passwords to never expire (recommended) box.
5. Click Save.

**To remediate using PowerShell:**

1. Connect to the Microsoft Graph service using Connect-MgGraph -Scopes "Domain.ReadWrite.All".
2. Run the following Microsoft Graph PowerShell command:

```
Update-MgDomain -DomainId <Domain> -PasswordValidityPeriodInDays 2147483647
```

**Default Value:**

If the property is not set, a default value of 90 days will be used

**References:**

1. https://pages.nist.gov/800-63-3/sp800-63b.html
2. https://www.cisecurity.org/white-papers/cis-password-policy-guide/
3. https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.2 Use Unique Passwords<br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | ● | ● | ● |
| v7 | 4.4 Use Unique Passwords<br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system. | | ● | ● |

## *1.3.2 (L2) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

A managed device is considered a device managed by Intune MDM or joined to a domain (Entra ID or Hybrid joined).

The following Microsoft 365 web apps are supported.

- Outlook Web App
- OneDrive
- SharePoint
- Microsoft Fabric
- Microsoft365.com and other start pages
- Microsoft 365 web apps (Word, Excel, PowerPoint)
- Microsoft 365 Admin Center
- M365 Defender Portal
- Microsoft Purview Compliance Portal

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

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

**Rationale:**

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

**Impact:**

If step 2 in the Audit/Remediation procedure is left out, then there is no issue with this from a security standpoint. However, it will require users on trusted devices to sign in more frequently which could result in credential prompt fatigue.

Users don’t get signed out in these cases:

- If they get single sign-on (SSO) into the web app from the device joined account.
- If they selected Stay signed in at the time of sign-in. For more info on hiding this option for your organization, see Add branding to your organization's sign-in page.
- If they're on a managed device, that is compliant or joined to a domain and using a supported browser, like Microsoft Edge, or Google Chrome with the Microsoft Single Sign On extension.

**Note:** Idle session timeout also affects the Azure Portal idle timeout if this is not explicitly set to a different timeout. The Azure Portal idle timeout applies to all kind of devices, not just unmanaged. See : change the directory timeout setting admin

**Audit:**

**Step 1 - Ensure Idle session timeout is configured:**

**To audit using the UI:**

1. Navigate to the `Microsoft 365 admin center` https://admin.microsoft.com/.
2. Click to expand `Settings` Select `Org settings`.
3. Click `Security & Privacy` tab.
4. Select `Idle session timeout`.
5. Verify `Turn on to set the period of inactivity for users to be signed off of Microsoft 365 web apps` is set to `3 hours` (or less).

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`:
2. Run the following script:

```
$TimeoutPolicy = Get-MgPolicyActivityBasedTimeoutPolicy
$BenchmarkTimeSpan = [TimeSpan]::Parse('03:00:00') # 3 hours

if ($TimeoutPolicy) {
    $PolicyDefinition = $TimeoutPolicy.Definition | ConvertFrom-Json
    $Timeout =
$PolicyDefinition.ActivityBasedTimeoutPolicy.ApplicationPolicies[0].WebSessio
nIdleTimeout
    $TimeSpan = [TimeSpan]::Parse($Timeout)
    $TimeoutReadable = "{0} days, {1} hours, {2} minutes" `
        -f $TimeSpan.Days, $TimeSpan.Hours, $TimeSpan.Minutes
    if ($TimeSpan -le $BenchmarkTimeSpan) {
        Write-Host "** PASS ** Timeout is set to $TimeoutReadable."
    } else {
        Write-Host "** FAIL ** Timeout is too long. It is set to
$TimeoutReadable."
    }
} else {
    Write-Host "** FAIL **: Idle session timeout is not configured."
}
```

3. Verify the policy exists and is `3 hours` or less.

**Step 2 - Ensure the Conditional Access policy is in place:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Expand `Protect` > `Conditional Access`.
3. Inspect existing conditional access rules for one that meets the below conditions:
    - `Users` is set to `All users`.
    - `Cloud apps or actions` > `Select apps` is set to `Office 365`.
    - `Conditions` > `Client apps` is `Browser` and nothing else.
    - `Session` is set to `Use app enforced restrictions`.
    - `Enable Policy` is set to `On`

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`:
2. Run the following script:

```
$Caps = Get-MgIdentityConditionalAccessPolicy -All |
    Where-Object {
$_.SessionControls.ApplicationEnforcedRestrictions.IsEnabled }
$CapReport = [System.Collections.Generic.List[Object]]::new()
# Filter to policies with "Use app enforced restrictions" enabled

# Loop through policies and generate a per policy report.
foreach ($policy in $Caps) {
    $Name = $policy.DisplayName
    $Users = $policy.Conditions.Users.IncludeUsers
    $Targets = $policy.Conditions.Applications.IncludeApplications
    $ClientApps = $policy.Conditions.ClientAppTypes
    $Restrictions =
$policy.SessionControls.ApplicationEnforcedRestrictions.IsEnabled
    $State = $policy.State

    $CountPass = $Targets.count -eq 1 -and $ClientApps.count -eq 1
    $Pass = $Targets -eq 'Office365' -and $ClientApps -eq 'browser' -and
            $Restrictions -and $CountPass -and $State -eq 'enabled'

    $obj = [PSCustomObject]@{
        DisplayName             = $Name
        AuditState              = if ($Pass) { "PASS" } else { "FAIL" }
        IncludeUsers            = $Users
        IncludeApplications     = $Targets
        ClientAppTypes          = $ClientApps
        AppEnforcedRestrictions = $Restrictions
        State                   = $State
    }
    $CapReport.Add($obj)
}

if ($Caps) {
    $CapReport
} else {
    Write-Host "** FAIL **: There are no qualifying conditional access
policies."
}
```

3. The script will output qualifying Conditional Access Policies. If one policy passes, then the recommendation passes. A passing policy will have the following properties:

```
DisplayName             : (CIS) Idle timeout for unmanaged
AuditState              : PASS
IncludeUsers            : {All}   # IncludeUsers not currently scored
IncludeApplications     : {Office365}
ClientAppTypes          : {browser}
AppEnforcedRestrictions : True
State                   : enabled
```

**Note:** Both steps 1 and 2 must pass audit checks in order for the recommendation to pass as a whole.

**Remediation:**

**Step 1 - Configure Idle session timeout:**

**To remediate using the UI:**

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

**Step 2 - Ensure the Conditional Access policy is in place:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Expand `Protect` > `Conditional Access`.
3. Click `New policy` and give the policy a name.
    - Select `Users` > `All users`.
    - Select `Cloud apps or actions` > `Select apps` and select `Office 365`
    - Select `Conditions` > `Client apps` > `Yes` check only `Browser` unchecking all other boxes.
    - Select `Sessions` and check `Use app enforced restrictions`.
4. Set `Enable policy` to `On` and click `Create`.

**Note:** To ensure that idle timeouts affect only unmanaged devices, both steps 1 and 2 must be completed. Otherwise managed devices will also be impacted by the timeout policy.

**Default Value:**

Not configured. (Idle sessions will not timeout.)

**References:**

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

**Additional Information:**

According to Microsoft idle session timeout isn't supported when third party cookies are disabled in the browser. Users won't see any sign-out prompts.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.3 Configure Automatic Session Locking on Enterprise Assets<br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. | ● | ● | ● |

## *1.3.3 (L2) Ensure 'External sharing' of calendars is not available (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

This functionality is not widely used. As a result, it is unlikely that implementation of this setting will cause an impact to most users. Users that do utilize this functionality are likely to experience a minor inconvenience when scheduling meetings or synchronizing calendars with people outside the tenant.

**Audit:**

**To audit using the UI:**

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

**To audit using PowerShell:**

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

```
Get-SharingPolicy -Identity "Default Sharing Policy" | ft Name,Enabled
```

3. Verify `Enabled` is set to `False`

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
Set-SharingPolicy -Identity "Default Sharing Policy" -Enabled $False
```

**Default Value:**

Enabled (True)

**References:**

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

**Additional Information:**

**The following script can be used to audit any mailboxes that might be sharing calendars prior to disabling the feature globally:**

```
$mailboxes = Get-Mailbox -ResultSize Unlimited

foreach ($mailbox in $mailboxes) {
    # Get the name of the default calendar folder (depends on the mailbox's
language)
    $calendarFolder = [string](Get-ExoMailboxFolderStatistics
$mailbox.PrimarySmtpAddress -FolderScope Calendar| Where-Object {
$_.FolderType -eq 'Calendar' }).Name

    # Get users calendar folder settings for their default Calendar folder
    # calendar has the format identity:\<calendar folder name>
    $calendar = Get-MailboxCalendarFolder -Identity
"$($mailbox.PrimarySmtpAddress):\$calendarFolder"

    if ($calendar.PublishEnabled) {
        Write-Host -ForegroundColor Yellow "Calendar publishing is enabled
for $($mailbox.PrimarySmtpAddress) on $($calendar.PublishedCalendarUrl)"
    }
}
```

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v7 | 14.6 Protect Information through Access Control Lists<br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

### *1.3.4 (L1) Ensure 'User owned apps and services' is restricted (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

By default, users can install add-ins in their Microsoft Word, Excel, and PowerPoint applications, allowing data access within the application.

Do not allow users to install add-ins in Word, Excel, or PowerPoint.

**Rationale:**

Attackers commonly use vulnerable and custom-built add-ins to access data in user applications.

While allowing users to install add-ins by themselves does allow them to easily acquire useful add-ins that integrate with Microsoft applications, it can represent a risk if not used and monitored carefully.

Disable future user's ability to install add-ins in Microsoft Word, Excel, or PowerPoint helps reduce your threat-surface and mitigate this risk.

**Impact:**

Implementation of this change will impact both end users and administrators. End users will not be able to install add-ins that they may want to install.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com.
2. Click to expand `Settings` > `Org settings`.
3. In `Services` select `User owned apps and services`.
4. Verify `Let users access the Office Store` and `Let users start trials on behalf of your organization` are **not checked**.

**To Audit using PowerShell:**

1. Connect to the Microsoft Graph service using `Connect-MgGraph -Scopes "OrgSettings-AppsAndServices.Read.All"`.
2. Run the following Microsoft Graph PowerShell command:

```
$Uri = "https://graph.microsoft.com/beta/admin/appsAndServices/settings"
Invoke-MgGraphRequest -Uri $Uri
```

3. Ensure both `isOfficeStoreEnabled` and `isAppAndServicesTrialEnabled` are `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand Settings > Org settings.
3. In Services select User owned apps and services.
4. Uncheck Let users access the Office Store and Let users start trials on behalf of your organization.
5. Click Save.

**To remediate using PowerShell**

1. Connect to the Microsoft Graph service using Connect-MgGraph -Scopes "OrgSettings-AppsAndServices.ReadWrite.All".
2. Run the following Microsoft Graph PowerShell commands:

```
$uri = "https://graph.microsoft.com/beta/admin/appsAndServices"
$body = @{
    "Settings" = @{
        "isAppAndServicesTrialEnabled" = $false
        "isOfficeStoreEnabled"         = $false
    }
} | ConvertTo-Json
Invoke-MgGraphRequest -Method PATCH -Uri $uri -Body $body
```

**Default Value:**

Let users access the Office Store is Checked

Let users start trials on behalf of your organization is Checked

**References:**

1. https://learn.microsoft.com/en-us/microsoft-365/admin/manage/manage-addins-in-the-admin-center?view=o365-worldwide#manage-add-in-downloads-by-turning-onoff-the-office-store-across-all-apps-except-outlook

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v7 | 5.1 Establish Secure Configurations<br>Maintain documented, standard security configuration standards for all authorized operating systems and software. | ● | ● | ● |

### *1.3.5 (L1) Ensure internal phishing protection for Forms is enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Microsoft Forms can be used for phishing attacks by asking personal or sensitive information and collecting the results. Microsoft 365 has built-in protection that will proactively scan for phishing attempt in forms such personal information request.

**Rationale:**

Enabling internal phishing protection for Microsoft Forms will prevent attackers using forms for phishing attacks by asking personal or other sensitive information and URLs.

**Impact:**

If potential phishing was detected, the form will be temporarily blocked and cannot be distributed, and response collection will not happen until it is unblocked by the administrator or keywords were removed by the creator.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 admin` center https://admin.microsoft.com.
2. Click to expand `Settings` then select `Org settings`.
3. Under Services select `Microsoft Forms`.
4. Ensure the checkbox labeled `Add internal phishing protection` is checked under `Phishing protection`.

**To Audit using PowerShell:**

1. Connect to the Microsoft Graph service using `Connect-MgGraph -Scopes "OrgSettings-Forms.Read.All"`.
2. Run the following Microsoft Graph PowerShell commands:

```
$uri = 'https://graph.microsoft.com/beta/admin/forms/settings'
Invoke-MgGraphRequest -Uri $uri | select isInOrgFormsPhishingScanEnabled
```

3. Ensure `isInOrgFormsPhishingScanEnabled` is 'True'.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com.
2. Click to expand `Settings` then select `Org settings`.
3. Under Services select `Microsoft Forms`.
4. Click the checkbox labeled `Add internal phishing protection` under `Phishing protection`.
5. Click Save.

**To remediate using PowerShell**

1. Connect to the Microsoft Graph service using `Connect-MgGraph -Scopes "OrgSettings-AppsAndServices.ReadWrite.All"`.
2. Run the following Microsoft Graph PowerShell commands:

```
$uri = 'https://graph.microsoft.com/beta/admin/forms/settings'
$body = @{ "isInOrgFormsPhishingScanEnabled" = $true } | ConvertTo-Json
Invoke-MgGraphRequest -Method PATCH -Uri $uri -Body $body
```

**Default Value:**

Internal Phishing Protection is enabled.

**References:**

1. https://learn.microsoft.com/en-US/microsoft-forms/administrator-settings-microsoft-forms
2. https://learn.microsoft.com/en-US/microsoft-forms/review-unblock-forms-users-detected-blocked-potential-phishing

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.1 Deploy and Maintain Anti-Malware Software<br>Deploy and maintain anti-malware software on all enterprise assets. | ● | ● | ● |
| v8 | 14.2 Train Workforce Members to Recognize Social Engineering Attacks<br>Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating. | ● | ● | ● |

## *1.3.6 (L2) Ensure the customer lockbox feature is enabled (Automated)*

**Profile Applicability:**

- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

Administrators will need to grant Microsoft access to the tenant environment prior to a Microsoft engineer accessing the environment for support or troubleshooting.

**Audit:**

**To audit using the UI:**

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

**To audit using SecureScore:**

1. Navigate to the Microsoft 365 SecureScore portal. https://securescore.microsoft.com
2. Search for `Turn on customer lockbox feature` under `Improvement actions`.

**To audit using PowerShell:**

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

```
Get-OrganizationConfig | Select-Object CustomerLockBoxEnabled
```

3. Verify the value is set to `True`.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
Set-OrganizationConfig -CustomerLockBoxEnabled $true
```

**Default Value:**

`Require approval for all data access requests` - `Unchecked`

`CustomerLockboxEnabled` - `False`

**References:**

1. https://learn.microsoft.com/en-us/purview/customer-lockbox-requests#turn-customer-lockbox-requests-on-or-off

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

### *1.3.7 (L2) Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web' (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

Ensure `Microsoft 365 on the web` third-party storage services are restricted.

**Rationale:**

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

**Impact:**

Impact associated with this change is highly dependent upon current practices in the tenant. If users do not use other storage providers, then minimal impact is likely. However, if users do regularly utilize providers outside of the tenant this will affect their ability to continue to do so.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com
2. Go to `Settings` > `Org Settings` > `Services` > `Microsoft 365 on the web`
3. Ensure `Let users open files stored in third-party storage services in Microsoft 365 on the web` is not checked.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Application.Read.All"`.
2. Run the following script:

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

if ((-not $SP) -or $SP.AccountEnabled) {
    Write-Host "Audit Result: ** FAIL **"
} else {
    Write-Host "Audit Result: ** PASS **"
}
```

3. To pass `AccountEnabled` must be `False`.

**Note:** The check will also fail if the Service Principal does not exist as users will still be able to open files stored in third-party storage services in Microsoft 365 on the web.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Application.ReadWrite.All"`
2. Run the following script:

```
$SP = Get-MgServicePrincipal -Filter "appId eq 'c1f33bc0-bdb4-4248-ba9b-
096807ddb43e'"
# If the service principal doesn't exist then create it first.
if (-not $SP) {
    $SP = New-MgServicePrincipal -AppId "c1f33bc0-bdb4-4248-ba9b-
096807ddb43e"
}

Update-MgServicePrincipal -ServicePrincipalId $SP.Id -AccountEnabled:$false
```

**Default Value:**

Enabled - Users are able to open files stored in third-party storage services

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v7 | 13.1 Maintain an Inventory Sensitive Information<br>Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider. | ● | ● | ● |
| v7 | 13.4 Only Allow Access to Authorized Cloud Storage or Email Providers<br>Only allow access to authorized cloud storage or email providers. | | ● | ● |

## *1.3.8 (L2) Ensure that Sways cannot be shared with people outside of your organization (Manual)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Sway is a Microsoft 365 app that lets organizations create interactive, web-based presentations using images, text, videos and other media. Its design engine simplifies the process, allowing for quick customization. Presentations can then be shared via a link.

This setting controls user Sway sharing capability, both within and outside of the organization. By default, Sway is enabled for everyone in the organization.

**Rationale:**

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

**Impact:**

Interactive reports, presentations, newsletters, and other items created in Sway will not be shared outside the organization by users.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com.
2. Click to expand `Settings` then select `Org settings`.
3. Under Services select `Sway`.
4. Confirm that under `Sharing` the following is not checked
    - Option: `Let people in your organization share their sways with people outside your organization`.

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

Let people in your organization share their sways with people outside your organization - Enabled

**References:**

1. https://support.microsoft.com/en-us/office/administrator-settings-for-sway-d298e79b-b6ab-44c6-9239-aa312f5784d4
2. https://learn.microsoft.com/en-us/office365/servicedescriptions/microsoft-sway-service-description

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v7 | 13.1 Maintain an Inventory Sensitive Information<br>Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider. | ● | ● | ● |

### *1.3.9 (L1) Ensure shared bookings paged are restricted to select users (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**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. It contains various settings to define services, manage staff members, configure schedules and availability, business hours and customize how appointments are scheduled. These pages can be customized to fit the diverse needs of your organization. It is an extension of Person Bookings.

The recommended state is to restrict the `OwaMailboxPolicy-Default` policy or disable at the organization level.

**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.

Additionally, attackers may create authoritative-looking addresses (e.g., admin@, hostmaster@) to conduct social engineering attacks on external parties aimed at the transfer of infrastructure control.

To reduce this risk, access to Shared Bookings should be limited to users with a clear business need and subject to monitoring and governance.

**Impact:**

Disabling Shared Bookings will limit users' ability to create self-service scheduling pages, which may reduce convenience for teams that rely on automated meeting coordination. Approved users will need to be added to a separate OWA Policy which will increase administrative overhead.

**Note:** Before modifying the default owa policy, ensure that any users who rely on Shared Bookings are assigned a separate policy that explicitly allows its use. This will help prevent unintended service disruptions.

**Audit:**

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:**

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

```
Get-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default | fl
BookingsMailboxCreationEnabled
```

3. Ensure `BookingsMailboxCreationEnabled` is set to `False`.

**Optionally:** If Bookings is disabled at the organization level, this is also considered a compliant state.

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

```
Get-OrganizationConfig | fl BookingsEnabled
```

3. If `BookingsEnabled` is set to `False`, the organization is using a more restrictive and compliant configuration. In this case changing the default OWA policy would not be required for compliance.

**Remediation:**

**To remediate using PowerShell:**

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

```
Set-OwaMailboxPolicy "OwaMailboxPolicy-Default" -
BookingsMailboxCreationEnabled:$false
```

**Optionally:** For a more restrictive state Bookings can be disabled at the organization level

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

```
Set-OrganizationConfig -BookingsEnabled $false
```

**Note:** Disabling Bookings at the tenant (organization) level will be more impactful to end users and is not required for compliance.

**Default Value:**

BookingsMailboxCreationEnabled : True (OwaMailboxPolicy-Default)

BookingsEnabled : True

**References:**

1. https://learn.microsoft.com/en-us/microsoft-365/bookings/turn-bookings-on-or-off?view=o365-worldwide
2. https://techcommunity.microsoft.com/blog/office365businessappsblog/enhancing-security-in-microsoft-bookings-best-practices-for-admins/4382447
3. https://learn.microsoft.com/en-us/microsoft-365/bookings/best-practices-shared-bookings?view=o365-worldwide&source=recommendations
4. https://www.cyberis.com/article/microsoft-bookings-facilitating-impersonation

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

# 2 Microsoft 365 Defender

Microsoft 365 Defender, also known as Security, contains settings relating to policies, rules, and security controls that are common to many Microsoft 365 applications.

Direct link: https://security.microsoft.com/

## 2.1 Email & collaboration

## *2.1.1 (L2) Ensure Safe Links for Office Applications is Enabled (Automated)*

**Profile Applicability:**

- E5 Level 2

**Description:**

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

**Note:** E5 Licensing includes a number of Built-in Protection policies. When auditing policies note which policy you are viewing, and keep in mind CIS recommendations often extend the Default or Built-in Policies provided by MS. In order to **Pass** the highest priority policy must match all settings recommended.

**Rationale:**

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

**Impact:**

User impact associated with this change is minor - users may experience a very short delay when clicking on URLs in Office documents before being directed to the requested site. Users should be informed of the change as, in the event a link is unsafe and blocked, they will receive a message that it has been blocked.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com
2. Under `Email & collaboration` select `Policies & rules`
3. Select `Threat policies` then `Safe Links`
4. Inspect each policy and attempt to identify one that matches the parameters outlined below.
5. Scroll down the pane and click on `Edit Protection settings` (Global Readers will look for on or off values)
6. Ensure the following protection settings are set as outlined:

   **Email**

   - Checked `On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default`
   - Checked `Apply Safe Links to email messages sent within the organization`
   - Checked `Apply real-time URL scanning for suspicious links and links that point to files`
   - Checked `Wait for URL scanning to complete before delivering the message`
   - Unchecked `Do not rewrite URLs, do checks via Safe Links API only.`

   **Teams**

   - Checked `On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten`

   **Office 365 Apps**

   - Checked `On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps. URLs are not rewritten`

   **Click protection settings**

   - Checked `Track user clicks`
   - Unchecked `Let users click through the original URL`
7. There is no recommendation for organization branding.
8. Click close

**To audit using PowerShell:**

1. Connect using `Connect-ExchangeOnline`.
2. Run the following to output properties from all Safe Links policies:

```
$params = @(
    'Identity',
    'EnableSafeLinksForEmail',
    'EnableSafeLinksForTeams',
    'EnableSafeLinksForOffice',
    'TrackClicks',
    'AllowClickThrough',
    'ScanUrls',
    'EnableForInternalSenders',
    'DeliverMessageAfterScan',
    'DisableUrlRewrite'
)

Get-SafeLinksPolicy | Select-Object -Property $Params
```

3. Verify there is at least one policy that matches the properties and values below:

```
Identity                  : <Example CIS SafeLinks Policy>
EnableSafeLinksForEmail   : True
EnableSafeLinksForTeams   : True
EnableSafeLinksForOffice  : True
TrackClicks               : True
AllowClickThrough         : False
ScanUrls                  : True
EnableForInternalSenders  : True
DeliverMessageAfterScan   : True
DisableUrlRewrite         : False
```

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com
2. Under `Email & collaboration` select `Policies & rules`
3. Select `Threat policies` then `Safe Links`
4. Click on `+Create`
5. Name the policy then click `Next`
6. In `Domains` select all valid domains for the organization and `Next`
7. Ensure the following `URL & click protection settings` are defined:

   **Email**

   - Checked `On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default`
   - Checked `Apply Safe Links to email messages sent within the organization`
   - Checked `Apply real-time URL scanning for suspicious links and links that point to files`
   - Checked `Wait for URL scanning to complete before delivering the message`
   - Unchecked `Do not rewrite URLs, do checks via Safe Links API only.`

   **Teams**

   - Checked `On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten`

   **Office 365 Apps**

   - Checked `On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office apps. URLs are not rewritten`

   **Click protection settings**

   - Checked `Track user clicks`
   - Unchecked `Let users click through the original URL`
   - There is no recommendation for organization branding.
8. Click `Next` twice and finally `Submit`

**To remediate using PowerShell:**

1. Connect using `Connect-ExchangeOnline`.
2. Run the following PowerShell script to create a policy at highest priority that will apply to all valid domains on the tenant:

```
# Create the Policy
$params = @{
    Name = "CIS SafeLinks Policy"
    EnableSafeLinksForEmail = $true
    EnableSafeLinksForTeams = $true
    EnableSafeLinksForOffice = $true
    TrackClicks = $true
    AllowClickThrough = $false
    ScanUrls = $true
    EnableForInternalSenders = $true
    DeliverMessageAfterScan = $true
    DisableUrlRewrite = $false

}

New-SafeLinksPolicy @params

# Create the rule for all users in all valid domains and associate with
Policy
New-SafeLinksRule -Name "CIS SafeLinks" -SafeLinksPolicy "CIS SafeLinks
Policy" -RecipientDomainIs (Get-AcceptedDomain).Name -Priority 0
```

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.1 Deploy and Maintain Anti-Malware Software<br>Deploy and maintain anti-malware software on all enterprise assets. | ● | ● | ● |
| v7 | 7.4 Maintain and Enforce Network-Based URL Filters<br>Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not. | | ● | ● |

## *2.1.2 (L1) Ensure the Common Attachment Types Filter is enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

The Common Attachment Types Filter lets a user block known and custom malicious file types from being attached to emails.

**Rationale:**

Blocking known malicious file types can help prevent malware-infested files from infecting a host.

**Impact:**

Blocking common malicious file types should not cause an impact in modern computing environments.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules`.
3. On the Policies & rules page select `Threat policies`.
4. Under **Policies** select `Anti-malware` and click on the `Default (Default)` policy.
5. On the policy page that appears on the righthand pane, under `Protection settings`, verify that the `Enable the common attachments filter` has the value of `On`.

**To audit using PowerShell:**

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

```
Get-MalwareFilterPolicy -Identity Default | Select-Object EnableFileFilter
```

3. Verify `EnableFileFilter` is set to `True`.

**Note:** Audit and Remediation guidance may focus on the **Default policy** however, if a Custom Policy exists in the organization's tenant, then ensure the setting is set as outlined in the highest priority policy listed.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules`.
3. On the Policies & rules page select `Threat policies`.
4. Under polices select `Anti-malware` and click on the `Default (Default)` policy.
5. On the Policy page that appears on the right hand pane scroll to the bottom and click on `Edit protection settings`, check the `Enable the common attachments filter`.
6. Click Save.

**To remediate using PowerShell:**

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

```
Set-MalwareFilterPolicy -Identity Default -EnableFileFilter $true
```

**Note:** Audit and Remediation guidance may focus on the **Default policy** however, if a Custom Policy exists in the organization's tenant, then ensure the setting is set as outlined in the highest priority policy listed.

**Default Value:**

Always on

**References:**

1. https://learn.microsoft.com/en-us/powershell/module/exchange/get-malwarefilterpolicy?view=exchange-ps
2. https://learn.microsoft.com/en-us/defender-office-365/anti-malware-policies-configure?view=o365-worldwide

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.6 Block Unnecessary File Types<br>Block unnecessary file types attempting to enter the enterprise's email gateway. | | ● | ● |
| v7 | 7.9 Block Unnecessary File Types<br>Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business. | | ● | ● |
| v7 | 8.1 Utilize Centrally Managed Anti-malware Software<br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | | ● | ● |

## *2.1.3 (L1) Ensure notifications for internal users sending malware is Enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Exchange Online Protection (EOP) is Microsoft's cloud-based filtering service that protects organizations against spam, malware, and other email threats. EOP is included in all Microsoft 365 organizations with Exchange Online mailboxes.

EOP uses flexible anti-malware policies for malware protection settings. These policies can be set to notify Admins of malicious activity.

**Rationale:**

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

**Impact:**

Notification of account with potential issues should not have an impact on the user.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `E-mail & Collaboration` select `Policies & rules`.
3. On the Policies & rules page select `Threat policies`.
4. Under Policies select `Anti-malware`.
5. Click on the `Default (Default)` policy.
6. Ensure the setting `Notify an admin about undelivered messages from internal senders` is set to `On` and that there is at least one email address under `Administrator email address`.

**To audit using PowerShell:**

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

```
Get-MalwareFilterPolicy | fl Identity,
EnableInternalSenderAdminNotifications, InternalSenderAdminAddress
```

3. Ensure `EnableInternalSenderAdminNotifications` is set to `True` and a `InternalSenderAdminAddress` address is defined.

**Note:** Audit and Remediation guidance may focus on the **Default policy** however, if a Custom Policy exists in the organization's tenant, then ensure the setting is set as outlined in the highest priority policy listed.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
Set-MalwareFilterPolicy -Identity '{Identity Name}' -
EnableInternalSenderAdminNotifications $True -InternalSenderAdminAddress
{admin@domain1.com}
```

**Note:** Audit and Remediation guidance may focus on the **Default policy** however, if a Custom Policy exists in the organization's tenant, then ensure the setting is set as outlined in the highest priority policy listed.

**Default Value:**

```
EnableInternalSenderAdminNotifications : False
InternalSenderAdminAddress             : $null
```

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/anti-malware-protection-about
2. https://learn.microsoft.com/en-us/defender-office-365/anti-malware-policies-configure

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 17.5 Assign Key Roles and Responsibilities<br>Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | | ● | ● |
| v7 | 7.1 Ensure Use of Only Fully Supported Browsers and Email Clients<br>Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor. | ● | ● | ● |
| v7 | 8.1 Utilize Centrally Managed Anti-malware Software<br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | | ● | ● |

## *2.1.4 (L2) Ensure Safe Attachments policy is enabled (Automated)*

**Profile Applicability:**

- E5 Level 2

**Description:**

The Safe Attachments policy helps protect users from malware in email attachments by scanning attachments for viruses, malware, and other malicious content. When an email attachment is received by a user, Safe Attachments will scan the attachment in a secure environment and provide a verdict on whether the attachment is safe or not.

**Rationale:**

Enabling Safe Attachments policy helps protect against malware threats in email attachments by analyzing suspicious attachments in a secure, cloud-based environment before they are delivered to the user's inbox. This provides an additional layer of security and can prevent new or unseen types of malware from infiltrating the organization's network.

**Impact:**

Delivery of email with attachments may be delayed while scanning is occurring.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `E-mail & Collaboration` select `Policies & rules`.
3. On the Policies & rules page select `Threat policies`.
4. Under `Policies` select `Safe Attachments`.
5. Inspect the highest priority policy.
6. Ensure `Users and domains` and `Included recipient domains` are in scope for the organization.
7. Ensure `Safe Attachments detection response:` is set to `Block - Block current and future messages and attachments with detected malware`.
8. Ensure the `Quarantine Policy` is set to `AdminOnlyAccessPolicy`.
9. Ensure the policy is not disabled.

**To audit using PowerShell:**

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

```
Get-SafeAttachmentPolicy | ft Identity,Enable,Action,QuarantineTag
```

3. Inspect the highest priority safe attachments policy and ensure the properties and values match the below:

```
Enable        : True
Action        : Block
QuarantineTag : AdminOnlyAccessPolicy
```

**Note:** To view the priority for a policy the `Get-SafeAttachmentRule` must be used. Built-in policies will always have a priority of `lowest` while presets like strict and standard can be viewed with `Get-ATPProtectionPolicyRule`. Strict and standard presets always operate at a higher priority than custom policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `E-mail & Collaboration` select `Policies & rules`.
3. On the Policies & rules page select `Threat policies`.
4. Under `Policies` select `Safe Attachments`.
5. Click `+ Create`.
6. Create a Policy Name and Description, and then click `Next`.
7. Select all valid domains and click `Next`.
8. Select `Block`.
9. Quarantine policy is `AdminOnlyAccessPolicy`.
10. Leave `Enable redirect` unchecked.
11. Click `Next` and finally `Submit`.

**To remediate using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. To change an existing policy modify the example below and run the following PowerShell command:

```
Set-SafeAttachmentPolicy -Identity 'Example policy' -Action 'Block' -
QuarantineTag 'AdminOnlyAccessPolicy' -Enable $true
```

3. Or, edit and run the below example to create a new safe attachments policy.

```
New-SafeAttachmentPolicy -Name "CIS 2.1.4" -Enable $true -Action 'Block' -
QuarantineTag 'AdminOnlyAccessPolicy'

New-SafeAttachmentRule -Name "CIS 2.1.4 Rule" -SafeAttachmentPolicy "CIS
2.1.4" -RecipientDomainIs 'exampledomain[.]com'
```

**Note:** Policy targets such as users and domains should include domains, or groups that provide coverage for a majority of users in the organization. Different inclusion and exclusion use cases are not covered in the benchmark.

**Default Value:**

```
Identity      : Built-In Protection Policy
Enable        : True
Action        : Block
QuarantineTag : AdminOnlyAccessPolicy
Priority      : (lowest)
```

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-about
2. https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-policies-configure

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |
| v7 | 7.10 Sandbox All Email Attachments<br>Use sandboxing to analyze and block inbound email attachments with malicious behavior. | | | ● |
| v7 | 8.1 Utilize Centrally Managed Anti-malware Software<br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | | ● | ● |

## *2.1.5 (L2) Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled (Automated)*

**Profile Applicability:**

- E5 Level 2

**Description:**

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams scans these services for malicious files.

**Rationale:**

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

**Impact:**

Impact associated with Safe Attachments is minimal, and equivalent to impact associated with anti-virus scanners in an environment.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com
2. Under `Email & collaboration` select `Policies & rules`
3. Select Threat policies then `Safe Attachments`.
4. Click on `Global settings`
5. Ensure the toggle is `Enabled` to `Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams`.
6. Ensure the toggle is `Enabled` to `Turn on Safe Documents for Office clients`.
7. Ensure the toggle is `Deselected/Disabled` to `Allow people to click through Protected View even if Safe Documents identified the file as malicious`.

**To audit using PowerShell:**

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

```
Get-AtpPolicyForO365 | fl
Name,EnableATPForSPOTeamsODB,EnableSafeDocs,AllowSafeDocsOpen
```

Verify the values for each parameter as below:

```
EnableATPForSPOTeamsODB : True
EnableSafeDocs : True
AllowSafeDocsOpen : False
```

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com
2. Under `Email & collaboration` select `Policies & rules`
3. Select Threat policies then `Safe Attachments`.
4. Click on `Global settings`
5. Click to `Enable Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams`
6. Click to `Enable Turn on Safe Documents for Office clients`
7. Click to `Disable Allow people to click through Protected View even if Safe Documents identified the file as malicious`.
8. Click `Save`

**To remediate using PowerShell:**

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

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

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-for-spo-odfb-teams-about

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |
| v8 | 10.1 Deploy and Maintain Anti-Malware Software<br>Deploy and maintain anti-malware software on all enterprise assets. | ● | ● | ● |
| v7 | 7.10 Sandbox All Email Attachments<br>Use sandboxing to analyze and block inbound email attachments with malicious behavior. | | | ● |
| v7 | 8.1 Utilize Centrally Managed Anti-malware Software<br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | | ● | ● |

## *2.1.6 (L1) Ensure Exchange Online Spam Policies are set to notify administrators (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

In Microsoft 365 organizations with mailboxes in Exchange Online or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, email messages are automatically protected against spam (junk email) by EOP.

Configure Exchange Online Spam Policies to copy emails and notify someone when a sender in the organization has been blocked for sending spam emails.

**Rationale:**

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

**Impact:**

Notification of users that have been blocked should not cause an impact to the user.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules` > `Threat policies`.
3. Under Policies select `Anti-spam`.
4. Click on the `Anti-spam outbound policy (default)`.
5. Verify that `Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups` is set to `On`, ensure the email address is correct.
6. Verify that `Notify these users and groups if a sender is blocked due to sending outbound spam` is set to `On`, ensure the email address is correct.

**To audit using PowerShell:**

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

```
Get-HostedOutboundSpamFilterPolicy | Select-Object Bcc*, Notify*
```

3. Verify both `BccSuspiciousOutboundMail` and `NotifyOutboundSpam` are set to `True` and the email addresses to be notified are correct.

**Note:** Audit and Remediation guidance may focus on the **Default policy** however, if a Custom Policy exists in the organization's tenant, then ensure the setting is set as outlined in the highest priority policy listed.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
$BccEmailAddress = @("<INSERT-EMAIL>")

$NotifyEmailAddress = @("<INSERT-EMAIL>")

Set-HostedOutboundSpamFilterPolicy -Identity Default -
BccSuspiciousOutboundAdditionalRecipients $BccEmailAddress -
BccSuspiciousOutboundMail $true -NotifyOutboundSpam $true -
NotifyOutboundSpamRecipients $NotifyEmailAddress
```

**Note:** Audit and Remediation guidance may focus on the **Default policy** however, if a Custom Policy exists in the organization's tenant, then ensure the setting is set as outlined in the highest priority policy listed.

**Default Value:**

```
BccSuspiciousOutboundAdditionalRecipients : {}
BccSuspiciousOutboundMail                 : False
NotifyOutboundSpamRecipients              : {}
NotifyOutboundSpam                        : False
```

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/outbound-spam-protection-about

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 17.5 Assign Key Roles and Responsibilities<br>Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | | ● | ● |
| v7 | 7.9 Block Unnecessary File Types<br>Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business. | | ● | ● |
| v7 | 7.10 Sandbox All Email Attachments<br>Use sandboxing to analyze and block inbound email attachments with malicious behavior. | | | ● |

## *2.1.7 (L2) Ensure that an anti-phishing policy has been created (Automated)*

**Profile Applicability:**

- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

Mailboxes that are used for support systems such as helpdesk and billing systems send mail to internal users and are often not suitable candidates for impersonation protection. Care should be taken to ensure that these systems are excluded from Impersonation Protection.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules`
3. Select `Threat policies`.
4. Under Policies select `Anti-phishing`.
5. Ensure an AntiPhish policy exists that is `On` and meets the following criteria:
6. Under **Users, groups, and domains**.
    - Verify that the included domains and groups includes a majority of the organization.
7. Under **Phishing threshold & protection**
    - Verify `Phishing email threshold` is at least `3 - More Aggressive`.
    - Verify `User impersonation protection` is `On` and contains a subset of users.
    - Verify `Domain impersonation protection` is `On for owned domains`.
    - Verify `Mailbox intelligence` and `Mailbox intelligence for impersonations` and `Spoof intelligence` are `On`.
8. Under **Actions** review the following:
    - Verify `If a message is detected as user impersonation` is set to `Quarantine the message`.
    - Verify `If a message is detected as domain impersonation` is set to `Quarantine the message`.
    - Verify `If Mailbox Intelligence detects an impersonated user` is set to `Quarantine the message`.
    - Verify `First contact safety tip` is `On`.
    - Verify `User impersonation safety tip` is `On`.
    - Verify `Domain impersonation safety tip` is `On`.
    - Verify `Unusual characters safety tip` is `On`.
    - Verify `Honor DMARC record policy when the message is detected as spoof` is `On`.

**Note:** `DefaultFullAccessWithNotificationPolicy` is suggested but not required. Users will be notified that impersonation emails are in the Quarantine.

**To audit using PowerShell:**

1. Connect to Exchange Online service using `Connect-ExchangeOnline`.
2. Run the following Exchange Online PowerShell commands:

```
$params = @(
    "name","Enabled","PhishThresholdLevel","EnableTargetedUserProtection"
    "EnableOrganizationDomainsProtection","EnableMailboxIntelligence"
    "EnableMailboxIntelligenceProtection","EnableSpoofIntelligence"
    "TargetedUserProtectionAction","TargetedDomainProtectionAction"
    "MailboxIntelligenceProtectionAction","EnableFirstContactSafetyTips"
    "EnableSimilarUsersSafetyTips","EnableSimilarDomainsSafetyTips"
    "EnableUnusualCharactersSafetyTips","TargetedUsersToProtect"
    "HonorDmarcPolicy"
)

Get-AntiPhishPolicy | fl $params
```

3. Verify there is a policy created that has matching values for the following parameters:

```
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
TargetedUsersToProtect               : {<contains users>}
HonorDmarcPolicy                     : True
```

4. Verify that `TargetedUsersToProtect` contains a subset of the organization, up to 350 users, for targeted Impersonation Protection.
5. Use PowerShell to verify the AntiPhishRule is configured and enabled.

```
Get-AntiPhishRule |
ft AntiPhishPolicy,Priority,State,SentToMemberOf,RecipientDomainIs
```

6. Identity correct rule from the matching `AntiPhishPolicy` name in step 3. Ensure the rule defines groups or domains that include the majority of the organization by inspecting `SentToMemberOf` or `RecipientDomainIs`.

**Note:** Audit guidance is intended to help identify a qualifying AntiPhish policy+rule that meets the recommended criteria while protecting the majority of the organization. It's understood some individual user exceptions may exist or exceptions for the entire policy if another product stands in as an equivalent control.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules`
3. Select `Threat policies`.
4. Under Policies select `Anti-phishing` and click `Create`.
5. Name the policy, continuing and clicking `Next` as needed:
    - Add `Groups` and/or `Domains` that contain a majority of the organization.
    - Set `Phishing email threshold` to `3 - More Aggressive`
    - Check `Enable users to protect` and add up to 350 users.
    - Check `Enable domains to protect` and check `Include domains I own`.
    - Check `Enable mailbox intelligence (Recommended)`.
    - Check `Enable Intelligence for impersonation protection (Recommended)`.
    - Check `Enable spoof intelligence (Recommended).`
6. Under **Actions** configure the following:
    - Set `If a message is detected as user impersonation` to `Quarantine the message`.
    - Set `If a message is detected as domain impersonation` to `Quarantine the message`.
    - Set `If Mailbox Intelligence detects an impersonated user` to `Quarantine the message`.
    - Leave `Honor DMARC record policy when the message is detected as spoof` checked.
    - Check `Show first contact safety tip (Recommended)`.
    - Check `Show user impersonation safety tip`.
    - Check `Show domain impersonation safety tip`.
    - Check `Show user impersonation unusual characters safety tip`.
7. Finally click `Next` and `Submit` the policy.

**Note:** `DefaultFullAccessWithNotificationPolicy` is suggested but not required. Users will be notified that impersonation emails are in the Quarantine.

**To remediate using PowerShell:**

1. Connect to Exchange Online service using `Connect-ExchangeOnline`.
2. Run the following Exchange Online PowerShell script to create an AntiPhish policy:

```
# Create the Policy
$params = @{
    Name = "CIS AntiPhish Policy"
    PhishThresholdLevel = 3
    EnableTargetedUserProtection = $true
    EnableOrganizationDomainsProtection = $true
    EnableMailboxIntelligence = $true
    EnableMailboxIntelligenceProtection = $true
    EnableSpoofIntelligence = $true
    TargetedUserProtectionAction = 'Quarantine'
    TargetedDomainProtectionAction = 'Quarantine'
    MailboxIntelligenceProtectionAction = 'Quarantine'
    TargetedUserQuarantineTag = 'DefaultFullAccessWithNotificationPolicy'
    MailboxIntelligenceQuarantineTag =
'DefaultFullAccessWithNotificationPolicy'
    TargetedDomainQuarantineTag = 'DefaultFullAccessWithNotificationPolicy'
    EnableFirstContactSafetyTips = $true
    EnableSimilarUsersSafetyTips = $true
    EnableSimilarDomainsSafetyTips = $true
    EnableUnusualCharactersSafetyTips = $true
    HonorDmarcPolicy = $true
}

New-AntiPhishPolicy @params

# Create the rule for all users in all valid domains and associate with
Policy
New-AntiPhishRule -Name $params.Name -AntiPhishPolicy $params.Name -
RecipientDomainIs (Get-AcceptedDomain).Name -Priority 0
```

3. The new policy can be edited in the UI or via PowerShell.

**Note:** Remediation guidance is intended to help create a qualifying AntiPhish policy that meets the recommended criteria while protecting the majority of the organization. It's understood some individual user exceptions may exist or exceptions for the entire policy if another product acts as a similar control.

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-protection-about
2. https://learn.microsoft.com/en-us/defender-office-365/anti-phishing-policies-eop-configure

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |
| v7 | 7 Email and Web Browser Protections<br>Email and Web Browser Protections | | | |

## *2.1.8 (L1) Ensure that SPF records are published for all Exchange Domains (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

For each domain that is configured in Exchange, a corresponding Sender Policy Framework (SPF) record should be created.

**Rationale:**

SPF records allow Exchange Online Protection and other mail systems to know where messages from domains are allowed to originate. This information can be used by that system to determine how to treat the message based on if it is being spoofed or is valid.

**Impact:**

There should be minimal impact of setting up SPF records however, organizations should ensure proper SPF record setup as email could be flagged as spam if SPF is not setup appropriately.

**Audit:**

**To audit using PowerShell:**

1. Open a command prompt.
2. Type the following command in PowerShell:

```
Resolve-DnsName [domain1.com] txt | fl
```

3. Ensure that a value exists and that it includes `v=spf1 include:spf.protection.outlook.com`. This designates Exchange Online as a designated sender.

**To verify the SPF records are published, use the REST API for each domain:**

```
https://graph.microsoft.com/v1.0/domains/[DOMAIN.COM]/serviceConfigurationRecords
```

1. Ensure that a value exists that includes `v=spf1 include:spf.protection.outlook.com`. This designates Exchange Online as a designated sender.

**Note:** Resolve-DnsName is not available on older versions of Windows prior to Windows 8 and Server 2012.

**Remediation:**

**To remediate using a DNS Provider:**

1. If all email in your domain is sent from and received by Exchange Online, add the following TXT record for each Accepted Domain:

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

2. If there are other systems that send email in the environment, refer to this article for the proper SPF configuration: https://docs.microsoft.com/en-us/office365/SecurityCompliance/set-up-spf-in-office-365-to-help-prevent-spoofing.

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.5 Implement DMARC<br>To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards. | | ● | ● |
| v7 | 7.8 Implement DMARC and Enable Receiver-Side Verification<br>To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards. | | ● | ● |

## *2.1.9 (L1) Ensure that DKIM is enabled for all Exchange Online Domains (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

DKIM is one of the trio of Authentication methods (SPF, DKIM and DMARC) that help prevent attackers from sending messages that look like they come from your domain.

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

Use of DKIM in addition to SPF and DMARC to help prevent malicious actors using spoofing techniques from sending messages that look like they are coming from your domain.

**Rationale:**

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

**Impact:**

There should be no impact of setting up DKIM however, organizations should ensure appropriate setup to ensure continuous mail-flow.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft 365 Defender https://security.microsoft.com/
2. Expand Email & collaboration > Policies & rules > Threat policies.
3. Under Rules section click Email authentication settings.
4. Select DKIM
5. Click on each domain and confirm that Sign messages for this domain with DKIM signatures is Enabled and Status reads Signing DKIM signatures for this domain.
6. A status of Not signing DKIM signatures for this domain is an audit fail.

**Note:** For step 5 these can also be audited the overview showing all domains. In this case a passing audit procedure will be Toggle set as Enabled and Status as Valid.

**To audit using PowerShell:**

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

```
Get-DkimSigningConfig | Format-Table Name,Enabled,Status
```

3. For each domain verify that Enabled is True and Status is Valid.

**Remediation:**

**To remediate using a DNS Provider:**

1. For each accepted domain in Exchange Online, two DNS entries are required.

