Center for Internet Security

CIS Benchmarks™

CIS Microsoft 365 Foundations Benchmark

v1.5.0 - 08-31-2022

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/

Table of Contents

Overview

All CIS 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 for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

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

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, Skype/Teams, Azure Active Directory, and inTune.

To ensure all PowerShell related cmdlets work in your tenant please download the latest versions of the PowerShell modules. Commands from this benchmark were tested using the following modules:

- ExchangeOnlineManagement `2.0.6-Preview6`
- AzureADPreview `2.0.2.149`
- MSOnline `1.1.183.66`
- MicrosoftTeams `4.3.0`
- Microsoft.Online.SharePoint.PowerShell `16.0.22615.12000`

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, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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. 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
Clifford Moten
Brian Greidanus
Daniel Stutz
Viktor Gazdag
Richard Handley
Lewis Hardy
Jennifer Jarose
Mike Owens
Mack Bodie
Shelby Kiger
Gururaj Pandurangi
Daniel Stutz
Juan Nieto

Editor
Dan Menicucci
Wacey Lanier
Cody McLees
Caleb Eifert

Recommendations

1 Account / Authentication

1.1 Azure Active Directory

Section on AAD as the underlying AuthN / AuthZ for SaaS

1.1.1 (L1) Ensure multifactor authentication is enabled for all users in administrative roles (Automated)

Profile Applicability:

- E3 Level 1

Description:

Enable multifactor authentication for all users who are members of administrative roles in the Microsoft 365 tenant. These include roles such as:

- Global Administrator
- Billing Administrator
- Exchange Administrator
- SharePoint Administrator
- Password Administrator
- Skype for Business Administrator
- Service Support Administrator
- User Administrator
- Dynamics 365 Service Administrator
- Power BI Administrator

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 verify the multifactor authentication configuration for administrators, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Enterprise applications` then, under `Security`, select `Conditional Access`.
4. Review the list of policies and ensure that there is a policy that requires the `Grant` access control with `Require multi-factor authentication` for the appropriate `Directory roles` under `Users and groups`

To verify the multifactor authentication configuration for administrators, use the M365 SecureScore service:

1. Log in to the Secure Score portal (https://security.microsoft.com) using admin permissions (global admin or a custom admin role) for an Office 365 Enterprise, Microsoft 365 Business, or Office 365 Business Premium subscription.
2. Click on `Require MFA for Azure AD privileged roles` policy to check MFA for admin users.
3. It will show the number of Admin users who do not have MFA configured.

This information is also available via the Microsoft Graph Security API:

```
GET https://graph.microsoft.com/beta/security/secureScores
```

Remediation:

To enable multifactor authentication for administrators, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Enterprise applications` then, under `Security`, select `Conditional Access`.
4. Click `New policy`
5. Go to `Assignments` > `Users and groups` > `Include` > `Select users and groups` > check `Directory roles`.
6. At a minimum, select the following roles: `Billing admin`, `Conditional Access admin`, `Exchange admin`, `Global admin`, `Helpdesk admin`, `Security admin`, `SharePoint admin`, and `User admin`.
7. Go to `Cloud apps or actions` > `Cloud apps` > `Include` > select `All cloud apps (and don't exclude any apps)`.
8. Under `Access controls` > `Grant` > select `Grant access` > check `Require multi-factor authentication` (and nothing else).
9. Leave all other conditions blank.
10. Make sure the policy is enabled.
11. Create.

References:

1. https://docs.microsoft.com/en-us/graph/api/resources/security-api-overview?view=graph-rest-beta

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access 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 Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

1.1.2 (L2) Ensure multifactor authentication is enabled for all users in all roles (Manual)

Profile Applicability:

- E3 Level 2

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.

Audit:

To verify the multifactor authentication configuration for all users, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Enterprise applications` then, under `Security`, select `Conditional Access`.
4. Review the list of policies and ensure that there is a policy that requires the `Grant` access control with `Require multi-factor authentication` for `All users` under `Users and groups`

To verify the multifactor authentication configuration for administrators, use the M365 SecureScore service:

1. Log in to the Secure Score portal (https://security.microsoft.com/securescore) using admin permissions (global admin or a custom admin role) for an Office 365 Enterprise, Microsoft 365 Business, or Office 365 Business Premium subscription.
2. Click on `Ensure all users can complete multi-factor authentication for secure access` recommended action to check MFA for all users.
3. It will show the number of users who do not have MFA configured.

This information is also available via the Microsoft Graph Security API:

```
GET https://graph.microsoft.com/beta/security/secureScores
```

Remediation:

To enable multifactor authentication for all users, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Enterprise applications` then, under `Security`, select `Conditional Access`.
4. Click `New policy`
5. Go to `Assignments` > `Users and groups` > `Include` > select `All users` (and do not exclude any user).
6. Select `Cloud apps or actions` > `All cloud apps` (and don't exclude any apps)
7. `Access Controls` > `Grant` > `Require multi-factor authentication` (and nothing else)
8. Leave all other conditions blank
9. Make sure the policy is Enabled/On
10. Create

Default Value:

Disabled

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa
2. https://docs.microsoft.com/en-us/azure/active-directory/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 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 Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

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

Profile Applicability:

- E3 Level 1

Description:

More than one global administrator should be designated so a single admin can be monitored and to provide redundancy should a single admin leave an organization. Additionally, there should be no more than four global admins set for any tenant. Ideally global administrators will have no licenses assigned to them.

Rationale:

If there is only one global tenant administrator, he or she can perform malicious activity without the possibility of being discovered by another admin. If there are numerous global tenant administrators, the more likely it is that one of their accounts will be successfully breached 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 verify the number of global tenant administrators, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Select `Users` > `Active Users`.
3. Select `Filter` then select `Global Admins`.
4. Review the list of `Global Admins` to confirm there are from two to four such accounts.

To verify the number of global tenant administrators, you can also use the Office 365 PowerShell MSOL:

1. Connect to Microsoft 365 using `Connect-MSOLService`
2. Run the following PowerShell commands:

```
Get-MsolRoleMember -RoleObjectId 62e90394-69f5-4237-9190-012177145e10
```

This information is also available via the Microsoft Graph Security API:

```
GET https://graph.microsoft.com/beta/security/secureScores
```

Remediation:

To correct the number of global tenant administrators, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
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`.