```
Host name:                      selector1._domainkey
Points to address or value:     selector1-
<domainGUID>._domainkey.<initialDomain>
TTL:                            3600
Host name:                      selector2._domainkey
Points to address or value:     selector2-
<domainGUID>._domainkey.<initialDomain>
TTL:                            3600
```

For Office 365, the selectors will always be `selector1` or `selector2`.

domainGUID is the same as the domainGUID in the customized MX record for your custom domain that appears before mail.protection.outlook.com. For example, in the following MX record for the domain contoso.com, the domainGUID is contoso-com:

```
contoso.com.  3600  IN  MX   5 contoso-com.mail.protection.outlook.com
```

The initial domain is the domain that you used when you signed up for Office 365. Initial domains always end with on.microsoft.com.

1. After the DNS records are created, enable DKIM signing in Defender.
2. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
3. Expand `Email & collaboration` > `Policies & rules` > `Threat policies`.
4. Under `Rules` section click `Email authentication settings`.
5. Select `DKIM`
6. Click on each domain and click `Enable` next to `Sign messages for this domain with DKIM signature`.

**Final remediation step using the Exchange Online PowerShell Module:**

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

```
Set-DkimSigningConfig -Identity < domainName > -Enabled $True
```

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.5 Implement DMARC<br>To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards. | | ● | ● |
| v7 | 7.8 Implement DMARC and Enable Receiver-Side Verification<br>To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards. | | ● | ● |

## *2.1.10 (L1) Ensure DMARC Records for all Exchange Online domains are published (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Rationale:**

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

Leaving a DMARC policy set to `p=none` can result in failed action when a spear phishing email fails DMARC but passes SPF and DKIM checks. Having DMARC fully configured is a critical part in preventing business email compromise.

**Impact:**

There should be no impact of setting up DMARC however, organizations should ensure appropriate setup to ensure continuous mail-flow.

**Audit:**

**To audit using PowerShell:**

1. Open a command prompt.
2. For each of the Accepted Domains in Exchange Online run the following in PowerShell:

```
Resolve-DnsName _dmarc.[domain1.com] txt
```

3. Ensure that the record exists and has at minimum the following flags defined as follows:

   `v=DMARC1;` (`p=quarantine` OR `p=reject`), `pct=100`, `rua=mailto:<reporting email address>` and `ruf=mailto:<reporting email address>`

The below example records would pass as they contain a policy that would either `quarantine` or `reject` messages failing DMARC, the policy affects 100% of mail `pct=100` as well as containing valid reporting addresses:

```
v=DMARC1; p=reject; pct=100; rua=mailto:rua@contoso.com;
ruf=mailto:ruf@contoso.com; fo=1

v=DMARC1; p=reject; pct=100; fo=1; ri=3600; rua=mailto:rua@contoso.com;
ruf=mailto:ruf@contoso.com

v=DMARC1; p=quarantine; pct=100; sp=none; fo=1; ri=3600;
rua=mailto:rua@contoso.com; ruf=ruf@contoso.com;
```

4. Ensure the Microsoft MOERA domain is also configured.

```
Resolve-DnsName _dmarc.[tenant].onmicrosoft.com txt
```

5. Ensure the record meets the same criteria listed in step #3.

**Note:** Resolve-DnsName is not available on older versions of Windows prior to Windows 8 and Server 2012.

**Remediation:**

**To remediate using a DNS Provider:**

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

```
Record:  _dmarc.domain1.com
Type:  TXT
Value:  v=DMARC1; p=none; rua=mailto:<rua-report@example.com>;
ruf=mailto:<ruf-report@example.com>
```

2. This will create a basic DMARC policy that will allow the organization to start monitoring message statistics.
3. One week is enough time for data generated by the reports to be useful in understanding email trends and traffic. The final step requires implementing a policy of `p=reject` OR `p=quarantine` and `pct=100` with the necessary `rua` and `ruf` email addresses defined:

```
Record:  _dmarc.domain1.com
Type:  TXT
Value:  v=DMARC1; p=reject; pct=100; rua=mailto:<rua-report@example.com>;
ruf=mailto:<ruf-report@example.com>
```

**Also remediate the MOREA domain using the UI:**

1. Navigate to the Microsoft 365 admin center https://admin.microsoft.com/
2. Expand `Settings` and select `Domains`.
3. Select your tenant domain (for example, contoso.onmicrosoft.com).
4. Select `DNS records` and click `+ Add record`.
5. Add a new record with the TXT name of `_dmarc` with the appropriate values outlined above.

**Note:** The remediation portion involves a multi-staged approach over a period of time. First, a baseline of the current state of email will be established with `p=none` and `rua` and `ruf`. Once the environment is better understood and reports have been analyzed an organization will move to the final state with dmarc record values as outlined in the audit section.

Microsoft has a list of best practices for implementing DMARC that cover these steps in detail.

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/email-authentication-dmarc-configure?view=o365-worldwide
2. https://learn.microsoft.com/en-us/defender-office-365/step-by-step-guides/how-to-enable-dmarc-reporting-for-microsoft-online-email-routing-address-moera-and-parked-domains?view=o365-worldwide
3. https://media.defense.gov/2024/May/02/2003455483/-1/-1/0/CSA-NORTH-KOREAN-ACTORS-EXPLOIT-WEAK-DMARC.PDF

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.5 Implement DMARC<br>To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards. | | ● | ● |
| v7 | 7.8 Implement DMARC and Enable Receiver-Side Verification<br>To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards. | | ● | ● |

## *2.1.11 (L2) Ensure comprehensive attachment filtering is applied (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

The Common Attachment Types Filter lets a user block known and custom malicious file types from being attached to emails. The policy provided by Microsoft covers 53 extensions, and an additional custom list of extensions can be defined.

The list of 184 extensions provided in this recommendation is comprehensive but not exhaustive.

**Rationale:**

Blocking known malicious file types can help prevent malware-infested files from infecting a host or performing other malicious attacks such as phishing and data extraction.

Defining a comprehensive list of attachments can help protect against additional unknown and known threats. Many legacy file formats, binary files and compressed files have been used as delivery mechanisms for malicious software. Organizations can protect themselves from Business E-mail Compromise (BEC) by allow-listing only the file types relevant to their line of business and blocking all others.

**Impact:**

For file types that are business necessary users will need to use other organizationally approved methods to transfer blocked extension types between business partners.

**Audit:**

For this control, a Level 2 comprehensive attachment policy is defined as one that includes at least 120 extensions. The 184 extensions included are a known vector for malicious activity. To pass, organizations must demonstrate at least a 90% adoption rate of the extension list referenced in the script below, with allowances for justified exceptions. Since individual extensions are not assigned specific risk weights, exceptions should be based on documented business needs.

**Note:** Utilizing the UI for auditing Anti-malware policies can be very time consuming so it is recommended to use a script like the one supplied below.

**To Audit using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Run the following script:

```
$AttachExts = @(
    "7z", "a3x", "ace", "ade", "adp", "ani", "app", "appinstaller",
    "applescript", "application", "appref-ms", "appx", "appxbundle", "arj",
    "asd", "asx", "bas", "bat", "bgi", "bz2", "cab", "chm", "cmd", "com",
    "cpl", "crt", "cs", "csh", "daa", "dbf", "dcr", "deb",
    "desktopthemepackfile", "dex", "diagcab", "dif", "dir", "dll", "dmg",
    "doc", "docm", "dot", "dotm", "elf", "eml", "exe", "fxp", "gadget", "gz",
    "hlp", "hta", "htc", "htm", "html", "hwpx", "ics", "img",
    "inf", "ins", "iqy", "iso", "isp", "jar", "jnlp", "js", "jse", "kext",
    "ksh", "lha", "lib", "library-ms", "lnk", "lzh", "macho", "mam", "mda",
    "mdb", "mde", "mdt", "mdw", "mdz", "mht", "mhtml", "mof", "msc", "msi",
    "msix", "msp", "msrcincident", "mst", "ocx", "odt", "ops", "oxps", "pcd",
    "pif", "plg", "pot", "potm", "ppa", "ppam", "ppkg", "pps", "ppsm", "ppt",
    "pptm", "prf", "prg", "ps1", "ps11", "ps11xml", "ps1xml", "ps2",
    "ps2xml", "psc1", "psc2", "pub", "py", "pyc", "pyo", "pyw", "pyz",
    "pyzw", "rar", "reg", "rev", "rtf", "scf", "scpt", "scr", "sct",
    "searchConnector-ms", "service", "settingcontent-ms", "sh", "shb", "shs",
    "shtm", "shtml", "sldm", "slk", "so", "spl", "stm", "svg", "swf", "sys",
    "tar", "theme", "themepack", "timer", "uif", "url", "uue", "vb", "vbe",
    "vbs", "vhd", "vhdx", "vxd", "wbk", "website", "wim", "wiz", "ws", "wsc",
    "wsf", "wsh", "xla", "xlam", "xlc", "xll", "xlm", "xls", "xlsb", "xlsm",
    "xlt", "xltm", "xlw", "xnk", "xps", "xsl", "xz", "z"
)

$MalwareFilterPolicies = Get-MalwareFilterPolicy
$MalwareFilterRules = Get-MalwareFilterRule
# A policy must have at least 90% of the extensions in the reference list to
pass.
# This allows for some flexibility with exceptions.
$PassingValue = .90 # 90%
$FailThreshold = [int]($AttachExts.count * (1 - $PassingValue))

# Only evaluate policies that have more than 120 extensions defined
# so we don't output failures on policies that aren't specific to
# extension filtering.
$CompPolicies = $MalwareFilterPolicies | Where-Object { $_.FileTypes.Count -
gt 120 }
if (-not $CompPolicies) {
    Write-Output "## FAIL ## No comprehensive policies found to evaluate."
    return
}

$ExtensionReport = foreach ($policy in $CompPolicies) {
    $Missing = Compare-Object -ReferenceObject $AttachExts `
        -DifferenceObject $policy.FileTypes `
        -PassThru | Where-Object { $_.SideIndicator -eq '<=' }
    $FoundRule = $MalwareFilterRules |
        Where-Object { $_.MalwareFilterPolicy -eq $policy.Id }

    # Define passing conditions to determine if this policy passes all
checks.
    $Pass = ($Missing.Count -lt $FailThreshold) -and
            ($FoundRule.State -eq 'Enabled') -and
            ($policy.EnableFileFilter -eq $true)

    [PSCustomObject]@{
        PolicyName        = $policy.Identity
```

```
        IsCISCompliant    = $Pass
        EnableFileFilter  = $policy.EnableFileFilter
        State             = $FoundRule.State
        MissingCount      = $Missing.count
        MissingExtensions = $Missing -join ", "
        ExtensionCount    = $policy.FileTypes.count
    }
}

# Output results in various formats
$ExtensionReport | Format-Table -AutoSize
<# Optional: Export methods
$ExtensionReport | Out-GridView -Title "Attachment Filter results"
$ExtensionReport | Export-Csv -Path "2.1.11.csv" -NoTypeInformation
$ExtensionReport | ConvertTo-Json | Out-File -FilePath "2.1.11.json"
#>
```

3. Review the results, only policies with over 120 extensions defined will be evaluated. At the end of the script examples of different output formats are given.
4. A pass is given for the following conditions:
    - A single active policy exists that covers all file extensions listed except those defined as an exception by the organization.
    - The policy has a state of `Enabled.`
    - The `EnableFileFilter` property is set to `True`.
5. The report includes a `IsCISCompliant` property, where `True` indicates in compliance, allowing for up to 10% of the listed extensions to be missing as documented exceptions.

**Note:** Organizations should evaluate any extensions missing from the report to determine if they are valid exceptions.

**Note:** The audit procedure intentionally does not include the action taken for matched extensions, e.g. Reject with NDR or Quarantine the message. These are considered organization specific and are not scored. When `FileTypeAction` is not specified the action will default to `Reject the message with a non-delivery receipt (NDR)`. The Quarantine Policy is also considered organization specific.

**Remediation:**

**To Remediate using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Run the following script after editing `InternalSenderAdminAddress`:

```
# Create an attachment policy and associated rule. The rule is
# intentionally disabled allowing the org to enable it when ready

$Policy = @{
    Name             = "CIS L2 Attachment Policy"
    EnableFileFilter = $true
    ZapEnabled       = $true
    EnableInternalSenderAdminNotifications = $true
    InternalSenderAdminAddress = 'admin@contoso.com' # Change this.
}

$L2Extensions = @(
    "7z", "a3x", "ace", "ade", "adp", "ani", "app", "appinstaller",
    "applescript", "application", "appref-ms", "appx", "appxbundle", "arj",
    "asd", "asx", "bas", "bat", "bgi", "bz2", "cab", "chm", "cmd", "com",
    "cpl", "crt", "cs", "csh", "daa", "dbf", "dcr", "deb",
    "desktopthemepackfile", "dex", "diagcab", "dif", "dir", "dll", "dmg",
    "doc", "docm", "dot", "dotm", "elf", "eml", "exe", "fxp", "gadget", "gz",
    "hlp", "hta", "htc", "htm", "html", "hwpx", "ics", "img",
    "inf", "ins", "iqy", "iso", "isp", "jar", "jnlp", "js", "jse", "kext",
    "ksh", "lha", "lib", "library-ms", "lnk", "lzh", "macho", "mam", "mda",
    "mdb", "mde", "mdt", "mdw", "mdz", "mht", "mhtml", "mof", "msc", "msi",
    "msix", "msp", "msrcincident", "mst", "ocx", "odt", "ops", "oxps", "pcd",
    "pif", "plg", "pot", "potm", "ppa", "ppam", "ppkg", "pps", "ppsm", "ppt",
    "pptm", "prf", "prg", "ps1", "ps11", "ps11xml", "ps1xml", "ps2",
    "ps2xml", "psc1", "psc2", "pub", "py", "pyc", "pyo", "pyw", "pyz",
    "pyzw", "rar", "reg", "rev", "rtf", "scf", "scpt", "scr", "sct",
    "searchConnector-ms", "service", "settingcontent-ms", "sh", "shb", "shs",
    "shtm", "shtml", "sldm", "slk", "so", "spl", "stm", "svg", "swf", "sys",
    "tar", "theme", "themepack", "timer", "uif", "url", "uue", "vb", "vbe",
    "vbs", "vhd", "vhdx", "vxd", "wbk", "website", "wim", "wiz", "ws", "wsc",
    "wsf", "wsh", "xla", "xlam", "xlc", "xll", "xlm", "xls", "xlsb", "xlsm",
    "xlt", "xltm", "xlw", "xnk", "xps", "xsl", "xz", "z"
)

# Create the policy
New-MalwareFilterPolicy @Policy -FileTypes $L2Extensions
# Create the rule for all accepted domains
$Rule = @{
    Name = $Policy.Name
    Enabled = $false
    MalwareFilterPolicy = $Policy.Name
    RecipientDomainIs = (Get-AcceptedDomain).Name
    Priority = 0
}

New-MalwareFilterRule @Rule
```

3. When prepared enable the rule either through the UI or PowerShell.

**Note:** Due to the number of extensions the UI method is not covered. The objects can however be edited in the UI or manually added using the list from the script.

1. Navigate to `Microsoft Defender` at https://security.microsoft.com/
2. Browse to `Policies & rules` > `Threat policies` > `Anti-malware`.

**Default Value:**

The following extensions are blocked by default:

ace, ani, apk, app, appx, 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

**References:**

1. https://learn.microsoft.com/en-us/powershell/module/exchange/get-malwarefilterpolicy?view=exchange-ps
2. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure?view=o365-worldwide
3. https://learn.microsoft.com/en-us/office/compatibility/office-file-format-reference

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.6 Block Unnecessary File Types<br>Block unnecessary file types attempting to enter the enterprise's email gateway. | | ● | ● |
| v7 | 7.9 Block Unnecessary File Types<br>Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business. | | ● | ● |
| v7 | 8.1 Utilize Centrally Managed Anti-malware Software<br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | | ● | ● |

## *2.1.12 (L1) Ensure the connection filter IP allow list is not used (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

In Microsoft 365 organizations with Exchange Online mailboxes or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, connection filtering and the default connection filter policy identify good or bad source email servers by IP addresses. The key components of the default connection filter policy are **IP Allow List**, **IP Block List** and **Safe list**.

The recommended state is `IP Allow List` empty or undefined.

**Rationale:**

Without additional verification like mail flow rules, email from sources in the IP Allow List skips spam filtering and sender authentication (SPF, DKIM, DMARC) checks. This method creates a high risk of attackers successfully delivering email to the Inbox that would otherwise be filtered. Messages that are determined to be malware or high confidence phishing are filtered.

**Impact:**

This is the default behavior. IP Allow lists may reduce false positives, however, this benefit is outweighed by the importance of a policy which scans all messages regardless of the origin. This supports the principle of zero trust.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand Email & collaboration select Policies & rules > Threat policies.
3. Under Policies select Anti-spam.
4. Click on the Connection filter policy (Default).
5. Ensure IP Allow list contains no entries.

**To audit using PowerShell:**

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

```
Get-HostedConnectionFilterPolicy -Identity Default | fl IPAllowList
```

3. Ensure IPAllowList is empty or {}

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand Email & collaboration select Policies & rules> Threat policies.
3. Under Policies select Anti-spam.
4. Click on the Connection filter policy (Default).
5. Click Edit connection filter policy.
6. Remove any IP entries from Always allow messages from the following IP addresses or address range:.
7. Click Save.

**To remediate using PowerShell:**

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

```
Set-HostedConnectionFilterPolicy -Identity Default -IPAllowList @{}
```

**Default Value:**

IPAllowList : {}

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/connection-filter-policies-configure
2. https://learn.microsoft.com/en-us/defender-office-365/create-safe-sender-lists-in-office-365#use-the-ip-allow-list
3. https://learn.microsoft.com/en-us/defender-office-365/how-policies-and-protections-are-combined#user-and-tenant-settings-conflict

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |

## *2.1.13 (L1) Ensure the connection filter safe list is off (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

In Microsoft 365 organizations with Exchange Online mailboxes or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, connection filtering and the default connection filter policy identify good or bad source email servers by IP addresses. The key components of the default connection filter policy are **IP Allow List**, **IP Block List** and **Safe list**.

The safe list is a pre-configured allow list that is dynamically updated by Microsoft.

The recommended safe list state is: `Off` or `False`

**Rationale:**

Without additional verification like mail flow rules, email from sources in the IP Allow List skips spam filtering and sender authentication (SPF, DKIM, DMARC) checks. This method creates a high risk of attackers successfully delivering email to the Inbox that would otherwise be filtered. Messages that are determined to be malware or high confidence phishing are filtered.

The safe list is managed dynamically by Microsoft, and administrators do not have visibility into which sender are included. Incoming messages from email servers on the safe list bypass spam filtering.

**Impact:**

This is the default behavior. IP Allow lists may reduce false positives, however, this benefit is outweighed by the importance of a policy which scans all messages regardless of the origin. This supports the principle of zero trust.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand Email & collaboration select Policies & rules > Threat policies.
3. Under Policies select Anti-spam.
4. Click on the Connection filter policy (Default).
5. Ensure Safe list is Off.

**To audit using PowerShell:**

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

```
Get-HostedConnectionFilterPolicy -Identity Default | fl EnableSafeList
```

3. Ensure EnableSafeList is False

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft 365 Defender https://security.microsoft.com.
2. Click to expand Email & collaboration select Policies & rules> Threat policies.
3. Under Policies select Anti-spam.
4. Click on the Connection filter policy (Default).
5. Click Edit connection filter policy.
6. Uncheck Turn on safe list.
7. Click Save.

**To remediate using PowerShell:**

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

```
Set-HostedConnectionFilterPolicy -Identity Default -EnableSafeList $false
```

**Default Value:**

EnableSafeList : False

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/connection-filter-policies-configure
2. https://learn.microsoft.com/en-us/defender-office-365/create-safe-sender-lists-in-office-365#use-the-ip-allow-list
3. https://learn.microsoft.com/en-us/defender-office-365/how-policies-and-protections-are-combined#user-and-tenant-settings-conflict

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |

## *2.1.14 (L1) Ensure inbound anti-spam policies do not contain allowed domains (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Anti-spam protection is a feature of Exchange Online that utilizes policies to help to reduce the amount of junk email, bulk and phishing emails a mailbox receives. These policies contain lists to allow or block specific senders or domains.

- The allowed senders list
- The allowed domains list
- The blocked senders list
- The blocked domains list

The recommended state is: Do not define any `Allowed domains`

**Rationale:**

Messages from entries in the allowed senders list or the allowed domains list bypass most email protection (except malware and high confidence phishing) and email authentication checks (SPF, DKIM and DMARC). Entries in the allowed senders list or the allowed domains list create a high risk of attackers successfully delivering email to the Inbox that would otherwise be filtered. The risk is increased even more when allowing common domain names as these can be easily spoofed by attackers.

Microsoft specifies in its documentation that allowed domains should be used for testing purposes only.

**Impact:**

This is the default behavior. Allowed domains may reduce false positives, however, this benefit is outweighed by the importance of having a policy which scans all messages regardless of the origin. As an alternative consider sender based lists. This supports the principle of zero trust.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules` > `Threat policies`.
3. Under Policies select `Anti-spam`.
4. Inspect each **inbound anti-spam** policy
5. Ensure that `Allowed domains` does not contain any domain names.
6. Repeat as needed for any additional inbound anti-spam policy.

**To audit using PowerShell:**

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

```
Get-HostedContentFilterPolicy | ft Identity,AllowedSenderDomains
```

3. Ensure `AllowedSenderDomains` is undefined for each inbound policy.

**Note:** Each inbound policy must pass for this recommendation to be considered to be in a passing state.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules`> `Threat policies`.
3. Under Policies select `Anti-spam`.
4. Open each out of compliance inbound anti-spam policy by clicking on it.
5. Click `Edit allowed and blocked senders and domains`.
6. Select `Allow domains`.
7. Delete each domain from the domains list.
8. Click `Done` > `Save`.
9. Repeat as needed.

**To remediate using PowerShell:**

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

```
Set-HostedContentFilterPolicy -Identity <Policy name> -AllowedSenderDomains
@{}
```

Or, run this to remove allowed domains from all inbound anti-spam policies:

```
$AllowedDomains = Get-HostedContentFilterPolicy | Where-Object
{$_.AllowedSenderDomains}
$AllowedDomains | Set-HostedContentFilterPolicy -AllowedSenderDomains @{}
```

**Default Value:**

AllowedSenderDomains : {}

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/anti-spam-protection-about#allow-and-block-lists-in-anti-spam-policies

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |

## *2.1.15 (L1) Ensure outbound anti-spam message limits are in place (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

The default outbound anti-spam policy in Microsoft Defender automatically applies to all users and is designed to detect and limit suspicious email-sending behavior. The policy enforces limits based on both volume and spam detection. If a user sends too many emails too quickly or if a high percentage of their messages are flagged as spam, their ability to send email can be temporarily restricted. This helps prevent abuse from compromised accounts or inadvertent spam campaigns.

When these limits are exceeded, Microsoft routes the messages through a high-risk delivery pool to protect its IP reputation and notifies administrators through built-in alert policies.

The recommended state is:

- External: `Restrict sending to external recipients (per hour)` - `500`
- Internal: `Restrict sending to internal recipients (per hour)` - `1000`
- Daily: `Maximum recipient limit per day` - `1000`
- Action: `Over limit action` - `Restrict the user from sending mail`

**Rationale:**

Message limit settings help lessen the impact of a Business Email Compromise (BEC) by automatically restricting accounts that send unusually high volumes of email. This containment prevents compromised accounts from launching large-scale attacks and helps ensure the organization's email remains trusted and deliverable. Without these limits, excessive or suspicious outbound traffic could result in Microsoft blocking the organization's email, disrupting communication and damaging reputation.

**Impact:**

Enforcing message limits may result in legitimate users being temporarily blocked from sending email if their bulk messaging activity resembles spam or exceeds volume thresholds. This can disrupt business operations, delay communication, and require administrative effort to investigate and restore access. However, these adverse effects typically stem from a lack of planning around mass mailings. To avoid triggering these limits, Microsoft recommends sending bulk email through custom subdomains or third-party bulk email providers.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules` > `Threat policies`.
3. Under Policies select `Anti-spam` and click to open `Anti-spam outbound policy (Default)`.
4. Ensure the following settings are to the recommended level or more restrictive:
    - External: `Restrict sending to external recipients (per hour)` - `500`
    - Internal: `Restrict sending to internal recipients (per hour)` - `1000`
    - Daily: `Maximum recipient limit per day` - `1000`
    - Action: `Over limit action` - `Restrict the user from sending mail`
5. Ensure a monitored mailbox is configured as a recipient under `Notify these users and groups if a sender is blocked due to sending outbound spam`.

**To audit using PowerShell:**

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

```
$params = (
    'RecipientLimitExternalPerHour',
    'RecipientLimitInternalPerHour',
    'RecipientLimitPerDay',
    'ActionWhenThresholdReached'
)

Get-HostedOutboundSpamFilterPolicy -Identity Default | fl $params
```

3. Ensure that each of the following properties is set to the recommended value listed below or to a more restrictive value.

```
RecipientLimitExternalPerHour : 500
RecipientLimitInternalPerHour : 1000
RecipientLimitPerDay          : 1000
ActionWhenThresholdReached    : BlockUser
```

4. Ensure the property `NotifyOutboundSpamRecipients` contains a monitored mailbox.

**Note:** Microsoft's *Recommended Strict* values represent a more restrictive and also compliant configuration. These values 400, 800, and 800 align with the sequence above. For further details on Standard and Strict settings, refer to the references section.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules`> `Threat policies`.
3. Under Policies select `Anti-spam` and click to open `Anti-spam outbound policy (Default)`.
4. Select `Edit protection settings`.
5. Set the following settings to the recommended values, *or* more restrictive values.
   - External: `Set an external message limit` - `500`
   - Internal: `Set an internal message limit` - `1000`
   - Daily: `Set a daily message limit` - `1000`
   - Action: `Restriction placed on users who reach the message limit` - `Restrict the user from sending mail`
6. Ensure `Notify these users and groups if a sender is blocked due to sending outbound spam` contains a monitored mailbox.

**To remediate using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Change the example email addresses below and run the following PowerShell commands:

```
$params = @{
    RecipientLimitExternalPerHour = 500
    RecipientLimitInternalPerHour = 1000
    RecipientLimitPerDay = 1000
    ActionWhenThresholdReached = 'BlockUser'
    NotifyOutboundSpamRecipients =
@('admin@example.com','security@example.com')
}

Set-HostedOutboundSpamFilterPolicy -Identity 'Default' @params
```

**Default Value:**

```
RecipientLimitExternalPerHour : 0
RecipientLimitInternalPerHour : 0
RecipientLimitPerDay          : 0
ActionWhenThresholdReached    : BlockUserForToday
```

The value of `0` means the service defaults are being used. More information on sending limits is here: https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#sending-limits-1

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/outbound-spam-protection-about
2. https://learn.microsoft.com/en-us/defender-office-365/recommended-settings-for-eop-and-office365#outbound-spam-policy-settings
3. https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#sending-limits-1

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |

## 2.2 Cloud apps

This section contains recommendations for Microsoft Defender for Cloud apps

## *2.2.1 (L1) Ensure emergency access account activity is monitored (Manual)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Organizations should monitor sign-in and audit log activity from the emergency accounts and trigger notifications to other administrators. When you monitor the activity for emergency access accounts, you can verify these accounts are only used for testing or actual emergencies. You can use Azure Monitor, Microsoft Sentinel, Defender for Cloud Apps or other tools to monitor the sign-in logs and trigger email and SMS alerts to your administrators whenever emergency access accounts sign in.

This recommendation uses Defender for Cloud Apps Policies to alert on emergency access account activity.

The recommended state is to monitor `Activity type Log on` on break-glass or emergency access accounts.

**Rationale:**

Emergency access accounts should be used in very few scenarios, for example, the last Global Administrator has left the organization and the account is inaccessible. All activity on an emergency access account should be reviewed at the time of the event to ensure the sign on is legitimate and authorized.

**Impact:**

There is no real world impact to monitoring these accounts beyond allocating staff. The frequency of emergency account sign on should be so low that any activity raises a red flag that is treated with the highest priority.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com
2. Under the **Cloud Apps** section select `Policies` -> `Policy management`.
3. Locate a **privileged accounts** policy that meets the following criteria
   - Policy severity is `High severity`.
   - Category is `Privileged accounts`.
   - Act on `Single activity` is selected.
   - Under **Activities matching all of the following** verify:
   - Filter1: `Activity type equals Log on`
   - Filter2: `User Name equals` <Emergency access account> as `Any role`
   - Ensure all additional emergency access accounts are accounted for.
   - Under **Alerts**, verify alerting is configured.
4. Repeat this process for any additional emergency access or break-glass accounts in the organization. If matching policies do not exist, then the audit procedure is considered a fail.

**Note:** Multiple accounts can be monitored by a single policy or by separate policies.

**Note:** Emergency access account activity can be monitored in various ways. The audit procedure passes as long as all emergency access account activity is monitored.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com
2. Under the **Cloud Apps** section select `Policies` -> `Policy management`.
3. Click on `All policies` and then `Create policy` -> `Activity policy`.
4. Give the policy a name and set the following:
   - Policy severity to `High severity`.
   - Category to `Privileged accounts`.
   - Act on `Single activity`.
   - Click `Select a filter` -> `Activity type equals Log on`.
   - Click `Add a filter` -> `User Name equals` <Emergency access account> as `Any role`.
   - Ensure all emergency access accounts are added to this policy or another.
   - Select an alert method such as `Send alert as email`.

**Note:** Multiple accounts can be monitored by a single policy or by separate policies.

**Default Value:**

A policy to monitor emergency access accounts does not exist by default.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access#monitor-sign-in-and-audit-logs
2. https://learn.microsoft.com/en-us/defender-cloud-apps/control-cloud-apps-with-policies

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 8.2 Collect Audit Logs<br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. | ● | ● | ● |
| v7 | 16 Account Monitoring and Control<br>Account Monitoring and Control | | | |

## 2.3 Audit

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

## 2.4 System

## *2.4.1 (L1) Ensure Priority account protection is enabled and configured (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Identify *priority accounts* to utilize Microsoft 365's advanced custom security features. This is an essential tool to bolster protection for users who are frequently targeted due to their critical positions, such as executives, leaders, managers, or others who have access to sensitive, confidential, financial, or high-priority information.

Once these accounts are identified, several services and features can be enabled, including threat policies, enhanced sign-in protection through conditional access policies, and alert policies, enabling faster response times for incident response teams.

**Rationale:**

Enabling priority account protection for users in Microsoft 365 is necessary to enhance security for accounts with access to sensitive data and high privileges, such as CEOs, CISOs, CFOs, and IT admins. These priority accounts are often targeted by spear phishing or whaling attacks and require stronger protection to prevent account compromise.

To address this, Microsoft 365 and Microsoft Defender for Office 365 offer several key features that provide extra security, including the identification of incidents and alerts involving priority accounts and the use of built-in custom protections designed specifically for them.

**Audit:**

**To audit using the UI:**

*Audit with a 3-step process*

**Step 1: Verify Priority account protection is enabled:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Select `Settings` near the bottom of the left most panel.
3. Select `E-mail & collaboration` > `Priority account protection`
4. Ensure `Priority account protection` is set to `On`

**Step 2: Verify that priority accounts are identified and tagged accordingly:**

5. Select `User tags`
6. Select the `PRIORITY ACCOUNT` tag and click `Edit`
7. Verify the assigned members match the organization's defined priority accounts or groups.
8. Repeat the previous 2 steps for any additional tags identified, such as Finance or HR.

**Step 3: Ensure alerts are configured:**

9. Expand `E-mail & Collaboration` on the left column.
10. Select `Policies & rules` > `Alert policy`
11. Ensure at least two alert policies are configured to monitor priority accounts for the activities `Detected malware in an email message` and `Phishing email detected at time of delivery`. These alerts should meet the following criteria:
    - Severity: `High`
    - Category: `Threat management`
    - Mail Direction: `Inbound`
    - Recipient Tags: Includes `Priority account`

**Remediation:**

**To remediate using the UI:**

*Remediate with a 3-step process*

**Step 1: Enable Priority account protection in Microsoft 365 Defender:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Click to expand `System` select `Settings`.
3. Select `E-mail & Collaboration` > `Priority account protection`
4. Ensure `Priority account protection` is set to `On`

**Step 2: Tag priority accounts:**

5. Select User tags
6. Select the PRIORITY ACCOUNT tag and click Edit
7. Select Add members to add users, or groups. **Groups are recommended.**
8. Repeat the previous 2 steps for any additional tags needed, such as Finance or HR.
9. Next and Submit.

**Step 3: Configure E-mail alerts for Priority Accounts:**

10. Expand E-mail & Collaboration on the left column.
11. Select Policies & rules > Alert policy
12. Select New Alert Policy
13. Enter a valid policy Name & Description. Set Severity to High and Category to Threat management.
14. Set Activity is to Detected malware in an e-mail message
15. Mail direction is Inbound
16. Select Add Condition and User: recipient tags are
17. In the Selection option field add chosen priority tags such as Priority account.
18. Select Every time an activity matches the rule.
19. Next and verify valid recipient(s) are selected.
20. Next and select Yes, turn it on right away. Click Submit to save the alert.
21. Repeat steps 12 - 18 to create a 2nd alert for the Activity field Activity is: Phishing email detected at time of delivery

**Note:** Any additional activity types may be added as needed. Above are the minimum recommended.

**Default Value:**

By default, priority accounts are undefined.

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |

## *2.4.2 (L1) Ensure Priority accounts have 'Strict protection' presets applied (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Preset security policies have been established by Microsoft, utilizing observations and experiences within datacenters to strike a balance between the exclusion of malicious content from users and limiting unwarranted disruptions. These policies can apply to all, or select users and encompass recommendations for addressing spam, malware, and phishing threats. The policy parameters are pre-determined and non-adjustable.

`Strict protection` has the most aggressive protection of the 3 presets.

- EOP: Anti-spam, Anti-malware and Anti-phishing
- Defender: Spoof protection, Impersonation protection and Advanced phishing
- Defender: Safe Links and Safe Attachments

**NOTE: The preset security polices cannot target Priority account TAGS currently, groups should be used instead.**

**Rationale:**

Enabling priority account protection for users in Microsoft 365 is necessary to enhance security for accounts with access to sensitive data and high privileges, such as CEOs, CISOs, CFOs, and IT admins. These priority accounts are often targeted by spear phishing or whaling attacks and require stronger protection to prevent account compromise.

The implementation of stringent, pre-defined policies may result in instances of false positive, however, the benefit of requiring the end-user to preview junk email before accessing their inbox outweighs the potential risk of mistakenly perceiving a malicious email as safe due to its placement in the inbox.

**Impact:**

Strict policies are more likely to cause false positives in anti-spam, phishing, impersonation, spoofing and intelligence responses.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Select to expand `E-mail & collaboration`.
3. Select `Policies & rules` > `Threat policies`.
4. From here visit each section in turn: `Anti-phishing` `Anti-spam` `Anti-malware` `Safe Attachments` `Safe Links`
5. Ensure in each there is a policy named `Strict Preset Security Policy` which includes the organization's priority Accounts/Groups.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Select to expand `E-mail & collaboration`.
3. Select `Policies & rules` > `Threat policies` > `Preset security policies`.
4. Click to `Manage protection settings` for `Strict protection` preset.
5. For `Apply Exchange Online Protection` select at minimum `Specific recipients` and include the Accounts/Groups identified as Priority Accounts.
6. For `Apply Defender for Office 365 Protection` select at minimum `Specific recipients` and include the Accounts/Groups identified as Priority Accounts.
7. For `Impersonation protection` click `Next` and add valid e-mails or priority accounts both internal and external that may be subject to impersonation.
8. For `Protected custom domains` add the organization's domain name, along side other key partners.
9. Click `Next` and finally `Confirm`

**Default Value:**

By default, presets are not applied to any users or groups.

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/preset-security-policies?view=o365-worldwide
2. https://learn.microsoft.com/en-us/defender-office-365/priority-accounts-security-recommendations
3. https://learn.microsoft.com/en-us/defender-office-365/recommended-settings-for-eop-and-office365?view=o365-worldwide#impersonation-settings-in-anti-phishing-policies-in-microsoft-defender-for-office-365

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |
| v8 | 10.7 Use Behavior-Based Anti-Malware Software<br>Use behavior-based anti-malware software. | | ● | ● |

## *2.4.3 (L2) Ensure Microsoft Defender for Cloud Apps is enabled and configured (Manual)*

**Profile Applicability:**

- E5 Level 2

**Description:**

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB). It provides visibility into suspicious activity in Microsoft 365, enabling investigation into potential security issues and facilitating the implementation of remediation measures if necessary.

Some risk detection methods provided by Entra Identity Protection also require Microsoft Defender for Cloud Apps:

- Suspicious manipulation of inbox rules
- Suspicious inbox forwarding
- New country detection
- Impossible travel detection
- Activity from anonymous IP addresses
- Mass access to sensitive files

**Rationale:**

Security teams can receive notifications of triggered alerts for atypical or suspicious activities, see how the organization's data in Microsoft 365 is accessed and used, suspend user accounts exhibiting suspicious activity, and require users to log back in to Microsoft 365 apps after an alert has been triggered.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Click to expand `System` select `Settings` > `Cloud apps`.
3. Scroll to `Connected apps` and select `App connectors`.
4. Ensure that **Microsoft 365** and **Microsoft Azure** both show in the list as `Connected`.
5. Go to `Cloud Discovery` > `Microsoft Defender for Endpoint` and check if the integration is enabled.
6. Go to `Information Protection` > `Files` and verify `Enable file monitoring` is checked.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Click to expand `System` select `Settings` > `Cloud apps`.
3. Scroll to `Information Protection` and select `Files`.
4. Check `Enable file monitoring`.
5. Scroll up to `Cloud Discovery` and select `Microsoft Defender for Endpoint.`
6. Check `Enforce app access`, configure a Notification URL and `Save`.

**Note:** Defender for Endpoint requires a Defender for Endpoint license.

**Configure App Connectors:**

1. Scroll to `Connected apps` and select `App connectors`.
2. Click on `Connect an app` and select `Microsoft 365`.
3. Check all Azure and Office 365 boxes then click `Connect Office 365`.
4. Repeat for the `Microsoft Azure` application.

**Default Value:**

Disabled

**References:**

1. https://learn.microsoft.com/en-us/defender-cloud-apps/protect-office-365#connect-microsoft-365-to-microsoft-defender-for-cloud-apps
2. https://learn.microsoft.com/en-us/defender-cloud-apps/protect-azure#connect-azure-to-microsoft-defender-for-cloud-apps
3. https://learn.microsoft.com/en-us/defender-cloud-apps/best-practices
4. https://learn.microsoft.com/en-us/defender-cloud-apps/get-started
5. https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks

**Additional Information:**

Additional Microsoft 365 Defender features include:

- The option to use Defender for cloud apps as a reverse proxy, allowing for the application of access or session controls through the definition of a conditional access policy.
- The purchase and implementation of the "App Governance" add-on, which provides more precise control over OAuth app permissions and includes additional built-in policies.

A list of Defender for Cloud Apps built-in policies for Office 365 can be found at https://learn.microsoft.com/en-us/defender-cloud-apps/protect-office-365.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.1 Deploy and Maintain Anti-Malware Software<br>Deploy and maintain anti-malware software on all enterprise assets. | ● | ● | ● |
| v8 | 10.5 Enable Anti-Exploitation Features<br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™. | | ● | ● |
| v7 | 6.2 Activate audit logging<br>Ensure that local logging has been enabled on all systems and networking devices. | ● | ● | ● |
| v7 | 16 Account Monitoring and Control<br>Account Monitoring and Control | | | |

## *2.4.4 (L1) Ensure Zero-hour auto purge for Microsoft Teams is on (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Zero-hour auto purge (ZAP) is a protection feature that retroactively detects and neutralizes malware and high confidence phishing. When ZAP for Teams protection blocks a message, the message is blocked for everyone in the chat. The initial block happens right after delivery, but ZAP occurs up to 48 hours after delivery.

**Rationale:**

ZAP is intended to protect users that have received zero-day malware messages or content that is weaponized after being delivered to users. It does this by continually monitoring spam and malware signatures taking automated retroactive action on messages that have already been delivered.

**Impact:**

As with any anti-malware or anti-phishing product, false positives may occur.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Defender` https://security.microsoft.com/
2. Click to expand `System` select `Settings` > `Email & collaboration` > `Microsoft Teams protection`.
3. Ensure `Zero-hour auto purge (ZAP)` is set to `On (Default)`
4. Under `Exclude these participants` review the list of exclusions and ensure they are justified and within tolerance for the organization.

**To audit using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Run the following cmdlets:

```
Get-TeamsProtectionPolicy | fl ZapEnabled
Get-TeamsProtectionPolicyRule | fl ExceptIf*
```

3. Ensure `ZapEnabled` is `True`.
4. Review the list of exclusions and ensure they are justified and within tolerance for the organization. If nothing returns from the 2nd cmdlet then there are no exclusions defined.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Defender` https://security.microsoft.com/
2. Click to expand `System` select `Settings` > `Email & collaboration` > `Microsoft Teams protection`.
3. Set `Zero-hour auto purge (ZAP)` to `On (Default)`

**To remediate using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Run the following cmdlet:

```
Set-TeamsProtectionPolicy -Identity "Teams Protection Policy" -ZapEnabled
$true
```

**Default Value:**

On (Default)

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/zero-hour-auto-purge?view=o365-worldwide#zero-hour-auto-purge-zap-in-microsoft-teams
2. https://learn.microsoft.com/en-us/defender-office-365/mdo-support-teams-about?view=o365-worldwide#configure-zap-for-teams-protection-in-defender-for-office-365-plan-2

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.1 Deploy and Maintain Anti-Malware Software<br>Deploy and maintain anti-malware software on all enterprise assets. | ● | ● | ● |

# 3 Microsoft Purview

Microsoft Purview, also known as Compliance, contains settings related to all things compliance, data governance, information protection and risk management.

Direct link: https://compliance.microsoft.com/

## 3.1 Audit

### *3.1.1 (L1) Ensure Microsoft 365 audit log search is Enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

When audit log search is enabled in the Microsoft Purview compliance portal, user and admin activity within the organization is recorded in the audit log and retained for 180 days by default. However, some organizations may prefer to use a third-party security information and event management (SIEM) application to access their auditing data. In this scenario, a global admin can choose to turn off audit log search in Microsoft 365.

**Rationale:**

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

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Purview` https://purview.microsoft.com/
2. Select `Solutions` and then `Audit` to open the audit search.
3. Choose a date and time frame in the past 30 days.
4. Verify search capabilities (e.g. try searching for Activities as `Accessed file` and results should be displayed).

**To audit using PowerShell:**

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

```
Get-AdminAuditLogConfig | Select-Object UnifiedAuditLogIngestionEnabled
```

3. Ensure `UnifiedAuditLogIngestionEnabled` is set to `True`.

**Note:** If the `Get-AdminAuditLogConfig` cmdlet is executed while connected to both Security & Compliance PowerShell as well as Exchange Online PowerShell then `UnifiedAuditLogIngestionEnabled` will always display `False`. This depends on the orders the module were imported. If Security & Compliance is needed in the same session be sure to connect to it first, and then Exchange PowerShell second.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Purview` https://purview.microsoft.com/
2. Select `Solutions` and then `Audit` to open the audit search.
3. Click blue bar `Start recording user and admin activity`.
4. Click `Yes` on the dialog box to confirm.

**To remediate using PowerShell:**

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

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

**Default Value:**

180 days

**References:**

1. https://learn.microsoft.com/en-us/purview/audit-log-enable-disable?view=o365-worldwide&tabs=microsoft-purview-portal
2. https://learn.microsoft.com/en-us/powershell/module/exchange/set-adminauditlogconfig?view=exchange-ps
3. https://learn.microsoft.com/en-us/purview/audit-log-enable-disable?view=o365-worldwide&tabs=microsoft-purview-portal#verify-the-auditing-status-for-your-organization

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 8.2 Collect Audit Logs<br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. | ● | ● | ● |
| v7 | 6.2 Activate audit logging<br>Ensure that local logging has been enabled on all systems and networking devices. | ● | ● | ● |

## 3.2 Data loss protection

### *3.2.1 (L1) Ensure DLP policies are enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Rationale:**

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

**Impact:**

Enabling a Teams DLP policy will allow sensitive data in Exchange Online and SharePoint Online to be detected or blocked. Always ensure to follow appropriate procedures during testing and implementation of DLP policies based on organizational standards.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Purview` https://purview.microsoft.com/
2. Click `Solutions` > `Data loss prevention` and then `Policies`.
3. Verify that the organization is using policies applicable to the types data that is in their interest to protect.
4. Verify the policies are `On`.

**Note:** The types of policies an organization should implement to protect information are specific to their industry. However, certain types of information, such as credit card numbers, social security numbers, and certain personally identifiable information (PII), are universally important to safeguard across all industries.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Purview` https://purview.microsoft.com/
2. Click `Solutions` > `Data loss prevention` then `Policies`.
3. Click `Create policy`.
4. Create a policy that is specific to the types of data the organization wishes to protect.

**References:**

1. https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp?view=o365-worldwide

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.1 Establish and Maintain a Data Management Process<br>Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| v7 | 13 Data Protection<br>Data Protection | | | |
| v7 | 14.7 Enforce Access Control to Data through Automated Tools<br>Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system. | | | ● |

## *3.2.2 (L1) Ensure DLP policies are enabled for Microsoft Teams (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

The default Teams Data Loss Prevention (DLP) policy rule in Microsoft 365 is a preconfigured rule that is automatically applied to all Teams conversations and channels. The default rule helps prevent accidental sharing of sensitive information by detecting and blocking certain types of content that are deemed sensitive or inappropriate by the organization.

By default, the rule includes a check for the sensitive info type *Credit Card Number* which is pre-defined by Microsoft.

**Rationale:**

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

DLP rules are not one size fits all, but at a minimum something should be defined. The organization should identify sensitive information important to them and seek to intercept it using DLP.

**Impact:**

End-users may be prevented from sharing certain types of content, which may require them to adjust their behavior or seek permission from administrators to share specific content. Administrators may receive requests from end-users for permission to share certain types of content or to modify the policy to better fit the needs of their teams.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Purview` compliance portal https://purview.microsoft.com/
2. Under `Solutions` select `Data loss prevention` then `Policies`.
3. Locate the `Default policy for Teams`.
4. Verify the `Status` is `On`.
5. Verify `Locations` include `Teams chat and channel messages - All accounts`.
6. Verify `Policy settings` incudes the Default Teams DLP policy rule or one specific to the organization.

**Note:** If there is not a default policy for teams inspect existing policies starting with step 4. DLP rules are specific to the organization and each organization should take steps to protect the data that matters to them. The default teams DLP rule will only alert on Credit Card matches.

**To audit using PowerShell:**

1. Connect to the Security & Compliance PowerShell using `Connect-IPPSSession`.
2. Run the following to return policies that include Teams chat and channel messages:

```
$DlpPolicy = Get-DlpCompliancePolicy
$DlpPolicy | Where-Object {$_.Workload -match "Teams"} |
    ft Name,Mode,TeamsLocation*
```

3. If nothing returns, then there are no policies that include Teams and remediation is required.
4. For any returned policy verify `Mode` is set to `Enable`.
5. Verify `TeamsLocation` includes `All`.
6. Verify `TeamsLocationException` includes only permitted exceptions.

**Note:** Some tenants may not have a default policy for teams as Microsoft started creating these by default at a particular point in time. In this case a new policy will have to be created that includes a rule to protect data important to the organization such as credit cards and PII.

**Remediation:**

**To remediate using the UI:**

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

**Note:** Some tenants may not have a default policy for teams as Microsoft started creating these by default at a particular point in time. In this case a new policy will have to be created that includes a rule to protect data important to the organization such as credit cards and PII.

**Default Value:**

Enabled (On)

**References:**

1. https://learn.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps
2. https://learn.microsoft.com/en-us/purview/dlp-teams-default-policy
3. https://learn.microsoft.com/en-us/powershell/module/exchange/connect-ippssession?view=exchange-ps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.1 Establish and Maintain a Data Management Process<br>Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |
| v7 | 13 Data Protection<br>Data Protection | | | |
| v7 | 14.7 Enforce Access Control to Data through Automated Tools<br>Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system. | | | ● |

## 3.3 Information Protection

## *3.3.1 (L1) Ensure Information Protection sensitivity label policies are published (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Sensitivity labels enable organizations to classify and label content across Microsoft 365 based on its sensitivity and business impact. These labels can be applied manually by users or automatically based on the content. When applied, labels can automatically encrypt content, provide "Confidential" watermarks, restrict access, and offer various data protection features.

Labels can be scoped to data assets and containers:

- Files & other data assets in Microsoft 365, Fabric, Azure, AWS and other platforms
- Email messages sent from all versions of Outlook
- Meeting calendar events and schedules in Outlook and Teams
- Teams, Microsoft 365 Groups and SharePoint sites

**Rationale:**

Consistent usage of sensitivity labels can help reduce the risk of data loss or exposure and enable more effective incident response if a breach does occur. They can also help organizations comply with regulatory requirements and provide visibility and control over sensitive information.

**Impact:**

Encryption configurations (control access, DKE, BYOK) in the individual labels may impact users' ability to access site documents and information. Careful consideration of the individual sensitivity label configurations should be exercised prior to applying an auto labeling policy, publishing policy, sensitivity label configuration, or PowerShell based label settings to SharePoint sites.

Additionally, when updating or deleting Sensitivity Labels, an assessment of the potential impacts should be conducted to avoid unintended consequences. If tenants are configured for sharing with guests or external domains and Sensitivity Labels have encryption applied, this can affect the ability to share documents via email stored in SharePoint. Some recipients may be unable to open the document depending on their email client, which could trigger Purview Advanced Encryptions and OME flows based on the recipient type and the cloud license from which the email is sent (e.g., government clouds vs. commercial clouds).

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft Purview compliance portal https://purview.microsoft.com/
2. Select Information protection > Policies > Label publishing policies.
3. Ensure that a Label policy exists and is published according to the organization's information protection needs.

**To audit using PowerShell:**

1. Connect to the Security & Compliance PowerShell using Connect-IPPSSession.
2. Run the following script:

```
$Policies = Get-LabelPolicy -WarningAction Ignore |
    Where-Object { $_.Type -eq "PublishedSensitivityLabel" }

if ($Policies) {
        $Policies | Format-List -Property Name, *Location*
       Write-Host "$($Policies.Count) Sensitivity Label policies found."
} else {
    Write-Host "No Sensitivity Label policies found"
}
```

3. Ensure there is at least one sensitivity label policy published.
4. Review the locations defined to ensure they're in scope with the organization's needs.

**Note:** These policies are specific to the information protection needs of each organization. Whether an organization passes the audit is open to interpretation by the auditor and depends largely on how effectively it implements information protection features to safeguard data.

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft Purview compliance portal https://purview.microsoft.com/
2. Select Information protection > Sensitivity labels.
3. Click Create a label to create a label.
4. Click Publish labels and select any newly created labels to publish according to the organization's information protection needs.

**Default Value:**

The "Global sensitivity label policy" exists by default.

**References:**

1. https://learn.microsoft.com/en-us/purview/sensitivity-labels
2. https://learn.microsoft.com/en-us/purview/create-sensitivity-labels

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.7 Establish and Maintain a Data Classification Scheme<br>Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as “Sensitive,” “Confidential,” and “Public,” and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard. | | ● | ● |
| v7 | 13.1 Maintain an Inventory Sensitive Information<br>Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider. | ● | ● | ● |
| v7 | 14.6 Protect Information through Access Control Lists<br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

# 4 Microsoft Intune admin center

This section includes settings specific to hardening the Microsoft 365 tenant itself through Intune settings.

CIS has other platform specific benchmarks for Intune which are intended to harden endpoints through Endpoint Manager (Microsoft Intune admin center). Those are developed in the following WorkBench communities:

**CIS Microsoft Intune for Windows:**

https://workbench.cisecurity.org/communities/116

**CIS Intune Apple iOS and iPadOS Benchmarks:**

https://workbench.cisecurity.org/communities/179

## *4.1 (L2) Ensure devices without a compliance policy are marked 'not compliant' (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Compliance policies are sets of rules and conditions that are used to evaluate the configuration of managed devices. These policies can help secure organizational data and resources from devices that don't meet those configuration requirements. Managed devices must satisfy the conditions you set in your policies to be considered compliant by Intune. When combined with conditional access, this allows more control over how non-compliant devices are treated.

The recommended state is `Mark devices with no compliance policy assigned as` as `Not compliant`

**Rationale:**

Implementing this setting is a first step in adopting compliance policies for devices. When used in together with Conditional Access policies the attack surface can be reduced by forcing an action to be taken for non-compliant devices.

**Note:** This section does not focus on which compliance policies to use, only that an organization should adopt and enforce them to their needs.

**Impact:**

Any devices without a compliance policy will be marked not compliant. Care should be taken to first deploy any new compliance policies with a Conditional Access (CA) policy that is in the **Report-only** state. After the environment's device compliance is better understood it is then appropriate to finally align with `Mark devices with no compliance policy assigned as` and enable any CA policies that enforce actions based on device compliance.

If a mature environment already has an existing device compliance CA policy and a large number of devices without an assigned compliance policy, this could cause disruption as those devices would then be suddenly considered not compliant.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Intune admin center` https://intune.microsoft.com/
2. Select `Devices` and then under **Manage devices** click `Compliance`
3. Click `Compliance settings`.
4. Ensure `Mark devices with no compliance policy assigned as` is set to `Not compliant`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "DeviceManagementConfiguration.Read.All"`
2. Run the following commands:

```
$Uri = 'https://graph.microsoft.com/v1.0/deviceManagement/settings'
Invoke-MgGraphRequest -Uri $Uri -Method GET
```

3. Ensure that `secureByDefault` is set to `True`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Intune admin center` https://intune.microsoft.com/
2. Select `Devices` and then under **Manage devices** click `Compliance`
3. Click `Compliance settings`.
4. Set `Mark devices with no compliance policy assigned as` to `Not compliant`.

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "DeviceManagementConfiguration.ReadWrite.All"`
2. Run the following commands:

```
$Uri = 'https://graph.microsoft.com/v1.0/deviceManagement'
$Body = @{
    settings = @{
        secureByDefault = $true
    }
} | ConvertTo-Json
Invoke-MgGraphRequest -Uri $Uri -Method PATCH -Body $Body
```

**Default Value:**

UI: "Compliant"

Graph: secureByDefault = $false

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *4.2 (L2) Ensure device enrollment for personally owned devices is blocked by default (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Device enrollment restrictions let you restrict devices from enrolling in Intune based on certain device attributes such as device limit, device platform, OS Version, manufacturer or device ownership (Personally owned devices).

The recommended state is to `Block` personally owned devices from enrollment.

**Rationale:**

Restricting the enrollment of personally owned devices prevents attackers who have bypassed other controls from registering a new device to gain an additional foothold, further hiding or obscuring their activities.

An attack path could be:

1. Account Compromise via Phishing and AiTM
2. Conditional Access Bypass
3. Reconnaissance using e.g. ROADrecon, GraphRunner or AADInternals
4. Lateral Movement, Privilege Escalation or Persistence through a newly registered device enrolled in Intune

**Impact:**

Per platform personally owned device enrollment impacts are listed below. It is important to test the changes to the defaults prior to moving into production and implementing this control.

**Windows Devices**

The following enrollment methods are authorized for corporate enrollment for Windows devices, any other enrollment method will be considered "Personal" and blocked:

- The device enrolls through Windows Autopilot.
- The device enrolls through GPO, or automatic enrollment from Configuration Manager for co-management.
- The device enrolls through a bulk provisioning package.
- The enrolling user is using a device enrollment manager account.

**MacOS**

By default, Intune classifies macOS devices as personally owned. To be classified as corporate-owned, a Mac must fulfill one of the following conditions:

- Registered with a serial number.
- Enrolled via Apple Automated Device Enrollment (ADE).

**iOS/IPadOS devices**

By default, Intune classifies iOS/iPadOS devices as personally owned. To be classified as corporate-owned, an iOS/iPadOS device must fulfill one of the following conditions:

- Registered with a serial number or IMEI.
- Enrolled by using Automated Device Enrollment (formerly Device Enrollment Program).

**Android devices**

By default, until you manually make changes in the admin center, your Android Enterprise work profile device settings and Android device administrator device settings are the same.

If you block Android Enterprise work profile enrollment on personal devices, only corporate-owned devices can enroll with personally owned work profiles.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Intune admin center` https://intune.microsoft.com/
2. Select `Devices` and then under **Device onboarding** click `Enrollment`
3. Under **Enrollment options** select `Device platform restriction`.
4. Inspect the policies listed under **Device type restrictions**
    - For the `Default` priority policy, click `All Users`.
    - Select `Properties`.
5. Ensure all platforms are set to `Block` in the `Personally owned` column.
6. If the `Platform` itself is set to `Block` for any of the platforms shown this is also a passing state for that platform.

**Note:** Blocking platforms that are not used in the organization is a more restrictive best practice and will also effectively block enrollment of personally owned devices for the selected platform, ensuring compliance for this recommendation.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "DeviceManagementConfiguration.Read.All"`
2. Run the following script:

```
$Uri =
'https://graph.microsoft.com/beta/deviceManagement/deviceEnrollmentConfigurat
ions'
$Config = (Invoke-MgGraphRequest -Uri $Uri -Method GET).value |
Where-Object { $_.id -match 'DefaultPlatformRestrictions' -and $_.priority -
eq 0 }

$Result = [PSCustomObject]@{
    WindowsPersonalDeviceEnrollmentBlocked        =
$Config.windowsRestriction.personalDeviceEnrollmentBlocked
    iOSPersonalDeviceEnrollmentBlocked            =
$Config.iosRestriction.personalDeviceEnrollmentBlocked
    AndroidForWorkPersonalDeviceEnrollmentBlocked =
$Config.androidForWorkRestriction.personalDeviceEnrollmentBlocked
    MacOPersonalDeviceEnrollmentBlocked           =
$Config.macOSRestriction.personalDeviceEnrollmentBlocked
    AndroidPersonalDeviceEnrollmentBlocked        =
$Config.androidRestriction.personalDeviceEnrollmentBlocked
}

$Result
```

3. Inspect the output, ensure each platform displays `True` next to it's property. A passing output will look like the below:

```
WindowsPersonalDeviceEnrollmentBlocked        : True
iOSPersonalDeviceEnrollmentBlocked            : True
AndroidForWorkPersonalDeviceEnrollmentBlocked : True
MacOPersonalDeviceEnrollmentBlocked           : True
AndroidPersonalDeviceEnrollmentBlocked        : True
```

**Note:** If `platformBlocked` is `true` then that platform is also in compliance as the platform is blocked from enrollment entirely. This is not currently reflected in the audit script but can be queried from the same API call.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Intune admin center` https://intune.microsoft.com/
2. Select `Devices` and then under **Device onboarding** click `Enrollment`
3. Under **Enrollment options** select `Device platform restriction`.
4. Inspect the policies listed under **Device type restrictions**
    - For the `Default` priority policy, click `All Users`.
    - Select `Properties`.
5. Click `Edit` to change **Platform settings**.
6. In the **Personally owned** column set each platform to `Block`.

**Note:** Blocking platforms that are not used in the organization is a more restrictive best practice and will also effectively block enrollment of personally owned devices for the selected platform, ensuring compliance for this recommendation.

**Default Value:**

Allow

**References:**

1. https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set
2. https://www.glueckkanja.com/blog/security/2025/01/compliant-device-bypass-en/

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v8 | 4.12 Separate Enterprise Workspaces on Mobile End-User Devices<br>Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data. | | | ● |

# 5 Microsoft Entra admin center

Microsoft Entra, also known as Identity, contains settings related to identity, conditional access, and was formerly named Azure AD.

Direct link: https://entra.microsoft.com/

## 5.1 Entra ID

### 5.1.1 Overview

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

### 5.1.2 Users

### *5.1.2.1 (L1) Ensure 'Per-user MFA' is disabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Legacy per-user Multi-Factor Authentication (MFA) can be configured to require individual users to provide multiple authentication factors, such as passwords and additional verification codes, to access their accounts. It was introduced in earlier versions of Office 365, prior to the more comprehensive implementation of Conditional Access (CA).

**Rationale:**

Both security defaults and conditional access with security defaults turned off are not compatible with per-user multi-factor authentication (MFA), which can lead to undesirable user authentication states. The CIS Microsoft 365 Benchmark explicitly employs Conditional Access for MFA as an enhancement over security defaults and as a replacement for the outdated per-user MFA. To ensure a consistent authentication state disable per-user MFA on all accounts.

**Impact:**

Accounts using per-user MFA will need to be migrated to use CA.

Prior to disabling per-user MFA the organization must be prepared to implement conditional access MFA to avoid security gaps and allow for a smooth transition. This will help ensure relevant accounts are covered by MFA during the change phase from disabling per-user MFA to enabling CA MFA. Section 5.2.2 in this document covers the creation of a CA rule for both administrators and all users in the tenant.

Microsoft has documentation on migrating from per-user MFA Convert users from per-user MFA to Conditional Access based MFA

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Users` select `All users`.
3. Click on `Per-user MFA` on the top row.
4. Ensure under the column `Multi-factor Auth Status` that each account is set to `Disabled`

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Users` select `All users`.
3. Click on `Per-user MFA` on the top row.
4. Click the empty box next to `Display Name` to select all accounts.
5. On the far right under *quick steps* click `Disable`.

**Default Value:**

Disabled

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userstates#convert-users-from-per-user-mfa-to-conditional-access
2. https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide#use-conditional-access-policies
3. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userstates#convert-per-user-mfa-enabled-and-enforced-users-to-disabled

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |

### *5.1.2.2 (L2) Ensure third party integrated applications are not allowed (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

The implementation of this change will impact both end users and administrators. End users will not be able to integrate third-party applications that they may wish to use. Administrators are likely to receive requests from end users to grant them permission to the necessary third-party applications.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Users` select `Users settings`.
3. Verify `Users can register applications` is set to `No`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`
2. Run the following command:

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | fl
AllowedToCreateApps
```

3. Ensure the returned value is `False`.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"`
2. Run the following commands:

```
$param = @{ AllowedToCreateApps = "$false" }
Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions $param
```

**Default Value:**

Yes (Users can register applications.)

**References:**

1. https://learn.microsoft.com/en-us/entra/identity-platform/how-applications-are-added

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 2.5 Allowlist Authorized Software<br>Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. | | ● | ● |
| v7 | 18.4 Only Use Up-to-date And Trusted Third-Party Components<br>Only use up-to-date and trusted third-party components for the software developed by the organization. | | ● | ● |

## *5.1.2.3 (L1) Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Non-privileged users can create tenants in the Microsoft Entra ID and Microsoft Entra administration portal under "Manage tenant". The creation of a tenant is recorded in the Audit log as category "DirectoryManagement" and activity "Create Company". By default, the user who creates a Microsoft Entra tenant is automatically assigned the Global Administrator role. The newly created tenant doesn't inherit any settings or configurations.

**Rationale:**

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

**Impact:**

Non-admin users will need to contact I.T. if they have a valid reason to create a tenant.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/
2. Click to expand Entra ID > Users > User settings.
3. Ensure Restrict non-admin users from creating tenants is set to Yes

**To audit using PowerShell:**

1. Connect to Microsoft Graph using Connect-MgGraph -Scopes "Policy.Read.All"
2. Run the following commands:

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions |
    Select-Object AllowedToCreateTenants
```

3. Ensure the returned value is False

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"
2. Run the following commands:

```
# Create hashtable and update the auth policy
$params = @{ AllowedToCreateTenants = $false }
Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions $params
```

**Default Value:**

No - Non-administrators can create tenants.

AllowedToCreateTenants is True

**References:**

1. https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions#restrict-member-users-default-permissions

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *5.1.2.4 (L1) Ensure access to the Entra admin center is restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Restrict non-privileged users from signing into the Microsoft Entra admin center.

**Note:** This recommendation only affects access to the web portal. It does not prevent privileged users from using other methods such as Rest API or PowerShell to obtain information. Those channels are addressed elsewhere in this document.

**Rationale:**

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

**Note:** Users will still be able to sign into Microsoft Entra admin center but will be unable to see directory information.

**Impact:**

In the event there are resources a user owns that need to be changed in the Entra Admin center, then an administrator would need to make those changes.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Entra ID` > `Users` > `User settings`.
3. Verify under the **Administration center** section that `Restrict access to Microsoft Entra admin center` is set to `Yes`.

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

No - Non-administrators can access the Microsoft Entra admin center.

**References:**

1. https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions#restrict-member-users-default-permissions

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *5.1.2.5 (L2) Ensure the option to remain signed in is hidden (Manual)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

The option for the user to `Stay signed in`, or the `Keep me signed in` option, will prompt a user after a successful login. When the user selects this option, a persistent refresh token is created. The refresh token lasts for 90 days by default and does not prompt for sign-in or multifactor.

**Rationale:**

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

**Impact:**

Once this setting is hidden users will no longer be prompted upon sign-in with the message `Stay signed in?`. This may mean users will be forced to sign in more frequently. Important: some features of SharePoint Online and Office 2010 have a dependency on users remaining signed in. If you hide this option, users may get additional and unexpected sign in prompts.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Users` > `User settings`.
3. Ensure `Show keep user signed in` is highlighted `No`.

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

Users may select `stay signed in`

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concepts-azure-multi-factor-authentication-prompts-session-lifetime
2. https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-stay-signed-in-prompt

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v7 | 16.3 Require Multi-factor Authentication<br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider. | | ● | ● |

## *5.1.2.6 (L2) Ensure 'LinkedIn account connections' is disabled (Manual)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

Users will not be able to sync contacts or use LinkedIn integration.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Users` select `User settings`.
3. Under `LinkedIn account connections` ensure `No` is highlighted.

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

LinkedIn integration is enabled by default.

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v7 | 13.3 Monitor and Block Unauthorized Network Traffic<br>Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals. | | | ● |

### 5.1.3 Groups

### *5.1.3.1 (L1) Ensure a dynamic group for guest users is created (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

The recommended state is to create a dynamic group that includes guest accounts.

**Rationale:**

Dynamic groups allow for an automated method to assign group membership.

Guest user accounts will be automatically added to this group and through this existing conditional access rules, access controls and other security measures will ensure that new guest accounts are restricted in the same manner as existing guest accounts.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Groups` select `All groups`.
3. On the right of the search field click `Add filter`.
4. Set `Filter` to `Membership type` and `Value` to `Dynamic` then apply.
5. Identify a dynamic group and select it.
6. Under manage, select `Dynamic membership rules` and ensure the rule syntax contains `(user.userType -eq "Guest")`
7. If necessary, inspect other dynamic groups for the value above.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Group.Read.All"`
2. Run the following commands:

```
$groups = Get-MgGroup -All | Where-Object { $_.GroupTypes -contains
"DynamicMembership" }
$groups | ft DisplayName,GroupTypes,MembershipRule
```

3. Look for a dynamic group containing the rule `(user.userType -eq "Guest")`

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Groups` select `All groups`.
3. Select `New group` and assign the following values:
   - Group type: `Security`
   - Microsoft Entra roles can be assigned to the group: `No`
   - Membership type: `Dynamic User`
4. Select `Add dynamic query`.
5. Above the `Rule syntax` text box, select `Edit`.
6. Place the following expression in the box:

```
(user.userType -eq "Guest")
```

7. Select `OK` and `Save`

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Group.ReadWrite.All"`
2. In the script below edit `DisplayName` and `MailNickname` as needed and run:

```
$params = @{
     DisplayName                   = "Dynamic Guest Group"
     MailNickname                  = "DynGuestUsers"
     MailEnabled                   = $false
     SecurityEnabled               = $true
     GroupTypes                    = "DynamicMembership"
     MembershipRule                = '(user.userType -eq "Guest")'
     MembershipRuleProcessingState = "On"
}

New-MgGroup @params
```

**Default Value:**

Undefined

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-create-rule
2. https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership
3. https://learn.microsoft.com/en-us/entra/external-id/use-dynamic-groups

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |

### *5.1.3.2 (L1) Ensure users cannot create security groups (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting allows users in the organization to create new security groups and add members to these groups in the Azure portal, API, or PowerShell. These new groups also show up in the Access Panel for all other users. If the policy setting on the group allows it, other users can create requests to join these groups.

The recommended state is `Users can create security groups in Azure portals, API or PowerShell` set to `No`.

**Rationale:**

Allowing end users to create security groups without oversight can lead to uncontrolled group sprawl, increasing the risk of inappropriate access to sensitive data. The default assignment of group ownership to the creator introduces a potential for privilege escalation, especially if IT teams overlook how these groups are later used to manage access.

A more malicious scenario arises when a compromised non-privileged user creates deceptively named security groups such as “Accounting” or “Break-glass”, or uses homograph techniques to mimic legitimate group names. Third-party IT teams may be particularly susceptible, as they might not be familiar with the environment or lack consistent naming conventions. An unsuspecting administrator could then mistakenly assign elevated privileges, grant access to sensitive data, or exclude these groups from Conditional Access policies, inadvertently creating a serious security gap.

**Impact:**

Restrictions may introduce some operational friction, particularly in fast-paced or decentralized environments where teams rely on self-service capabilities for collaboration and access management.

This can increase reliance on IT teams for routine tasks, potentially causing delays. However, these impacts can be minimized through automated approval workflows and clear governance processes.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Groups` select `General`.
3. Ensure `Users can create security groups in Azure portals, API or PowerShell` is set to `No`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`
2. Run the following command:

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | fl
```

3. Ensure `AllowedToCreateSecurityGroups` is set to `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Groups` select `General`.
3. Set `Users can create security groups in Azure portals, API or PowerShell` to `No`.

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"`
2. Run the following commands:

```
$params = @{
        defaultUserRolePermissions = @{
                AllowedToCreateSecurityGroups = $false
        }
}

Update-MgPolicyAuthorizationPolicy -BodyParameter $params
```

**Default Value:**

AllowedToCreateSecurityGroups : True

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management?WT.mc_id=Portal-Microsoft_AAD_IAM#group-settings
2. https://learn.microsoft.com/en-us/graph/api/authorizationpolicy-get?view=graph-rest-1.0&tabs=http

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |

### 5.1.4 Devices

This section contains settings related to device management. While some organizations may opt not to use Intune for managing devices, it is still advisable to harden these configurations beyond their default values. Doing so ensures a stronger security posture should these features be utilized in the future.

### *5.1.4.1 (L2) Ensure the ability to join devices to Entra is restricted (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

This setting enables you to select the users who can register their devices as Microsoft Entra joined devices.

The recommended state is `Selected` or `None`.

**Note:** This setting is applicable only to Microsoft Entra join on Windows 10 or newer. This setting doesn't apply to Microsoft Entra hybrid joined devices, Microsoft Entra joined VMs in Azure, or Microsoft Entra joined devices that use Windows Autopilot self-deployment mode because these methods work in a userless context.

**Rationale:**

If a threat actor compromises a standard user account, they can enroll a rogue device under that user's identity. This device may inherit MDM policies and appear compliant, giving attackers persistent access to cloud resources without triggering MFA.

In a 2023 blog, Microsoft IR reports that it has detected threat actors registering their own devices to the Microsoft Entra tenant, giving them a platform to escalate the cyberattack. While simply joining a device to a Microsoft Entra tenant may present limited immediate risk, it could allow a threat actor to establish a foothold in the environment.

**Impact:**

Restricting the setting requires IT teams to assign enrollment permissions to specific staff, such as helpdesk or provisioning personnel, which may impact user-driven Autopilot scenarios and increase administrative overhead for device onboarding and support.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Ensure `Users may join devices to Microsoft Entra` is set to `Selected` *or* `None`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.DeviceConfiguration"`
2. Run the following commands:

```
$Uri = "https://graph.microsoft.com/beta/policies/deviceRegistrationPolicy"
(Invoke-MgGraphRequest -Method GET -Uri $Uri).azureADJoin.allowedToJoin
```

3. Ensure that the key `@odata.type` is set to either `#microsoft.graph.enumeratedDeviceRegistrationMembership` **(Selected)** *or* `#microsoft.graph.noDeviceRegistrationMembership` **(None)**.

**Note:** When set to the setting is set to `Selected` users and groups will also appear in the output of the Graph Request.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Set `Users may join devices to Microsoft Entra` to `Selected` (and add members) or `None`.

**Default Value:**

All

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings
2. https://www.microsoft.com/en-us/security/blog/2023/12/05/microsoft-incident-response-lessons-on-preventing-cloud-identity-compromise/#poor-device
3. https://learn.microsoft.com/en-us/graph/api/resources/deviceregistrationpolicy?view=graph-rest-beta

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

## *5.1.4.2 (L1) Ensure the maximum number of devices per user is limited (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting defines the maximum number of Microsoft Entra joined or registered devices that a user can have in Microsoft Entra ID. Once this limit is reached, no additional devices can be added until existing ones are removed. Values above 100 are automatically capped at 100.

The recommended state is `20` or less.

**Rationale:**

Microsoft incident response teams have observed threat actors enrolling their own devices to establish persistence after a non-privileged user has been compromised. High device quotas can exacerbate this risk by enabling attackers to register multiple devices that appear legitimate, while also contributing to unmanaged or personal devices cluttering the environment, driving up licensing costs and complicating compliance efforts.

Enforcing a reasonable device limit per user supports good governance, reduces the attack surface, and encourages administrators to reassess and clean up legacy or unused device enrollments.

**Impact:**

IT staff who need to enroll more than 20 devices on behalf of the organization must be assigned the role of Device Enrollment Manager in the Intune admin center. Device Enrollment Managers are non-administrator accounts that can enroll and manage up to 1,000 devices. It is recommended to use dedicated service accounts for this role rather than assigning it to users' primary or daily-use accounts.

**Warning:** Do not delete accounts assigned as a Device enrollment manager if any devices were enrolled using the account. Doing so will lead to issues with these devices.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Ensure `Maximum number of devices per user` is set to `20 (Recommended)` or less.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.DeviceConfiguration"`
2. Run the following commands:

```
$Uri = "https://graph.microsoft.com/beta/policies/deviceRegistrationPolicy"
Invoke-MgGraphRequest -Method GET -Uri $Uri
```

3. Ensure the key `userDeviceQuota` is set to `20` or less.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Set `Maximum number of devices per user` to `20 (Recommended)` or less.

**Default Value:**

50

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings
2. https://learn.microsoft.com/en-us/intune/intune-service/enrollment/device-enrollment-manager-enroll
3. https://learn.microsoft.com/en-us/graph/api/resources/deviceregistrationpolicy?view=graph-rest-beta

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

## *5.1.4.3 (L1) Ensure the GA role is not added as a local administrator during Entra join (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting controls whether the Global Administrator role is automatically added to the local administrators group on a device during the Microsoft Entra join process.

The recommended state is `No`.

**Rationale:**

System administrators may be inclined to use over-privileged accounts for convenience when managing devices. Enforcing this control helps discourage that behavior by requiring administrative actions to be performed using accounts specifically designated for local administration. This promotes adherence to the principle of least privilege and reduces the risk associated with using high-level roles for routine tasks. For example, using a Global Administrator account to authenticate to a compromised endpoint and continue performing tasks significantly increases the risk of broader organizational compromise.

**Impact:**

Restricting the default behavior and requiring manual assignment to least privilege roles introduces minor administrative overhead. During the Microsoft Entra join process, the **Microsoft Entra Joined Device Local Administrator** role is automatically added to the device's local administrators group and should be used instead.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Ensure `Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)` is set to `No`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.DeviceConfiguration"`
2. Run the following commands:

```
$Uri = "https://graph.microsoft.com/beta/policies/deviceRegistrationPolicy"
(Invoke-MgGraphRequest -Method GET -Uri $Uri).azureADJoin.localAdmins
```

3. Ensure the key `enableGlobalAdmins` is set to `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Set `Global administrator role is added as local administrator on the device during Microsoft Entra join (Preview)` to `No`.

**Default Value:**

Yes

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings
2. https://learn.microsoft.com/en-us/graph/api/resources/deviceregistrationpolicy?view=graph-rest-beta
3. https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

### *5.1.4.4 (L1) Ensure local administrator assignment is limited during Entra join (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting determines if the Microsoft Entra user registering their device as Microsoft Entra join be added to the local administrators group. This setting applies only once during the actual registration of the device as Microsoft Entra join.

The recommended state is `Selected` *or* `None`.

**Rationale:**

To uphold the principle of least privilege, the assignment of local administrator rights during Microsoft Entra join should be centrally managed using appropriate built-in roles through Intune. This approach minimizes the number of disparate users with elevated privileges, reducing the attack surface and potential for misuse. Centralized management also streamlines the deprovisioning process, ensuring that administrative access can be revoked efficiently and consistently across all devices, rather than requiring manual intervention on each individual endpoint.

**Impact:**

Restricting the default behavior and requiring manual assignment to built-in roles introduces minor administrative overhead. During the Microsoft Entra join process, the **Microsoft Entra Joined Device Local Administrator** role is automatically added to the device's local administrators group and should be used instead.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Ensure `Registering user is added as local administrator on the device during Microsoft Entra join (Preview)` is set to `Selected` *or* `None`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.DeviceConfiguration"`
2. Run the following commands:

```
$Uri = "https://graph.microsoft.com/beta/policies/deviceRegistrationPolicy"
(Invoke-MgGraphRequest -Method GET -Uri
$Uri).azureADJoin.localAdmins.registeringUsers
```

3. Ensure the key `@odata.type` is set to `#microsoft.graph.enumeratedDeviceRegistrationMembership` **(Selected)** *or* `#microsoft.graph.noDeviceRegistrationMembership` **(None)**.

**Note:** When set to the setting is set to Selected users and groups will also appear in the output of the Graph Request.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Set `Registering user is added as local administrator on the device during Microsoft Entra join (Preview)` to `Selected` (and add members) *or* `None`.

**Default Value:**

All

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings
2. https://learn.microsoft.com/en-us/graph/api/resources/deviceregistrationpolicy?view=graph-rest-beta
3. https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

## *5.1.4.5 (L1) Ensure Local Administrator Password Solution is enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Local Administrator Password Solution (LAPS) is the management of local account passwords on Windows devices. LAPS provides a solution to securely manage and retrieve the built-in local admin password. With cloud version of LAPS, customers can enable storing and rotation of local admin passwords for both Microsoft Entra and Microsoft Entra hybrid join devices

The recommended state is `Yes`.

**Rationale:**

Managing local Administrator passwords across multiple systems can be challenging. As a result, many organizations opt to configure the same password on all workstations and/or member servers during deployment. However, this practice introduces a significant security risk: if an attacker compromises one system and obtains the local Administrator password, they can potentially gain administrative access to every other system using that same password.

Additionally, enabling LAPS at the tenant level is a prerequisite for implementing LAPS-related recommendations outlined in the CIS Microsoft Intune for Windows Workstation Benchmarks.

**Note:** Enabling LAPS at the tenant level does not automatically enforce password rotation for built-in Administrator accounts. To activate LAPS functionality, appropriate policies must be configured in Intune Settings Catalog or under the `Endpoint security` > `Account protection` blade. The CIS Microsoft 365 Foundations Benchmark focuses on hardening at the tenant level, while the CIS Intune Benchmarks focus on endpoint-specific configurations.

**Impact:**

Enabling LAPS requires some additional operational overhead.

Although unlikely if a password is rotated and not retrieved or backed up before the device becomes unreachable (e.g., due to hardware failure, network isolation, or being decommissioned), administrators may be locked out.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Ensure `Enable Microsoft Entra Local Administrator Password Solution (LAPS)` is set to `Yes`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.DeviceConfiguration"`
2. Run the following commands:

```
$Uri = "https://graph.microsoft.com/beta/policies/deviceRegistrationPolicy"
(Invoke-MgGraphRequest -Method GET -Uri $Uri).localAdminPassword
```

3. Ensure the key `isEnabled` is set to `True`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Set `Enable Microsoft Entra Local Administrator Password Solution (LAPS)` to `Yes`.

**Default Value:**

No

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings
2. https://learn.microsoft.com/en-us/graph/api/resources/deviceregistrationpolicy?view=graph-rest-beta
3. https://learn.microsoft.com/en-us/entra/identity/devices/howto-manage-local-admin-passwords

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.2 Use Unique Passwords<br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | ● | ● | ● |

### *5.1.4.6 (L2) Ensure users are restricted from recovering BitLocker keys (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

This setting determines if users can self-service recover their BitLocker key(s). 'Yes' restricts non-admin users from being able to see the BitLocker key(s) for their owned devices if there are any. 'No' allows all users to recover their BitLocker key(s).

The recommended state is `Yes`.

**Rationale:**

Restricting user access to the self-service BitLocker recovery key portal helps mitigate the risk of recovery key exposure in the event of a compromised user account. If an attacker gains access to both the user's credentials and the physical device, they could potentially retrieve the recovery key and decrypt sensitive data. The recovery key itself is also considered sensitive information.

**Impact:**

Restricting this setting will increase administrative overhead and may introduce friction between end users and the helpdesk, as users will no longer be able to retrieve BitLocker recovery keys through the self-service portal. This portal was originally designed to streamline recovery and reduce support burden. During the CrowdStrike Falcon Sensor outage in July 2024, many endpoints entered recovery mode, and delays in accessing recovery keys contributed to prolonged downtime. Limiting self-service access could exacerbate such delays in future incidents, especially in large or distributed environments.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Ensure `Restrict users from recovering the BitLocker key(s) for their owned devices` is set to `Yes`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`
2. Run the following:

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | fl
```

3. Ensure that the property `AllowedToReadBitlockerKeysForOwnedDevice` is set to `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Devices` select `Device settings`.
3. Set `Restrict users from recovering the BitLocker key(s) for their owned devices` to `Yes`.

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"`
2. Run the following:

```
$params = @{
        defaultUserRolePermissions = @{
                AllowedToReadBitlockerKeysForOwnedDevice = $false
        }
}

Update-MgPolicyAuthorizationPolicy -BodyParameter $params
```

**Default Value:**

No

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/devices/manage-device-identities#configure-device-settings
2. https://learn.microsoft.com/en-us/graph/api/authorizationpolicy-get?view=graph-rest-1.0
3. https://techcommunity.microsoft.com/blog/intunecustomersuccess/user-self-service-bitlocker-recovery-key-access-with-intune-company-portal-websi/4150458
4. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/recovery-process#self-recovery

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |

### 5.1.5 Applications

### *5.1.5.1 (L2) Ensure user consent to apps accessing company data on their behalf is not allowed (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Rationale:**

Attackers commonly use custom applications to trick users into granting them access to company data. Restricting user consent mitigates this risk and helps to reduce the threat-surface.

**Impact:**

If user consent is disabled, previous consent grants will still be honored but all future consent operations must be performed by an administrator. Tenant-wide admin consent can be requested by users through an integrated administrator consent request workflow or through organizational support processes.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` and select `Enterprise apps`.
3. Under `Security` select `Consent and permissions` > `User consent settings`.
4. Verify `User consent for applications` is set to `Do not allow user consent`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`
2. Run the following command:

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions |
    Select-Object -ExpandProperty PermissionGrantPoliciesAssigned
```

3. Verify that the returned string does not contain either `ManagePermissionGrantsForSelf.microsoft-user-default-low` or `ManagePermissionGrantsForSelf.microsoft-user-default-legacy`. If either of these strings is present, the audit fails.

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

UI - `Allow user consent for apps`

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=portal

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v7 | 14.6 Protect Information through Access Control Lists<br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

## *5.1.5.2 (L1) Ensure the admin consent workflow is enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Rationale:**

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

**Impact:**

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Entra ID and select Enterprise apps.
3. Under Security select Consent and permissions.
4. Under Manage select Admin consent settings.
5. Verify that Users can request admin consent to apps they are unable to consent to is set to Yes.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using Connect-MgGraph -Scopes "Policy.Read.All"
2. Run the following command:

```
Get-MgPolicyAdminConsentRequestPolicy |
    fl IsEnabled,NotifyReviewers,RemindersEnabled
```

3. Ensure IsEnabled is set to True.

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Entra ID and select Enterprise apps.
3. Under Security select Consent and permissions.
4. Under Manage select Admin consent settings.
5. Set Users can request admin consent to apps they are unable to consent to to Yes under Admin consent requests.
6. Under the Reviewers choose the Roles and Groups that will review user generated app consent requests.
7. Set Selected users will receive email notifications for requests to Yes
8. Select Save at the top of the window.

**Default Value:**

- Users can request admin consent to apps they are unable to consent to: No
- Selected users to review admin consent requests: None
- Selected users will receive email notifications for requests: Yes
- Selected users will receive request expiration reminders: Yes
- Consent request expires after (days): 30

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 2.5 Allowlist Authorized Software<br>Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. | | ● | ● |
| v7 | 18.3 Verify That Acquired Software is Still Supported<br>Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations. | | ● | ● |

### 5.1.6 External Identities

### *5.1.6.1 (L2) Ensure that collaboration invitations are sent to allowed domains only (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

B2B collaboration is a feature within Microsoft Entra External ID that allows for guest invitations to an organization.

Ensure users can only send invitations to `specified domains`.

**Note:** This list works independently from OneDrive for Business and SharePoint Online allow/block lists. To restrict individual file sharing in SharePoint Online, set up an allow or blocklist for OneDrive for Business and SharePoint Online. For instance, in SharePoint or OneDrive users can still share with external users from prohibited domains by using Anyone links if they haven't been disabled.

**Rationale:**

By specifying allowed domains for collaborations, external user's companies are explicitly identified. Also, this prevents internal users from inviting unknown external users such as personal accounts and granting them access to resources.

**Impact:**

This could make collaboration more difficult if the setting is not quickly updated when a new domain is identified as "allowed".

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `External Identities` select `External collaboration settings`.
3. Under **Collaboration restrictions**, verify that `Allow invitations only to the specified domains (most restrictive)` is selected. Then verify allowed domains are specified under `Target domains`.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`
2. Run the following:

```
$Uri = "https://graph.microsoft.com/beta/legacy/policies"
$Response = (Invoke-MgGraphRequest -Uri $Uri).value |
Where-Object { $_.type -eq 'B2BManagementPolicy' }

if ($Response) {
    $Definition = $Response.definition | ConvertFrom-Json
    $DomainsPolicy =
$Definition.B2BManagementPolicy.InvitationsAllowedAndBlockedDomainsPolicy
} else {
    Write-Output "No policy found."
    return
}

$DomainsPolicy
```

3. Ensure the output includes an `AllowedDomains` property that either contains no domains or lists only organizationally approved domains. If a *BlockedDomains* property is present, the configuration is considered non-compliant.

Example of a compliant output with AllowedDomains defined:

```
AllowedDomains
--------------
{cisecurity.org, contoso.com, example.com}
```

Allowed with no domains allowed (also compliant):

```
AllowedDomains
--------------
{}
```

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `External Identities` select `External collaboration settings`.
3. Under **Collaboration restrictions**, select `Allow invitations only to the specified domains (most restrictive)` is selected. Then specify the allowed domains under `Target domains`.