To correct the number of global tenant administrators, you can also use the Office 365 PowerShell MSOL:

1. Connect to Microsoft 365 using `Connect-MSOLService`
2. Run the following PowerShell command to create a new Global Admin:

```
Add-MsolRoleMember -RoleObjectId 62e90394-69f5-4237-9190-012177145e10 -
RoleMemberEmailAddress "AdeleV@contoso.com"
```

4. Run the following PowerShell command to remove Global Admins:

```
Remove-MsolRoleMember -RoleObjectId 62e90394-69f5-4237-9190-012177145e10 -
RoleMemberEmailAddress "AdeleV@contoso.com"
```

References:

1. https://docs.microsoft.com/en-us/office365/enterprise/powershell/assign-roles-to-user-accounts-with-office-365-powershell
2. https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#role-template-ids

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts 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 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 self-service password reset is enabled (Manual)

Profile Applicability:

- E3 Level 1

Description:

Enabling self-service password reset allows users to reset their own passwords in Azure AD. When your 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. As of August 2020 combined registration is enabled by default.

Reference: How to enable combined registration

Rationale:

Users will no longer need to engage the helpdesk for password resets, and the password reset mechanism will automatically block common, easily guessable passwords. Combined registration should be enabled if not already, as of August of 2020 combined registration is automatic for new tenants therefor users will not need to register for password reset separately from multi-factor authentication.

Impact:

The impact associated with this setting is that 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. As of August of 2020 combined registration is automatic for new tenants therefor users will not need to register for password reset separately from multi-factor authentication.

NOTE: This will not work if using Azure AD Connect / Sync.

Audit:

To verify self-service password reset is enabled, use the Microsoft 365 Admin Center:

1. Under `Admin centers` choose `Azure Active Directory`.
2. Choose `Users` from the left hand navigation.
3. Choose `Password reset`.
4. On the Properties page, ensure that `All` is selected under `Self service password reset enabled`.

Remediation:

To enable self-service password reset, use the Microsoft 365 Admin Center:

1. Under `Admin centers` choose `Azure Active Directory`.
2. Choose `Users` from the left hand navigation.
3. Choose `Password reset`.
4. On the Properties page, select `All` under `Self service password reset enabled`.
5. Select `Save`.

References:

1. https://support.office.com/en-us/article/let-users-reset-their-own-passwords-in-office-365-5bc3f460-13cc-48c0-abd6-b80bae72d04a
2. https://gallery.technet.microsoft.com/office/Enable-Self-Service-59846d88
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-registration-mfa-sspr-combined

1.1.5 (L1) Ensure that password protection is enabled for Active Directory (Manual)

Profile Applicability:

- E3 Level 1

Description:

Enable Azure Active Directory Password Protection to Active Directory to protect against the use of common passwords.

Note: This recommendation applies to Hybrid deployments only, and will have no impact unless working with on-premises Active Directory.

Rationale:

Azure Active Directory 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 Azure Active Directory Password Protection may require users to change passwords, and adhere to more stringent requirements than they have been accustomed to.

Audit:

To verify that Azure Active Directory Password Protection is enabled, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Azure Active Directory` then `Security` on the left side navigation followed by `Authentication methods`.
4. Select `Password protection` and ensure that `Enable password protection on Windows Server Active Directory` is set to `Yes` and also that `Mode` is set to `Enforced`
5. Verify that the Domain Controller Agent and Proxy's are deployed to the Domain Controllers in the environment

This information is also available via the Microsoft Graph Security API:

```
https://graph.microsoft.com/beta/[Domain name]/settings
```

Ensure `Enable password protection on Windows Server Active Directory`.

Remediation:

To setup Azure Active Directory Password Protection, use the following steps:

1. Download and install the `Azure AD Password Proxies` and `DC Agents` from the following location: https://www.microsoft.com/download/details.aspx?id=57071
2. After the installation is complete, login to `https://admin.microsoft.com` as a `Global Administrator`.
3. Go to `Admin centers` and click on `Azure Active Directory`.
4. Select `Azure Active Directory` then `Security` on the left side navigation followed by `Authentication methods`.
5. Select `Password protection` and toggle `Enable password protection on Windows Server Active Directory` to `Yes` and `Mode` to `Enforced`
6. Click Save at the top of the right pane.

Default Value:

Enabled / Enforced

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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 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.		●	●

1.1.6 (L1) Enable Conditional Access policies to block legacy authentication (Automated)

Profile Applicability:

- E3 Level 1

Description:

Use Conditional Access to block legacy authentication protocols in Office 365.

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.

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.

Audit:

To verify that legacy authentication is blocked, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Azure Active Directory` then `Security`.
4. Select `Conditional Access`.
5. Verify that either the policy `Baseline policy: Block legacy authentication` is set to On or find another with the following settings enabled:
    - Under `Conditions` then `Client apps` ensure the settings are enabled for and `Exchange ActiveSync clients` and `other clients`.
    - Under `Access controls` ensure the `Grant` is set to `Block access`
    - Under `Assignments` ensure `All users` is enabled
    - Under `Assignments` and `Users and groups` ensure the `Exclude` is set to least one low risk account or directory role. This is required as a best practice.

This information is also available via the Microsoft Graph Security API:

```
GET https://graph.microsoft.com/beta/security/secureScores
```

Remediation:

To setup a conditional access policy to block legacy authentication, use the following steps:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Azure Active Directory` then `Security`.
4. Select `Conditional Access`.
5. Create a new policy by selecting `New policy`.
6. Set the following conditions within the policy.
    - Select `Conditions` then `Client apps` enable the settings for and `Exchange ActiveSync clients` and `other clients`.
    - Under `Access controls` set the `Grant` section to `Block access`
    - Under `Assignments` enable `All users`
    - Under `Assignments` and `Users and groups` set the `Exclude` to be at least one low risk account or directory role. This is required as a best practice.

Default Value:

Legacy authentication is enabled by default.

References:

1. https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

Additional Information:

NOTE: For more granularity the following Audit/Remediation procedure could be utilized.