**Default Value:**

Allow invitations to be sent to any domain (most inclusive)

**References:**

1. https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list
2. https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.1 Establish an Access Granting Process<br>Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. | ● | ● | ● |
| v7 | 13.1 Maintain an Inventory Sensitive Information<br>Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider. | ● | ● | ● |

### *5.1.6.2 (L1) Ensure that guest user access is restricted (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Microsoft Entra ID, part of Microsoft Entra, allows you to restrict what external guest users can see in their organization in Microsoft Entra ID. Guest users are set to a limited permission level by default in Microsoft Entra ID, while the default for member users is the full set of user permissions.

These directory level permissions are enforced across Microsoft Entra services including Microsoft Graph, PowerShell v2, the Azure portal, and My Apps portal. Microsoft 365 services leveraging Microsoft 365 groups for collaboration scenarios are also affected, specifically Outlook, Microsoft Teams, and SharePoint. They do not override the SharePoint or Microsoft Teams guest settings.

The recommended state is at least `Guest users have limited access to properties and memberships of directory objects` or more restrictive.

**Rationale:**

By limiting guest access to the *most restrictive* state this helps prevent malicious group and user object enumeration in the Microsoft 365 environment. This first step, known as *reconnaissance* in The Cyber Kill Chain, is often conducted by attackers prior to more advanced targeted attacks.

**Impact:**

The default is `Guest users have limited access to properties and memberships of directory objects`.

When using the 'most restrictive' setting, guests will only be able to access their own profiles and will not be allowed to see other users' profiles, groups, or group memberships.

There are some known issues with Yammer that will prevent guests that are signed in from leaving the group.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `External Identities` select `External collaboration settings`.
3. Under **Guest user access** verify that `Guest user access restrictions` is set to one of the following:
    - State: `Guest users have limited access to properties and memberships of directory objects`
    - State: `Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)`

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`
2. Run the following command:

```
Get-MgPolicyAuthorizationPolicy | fl GuestUserRoleId
```

3. Ensure the value returned is `10dae51f-b6af-4016-8d66-8c2a99b929b3` or `2af84b1e-32c8-42b7-82bc-daa82404023b` (most restrictive)

**Note:** Either setting allows for a passing state.

**Note 2:** The value of `a0b1b346-4d3e-4e8b-98f8-753987be4970` is equal to `Guest users have the same access as members (most inclusive)` and should not be used.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `External Identities` select `External collaboration settings`.
3. Under **Guest user access** set `Guest user access restrictions` to one of the following:
    - State: `Guest users have limited access to properties and memberships of directory objects`
    - State: `Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)`

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"`
2. Run the following command to set the guest user access restrictions to default:

```
# Guest users have limited access to properties and memberships of directory objects
Update-MgPolicyAuthorizationPolicy -GuestUserRoleId '10dae51f-b6af-4016-8d66-8c2a99b929b3'
```

3. Or, run the following command to set it to the "most restrictive":

```
# Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)
Update-MgPolicyAuthorizationPolicy -GuestUserRoleId '2af84b1e-32c8-42b7-82bc-daa82404023b'
```

**Note:** Either setting allows for a passing state.

**Default Value:**

- UI: `Guest users have limited access to properties and memberships of directory objects`
- PowerShell: `10dae51f-b6af-4016-8d66-8c2a99b929b3`

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/users/users-restrict-guest-permissions
2. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.1 Establish an Access Granting Process<br>Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. | ● | ● | ● |

### *5.1.6.3 (L2) Ensure guest user invitations are limited to the Guest Inviter role (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

By default, all users in the organization, including B2B collaboration guest users, can invite external users to B2B collaboration. The ability to send invitations can be limited by turning it on or off for everyone, or by restricting invitations to certain roles.

The recommended state for guest invite restrictions is `Only users assigned to specific admin roles can invite guest users`.

**Rationale:**

Restricting who can invite guests limits the exposure the organization might face from unauthorized accounts.

**Impact:**

This introduces an obstacle to collaboration by restricting who can invite guest users to the organization. Designated Guest Inviters must be assigned, and an approval process established and clearly communicated to all users.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `External Identities` select `External collaboration settings`.
3. Under **Guest invite settings** verify that `Guest invite restrictions` is set to `Only users assigned to specific admin roles can invite guest users` or more restrictive.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.Read.All"`
2. Run the following command:

```
Get-MgPolicyAuthorizationPolicy | fl AllowInvitesFrom
```

3. Ensure the value returned is `adminsAndGuestInviters` or more restrictive.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `External Identities` select `External collaboration settings`.
3. Under **Guest invite settings** set `Guest invite restrictions` to `Only users assigned to specific admin roles can invite guest users`.

**To remediate using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"`
2. Run the following command:

```
Update-MgPolicyAuthorizationPolicy -AllowInvitesFrom 'adminsAndGuestInviters'
```

**Note:** The more restrictive position of the value will also pass audit, it is however not required.

**Default Value:**

- UI: `Anyone in the organization can invite guest users including guests and non-admins (most inclusive)`
- PowerShell: `everyone`

**References:**

1. https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure
2. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#guest-inviter

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.1 Establish an Access Granting Process<br>Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. | ● | ● | ● |
| v7 | 13.1 Maintain an Inventory Sensitive Information<br>Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider. | ● | ● | ● |

## 5.1.7 User experiences

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

### 5.1.8 Hybrid management

### *5.1.8.1 (L1) Ensure that password hash sync is enabled for hybrid deployments (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Password hash synchronization is one of the sign-in methods used to accomplish hybrid identity synchronization. Microsoft Entra Connect synchronizes a hashed version of the user's password hash from an on-premises Active Directory to a cloud-based Entra ID instance.

**Note:** The original MD4 hash isn't transmitted to Microsoft Entra ID. Instead, the SHA256 hash of the original MD4 hash is transmitted. As a result, if the hash stored in Microsoft Entra ID is obtained, it can't be used in an on-premises pass-the-hash attack.

**Rationale:**

Password hash synchronization helps by reducing the number of passwords your users need to maintain to just one and enables leaked credential detection for your hybrid accounts. Leaked credential protection is leveraged through Entra ID Protection and is a subset of that feature which can help identify if an organization's user account passwords have appeared on the dark web or public spaces.

Using other options for your directory synchronization may be less resilient as Microsoft can still process sign-ins to 365 with Hash Sync even if a network connection to your on-premises environment is not available. This minimizes downtime and ensures business continuity.

**Impact:**

Compliance or regulatory restrictions may exist, depending on the organization's business sector, that preclude hashed versions of passwords from being securely transmitted to cloud data centers.

**Audit:**

**To audit using the UI:**

*Only Global Admin and Hybrid Identity Administrator roles have access to view the actual **Password Hash Sync** status message. Inadequate role access will result in a default message stating: "Unable to retrieve your tenant's password hash sync information."*

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Entra Connect`.
3. Select `Connect Sync`.
4. Under **Microsoft Entra Connect sync**, verify the `Password Hash Sync` status message indicates that synchronization is occurring and no errors are present, with one of the following messages:
    - Password hash synchronization is enabled
    - Password hash synchronization cloud configuration is enabled
    - Password hash synchronization heartbeat detected

**To audit for the on-prem tool:**

1. Log in to the server that hosts the Microsoft Entra Connect tool.
2. Run `Azure AD Connect`, and then click `Configure` and `View or export current configuration`.
3. Determine whether `PASSWORD HASH SYNCHRONIZATION` is enabled on your tenant.

**To audit using PowerShell:**

1. Open PowerShell on the on-premises server running Microsoft Entra Connect.
2. Run the following cmdlet:

```
Get-ADSyncAADCompanyFeature
```

3. Ensure `PasswordHashSync` is `True`.

**Note:** Audit and remediation procedures in this recommendation only apply to Microsoft 365 tenants operating in a hybrid configuration using Entra Connect sync, and do not apply to federated domains.

**Remediation:**

**To remediate using the on-prem Microsoft Entra Connect tool:**

1. Log in to the on premises server that hosts the Microsoft Entra Connect tool
2. Double-click the `Azure AD Connect` icon that was created on the desktop
3. Click `Configure`.
4. On the `Additional tasks` page, select `Customize synchronization options` and click `Next`.
5. Enter the username and password for your global administrator.
6. On the `Connect your directories` screen, click `Next`.
7. On the `Domain and OU filtering` screen, click `Next`.
8. On the `Optional features` screen, check `Password hash synchronization` and click `Next`.
9. On the `Ready to configure` screen click `Configure`.
10. Once the configuration completes, click `Exit`.

**Default Value:**

- Microsoft Entra Connect sync `disabled` by default
- Password Hash Sync is Microsoft's recommended setting for new deployments

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-phs
2. https://www.microsoft.com/en-us/download/details.aspx?id=47594
3. https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-staging-server
4. https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.7 Centralize Access Control<br>Centralize access control for all enterprise assets through a directory service or SSO provider, where supported. | | ● | ● |
| v7 | 16.4 Encrypt or Hash all Authentication Credentials<br>Encrypt or hash with a salt all authentication credentials when stored. | | ● | ● |

## 5.2 ID Protection

### 5.2.1 Identity Protection

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

### 5.2.2 Risk-based Conditional Access

### *5.2.2.1 (L1) Ensure multifactor authentication is enabled for all users in administrative roles (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Multifactor authentication is a process that requires an additional form of identification during the sign-in process, such as a code from a mobile device or a fingerprint scan, to enhance security.

Ensure users in administrator roles have MFA capabilities enabled.

**Rationale:**

Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

**Impact:**

Implementation of multifactor authentication for all users in administrative roles will necessitate a change to user routine. All users in administrative roles will be required to enroll in multifactor authentication using phone, SMS, or an authentication application. After enrollment, use of multifactor authentication will be required for future access to the environment.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `Directory roles` specific to administrators are included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `All resources (formerly 'All cloud apps')` is selected with no exclusions.
    - Under `Grant` verify `Grant Access` is on and either `Require multifactor authentication` or `Require authentication strength` is checked.
4. Ensure `Enable policy` is set to `On`.

**Note:** A list of `Directory roles` can be found in the Remediation section.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com.
2. Click expand ID Protection > Risk-based Conditional Access.
3. Click New policy.
    - Under Users include Select users and groups and check Directory roles.
    - At a minimum, include the directory roles listed below in this section of the document.
    - Under Target resources include All resources (formerly 'All cloud apps') and do not create any exclusions.
    - Under Grant select Grant Access and check either Require multifactor authentication or Require authentication strength.
    - Click Select at the bottom of the pane.
4. Under Enable policy set it to Report-only until the organization is ready to enable it.
5. Click Create.

**At minimum these directory roles should be included for MFA:**

- Application administrator
- Authentication administrator
- Billing administrator
- Cloud application administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Global reader
- Helpdesk administrator
- Password administrator
- Privileged authentication administrator
- Privileged role administrator
- Security administrator
- SharePoint administrator
- User administrator

**Note:** Report-only is an acceptable first stage when introducing any CA policy. The control, however, is not complete until the policy is on.

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.5 Require MFA for Administrative Access<br>Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. | ● | ● | ● |
| v7 | 16.3 Require Multi-factor Authentication<br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider. | | ● | ● |

### *5.2.2.2 (L1) Ensure multifactor authentication is enabled for all users (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Enable multifactor authentication for all users in the Microsoft 365 tenant. Users will be prompted to authenticate with a second factor upon logging in to Microsoft 365 services. The second factor is most commonly a text message to a registered mobile phone number where they type in an authorization code, or with a mobile application like Microsoft Authenticator.

**Rationale:**

Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

**Impact:**

Implementation of multifactor authentication for all users will necessitate a change to user routine. All users will be required to enroll in multifactor authentication using phone, SMS, or an authentication application. After enrollment, use of multifactor authentication will be required for future authentication to the environment.

External identities that attempt to access documents that utilize Purview Information Protection (Sensitivity Labels) will find their access disrupted. In order to mitigate this create an exclusion for `Microsoft Rights Management Services` ID: 00000012-0000-0000-c000-000000000000

**Note:** Organizations that struggle to enforce MFA globally due to budget constraints preventing the provision of company-owned mobile devices to every user, or due to regulations, unions, or policies that prevent forcing end users to use their personal devices, have another option. FIDO2 security keys can be used as an alternative. They are more secure, phishing-resistant, and affordable for organizations to issue to every end user.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `All users` is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `All resources (formerly 'All cloud apps')` is selected with no exclusions.
    - Under `Grant` verify `Grant Access` and either `Require multifactor authentication` or `Require authentication strength` is checked.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Click `New policy`.
    - Under `Users` include `All users`.
    - Under `Target resources` include `All resources (formerly 'All cloud apps')` and do not create any exclusions.
    - Under `Grant` select `Grant Access` and check either `Require multifactor authentication` or `Require authentication strength`.
    - Click `Select` at the bottom of the pane.
4. Under `Enable policy` set it to `Report-only` until the organization is ready to enable it.
5. Click `Create`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |
| v7 | 16.3 Require Multi-factor Authentication<br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider. | | ● | ● |

## *5.2.2.3 (L1) Enable Conditional Access policies to block legacy authentication (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Entra ID supports the most widely used authentication and authorization protocols including legacy authentication. This authentication pattern includes basic authentication, a widely used industry-standard method for collecting username and password information.

The following messaging protocols support legacy authentication:

- Authenticated SMTP - Used to send authenticated email messages.
- Autodiscover - Used by Outlook and EAS clients to find and connect to mailboxes in Exchange Online.
- Exchange ActiveSync (EAS) - Used to connect to mailboxes in Exchange Online.
- Exchange Online PowerShell - Used to connect to Exchange Online with remote PowerShell. If you block Basic authentication for Exchange Online PowerShell, you need to use the Exchange Online PowerShell Module to connect. For instructions, see Connect to Exchange Online PowerShell using multifactor authentication.
- Exchange Web Services (EWS) - A programming interface that's used by Outlook, Outlook for Mac, and third-party apps.
- IMAP4 - Used by IMAP email clients.
- MAPI over HTTP (MAPI/HTTP) - Primary mailbox access protocol used by Outlook 2010 SP2 and later.
- Offline Address Book (OAB) - A copy of address list collections that are downloaded and used by Outlook.
- Outlook Anywhere (RPC over HTTP) - Legacy mailbox access protocol supported by all current Outlook versions.
- POP3 - Used by POP email clients.
- Reporting Web Services - Used to retrieve report data in Exchange Online.
- Universal Outlook - Used by the Mail and Calendar app for Windows 10.
- Other clients - Other protocols identified as utilizing legacy authentication.

**Rationale:**

Legacy authentication protocols do not support multi-factor authentication. These protocols are often used by attackers because of this deficiency. Blocking legacy authentication makes it harder for attackers to gain access.

**Note:** Basic authentication is now disabled in all tenants. Before December 31 2022, you could re-enable the affected protocols if users and apps in your tenant couldn't connect. Now no one (you or Microsoft support) can re-enable Basic authentication in your tenant.

**Impact:**

Enabling this setting will prevent users from connecting with older versions of Office, ActiveSync or using protocols like IMAP, POP or SMTP and may require upgrades to older versions of Office, and use of mobile mail clients that support modern authentication.

This will also cause multifunction devices such as printers from using scan to e-mail function if they are using a legacy authentication method. Microsoft has mail flow best practices in the link below which can be used to configure a MFP to work with modern authentication:

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

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `All users` is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `All resources (formerly 'All cloud apps')` is selected.
    - Ensure that only documented resource exclusions exist and that they are reviewed annually.
    - Under `Conditions` select `Client apps` then verify `Exchange ActiveSync clients` and `Other clients` is checked.
    - Under `Grant` verify `Block access` is selected.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Create a new policy by selecting `New policy`.
    - Under `Users` include `All users`.
    - Under `Target resources` include `All resources (formerly 'All cloud apps')`.
    - Under `Conditions` select `Client apps` and check the boxes for `Exchange ActiveSync clients` and `Other clients`.
    - Under `Grant` select `Block Access`.
    - Click `Select`.
4. Set the policy `On` and click `Create`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Default Value:**

Basic authentication is disabled by default as of January 2023.

**References:**

1. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online
2. 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
3. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |
| v7 | 9.2 Ensure Only Approved Ports, Protocols and Services Are Running<br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system. | | ● | ● |

### *5.2.2.4 (L1) Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

In complex deployments, organizations might have a need to restrict authentication sessions. Conditional Access policies allow for the targeting of specific user accounts. Some scenarios might include:

- Resource access from an unmanaged or shared device
- Access to sensitive information from an external network
- High-privileged users
- Business-critical applications

**Note:** This CA policy can be added to the previous CA policy in this benchmark "Ensure multifactor authentication is enabled for all users in administrative roles"

**Rationale:**

Forcing a time out for MFA will help ensure that sessions are not kept alive for an indefinite period of time, ensuring that browser sessions are not persistent will help in prevention of drive-by attacks in web browsers, this also prevents creation and saving of session cookies leaving nothing for an attacker to take.

**Impact:**

Users with Administrative roles will be prompted at the frequency set for MFA.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `Directory roles` specific to administrators are included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `All resources (formerly 'All cloud apps')` is selected.
    - Ensure that only documented resource exclusions exist and that they are reviewed annually.
    - Under `Session` verify `Sign-in frequency` is checked and set to `Periodic reauthentication`.
    - Verify the timeframe is set to the time determined by the organization.
    - Ensure `Periodic reauthentication` does not exceed `4 hours` (or less).
    - Verify `Persistent browser session` is set to `Never persistent`.
4. Ensure `Enable policy` is set to `On`

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Note:** A list of directory roles applying to Administrators can be found in the remediation section.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Click `New policy`.
    - Under `Users` include `Select users and groups` and check `Directory roles`.
    - At a minimum, include the directory roles listed below in this section of the document.
    - Under `Target resources` include `All resources (formerly 'All cloud apps')`.
    - Under `Grant` select `Grant Access` and check `Require multifactor authentication`.
    - Under `Session` select `Sign-in frequency` select `Periodic reauthentication` and set it to `4 hours` (or less).
    - Check `Persistent browser session` then select `Never persistent` in the drop-down menu.
4. Under `Enable policy` set it to `Report-only` until the organization is ready to enable it.

**At minimum these directory roles should be included in the policy:**

- Application administrator
- Authentication administrator
- Billing administrator
- Cloud application administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Global reader
- Helpdesk administrator
- Password administrator
- Privileged authentication administrator
- Privileged role administrator
- Security administrator
- SharePoint administrator
- User administrator

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Default Value:**

The default configuration for user sign-in frequency is a rolling window of 90 days.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-session-lifetime

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.3 Configure Automatic Session Locking on Enterprise Assets<br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. | ● | ● | ● |
| v7 | 16.3 Require Multi-factor Authentication<br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider. | | ● | ● |

## *5.2.2.5 (L2) Ensure 'Phishing-resistant MFA strength' is required for Administrators (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Authentication strength is a Conditional Access control that allows administrators to specify which combination of authentication methods can be used to access a resource. For example, they can make only phishing-resistant authentication methods available to access a sensitive resource. But to access a non-sensitive resource, they can allow less secure multifactor authentication (MFA) combinations, such as password + SMS.

Microsoft has 3 built-in authentication strengths. MFA strength, Passwordless MFA strength, and Phishing-resistant MFA strength. Ensure administrator roles are using a CA policy with `Phishing-resistant MFA strength`.

Administrators can then enroll using one of 3 methods:

- FIDO2 Security Key
- Windows Hello for Business
- Certificate-based authentication (Multi-Factor)

**Note:** Additional steps to configure methods such as FIDO2 keys are not covered here but can be found in related MS articles in the references section. The Conditional Access policy only ensures 1 of the 3 methods is used.

**Warning:** Administrators should be pre-registered for a strong authentication mechanism before this Conditional Access Policy is enforced. Additionally, as stated elsewhere in the CIS Benchmark a break-glass administrator account should be excluded from this policy to ensure unfettered access in the case of an emergency.

**Rationale:**

Sophisticated attacks targeting MFA are more prevalent as the use of it becomes more widespread. These 3 methods are considered phishing-resistant as they remove passwords from the login workflow. It also ensures that public/private key exchange can only happen between the devices and a registered provider which prevents login to fake or phishing websites.

**Impact:**

If administrators aren't pre-registered for a strong authentication method prior to a conditional access policy being created, then a condition could occur where a user can't register for strong authentication because they don't meet the conditional access policy requirements and therefore are prevented from signing in.

Additionally, Internet Explorer based credential prompts in PowerShell do not support prompting for a security key. Implementing phishing-resistant MFA with a security key may prevent admins from running their existing sets of PowerShell scripts. Device Authorization Grant Flow can be used as a workaround in some instances.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `Directory roles` specific to administrators are included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Directory Roles should include at minimum the roles listed in the remediation section.
    - Under `Target resources` verify `All resources (formerly 'All cloud apps')` is selected with no exclusions.
    - Under `Grant` verify `Grant Access` is selected and `Require authentication strength` is checked with `Phishing-resistant MFA` set as the value.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Click `New policy`.
    - Under `Users` include `Select users and groups` and check `Directory roles`.
    - At a minimum, include the directory roles listed below in this section of the document.
    - Under `Target resources` include `All resources (formerly 'All cloud apps')` and do not create any exclusions.
    - Under `Grant` select `Grant Access` and check `Require authentication strength` and set `Phishing-resistant MFA` in the dropdown box.
    - Click `Select`.
4. Under `Enable policy` set it to `Report-only` until the organization is ready to enable it.
5. Click `Create`.

**At minimum these directory roles should be included for the policy:**

- Application administrator
- Authentication administrator
- Billing administrator
- Cloud application administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Global reader
- Helpdesk administrator
- Password administrator
- Privileged authentication administrator
- Privileged role administrator
- Security administrator
- SharePoint administrator
- User administrator

**Warning:** Ensure administrators are pre-registered with strong authentication before enforcing the policy. After which the policy must be set to `On`.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless#fido2-security-keys
2. https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2
3. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths
4. https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-mfa-policy

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.5 Require MFA for Administrative Access<br>Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. | ● | ● | ● |

## *5.2.2.6 (L1) Enable Identity Protection user risk policies (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Microsoft Entra ID Protection user risk policies detect the probability that a user account has been compromised.

**Note:** While Identity Protection also provides two risk policies with limited conditions, Microsoft highly recommends setting up risk-based policies in Conditional Access as opposed to the "legacy method" for the following benefits:

- Enhanced diagnostic data
- Report-only mode integration
- Graph API support
- Use more Conditional Access attributes like sign-in frequency in the policy

**Rationale:**

With the user risk policy turned on, Entra ID protection detects the probability that a user account has been compromised. Administrators can configure a user risk conditional access policy to automatically respond to a specific user risk level.

**Impact:**

Upon policy activation, account access will be either blocked or the user will be required to use multi-factor authentication (MFA) and change their password. Users without registered MFA will be denied access, necessitating an admin to recover the account. To avoid inconvenience, it is advised to configure the MFA registration policy for all users under the User Risk policy.

Additionally, users identified in the Risky Users section will be affected by this policy. To gain a better understanding of the impact on the organization's environment, the list of Risky Users should be reviewed before enforcing the policy.

**Audit:**

**To audit using the UI:**

1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com.
2. Click expand ID Protection > Risk-based Conditional Access.
3. Ensure that a policy exists with the following criteria and is set to On:
    - Under Users verify All users is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under Target resources verify All resources (formerly 'All cloud apps') is selected.
    - Under Conditions verify User risk is set to High.
    - Under Grant verify Grant access is selected and either Require multifactor authentication or Require authentication strength are checked. Then verify Require password change is checked.
    - Under Session ensure Sign-in frequency is set to Every time.
4. Ensure Enable policy is set to On.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com.
2. Click expand ID Protection > Risk-based Conditional Access.
3. Create a new policy by selecting New policy.
4. Set the following conditions within the policy:
    - Under Users choose All users
    - Under Target resources choose All resources (formerly 'All cloud apps')
    - Under Conditions choose User risk then Yes and select the user risk level High.
    - Under Grant select Grant access then check Require multifactor authentication or Require authentication strength. Finally check Require password change.
    - Under Session set Sign-in frequency to Every time.
    - Click Select.
5. Under Enable policy set it to Report-only until the organization is ready to enable it.
6. Click Create or Save.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**References:**

1. https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-risk-feedback
2. https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 13.3 Deploy a Network Intrusion Detection Solution<br>Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. | | ● | ● |
| v7 | 16.13 Alert on Account Login Behavior Deviation<br>Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration. | | | ● |

## *5.2.2.7 (L1) Enable Identity Protection sign-in risk policies (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Microsoft Entra ID Protection sign-in risk detects risks in real-time and offline. A risky sign-in is an indicator for a sign-in attempt that might not have been performed by the legitimate owner of a user account.

**Note:** While Identity Protection also provides two risk policies with limited conditions, Microsoft highly recommends setting up risk-based policies in Conditional Access as opposed to the "legacy method" for the following benefits:

- Enhanced diagnostic data
- Report-only mode integration
- Graph API support
- Use more Conditional Access attributes like sign-in frequency in the policy

**Rationale:**

Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication.

**Impact:**

When the policy triggers, the user will need MFA to access the account. In the case of a user who hasn't registered MFA on their account, they would be blocked from accessing their account. It is therefore recommended that the MFA registration policy be configured for all users who are a part of the Sign-in Risk policy.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `All users` is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `All resources (formerly 'All cloud apps')` is selected.
    - Under `Conditions` verify `Sign-in risk` is set to `Yes` ensuring `High` and `Medium` are selected.
    - Under `Grant` verify grant `Grant access` is selected and `Require multifactor authentication` checked.
    - Under `Session` verify `Sign-in Frequency` is set to `Every time`.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Create a new policy by selecting `New policy`.
4. Set the following conditions within the policy.
    - Under `Users` choose `All users`.
    - Under `Target resources` choose `All resources (formerly 'All cloud apps')`.
    - Under `Conditions` choose `Sign-in risk` then `Yes` and check the risk level boxes `High` and `Medium`.
    - Under `Grant` click `Grant access` then select `Require multifactor authentication`.
    - Under `Session` select `Sign-in Frequency` and set to `Every time`.
    - Click `Select`.
5. Under `Enable policy` set it to `Report-only` until the organization is ready to enable it.
6. Click `Create`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**References:**

1. https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-risk-feedback
2. https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 13.3 Deploy a Network Intrusion Detection Solution<br>Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. | | ● | ● |
| v7 | 16.13 Alert on Account Login Behavior Deviation<br>Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration. | | | ● |

## *5.2.2.8 (L2) Ensure 'sign-in risk' is blocked for medium and high risk (Automated)*

**Profile Applicability:**

- E5 Level 2

**Description:**

Microsoft Entra ID Protection sign-in risk detects risks in real-time and offline. A risky sign-in is an indicator for a sign-in attempt that might not have been performed by the legitimate owner of a user account.

**Note:** While Identity Protection also provides two risk policies with limited conditions, Microsoft highly recommends setting up risk-based policies in Conditional Access as opposed to the "legacy method" for the following benefits:

- Enhanced diagnostic data
- Report-only mode integration
- Graph API support
- Use more Conditional Access attributes like sign-in frequency in the policy

**Rationale:**

Sign-in risk is determined at the time of sign-in and includes criteria across both real-time and offline detections for risk. Blocking sign-in to accounts that have risk can prevent undesired access from potentially compromised devices or unauthorized users.

**Impact:**

Sign-in risk is heavily dependent on detecting risk based on atypical behaviors. Due to this it is important to run this policy in a report-only mode to better understand how the organization's environment and user activity may influence sign-in risk before turning the policy on. Once it's understood what actions may trigger a medium or high sign-in risk event I.T. can then work to create an environment to reduce false positives. For example, employees might be required to notify security personnel when they intend to travel with intent to access work resources.

**Note:** Break-glass accounts should always be excluded from risk detection.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `All users` is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `All resources (formerly 'All cloud apps')` is selected with no exclusions.
    - Under `Conditions` verify `Sign-in risk` values of `High` and `Medium` are selected.
    - Under `Grant` verify `Block access` is selected.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Create a new policy by selecting `New policy`.
4. Set the following conditions within the policy.
    - Under `Users` include `All users`.
    - Under `Target resources` include `All resources (formerly 'All cloud apps')` and do not set any exclusions.
    - Under `Conditions` choose `Sign-in risk` values of `High` and `Medium` and click `Done`.
    - Under `Grant` choose `Block access` and click `Select`.
5. Under `Enable policy` set it to `Report-only` until the organization is ready to enable it.
6. Click `Create`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**References:**

1. https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#risk-detections-mapped-to-riskeventtype

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 13.3 Deploy a Network Intrusion Detection Solution<br>Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. | | ● | ● |

### *5.2.2.9 (L1) Ensure a managed device is required for authentication (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Conditional Access (CA) can be configured to enforce access based on the device's compliance status or whether it is Entra hybrid joined. Collectively this allows CA to classify devices as managed or unmanaged, providing more granular control over authentication policies.

When using `Require device to be marked as compliant`, the device must pass checks configured in **Compliance** policies defined within Intune (Endpoint Manager). Before these checks can be applied, the device must first be enrolled in Intune MDM.

By selecting `Require Microsoft Entra hybrid joined device` this means the device must first be synchronized from an on-premises Active Directory to qualify for authentication.

When configured to the recommended state below only one condition needs to be met for the user to authenticate from the device. This functions as an "OR" operator.

The recommended state is:

- `Require device to be marked as compliant`
- `Require Microsoft Entra hybrid joined device`
- `Require one of the selected controls`

**Rationale:**

"Managed" devices are considered more secure because they often have additional configuration hardening enforced through centralized management such as Intune or Group Policy. These devices are also typically equipped with MDR/EDR, managed patching and alerting systems. As a result, they provide a safer environment for users to authenticate and operate from.

This policy also ensures that attackers must first gain access to a compliant or trusted device before authentication is permitted, reducing the risk posed by compromised account credentials. When combined with other distinct Conditional Access (CA) policies, such as requiring multi-factor authentication, this adds one additional factor before authentication is permitted.

**Note:** Avoid combining these two settings with other `Grant` settings in the same policy. In a single policy you can only choose between `Require all the selected controls` or `Require one of the selected controls`, which limits the ability to integrate this recommendation with others in this benchmark. CA policies function as an "AND" operator across multiple policies. The goal here is to both (Require MFA for all users) **AND** (Require device to be marked as compliant **OR** Require Microsoft Entra hybrid joined device).

**Impact:**

Unmanaged devices will not be permitted as a valid authenticator. As a result this may require the organization to mature their device enrollment and management. The following devices can be considered managed:

- Entra hybrid joined from Active Directory
- Entra joined and enrolled in Intune, with compliance policies
- Entra registered and enrolled in Intune, with compliances policies

If `Guest or external users` are collaborating with the organization, they must either be excluded or onboarded with a compliant device to authenticate. Failure to adequately survey the environment and test the Conditional Access (CA) policy in the `Report-only` state could result in access disruptions for these guest users.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `All users` is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `All resources (formerly 'All cloud apps')` is selected.
    - Ensure that only documented resource exclusions exist and that they are reviewed annually.
    - Under `Grant` verify that only `Require device to be marked as compliant` and `Require Microsoft Entra hybrid joined device` are checked.
    - Under `Grant` verify `Require one of the selected controls` is selected.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Create a new policy by selecting `New policy`.
    - Under `Users` include `All users`.
    - Under `Target resources` include `All resources (formerly 'All cloud apps')`.
    - Under `Grant` select `Grant access`.
    - Select only the checkboxes `Require device to be marked as compliant` and `Require Microsoft Entra hybrid joined device`.
    - Choose `Require one of the selected controls` and click `Select` at the bottom.
4. Under `Enable policy` set it to `Report-only` until the organization is ready to enable it.
5. Click `Create`.

**Note:** Guest user accounts, if collaborating with the organization, should be considered when testing this policy.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant#require-device-to-be-marked-as-compliant
2. https://learn.microsoft.com/en-us/entra/identity/devices/concept-hybrid-join
3. https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |

### *5.2.2.10 (L1) Ensure a managed device is required to register security information (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Conditional Access (CA) can be configured to enforce access based on the device's compliance status or whether it is Entra hybrid joined. Collectively this allows CA to classify devices as managed or not, providing more granular control over whether or not a user can register MFA on a device.

When using `Require device to be marked as compliant`, the device must pass checks configured in **Compliance** policies defined within Intune (Endpoint Manager). Before these checks can be applied, the device must first be enrolled in Intune MDM.

By selecting `Require Microsoft Entra hybrid joined device` this means the device must first be synchronized from an on-premises Active Directory to qualify for authentication.

When configured to the recommended state below only one condition needs to be met for the user to register MFA from the device. This functions as an "OR" operator.

The recommended state is to restrict `Register security information` to a device that is marked as compliant or Entra hybrid joined.

**Rationale:**

Requiring registration on a managed device significantly reduces the risk of bad actors using stolen credentials to register security information. Accounts that are created but never registered with an MFA method are particularly vulnerable to this type of attack. Enforcing this requirement will both reduce the attack surface for fake registrations and ensure that legitimate users register using trusted devices which typically have additional security measures in place already.

**Impact:**

The organization will be required to have a mature device management process. New devices provided to users will need to be pre-enrolled in Intune, auto-enrolled or be Entra hybrid joined. Otherwise, the user will be unable to complete registration, requiring additional resources from I.T. This could be more disruptive in remote worker environments where the MDM maturity is low.

In these cases where the person enrolling in MFA (enrollee) doesn't have physical access to a managed device, a help desk process can be created using a Teams meeting to complete enrollment using: 1) a durable process to verify the enrollee's identity including government identification with a photograph held up to the camera, information only the enrollee should know, and verification by the enrollee's direct manager in the same meeting; 2) complete enrollment in the same Teams meeting with the enrollee being granted screen and keyboard access to the help desk person's InPrivate Edge browser session.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `All users` is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `User actions` is selected with `Register security information` checked.
    - Under `Grant` verify that only `Require device to be marked as compliant` and `Require Microsoft Entra hybrid joined device` are checked.
    - Under `Grant` verify `Require one of the selected controls` is selected.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com.
2. Click expand ID Protection > Risk-based Conditional Access.
3. Create a new policy by selecting New policy.
    - Under Users include All users.
    - Under Target resources select User actions and check Register security information.
    - Under Grant select Grant access.
    - Check only Require multifactor authentication and Require Microsoft Entra hybrid joined device.
    - Choose Require one of the selected controls and click Select at the bottom.
4. Under Enable policy set it to Report-only until the organization is ready to enable it.
5. Click Create.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-grant#require-device-to-be-marked-as-compliant
2. https://learn.microsoft.com/en-us/entra/identity/devices/concept-hybrid-join
3. https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment
4. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-cloud-apps#user-actions

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |

### *5.2.2.11 (L1) Ensure sign-in frequency for Intune Enrollment is set to 'Every time' (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource. The Microsoft Entra ID default configuration for user sign-in frequency is a rolling window of 90 days.

The recommended state is a `Sign-in frequency` of `Every time` for `Microsoft Intune Enrollment`

**Note:** Microsoft accounts for a five-minute clock skew when 'every time' is selected in a conditional access policy, ensuring that users are not prompted more frequently than once every five minutes.

**Rationale:**

Intune Enrollment is considered a sensitive action and should be safeguarded. An attack path exists that allows for a bypass of device compliance Conditional Access rule. This could allow compromised credentials to be used through a newly registered device enrolled in Intune, enabling persistence and privilege escalation.

Setting sign-in frequency to every time limits the timespan an attacker could use fresh credentials to enroll a new device to Intune.

**Impact:**

New users enrolling into Intune through an automated process may need to sign-in again if the enrollment process goes on for too long.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `All users` is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `Resources (formerly cloud apps)` includes `Microsoft Intune Enrollment`.
    - Under `Grant` verify `Require multifactor authentication` or `Require authentication strength` is checked.
    - Under `Session` verify `Sign-in frequency` is set to `Every time`.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Create a new policy by selecting `New policy`.
    - Under `Users` include `All users`.
    - Under `Target resources` select `Resources (formerly cloud apps)`, choose `Select resources` and add `Microsoft Intune Enrollment` to the list.
    - Under `Grant` select `Grant access`.
    - Check either `Require multifactor authentication` or `Require authentication strength`.
    - Under `Session` check `Sign-in frequency` and select `Every time`.
4. Under `Enable policy` set it to `Report-only` until the organization is ready to enable it.
5. Click `Create`.

**Note:** If the Microsoft Intune Enrollment cloud app isn't available then it must be created. To add the app for new tenants, a Microsoft Entra administrator must create a service principal object, with app ID `d4ebce55-015a-49b5-a083-c84d1797ae8c`, in PowerShell or Microsoft Graph.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Default Value:**

Sign-in frequency defaults to 90 days.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-session-lifetime#require-reauthentication-every-time
2. https://www.blackhat.com/eu-24/briefings/schedule/#unveiling-the-power-of-intune-leveraging-intune-for-breaking-into-your-cloud-and-on-premise-42176
3. https://www.glueckkanja.com/blog/security/2025/01/compliant-device-bypass-en/

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |

### *5.2.2.12 (L1) Ensure the device code sign-in flow is blocked (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

The Microsoft identity platform supports the device authorization grant, which allows users to sign in to input-constrained devices such as a smart TV, IoT device, or a printer. To enable this flow, the device has the user visit a webpage in a browser on another device to sign in. Once the user signs in, the device is able to get access tokens and refresh tokens as needed.

The recommended state is to `Block access` for `Device code flow` in Conditional Access.

**Rationale:**

Since August 2024, Microsoft has observed threat actors, such as Storm-2372, employing "device code phishing" attacks. These attacks deceive users into logging into productivity applications, capturing authentication tokens to gain further access to compromised accounts.

To mitigate this specific attack, block authentication code flows and permit only those from devices within trusted environments, identified by specific IP addresses.

**Impact:**

Some administrative overhead will be required for stricter management of these devices. Since exclusions do not violate compliance, this feature can still be utilized effectively within a controlled environment.

**Audit:**

**To audit using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Ensure that a policy exists with the following criteria and is set to `On`:
    - Under `Users` verify `All users` is included.
    - Ensure that only documented user exclusions exist and that they are reviewed annually.
    - Under `Target resources` verify `Resources (formerly cloud apps)` includes `All resources (formerly 'All cloud apps')`
    - Under `Conditions` > `Authentication flows` verify `Configure` is set to `Yes` and `Device code flow` is checked.
    - Under `Grant` verify `Block access` is selected.
4. Ensure `Enable policy` is set to `On`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**Remediation:**

**To remediate using the UI:**

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `ID Protection` > `Risk-based Conditional Access`.
3. Create a new policy by selecting `New policy`.
    - Under `Users` include `All users`.
    - Under `Target resources` > `Resources (formerly cloud apps)` include `All resources (formerly 'All cloud apps')`.
    - Under `Conditions` > `Authentication flows` set `Configure` is set to `Yes`, select `Device code flow` and click `Save`.
    - Under `Grant` select `Block access` and click `Select`.
4. Under `Enable policy` set it to `Report-only` until the organization is ready to enable it.
5. Click `Create`.

**Note:** Break-glass accounts should be excluded from all Conditional Access policies.

**References:**

1. https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-device-code
2. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-authentication-flows
3. https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
4. https://securing365.com/secure-your-device-code-auth-flows-now/
5. https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows#device-code-flow-policies

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 16.7 Use Standard Hardening Configuration Templates for Application Infrastructure<br>Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening. | | ● | ● |

### 5.2.3 Authentication Methods

### *5.2.3.1 (L1) Ensure Microsoft Authenticator is configured to protect against MFA fatigue (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Microsoft provides supporting settings to enhance the configuration of the Microsoft Authenticator application. These settings provide users with additional information and context when they receive MFA passwordless and push requests, including the geographic location of the request, the requesting application, and a requirement for number matching.

Ensure the following are `Enabled`.

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

**NOTE:** On February 27, 2023 Microsoft started enforcing number matching tenant-wide for all users using Microsoft Authenticator.

**Rationale:**

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

**Impact:**

Additional interaction will be required by end users using number matching as opposed to simply pressing "Approve" for login attempts.

**Audit:**

**To audit using the UI:**

1. Navigate to the Microsoft Entra admin center https://entra.microsoft.com.
2. Click to expand Entra ID > Authentication methods select Policies.
3. Under **Method** select Microsoft Authenticator.
4. Under Enable and Target verify the setting is set to Enable.
5. In the Include tab ensure All users is selected.
6. In the Exclude tab ensure only valid groups are present (i.e. Break Glass accounts).
7. Select Configure
8. Verify the following Microsoft Authenticator settings:
    - Require number matching for push notifications Status is set to Enabled, Target All users
    - Show application name in push and passwordless notifications is set to Enabled, Target All users
    - Show geographic location in push and passwordless notifications is set to Enabled, Target All users
9. In each setting select Exclude and verify only groups are present (i.e. Break Glass accounts).

**Remediation:**

**To remediate using the UI:**

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

**Note:** Valid groups such as break glass accounts can be excluded per organization policy.

**Default Value:**

Microsoft-managed

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.4 Require MFA for Remote Network Access<br>Require MFA for remote network access. | ● | ● | ● |

## *5.2.3.2 (L1) Ensure custom banned passwords lists are used (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

With Entra Password Protection, default global banned password lists are automatically applied to all users in an Entra ID tenant. To support business and security needs, custom banned password lists can be defined. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.

A custom banned password list should include some of the following examples:

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

**Rationale:**

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

**Impact:**

If a custom banned password list includes too many common dictionary words, or short words that are part of compound words, then perfectly secure passwords may be blocked. The organization should consider a balance between security and usability when creating a list.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Entra ID` > `Authentication methods`.
3. Select `Password protection`
4. Verify `Enforce custom list` is set to `Yes`
5. Verify `Custom banned password list` contains entries specific to the organization or matches a pre-determined list.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Directory.Read.All"`
2. Run the following commands:

```
$PwRuleSettings = '5cf42378-d67d-4f36-ba46-e8b86229381d'
Get-MgGroupSetting | Where-Object TemplateId -eq $PwRuleSettings |
    Select-Object -ExpandProperty Values
```

3. Ensure `EnableBannedPasswordCheck` is `True` and `BannedPasswordList` is populated with banned passwords.

**Remediation:**

**To remediate using the UI:**

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

**Note:** Below is a list of examples that can be used as a starting place. The references section contains more suggestions.

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

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad#custom-banned-password-list
2. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.2 Use Unique Passwords<br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | ● | ● | ● |

### *5.2.3.3 (L1) Ensure password protection is enabled for on-prem Active Directory (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Microsoft Entra Password Protection provides a global and custom banned password list. A password change request fails if there's a match in these banned password list. To protect on-premises Active Directory Domain Services (AD DS) environment, install and configure Entra Password Protection.

**Note**: This recommendation applies to Hybrid deployments only and will have no impact unless working with on-premises Active Directory.

**Rationale:**

This feature protects an organization by prohibiting the use of weak or leaked passwords. In addition, organizations can create custom banned password lists to prevent their users from using easily guessed passwords that are specific to their industry. Deploying this feature to Active Directory will strengthen the passwords that are used in the environment.

**Impact:**

The potential impact associated with implementation of this setting is dependent upon the existing password policies in place in the environment. For environments that have strong password policies in place, the impact will be minimal. For organizations that do not have strong password policies in place, implementation of Microsoft Entra Password Protection may require users to change passwords and adhere to more stringent requirements than they have been accustomed to.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Entra ID > Authentication methods.
3. Select Password protection and ensure that Enable password protection on Windows Server Active Directory is set to Yes and that Mode is set to Enforced.

**To audit using PowerShell:**

1. Connect to Microsoft Graph using Connect-MgGraph -Scopes "Directory.Read.All"
2. Run the following command:

```
(Get-MgGroupSetting | ? { $_.TemplateId -eq '5cf42378-d67d-4f36-ba46-e8b86229381d' }).Values
```

3. Ensure that EnableBannedPasswordCheckOnPremises is set to True and BannedPasswordCheckOnPremisesMode is set to Enforce.

**Remediation:**

**To remediate using the UI:**

- Download and install the Azure AD Password Proxies and DC Agents from the following location: https://www.microsoft.com/download/details.aspx?id=57071 After installed follow the steps below.

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Protection select Authentication methods.
3. Select Password protection and set Enable password protection on Windows Server Active Directory to Yes and Mode to Enforced.

**Default Value:**

Enable - Yes

Mode - Audit

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-ban-bad-on-premises-operations

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.2 Use Unique Passwords<br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | ● | ● | ● |
| v7 | 4.4 Use Unique Passwords<br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system. | | ● | ● |

### *5.2.3.4 (L1) Ensure all member users are 'MFA capable' (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Microsoft defines Multifactor authentication capable as being registered and enabled for a strong authentication method. The method must also be allowed by the authentication methods policy.

Ensure all member users are `MFA capable`.

**Rationale:**

Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted.

Users who are not `MFA Capable` have never registered a strong authentication method for multifactor authentication that is within policy and may not be using MFA. This could be a result of having never signed in, exclusion from a Conditional Access (CA) policy requiring MFA, or a CA policy does not exist. Reviewing this list of users will help identify possible lapses in policy or procedure.

**Impact:**

When using the UI audit method guest users will appear in the report and unless the organization is applying MFA rules to guests then they will need to be manually filtered. Accounts that provide on-premises directory synchronization also appear in these reports.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Authentication methods`.
3. Select `User registration details`.
4. Set the filter option `Multifactor authentication capable` to `Not Capable`.
5. Review the non-guest users in this list.
6. Excluding any exceptions users found in this report may require remediation.

**To audit using PowerShell:**

1. Connect to Graph using `Connect-MgGraph -Scopes "UserAuthenticationMethod.Read.All,AuditLog.Read.All"`
2. Run the following:

```
Get-MgReportAuthenticationMethodUserRegistrationDetail `
    -Filter "IsMfaCapable eq false and UserType eq 'Member'" |
        ft UserPrincipalName,IsMfaCapable,IsAdmin
```

3. Ensure `IsMfaCapable` is set to `True`.
4. Excluding any exceptions users found in this report may require remediation.

**Note:** The CA rule must be in place for a successful deployment of Multifactor Authentication. This policy is outlined in the conditional access section 5.2.2

**Note 2:** Possible exceptions include on-premises synchronization accounts.

**Remediation:**

Remediation steps will depend on the status of the personnel in question or configuration of Conditional Access policies and will not be covered in detail. Administrators should review each user identified on a case-by-case basis using the conditions below.

**User has never signed on:**

- Employment status should be reviewed, and appropriate action taken on the user account's roles, licensing and enablement.

**Conditional Access policy applicability:**

- Ensure a CA policy is in place requiring all users to use MFA.
- Ensure the user is not excluded from the CA MFA policy.
- Ensure the policy's state is set to `On`.
- Use `What if` to determine applicable CA policies. (Protection > Conditional Access > Policies)
- Review the user account in `Sign-in logs`. Under the `Activity Details` pane click the `Conditional Access` tab to view applied policies.

**Note:** Conditional Access is covered step by step in section 5.2.2

**References:**

1. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.reports/update-mgreportauthenticationmethoduserregistrationdetail?view=graph-powershell-1.0#-ismfacapable
2. https://learn.microsoft.com/en-us/entra/identity/monitoring-health/how-to-view-applied-conditional-access-policies
3. https://learn.microsoft.com/en-us/entra/identity/conditional-access/what-if-tool
4. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-authentication-methods-activity

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |
| v7 | 16.3 Require Multi-factor Authentication<br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider. | | ● | ● |

## *5.2.3.5 (L1) Ensure weak authentication methods are disabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Authentication methods support a wide variety of scenarios for signing in to Microsoft 365 resources. Some of these methods are inherently more secure than others but require more investment in time to get users enrolled and operational.

SMS and Voice Call rely on telephony carrier communication methods to deliver the authenticating factor.

The recommended state is to `Disable` these methods:

- SMS
- Voice Call

**Rationale:**

Traditional MFA methods such as SMS codes, email-based OTPs, and push notifications are becoming less effective against today's attackers. Sophisticated phishing campaigns have demonstrated that second factors can be intercepted or spoofed. Attackers now exploit social engineering, man-in-the-middle tactics, and user fatigue (e.g., MFA bombing) to bypass these mechanisms. These risks are amplified in distributed, cloud-first organizations with hybrid workforces and varied device ecosystems.

The SMS and Voice call methods are vulnerable to SIM swapping which could allow an attacker to gain access to your Microsoft 365 account.

**Impact:**

There may be increased administrative overhead in adopting more secure authentication methods depending on the maturity of the organization.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Entra ID > Authentication methods.
3. Select Policies.
4. Verify that the following methods in the Enabled column are set to No.
    - Method: SMS
    - Method: Voice call

**To audit using Powershell:**

1. Connect to Graph using Connect-MgGraph -Scopes "Policy.Read.All"
2. Run the following:

```
(Get-MgPolicyAuthenticationMethodPolicy).AuthenticationMethodConfigurations
```

3. Ensure Sms and Voice are disabled.

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Entra ID > Authentication methods.
3. Select Policies.
4. Inspect each method that is out of compliance and remediate:
    - Click on the method to open it.
    - Change the Enable toggle to the off position.
    - Click Save.

**Note:** If the save button remains greyed out after toggling a method off, then first turn it back on and then change the position of the Target selection (all users or select groups). Turn the method off again and save. This was observed to be a bug in the UI at the time this document was published.

**To remediate using Powershell:**

1. Connect to Graph using `Connect-MgGraph -Scopes "Policy.ReadWrite.AuthenticationMethod"`
2. Run the following to disable all three authentication methods:

```
$params = @(
        @{ Id = "Sms"; State = "disabled" },
        @{ Id = "Voice"; State = "disabled" }
)

Update-MgPolicyAuthenticationMethodPolicy -AuthenticationMethodConfigurations
$params
```

**Default Value:**

- SMS : Disabled
- Voice Call : Disabled

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods-manage
2. https://learn.microsoft.com/en-us/security/zero-trust/sfi/phishing-resistant-mfa#context-and-problem
3. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-sim-swapping

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |

### *5.2.3.6 (L1) Ensure system-preferred multifactor authentication is enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

System-preferred multifactor authentication (MFA) prompts users to sign in by using the most secure method they registered.

The user is prompted to sign-in with the most secure method according to the below order. The order of authentication methods is dynamic. It's updated by Microsoft as the security landscape changes, and as better authentication methods emerge.

1. Temporary Access Pass
2. Passkey (FIDO2)
3. Microsoft Authenticator notifications
4. External authentication methods
5. Time-based one-time password (TOTP)
6. Telephony
7. Certificate-based authentication

The recommended state is `Enabled`.

**Rationale:**

Regardless of the authentication method enabled by an administrator or set as preferred by the user, the system will dynamically select the most secure option available at the time of authentication. This approach acts as an additional safeguard to prevent the use of weaker methods, such as voice calls, SMS, and email OTPs, which may have been inadvertently left enabled due to misconfiguration or lack of configuration hardening.

Enforcing the default behavior also ensures the feature is not disabled.

**Impact:**

The Microsoft managed value of system-preferred MFA is Enabled and as such enforces the default behavior. No additional impact is expected.

**Note:** Due to known issues with certificate-based authentication (CBA) and system-preferred MFA, Microsoft moved CBA to the bottom of the list. It is still considered a strong authentication method.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Authentication methods`.
3. Select `Settings`.
4. Verify the **System-preferred multifactor authentication** `State` is set to `Enabled` and `All users` are included.
5. Ensure that only documented exclusions exist and that they are reviewed annually

**To audit using PowerShell:**

1. Connect to Microsoft Graph using Connect-MgGraph -Scopes "Policy.Read.AuthenticationMethod"
2. Run the following commands:

```
$Uri =
'https://graph.microsoft.com/beta/policies/authenticationMethodsPolicy'
(Invoke-MgGraphRequest -Method GET -Uri $Uri).systemCredentialPreferences
```

3. Ensure that `includeTargets` is set to `all_users` and `state` is set to `enabled`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Authentication methods`.
3. Select `Settings`.
4. Set the **System-preferred multifactor authentication** `State` to `Enabled` and include `All users`.
5. Any users exclusions should be documented and reviewed annually.

**Default Value:**

Microsoft Managed (Enabled)

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-system-preferred-multifactor-authentication
2. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-system-preferred-multifactor-authentication#how-does-system-preferred-mfa-determine-the-most-secure-method

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |

## *5.2.3.7 (L2) Ensure the email OTP authentication method is disabled (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Authentication methods support a wide variety of scenarios for signing in to Microsoft 365 resources. Some of these methods are inherently more secure than others but require more investment in time to get users enrolled and operational.

The email one-time passcode feature is a way to authenticate B2B collaboration users when they can't be authenticated through other means, such as Microsoft Entra ID, Microsoft account (MSA), or social identity providers. When a B2B guest user tries to redeem your invitation or sign in to your shared resources, they can request a temporary passcode, which is sent to their email address. Then they enter this passcode to continue signing in.

The recommended state is to `Disable` email OTP.

**Rationale:**

Traditional MFA methods such as SMS codes, email-based OTPs, and push notifications are becoming less effective against today’s attackers. Sophisticated phishing campaigns have demonstrated that second factors can be intercepted or spoofed. Attackers now exploit social engineering, man-in-the-middle tactics, and user fatigue (e.g., MFA bombing) to bypass these mechanisms. These risks are amplified in distributed, cloud-first organizations with hybrid workforces and varied device ecosystems.

**Impact:**

Disabling Email OTP will prevent one-time pass codes from being sent to unverified guest users accessing Microsoft 365 resources on the tenant such as "@yahoo.com". They will be required to use a personal Microsoft account, a managed Microsoft Entra account, be part of a federation or be configured as a guest in the host tenant's Microsoft Entra ID.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Entra ID > Authentication methods.
3. Select Policies.
4. Verify that Email OTP is set to No in the Enabled column.

**To audit using Powershell:**

1. Connect to Graph using Connect-MgGraph -Scopes "Policy.Read.All"
2. Run the following:

```
(Get-MgPolicyAuthenticationMethodPolicy).AuthenticationMethodConfigurations
```

3. Ensure the id type Email is set to disabled.

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Entra ID > Authentication methods.
3. Select Policies.
4. Click on Email OTP.
5. Change the Enable toggle to the off position\
6. Click Save.

**Note:** If the save button remains greyed out after toggling a method off, then first turn it back on and then change the position of the Target selection (all users or select groups). Turn the method off again and save. This was observed to be a bug in the UI at the time this document was published.

**To remediate using Powershell:**

1. Connect to Graph using `Connect-MgGraph -Scopes "Policy.ReadWrite.AuthenticationMethod"`
2. Run the following:

```
$params = @(
        @{ Id = "Email"; State = "disabled" }
)

Update-MgPolicyAuthenticationMethodPolicy -AuthenticationMethodConfigurations
$params
```

**Default Value:**

- Email OTP : Enabled

**References:**

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods-manage
2. https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode
3. https://learn.microsoft.com/en-us/security/zero-trust/sfi/phishing-resistant-mfa#context-and-problem

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.3 Require MFA for Externally-Exposed Applications<br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. | | ● | ● |

### 5.2.4 Password reset

## *5.2.4.1 (L1) Ensure 'Self service password reset enabled' is set to 'All' (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Note:** Effective Oct. 1st, 2022, Microsoft will begin to enable combined registration for all users in Entra ID tenants created before August 15th, 2020. Tenants created after this date are enabled with combined registration by default.

**Rationale:**

Enabling Self-Service Password Reset (SSPR) significantly reduces helpdesk interactions, streamlining support operations and improving user experience. Traditional methods involving temporary passwords pose notable security risks—they are often weak, predictable, and susceptible to interception. This creates a window of opportunity for threat actors to compromise accounts before users can update their credentials. SSPR minimizes credential exposure and strengthens overall identity protection.

**Impact:**

Users will be required to provide additional contact information to enroll in self-service password reset. Additionally, minor user education may be required for users that are used to calling a help desk for assistance with password resets.

**Note:** This is unavailable if using Entra Connect / Sync in a hybrid environment.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Entra ID` > `Password reset` select `Properties`.
3. Ensure `Self service password reset enabled` is set to `All`

**Remediation:**

**To remediate using the UI:**

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

**References:**

1. https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/let-users-reset-passwords?view=o365-worldwide
2. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr
3. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-registration-mfa-sspr-combined

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## 5.3 ID Governance

## *5.3.1 (L2) Ensure 'Privileged Identity Management' is used to manage roles (Automated)*

**Profile Applicability:**

- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

The implementation of Just in Time privileged access is likely to necessitate changes to administrator routine. Administrators will only be granted access to administrative roles when required. When administrators request role activation, they will need to document the reason for requiring role access, anticipated time required to have the access, and to reauthenticate to enable role access.

**Note:** If all global admins become eligible then there will be no global admin to receive notifications, by default. Alerts are sent to TenantAdmins, including Global Administrators, by default. To ensure proper receipt, configure alerts to be sent to security or operations staff with valid email addresses or a security operations center. Otherwise, after adoption of this recommendation, alerts sent to TenantAdmins may go unreceived due to the lack of a licensed permanently active Global Administrator.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity Governance` select `Privileged Identity Management`.
3. Under **Manage** select `Microsoft Entra Roles`.
4. Under **Manage** select `Roles`.
5. Inspect at a minimum the following sensitive roles to ensure the members are `Eligible` and not `Permanent`:

- `Application Administrator`
- `Authentication Administrator`
- `Azure Information Protection Administrator`
- `Billing Administrator`
- `Cloud Application Administrator`
- `Cloud Device Administrator`
- `Compliance Administrator`
- `Customer LockBox Access Approver`
- `Exchange Administrator`
- `Fabric Administrator`
- `Global Administrator`
- `HelpDesk Administrator`
- `Intune Administrator`
- `Kaizala Administrator`
- `License Administrator`
- `Microsoft Entra Joined Device Local Administrator`
- `Password Administrator`
- `Privileged Authentication Administrator`
- `Privileged Role Administrator`
- `Security Administrator`
- `SharePoint Administrator`
- `Skype for Business Administrator`
- `Teams Administrator`
- `User Administrator`

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity Governance` select `Privileged Identity Management`.
3. Under **Manage** select `Microsoft Entra Roles`.
4. Under **Manage** select `Roles`.
5. Inspect at a minimum the following sensitive roles. For each of the members that have an `ASSIGNMENT TYPE` of `Permanent`, click on the `...` and choose `Make eligible`:

- `Application Administrator`
- `Authentication Administrator`
- `Azure Information Protection Administrator`
- `Billing Administrator`
- `Cloud Application Administrator`
- `Cloud Device Administrator`
- `Compliance Administrator`
- `Customer LockBox Access Approver`
- `Exchange Administrator`
- `Fabric Administrator`
- `Global Administrator`
- `HelpDesk Administrator`
- `Intune Administrator`
- `Kaizala Administrator`
- `License Administrator`
- `Microsoft Entra Joined Device Local Administrator`
- `Password Administrator`
- `Privileged Authentication Administrator`
- `Privileged Role Administrator`
- `Security Administrator`
- `SharePoint Administrator`
- `Skype for Business Administrator`
- `Teams Administrator`
- `User Administrator`

**References:**

1. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.1 Establish an Access Granting Process<br>Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. | ● | ● | ● |
| v8 | 6.2 Establish an Access Revoking Process<br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. | ● | ● | ● |
| v7 | 4.1 Maintain Inventory of Administrative Accounts<br>Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. | | ● | ● |

### *5.3.2 (L1) Ensure 'Access reviews' for Guest Users are configured (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organization.

Ensure `Access reviews` for Guest Users are configured to be performed no less frequently than `monthly`.

**Rationale:**

Access to groups and applications for guests can change over time. If a guest user's access to a particular folder goes unnoticed, they may unintentionally gain access to sensitive data if a member adds new files or data to the folder or application. Access reviews can help reduce the risks associated with outdated assignments by requiring a member of the organization to conduct the reviews. Furthermore, these reviews can enable a fail-closed mechanism to remove access to the subject if the reviewer does not respond to the review.

**Impact:**

Access reviews that are ignored may cause guest users to lose access to resources temporarily.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity Governance` and select `Access reviews`
3. Inspect the access reviews, and ensure an access review is created with the following criteria:
    - `Overview`: `Scope` is set to `Guest users only` and status is `Active`
    - `Reviewers`: Ensure appropriate reviewer(s) are designated.
    - `Settings` > `General`: `Mail notifications` and `Reminders` are set to `Enable`
    - `Reviewers`: `Require reason on approval` is set to `Enable`
    - `Scheduling`: `Frequency` is `Monthly` or more frequent.
    - `When completed`: `Auto apply results to resource` is set to `Enable`
    - `When completed`: `If reviewers don't respond` is set to `Remove access`

**To audit using PowerShell:**

1. Connect to Microsoft Graph using `Connect-MgGraph -Scope AccessReview.Read.All`
2. Run the following script to output a list of Access Reviews that target only Guest Users.

```
$Uri =
'https://graph.microsoft.com/v1.0/identityGovernance/accessReviews/definition
s'
$Response = Invoke-MgGraphRequest -Uri $Uri -Method Get |
    Select-Object -ExpandProperty Value

$GuestReviews = $Response |
    Where-Object { $_.scope.query -match "userType eq 'Guest'" -or
    $_.scope.principalscopes.query -match "userType eq 'Guest'" }

$AccessReviewReport = foreach ($review in $GuestReviews) {
    $value = $review.settings
    $RecurrenceType = $value.recurrence.pattern.type
    $RecurrencePass = $RecurrenceType -eq 'absoluteMonthly' -or
                      $RecurrenceType -eq 'weekly'
    $IsCISCompliant = $review.status -eq 'InProgress' -and
        $value.mailNotificationsEnabled -eq $true -and
        $value.reminderNotificationsEnabled -eq $true -and
        $value.justificationRequiredOnApproval -eq $true -and
        $RecurrencePass -and
        $value.autoApplyDecisionsEnabled -eq $true -and
        $value.defaultDecision -eq 'Deny'

    [PSCustomObject]@{
        Name                            = $review.DisplayName
        Status                          = $review.Status
        mailNotificationsEnabled        = $value.mailNotificationsEnabled
        Reminders                       = $value.reminderNotificationsEnabled
        justificationRequiredOnApproval =
$value.justificationRequiredOnApproval
        Frequency                       = $RecurrenceType
        autoApplyDecisionsEnabled       = $value.autoApplyDecisionsEnabled
        defaultDecision                 = $value.defaultDecision
        IsCISCompliant                  = $IsCISCompliant
    }
}

$AccessReviewReport
```

3. Review the output, if nothing returns then the audit fails.
4. Only one access review that satisfies all required parameters is necessary to achieve compliance. A passing review must meet the below properties with their corresponding values. A `Frequency` of `weekly` is also considered a passing state.

```
Name                              : < Access review name >
Status                            : InProgress
mailNotificationsEnabled          : True
Reminders                         : True
justificationRequiredOnApproval   : True
Frequency                         : absoluteMonthly
autoApplyDecisionsEnabled         : True
defaultDecision                   : Deny
IsCISCompliant                    : True
```

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity Governance` and select `Access reviews`
3. Click `New access review`.
4. `Select what to review` choose `Teams + Groups`.
5. `Review Scope` set to `All Microsoft 365 groups with guest users`, do not exclude groups.
6. `Scope` set to `Guest users only` then click `Next: Reviews`.
7. `Select reviewers` an appropriate user that is NOT the guest user themselves.
8. `Duration (in days)` at most `3`.
9. `Review recurrence` is `Monthly` or more frequent.
10. `End` is set to `Never`, then click `Next: Settings`.
11. Check `Auto apply results to resource`.
12. Set `If reviewers don't respond` to `Remove access`.
13. Check the following: `Justification required`, `E-mail notifications`, `Reminders`.
14. Click `Next: Review + Create` and finally click `Create`.

**Default Value:**

By default access reviews are not configured.

**References:**

1. https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview
2. https://learn.microsoft.com/en-us/entra/id-governance/create-access-review

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.1 Establish and Maintain an Inventory of Accounts<br>Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | ● | ● | ● |
| v8 | 5.3 Disable Dormant Accounts<br>Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. | ● | ● | ● |

## *5.3.3 (L1) Ensure 'Access reviews' for privileged roles are configured (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organization.

Ensure `Access reviews` for high privileged Entra ID roles are done `monthly` or more frequently. These reviews should include **at a minimum** the roles listed below:

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

**Note:** An access review is created for each role selected after completing the process.

**Rationale:**

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

**Impact:**

In order to avoid disruption reviewers who have the authority to revoke roles should be trusted individuals who understand the significance of access reviews. Additionally, the principle of separation of duties should be applied to ensure that no administrator is responsible for reviewing their own access levels. This will cause additional administrative overhead.

If the reviews are configured to automatically revoke highly privileged roles like the Global Administrator role, then this could result in removing all Global Administrators from the organization. Care should be taken when configuring this setting especially in the case of break-glass accounts which would be included by association.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity Governance` and select `Privileged Identity Management`
3. Select `Microsoft Entra Roles` under Manage
4. Select `Access reviews`
5. Ensure there are access reviews configured for each high privileged roles and each meets the criteria laid out below:
    - `Scope` - `Everyone`
    - `Status` - `Active`
    - `Reviewers` - Role reviewers should be designated personnel. Preferably not a self-review.
    - `Mail notifications` - `Enable`
    - `Reminders` - `Enable`
    - `Require reason on approval` - `Enable`
    - `Frequency` - `Monthly` or more frequently.
    - `Duration (in days)` - `14` at most
    - `Auto apply results to resource` - `Enable`
    - `If reviewers don't respond` - `No change`

Any remaining settings are discretionary.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity Governance` and select `Privileged Identity Management`
3. Select `Microsoft Entra Roles` under Manage
4. Select `Access reviews` and click `New access review`.
    - Provide a name and description.
    - Set `Frequency` to `Monthly` or more frequently.
    - Set `Duration (in days)` to at most `14`.
    - Set `End` to `Never`.
    - Set `Users scope` to `All users and groups`.
    - In `Role` select these roles: `Global Administrator`,`Exchange Administrator`,`SharePoint Administrator`,`Teams Administrator`,`Security Administrator`
    - Set `Assignment type` to `All active and eligible assignments`.
    - Set `Reviewers` member(s) responsible for this type of review, other than self.
5. **Upon completion settings:**
    - Set `Auto apply results to resource` to `Enable`.
    - Set `If reviewers don't respond` to `No change`.
6. **Advanced settings:**
    - Set `Show recommendations` to `Enable`
    - Set `Require reason on approval` to `Enable`
    - Set `Mail notifications` to `Enable`
    - Set `Reminders` to `Enable`
7. Click `Start` to save the review.

**Warning:** Care should be taken when configuring the `If reviewers don't respond` setting for Global Administrator reviews, if misconfigured break-glass accounts could automatically have roles revoked. Additionally, reviewers should be educated on the purpose of break-glass accounts to prevent accidental manual removal of roles.

**Default Value:**

By default access reviews are not configured.

**References:**

1. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-create-roles-and-resource-roles-review
2. https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.1 Establish and Maintain an Inventory of Accounts<br>Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently. | ● | ● | ● |
| v8 | 5.3 Disable Dormant Accounts<br>Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported. | ● | ● | ● |

## *5.3.4 (L1) Ensure approval is required for Global Administrator role activation (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Microsoft Entra Privileged Identity Management can be used to audit roles, allow just in time activation of roles and allow for periodic role attestation. Requiring approval before activation allows one of the selected approvers to first review and then approve the activation prior to PIM granted the role. The approver doesn't have to be a group member or owner.

The recommended state is `Require approval to activate` for the `Global Administrator` role.

**Rationale:**

Requiring approval for Global Administrator role activation enhances visibility and accountability every time this highly privileged role is used. This process reduces the risk of an attacker elevating a compromised account to the highest privilege level, as any activation must first be reviewed and approved by a trusted party.

**Note:** This only acts as protection for eligible users that are activating a role. Directly assigning a role does require an approval workflow so therefore it is important to implement and use PIM correctly.

**Impact:**

Approvers do not need to be assigned the same role or be members of the same group. It's important to have at least two approvers and an emergency access (break-glass) account to prevent a scenario where no Global Administrators are available. For example, if the last active Global Administrator leaves the organization, and only eligible but inactive Global Administrators remain, a trusted approver without the Global Administrator role or an emergency access account would be essential to avoid delays in critical administrative tasks.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity Governance` select `Privileged Identity Management`.
3. Under **Manage** select `Microsoft Entra Roles`.
4. Under **Manage** select `Roles`.
5. Select `Global Administrator` in the list.
6. Select `Role settings`..
7. Verify `Require approval to activate` is set to `Yes`.
8. Verify there are at least two `approvers` in the list.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity Governance` select `Privileged Identity Management`.
3. Under **Manage** select `Microsoft Entra Roles`.
4. Under **Manage** select `Roles`.
5. Select `Global Administrator` in the list.
6. Select `Role settings` and click `Edit`.
7. Check the `Require approval to activate` box.
8. Add at least two approvers.
9. Click `Update`.

**Default Value:**

`Require approval to activate` : `No`.

**References:**

1. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure
2. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/groups-role-settings#require-approval-to-activate

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.1 Establish an Access Granting Process<br>Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. | ● | ● | ● |
| v8 | 6.2 Establish an Access Revoking Process<br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. | ● | ● | ● |
| v7 | 4.1 Maintain Inventory of Administrative Accounts<br>Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. | | ● | ● |

## *5.3.5 (L1) Ensure approval is required for Privileged Role Administrator activation (Automated)*

**Profile Applicability:**

- E5 Level 1

**Description:**

Microsoft Entra Privileged Identity Management can be used to audit roles, allow just in time activation of roles and allow for periodic role attestation. Requiring approval before activation allows one of the selected approvers to first review and then approve the activation prior to PIM granted the role. The approver doesn't have to be a group member or owner.

The recommended state is `Require approval to activate` for the `Privileged Role Administrator` role.

**Rationale:**

This role grants the ability to manage assignments for all Microsoft Entra roles including the Global Administrator role. This role does not include any other privileged abilities in Microsoft Entra ID like creating or updating users. However, users assigned to this role can grant themselves or others additional privilege by assigning additional roles.

Requiring approval for activation enhances visibility and accountability every time this highly privileged role is used. This process reduces the risk of an attacker elevating a compromised account to the highest privilege level, as any activation must first be reviewed and approved by a trusted party.

**Note:** This only acts as protection for eligible users that are activating a role. Directly assigning a role does require an approval workflow so therefore it is important to implement and use PIM correctly.

**Impact:**

Requiring approvers for automatic role assignment can slightly increase administrative overhead and add delays to tasks.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity Governance` select `Privileged Identity Management`.
3. Under **Manage** select `Microsoft Entra Roles`.
4. Under **Manage** select `Roles`.
5. Select `Privileged Role Administrator` in the list.
6. Select `Role settings`.
7. Verify `Require approval to activate` is set to `Yes`.
8. Verify there are at least two `approvers` in the list.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity Governance` select `Privileged Identity Management`.
3. Under **Manage** select `Microsoft Entra Roles`.
4. Under **Manage** select `Roles`.
5. Select `Privileged Role Administrator` in the list.
6. Select `Role settings` and click `Edit`.
7. Check the `Require approval to activate` box.
8. Add at least two approvers.
9. Click `Update`.

**Default Value:**

`Require approval to activate` : `No`.

**References:**

1. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure
2. https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/groups-role-settings#require-approval-to-activate

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.1 Establish an Access Granting Process<br>Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. | ● | ● | ● |
| v8 | 6.2 Establish an Access Revoking Process<br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. | ● | ● | ● |
| v7 | 4.1 Maintain Inventory of Administrative Accounts<br>Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. | | ● | ● |

# 6 Exchange admin center

The Exchange admin center contains settings related to everything Exchange Online.

Direct link: https://admin.exchange.microsoft.com/

The PowerShell module most used in this section is `ExchangeOnlineManagement` and uses `Connect-ExchangeOnline` as the connection cmdlet.

The latest version of the module can be downloaded here:
https://www.powershellgallery.com/packages/ExchangeOnlineManagement/

## 6.1 Audit

## *6.1.1 (L1) Ensure 'AuditDisabled' organizationally is set to 'False' (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

The value False indicates that mailbox auditing on by default is turned on for the organization. Mailbox auditing on by default in the organization overrides the mailbox auditing settings on individual mailboxes. For example, if mailbox auditing is turned off for a mailbox (the AuditEnabled property on the mailbox is False), the default mailbox actions are still audited for the mailbox, because mailbox auditing on by default is turned on for the organization.

Turning off mailbox auditing on by default ($true) has the following results:

- Mailbox auditing is turned off for your organization.
- From the time you turn off mailbox auditing on by default, no mailbox actions are audited, even if mailbox auditing is enabled on a mailbox (the AuditEnabled property on the mailbox is True).
- Mailbox auditing isn't turned on for new mailboxes and setting the AuditEnabled property on a new or existing mailbox to True is ignored.
- Any mailbox audit bypass association settings (configured by using the Set-MailboxAuditBypassAssociation cmdlet) are ignored.
- Existing mailbox audit records are retained until the audit log age limit for the record expires.

The recommended state for this setting is `False` at the organization level. This will enable auditing and enforce the default.

**Rationale:**

Enforcing the default ensures auditing was not turned off intentionally or accidentally. Auditing mailbox actions will allow forensics and IR teams to trace various malicious activities that can generate TTPs caused by inbox access and tampering.

**Note:** Without advanced auditing (E5 function) the logs are limited to 90 days.

**Impact:**

None - this is the default behavior as of 2019.

**Audit:**

**To audit using PowerShell:**

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

```
Get-OrganizationConfig | Format-List AuditDisabled
```

3. Ensure `AuditDisabled` is set to `False`.

**Remediation:**

**To remediate using PowerShell:**

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

```
Set-OrganizationConfig -AuditDisabled $false
```

**Default Value:**

False

**References:**

1. https://learn.microsoft.com/en-us/purview/audit-mailboxes?view=o365-worldwide
2. https://learn.microsoft.com/en-us/powershell/module/exchange/set-organizationconfig?view=exchange-ps#-auditdisabled

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 8.2 Collect Audit Logs<br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. | ● | ● | ● |
| v7 | 6.2 Activate audit logging<br>Ensure that local logging has been enabled on all systems and networking devices. | ● | ● | ● |

## *6.1.2 (L1) Ensure mailbox audit actions are configured (Automated)*

**Profile Applicability:**

- E5 Level 1
- E3 Level 1

**Description:**

Mailbox audit logging is turned on by default in all organizations. This effort started in January 2019, and means that certain actions performed by mailbox owners, delegates, and admins are automatically logged. The corresponding mailbox audit records are available for admins to search in the mailbox audit log.

Mailboxes and shared mailboxes have actions assigned to them individually in order to audit the data the organization determines valuable at the mailbox level.

The recommended state per mailbox is `AuditEnabled` to `True` including all default audit actions with additional actions outlined below in the audit and remediation sections.

**Note:** Audit (Standard) licensing allows for up to 180 days log retention as of October 2023.

**Rationale:**

Whether it is for regulatory compliance or for tracking unauthorized configuration changes in Microsoft 365, enabling mailbox auditing and ensuring the proper mailbox actions are accounted for allows for Microsoft 365 teams to run security operations, forensics or general investigations on mailbox activities.

The following mailbox types ignore the organizational default and must have `AuditEnabled` set to `True` at the mailbox level in order to capture relevant audit data.

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

**Impact:**

Adding additional audit action types and increasing the AuditLogAgeLimit from 90 to 180 days will have a limited impact on mailbox storage. Mailbox audit log records are stored in a subfolder (named Audits) in the Recoverable Items folder in each user's mailbox.

- Mailbox audit records count against the storage quota of the Recoverable Items folder.
- Mailbox audit records also count against the folder limit for the Recoverable Items folder. A maximum of 3 million items (audit records) can be stored in the Audits subfolder.

The following cmdlet in Exchange Online PowerShell can be run to display the size and number of items in the Audits subfolder in the Recoverable Items folder:

```
Get-MailboxFolderStatistics -Identity <MailboxIdentity> -FolderScope
RecoverableItems |
Where-Object {$_.Name -eq 'Audits'} | Format-List
FolderPath,FolderSize,ItemsInFolder
```

**Note:** It's unlikely that mailbox auditing on by default impacts the storage quota or the folder limit for the Recoverable Items folder.

**Audit:**

Inspect each `UserMailbox` and ensure `AuditEnabled` is `True` and the following audit actions are included *in addition* to default actions of each sign-in type.

- Admin actions: `Copy`, `FolderBind` and `Move`.
- Delegate actions: `FolderBind` and `Move`.
- Owner actions: `Create`, `MailboxLogin` and `Move`.

**Note:** The defaults can be found in the **Default Value** section and the combined total can be found in the scripts of the Audit/Remediation sections.

**To audit using PowerShell:**

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

```
$AdminActions = @(
    "ApplyRecord", "Copy", "Create", "FolderBind", "HardDelete",
    "MailItemsAccessed", "Move", "MoveToDeletedItems", "SendAs",
    "SendOnBehalf", "Send", "SoftDelete", "Update",
"UpdateCalendarDelegation",
    "UpdateFolderPermissions", "UpdateInboxRules"
)

$DelegateActions = @(
    "ApplyRecord", "Create", "FolderBind", "HardDelete", "Move",
    "MailItemsAccessed", "MoveToDeletedItems", "SendAs", "SendOnBehalf",
    "SoftDelete", "Update", "UpdateFolderPermissions", "UpdateInboxRules"
)

$OwnerActions = @(
    "ApplyRecord", "Create", "HardDelete", "MailboxLogin", "Move",
    "MailItemsAccessed", "MoveToDeletedItems", "Send", "SoftDelete",
"Update",
    "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"
)

function VerifyActions {
    param (
        [array]$ExpectedActions,
        [array]$ActualActions
    )

    $Missing = $ExpectedActions | Where-Object { $_ -notin $ActualActions }
    return $Missing
}

$Mailboxes = Get-EXOMailbox -PropertySets Audit, Minimum -ResultSize
Unlimited |
Where-Object { $_.RecipientTypeDetails -eq "UserMailbox" }

$Results = foreach ($mailbox in $Mailboxes) {
    $AdminMissing = VerifyActions -ExpectedActions $AdminActions -
ActualActions $mailbox.AuditAdmin
    $DelegateMissing = VerifyActions -ExpectedActions $DelegateActions -
ActualActions $mailbox.AuditDelegate
    $OwnerMissing = VerifyActions -ExpectedActions $OwnerActions -
ActualActions $mailbox.AuditOwner

    $IsCompliant = $AdminMissing.Count -eq 0 -and
                   $DelegateMissing.Count -eq 0 -and
                   $OwnerMissing.Count -eq 0 -and
                   $mailbox.AuditEnabled

    [PSCustomObject]@{
        Mailbox         = $mailbox.UserPrincipalName
        AuditEnabled    = $mailbox.AuditEnabled
        AdminMissing    = if ($AdminMissing.Count -gt 0) { $AdminMissing -
join ", " } else { "None" }
        DelegateMissing = if ($DelegateMissing.Count -gt 0) {
$DelegateMissing -join ", " } else { "None" }
        OwnerMissing    = if ($OwnerMissing.Count -gt 0) { $OwnerMissing -
join ", " } else { "None" }
```

```
        ComplianceState = if ($IsCompliant) { "Compliant" } else { "Non-
Compliant" }
    }
}

# Display results in table format
$Results | Format-Table -AutoSize
<# Optional: Export methods
$Results | Out-GridView -Title "Mailbox Audit Results"
$Results | Export-Csv -Path "6.1.2.csv" -NoTypeInformation
$Results | ConvertTo-Json | Out-File -FilePath "6.1.2.json"
#>
```

3. Inspect the results. Mailboxes will be labeled as either `Compliant` or `Non-compliant`, accompanied by supporting details that outline the missing actions for each type and the current state of AuditEnabled. Optional methods for exporting the data to CSV, JSON, or GridView are also shown at the end of the script.

**Note:** Mailboxes with Audit (Premium) licenses, which is included with E5, can retain audit logs beyond 180 days.

**Remediation:**

For each `UserMailbox` ensure `AuditEnabled` is `True` and the following audit actions are included *in addition* to default actions of each sign-in type.

- Admin actions: `Copy`, `FolderBind` and `Move`.
- Delegate actions: `FolderBind` and `Move`.
- Owner actions: `Create`, `MailboxLogin` and `Move`.

**Note:** The defaults can be found in the **Default Value** section and the combined total can be found in the scripts of the Audit/Remediation sections.

**To remediate using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Run the following PowerShell script to remediate every 'UserMailbox' in the organization:

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

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

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


$MBX = Get-EXOMailbox -ResultSize Unlimited | Where-Object {
$_.RecipientTypeDetails -eq "UserMailbox" }
$MBX | Set-Mailbox -AuditEnabled $true `
-AuditLogAgeLimit 180 -AuditAdmin $AuditAdmin -AuditDelegate $AuditDelegate `
-AuditOwner $AuditOwner
```

3. The script will apply the prescribed Audit Actions for each sign-in type (Owner, Delegate, Admin) and the AuditLogAgeLimit to each UserMailbox in the organization.

**Note:** Mailboxes with Audit (Premium) licenses, which is included with E5, can retain audit logs beyond 180 days.

**Default Value:**

`AuditEnabled`: `True` for all mailboxes except below:

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

**AuditAdmin:** ApplyRecord, Create, HardDelete, MailItemsAccessed, MoveToDeletedItems, Send, SendAs, SendOnBehalf, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules

**AuditDelegate:** ApplyRecord, Create, HardDelete, MailItemsAccessed, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update, UpdateFolderPermissions, UpdateInboxRules

**AuditOwner:** ApplyRecord, HardDelete, MailItemsAccessed, MoveToDeletedItems, Send, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 8.2 Collect Audit Logs<br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. | ● | ● | ● |
| v7 | 6.2 Activate audit logging<br>Ensure that local logging has been enabled on all systems and networking devices. | ● | ● | ● |

## *6.1.3 (L1) Ensure 'AuditBypassEnabled' is not enabled on mailboxes (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

When configuring a user or computer account to bypass mailbox audit logging, the system will not record any access, or actions performed by the said user or computer account on any mailbox. Administratively this was introduced to reduce the volume of entries in the mailbox audit logs on trusted user or computer accounts.

Ensure `AuditBypassEnabled` is not enabled on accounts without a written exception.

**Rationale:**

If a mailbox audit bypass association is added for an account, the account can access any mailbox in the organization to which it has been assigned access permissions, without generating any mailbox audit logging entries for such access or recording any actions taken, such as message deletions.

Enabling this parameter, whether intentionally or unintentionally, could allow insiders or malicious actors to conceal their activity on specific mailboxes. Ensuring proper logging of user actions and mailbox operations in the audit log will enable comprehensive incident response and forensics.

**Impact:**

None - this is the default behavior.

**Audit:**

**To audit using PowerShell:**

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

```
$MBXData = Get-MailboxAuditBypassAssociation -ResultSize unlimited
$Report = $MBXData | ? {$_.AuditBypassEnabled -eq $true} |
select Name,AuditBypassEnabled

$Report
<# Optional: Export methods
$Report | Out-GridView -Title "Mailbox Audit Bypass Association"
$Report | Export-Csv -Path "6.1.3.csv" -NoTypeInformation
#>
```

3. If nothing is returned, then there are no accounts with Audit Bypass enabled.

**Note:** The cmdlet `Get-MailboxAuditBypassAssociation` may display a WARNING on system objects that begin with "Asc-2X1", this is not part of the Audit procedure and can be ignored.

**Remediation:**

**To remediate using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. The following example PowerShell script will disable AuditBypass for all mailboxes which currently have it enabled:

```
# Get mailboxes with AuditBypassEnabled set to $true
$MBXAudit = Get-MailboxAuditBypassAssociation -ResultSize unlimited | Where-
Object { $_.AuditBypassEnabled -eq $true }

foreach ($mailbox in $MBXAudit) {
    $mailboxName = $mailbox.Name
    Set-MailboxAuditBypassAssociation -Identity $mailboxName -
AuditBypassEnabled $false
    Write-Host "Audit Bypass disabled for mailbox Identity: $mailboxName" -
ForegroundColor Green
}
```

**Default Value:**

AuditBypassEnabled `False`

**References:**

1. https://learn.microsoft.com/en-us/powershell/module/exchange/get-mailboxauditbypassassociation?view=exchange-ps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 8.5 Collect Detailed Audit Logs<br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. | | ● | ● |

## 6.2 Mail flow

### *6.2.1 (L1) Ensure all forms of mail forwarding are blocked and/or disabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

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

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

**NOTE:** Any exclusions should be implemented based on organizational policy.

**Rationale:**

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

**Impact:**

Care should be taken before implementation to ensure there is no business need for case-by-case auto-forwarding. Disabling auto-forwarding to remote domains will affect all users and in an organization. Any exclusions should be implemented based on organizational policy.

**Audit:**

**Note:** *Audit is a two step procedure as follows:*

**STEP 1: Transport rules**

**To audit using the UI:**

1. Select `Exchange` to open the Exchange admin center.
2. Select `Mail Flow` then `Rules`.
3. Review the rules and verify that none of them are forwards or redirects e-mail to external domains.

**To audit using PowerShell:**

1. Connect to Exchange online using `Connect-ExchangeOnline`.
2. Run the following PowerShell command to review the Transport Rules that are redirecting email:

```
Get-TransportRule | Where-Object {$_.RedirectMessageTo -ne $null} | ft
Name,RedirectMessageTo
```

3. Verify that none of the addresses listed belong to external domains outside of the organization. If nothing returns then there are no transport rules set to redirect messages.

**STEP 2: Anti-spam outbound policy**

**To audit using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Expand `E-mail & collaboration` then select `Policies & rules`.
3. Select `Threat policies` > `Anti-spam`.
4. Inspect `Anti-spam outbound policy (default)` and ensure `Automatic forwarding` is set to `Off - Forwarding is disabled`
5. Inspect any additional custom outbound policies and ensure `Automatic forwarding` is set to `Off - Forwarding is disabled`, in accordance with the organization's exclusion policies.

**To audit using PowerShell:**

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

```
Get-HostedOutboundSpamFilterPolicy | ft Name, AutoForwardingMode
```

3. In each outbound policy verify `AutoForwardingMode` is `Off`.

**Note:** According to Microsoft if a recipient is defined in multiple policies of the same type (anti-spam, anti-phishing, etc.), only the policy with the highest priority is applied to the recipient. Any remaining policies of that type are not evaluated for the recipient (including the default policy). However, it is our recommendation to audit the default policy as well in the case a higher priority custom policy is removed. This will keep the organization's security posture strong.

**Remediation:**

**Note:** *Remediation is a two step procedure as follows:*

**STEP 1: Transport rules**

**To remediate using the UI:**

1. Select `Exchange` to open the Exchange admin center.
2. Select `Mail Flow` then `Rules`.
3. For each rule that redirects email to external domains, select the rule and click the 'Delete' icon.

**To remediate using PowerShell:**

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

```
Remove-TransportRule {RuleName}
```

**STEP 2: Anti-spam outbound policy**

**To remediate using the UI:**

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Expand `E-mail & collaboration` then select `Policies & rules`.
3. Select `Threat policies` > `Anti-spam`.
4. Select `Anti-spam outbound policy (default)`
5. Click `Edit protection settings`
6. Set `Automatic forwarding rules` dropdown to `Off - Forwarding is disabled` and click `Save`
7. Repeat steps 4-6 for any additional higher priority, custom policies.

**To remediate using PowerShell:**

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

```
Set-HostedOutboundSpamFilterPolicy -Identity {policyName} -AutoForwardingMode
Off
```

3. To remove AutoForwarding from all outbound policies you can also run:

```
Get-HostedOutboundSpamFilterPolicy | Set-HostedOutboundSpamFilterPolicy -
AutoForwardingMode Off
```

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *6.2.2 (L1) Ensure mail transport rules do not whitelist specific domains (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Rationale:**

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

**Note:** If an organization identifies a business need for an exception, the domain should only be whitelisted if inbound emails from that domain originate from a specific IP address. These exceptions should be documented and regularly reviewed.

**Impact:**

Care should be taken before implementation to ensure there is no business need for case-by-case whitelisting. Removing all whitelisted domains could affect incoming mail flow to an organization although modern systems sending legitimate mail should have no issue with this.

**Audit:**

**To audit using the UI:**

1. Navigate to `Exchange admin center` https://admin.exchange.microsoft.com..
2. Click to expand `Mail Flow` and then select `Rules`.
3. Review each rule and ensure that a single rule does not contain both of these properties together:
    - Under **Apply this rule if:** `Sender's address domain portion belongs to any of these domains: '<domain>'`
    - Under **Do the following:** `Set the spam confidence level (SCL) to '-1'`

**Note:** Setting the spam confidence level to -1 indicates the message is from a trusted sender, so the message bypasses spam filtering. The recommendation fails if any external domain has a SCL of -1.

**To audit using PowerShell:**

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

```
Get-TransportRule | Where-Object { $_.setscl -eq -1 -and $_.SenderDomainIs -
ne $null }  | ft Name,SenderDomainIs,SetSCL
```

3. Transport rules that fail the audit will be shown. If no output is shown, the recommendation passes. To pass, all rules with `SetSCL` set to `-1` must not include any domains in the `SenderDomainIs` property.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Exchange admin center` https://admin.exchange.microsoft.com..
2. Click to expand `Mail Flow` and then select `Rules`.
3. For each rule that sets the spam confidence level to -1 for a specific domain, select the rule and click `Delete`.

**To remediate using PowerShell:**

1. Connect to Exchange online using `Connect-ExchangeOnline`.
2. To modify the rule:

```
Remove-TransportRule {RuleName}
```

3. Verify the rules no longer exists by re-running the audit procedure.

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.7 Deploy and Maintain Email Server Anti-Malware Protections<br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing. | | | ● |

## *6.2.3 (L1) Ensure email from external senders is identified (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

External callouts provide a native experience to identify emails from senders outside the organization. This is achieved by presenting a new tag on emails called "External" (the string is localized based on the client language setting) and exposing related user interface at the top of the message reading view to see and verify the real sender's email address.

The recommended state is `ExternalInOutlook` set to `Enabled True`

**Rationale:**

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

Mail flow rules are often used by Exchange administrators to accomplish the External email tagging by appending a tag to the front of a subject line. There are limitations to this outlined here. The preferred method in the CIS Benchmark is to use the native experience.

**Note:** Existing emails in a user's inbox from external senders are not tagged retroactively.

**Impact:**

Mail flow rules using external tagging must be disabled, along with third-party mail filtering tools that offer similar features, to avoid duplicate [External] tags.

External tags can consume additional screen space on systems with limited real estate, such as thin clients or mobile devices.

After enabling this feature via PowerShell, it may take 24-48 hours for users to see the External sender tag in emails from outside your organization. Rolling back the feature takes the same amount of time.

**Note:** Third-party tools that provide similar functionality will also meet compliance requirements, although Microsoft recommends using the native experience for better interoperability.

**Audit:**

**To audit using PowerShell:**

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

```
Get-ExternalInOutlook
```

3. For each identity verify `Enabled` is set to `True` and the `AllowList` only contains email addresses the organization has permitted to bypass external tagging.

**Remediation:**

**To remediate using PowerShell:**

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

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

**Default Value:**

Disabled (False)

**References:**

1. https://techcommunity.microsoft.com/t5/exchange-team-blog/native-external-sender-callouts-on-email-in-outlook/ba-p/2250098
2. https://learn.microsoft.com/en-us/powershell/module/exchange/set-externalinoutlook?view=exchange-ps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## 6.3 Roles

## *6.3.1 (L2) Ensure users installing Outlook add-ins is not allowed (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Specify the administrators and users who can install and manage add-ins for Outlook in Exchange Online

By default, users can install add-ins in their Microsoft Outlook Desktop client, allowing data access within the client application.

**Rationale:**

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

**Impact:**

Implementing this change will impact both end users and administrators. End users will be unable to integrate third-party applications they desire, and administrators may receive requests to grant permission for necessary third-party apps.

**Audit:**

**To audit using the UI:**

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

**Note:** As of this release of the Benchmark the manage permissions link no longer displays anything when a user assigned the Global Reader role clicks on it. Global Readers as an alternative can inspect the Roles column or use the PowerShell method to perform the audit.

**To audit using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Run the following script:

```
$RoleList = @(
    "My Custom Apps", "My Marketplace Apps", "My ReadWriteMailbox Apps"
)

$AssignedPolicies = Get-EXOMailbox -PropertySets Policy |
Select-Object -Unique RoleAssignmentPolicy

$Report = foreach ($policy in $AssignedPolicies) {
    $RolePolicy = Get-RoleAssignmentPolicy -Identity `
        $policy.RoleAssignmentPolicy
    $NonCompliantRoles = $RolePolicy.AssignedRoles |
    Where-Object { $RoleList -eq $_ }

    [pscustomobject]@{
        Identity     = $RolePolicy.Identity
        FailingRoles = if ($NonCompliantRoles) {
            ($NonCompliantRoles -join ", ")
        }
        else { "None" }
    }
}

$Report
```

3. The output will show a list of all assigned policies and along with any roles assigned to those policies that are not compliant.
    - Verify `My Custom Apps`, `My Marketplace Apps` and `My ReadWriteMailbox Apps` are not present in any policy (Identity) displayed.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
$policy = "Role Assignment Policy - Prevent Add-ins"
$roles = "MyTextMessaging", "MyDistributionGroups", `
         "MyMailSubscriptions", "MyBaseOptions", "MyVoiceMail", `
         "MyProfileInformation", "MyContactInformation",
"MyRetentionPolicies", `
         "MyDistributionGroupMembership"

New-RoleAssignmentPolicy -Name $policy -Roles $roles
Set-RoleAssignmentPolicy -id $policy -IsDefault

# Assign new policy to all mailboxes
Get-EXOMailbox -ResultSize Unlimited | Set-Mailbox -RoleAssignmentPolicy
$policy
```

**If you have other Role Assignment Policies modify the last line to filter out your custom policies**

**Default Value:**

UI - `My Custom Apps`, `My Marketplace Apps`, and `My ReadWriteMailbox Apps` are checked

PowerShell - `My Custom Apps` `My Marketplace Apps` and `My ReadWriteMailbox Apps` are assigned

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions<br>Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications. | | ● | ● |
| v7 | 5.1 Establish Secure Configurations<br>Maintain documented, standard security configuration standards for all authorized operating systems and software. | ● | ● | ● |

## 6.4 Reports

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

## 6.5 Settings

## *6.5.1 (L1) Ensure modern authentication for Exchange Online is enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Modern authentication in Microsoft 365 enables authentication features like multifactor authentication (MFA) using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers. When you enable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use modern authentication to log in to Microsoft 365 mailboxes. When you disable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use basic authentication to log in to Microsoft 365 mailboxes.