AUDIT

To verify basic authentication is disabled, use the Exchange Online PowerShell Module:

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

```
Get-OrganizationConfig | Select-Object -ExpandProperty
DefaultAuthenticationPolicy | ForEach { Get-AuthenticationPolicy $_ | Select-
Object AllowBasicAuth* }
```

4. Verify each of the basic authentication types is set to `false`. If no results are shown or an error is displayed, then no default authentication policy has been defined for your organization.
5. Verify Exchange Online users are configured to use the appropriate authentication policy (in this case Block Basic Auth) by running the following PowerShell command:

```
Get-User -ResultSize Unlimited | Select-Object UserPrincipalName,
AuthenticationPolicy
```

REMEDIATION

To disable basic authentication, use the Exchange Online PowerShell Module:

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

*Note: If a policy exists and a command fails you may run `Remove-AuthenticationPolicy` first to ensure policy creation/application occurs as expected.

```
$AuthenticationPolicy = Get-OrganizationConfig | Select-Object
DefaultAuthenticationPolicy

If (-not $AuthenticationPolicy.Identity) {
  $AuthenticationPolicy = New-AuthenticationPolicy "Block Basic Auth"
  Set-OrganizationConfig -DefaultAuthenticationPolicy
$AuthenticationPolicy.Identity
}

Set-AuthenticationPolicy -Identity $AuthenticationPolicy.Identity -
AllowBasicAuthActiveSync:$false -AllowBasicAuthAutodiscover:$false -
AllowBasicAuthImap:$false -AllowBasicAuthMapi:$false -
AllowBasicAuthOfflineAddressBook:$false -AllowBasicAuthOutlookService:$false
-AllowBasicAuthPop:$false -AllowBasicAuthPowershell:$false -
AllowBasicAuthReportingWebServices:$false -AllowBasicAuthRpc:$false -
AllowBasicAuthSmtp:$false -AllowBasicAuthWebServices:$false

Get-User -ResultSize Unlimited | ForEach-Object { Set-User -Identity
$_.Identity -AuthenticationPolicy $AuthenticationPolicy.Identity -
STSRefreshTokensValidFrom $([System.DateTime]::UtcNow) }
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software 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 Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

1.1.7 (L1) Ensure that password hash sync is enabled for hybrid deployments (Manual)

Profile Applicability:

- E3 Level 1

Description:

Password hash synchronization is one of the sign-in methods used to accomplish hybrid identity synchronization. Azure AD Connect synchronizes a hash, of the hash, of a user's password from an on-premises Active Directory instance to a cloud-based Azure AD instance.

Note: Audit and remediation procedures in this recommendation only apply to Microsoft 365 tenants operating in a hybrid configuration using Azure AD Connect sync.

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 Azure AD Identity Protection and is a subset of that feature which can help identity 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 resislient 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.

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:

Verify if Password Hash Sync is enabled using the Azure Admin Center

1. From the Microsoft 365 admin center, click on `Azure Active Directory` under Admin centers.
2. Select `Azure Active Directory`
3. Underneath **Manage** select `Azure AD Connect`
4. Under **Azure AD Connect Sync**, verify Password Hash Sync is `Enabled`

Verify if Password Hash Sync is enabled using the Azure AD Connect tool:

1. Log in to the server that hosts the Azure AD Connect tool
2. Run `Azure AD Connect`, and then click `View current configuration`. In the details pane, check whether Password synchronization is enabled on your tenant.

This information is also available via the Microsoft Graph Security API:

```
GET https://graph.microsoft.com/beta/security/secureScores
```

To verify if Password Hash Sync is enabled, you may utilize the following PowerShell

```
Get-MsolCompanyInformation | select-object PasswordSynchronizationEnabled
```

Remediation:

To setup Password Hash Sync, use the following steps:

1. Log in to the server that hosts the Azure AD 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:

- Azure AD Connect sync `disabled` by default
- Password Hash Sync is Microsoft's recommended setting for new deployments

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs
2. https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#user-linked-detections

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control 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 Encrypt or hash with a salt all authentication credentials when stored.		●	●

1.1.8 (L2) Enable Azure AD Identity Protection sign-in risk policies (Manual)

Profile Applicability:

- E5 Level 2

Description:

Azure Active Directory Identity 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.

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 verify if a Sign-In risk policy is enabled, use the following steps:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Azure Active Directory` then `Security`.
4. Select `Conditional Access`.
5. Ensure that a policy exist with the following characteristics and is set to `on`.
    - Under `Users or workload identities` choose `All users`
    - Under `Cloud apps or actions` choose `All cloud apps`
    - Under `Conditions` choose `Sign-in risk` then `Yes` in the right pane followed by the appropriate level.
    - Under `Access Controls` select `Grant` then in the right pane click `Grant access` then select `Require muilti-factor authentication`.

Remediation:

To configure a Sign-In risk policy, use the following steps:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Azure Active Directory` then `Security`.
4. Select `Conditional Access`.
5. Create a new policy by selecting `New policy`.
6. Set the following conditions within the policy.
    - Under `Users or workload identities` choose `All users`
    - Under `Cloud apps or actions` choose `All cloud apps`
    - Under `Conditions` choose `Sign-in risk` then `Yes` in the right pane followed by the appropriate level.
    - Under `Access Controls` select `Grant` then in the right pane click `Grant access` then select `Require muilti-factor authentication`.
7. Click `Select`
8. You may opt to begin in a state of `Report Only` as you step through implementation however, the policy will need to be set to `On` to be in effect.
9. Click `Create`.

NOTE: for more information regarding risk levels refer to Microsoft's Identity Protection & Risk Doc

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback
2. https://docs.microsoft.com/en-us/azure/active-directory/identity-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 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 Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

1.1.9 (L2) Enable Azure AD Identity Protection user risk policies (Manual)

Profile Applicability:

- E5 Level 2

Description:

Azure Active Directory Identity Protection user risk policies detect the probability that a user account has been compromised.

Rationale:

With the user risk policy turned on, Azure AD detects the probability that a user account has been compromised. As an administrator, you can configure a user risk conditional access policy to automatically respond to a specific user risk level. For example, you can block access to your resources or require a password change to get a user account back into a clean state.

Impact:

When the policy triggers, access to the account will either be blocked or the user would be required to use multi-factor authentication and change their password. Users who haven't registered MFA on their account will be blocked from accessing it. If account access is blocked, an admin would need to recover the account. It is therefore recommended that the MFA registration policy be configured for all users who are a part of the User Risk policy.

Audit:

To verify if a User Risk policy is enabled, use the following steps:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Azure Active Directory` then `Security`.
4. Select `Conditional Access`.
5. Ensure that a policy exist with the following characteristics and is set to `on`.
    - Under `Users or workload identities` choose `All users`
    - Under `Cloud apps or actions` choose `All cloud apps`
    - Under `Conditions` choose `User risk` then `Yes` in the right pane followed by the appropriate level.
    - Under `Access Controls` select `Grant` then in the right pane click `Grant access` then select `Require password change`.

Remediation:

To configure a User risk policy, use the following steps:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Azure Active Directory` then `Security`.
4. Select `Conditional Access`.
5. Create a new policy by selecting `New policy`.
6. Set the following conditions within the policy.
    - Under `Users or workload identities` choose `All users`
    - Under `Cloud apps or actions` choose `All cloud apps`
    - Under `Conditions` choose `User risk` then `Yes` in the right pane followed by the appropriate level.
    - Under `Access Controls` select `Grant` then in the right pane click `Grant access` then select `Require password change`.
7. Click `Select`
8. You may opt to begin in a state of `Report Only` as you step through implementation however, the policy will need to be set to `On` to be in effect.
9. Click `Create`.

NOTE: for more information regarding risk levels refer to Microsoft's Identity Protection & Risk Doc

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback
2. https://docs.microsoft.com/en-us/azure/active-directory/identity-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 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 Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

1.1.10 (L2) Use Just In Time privileged access to Office 365 roles (Manual)

Profile Applicability:

- E5 Level 2

Description:

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

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 Azure AD and Office 365. Organizations can give users just-in-time (JIT) privileged access to roles. There is a need for oversight for what those users are doing with their administrator privileges. PIM helps to mitigate the risk of excessive, unnecessary, or misused access rights.

Impact:

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.

Audit:

To verify if Privileged Identity Management is being used for Role activation, use the following steps:

1. Sign-on to your Azure portal as global administrator by going to `https://portal.azure.com`
2. In the Azure portal, click `Services` and search for and click on `Azure AD Privileged Identity management`.
3. Under `Manage` click on `Azure AD Roles`.
4. Under `Manage` click on `Roles`.
5. Inspect the following sensitive roles to ensure that the members are `Eligible` and not `Permanent`:

```
Application Administrator
Authentication Administrator
Billing Administrator
Cloud Application Administrator
Cloud Device Administrator
Compliance Administrator
Customer LockBox Access Approver
Device Administrators
Exchange Administrators
Global Administrators
HelpDesk Administrator
Information Protection Administrator
Intune Service Administrator
Kaizala Administrator
License Administrator
Password Administrator
PowerBI Service Administrator
Privileged Authentication Administrator
Privileged Role Administrator
Security Administrator
SharePoint Service Administrator
Skype for Business Administrator
Teams Service Administrator
User Administrator
```

Remediation:

To configure sensitive Azure AD roles for Privileged Identity Management Role activation, use the following steps:

1. Sign-on to your Azure portal as global administrator by going to `https://portal.azure.com`
2. In the Azure portal, click `Services` and search for and click on `Azure AD Privileged Identity management`.
3. Under `Manage` click on `Azure AD Roles`.
4. Under `Manage` click on `Roles`.
5. Inspect the following sensitive roles. For each of the members that have an `ASSIGNMENT TYPE` of `Permanent`, click on the `...` and choose `Make eligible`:

```
Application Administrator
Authentication Administrator
Billing Administrator
Cloud Application Administrator
Cloud Device Administrator
Compliance Administrator
Customer LockBox Access Approver
Device Administrators
Exchange Administrators
Global Administrators
HelpDesk Administrator
Information Protection Administrator
Intune Service Administrator
Kaizala Administrator
License Administrator
Password Administrator
PowerBI Service Administrator
Privileged Authentication Administrator
Privileged Role Administrator
Security Administrator
SharePoint Service Administrator
Skype for Business Administrator
Teams Service Administrator
User Administrator
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process 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 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 Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.1.11 (L1) Ensure Security Defaults is disabled on Azure Active Directory (Manual)

Profile Applicability:

- E3 Level 1

Description:

Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks.

Microsoft is making security defaults available to everyone. The goal is to ensure that all organizations have a basic level of security-enabled at no extra cost. You turn on security defaults in the Azure portal.

The use of security defaults however will prohibit custom settings which are being set with more advanced settings from this benchmark.

Rationale:

Security defaults provide secure default settings that we manage on behalf of organizations to keep customers safe until they are ready to manage their own identity security settings.

For example doing the following:

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

Impact:

The potential impact associated with disabling of Security Defaults is dependent upon the security controls implemented in the environment. It is likely that most organizations disabling Security Defaults plan to implement equivalent controls to replace Security Defaults.

It may be necessary to check settings in other Microsoft products, such as Azure, to ensure settings and functionality are as expected when disabling security defaults for MS365.

Audit:

To ensure security defaults is disabled in your directory:

1. Sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.
2. Browse to Azure Active Directory > Properties.
3. Select `Manage security defaults`.
4. Verify the Enable security defaults toggle to `No`.

Remediation:

To disable security defaults in your directory:

1. Sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.
2. Browse to Azure Active Directory > Properties.
3. Select `Manage security defaults`.
4. Set the Enable security defaults toggle to `No`.
5. Select Save.

References:

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

1.1.12 (L2) Ensure that only organizationally managed/approved public groups exist (Manual)

Profile Applicability:

- E3 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. While there are several different types of group types this recommendation is concerned with **Microsoft 365 Groups**.

In the Administration panel, when a group is created, the default privacy value is "Public".

Rationale:

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

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

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

NOTE: Public in this case meaning public to the identities within organization.

Impact:

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

Audit:

Using the Microsoft 365 Administration portal:
In the Microsoft 365 Administration portal, go to:

1. Teams & groups
2. Active teams & groups
3. Check that no groups have the status 'Public' in the privacy column

Using the Microsoft.Graph PowerShell module:
To get the list of public groups, run the following.

```
Connect-Graph -Scopes "Group.Read.All"
Get-MgGroup | where {$_.Visibility -eq "Public"} | select
DisplayName,Visibility
```

Remediation:

In the Microsoft 365 Administration portal, go to:

1. Teams & groups
2. Active teams & groups
3. Select a Public group
4. Go to 'Settings'
5. Set Privacy to 'Private'

Default Value:

Public when create from the Administration portal; private otherwise.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-self-service-management#self-service-group-membership-defaults
2. https://docs.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 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 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.	●	●	●

1.1.13 (L2) Ensure that collaboration invitations are sent to allowed domains only (Manual)

Profile Applicability:

- E3 Level 2

Description:

Users should be able to send collaboration invitations to allowed domains only.

Rationale:

By specifying allowed domains for collaborations, external users companies are explicitly identified. Also, this prevents internal users from inviting unknown external users such as personal accounts and give them access to resources.