When users initially configure certain email clients, like Outlook 2013 and Outlook 2016, they may be required to authenticate using enhanced authentication mechanisms, such as multifactor authentication. Other Outlook clients that are available in Microsoft 365 (for example, Outlook Mobile and Outlook for Mac 2016) always use modern authentication to log in to Microsoft 365 mailboxes.

**Rationale:**

Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by Exchange Online email clients such as Outlook 2016 and Outlook 2013. Enabling modern authentication for Exchange Online ensures strong authentication mechanisms are used when establishing sessions between email clients and Exchange Online.

**Impact:**

Users of older email clients, such as Outlook 2013 and Outlook 2016, will no longer be able to authenticate to Exchange using Basic Authentication, which will necessitate migration to modern authentication practices.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand Settings select Org Settings.
3. Select Modern authentication.
4. Verify Turn on modern authentication for Outlook 2013 for Windows and later (recommended) is checked.

**To audit using PowerShell:**

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

```
Get-OrganizationConfig | Format-Table -Auto Name, OAuth*
```

4. Verify OAuth2ClientProfileEnabled is True.

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft 365 admin center https://admin.microsoft.com.
2. Click to expand Settings select Org Settings.
3. Select Modern authentication.
4. Check Turn on modern authentication for Outlook 2013 for Windows and later (recommended) to enable modern authentication.

**To remediate using PowerShell:**

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

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $True
```

**Default Value:**

True

**References:**

1. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.10 Encrypt Sensitive Data in Transit<br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | | ● | ● |
| v7 | 16.3 Require Multi-factor Authentication<br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider. | | ● | ● |
| v7 | 16.5 Encrypt Transmittal of Username and Authentication Credentials<br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. | | ● | ● |

## *6.5.2 (L1) Ensure MailTips are enabled for end users (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Rationale:**

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

**Impact:**

Not applicable.

**Audit:**

**To audit using PowerShell:**

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

```
Get-OrganizationConfig | fl MailTips*
```

3. Verify the values for `MailTipsAllTipsEnabled`, `MailTipsExternalRecipientsTipsEnabled`, and `MailTipsGroupMetricsEnabled` are set to `True` and `MailTipsLargeAudienceThreshold` is set to an acceptable value; `25` is the default value.

**Remediation:**

**To remediate using PowerShell:**

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

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

Set-OrganizationConfig @TipsParams
```

**Default Value:**

MailTipsAllTipsEnabled: True MailTipsExternalRecipientsTipsEnabled: False MailTipsGroupMetricsEnabled: True MailTipsLargeAudienceThreshold: 25

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *6.5.3 (L2) Ensure additional storage providers are restricted in Outlook on the web (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

Ensure `AdditionalStorageProvidersAvailable` is restricted on the default OWA policy.

**Rationale:**

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

**Impact:**

The impact associated with this change is highly dependent upon current practices in the tenant. If users do not use other storage providers, then minimal impact is likely. However, if users do regularly utilize providers outside of the tenant this will affect their ability to continue to do so.

**Audit:**

**To audit using PowerShell:**

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. Run the following PowerShell command to audit the default OWA policy:

```
Get-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default |
fl AdditionalStorageProvidersAvailable
```

3. Verify that `AdditionalStorageProvidersAvailable` is `False`.

**Remediation:**

**To remediate using PowerShell:**

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

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

**Default Value:**

```
AdditionalStorageProvidersAvailable : True
```

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v7 | 13.1 Maintain an Inventory Sensitive Information<br>Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider. | ● | ● | ● |
| v7 | 13.4 Only Allow Access to Authorized Cloud Storage or Email Providers<br>Only allow access to authorized cloud storage or email providers. | | ● | ● |

## *6.5.4 (L1) Ensure SMTP AUTH is disabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting enables or disables authenticated client SMTP submission (SMTP AUTH) at an organization level in Exchange Online.

The recommended state is `Turn off SMTP AUTH protocol for your organization` (checked).

**Rationale:**

SMTP AUTH is a legacy protocol. Disabling it at the organization level supports the principle of least functionality and serves to further back additional controls that block legacy protocols, such as in Conditional Access. Virtually all modern email clients that connect to Exchange Online mailboxes in Microsoft 365 can do so without using SMTP AUTH.

**Impact:**

This enforces the default behavior, so no impact is expected unless the organization is using it globally. A per-mailbox setting exists that overrides the tenant-wide setting, allowing an individual mailbox SMTP AUTH capability for special cases.

**Audit:**

**To audit using the UI:**

1. Navigate to `Exchange admin center` https://admin.exchange.microsoft.com.
2. Select `Settings` > `Mail flow`.
3. Ensure `Turn off SMTP AUTH protocol for your organization` is checked.

**To audit using PowerShell:**

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

```
Get-TransportConfig | Format-List SmtpClientAuthenticationDisabled
```

3. Verify that the value returned is `True`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Exchange admin center` https://admin.exchange.microsoft.com.
2. Select `Settings` > `Mail flow`.
3. Check `Turn off SMTP AUTH protocol for your organization` to disable the protocol.

**To remediate using PowerShell:**

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

```
Set-TransportConfig -SmtpClientAuthenticationDisabled $true
```

**Default Value:**

SmtpClientAuthenticationDisabled : True

**References:**

1. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/authenticated-client-smtp-submission

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 12.6 Use of Secure Network Management and Communication Protocols<br>Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater). | | ● | ● |

## *6.5.5 (L2) Ensure Direct Send submissions are rejected (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Direct Send is a method used to send emails directly to an Exchange Online customer's hosted mailboxes from on-premises devices, applications, or third-party cloud services using the customer's own accepted domain. This method does not require any form of authentication because, by its nature, it mimics incoming anonymous emails from the internet, apart from the sender domain.

The recommended state is to configure `RejectDirectSend` to `True`.

**Rationale:**

Direct Send allows devices and applications to transmit unauthenticated email directly to Exchange Online. While this method may support legacy systems such as printers or scanners, it introduces significant security risks:

- Unauthenticated Email Delivery: Direct Send does not require authentication, making it an attractive vector for threat actors to deliver spoofed or malicious emails that appear to originate from trusted internal sources.
- Phishing and Spoofing Risks: Because these emails bypass standard authentication mechanisms, they can easily impersonate internal users or services, increasing the likelihood of successful phishing attacks.
- Lack of Visibility and Control: Emails sent via Direct Send may not be subject to the same security policies, logging, or filtering as authenticated traffic, reducing the organization's ability to monitor and respond to threats effectively.

Threat research from Varonis has shown that attackers are actively exploiting Direct Send to impersonate internal accounts and distribute malicious content without needing to compromise any credentials. These campaigns have successfully targeted organizations by leveraging predictable infrastructure and public user data to craft convincing phishing emails. Because these messages originate from outside the tenant but appear internal, they often evade detection and filtering mechanisms.

**Impact:**

Microsoft has identified some known issues with disabling Direct Send:

- There is a forwarding scenario that could be affected by this feature. It is possible that someone in your organization sends a message to a 3rd party and they in turn forward it to another mailbox in your organization. If the 3rd party's email provider does not support Sender Rewriting Scheme (SRS), the message will return with the original sender's address. Prior to this feature being enabled, those messages will already be punished by SPF failing but could still end up in inboxes. Enabling the Reject Direct Send feature without a partner mail flow connector being set up will lead to these messages being rejected outright.
- If you are using the Azure Communication Services (ACS) to send emails to your tenant, and if those emails are sent using a "MAIL FROM" address that is one of your Microsoft 365 accepted domains, enabling RejectDirectSend would block those emails sent to your Microsoft 365 tenant. A solution for ACS traffic to be compatible with the setting is being worked on. In case the domains used to send emails from ACS are not one of the Microsoft 365 accepted domains or sub-domains, enabling RejectDirectSend should not have an impact on ACS traffic. If ACS email traffic is using an Exchange Online domain where the MX is pointed to a 3rd party service, please refer to the FAQ's below, which provide instructions on mail connectors required to enable traffic in Exchange Online.

**Audit:**

**To audit using PowerShell:**

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

```
Get-OrganizationConfig | fl RejectDirectSend
```

3. Verify that the value returned for `RejectDirectSend` is `True`.

**Remediation:**

**To remediate using PowerShell:**

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

```
Set-OrganizationConfig -RejectDirectSend $true
```

**Default Value:**

RejectDirectSend : False

**References:**

1. https://techcommunity.microsoft.com/blog/exchange/introducing-more-control-over-direct-send-in-exchange-online/4408790?WT.mc_id=M365-MVP-9501
2. https://techcommunity.microsoft.com/blog/exchange/direct-send-vs-sending-directly-to-an-exchange-online-tenant/4439865
3. https://learn.microsoft.com/en-us/powershell/module/exchangepowershell/set-organizationconfig?view=exchange-ps
4. https://www.varonis.com/blog/direct-send-exploit
5. https://techcommunity.microsoft.com/discussions/microsoft-365/disable-direct-send-in-exchange-online-to-mitigate-ongoing-phishing-threats/4434649

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 12.6 Use of Secure Network Management and Communication Protocols<br>Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater). | | ● | ● |

# 7 SharePoint admin center

The SharePoint admin center contains settings related to SharePoint and OneDrive.

UI Direct link: https://admin.microsoft.com/sharepoint

The PowerShell module most used in this section is `Microsoft.Online.SharePoint.PowerShell` and uses `Connect-SPOService -Url https://contoso-admin.sharepoint.com` as the connection cmdlet (replacing tenant name with your value).

The latest version of the module can be downloaded here: https://www.powershellgallery.com/packages/Microsoft.Online.SharePoint.PowerShell/

## 7.1 Sites

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

## 7.2 Policies

## *7.2.1 (L1) Ensure modern authentication for SharePoint applications is required (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Rationale:**

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

**Impact:**

Implementation of modern authentication for SharePoint will require users to authenticate to SharePoint using modern authentication. This may cause a minor impact to typical user behavior.

This may also prevent third-party apps from accessing SharePoint Online resources. Also, this will also block apps using the SharePointOnlineCredentials class to access SharePoint Online resources.

**Audit:**

**To audit using the UI:**

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint.
2. Click to expand `Policies` select `Access control`.
3. Select `Apps that don't use modern authentication` and ensure that it is set to `Block access`.

**To audit using PowerShell:**

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com` replacing tenant with your value.
2. Run the following SharePoint Online PowerShell command:

```
Get-SPOTenant | ft LegacyAuthProtocolsEnabled
```

3. Ensure the returned value is `False`.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com` replacing tenant with your value.
2. Run the following SharePoint Online PowerShell command:

```
Set-SPOTenant -LegacyAuthProtocolsEnabled $false
```

**Default Value:**

True (Apps that don't use modern authentication are allowed)

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.10 Encrypt Sensitive Data in Transit<br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). | | ● | ● |
| v7 | 16.3 Require Multi-factor Authentication<br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider. | | ● | ● |

## *7.2.2 (L1) Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Note:** Global Reader role currently can't access SharePoint using PowerShell.

**Rationale:**

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

**Impact:**

B2B collaboration is used with other Entra services so should not be new or unusual. Microsoft also has made the experience seamless when turning on integration on SharePoint sites that already have active files shared with guest users. The referenced Microsoft article on the subject has more details on this.

**Audit:**

**To audit using PowerShell:**

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

```
Get-SPOTenant | ft EnableAzureADB2BIntegration
```

3. Ensure the returned value is `True`.

**Remediation:**

**To remediate using PowerShell:**

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

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

**Default Value:**

False

**References:**

1. https://learn.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration#enabling-the-integration
2. https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b
3. https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *7.2.3 (L1) Ensure external content sharing is restricted (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

The external sharing settings govern sharing for the organization overall. Each site has its own sharing setting that can be set independently, though it must be at the same or more restrictive setting as the organization.

The new and existing guests option requires people who have received invitations to sign in with their work or school account (if their organization uses Microsoft 365) or a Microsoft account, or to provide a code to verify their identity. Users can share with guests already in your organization's directory, and they can send invitations to people who will be added to the directory if they sign in.

The recommended state is `New and existing guests` or less permissive.

**Rationale:**

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

**Impact:**

When using B2B integration, Entra ID external collaboration settings, such as guest invite settings and collaboration restrictions apply.

**Audit:**

**To audit using the UI:**

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Click to expand Policies > Sharing.
3. Locate the External sharing section.
4. Under SharePoint, ensure the slider bar is set to New and existing guests or a less permissive level.

**To audit using PowerShell:**

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

```
Get-SPOTenant | fl SharingCapability
```

3. Ensure SharingCapability is set to one of the following values:
    - Value1: ExternalUserSharingOnly
    - Value2: ExistingExternalUserSharingOnly
    - Value3: Disabled

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

1. Connect to SharePoint Online service using Connect-SPOService.
2. Run the following cmdlet to establish the minimum recommended state:

```
Set-SPOTenant -SharingCapability ExternalUserSharingOnly
```

**Note:** Other acceptable values for this parameter that are more restrictive include: Disabled and ExistingExternalUserSharingOnly.

**Default Value:**

Anyone (ExternalUserAndGuestSharing)

**References:**

1. https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off
2. https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |

## *7.2.4 (L2) Ensure OneDrive content sharing is restricted (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

This setting governs the global permissiveness of OneDrive content sharing in the organization.

OneDrive content sharing can be restricted independent of SharePoint but can never be more permissive than the level established with SharePoint.

The recommended state is `Only people in your organization`.

**Rationale:**

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

**Impact:**

Users will be required to take additional steps to share OneDrive content or use other official channels.

**Audit:**

**To audit using the UI:**

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

**To audit using PowerShell:**

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

```
Get-SPOTenant | fl OneDriveSharingCapability
```

3. Ensure the returned value is Disabled.

**Alternative audit method using PowerShell:**

1. Connect to SharePoint Online.
2. Use one of the following methods:

```
# Replace [tenant] with your tenant id
Get-SPOSite -Identity https://[tenant]-my.sharepoint.com/ | fl
Url,SharingCapability

# Or run this to filter to the specific site without supplying the tenant
name.
$OneDriveSite = Get-SPOSite -Filter { Url -like "*-my.sharepoint.com/" }
Get-SPOSite -Identity $OneDriveSite | fl Url,SharingCapability
```

2. Ensure the returned value for SharingCapability is Disabled

**Note:** As of March 2024, using Get-SPOSite with Where-Object or filtering against the entire site and then returning the SharingCapability parameter can result in a different value as opposed to running the cmdlet specifically against the OneDrive specific site using the -Identity switch as shown in the example.

**Note 2:** The parameter OneDriveSharingCapability may not be yet fully available in all tenants. It is demonstrated in official Microsoft documentation as linked in the references section but not in the Set-SPOTenant cmdlet itself. If the parameter is unavailable, then either use the UI method or alternative PowerShell audit method.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
Set-SPOTenant -OneDriveSharingCapability Disabled
```

**Alternative remediation method using PowerShell:**

1. Connect to SharePoint Online.
2. Run one of the following:

```
# Replace [tenant] with your tenant id
Set-SPOSite -Identity https://[tenant]-my.sharepoint.com/ -SharingCapability
Disabled

# Or run this to filter to the specific site without supplying the tenant
name.
$OneDriveSite = Get-SPOSite -Filter { Url -like "*-my.sharepoint.com/" }
Set-SPOSite -Identity $OneDriveSite -SharingCapability Disabled
```

**Default Value:**

Anyone (ExternalUserAndGuestSharing)

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |

## *7.2.5 (L2) Ensure that SharePoint guest users cannot share items they don't own (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

The impact associated with this change is highly dependent upon current practices. If users do not regularly share with external parties, then minimal impact is likely. However, if users do regularly share with guests/externally, minimum impacts could occur as those external users will be unable to 're-share' content.

**Audit:**

**To audit using the UI:**

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

**To audit using PowerShell:**

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

```
Get-SPOTenant | ft PreventExternalUsersFromResharing
```

3. Ensure the returned value is True.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
Set-SPOTenant -PreventExternalUsersFromResharing $True
```

**Default Value:**

Checked (False)

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v7 | 14.6 Protect Information through Access Control Lists<br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

## *7.2.6 (L2) Ensure SharePoint external sharing is restricted (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

The external sharing features of SharePoint and OneDrive let users in the organization share content with people outside the organization (such as partners, vendors, clients, or customers). It can also be used to share between licensed users on multiple Microsoft 365 subscriptions if your organization has more than one subscription.

The recommended state is `Limit external sharing by domain` > `Allow only specific domains`

**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:**

Enabling this feature will prevent users from sharing documents with domains outside of the organization unless allowed.

**Audit:**

**To audit using the UI:**

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Expand Policies then click Sharing.
3. Expand More external sharing settings and confirm that Limit external sharing by domain is checked.
4. Click on Add domains and verify the the sub setting Allow only specific domains is selected and with an approved list domains.

**To audit using PowerShell:**

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

```
Get-SPOTenant | fl SharingDomainRestrictionMode,SharingAllowedDomainList
```

3. Ensure that SharingDomainRestrictionMode is set to AllowList and SharingAllowedDomainList contains domains trusted by the organization for external sharing.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
Set-SPOTenant -SharingDomainRestrictionMode AllowList -
SharingAllowedDomainList "domain1.com domain2.com"
```

**Default Value:**

Limit external sharing by domain is unchecked

SharingDomainRestrictionMode: None

SharingDomainRestrictionMode: <Undefined>

**References:**

1. https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo#more-external-sharing-settings

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v7 | 13.4 Only Allow Access to Authorized Cloud Storage or Email Providers<br>Only allow access to authorized cloud storage or email providers. | | ● | ● |
| v7 | 14.6 Protect Information through Access Control Lists<br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

## *7.2.7 (L1) Ensure link sharing is restricted in SharePoint and OneDrive (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting sets the default link type that a user will see when sharing content in OneDrive or SharePoint. It does not restrict or exclude any other options.

The recommended state is `Specific people (only the people the user specifies)` or `Only people in your organization` (more restrictive).

**Rationale:**

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

**Audit:**

**To audit using the UI:**

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to `File and folder links`.
4. Ensure that the setting `Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive` is set to `Specific people (only the people the user specifies)` or `Only people in your organization` (more restrictive).

**To audit using PowerShell:**

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

```
Get-SPOTenant | fl DefaultSharingLinkType
```

3. Ensure the returned value is `Direct` or `Internal` (more restrictive).

**Remediation:**

**To remediate using the UI:**

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to `File and folder links`.
4. Set `Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive` to `Specific people (only the people the user specifies)` or `Only people in your organization`.

**To remediate using PowerShell:**

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

```
Set-SPOTenant -DefaultSharingLinkType Direct
```

3. Or, to set a more restrictive state:

```
Set-SPOTenant -DefaultSharingLinkType Internal
```

**Default Value:**

Only people in your organization (Internal)

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |

## *7.2.8 (L2) Ensure external sharing is restricted by security group (Manual)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

The recommended state is `Enabled` or `Checked`.

**Note:** Users in these security groups must be allowed to invite guests in the guest invite settings in Microsoft Entra. Identity > External Identities > External collaboration settings

**Rationale:**

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

**Impact:**

OneDrive will also be governed by this and there is no granular control at the SharePoint site level.

**Audit:**

**To audit using the UI:**

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to and expand `More external sharing settings`.
4. Ensure the following:
    - Verify `Allow only users in specific security groups to share externally` is checked
    - Verify `Manage security groups` is defined and accordance with company procedure.

**Note:** The **More external sharing settings** drop down in step 3 above may be unavailable or limited if the **External Sharing** slider settings above are set to "Least permissive."

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

Unchecked/Undefined

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

## *7.2.9 (L1) Ensure guest access to a site or OneDrive will expire automatically (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

The recommended state is `30` or less.

**Rationale:**

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

**Note:** Guest membership applies at the Microsoft 365 group level. Guests who have permission to view a SharePoint site or use a sharing link may also have access to a Microsoft Teams team or security group.

**Impact:**

Site collection administrators will have to renew access to guests who still need access after 30 days. They will receive an e-mail notification once per week about guest access that is about to expire.

**Note:** The guest expiration policy only applies to guests who use sharing links or guests who have direct permissions to a SharePoint site after the guest policy is enabled. The guest policy does not apply to guest users that have pre-existing permissions or access through a sharing link before the guest expiration policy is applied.

**Audit:**

**To audit using the UI:**

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Click to expand Policies > Sharing.
3. Scroll to and expand More external sharing settings.
4. Ensure Guest access to a site or OneDrive will expire automatically after this many days is checked and set to 30 or less.

**To audit using PowerShell:**

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

```
Get-SPOTenant | fl ExternalUserExpirationRequired,ExternalUserExpireInDays
```

3. Ensure the following values are returned:
    - ExternalUserExpirationRequired is True.
    - ExternalUserExpireInDays is 30 or less.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
Set-SPOTenant -ExternalUserExpireInDays 30 -ExternalUserExpirationRequired
$True
```

**Default Value:**

ExternalUserExpirationRequired $false

ExternalUserExpireInDays 60 days

**References:**

1. https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off#change-the-organization-level-external-sharing-setting
2. https://learn.microsoft.com/en-us/microsoft-365/community/sharepoint-security-a-team-effort

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *7.2.10 (L1) Ensure reauthentication with verification code is restricted (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

The recommended state is `15` or less.

**Rationale:**

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

**Impact:**

Guests who use Microsoft 365 in their organization can sign in using their work or school account to access the site or document. After the one-time passcode for verification has been entered for the first time, guests will authenticate with their work or school account and have a guest account created in the host's organization.

**Note:** If OneDrive and SharePoint integration with Entra ID B2B is enabled as per the CIS Benchmark the one-time-passcode experience will be replaced. Please visit Secure external sharing in SharePoint - SharePoint in Microsoft 365 | Microsoft Learn for more information.

**Audit:**

**To audit using the UI:**

1. Navigate to SharePoint admin center https://admin.microsoft.com/sharepoint
2. Click to expand Policies > Sharing.
3. Scroll to and expand More external sharing settings.
4. Ensure People who use a verification code must reauthenticate after this many days is set to 15 or less.

**To audit using PowerShell:**

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

```
Get-SPOTenant | fl EmailAttestationRequired,EmailAttestationReAuthDays
```

3. Ensure the following values are returned:
    - EmailAttestationRequired True
    - EmailAttestationReAuthDays 15 or less days.

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

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

```
Set-SPOTenant -EmailAttestationRequired $true -EmailAttestationReAuthDays 15
```

**Default Value:**

EmailAttestationRequired : False

EmailAttestationReAuthDays : 30

**References:**

1. https://learn.microsoft.com/en-us/sharepoint/what-s-new-in-sharing-in-targeted-release
2. https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off#change-the-organization-level-external-sharing-setting
3. https://learn.microsoft.com/en-us/entra/external-id/one-time-passcode

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *7.2.11 (L1) Ensure the SharePoint default sharing link permission is set (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting configures the permission that is selected by default for sharing link from a SharePoint site.

The recommended state is `View`.

**Rationale:**

Setting the view permission as the default ensures that users must deliberately select the edit permission when sharing a link. This approach reduces the risk of unintentionally granting edit privileges to a resource that only requires read access, supporting the principle of least privilege.

**Impact:**

Not applicable.

**Audit:**

**To audit using the UI:**

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to **File and folder links**.
4. Ensure `Choose the permission that's selected by default for sharing links` is set to `View`.

**To audit using PowerShell:**

1. Connect to SharePoint Online service using `Connect-SPOService`.
2. Run the following cmdlet:

```
Get-SPOTenant | fl DefaultLinkPermission
```

3. Ensure the returned value is `View`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to **File and folder links**.
4. Set `Choose the permission that's selected by default for sharing links` to `View`.

**To remediate using PowerShell:**

1. Connect to SharePoint Online service using `Connect-SPOService`.
2. Run the following cmdlet:

```
Set-SPOTenant -DefaultLinkPermission View
```

**Default Value:**

DefaultLinkPermission : Edit

**References:**

1. https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off#file-and-folder-links

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## 7.3 Settings

## *7.3.1 (L2) Ensure Office 365 SharePoint infected files are disallowed for download (Automated)*

**Profile Applicability:**

- E5 Level 2

**Description:**

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

**Rationale:**

Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams protects your organization from inadvertently sharing malicious files. When an infected file is detected that file is blocked so that no one can open, copy, move, or share it until further actions are taken by the organization's security team.

**Impact:**

The only potential impact associated with implementation of this setting is potential inconvenience associated with the small percentage of false positive detections that may occur.

**Audit:**

**To audit using PowerShell:**

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com`, replacing "tenant" with the appropriate value.
2. Run the following PowerShell command:

```
Get-SPOTenant | Select-Object DisallowInfectedFileDownload
```

3. Ensure the value for `DisallowInfectedFileDownload` is set to `True`.

**Note:** According to Microsoft, SharePoint cannot be accessed through PowerShell by users with the Global Reader role. For further information, please refer to the reference section.

**Remediation:**

**To remediate using PowerShell:**

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com`, replacing "tenant" with the appropriate value.
2. Run the following PowerShell command to set the recommended value:

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

**Note:** The Global Reader role cannot access SharePoint using PowerShell according to Microsoft. See the reference section for more information.

**Default Value:**

False

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-for-spo-odfb-teams-configure?view=o365-worldwide
2. https://learn.microsoft.com/en-us/defender-office-365/anti-malware-protection-for-spo-odfb-teams-about?view=o365-worldwide
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#global-reader

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 10.1 Deploy and Maintain Anti-Malware Software<br>Deploy and maintain anti-malware software on all enterprise assets. | ● | ● | ● |
| v7 | 7.10 Sandbox All Email Attachments<br>Use sandboxing to analyze and block inbound email attachments with malicious behavior. | | | ● |
| v7 | 8.1 Utilize Centrally Managed Anti-malware Software<br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. | | ● | ● |

## *7.3.2 (L2) Ensure OneDrive sync is restricted for unmanaged devices (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Microsoft OneDrive allows users to sign in their cloud tenant account and begin syncing select folders or the entire contents of OneDrive to a local computer. By default, this includes any computer with OneDrive already installed, whether it is Entra Joined , Entra Hybrid Joined or Active Directory Domain joined.

The recommended state for this setting is `Allow syncing only on computers joined to specific domains Enabled: Specify the AD domain GUID(s)`

**Rationale:**

Unmanaged devices pose a risk, since their security cannot be verified through existing security policies, brokers or endpoint protection. Allowing users to sync data to these devices takes that data out of the control of the organization. This increases the risk of the data either being intentionally or accidentally leaked.

**Note:** This setting is only applicable to **Active Directory domains** when operating in a hybrid configuration. It does not apply to Entra domains. If there are devices which are only Entra ID joined, consider using a Conditional Access Policy instead.

**Impact:**

Enabling this feature will prevent users from using the OneDrive for Business Sync client on devices that are not joined to the domains that were defined.

**Audit:**

**To audit using the UI:**

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click `Settings` followed by `OneDrive - Sync`
3. Verify that `Allow syncing only on computers joined to specific domains` is checked.
4. Verify that the Active Directory domain GUIDS are listed in the box.
    - Use the `Get-ADDomain` PowerShell command on the on-premises server to obtain the GUID for each on-premises domain.

**To audit using PowerShell:**

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com`, replacing "tenant" with the appropriate value.
2. Run the following PowerShell command:

```
Get-SPOTenantSyncClientRestriction | fl
TenantRestrictionEnabled,AllowedDomainList
```

3. Ensure `TenantRestrictionEnabled` is set to `True` and `AllowedDomainList` contains the trusted domains GUIDs from the on premises environment.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click `Settings` then select `OneDrive - Sync`.
3. Check the `Allow syncing only on computers joined to specific domains`.
4. Use the `Get-ADDomain` PowerShell command on the on-premises server to obtain the GUID for each on-premises domain.
5. Click `Save`.

**To remediate using PowerShell:**

1. Connect to SharePoint Online using `Connect-SPOService`
2. Run the following PowerShell command and provide the DomainGuids from the Get-AADomain command:

```
Set-SPOTenantSyncClientRestriction -Enable -DomainGuids "786548DD-877B-4760-A749-6B1EFBC1190A; 877564FF-877B-4760-A749-6B1EFBC1190A"
```

**Note:** Utilize the `-BlockMacSync:$true` parameter if you are not using conditional access to ensure Macs cannot sync.

**Default Value:**

By default there are no restrictions applied to the syncing of OneDrive.

TenantRestrictionEnabled : `False`

AllowedDomainList : `{}`

**References:**

1. https://learn.microsoft.com/en-us/sharepoint/allow-syncing-only-on-specific-domains
2. https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenantsyncclientrestriction?view=sharepoint-ps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

# 8 Microsoft Teams admin center

The Microsoft Teams admin center contains settings related to Microsoft Teams.

UI Direct link: https://admin.teams.microsoft.com/

Following the October 2025 benchmark release, some subsections within this section assume your tenant has transitioned to the updated settings and policies experience. The guidance provided reflects the new blade design.

This experience is introduced with the message: “Save time and manage your organization’s settings and policies more efficiently with our simplified, all-in-one management center” and is accessible via the `Try the new experience button`. Using the new layout is not a prerequisite of applying the configuration hardening guidance but is recommended.

## *PowerShell specifics*

- The PowerShell module most commonly used in this section is `MicrosoftTeams` and uses `Connect-MicrosoftTeams` as the connection cmdlet.
- The latest version of the module can be downloaded here: https://www.powershellgallery.com/packages/MicrosoftTeams/

In certain scenarios, the Microsoft Teams PowerShell module may throw unexpected errors during connection attempts. A reliable workaround is to launch PowerShell in single-threaded mode using the `-STA` (Single-Threaded Apartment) argument before executing any script blocks. This approach can help avoid issues related to multi-threading conflicts.

For PowerShell 5

```
powershell.exe -sta
```

For PowerShell 7.x

```
pwsh.exe -sta
```

## 8.1 Teams

### *8.1.1 (L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Note:** Skype for business is deprecated as of July 31, 2021 although these settings may still be valid for a period of time. See the link in the references section for more information.

**Rationale:**

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

**Impact:**

The impact associated with this change is highly dependent upon current practices in the tenant. If users do not use other storage providers, then minimal impact is likely. However, if users do regularly utilize providers outside of the tenant this will affect their ability to continue to do so.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Click `Teams` to open the **Teams settings** section.
4. Under **files** verify that only organizationally authorized cloud storage options are set to `On` and all others `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following to verify the recommended state:

```
$Params = @(
   'AllowDropbox'
   'AllowBox'
   'AllowGoogleDrive'
   'AllowShareFile'
   'AllowEgnyte'
)

Get-CsTeamsClientConfiguration -Identity Global | fl $Params
```

3. Verify that only authorized providers are set to `True` and all others `False.`

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Click `Teams` to open the **Teams settings** section.
4. Under **files** set storages providers to `Off` unless they have first been authorized by the organization.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following PowerShell command to disable external providers that are not authorized. (the example disables Citrix Files, DropBox, Box, Google Drive and Egnyte)

```
$Params = @{
    Identity = 'Global'
    AllowGoogleDrive = $false
    AllowShareFile = $false
    AllowBox = $false
    AllowDropBox = $false
    AllowEgnyte = $false
}

Set-CsTeamsClientConfiguration @Params
```

**Default Value:**

AllowDropBox : `True`

AllowBox : `True`

AllowGoogleDrive : `True`

AllowShareFile : `True`

AllowEgnyte : `True`

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/teams-powershell-managing-teams

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v7 | 14.7 Enforce Access Control to Data through Automated Tools<br>Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system. | | | ● |

### *8.1.2 (L1) Ensure users can't send emails to a channel email address (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting controls whether Teams channels are allowed to receive emails sent to their unique email addresses. When enabled, emails sent to a channel's address will be delivered and appear in the channel's conversation thread; when disabled, the channel will reject incoming emails, preventing them from being posted.

The recommended state is `Off`.

**Rationale:**

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

**Impact:**

Depending on the organization's adoption, disabling this may disrupt workflows that rely on email-to-channel communication, particularly in environments where email is used to bridge external systems or vendors into Teams. This could include reduced visibility of important updates or alerts that were previously routed into Teams channels via email.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Click `Teams` to open the **Teams settings** section.
4. Under **email integration** verify that `Users can send emails to a channel email address` is `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsClientConfiguration -Identity Global | fl AllowEmailIntoChannel
```

3. Ensure the returned value is `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Click `Teams` to open the **Teams settings** section.
4. Under **email integration** set `Users can send emails to a channel email address` to `Off`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsClientConfiguration -Identity Global -AllowEmailIntoChannel $false
```

**Default Value:**

On (True)

**References:**

1. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#restricting-channel-email-messages-to-approved-domains
2. https://learn.microsoft.com/en-us/microsoftteams/settings-policies-reference#email-integration
3. https://support.microsoft.com/en-us/office/send-an-email-to-a-channel-in-microsoft-teams-d91db004-d9d7-4a47-82e6-fb1b16dfd51e

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## 8.2 Users

## *8.2.1 (L2) Ensure external domains are restricted in the Teams admin center (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

This policy controls whether external domains are allowed, blocked or permitted based on an allowlist or denylist. When external domains are allowed, users in your organization can chat, add users to meetings, and use audio video conferencing with users in external organizations.

The recommended state is `Allow only specific external domains` or `Block all external domains`.

**Rationale:**

Allowlisting external domains that an organization is collaborating with allows for stringent controls over who an organization's users are allowed to make contact with.

Some real-world attacks and exploits delivered via Teams over external access channels include:

- DarkGate malware
- Social engineering / Phishing attacks by "Midnight Blizzard"
- GIFShell
- Username enumeration

**Impact:**

The impact in terms of the type of collaboration users are allowed to participate in and the I.T. resources expended to manage an allowlist will increase. If a user attempts to join the inviting organization's meeting they will be prevented from joining unless they were created as a guest in EntraID or their domain was added to the allowed external domains list.

**Note** Organizations may choose create additional policies for specific groups needing external access.

**Audit:**

The focus of this control at a minimum is the `Global (Org-wide default)` policy. If the organization-wide setting is configured to `Allow only specific external domains` or `Block all external domains`, then this is also considered a passing state due to its increased restrictiveness.

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Select the `Policies` tab.
4. Click on the `Global (Org-wide default)` policy.
5. Ensure `Teams and Skype for Business users in external organizations` is set to `Off`.

**Organization settings: Additional passing state**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Select the `Organization settings` tab.
4. Ensure `Teams and Skype for Business users in external organizations` is set to one of the following:
    - Allowlist: `Allow only specific external domains`
    - Disabled: `Block all external domains`

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command:

```
Get-CsExternalAccessPolicy -Identity Global
```

3. Ensure `EnableFederationAccess` is `False`.

**Organization settings: Additional passing state**

1. Run the following command:

```
Get-CsTenantFederationConfiguration | fl AllowFederatedUsers,AllowedDomains
```

Ensure the following conditions:

- State: `AllowFederatedUsers` is set to `False` **OR**,
- If: `AllowFederatedUsers` is `True` then ensure `AllowedDomains` contains authorized domain names and is *not* set to `AllowAllKnownDomains`.

**Note:** The organization settings take precedence over the policy settings. The audit is considered satisfied if the organizational setting is configured as prescribed, regardless of whether the Global default policy value is `True` or `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Select the `Policies` tab
4. Click on the `Global (Org-wide default)` policy.
5. Set `Teams and Skype for Business users in external organizations` to `Off`.
6. Click `Save`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command to configure the Global (Org-wide default)` policy.

```
Set-CsExternalAccessPolicy -Identity Global -EnableFederationAccess $false
```

**Note:** Configuring this setting at the organization level in `Organization settings` to either `Block all external domains` or `Allow only specific external domains` is also a compliant configuration for this control.

**Default Value:**

EnableFederationAccess - $True

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings
2. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
3. https://www.bitdefender.com/blog/hotforsecurity/gifshell-attack-lets-hackers-create-reverse-shell-through-microsoft-teams-gifs/

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

### *8.2.2 (L1) Ensure communication with unmanaged Teams users is disabled (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

The recommended state is: `People in my organization can communicate with unmanaged Teams accounts` set to `Off`.

**Rationale:**

Allowing users to communicate with unmanaged Teams users presents a potential security threat as little effort is required by threat actors to gain access to a trial or free Microsoft Teams account.

Some real-world attacks and exploits delivered via Teams over external access channels include:

- DarkGate malware
- Social engineering / Phishing attacks by "Midnight Blizzard"
- GIFShell
- Username enumeration

**Impact:**

Users will be unable to communicate with Teams users who are not managed by an organization.

Organizations may choose create additional policies for specific groups needing to communicating with unmanaged external users.

**Note:** The settings that govern chats and meetings with external unmanaged Teams users aren't available in GCC, GCC High, or DOD deployments, or in private cloud environments.

**Audit:**

The focus of this control at a minimum is the `Global (Org-wide default)` policy. If the equivalent organization-wide setting is configured to `Off`, then this is also considered a passing state due to its increased restrictiveness.

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`
3. Select the `Policies` tab.
4. Click on the `Global (Org-wide default)` policy.
5. Ensure `People in my organization can communicate with unmanaged Teams accounts` is set to `Off`.

**Organization settings: Additional passing state**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`
3. Select the `Organization settings` tab.
4. Ensure `People in my organization can communicate with unmanaged Teams accounts` is set to `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command:

```
Get-CsExternalAccessPolicy -Identity Global
```

Ensure `EnableTeamsConsumerAccess` is set to `False`.

**Organization settings: Additional passing state**

1. Run the following command:

```
Get-CsTenantFederationConfiguration | fl AllowTeamsConsumer
```

Ensure `AllowTeamsConsumer` is `False`

**Note:** The organization settings take precedence over the policy settings. The audit is considered satisfied if the organizational setting is configured as prescribed, regardless of whether the Global default policy value is `True` or `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Select the `Policies` tab
4. Click on the `Global (Org-wide default)` policy.
5. Set `People in my organization can communicate with unmanaged Teams accounts` to `Off`.
6. Click `Save`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command:

```
Set-CsExternalAccessPolicy -Identity Global -EnableTeamsConsumerAccess $false
```

**Note:** Configuring the organization settings to block communication is also in compliance with this control.

**Default Value:**

- EnableTeamsConsumerAccess : `True`

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings
2. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
3. https://www.bitdefender.com/blog/hotforsecurity/gifshell-attack-lets-hackers-create-reverse-shell-through-microsoft-teams-gifs/

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *8.2.3 (L1) Ensure external Teams users cannot initiate conversations (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting prevents external users who are not managed by an organization from initiating contact with users in the protected organization.

The recommended state is to uncheck `External users with Teams accounts not managed by an organization can contact users in my organization`.

**Note:** Disabling this setting is used as an additional stop gap for the previous setting which disables communication with unmanaged Teams users entirely. If an organization chooses to have an exception to **(L1) Ensure communication with unmanaged Teams users is disabled** they can do so while also disabling the ability for the same group of users to initiate contact. Disabling communication entirely will also disable the ability for unmanaged users to initiate contact.

**Rationale:**

Allowing users to communicate with unmanaged Teams users presents a potential security threat as little effort is required by threat actors to gain access to a trial or free Microsoft Teams account.

Some real-world attacks and exploits delivered via Teams over external access channels include:

- DarkGate malware
- Social engineering / Phishing attacks by "Midnight Blizzard"
- GIFShell
- Username enumeration

**Impact:**

The impact of disabling this is very low.

Organizations may choose to create additional policies for specific groups that need to communicate with unmanaged external users.

**Note:** Chats and meetings with external unmanaged Teams users isn't available in GCC, GCC High, or DOD deployments, or in private cloud environments.

**Audit:**

The focus of this control at a minimum is the `Global (Org-wide default)` policy. If the equivalent organization-wide setting is disabled, then this is also considered a passing state due to its increased restrictiveness.

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Select the `Policies` tab.
4. Click on the `Global (Org-wide default)` policy.
5. Ensure `External users with Teams accounts not managed by an organization can contact users in my organization` is not checked (false).

**Organization settings: Additional passing state**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Select the `Organization settings` tab.
4. Locate the parent setting **People in my organization can communicate with unmanaged Teams accounts**.
5. Ensure `External users with Teams accounts not managed by an organization can contact users in my organization` is not checked (false).

**Note:** If the parent setting `People in my organization can communicate with unmanaged Teams accounts` is already set to `Off` then this setting will not be visible in the UI.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command:

```
Get-CsExternalAccessPolicy -Identity Global
```

Ensure `EnableTeamsConsumerInbound` is `False`

**Organization settings: Additional passing state**

1. Run the following command:

```
Get-CsTenantFederationConfiguration | fl AllowTeamsConsumerInbound
```

Ensure `AllowTeamsConsumerInbound` is `False`

**Note:** The organization settings take precedence over the policy settings. The audit is considered satisfied if the organizational setting is configured as prescribed, regardless of whether the Global default policy value is `True` or `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Select the `Policies` tab.
4. Click on the `Global (Org-wide default)` policy.
5. Locate the parent setting **People in my organization can communicate with unmanaged Teams accounts**.
6. Uncheck `External users with Teams accounts not managed by an organization can contact users in my organization`.
7. Click `Save`.

**Note:** If `People in my organization can communicate with unmanaged Teams accounts` is already set to `Off` then this setting will not be visible and will satisfy the requirements of this recommendation.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command:

```
Set-CsExternalAccessPolicy -Identity Global -EnableTeamsConsumerInbound
$false
```

**Note:** Configuring the organization settings to block inbound communication is also in compliance with this control.

**Default Value:**

- EnableTeamsConsumerInbound : `True`

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings
2. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
3. https://www.bitdefender.com/blog/hotforsecurity/gifshell-attack-lets-hackers-create-reverse-shell-through-microsoft-teams-gifs/

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *8.2.4 (L1) Ensure the organization cannot communicate with accounts in trial Teams tenants (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting controls the organization's external access with Teams "trial-only" tenants. These are tenants that don't have any purchased seats.

When set to Blocked, users from these trial-only tenants aren't able to search and contact your users via chats, Teams calls, and meetings (using the users' authenticated identities) and your users aren't able to reach users in these trial-only tenants. Users from the trial-only tenant are also removed from existing chats.

The recommended state for `People in my organization can communicate with accounts in trial Teams tenant` is `Off`.

**Rationale:**

Microsoft introduced this setting as `Off` by default on July 29, 2029 in order to block attack vectors being exploited by threat actors who have abused trial tenants. Enforcing the default ensures the setting is not reenabled for any reason.

Allowing users to communicate with unmanaged Teams users presents a potential security threat as little effort is required by threat actors to gain access to a trial or free Microsoft Teams account.

Some real-world attacks and exploits delivered via Teams over external access channels include:

- DarkGate malware
- Social engineering / Phishing attacks by "Midnight Blizzard"
- GIFShell
- Username enumeration

**Impact:**

There is minimal to no legitimate business need for users to communicate with accounts in trial tenants. For temporary or testing scenarios, alternative communication methods are readily available that do not require enabling this setting.

**Audit:**

**To audit using the UI:**

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com/.
2. Click to expand Users select External access.
3. Select the Organization settings tab.
4. Ensure People in my organization can communicate with accounts in trial Teams tenant is set to Off.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using Connect-MicrosoftTeams
2. Run the following command:

```
Get-CsTenantFederationConfiguration
```

Ensure ExternalAccessWithTrialTenants is set to Blocked.

**Remediation:**

**To remediate using the UI:**

1. Navigate to Microsoft Teams admin center https://admin.teams.microsoft.com/.
2. Click to expand Users select External access.
3. Select the Organization settings tab.
4. Set People in my organization can communicate with accounts in trial Teams tenant to Off.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using Connect-MicrosoftTeams
2. Run the following command:

```
Set-CsTenantFederationConfiguration -ExternalAccessWithTrialTenants "Blocked"
```

**Default Value:**

Off or Blocked

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings#block-federation-with-teams-trial-only-tenants
2. https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
3. https://www.bitdefender.com/en-us/blog/hotforsecurity/gifshell-attack-lets-hackers-create-reverse-shell-through-microsoft-teams-gifs

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## 8.3 Teams devices

This section is intentionally blank and exists to ensure the structure of the benchmark is consistent.

## 8.4 Teams apps

### *8.4.1 (L1) Ensure app permission policies are configured (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This policy setting controls which class of apps are available for users to install.

**Rationale:**

Allowing users to install third-party or unverified apps poses a potential risk of introducing malicious software to the environment.

**Impact:**

Users will only be able to install approved classes of apps.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Teams apps` select `Manage apps`.
3. In the upper right click `Actions` > `Org-wide app settings`.
4. For `Microsoft apps` verify that `Let users install and use available apps by default` is `On` or less permissive.
5. For `Third-party apps` verify `Let users install and use available apps by default` is `Off`.
6. For `Custom apps` verify `Let users install and use available apps by default` is `Off`.
7. For `Custom apps` verify `Let users interact with custom apps in preview` is `Off`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Teams apps` select `Manage apps`.
3. In the upper right click `Actions` > `Org-wide app settings`.
4. For `Microsoft apps` set `Let users install and use available apps by default` to `On` or less permissive.
5. For `Third-party apps` set `Let users install and use available apps by default` to `Off`.
6. For `Custom apps` set `Let users install and use available apps by default` to `Off`.
7. For `Custom apps` set `Let users interact with custom apps in preview` to `Off`.

**Default Value:**

Microsoft apps: On

Third-party apps: On

Custom apps: On

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/app-centric-management
2. https://learn.microsoft.com/en-us/defender-office-365/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#disabling-third-party--custom-apps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 2.5 Allowlist Authorized Software<br>Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. | | ● | ● |
| v7 | 2.7 Utilize Application Whitelisting<br>Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets. | | | ● |

## 8.5 Meetings

## *8.5.1 (L2) Ensure anonymous users can't join a meeting (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

Anonymous users are users whose identity can't be verified. They may be logged in to an organization without a mutual trust relationship or they may not have an account (guest or user). Anonymous participants appear with "(Unverified)" appended to their name in meetings.

These users could include:

- Users who aren't logged in to Teams with a work or school account.
- Users from non-trusted organizations (as configured in external access) and from organizations that you trust but which don't trust your organization. When defining trusted organizations for external meetings and chat, ensure both organizations allow each other's domains. Meeting organizers and participants should have user policies that allow external access. These settings prevent attendees from being considered anonymous due to external access settings. For details, see IT Admins - Manage external meetings and chat with people and organizations using Microsoft identities

The recommended state is `Anonymous users can join a meeting unverified` set to `Off`.

**Rationale:**

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

**Note:** Those companies that don't normally operate at a Level 2 environment, but do deal with sensitive information, may want to consider this policy setting.

**Impact:**

Individuals who were not sent or forwarded a meeting invite will not be able to join the meeting automatically.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting join & lobby** verify that `Anonymous users can join a meeting unverified` is set to `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl
AllowAnonymousUsersToJoinMeeting
```

3. Ensure the returned value is `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting join & lobby** set `Anonymous users can join a meeting unverified` to `Off`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToJoinMeeting
$false
```

**Default Value:**

On (True)

**References:**

1. https://learn.microsoft.com/en-us/defender-office-365/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#configure-meeting-settings
2. https://learn.microsoft.com/en-us/microsoftteams/settings-policies-reference?WT.mc_id=TeamsAdminCenterCSH#meeting-join--lobby
3. https://learn.microsoft.com/en-us/MicrosoftTeams/configure-meetings-sensitive-protection
4. https://learn.microsoft.com/en-us/microsoftteams/anonymous-users-in-meetings
5. https://learn.microsoft.com/en-us/microsoftteams/plan-meetings-external-participants

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *8.5.2 (L1) Ensure anonymous users and dial-in callers can't start a meeting (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This policy setting controls if an anonymous participant can start a Microsoft Teams meeting without someone in attendance. Anonymous users and dial-in callers must wait in the lobby until the meeting is started by someone in the organization or an external user from a trusted organization.

Anonymous participants are classified as:

- Participants who are not logged in to Teams with a work or school account.
- Participants from non-trusted organizations (as configured in external access).
- Participants from organizations where there is not mutual trust.

**Note:** This setting only applies when `Who can bypass the lobby` is set to `Everyone`. If the `anonymous users can join a meeting` organization-level setting or meeting policy is `Off`, this setting only applies to dial-in callers.

**Rationale:**

Not allowing anonymous participants to automatically join a meeting reduces the risk of meeting spamming.

**Impact:**

Anonymous participants will not be able to start a Microsoft Teams meeting.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting join & lobby** verify that `Anonymous users and dial-in callers can start a meeting` is set to `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl
AllowAnonymousUsersToStartMeeting
```

3. Ensure the returned value is `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting join & lobby** set `Anonymous users and dial-in callers can start a meeting` to `Off`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToStartMeeting
$false
```

**Default Value:**

Off (False)

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/anonymous-users-in-meetings
2. https://learn.microsoft.com/en-us/microsoftteams/who-can-bypass-meeting-lobby#overview-of-lobby-settings-and-policies

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *8.5.3 (L1) Ensure only people in my org can bypass the lobby (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

The recommended state is `People who were invited` or more restrictive.

**Rationale:**

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

**Impact:**

Individuals who are not part of the organization will have to wait in the lobby until they're admitted by an organizer, co-organizer, or presenter of the meeting.

Any individual who dials into the meeting regardless of status will also have to wait in the lobby. This includes internal users who are considered unauthenticated when dialing in.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting join & lobby** verify `Who can bypass the lobby` is set to `People who were invited` or a more restrictive value: `People in my org`, `Only organizers and co-organizers`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl AutoAdmittedUsers
```

3. Ensure the returned value is `InvitedUsers` or more restrictive: `EveryoneInCompanyExcludingGuests`, `OrganizerOnly`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under meeting join & lobby set `Who can bypass the lobby` to `People who were invited` or a more restrictive value: `People in my org`, `Only organizers and co-organizers`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AutoAdmittedUsers "InvitedUsers"
```

**Note:** More restrictive values `EveryoneInCompanyExcludingGuests` or `OrganizerOnly` are also in compliance.

**Default Value:**

People in my org and guests (EveryoneInCompany)

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/who-can-bypass-meeting-lobby#overview-of-lobby-settings-and-policies
2. https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

### *8.5.4 (L1) Ensure users dialing in can't bypass the lobby (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This policy setting controls if users who dial in by phone can join the meeting directly or must wait in the lobby. Admittance to the meeting from the lobby is authorized by the meeting organizer, co-organizer, or presenter of the meeting.

**Rationale:**

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly from the organization.

**Impact:**

Individuals who are dialing in to the meeting must wait in the lobby until a meeting organizer, co-organizer, or presenter admits them.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting join & lobby** verify that `People dialing in can bypass the lobby` is set to `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl AllowPSTNUsersToBypassLobby
```

3. Ensure the value is `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting join & lobby** set `People dialing in can bypass the lobby` to `Off`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowPSTNUsersToBypassLobby $false
```

**Default Value:**

Off (False)

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/who-can-bypass-meeting-lobby#overview-of-lobby-settings-and-policies
2. https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *8.5.5 (L2) Ensure meeting chat does not allow anonymous users (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

Only authorized individuals will be able to read and write chat messages during a meeting.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting engagement** verify that `Meeting chat` is set to `On for everyone but anonymous users` or a more restrictive value: `In-meeting only except anonymous` or `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl MeetingChatEnabledType
```

3. Ensure the returned value is `EnabledExceptAnonymous` or a more restrictive value `EnabledInMeetingOnlyForAllExceptAnonymous` or `Disabled`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting engagement** set `Meeting chat` to `On for everyone but anonymous users`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the minimum recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -MeetingChatEnabledType
"EnabledExceptAnonymous"
```

**Note:** The audit section outlines additional compliant states which are more restrictive than the recommended state.

**Default Value:**

On for everyone (Enabled)

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *8.5.6 (L2) Ensure only organizers and co-organizers can present (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Note:** Organizers and co-organizers can change this setting when the meeting is set up.

**Rationale:**

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

**Impact:**

Only organizers and co-organizers will be able to present without being granted permission.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **content sharing** verify `Who can present` is set to `Only organizers and co-organizers`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl DesignatedPresenterRoleMode
```

3. Ensure the returned value is `OrganizerOnlyUserOverride`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **content sharing** set `Who can present` to `Only organizers and co-organizers`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -DesignatedPresenterRoleMode
"OrganizerOnlyUserOverride"
```

**Default Value:**

Everyone (EveryoneUserOverride)

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *8.5.7 (L1) Ensure external participants can't give or request control (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

**Rationale:**

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

External participants are categorized as follows: external users, guests, and anonymous users.

**Impact:**

External participants will not be able to present or request control during the meeting.

**Warning:** This setting also affects webinars.

**Note:** At this time, to give and take control of shared content during a meeting, both parties must be using the Teams desktop client. Control isn't supported when either party is running Teams in a browser.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **content sharing** verify that `External participants can give or request control` is `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl
AllowExternalParticipantGiveRequestControl
```

3. Ensure the returned value is `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **content sharing** set `External participants can give or request control` to `Off`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -
AllowExternalParticipantGiveRequestControl $false
```

**Default Value:**

Off (False)

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *8.5.8 (L2) Ensure external meeting chat is off (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

This meeting policy setting controls whether users can read or write messages in external meeting chats with untrusted organizations. If an external organization is on the list of trusted organizations this setting will be ignored.

**Rationale:**

Restricting access to chat in meetings hosted by external organizations limits the opportunity for an exploit like GIFShell or DarkGate malware from being delivered to users.

**Impact:**

When joining external meetings users will be unable to read or write chat messages in Teams meetings with organizations that they don't have a trust relationship with. This will completely remove the chat functionality in meetings. From an I.T. perspective both the upkeep of adding new organizations to the trusted list and the decision-making process behind whether to trust or not trust an external partner will increase time expenditure.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting engagement** verify that `External meeting chat` is set to `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl
AllowExternalNonTrustedMeetingChat
```

3. Ensure the returned value is `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **meeting engagement** set `External meeting chat` to `Off`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowExternalNonTrustedMeetingChat
$false
```

**Default Value:**

On(True)

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/settings-policies-reference#meeting-engagement

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 16.10 Apply Secure Design Principles in Application Architectures<br>Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts. | | ● | ● |

## *8.5.9 (L2) Ensure meeting recording is off by default (Automated)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

This setting controls the ability for a user to initiate a recording of a meeting in progress.

The recommended state is `Off` for the `Global (Org-wide default)` meeting policy.

**Rationale:**

Disabling meeting recordings in the Global meeting policy ensures that only authorized users, such as organizers, co-organizers, and leads, can initiate a recording. This measure helps safeguard sensitive information by preventing unauthorized individuals from capturing and potentially sharing meeting content. Restricting recording capabilities to specific roles allows organizations to exercise greater control over what is recorded, aligning it with the meeting's confidentiality requirements.

**Note:** Creating a separate policy for users or groups who are allowed to record is expected and in compliance. This control is only for the default meeting policy.

**Impact:**

If there are no additional policies allowing anyone to record, then recording will effectively be disabled.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **Recording & transcription** verify that `Meeting recording` is set to `Off`.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl AllowCloudRecording
```

3. Ensure the returned value is `False`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Meetings` to open the **meeting settings** section.
4. Under **Recording & transcription** set `Meeting recording` to `Off`.

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowCloudRecording $false
```

**Default Value:**

On (True)

**References:**

1. https://learn.microsoft.com/en-us/microsoftteams/settings-policies-reference#recording--transcription

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 16.10 Apply Secure Design Principles in Application Architectures<br>Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts. | | ● | ● |

## 8.6 Messaging

## *8.6.1 (L1) Ensure users can report security concerns in Teams (Automated)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

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

**Rationale:**

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

**Note:**

- The reported message remains visible to the user in the Teams client.
- Users can report the same message multiple times.
- The message sender isn't notified that messages were reported.

**Impact:**

Enabling message reporting has an impact beyond just addressing security concerns. When users of the platform report a message, the content could include messages that are threatening or harassing in nature, possibly stemming from colleagues.

Due to this the security staff responsible for reviewing and acting on these reports should be equipped with the skills to discern and appropriately direct such messages to the relevant departments, such as Human Resources (HR).

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Select `Settings & policies` > `Global (Org-wide default) settings`.
3. Select `Messaging` to open the **messaging settings** section.
4. Ensure `Report a security concern` is `On`.
5. Next, navigate to `Microsoft 365 Defender` https://security.microsoft.com/
6. Click on `Settings` > `Email & collaboration` > `User reported settings`.
7. Scroll to `Microsoft Teams`.
8. Ensure `Monitor reported messages in Microsoft Teams` is checked.
9. Ensure `Send reported messages to:` is set to `My reporting mailbox only` with report email addresses defined for authorized staff.

**To audit using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following cmdlet for to assess Teams:

```
Get-CsTeamsMessagingPolicy -Identity Global | fl
AllowSecurityEndUserReporting
```

3. Ensure the value returned is `True`.
4. Connect to Exchange Online PowerShell using `Connect-ExchangeOnline`.
5. Run this cmdlet to assess Defender:

```
Get-ReportSubmissionPolicy | fl Report*
```

6. Ensure the output matches the following values with organization specific email addresses:

```
ReportJunkToCustomizedAddress                : True
ReportNotJunkToCustomizedAddress             : True
ReportPhishToCustomizedAddress               : True
ReportJunkAddresses                          : {SOC@contoso.com}
ReportNotJunkAddresses                       : {SOC@contoso.com}
ReportPhishAddresses                         : {SOC@contoso.com}
ReportChatMessageEnabled                     : False
ReportChatMessageToCustomizedAddressEnabled : True
```

**Remediation:**

**To remediate using the UI:**

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

**To remediate using PowerShell:**

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Connect to Exchange Online PowerShell using `Connect-ExchangeOnline`.
3. Run the following cmdlet:

```
Set-CsTeamsMessagingPolicy -Identity Global -AllowSecurityEndUserReporting
$true
```

4. To configure the Defender reporting policies, edit and run this script:

```
$usersub = "userreportedmessages@fabrikam.com" # Change this.

$params = @{
    Identity                          = "DefaultReportSubmissionPolicy"
    EnableReportToMicrosoft           = $false
    ReportChatMessageEnabled          = $false
    ReportChatMessageToCustomizedAddressEnabled = $true
    ReportJunkToCustomizedAddress     = $true
    ReportNotJunkToCustomizedAddress  = $true
    ReportPhishToCustomizedAddress    = $true
    ReportJunkAddresses               = $usersub
    ReportNotJunkAddresses            = $usersub
    ReportPhishAddresses              = $usersub
}

Set-ReportSubmissionPolicy @params

New-ReportSubmissionRule -Name DefaultReportSubmissionRule -
ReportSubmissionPolicy DefaultReportSubmissionPolicy -SentTo $usersub
```

**Default Value:**

On (`True`)

Report message destination: `Microsoft Only`

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |
| v7 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

# 9 Microsoft Fabric

Microsoft Fabric is also known as Power BI and contains settings to everything related to Power BI configuration.

Direct link: https://app.powerbi.com/admin-portal/

## 9.1 Tenant settings

### *Required Roles*

To audit the Tenant settings section within the Microsoft Fabric admin center, users must have either the `Power BI Administrator` or `Global Administrator` role. The Global Reader role does not currently provide sufficient permissions to access or audit these settings.

### *9.1.1 (L1) Ensure guest user access is restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting allows business-to-business (B2B) guests access to Microsoft Fabric, and contents that they have permissions to. With the setting turned off, B2B guest users receive an error when trying to access Power BI.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Rationale:**

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

**Impact:**

Security groups will need to be more closely tended to and monitored.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Guest users can access Microsoft Fabric` adheres to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

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

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Enabled for the entire organization

**References:**

1. https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-export-sharing

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

### *9.1.2 (L1) Ensure external user invitations are restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting helps organizations choose whether new external users can be invited to the organization through Power BI sharing, permissions, and subscription experiences. This setting only controls the ability to invite through Power BI.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Note:** To invite external users to the organization, the user must also have the Microsoft Entra Guest Inviter role.

**Rationale:**

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

**Impact:**

Guest user invitations will be limited to only specific employees.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Users can invite guest users to collaborate through item sharing and permissions` adheres to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Users can invite guest users to collaborate through item sharing and permissions` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Enabled for the entire organization

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

### *9.1.3 (L1) Ensure guest access to content is restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

This setting allows Microsoft Entra B2B guest users to have full access to the browsing experience using the left-hand navigation pane in the organization. Guest users who have been assigned workspace roles or specific item permissions will continue to have those roles and/or permissions, even if this setting is disabled.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Rationale:**

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

**Impact:**

Security groups will need to be more closely tended to and monitored.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Guest users can browse and access Fabric content` adheres to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Guest users can browse and access Fabric content` to one of these states:
   - State 1: `Disabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Disabled

**References:**

1. https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-export-sharing

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v7 | 14.6 Protect Information through Access Control Lists<br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

### *9.1.4 (L1) Ensure 'Publish to web' is restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Power BI enables users to share reports and materials directly on the internet from both the application's desktop version and its web user interface. This functionality generates a publicly reachable web link that doesn't necessitate authentication or the need to be an Entra ID user in order to access and view it.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Rationale:**

When using Publish to Web anyone on the Internet can view a published report or visual. Viewing requires no authentication. It includes viewing detail-level data that your reports aggregate. By disabling the feature, restricting access to certain users and allowing existing embed codes organizations can mitigate the exposure of confidential or proprietary information.

**Impact:**

Depending on the organization's utilization administrators may experience more overhead managing embed codes, and requests.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Publish to web` adheres to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Choose how embed codes work` set to `Only allow existing codes` **AND** `Specific security groups` selected and defined

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Publish to web` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Choose how embed codes work` set to `Only allow existing codes` **AND** `Specific security groups` selected and defined

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Enabled for the entire organization

Only allow existing codes

**References:**

1. https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-publish-to-web
2. https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-export-sharing#publish-to-web

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 16.10 Apply Secure Design Principles in Application Architectures<br>Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts. | | ● | ● |

### *9.1.5 (L2) Ensure 'Interact with and share R and Python' visuals is 'Disabled' (Manual)*

**Profile Applicability:**

- E3 Level 2
- E5 Level 2

**Description:**

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

**Rationale:**

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

**Impact:**

Use of R and Python scripting will require exceptions for developers, along with more stringent code review.

**Audit:**

**To audit using the UI:**

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

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

Enabled

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |

### *9.1.6 (L1) Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled' (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Information protection tenant settings help to protect sensitive information in the Power BI tenant. Allowing and applying sensitivity labels to content ensures that information is only seen and accessed by the appropriate users.

The recommended state is `Enabled` or `Enabled for a subset of the organization`.

**Note:** Sensitivity labels and protection are only applied to files exported to Excel, PowerPoint, or PDF files, that are controlled by "Export to Excel" and "Export reports as PowerPoint presentation or PDF documents" settings. All other export and sharing options do not support the application of sensitivity labels and protection.

**Note 2:** There are some prerequisite steps that need to be completed in order to fully utilize labeling. See here.

**Rationale:**

Establishing data classifications and affixing labels to data at creation enables organizations to discern the data's criticality, sensitivity, and value. This initial identification enables the implementation of appropriate protective measures, utilizing technologies like Data Loss Prevention (DLP) to avert inadvertent exposure and enforcing access controls to safeguard against unauthorized access.

This practice can also promote user awareness and responsibility in regard to the nature of the data they interact with. Which in turn can foster awareness in other areas of data management across the organization.

**Impact:**

Additional license requirements like Power BI Pro are required, as outlined in the Licensed and requirements page linked in the description and references sections.

**Audit:**

**To audit using the UI:**

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

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

Disabled

**References:**

1. https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-enable-data-sensitivity-labels
2. https://learn.microsoft.com/en-us/fabric/governance/data-loss-prevention-overview
3. https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-enable-data-sensitivity-labels#licensing-and-requirements

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.2 Establish and Maintain a Data Inventory<br>Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data. | ● | ● | ● |
| v8 | 3.7 Establish and Maintain a Data Classification Scheme<br>Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard. | | ● | ● |

### *9.1.7 (L1) Ensure shareable links are restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Creating a shareable link allows a user to create a link to a report or dashboard, then add that link to an email or another messaging application.

There are 3 options that can be selected when creating a shareable link:

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

This setting solely deals with restrictions to `People in the organization`. External users by default are not included in any of these categories, and therefore cannot use any of these links regardless of the state of this setting.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Rationale:**

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

**Impact:**

If the setting is `Enabled` then only specific people in the organization would be allowed to create general links viewable by the entire organization.

**Audit:**

**To audit using the UI:**

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

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

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

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Enabled for the entire organization

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |

## *9.1.8 (L1) Ensure enabling of external data sharing is restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Rationale:**

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

**Impact:**

Security groups will need to be more closely tended to and monitored.

**Audit:**

**To audit using the UI:**

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

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

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

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Enabled for the entire organization

**References:**

1. https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-export-sharing

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 3.3 Configure Data Access Control Lists<br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. | ● | ● | ● |
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

### *9.1.9 (L1) Ensure 'Block ResourceKey Authentication' is 'Enabled' (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

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

The recommended state is `Enabled`.

**Rationale:**

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

**Impact:**

Developers will need to request a special exception in order to use this feature.

**Audit:**

**To audit using the UI:**

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

**Remediation:**

**To remediate using the UI:**

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

**Default Value:**

Disabled for the entire organization

**References:**

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

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |

### *9.1.10 (L1) Ensure access to APIs by service principals is restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Use a service principal to access Fabric public APIs that include create, read, update, and delete (CRUD) operations, and are protected by a Fabric permission model.

To allow an app to use service principal authentication, its service principal must be included in an allowed security group. You can control who can access service principals by creating dedicated security groups and using these groups in other tenant settings.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Rationale:**

Leaving API access unrestricted increases the attack surface in the event an adversary gains access to a Service Principal. APIs are a feature-rich method for programmatic access to many areas of Power Bi and should be guarded closely.

**Impact:**

Service principals will need to be members of specific security groups in order to perform public API calls.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Developer settings`.
4. Ensure that `Service principals can call Fabric public APIs` adheres to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Developer settings`.
4. Set `Service principals can call Fabric public APIs` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Enabled for the entire organization

**References:**

1. https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-developer

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |

### *9.1.11 (L1) Ensure service principals cannot create and use profiles (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Service principal profiles provide a flexible solution for apps used in a multitenancy deployment. The profiles enable customer data isolation and tighter security boundaries between customers that are utilizing the app.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Rationale:**

Service Principals should be restricted to a security group to limit which Service Principals can interact with profiles. This supports the principle of least privilege.

**Impact:**

Disabled is the default behavior.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Developer settings`.
4. Ensure that `Allow service principals to create and use profiles` adheres to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Developer settings`.
4. Set `Allow service principals to create and use profiles` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Disabled for the entire organization

**References:**

1. https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-developer
2. https://learn.microsoft.com/en-us/power-bi/developer/embedded/embed-multi-tenancy

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |

### *9.1.12 (L1) Ensure service principals ability to create workspaces, connections and deployment pipelines is restricted (Manual)*

**Profile Applicability:**

- E3 Level 1
- E5 Level 1

**Description:**

Use a service principal to access these Fabric APIs that aren't protected by a Fabric permission model.

- Create Workspace
- Create Connection
- Create Deployment Pipeline

To allow an app to use service principal authentication, its service principal must be included in an allowed security group. You can control who can access service principals by creating dedicated security groups and using these groups in other tenant settings.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

**Rationale:**

Leaving API access unrestricted increases the attack surface in the event an adversary gains access to a Service Principal. APIs are a feature-rich method for programmatic access to many areas of Power Bi and should be guarded closely.

**Impact:**

Service principals will need to be members of specific security groups in order to perform public API calls.

**Audit:**

**To audit using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Developer settings`.
4. Ensure that `Service principals can create workspaces, connections, and deployment pipelines` adheres to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Remediation:**

**To remediate using the UI:**

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Developer settings`.
4. Set `Service principals can create workspaces, connections, and deployment pipelines` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

**Important:** If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

**Default Value:**

Disabled for the entire organization

**References:**

1. https://learn.microsoft.com/en-us/fabric/admin/service-admin-portal-developer

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. | | ● | ● |

# Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| **1** | **Microsoft 365 admin center** | | |
| **1.1** | **Users** | | |
| 1.1.1 | (L1) Ensure Administrative accounts are cloud-only (Automated) | ☐ | ☐ |
| 1.1.2 | (L1) Ensure two emergency access accounts have been defined (Manual) | ☐ | ☐ |
| 1.1.3 | (L1) Ensure that between two and four global admins are designated (Automated) | ☐ | ☐ |
| 1.1.4 | (L1) Ensure administrative accounts use licenses with a reduced application footprint (Automated) | ☐ | ☐ |
| **1.2** | **Teams & groups** | | |
| 1.2.1 | (L2) Ensure that only organizationally managed/approved public groups exist (Automated) | ☐ | ☐ |
| 1.2.2 | (L1) Ensure sign-in to shared mailboxes is blocked (Automated) | ☐ | ☐ |
| **1.3** | **Settings** | | |
| 1.3.1 | (L1) Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)' (Automated) | ☐ | ☐ |
| 1.3.2 | (L2) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices (Automated) | ☐ | ☐ |
| 1.3.3 | (L2) Ensure 'External sharing' of calendars is not available (Automated) | ☐ | ☐ |
| 1.3.4 | (L1) Ensure 'User owned apps and services' is restricted (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.3.5 | (L1) Ensure internal phishing protection for Forms is enabled (Automated) | ☐ | ☐ |
| 1.3.6 | (L2) Ensure the customer lockbox feature is enabled (Automated) | ☐ | ☐ |
| 1.3.7 | (L2) Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web' (Automated) | ☐ | ☐ |
| 1.3.8 | (L2) Ensure that Sways cannot be shared with people outside of your organization (Manual) | ☐ | ☐ |
| 1.3.9 | (L1) Ensure shared bookings paged are restricted to select users (Automated) | ☐ | ☐ |
| **2** | **Microsoft 365 Defender** | | |
| **2.1** | **Email & collaboration** | | |
| 2.1.1 | (L2) Ensure Safe Links for Office Applications is Enabled (Automated) | ☐ | ☐ |
| 2.1.2 | (L1) Ensure the Common Attachment Types Filter is enabled (Automated) | ☐ | ☐ |
| 2.1.3 | (L1) Ensure notifications for internal users sending malware is Enabled (Automated) | ☐ | ☐ |
| 2.1.4 | (L2) Ensure Safe Attachments policy is enabled (Automated) | ☐ | ☐ |
| 2.1.5 | (L2) Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled (Automated) | ☐ | ☐ |
| 2.1.6 | (L1) Ensure Exchange Online Spam Policies are set to notify administrators (Automated) | ☐ | ☐ |
| 2.1.7 | (L2) Ensure that an anti-phishing policy has been created (Automated) | ☐ | ☐ |
| 2.1.8 | (L1) Ensure that SPF records are published for all Exchange Domains (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 2.1.9 | (L1) Ensure that DKIM is enabled for all Exchange Online Domains (Automated) | ☐ | ☐ |
| 2.1.10 | (L1) Ensure DMARC Records for all Exchange Online domains are published (Automated) | ☐ | ☐ |
| 2.1.11 | (L2) Ensure comprehensive attachment filtering is applied (Automated) | ☐ | ☐ |
| 2.1.12 | (L1) Ensure the connection filter IP allow list is not used (Automated) | ☐ | ☐ |
| 2.1.13 | (L1) Ensure the connection filter safe list is off (Automated) | ☐ | ☐ |
| 2.1.14 | (L1) Ensure inbound anti-spam policies do not contain allowed domains (Automated) | ☐ | ☐ |
| 2.1.15 | (L1) Ensure outbound anti-spam message limits are in place (Automated) | ☐ | ☐ |
| **2.2** | **Cloud apps** | | |
| 2.2.1 | (L1) Ensure emergency access account activity is monitored (Manual) | ☐ | ☐ |
| **2.3** | **Audit** | | |
| **2.4** | **System** | | |
| 2.4.1 | (L1) Ensure Priority account protection is enabled and configured (Automated) | ☐ | ☐ |
| 2.4.2 | (L1) Ensure Priority accounts have 'Strict protection' presets applied (Automated) | ☐ | ☐ |
| 2.4.3 | (L2) Ensure Microsoft Defender for Cloud Apps is enabled and configured (Manual) | ☐ | ☐ |
| 2.4.4 | (L1) Ensure Zero-hour auto purge for Microsoft Teams is on (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| **3** | **Microsoft Purview** | | |
| **3.1** | **Audit** | | |
| 3.1.1 | (L1) Ensure Microsoft 365 audit log search is Enabled (Automated) | ☐ | ☐ |
| **3.2** | **Data loss protection** | | |
| 3.2.1 | (L1) Ensure DLP policies are enabled (Automated) | ☐ | ☐ |
| 3.2.2 | (L1) Ensure DLP policies are enabled for Microsoft Teams (Automated) | ☐ | ☐ |
| **3.3** | **Information Protection** | | |
| 3.3.1 | (L1) Ensure Information Protection sensitivity label policies are published (Automated) | ☐ | ☐ |
| **4** | **Microsoft Intune admin center** | | |
| 4.1 | (L2) Ensure devices without a compliance policy are marked 'not compliant' (Automated) | ☐ | ☐ |
| 4.2 | (L2) Ensure device enrollment for personally owned devices is blocked by default (Automated) | ☐ | ☐ |
| **5** | **Microsoft Entra admin center** | | |
| **5.1** | **Entra ID** | | |
| **5.1.1** | **Overview** | | |
| **5.1.2** | **Users** | | |
| 5.1.2.1 | (L1) Ensure 'Per-user MFA' is disabled (Automated) | ☐ | ☐ |
| 5.1.2.2 | (L2) Ensure third party integrated applications are not allowed (Automated) | ☐ | ☐ |
| 5.1.2.3 | (L1) Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 5.1.2.4 | (L1) Ensure access to the Entra admin center is restricted (Manual) | ☐ | ☐ |
| 5.1.2.5 | (L2) Ensure the option to remain signed in is hidden (Manual) | ☐ | ☐ |
| 5.1.2.6 | (L2) Ensure 'LinkedIn account connections' is disabled (Manual) | ☐ | ☐ |
| **5.1.3** | **Groups** | | |
| 5.1.3.1 | (L1) Ensure a dynamic group for guest users is created (Automated) | ☐ | ☐ |
| 5.1.3.2 | (L1) Ensure users cannot create security groups (Automated) | ☐ | ☐ |
| **5.1.4** | **Devices** | | |
| 5.1.4.1 | (L2) Ensure the ability to join devices to Entra is restricted (Automated) | ☐ | ☐ |
| 5.1.4.2 | (L1) Ensure the maximum number of devices per user is limited (Automated) | ☐ | ☐ |
| 5.1.4.3 | (L1) Ensure the GA role is not added as a local administrator during Entra join (Automated) | ☐ | ☐ |
| 5.1.4.4 | (L1) Ensure local administrator assignment is limited during Entra join (Automated) | ☐ | ☐ |
| 5.1.4.5 | (L1) Ensure Local Administrator Password Solution is enabled (Automated) | ☐ | ☐ |
| 5.1.4.6 | (L2) Ensure users are restricted from recovering BitLocker keys (Automated) | ☐ | ☐ |
| **5.1.5** | **Applications** | | |
| 5.1.5.1 | (L2) Ensure user consent to apps accessing company data on their behalf is not allowed (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 5.1.5.2 | (L1) Ensure the admin consent workflow is enabled (Automated) | ☐ | ☐ |
| **5.1.6** | **External Identities** | | |
| 5.1.6.1 | (L2) Ensure that collaboration invitations are sent to allowed domains only (Automated) | ☐ | ☐ |
| 5.1.6.2 | (L1) Ensure that guest user access is restricted (Automated) | ☐ | ☐ |
| 5.1.6.3 | (L2) Ensure guest user invitations are limited to the Guest Inviter role (Automated) | ☐ | ☐ |
| **5.1.7** | **User experiences** | | |
| **5.1.8** | **Hybrid management** | | |
| 5.1.8.1 | (L1) Ensure that password hash sync is enabled for hybrid deployments (Manual) | ☐ | ☐ |
| **5.2** | **ID Protection** | | |
| **5.2.1** | **Identity Protection** | | |
| **5.2.2** | **Risk-based Conditional Access** | | |
| 5.2.2.1 | (L1) Ensure multifactor authentication is enabled for all users in administrative roles (Automated) | ☐ | ☐ |
| 5.2.2.2 | (L1) Ensure multifactor authentication is enabled for all users (Automated) | ☐ | ☐ |
| 5.2.2.3 | (L1) Enable Conditional Access policies to block legacy authentication (Automated) | ☐ | ☐ |
| 5.2.2.4 | (L1) Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users (Automated) | ☐ | ☐ |
| 5.2.2.5 | (L2) Ensure 'Phishing-resistant MFA strength' is required for Administrators (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 5.2.2.6 | (L1) Enable Identity Protection user risk policies (Automated) | ☐ | ☐ |
| 5.2.2.7 | (L1) Enable Identity Protection sign-in risk policies (Automated) | ☐ | ☐ |
| 5.2.2.8 | (L2) Ensure 'sign-in risk' is blocked for medium and high risk (Automated) | ☐ | ☐ |
| 5.2.2.9 | (L1) Ensure a managed device is required for authentication (Automated) | ☐ | ☐ |
| 5.2.2.10 | (L1) Ensure a managed device is required to register security information (Automated) | ☐ | ☐ |
| 5.2.2.11 | (L1) Ensure sign-in frequency for Intune Enrollment is set to 'Every time' (Automated) | ☐ | ☐ |
| 5.2.2.12 | (L1) Ensure the device code sign-in flow is blocked (Automated) | ☐ | ☐ |
| **5.2.3** | **Authentication Methods** | | |
| 5.2.3.1 | (L1) Ensure Microsoft Authenticator is configured to protect against MFA fatigue (Automated) | ☐ | ☐ |
| 5.2.3.2 | (L1) Ensure custom banned passwords lists are used (Automated) | ☐ | ☐ |
| 5.2.3.3 | (L1) Ensure password protection is enabled for on-prem Active Directory (Automated) | ☐ | ☐ |
| 5.2.3.4 | (L1) Ensure all member users are 'MFA capable' (Automated) | ☐ | ☐ |
| 5.2.3.5 | (L1) Ensure weak authentication methods are disabled (Automated) | ☐ | ☐ |
| 5.2.3.6 | (L1) Ensure system-preferred multifactor authentication is enabled (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 5.2.3.7 | (L2) Ensure the email OTP authentication method is disabled (Automated) | ☐ | ☐ |
| **5.2.4** | **Password reset** | | |
| 5.2.4.1 | (L1) Ensure 'Self service password reset enabled' is set to 'All' (Manual) | ☐ | ☐ |
| **5.3** | **ID Governance** | | |
| 5.3.1 | (L2) Ensure 'Privileged Identity Management' is used to manage roles (Automated) | ☐ | ☐ |
| 5.3.2 | (L1) Ensure 'Access reviews' for Guest Users are configured (Automated) | ☐ | ☐ |
| 5.3.3 | (L1) Ensure 'Access reviews' for privileged roles are configured (Automated) | ☐ | ☐ |
| 5.3.4 | (L1) Ensure approval is required for Global Administrator role activation (Automated) | ☐ | ☐ |
| 5.3.5 | (L1) Ensure approval is required for Privileged Role Administrator activation (Automated) | ☐ | ☐ |
| **6** | **Exchange admin center** | | |
| **6.1** | **Audit** | | |
| 6.1.1 | (L1) Ensure 'AuditDisabled' organizationally is set to 'False' (Automated) | ☐ | ☐ |
| 6.1.2 | (L1) Ensure mailbox audit actions are configured (Automated) | ☐ | ☐ |
| 6.1.3 | (L1) Ensure 'AuditBypassEnabled' is not enabled on mailboxes (Automated) | ☐ | ☐ |
| **6.2** | **Mail flow** | | |
| 6.2.1 | (L1) Ensure all forms of mail forwarding are blocked and/or disabled (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 6.2.2 | (L1) Ensure mail transport rules do not whitelist specific domains (Automated) | ☐ | ☐ |
| 6.2.3 | (L1) Ensure email from external senders is identified (Automated) | ☐ | ☐ |
| **6.3** | **Roles** | | |
| 6.3.1 | (L2) Ensure users installing Outlook add-ins is not allowed (Automated) | ☐ | ☐ |
| **6.4** | **Reports** | | |
| **6.5** | **Settings** | | |
| 6.5.1 | (L1) Ensure modern authentication for Exchange Online is enabled (Automated) | ☐ | ☐ |
| 6.5.2 | (L1) Ensure MailTips are enabled for end users (Automated) | ☐ | ☐ |
| 6.5.3 | (L2) Ensure additional storage providers are restricted in Outlook on the web (Automated) | ☐ | ☐ |
| 6.5.4 | (L1) Ensure SMTP AUTH is disabled (Automated) | ☐ | ☐ |
| 6.5.5 | (L2) Ensure Direct Send submissions are rejected (Automated) | ☐ | ☐ |
| **7** | **SharePoint admin center** | | |
| **7.1** | **Sites** | | |
| **7.2** | **Policies** | | |
| 7.2.1 | (L1) Ensure modern authentication for SharePoint applications is required (Automated) | ☐ | ☐ |
| 7.2.2 | (L1) Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 7.2.3 | (L1) Ensure external content sharing is restricted (Automated) | ☐ | ☐ |
| 7.2.4 | (L2) Ensure OneDrive content sharing is restricted (Automated) | ☐ | ☐ |
| 7.2.5 | (L2) Ensure that SharePoint guest users cannot share items they don't own (Automated) | ☐ | ☐ |
| 7.2.6 | (L2) Ensure SharePoint external sharing is restricted (Automated) | ☐ | ☐ |
| 7.2.7 | (L1) Ensure link sharing is restricted in SharePoint and OneDrive (Automated) | ☐ | ☐ |
| 7.2.8 | (L2) Ensure external sharing is restricted by security group (Manual) | ☐ | ☐ |
| 7.2.9 | (L1) Ensure guest access to a site or OneDrive will expire automatically (Automated) | ☐ | ☐ |
| 7.2.10 | (L1) Ensure reauthentication with verification code is restricted (Automated) | ☐ | ☐ |
| 7.2.11 | (L1) Ensure the SharePoint default sharing link permission is set (Automated) | ☐ | ☐ |
| **7.3** | **Settings** | | |
| 7.3.1 | (L2) Ensure Office 365 SharePoint infected files are disallowed for download (Automated) | ☐ | ☐ |
| 7.3.2 | (L2) Ensure OneDrive sync is restricted for unmanaged devices (Automated) | ☐ | ☐ |
| **8** | **Microsoft Teams admin center** | | |
| **8.1** | **Teams** | | |
| 8.1.1 | (L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 8.1.2 | (L1) Ensure users can't send emails to a channel email address (Automated) | ☐ | ☐ |
| **8.2** | **Users** | | |
| 8.2.1 | (L2) Ensure external domains are restricted in the Teams admin center (Automated) | ☐ | ☐ |
| 8.2.2 | (L1) Ensure communication with unmanaged Teams users is disabled (Automated) | ☐ | ☐ |
| 8.2.3 | (L1) Ensure external Teams users cannot initiate conversations (Automated) | ☐ | ☐ |
| 8.2.4 | (L1) Ensure the organization cannot communicate with accounts in trial Teams tenants (Automated) | ☐ | ☐ |
| **8.3** | **Teams devices** | | |
| **8.4** | **Teams apps** | | |
| 8.4.1 | (L1) Ensure app permission policies are configured (Manual) | ☐ | ☐ |
| **8.5** | **Meetings** | | |
| 8.5.1 | (L2) Ensure anonymous users can't join a meeting (Automated) | ☐ | ☐ |
| 8.5.2 | (L1) Ensure anonymous users and dial-in callers can't start a meeting (Automated) | ☐ | ☐ |
| 8.5.3 | (L1) Ensure only people in my org can bypass the lobby (Automated) | ☐ | ☐ |
| 8.5.4 | (L1) Ensure users dialing in can't bypass the lobby (Automated) | ☐ | ☐ |
| 8.5.5 | (L2) Ensure meeting chat does not allow anonymous users (Automated) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 8.5.6 | (L2) Ensure only organizers and co-organizers can present (Automated) | ☐ | ☐ |
| 8.5.7 | (L1) Ensure external participants can't give or request control (Automated) | ☐ | ☐ |
| 8.5.8 | (L2) Ensure external meeting chat is off (Automated) | ☐ | ☐ |
| 8.5.9 | (L2) Ensure meeting recording is off by default (Automated) | ☐ | ☐ |
| **8.6** | **Messaging** | | |
| 8.6.1 | (L1) Ensure users can report security concerns in Teams (Automated) | ☐ | ☐ |
| **9** | **Microsoft Fabric** | | |
| **9.1** | **Tenant settings** | | |
| 9.1.1 | (L1) Ensure guest user access is restricted (Manual) | ☐ | ☐ |
| 9.1.2 | (L1) Ensure external user invitations are restricted (Manual) | ☐ | ☐ |
| 9.1.3 | (L1) Ensure guest access to content is restricted (Manual) | ☐ | ☐ |
| 9.1.4 | (L1) Ensure 'Publish to web' is restricted (Manual) | ☐ | ☐ |
| 9.1.5 | (L2) Ensure 'Interact with and share R and Python' visuals is 'Disabled' (Manual) | ☐ | ☐ |
| 9.1.6 | (L1) Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled' (Manual) | ☐ | ☐ |
| 9.1.7 | (L1) Ensure shareable links are restricted (Manual) | ☐ | ☐ |
| 9.1.8 | (L1) Ensure enabling of external data sharing is restricted (Manual) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 9.1.9 | (L1) Ensure 'Block ResourceKey Authentication' is 'Enabled' (Manual) | ☐ | ☐ |
| 9.1.10 | (L1) Ensure access to APIs by service principals is restricted (Manual) | ☐ | ☐ |
| 9.1.11 | (L1) Ensure service principals cannot create and use profiles (Manual) | ☐ | ☐ |
| 9.1.12 | (L1) Ensure service principals ability to create workspaces, connections and deployment pipelines is restricted (Manual) | ☐ | ☐ |