Impact:

This could make harder collaboration if the setting is not quickly updated when a new domain is identified as "allowed".

Audit:

From the Azure portal:

1. Go to Azure Active Directory
2. Go to `Users`
3. Go to `User settings`
4. Under `External users`, click on `Manage external collaboration settings`
5. Under `Collaboration restrictions`, make sure that `Allow invitations only to the specified domains (most restrictive)` is selected. Then make sure that `Target domains` is checked and that allowed domains are specified.

Remediation:

From the Azure portal:

1. Go to Azure Active Directory
2. Go to `Users`
3. Go to `User settings`
4. Under `External users`, click on `Manage external collaboration settings`
5. Under `Collaboration restrictions`, select `Allow invitations only to the specified domains (most restrictive)`, check the `Target domains` setting, and specify the domains allowed to collaborate.

Default Value:

Default value is `Allow invitations to be sent to any domain (most inclusive)` and thus no domain is specified.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/external-identities/allow-deny-list

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process 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 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.	●	●	●

1.1.14 (L2) Ensure that LinkedIn contact synchronization is disabled. (Manual)

Profile Applicability:

- E3 Level 2

Description:

You should disable integration with LinkedIn as a measure to help prevent phishing scams.

Rationale:

Office 365 is the prime target of phishing scams. Phishing attacks are a subset of social engineering strategy that imitate a trusted source and concoct a seemingly logical scenario for handing over sensitive information. Social networking sites have made social engineering attacks easier to conduct.

LinkedIn integration is enabled by default in Office 365 that could lead to a risk scenario where an external party could be accidentally disclosed sensitive information.

Impact:

Users will not be able to sync contacts or use LinkedIn integration.

Audit:

To verify that LinkedIn contacts synchronization is disabled, perform the following steps via the Azure Active Directory admin center:

1. Navigate to `https://admin.microsoft.com` and login as a Global Admin.
2. Expand `Admin centers` then select `Azure Active Directory`.
3. Once the Azure AD Admin center is open select `Users` followed by `User Settings` then `User settings`.
4. Under `LinkedIn account connections` ensure `No` is highlighted.

Remediation:

To disabled LinkedIn account data sharing, perform the following steps via the Azure Active Directory admin center:

1. Navigate to `https://admin.microsoft.com` and login as a Global Admin.
2. Expand `Admin centers` then select `Azure Active Directory`.
3. Once the Azure AD Admin center is open select `Users` followed by `User Settings` then `User settings`.
4. Under `LinkedIn account connections` then click `No`.
5. Click `Save` at the top of the page.

Default Value:

LinkedIn integration is enabled by default.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/linkedin-integration

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software 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 Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

1.1.15 (L1) Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users. (Manual)

Profile Applicability:

- E3 Level 1

Description:

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.

Administrative roles this should apply to include those such as.

- Global Administrator
- Billing Administrator
- Exchange Administrator
- SharePoint Administrator
- Password Administrator
- Skype for Business Administrator
- Service Support Administrator
- User Administrator
- Dynamics 365 Service Administrator
- Power BI Administrator

NOTE: The frequency at which MFA is prompted will be determined by your organization's policy and need.

Rationale:

Ensuring these additional controls are present for Administrative users adds an additional layer of defense against drive-by attacks and even some ransomware attacks.

Impact:

Users with Administrative roles will be prompted at the frequency set for MFA.

Audit:

To verify the multifactor timeout and persistent browser settings are set for administrators, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Enterprise applications` then, under `Security`, select `Conditional Access`.
4. Review the list of policies and ensure that there is a policy that have `Sign-in frequency` set to the time determined by your organization and that `Persistent browser session` is set to `Never persistent`.

Remediation:

To enable the multifactor timeout and persistent browser settings are set for administrators, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Enterprise applications` then, under `Security`, select `Conditional Access`.
4. Click `New policy`
5. Go to `Assignments` > `Users and groups` > `Include` > `Select users and groups` > check `Directory roles`.
6. At a minimum, select the following roles: `Billing admin`, `Conditional Access admin`, `Exchange admin`, `Global admin`, `Helpdesk admin`, `Security admin`, `SharePoint admin`, and `User admin`.

- Targeting any role with the word `admin` will ensure that any users with additional privileges will be targeted.

7. Go to `Cloud apps or actions` > `Cloud apps` > `Include` > select `All cloud apps (and don't exclude any apps)`.
8. Under `Access controls` > `Grant` > select `Grant access` > check `Require multi-factor authentication` (and nothing else).
9. Under `Session` check `Sign-in frequency` and enter the value determined by your organization.
10. Check `Persistent browser session` then select `Never persistent` in the drop-down menu.
11. Create.

NOTE: After creation ensure that the policy is set to enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets 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 Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

1.1.16 (L2) Ensure the option to remain signed in is hidden (Manual)

Profile Applicability:

- E3 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. Typically this lasts for 90 days and does not prompt for sign-in or Multi-Factor.

Rationale:

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

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 verify the option to remain signed in is disabled, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`, once in the AD Admin Center select `Azure Active Directory`.
3. Under `Manage` select `Company branding` followed by the appropriate Locale policy.

- If you only see `Configure` then no locale or policy exists and this setting is not applied, proceed to remediation.

4. Scroll to the bottom of the newly opened pane and ensure `Show option to remain signed in` is not checked.

Remediation:

To verify the option to remain signed in is disabled, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`, once in the AD Admin Center select `Azure Active Directory`.
3. Under `Manage` select `Company branding` followed by the appropriate Locale policy.

- If no policy exists you will need to click `Configure` to create one

4. Scroll to the bottom of the newly opened pane and ensure `Show option to remain signed in` is not checked.
5. Click `Save`.

Default Value:

Users may select `stay signed in`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

1.2 (L1) Ensure modern authentication for Exchange Online is enabled (Automated)

Profile Applicability:

- E3 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 verify modern authentication is enabled, use the Exchange Online PowerShell Module:

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 enable modern authentication, use the Exchange Online PowerShell Module:

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://support.office.com/en-gb/article/enable-or-disable-modern-authentication-in-exchange-online-58018196-f918-49cd-8238-56f57f38d662

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit 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 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 Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

1.3 (L1) Ensure modern authentication for SharePoint applications is required (Automated)

Profile Applicability:

- E3 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.