# Appendix: Change History

| Date: 10/31/2025 Version: 6.0.0 |
| --- |
| ADD - 1.3.9 (L1) Ensure shared bookings paged are restricted to select users<br>Ticket #25964 |
| ADD - 2.1.15 (L1) Ensure outbound anti-spam message limits are in place<br>Ticket #25610 |
| ADD - 5.1.3.2 (L1) Ensure users cannot create security groups<br>Ticket #26252 |
| ADD - 5.1.4.1 (L2) Ensure the ability to join devices to Entra is restricted<br>Ticket #26280 |
| ADD - 5.1.4.2 (L2) Ensure the maximum number of devices per user is limited<br>Ticket #26281 |
| ADD - 5.1.4.3 (L1) Ensure the GA role is not added as a local administrator during Entra join<br>Ticket #26282 |
| ADD - 5.1.4.4 (L1) Ensure local administrator assignment is limited during Entra join<br>Ticket #26284 |
| ADD - 5.1.4.5 (L1) Ensure Local Administrator Password Solution is enabled<br>Ticket #26285 |
| ADD - 5.1.4.6 (L2) Ensure users are restricted from recovering BitLocker keys<br>Ticket #26300 |
| ADD - 5.2.3.7 (L2) Ensure the email OTP authentication method is disabled<br>Ticket #26307 |
| ADD - 6.5.5 (L2) Ensure Direct Send submissions are rejected<br>Ticket #25791 |

| |
|---|
| ADD - 8.2.X (L1) Ensure the organization cannot communicate with accounts in trial Teams tenants<br><br>Ticket #25902 |
| ADD - 9.1.12 (L1) Ensure service principals ability to create workspaces, connections and deployment pipelines is restricted<br><br>Ticket #26315 |
| REMOVE - 7.3.3 (L1) Ensure custom script execution is restricted on personal sites - Setting now unavailable in SharePoint<br><br>Ticket #25452 |
| REMOVE - 7.3.4 (L1) Ensure custom script execution is restricted on site collections - Property is automatically disabled by MS after 24 hours<br><br>Ticket #25741 |
| REMOVE - 8.2.4 (L1) Ensure communication with Skype users is disabled<br><br>Ticket #24834 |
| UPDATE - 5.1.8.1 (L1) Ensure that password hash sync is enabled for hybrid deployments - Clarify audit procedure and required roles<br><br>Ticket #26319 |
| UPDATE - 1.2.1 (L2) Ensure that only organizationally managed/approved public groups exist - Minor updates to description and rationale<br><br>Ticket #26047 |
| UPDATE - 1.3.2 (L2) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices - Corrected audit procedure script results in CA step<br><br>Ticket #25255 |
| UPDATE - 1.3.6 (L2) Ensure the customer lockbox feature is enabled - Added the correct reference<br><br>Ticket #24733 |
| UPDATE - 2.1.1 (L2) Ensure Safe Links for Office Applications is Enabled - Improved powershell audit method<br><br>Ticket #26316 |

| |
|---|
| UPDATE - 2.1.11 (L2) Ensure comprehensive attachment filtering is applied - Simplify audit script, provide new output methods, clarify audit steps<br><br>Ticket #25623 |
| UPDATE - 2.1.3 (L1) Ensure notifications for internal users sending malware is Enabled - Include values in PSH audit procedure<br><br>Ticket #25622 |
| UPDATE - 3.1.1(L1) Ensure Microsoft 365 audit log search is Enabled Draft - Add note about PowerShell module issue<br><br>Ticket #25569 |
| UPDATE - 3.3.1 (L1) Ensure Information Protection sensitivity label policies are published - Add method to audit with PowerShell<br><br>Ticket #23463 |
| UPDATE - 4.2 (L2) Ensure device enrollment for personally owned devices is blocked by default - Modify audit script<br><br>Ticket #26320 |
| UPDATE - 5 Microsoft Entra admin center - Minor navigation changes to Entra blades through section 5<br><br>Ticket #25426 |
| UPDATE - 5.1.3.1(L1) Ensure a dynamic group for guest users is created - Add '-All' switch to Get-MgGroup cmdlet<br><br>Ticket #25575 |
| UPDATE - 5.1.6.1 (L2) Ensure that collaboration invitations are sent to allowed domains only - Add PowerShell audit procedure<br><br>Ticket #23464 |
| UPDATE - 5.2.3.3 (L1) Ensure password protection is enabled for on-prem Active Directory - Add PowerShell audit method<br><br>Ticket #25298 |
| UPDATE - 5.2.3.5 (L1) Ensure weak authentication methods are disabled - Move email OTP to its own L2 control<br><br>Ticket #24211 |

| |
|---|
| UPDATE - 5.2.3.6 (L1) Ensure system-preferred multifactor authentication is enabled - Add PowerShell audit method<br><br>Ticket #24839 |
| UPDATE - 5.2.4.1 (L1) Ensure 'Self service password reset enabled' is set to 'All' - Now has a more relevant security rationale<br><br>Ticket #26251 |
| UPDATE - 5.3.1 (L2) Ensure 'Privileged Identity Management' is used to manage roles - Add impact note about alert configuration<br><br>Ticket #25577 |
| UPDATE - 5.3.2 (L1) Ensure 'Access reviews' for Guest Users are configured - Changed audit script, tests for compliance now<br><br>Ticket #26270 |
| UPDATE - 5.3.3 (L1) Ensure 'Access reviews' for privileged roles are configured - Change maximum review duration to 14 days<br><br>Ticket #25253 |
| UPDATE - 6.1.2 (L1) Ensure mailbox audit actions are configured - Updated audit script to output to preferred formats<br><br>Ticket #25264 |
| UPDATE - 6.1.3 (L1) Ensure 'AuditBypassEnabled' is not enabled on mailboxes - Added output options in powershell audit procedure<br><br>Ticket #25624 |
| UPDATE - 6.2.2 (L1) Ensure mail transport rules do not whitelist specific domains - Define what the passing values are in the powershell audit procedure<br><br>Ticket #25621 |
| UPDATE - 6.5.4 (L1) Ensure SMTP AUTH is disabled - Remediation step 3 now correctly states to 'Check' instead of 'Uncheck' the setting, matching the Audit<br><br>Ticket #25296 |
| UPDATE - 7.2.6 (L2) Ensure SharePoint external sharing is restricted - New title, clarify title, description and audit procedure<br><br>Ticket #23794 |

| |
|---|
| UPDATE - 8 Microsoft Teams admin center - Added information about PowerShell and Single Threaded Apartment.<br><br>Ticket #25304 |
| UPDATE - 8.1.1 (L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services - Now uses new settings blade<br><br>Ticket #26216 |
| UPDATE - 8.1.1 (L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services - Remediation now correctly targets the Global policy<br><br>Ticket #26448 |
| UPDATE - 8.1.2 (L1) Ensure users can't send emails to a channel email address - Clarify Description and Impact<br><br>Ticket #26298 |
| UPDATE - 8.1.2 (L1) Ensure users can't send emails to a channel email address - Now uses new settings blade<br><br>Ticket #26217 |
| UPDATE - 8.4.1(L1) Ensure app permission policies are configured - Removed note about Teams Administrator role requirement<br><br>Ticket #25718 |
| UPDATE - 8.5 Meetings - Updated section to use new settings & policies blade<br><br>Ticket #26218 |
| UPDATE - 8.5.5 (L2) Ensure meeting chat does not allow anonymous users - Add more restrictive values for compliance<br><br>Ticket #24833 |
| UPDATE - 8.6 Messaging - Updated section to use new settings & policies blade<br><br>Ticket #26219 |
| UPDATE - 9.1.10 (L1) Ensure access to APIs by Service Principals is restricted - Updated to reflect new setting name<br><br>Ticket #25242 |

UPDATE - 6.5.3 (L2) Ensure additional storage providers are restricted in Outlook on the web - Audit procedure now targets default policy

Ticket #26441

| Date: 04/30/2025 Version: 5.0.0 |
| --- |
| ADD - 2.2.1 (L1) Ensure emergency access account activity is monitored<br><br>Ticket #17934 |
| ADD - 4.1 (L2) Ensure devices without a compliance policy are marked 'not compliant'<br><br>Ticket #23878 |
| ADD - 4.2 (L2) Ensure device enrollment for personally owned devices is blocked by default<br><br>Ticket #23879 |
| ADD - 5.2.2.11 (L1) Ensure sign-in frequency for Intune Enrollment is set to 'Every time'<br><br>Ticket #23851 |
| ADD - 5.2.2.12 (L1) Ensure the device code sign-in flow is blocked<br><br>Ticket #24470 |
| ADD - 5.2.3.6 (L1) Ensure system-preferred multifactor authentication is enabled<br><br>Ticket #18250 |
| ADD - 5.3.4 (L1) Ensure approval is required for Privileged Role Administrator activation<br><br>Ticket #24535 |
| REMOVE - 5.1.1.1 (L1) Ensure Security Defaults is disabled<br><br>Ticket #22190 |
| REMOVE - 5.2.2.8 (L2) Ensure admin center access is limited to administrative roles<br><br>Ticket #24626 |
| REMOVE - 6.1.2 (L1) Ensure mailbox auditing for E3 users is Enabled<br><br>Ticket #24120 |
| UPDATE - Changes in audit procedures around exclusions made in all CA recommendations<br><br>Ticket #23884 |
| UPDATE - 1.1.1 (L1) Ensure Administrative accounts are cloud-only - AUDIT, Fixed variable missing character in script<br><br>Ticket #22992 |

| |
|---|
| UPDATE - 1.1.3 (L1) Ensure that between two and four global admins are designated - Audit procedure requires group inspection now<br><br>Ticket #24117 |
| UPDATE - 1.1.4 (L1) Ensure administrative accounts use licenses with a reduced application footprint - PIM will satisfy requirements<br><br>Ticket #24529 |
| UPDATE - 1.2.1 (L2) Ensure that only organizationally managed/approved public groups exist - Add 'all' switch to audit procedure<br><br>Ticket #23848 |
| UPDATE - 1.2.2 (L1) Ensure sign-in to shared mailboxes is blocked - Graph permission for Audit changed to 'User.Read.All'<br><br>Ticket #22966 |
| UPDATE - 1.3.2 (L1) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices - Added audit powershell method<br><br>Ticket #23461 |
| UPDATE - 1.3.2 (L2) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices - Changed to L2 profile<br><br>Ticket #23659 |
| UPDATE - 1.3.4 (L1) Ensure 'User owned apps and services' is restricted - Added PowerShell automation steps<br><br>Ticket #23448 |
| UPDATE - 1.3.5 (L1) Ensure internal phishing protection for Forms is enabled - Added PowerShell automation methods<br><br>Ticket #23452 |
| UPDATE - 1.3.7 (L2) Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web' - Added audit and remediation methods for PowerShell<br><br>Ticket #23457 |
| UPDATE - 2.1.11 (L2) Ensure comprehensive attachment filtering is applied - Clarify exceptions in audit procedure note<br><br>Ticket #22912 |

| |
|---|
| UPDATE - 2.1.11 (L2) Ensure comprehensive attachment filtering is applied - Removed duplicate extension entry from script<br><br>Ticket #23340 |
| UPDATE - 2.1.4 (L2) Ensure Safe Attachments policy is enabled - Clarify audit PS procedure, add remediation PS method<br><br>Ticket #22890 |
| UPDATE - 2.1.6 (L1) Ensure Exchange Online Spam Policies are set to notify administrators - Added additional setting to audit procedure<br><br>Ticket #23081 |
| UPDATE - 2.1.9 (L1) Ensure that DKIM is enabled for all Exchange Online Domains - Add additional check to audit procedure<br><br>Ticket #23282 |
| UPDATE - 2.4.1 (L1) Ensure Priority account protection is enabled and configured - Define steps in audit procedure to better match remediation<br><br>Ticket #22143 |
| UPDATE - 3.1.1 (L1) Ensure Microsoft 365 audit log search is Enabled - New purview portal<br><br>Ticket #23503 |
| UPDATE - 3.2.1 (L1) Ensure DLP policies are enabled - New purview portal, add some clarifying audit information<br><br>Ticket #23989 |
| UPDATE - 3.3.1 (L1) Ensure Information Protection sensitivity label policies are published - Change title, update description, rationale, impact<br><br>Ticket #24636 |
| UPDATE - 5.1.5.1 (L2) Ensure user consent to apps accessing company data on their behalf is not allowed - Change AUDIT pass conditions for PowerShell to be more explicit<br><br>Ticket #23470 |
| UPDATE - 5.1.5.2 (L1) Ensure the admin consent workflow is enabled - Add PowerShell audit method<br><br>Ticket #23394 |

| |
|---|
| UPDATE - 5.1.8.1 (L1) Ensure that password hash sync is enabled for hybrid deployments - Use correct PowerShell audit procedure<br><br>Ticket #23017 |
| UPDATE - 5.2.2.10 (L1) Ensure a managed device is required for authentication - Renumbered to 5.2.2.9<br><br>Ticket #24628 |
| UPDATE - 5.2.2.11 (L1) Ensure a managed device is required for MFA registration - Title change, and Renumbered to 5.2.2.10<br><br>Ticket #23850 |
| UPDATE - 5.2.2.2 (L1) Ensure multifactor authentication is enabled for all users - Add additional impact<br><br>Ticket #22501 |
| UPDATE - 5.2.2.4 (L1) Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users - Audit procedure changes<br><br>Ticket #23885 |
| UPDATE - 5.2.2.9 (L1) Ensure a managed device is required for authentication - Add additional impact and notes about Guests<br><br>Ticket #23892 |
| UPDATE - 5.2.2.9 (L1) Ensure a managed device is required for authentication - Fix mistake in remediation section<br><br>Ticket #24494 |
| UPDATE - 5.2.2.9 (L2) Ensure 'sign-in risk' is blocked for medium and high risk - Renumbered to 5.2.2.8<br><br>Ticket #24627 |
| UPDATE - 5.2.3.2 (L1) Ensure custom banned passwords lists are used - Added PowerShell audit method<br><br>Ticket #23404 |
| UPDATE - 5.2.3.5 (L1) Ensure weak authentication methods are disabled - Add PowerShell methods<br><br>Ticket #23418 |

| |
|---|
| UPDATE - 5.3.2 (L1) Ensure 'Access reviews' for Guest Users are configured - Added powershell audit method<br><br>Ticket #23469 |
| UPDATE - 6.1.2 (L1) Ensure mailbox audit actions are configured - Clarify audit/remediation script output details<br><br>Ticket #24600 |
| UPDATE - 6.1.x (L1) Ensure mailbox auditing for E5 users is Enabled - Merged E3/E5 controls due to licensing changes<br><br>Ticket #24118 |
| UPDATE - 6.2.2 (L1) Ensure mail transport rules do not whitelist specific domains - UI Audit procedure steps made more specific<br><br>Ticket #22306 |
| UPDATE - 6.2.3 (L1) Ensure email from external senders is identified - Add impact<br><br>Ticket #24498 |
| UPDATE - 6.3.1 (L2) Ensure users installing Outlook add-ins is not allowed - Audit script updated to display better output<br><br>Ticket #22309 |
| UPDATE - 6.5.1 (L1) Ensure modern authentication for Exchange Online is enabled - Added UI methods<br><br>Ticket #24181 |
| UPDATE - 7.2.7 (L1) Ensure link sharing is restricted in SharePoint and OneDrive' - Add more the more restrictive passing state<br><br>Ticket #22509 |
| UPDATE - 8.2.1 (L2) Ensure external domains are restricted in the Teams admin center - Global Policy is now the target property<br><br>Ticket #24532 |
| UPDATE - 8.2.2 (L1) Ensure communication with unmanaged Teams users is disabled - Global Policy is now the target property<br><br>Ticket #24533 |

| |
|---|
| UPDATE - 8.2.3 (L1) Ensure external Teams users cannot initiate conversations - Now reflects minor changes done to the UI<br><br>Ticket #24102 |
| UPDATE - 8.2.4 (L1) Ensure communication with Skype users is disabled - Updated to reflect minor UI changes<br><br>Ticket #24534 |
| UPDATE - 8.4.1 (L1) Ensure app permission policies are configured - Navigation change<br><br>Ticket #24180 |
| UPDATE - 8.5.1 (L2) Ensure anonymous users can't join a meeting - Description and references update<br><br>Ticket #24431 |
| UPDATE - 8.5.3 (L1) Ensure only people in my org can bypass the lobby - Changed value to 'People who were invited'<br><br>Ticket #21912 |
| UPDATE - 6.1.4 (L1) Ensure 'AuditBypassEnabled' is not enabled on mailboxes - Renumbered to 6.1.3<br><br>Ticket #24121 |
| **Date: 10/31/2024 Version: 4.0.0** |
| UPDATE - 2.1.7 (L2) Ensure that an anti-phishing policy has been created - Changed to L2, changed audit/remediation<br><br>Ticket #18413 |
| UPDATE - 1.1.1 (L1) Ensure Administrative accounts are cloud-only - Add PowerShell audit method<br><br>Ticket #19472 |
| UPDATE - 1.1.1 (L1) Ensure Administrative accounts are cloud-only - Add additional impact information<br><br>Ticket #20816 |
| UPDATE - 1.1.1 (L1) Ensure Administrative accounts are cloud-only - Separated controls into a 2nd recommendation<br><br>Ticket #21069 |

| |
|---|
| RENAME - 5.1.1.1 (L1) Ensure Security Defaults is disabled - Removed Azure from title<br><br>Ticket #21505 |
| UPDATE - 5.1.2.4 (L1) Ensure access to the Entra admin center is restricted - Changed recommendation title<br><br>Ticket #21506 |
| UPDATE - 5.2.2.6 (L1) Enable Identity Protection user risk policies - Change to Level 1, new title<br><br>Ticket #21514 |
| UPDATE - 5.2.2.7 (L1) Enable Identity Protection sign-in risk policies - Move to L1 and new title<br><br>Ticket #21515 |
| UPDATE - 5.3.1 (L2) Ensure 'Privileged Identity Management' is used to manage roles - Fixed several role names<br><br>Ticket #21991 |
| UPDATE -7.3.3 (L1) Ensure custom script execution is restricted on personal sites - Removed personal sites setting<br><br>Ticket #21992 |
| UPDATE - 5.2.2.5 (L2) Ensure 'Phishing-resistant MFA strength' is required for Administrators - Additional impact added<br><br>Ticket #22255 |
| UPDATE – 1.3.1 (L1) Ensure the 'Password expiration policy' is set to 'Set passwords to never expire (recommended)' - Remediation param change<br><br>Ticket #22401 |
| UPDATE - 1.1.2 (L1) Ensure two emergency access accounts have been defined - Added warning about break glass and new MFA requirements<br><br>Ticket #22414 |
| ADD - 7.2.11 (L1) Ensure the SharePoint default sharing link permission is set<br><br>Ticket #22506 |
| ADD - 8.5.9 (L2) Ensure meeting recording is off by default<br><br>Ticket #22507 |

| |
|---|
| UPDATE - 2.4 Settings - Section renamed to 'System'<br><br>Ticket #22512 |
| UPDATE - 8.2.1 (L2) Ensure external domains are restricted in the Teams admin center - Change to level 2, split out other settings to new recommendations<br><br>Ticket #22529 |
| ADD - 8.2.2 (L1) Ensure communication with unmanaged Teams users is disabled<br><br>Ticket #22531 |
| ADD - 8.2.3 (L1) Ensure external Teams users cannot initiate conversations<br><br>Ticket #22532 |
| ADD - 8.2.4 (L1) Ensure communication with Skype users is disabled<br><br>Ticket #22533 |
| ADD - 9.1.10 (L1) Ensure access to APIs by Service Principals is restricted<br><br>Ticket #22535 |
| ADD - 9.1.11 (L1) Ensure Service Principals cannot create and use profiles<br><br>Ticket #22536 |
| UPDATE - 2.1.11 (L2) Ensure comprehensive attachment filtering is applied - Removed XML extension<br><br>Ticket #22564 |
| ADD - 6.5.4 (L1) Ensure SMTP AUTH is disabled<br><br>Ticket #22578 |
| ADD - 2.1.12 (L1) Ensure the connection filter IP allow list is not used<br><br>Ticket #22580 |
| ADD - 2.1.13 (L1) Ensure the connection filter safe list is off<br><br>Ticket #22588 |
| ADD - 2.1.14 (L1) Ensure inbound anti-spam policies do not contain allowed domains<br><br>Ticket #22589 |

| |
|---|
| ADD - 5.2.2.9 (L2) Ensure 'sign-in risk' is blocked for medium and high risk<br><br>Ticket #22590 |
| UPDATE - 5.2.2.3 (L1) Enable Conditional Access policies to block legacy authentication - Clarified steps<br><br>Ticket #22591 |
| UPDATE - 5.2.2.4 (L1) Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users - Clarified and standardized steps<br><br>Ticket #22601 |
| ADD - 5.2.3.5 (L1) Ensure weak authentication methods are disabled<br><br>Ticket #22603 |
| UPDATE - 1.3.2 (L1) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices - Add additional impact item<br><br>Ticket #22612 |
| ADD - 5.2.2.10 (L1) Ensure a managed device is required for authentication<br><br>Ticket #22614 |
| ADD - 5.2.2.11 (L1) Ensure a managed device is required for MFA registration<br><br>Ticket #22618 |
| ADD - 5.3.4 (L1) Ensure approval is required for Global Administrator role activation<br><br>Ticket #22637 |
| ADD - 5.1.6.2 (L1) Ensure that guest user access is restricted<br><br>Ticket #22639 |
| ADD - 5.1.6.3 (L2) Ensure guest user invitations are limited to the Guest Inviter role<br><br>Ticket #22641 |
| REMOVE - 5.1.5.1 (L1) Ensure the Application Usage report is reviewed at least weekly<br><br>Ticket #22660 |
| UPDATE - Renumbered 5.1.5.2 to 5.1.5.1<br><br>Ticket #22661 |

| |
|---|
| UPDATE - Renumbered 5.1.5.3 to 5.1.5.2<br><br>Ticket #22662 |
| REMOVE - 1.1.4 (L1) Ensure Guest Users are reviewed at least biweekly<br><br>Ticket #22663 |
| REMOVE - 2.1.11 (L1) Ensure the spoofed domains report is reviewed weekly<br><br>Ticket #22664 |
| REMOVE - 2.1.12 (L1) Ensure the 'Restricted entities' report is reviewed weekly<br><br>Ticket #22665 |
| REMOVE - 2.1.13 (L1) Ensure malware trends are reviewed at least weekly<br><br>Ticket #22666 |
| UPDATE - Renumbered 2.1.14 to 2.1.11<br><br>Ticket #22667 |
| REMOVE - 2.3.1 (L1) Ensure the Account Provisioning Activity report is reviewed at least weekly<br><br>Ticket #22668 |
| REMOVE - 2.3.2 (L1) Ensure non-global administrator role group assignments are reviewed at least weekly<br><br>Ticket #22669 |
| REMOVE - 3.1.2 (L1) Ensure user role group changes are reviewed at least weekly<br><br>Ticket #22670 |
| REMOVE - 5.2.4.2 (L1) Ensure the self-service password reset activity report is reviewed at least weekly<br><br>Ticket #22671 |
| REMOVE - 5.2.6.1 (L1) Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly<br><br>Ticket #22672 |
| REMOVE - 6.4.1 (L1) Ensure mail forwarding rules are reviewed at least weekly<br><br>Ticket #22673 |

| |
|---|
| ADD - 1.1.4 Ensure administrative accounts use licenses with a reduced application footprint<br><br>Ticket #22675 |
| UPDATE - 5.2.2.8 (L2) Ensure admin center access is limited to administrative roles - Moved to level 2, added additional rationale and impacts<br><br>Ticket #22841 |
| UPDATE - 5.3.3 (L1) Ensure 'Access reviews' for privileged roles are configured - Changed the title of 5.3.3<br><br>Ticket #22842 |
| UPDATE - 5.3.3 (L1) Ensure 'Access reviews' for privileged roles are configured - Frequency change to monthly<br><br>Ticket #22892 |
| **Date: 04/29/2024 Version: 3.1.0** |
| ADD - 8.5.8 '(L2) Ensure external meeting chat is off'<br><br>Ticket #20237 |
| ADD - '2.4.4 (L1) Ensure Zero-hour auto purge for Microsoft Teams is on'<br><br>Ticket #18256 |
| ADD - 'Ensure comprehensive attachment filtering is applied'<br><br>Ticket #16477 |
| ADD - 5.2.3.4 '(L1) Ensure all  member users are 'MFA capable''<br><br>Ticket #16466 |
| UPDATE - 'Ensure meeting chat does not allow anonymous users' - Change to Level 2<br><br>Ticket #20416 |
| UPDATE - 'Ensure only organizers and co-organizers can present' - Change to Level 2<br><br>Ticket #20415 |
| UPDATE - 2.1.10 'Ensure DMARC Records for all Exchange Online domains are published' - Additional requirements for dmarc values and MOERA added<br><br>Ticket #18261 |

| |
|---|
| UPDATE - 2.1.13 '(L1) Ensure malware trends are reviewed at least weekly' - Changed title name<br><br>Ticket #20626 |
| UPDATE - 2.1.8 (L1) Ensure that SPF records are published for all Exchange Domains - Change audit to use PowerShell instead of nslookup<br><br>Ticket #21124 |
| UPDATE - 5.1.2.1 (L1) Ensure 'Per-user MFA' is disabled - Remove MSOL audit script due to deprecation<br><br>Ticket #20742 |
| UPDATE - 5.1.2.2 `(L2) Ensure third party integrated applications are not allowed ` - Added PowerShell methods<br><br>Ticket #20047 |
| UPDATE - 5.1.3.1 '(L1) Ensure a dynamic group for guest users is created' - Changed assessment status to Automated<br><br>Ticket #21268 |
| UPDATE - 5.1.5.2 '(L2) Ensure user consent to apps accessing company data on their behalf is not allowed' - Add PowerShell audit method<br><br>Ticket #20369 |
| UPDATE - 5.1.6.1 '(L2) Ensure that collaboration invitations are sent to allowed domains only' - Fixed confusing language in the audit/remediation<br><br>Ticket #21259 |
| UPDATE - 5.2.2.1 '(L1) Ensure multifactor authentication is enabled for all users in administrative role' - Added "All could apps" to audit section<br><br>Ticket #20225 |
| UPDATE - 5.2.2.2 '(L1) Ensure multifactor authentication is enabled for all users Draft' - Added All Cloud apps to audit procedure and clarified steps<br><br>Ticket #20224 |
| UPDATE - 5.2.2.5 '(L2) Ensure 'Phishing-resistant MFA strength' is required for Administrators' - Add additional item to impact statement<br><br>Ticket #20775 |

| |
|---|
| UPDATE - 5.2.2.8 `(L1) Ensure admin center access is limited to administrative roles' - Title change and changed app to Microsoft Admin Portals<br><br>Ticket #18965 |
| UPDATE - 5.2.3.1 '(L1) Ensure Microsoft Authenticator is configured to protect against MFA fatigue' - Added guidance for exclusions<br><br>Ticket #19856 |
| UPDATE - 5.3.1 '(L2) Ensure 'Privileged Identity Management' is used to manage roles' - Add additional roles to the list<br><br>Ticket #20258 |
| UPDATE - 6.2.1 '(L1) Ensure all forms of mail forwarding are blocked and/or disabled' - Include PSH methods for Step 2<br><br>Ticket #19710 |
| UPDATE - 6.3.1 '(L2) Ensure users installing Outlook add-ins is not allowed' - Note added in audit about global readers<br><br>Ticket #21057 |
| UPDATE - 6.5.2 '(L1) Ensure MailTips are enabled for end users' - Moved to Level 1<br><br>Ticket #20257 |
| UPDATE - 1.1.2 '(L1) Ensure two emergency access accounts have been defined' - Add additional note on management of emergency accounts<br><br>Ticket #19357 |
| UPDATE - 1.2.2 '(L1) Ensure sign-in to shared mailboxes is blocked Draft' - Uses Graph instead of AzureAD PowerShell now<br><br>Ticket #20153 |
| UPDATE - 1.3.3 '(L2) Ensure 'External sharing' of calendars is not available' - Change PowerShell method to target default policy<br><br>Ticket #21284 |
| UPDATE - '9.1.1 (L1) Ensure guest user access is restricted Draft' - Name of setting changed<br><br>Ticket #20954 |

| |
|---|
| UPDATE - '9.1.2 (L1) Ensure external user invitations are restricted' - Name of setting changed<br><br>Ticket #20955 |
| UPDATE - '9.1.3 (L1) Ensure guest access to content is restricted Draft' - Name of setting changed<br><br>Ticket #20956 |
| UPDATE - 3.2.2 '(L1) Ensure DLP policies are enabled for Microsoft Teams' - Overhaul audit steps and added additional notes about DLP<br><br>Ticket #19831 |
| UPDATE - 7.2.4 '(L2) Ensure OneDrive content sharing is restricted' - Included alternate PowerShell cmdlets and notes<br><br>Ticket #21034 |
| UPDATE - 7.3.4 '(L1) Ensure custom script execution is restricted on site collections' - Audit procedure now returns only sites that fail<br><br>Ticket #20419 |
| UPDATE - 8.2.1 'Ensure 'external access' is restricted in the Teams admin center' - Move to Level 1 profile<br><br>Ticket #20242 |
| UPDATE - 8.4.1 '(L1) Ensure app permission policies are configured' - Changed instructions to use new app centric management<br><br>Ticket #20815 |
| UPDATE - 8.5.3 '(L1) Ensure only people in my org can bypass the lobby' - Added to impact statement<br><br>Ticket #21267 |
| **Date: 09/29/2023 Version: 3.0.0** |
| ADD - 'Ensure external user invitations are restricted<br><br>Ticket #19537 |
| ADD - 'Ensure a dynamic group for guest users is created'<br><br>Ticket #19532 |

| |
|---|
| ADD - 'Ensure 'AuditBypassEnabled' is not enabled on user mailboxes'<br>Ticket #16473 |
| ADD - 'Ensure `AuditDisabled` for the organization is set to `False`<br>Ticket #19517 |
| ADD - 'Ensure email from external senders is identified'<br>Ticket #18286 |
| ADD - 'Ensure mailbox auditing for E3 users is Enabled Draft'<br>Ticket #19819 |
| ADD - 'Ensure Per-user MFA is disabled'<br>Ticket #18465 |
| ADD - 'Ensure sign-in to shared mailboxes is blocked'<br>Ticket #18280 |
| ADD - 'Ensure 'Block ResourceKey Authentication' is Enabled'<br>Ticket #19538 |
| ADD - 'Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled'<br>Ticket #19540 |
| ADD - 'Ensure 'Interact with and share R and Python visuals' is 'Disabled''<br>Ticket #19539 |
| ADD - 'Ensure 'Publish to web' is restricted'<br>Ticket #19536 |
| ADD - 'Ensure AAD guest access to content is restricted'<br>Ticket #19535 |
| ADD - 'Ensure AAD guest user access is restricted'<br>Ticket #19533 |
| ADD - 'Ensure enabling of external data sharing is restricted'<br>Ticket #19534 |

| |
|---|
| ADD - 'Ensure shareable links are restricted'<br>Ticket #19541 |
| ADD - 'Ensure OneDrive content sharing is restricted Draft'<br>Ticket #19718 |
| ADD - 'Ensure custom script execution is restricted on personal sites'<br>Ticket #19723 |
| ADD - 'Ensure custom script execution is restricted on site collections'<br>Ticket #19738 |
| ADD - 'Ensure external content sharing is restricted'<br>Ticket #19719 |
| ADD - 'Ensure external sharing is restricted by security group '<br>Ticket #19720 |
| ADD - 'Ensure guest access to a site or OneDrive will expire automatically'<br>Ticket #19721 |
| ADD - 'Ensure link sharing is restricted in SharePoint and OneDrive'<br>Ticket #19717 |
| ADD - 'Ensure reauthentication with verification codes is restricted'<br>Ticket #19722 |
| ADD - 'Ensure anonymous users and dial-in callers can't start a meeting'<br>Ticket #19665 |
| ADD - 'Ensure anonymous users can't join a meeting'<br>Ticket #19664 |
| ADD - 'Ensure app permission policies are configured'<br>Ticket #19663 |
| ADD - 'Ensure external participants can't give or request control'<br>Ticket #19670 |

| |
|---|
| ADD - 'Ensure meeting chat does not allow anonymous users'<br>Ticket #19668 |
| ADD - 'Ensure only organizers and co-organizers can present'<br>Ticket #19669 |
| ADD - 'Ensure only people in my org can bypass the lobby'<br>Ticket #19666 |
| ADD - 'Ensure users can report security concerns in Teams'<br>Ticket #19575 |
| ADD - 'Ensure users can't send emails to a channel email address'<br>Ticket #19661 |
| ADD - 'Ensure users dialing in can't bypass the lobby'<br>Ticket #19667 |
| REMOVE - '(L1) Ensure expiration time for external sharing links is set'<br>Ticket #19497 |
| UPDATE - 'Ensure Administrative accounts are separate and cloud-only' - Included important note about alerts<br>Ticket #18728 |
| UPDATE - 'Ensure Microsoft Defender for Cloud Apps is enabled and configured' - UI instructions updated due to integration of legacy portal into Defender.<br>Ticket #18085 |
| UPDATE - 'Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled' Include check for Safe Documents setting<br>Ticket #18412 |
| UPDATE - 'Ensure user consent to apps accessing company data on their behalf is not allowed' Changed to manual assessment status<br>Ticket #19711 |
| UPDATE - 'Ensure 'Microsoft Azure Management' is limited to administrative roles' - Add impact information about PIM<br>Ticket #19542 |

| |
|---|
| UPDATE - 'Ensure users installing Outlook add-ins is not allowed' - Updated UI instructions<br><br>Ticket #19496 |
| UPDATE - 'Sign-in risk policy' - Specify user risk levels and session control<br><br>Ticket #18083 |
| UPDATE - 'User risk policy' - Specify user risk level, and session control<br><br>Ticket #18084 |
| UPDATE - Ensure 'Restrict non-admin users from creating tenants' - Graph cmdlet is no longer beta, switch to automated assessment<br><br>Ticket #19753 |
| UPDATE - 'Ensure mailbox auditing for E5 users is Enabled' - Add audit script, update remediation script<br><br>Ticket #19642 |
| UPDATE - 'Ensure mailbox auditing for E5 users is Enabled' - Fixed critical issue in remediation script<br><br>Ticket #19249 |
| UPDATE - 'Ensure 'third-party storage services' are restricted in 'Microsoft 365 on the web'' - Assessment status changed to Manual<br><br>Ticket #19712 |
| UPDATE - 'Ensure that Sways cannot be shared with people outside of your organization' - Move to L2<br><br>Ticket #19059 |
| UPDATE - 'Idle session timeout' is set to '1 hour (or less)' for unmanaged devices - Change value to 3 hours<br><br>Ticket #19346 |
| UPDATE - 'Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled' Change status to Automated<br><br>Ticket #19709 |
| **Date: 03/15/2023 Version: 2.0.0** |
| UPDATE - 'Azure AD Risky sign-ins report' moved to E5 profile<br><br>Ticket #16420 |

| |
|---|
| UPDATE - 'Multifactor authentication is enabled for all users' move to L1<br><br>Ticket #16974 |
| UPDATE - 'SSPR' to include more information on Combined Registration<br><br>Ticket #16421 |
| UPDATE - 'Passwords Are Not Set to Expire' to MgGraph<br><br>Ticket #17399 |
| UPDATE - 'Security defaults' Included MgGraph method<br><br>Ticket #16469 |
| UPDATE- 'Security Defaults' Order and remediation info<br><br>Ticket #16331 |
| UPDATE - 'External file sharing in Teams' Remove skype references, update remediation<br><br>Ticket #17470 |
| UPDATE - 'Password hash sync' to use MgGraph<br><br>Ticket #16455 |
| UPDATE - 'Guest Users are reviewed at least biweekly' For MgGraph<br><br>Ticket #17522 |
| UPDATE - 'Ensure between two and four global admins' Update MSOL<br><br>Ticket #16456 |
| ADD - New recommendation for users tagged as priority accounts<br><br>Ticket #16472 |
| ADD - 'Strict protection preset for Priority accounts'<br><br>Ticket #17646 |
| UPDATE - 'Microsoft Defender for Cloud Apps'<br><br>Ticket #16479 |
| ADD - 'Restrict access to the Azure AD administration portal' is set to 'Yes'<br><br>Ticket #17153 |
| ADD - 'Microsoft Azure Management restrictions'<br><br>Ticket #17659 |
| UPDATE - 'MFA for all admins' Define list of directory roles<br><br>Ticket #16275 |

| |
|---|
| ADD - 'Microsoft Authenticator is configured to protect against MFA fatigue'<br>Ticket #16976 |
| ADD - 'Ensure 'Phishing-resistant MFA strength' is required for Administrators`<br>Ticket #16975 |
| ADD - 'Idle session timeout'<br>Ticket #16470 |
| ADD - 'Ensure custom banned passwords lists are used'<br>Ticket #17699 |
| UPDATE - 'Block legacy authentication' to include more on Impact<br>Ticket #16422 |
| UPDATE - 'DKIM for Exchange Online' = Audit/Remediation procedure<br>Ticket #17311 |
| UPDATE - 'Mail forwarding rules review..' remove MSOL dependency<br>Ticket #17520 |
| UPDATE - 'option to remain signed in is hidden'  Moved to Entra.<br>Ticket #17252 |
| UPDATE - 'Safe links policy' define all settings, and fix PowerShell remediation<br>Ticket #16460 |
| ADD - 'Restrict non-admin users from creating tenants'<br>Ticket #17033 |
| UPDATE - 'Admin consent workflow' Change to L1<br>Ticket #17720 |
| UPDATE - 'Disallow download of infected files in SharePoint' Added note about roles<br>Ticket #16488 |
| UPDATE - 'User installs of Outlook add-ins' PowerShell remediation<br>Ticket #17708 |
| UPDATE - 'DLP policies are enabled for Teams' Included note about Connect-IPPSSession<br>Ticket #17711 |
| UPDATE - 'SharePoint guest restrictions' to include defaults<br>Ticket #17736 |

| |
|---|
| UPDATE - 'Role group change reviews' Fixed PowerShell method<br>Ticket #17786 |
| ADD - 'Microsoft 365 on the web restrictions'<br>Ticket #17803 |
| UPDATE - 'External storage provides'<br>Ticket #16487 |
| UPDATE - 'Review the restricted entities report' added PS method<br>Ticket #17801 |
| ADD - 'Access reviews for Guests E5'<br>Ticket #14853 |
| UPDATE - 'Teams external access restrictions' Add PowerShell methods<br>Ticket #16486 |
| UPDATE - 'User consent to apps' removed MSOL methods<br>Ticket #17469 |
| UPDATE - ‘Ensure al forms of mail forwarding are blocked'  Changed to two steps for equal coverage<br>Ticket #16459 |
| UPDATE - 'anti-phishing policy' determine baseline settings in audit section<br>Ticket #17719 |
| REMOVE - 'Removed Endpoint Manager recommendations'<br>Ticket #17834 |
| UPDATE - 'External sharing of calendars' additional script to check for published calendars<br>Ticket #17820 |
| UPDATE - 'Mobile device requirements' compliance policy<br>Ticket #16970 |
| ADD - 'SharePoint and OneDrive integration with Azure AD B2B'<br>Ticket #17034 |
| UPDATE - 'Risky sign-ins report' removed bad request in Graph Explorer<br>Ticket #16404 |

| |
|---|
| UPDATE - 'collaboration invitations' to include notes about sharing<br><br>Ticket #16854 |
| ADD - 'Ensure two Emergency Access accounts have been defined'<br><br>Ticket #16891 |
| ADD - 'Access reviews for high privileged Azure AD roles'<br><br>Ticket #17863 |
| UPDATE - 'Application usage report' To include step for "Usage & insights"<br><br>Ticket #17784 |
| UPDATE - 'Just in time privileged access' Title change to Privileged Identity Management<br><br>Ticket #17875 |
| UPDATE - 'Sign-in frequency and persistence'<br><br>Ticket #17613 |
| UPDATE - URLS in references sections to adjust for redirections, and length<br><br>Ticket #17930 |
| **Date: 08/18/2022 Version: 1.5.0** |
| UPDATE - Cannot audit LinkedIn Contact sync programmatically - Make Manual<br><br>Ticket #15139 |
| UPDATE - API is available to assess Password Protection<br><br>Ticket #14800 |
| UPDATE - Audit Procedure Wording for skype/teams<br><br>Ticket #15103 |
| MOVED - Ensure Safe Links for Office Applications is Enabled moved under section 2 - ensure safe links for office apps.<br><br>Ticket #15026 |
| MOVED - What is difference between the checks 4.5 and 2.3 ? (Safe Links for Exchange and Office Apps)<br><br>Ticket #14991 |

| |
|---|
| UPDATE - Safe Links Policy cmdlet: the parameter 'IsEnabled' is no longer supported.<br>Ticket #15493 |
| UPDATE - Remove AdminAuditLogEnabled - ON-PREM only command<br>Ticket #15109 |
| UPDATE - Audit DLP for Teams via PowerShell<br>Ticket #14990 |
| UPDATE - Parameter AllowClickThrough is deprecated for SafeLinksPolicy<br>Ticket #14992 |
| UPDATE - PowerShell cmdlet for assessing password hash sync<br>Ticket #15022 |
| UPDATE - Only works in the new Exchange Admin center, Fixed PS remediation<br>Ticket #15972 |
| UPDATE - Clarify breadth of report<br>Ticket #16097 |
| UPDATE - PowerShell guidance, Role Name to Role Object ID<br>Ticket #16125 |
| UPDATE - Missing a step<br>Ticket #15967 |
| REMOVE - Ensure modern authentication for Skype for Business Online is enabled<br>Ticket #15719 |
| UPDATE - Improve PowerShell Audit Procedure guidance<br>Ticket #15970 |
| UPDATE - Block OneDrive, clarify scope and accuracy of recommendation<br>Ticket #16147 |
| UPDATE - PS cmdlet correction<br>Ticket #16140 |

| |
|---|
| UPDATE - DLP settings found in SecureScore Portal/API<br><br>Ticket #13747 |
| UPDATE - 'Ensure the option to stay signed in' Audit and Remediation steps<br><br>Ticket #16016 |
| UPDATE - Provide more detailed path for audit<br><br>Ticket #15968 |
| UPDATE - Safe Links Audit+Remediation Ticket #16025 |
| UPDATE - Connect-EXOPSSession V1 cmdlet replaced with V2 Connect-ExchangeOnline<br><br>Ticket #15942 |
| UPDATE - Ensure the spoofed domains report is reviewed weekly<br><br>Ticket #15317 |
| UPDATE - Microsoft Compliance became Microsoft Purview<br><br>Ticket #15432 |
| UPDATE - Fix rationale<br><br>Ticket #16107 |
| UPDATE - Role group changes procedures<br><br>Ticket #16037 |
| UPDATE - Password hash sync audit procedure<br><br>Ticket #16184 |
| UPDATE - change 'unlicensed' to 'un-assigned' to clarify the point that 'apps' are not assigned.<br><br>Ticket #15015 |
| UPDATE - Implement Spam Filter Policy w/transport rule to simplify<br><br>Ticket #14642 |
| UPDATE - Modern Authentication Clients option no longer listed<br><br>Ticket #15318 |

| |
|---|
| REMOVE - Non-Owners Report is deprecated<br><br>Ticket #16195 |
| UPDATE - Ensure notifications for internal users sending malware is Enabled should be check for Default Policy or for all polices<br><br>Ticket #15725 |
| UPDATE - Ensure Safe Links for Office Applications is Enabled<br><br>Ticket #15482 |