Audit:

To verify SharePoint settings, use the Microsoft 365 Admin Center:

1. Under `Admin centers` select `SharePoint`.
2. Expand the `Policies` section then select `Access control`.
3. Select `Apps that don't use modern authentication` and ensure that it is set to `Block access`.

To verify Apps that don't use modern authentication is set to Block, use the SharePoint Online PowerShell Module:

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. Verify `LegacyAuthProtocolsEnabled` is set False

Remediation:

To set SharePoint settings, use the Microsoft 365 Admin Center:

1. Under `Admin centers` select `SharePoint`.
2. Expand the `Policies` section then select `Access control`.
3. Select `Apps that don't use modern authentication`
4. Select the radio button for `Block access`.
5. Click `Save`.

To set Apps that don't use modern authentication is set to Block, use the SharePoint Online PowerShell Module:

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:

The default is to allow apps that don't use modern authentication.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit 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 Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

1.4 (L1) Ensure that Office 365 Passwords Are Not Set to Expire (Automated)

Profile Applicability:

- E3 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 not 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 Azure AD.

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
- Enforce Multi-Factor Authentication registration

Audit:

To verify Office 365 Passwords Are Not Set to Expire, use the Microsoft 365 Admin Center:

1. Expand `Settings` then select the `Org Settings` subcategory.
2. Click on `Security & privacy`.
3. Select `Password expiration policy` ensure that `Set passwords to never expire (recommended)` has been checked.

To verify Office 365 Passwords Are Not Set to Expire, use the Microsoft Online PowerShell Module:

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

```
Get-MsolPasswordPolicy -DomainName <DomainName> | ft ValidityPeriod
```

Remediation:

To set Office 365 Passwords to Expire, use the Microsoft 365 Admin Center:

1. Expand `Settings` then select the `Org Settings` subcategory.
2. Click on `Security & privacy`.
3. Select `Password expiration policy`.
4. If the `Set passwords to never expire (recommended)` box is unchecked, check it.
5. Click `Save`.

To set Office 365 Passwords Are Not Set to Expire, use the Microsoft Online PowerShell Module:

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

```
Set-MsolPasswordPolicy -ValidityPeriod 2147483647 -DomainName <DomainName> -
NotificationDays 30
```

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://docs.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 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 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.		●	●

1.5 (L1) Ensure Administrative accounts are separate and cloud-only (Manual)

Profile Applicability:

- E3 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 separated from on-prem accounts. Administrative accounts should not have applications assigned so that they have no access to potentially vulnerable services (EX. email, Teams, SharePoint, etc.) and only access to perform tasks as needed for Administrative purposes.

Rationale:

Ensuring administrative accounts are cloud-only, without applications assigned to them will reduce the attack surface of high privileged identities in your environment. In order to participate in Microsoft 365 security services such as Identity Protection, PIM and Conditional Access an administrative account will need a license attached to it. Ensure that the license used does not include any applications with potentially vulnerable services by using either **Azure Premium P1** or **Azure Premium P2** for the cloud-only account with administrator roles.

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

Impact:

Administrative users will have to switch accounts and utilizing login/logout functionality when performing Administrative tasks, as well as not benefiting from SSO.

Audit:

To verify appropriately licensed, separate Administrative accounts are being utilized, use the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Select `Users` > `Active users` then sort by the `Licenses` column.
3. For each user account in an administrative role verify the following:
    - The account is Cloud only (not synced)
    - The account is assigned a license that is not associated with applications (Azure Premium P1, Azure Premium P2)

Remediation:

To created licensed, separate Administrative accounts for Administrative users, using the Microsoft 365 Admin Center:

1. Log in to `https://admin.microsoft.com` as a `Global Administrator`.
2. Go to `Admin centers` and click on `Azure Active Directory`.
3. Select `Users` > `Active users` then click `Add a user`.
4. Fill out the appropriate fields for Name, user, etc.
5. When prompted to assign licenses select as needed `Azure Premium P1` or `Azure Premium P2`, then click `Next`.
6. Under the `Option settings` screen you may choose from several types of Administrative access roles. Choose `Admin center access` followed by the appropriate role then click `Next`.
7. Select `Finish adding`.

Default Value:

N/A

References:

1. https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/add-users?view=o365-worldwide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts 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 Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

2 Application Permissions

2.1 (L2) Ensure third party integrated applications are not allowed (Manual)

Profile Applicability:

- E3 Level 2

Description:

Do not allow third party integrated applications to connect to your services.

Rationale:

You should not allow third party integrated applications to connect to your services unless there is a very clear value and you have robust security controls 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:

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 necessary third-party applications.

Audit:

To verify that third party integrated applications are not allowed, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Azure Active Directory`.
2. Select `Users` from the Azure navigation pane
3. Select `Users settings`.
4. Verify `App registrations` is set to `No`.

Remediation:

To prohibit third party integrated applications, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Azure Active Directory`.
2. Select `Users` from the Azure navigation pane
3. Select `Users settings`.
4. Set `App registrations` is set to `No`.
5. Click Save.

Default Value:

Yes

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software 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 Only use up-to-date and trusted third-party components for the software developed by the organization.		●	●

2.2 (L2) Ensure calendar details sharing with external users is disabled (Automated)

Profile Applicability:

- E3 Level 2

Description:

You should not allow your users to share the full details of their calendars with external users.

Rationale:

Attackers often spend time learning about your organization 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 verify calendar details sharing with external users is disabled, use the Microsoft 365 Admin Center:

1. Select `Admin Center` and Click to expand `Settings`.
2. Click `Org settings`.
3. 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 verify calendar details sharing with external users is disabled, use the Exchange Online PowerShell Module:

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

```
Get-SharingPolicy | Where-Object { $_.Domains -like '*CalendarSharing*' }
```

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

Remediation:

To disable calendar details sharing with external users, use the Microsoft 365 Admin Center:

1. Select `Admin Center` and Click to expand `Settings`.
2. Click `Org settings`.
3. 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 disable calendar details sharing with external users policy, use the Exchange Online PowerShell Module:

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

```
Set-SharingPolicy -Identity "Name of the policy" -Enabled $False
```

Default Value:

On

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software 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 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.	●	●	●

2.3 (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 Build-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 verify Defender for Office Safe Links policy for Office is enabled, use the Microsoft 365 Admin Center:

1. Under `Admin centers` click `Security`.
2. Under `Email & collaboration` select `Policies & rules`
3. Select `Threat policies` then `Safe Links`
4. Click on the policy, a new pane should open on the right hand side.
5. Scroll down the pane and click on `Edit Protection settings`
6. Ensure the following boxes are checked in the section `URL & Click protection settings`:

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

7. Under `Click protection settings` the setting `Let users click through to the original URL` should be unchecked.

To verify the Safe Links policy is enabled, use the Exchange Online PowerShell Module:

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

```
Get-SafeLinksPolicy | Format-Table Name
```

3. Once this returns the list of policies run the following command to view the policies.

```
Get-SafeLinksPolicy -Identity "Policy Name"
```

4. Verify the value for the following.
    - `EnableSafeLinksForEmail: True`
    - `EnableSafeLinksForTeams: True`
    - `EnableSafeLinksForOffice: True`
    - `AllowClickThrough: False`
    - `ScanUrls: True`
    - `EnableForInternalSenders: True`
    - `DeliverMessageAfterScan: True`

Remediation:

To enable Defender for Office Safe Links policy for Office, use the Microsoft 365 Admin Center:

1. Under `Admin centers` click `Security`.
2. Under `Email & collaboration` select `Policies & rules`
3. Select `Threat policies` then `Safe Links`
4. Click on the policy, a new pane should open on the right hand side.
5. Under `Protection settings` click `Edit protection settings`
6. Ensure the follow boxes are checked:

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

7. Under `Click protection settings` check `Track user clicks` and **uncheck** `Let users click through to the original URL`
8. Select `Save`

To enable the Safe Links policy for Office 365, use the Exchange Online PowerShell Module:

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

```
New-SafeLinksPolicy -Name "My SafeLinks Policy" -EnableSafeLinksForEmail
$true -EnableSafeLinksForTeams $true -EnableSafeLinksForOffice $true -
ScanUrls $true -DeliverMessageAfterScan $true -EnableForInternalSenders $true
-AllowClickThrough $false
```

References:

1. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-safe-links-policies?view=o365-worldwide
2. https://docs.microsoft.com/en-us/powershell/module/exchange/set-safelinkspolicy?view=exchange-ps
3. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/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 Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters 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.		●	●

2.4 (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 protects your organization 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 verify that Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is enabled, use the Microsoft 365 Admin Center:

1. Under `Admin centers` click `Security` to open the `Microsoft 365 Defender`.
2. Under `Email & collaboration` select `Policies & rules`
3. Select Threat policies then `Safe Attachments`.
4. Click on `Global settings`
5. Verify that toggle is selected to `Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams`.

To verify that Safe Attachments is enabled for SharePoint, OneDrive, and Microsoft Teams, use the Exchange Online PowerShell Module:

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

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

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

Remediation:

To enable Safe Attachments for SharePoint, OneDrive, and Microsoft Teams, use the Microsoft 365 Admin Center:

1. Under `Admin centers` click `Security` to open the `Microsoft 365 Defender`.
2. Under `Email & collaboration` select `Policies & rules`
3. Click on `Global settings`
4. Click the toggle to `Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams`
5. Click `Save`

To enable Safe Attachments for SharePoint, OneDrive, and Microsoft Teams, use the Exchange Online PowerShell Module:

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

```
Set-AtpPolicyForO365 -EnableATPForSPOTeamsODB $True
```

CIS Controls:

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

2.5 (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 check that O365 SharePoint is set to not allow infected files to be downloaded, use PowerShell:

1. Connect using `Connect-SPOService`, you will need to enter the URL for your SharePoint Online admin page `https://*-admin.sharepoint.com` as well as a Global Admin account.
2. Run the following PowerShell command

```
Get-SPOTenant | Select-Object DisallowInfectedFileDownload
```

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

Remediation:

To set O365 SharePoint to disallow download of infected files, use PowerShell:

1. Connect using `Connect-SPOService`, you will need to enter the URL for your Sharepoint Online admin page `https://*-admin.sharepoint.com` as well as a Global Admin account.
2. Run the following PowerShell command to set the value to `True`.

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

3. After several minutes run the following to verify the value for `DisallowInfectedFileDownload` has been set to `True`.

```
Get-SPOTenant | Select-Object DisallowInfectedFileDownload
```

References:

1. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/turn-on-mdo-for-spo-odb-and-teams?view=o365-worldwide
2. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/virus-detection-in-spo?view=o365-worldwide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	7.10 Sandbox All Email Attachments Use sandboxing to analyze and block inbound email attachments with malicious behavior.			●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

2.6 (L2) Ensure user consent to apps accessing company data on their behalf is not allowed (Automated)

Profile Applicability:

- E3 Level 2

Description:

By default, users can consent to applications accessing your organization's data, although only for some permissions. For example, by default a user can consent to allow an app to access their own mailbox or the Teams conversations for a team the user owns, but cannot consent to allow an app unattended access to read and write to all SharePoint sites in your organization.

Do not allow users to grant consent to apps accessing company data on their behalf.

Rationale:

Attackers commonly use custom applications to trick users into granting them access to company data.

While allowing users to consent by themselves does allow users to easily acquire useful applications that integrate with Microsoft 365, Azure and other services, it can represent a risk if not used and monitored carefully.

Disable future user consent operations to help reduce your threat-surface and mitigate this risk. If user consent is disabled, previous consent grants will still be honored but all future consent operations must be performed by an administrator.

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 verify that user consent to apps accessing company data on their behalf is not allowed, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Azure Active Directory`.
2. Select `Enterprise applications` from the Azure navigation pane.
3. Under `Security` select `Consent and permissions`.
4. Verify `User consent for applications` is set to `Do not allow user consent`.

To verify that user consent to apps accessing company data on their behalf is not allowed, use the Microsoft Online PowerShell Module:

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

```
Get-MsolCompanyInformation | Select-Object
UsersPermissionToUserConsentToAppEnabled
```

3. Verify the value for `UsersPermissionToUserConsentToAppEnabled` is set to `False`.

Remediation:

To prohibit user consent to apps accessing company data on their behalf, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Azure Active Directory`.
2. Select `Enterprise applications` from the Azure navigation pane.
3. Under `Security` select `Consent and permissions`.
4. Under `User consent for applications` select `Do not allow user consent`.
5. Click the `Save` option at the top of the window.

To prohibit user consent to apps accessing company data on their behalf, use the Microsoft Online PowerShell Module:

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

```
Set-MsolCompanySettings -UsersPermissionToUserConsentToAppEnabled $False
```

Default Value:

UI - `Allow user consent for apps` PowerShell - `True`

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists 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 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.	●	●	●

2.7 (L2) Ensure the admin consent workflow is enabled (Automated)

Profile Applicability:

- E3 Level 2

Description:

Without an admin consent workflow (Preview), a user in a tenant where user consent is disabled will be blocked when they try to access any app that requires permissions to access organizational data. The user sees a generic error message that says they're unauthorized to access the app and they should ask their admin for help.

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 verify the admin consent workflow (Preview) is enabled, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Azure Active Directory`.
2. Select `Enterprise applications` from the Azure Navigation pane.
3. Under `Manage` select `Users settings`.
4. Verify that `Users can request admin consent to apps they are unable to consent to` is set to `Yes`.

Remediation:

To enable the admin consent workflow (Preview), use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Azure Active Directory`.
2. Select `Enterprise applications` from the Azure Navigation pane.
3. Under `Manage` select `Users settings`.
4. Set `Users can request admin consent to apps they are unable to consent to` to `Yes` under `Admin consent requests`.
5. Under the `Reviewers` choose the Roles, Groups that you would like to review user generated app consent requests.
6. 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`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software 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 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.		●	●

2.8 (L2) - Ensure users installing Outlook add-ins is not allowed (Automated)

Profile Applicability:

- E3 Level 2

Description:

By default, users can install add-ins in their Microsoft Outlook Desktop client, allowing data access within the client application.

Do not allow users to install add-ins in Outlook.

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 Outlook 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 integrate third-party applications that they may wish to use. Administrators are likely to receive requests from end users to grant them permission to necessary third-party applications.

Audit:

To verify that users installing Outlook add-ins is not allowed, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Exchange`.
2. Click on the `Classic Exchange admin center` at the bottom.
3. Select `permissions` from the Exchange navigation pane.
4. Select `user roles`.
5. Double click `Default Role Assignment` to open it and verify `My Custom Apps` `My Marketplace Apps` and `My ReadWriteMailboxApps` are `Not Checked`.

To verify that users installing Outlook add-ins is not allowed, use the Microsoft Online PowerShell Module:

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

```
Get-EXOMailbox | Select-Object -Unique RoleAssignmentPolicy | ForEach-Object
{ Get-RoleAssignmentPolicy -Identity $_.RoleAssignmentPolicy | Where-Object
{$_.AssignedRoles -like "*Apps*"}} | Select-Object Identity,
@{Name="AssignedRoles"; Expression={Get-Mailbox | Select-Object -Unique
RoleAssignmentPolicy | ForEach-Object { Get-RoleAssignmentPolicy -Identity
$_.RoleAssignmentPolicy | Select-Object -ExpandProperty AssignedRoles |
Where-Object {$_ -like "*Apps*"}}}}
```

3. Verify `My Custom Apps` `My Marketplace Apps` and `My ReadWriteMailboxApps` are not present.

Remediation:

To prohibit users installing Outlook add-ins, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Exchange`.
2. Click on the `Classic Exchange admin center` at the bottom.
3. Select `permissions` from the Exchange navigation pane.
4. Select `user roles`.
5. Double click `Default Role Assignment` and deselect `My Custom Apps` `My Marketplace Apps` and `My ReadWriteMailboxApps`.

To prohibit users installing Outlook add-ins, use the Microsoft Online PowerShell Module:

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

```
$newPolicyName = "Role Assignment Policy - Prevent Add-ins"
$revisedRoles = "MyTeamMailboxes", "MyTextMessaging", "MyDistributionGroups",
"MyMailSubscriptions", "MyBaseOptions", "MyVoiceMail",
"MyProfileInformation", "MyContactInformation", "MyRetentionPolicies",
"MyDistributionGroupMembership"

New-RoleAssignmentPolicy -Name $newPolicyName -Roles $revisedRoles
Set-RoleAssignmentPolicy -id $newPolicyName -IsDefault
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -RoleAssignmentPolicy
$newPolicyName
```

If you have other Role Assignment Policies modify the last line to filter out your custom policies

Default Value:

UI - `My Custom Apps` is `Checked`, `My Marketplace Apps` is `Checked`, and `My ReadWriteMailboxApps` is `Checked`

PowerShell - `My Custom Apps` `My Marketplace Apps` and `My ReadWriteMailboxApps` are `Present`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions 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 Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.9 (L1) - Ensure users installing Word, Excel, and PowerPoint add-ins is not allowed (Manual)

Profile Applicability:

- E3 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 verify that users installing Word, Excel, and PowerPoint add-ins is not allowed, use the Microsoft 365 Admin Center:

1. Select `Settings` from the navigation pane.
2. Select `Org settings` from the navigation pane.
3. Under `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`.

Remediation:

To prohibit users installing Word, Excel, and PowerPoint add-ins, use the Microsoft 365 Admin Center:

1. Select `Settings` from the navigation pane.
2. Select `Org Settings` from the navigation pane.
3. Under `Services` select `User owned apps and services`.
4. De-Select `Let users access the Office Store` and `Let users start trials on behalf of your organization`.
5. Click `Save`.

Default Value:

`Let users access the Office Store` is `Checked`

`Let users start trials on behalf of your organization` is `Checked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software 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 Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.10 (L1) Ensure internal phishing protection for Forms is enabled (Manual)

Profile Applicability:

- E3 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 verify Microsoft Forms settings use the Microsoft 365 Admin Center:

1. Expand `Settings` then select `Org settings`.
2. Under Services select `Microsoft Forms`.
3. Ensure the checkbox labeled `Add internal phishing protection` is checked under `Phishing protection`.

Remediation:

To set Microsoft Forms settings use the Microsoft 365 Admin Center:

1. Expand `Settings` then select `Org settings`.
2. Under Services select `Microsoft Forms`.
3. Select the checkbox for `Add internal phishing protection` under `Phishing protection`.
4. Click Save.

Default Value:

Internal Phishing Protection enabled.

References:

1. https://support.microsoft.com/en-us/office/administrator-settings-for-microsoft-forms-48161c55-fbae-4f37-8951-9e3befc0248b
2. https://support.microsoft.com/en-us/office/review-and-unblock-forms-or-users-detected-and-blocked-for-potential-phishing-879a90d7-6ef9-4145-933a-fb53a430bced

CIS Controls:

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

2.11 (L1) Ensure that Sways cannot be shared with people outside of your organization (Manual)

Profile Applicability:

- E3 Level 1

Description:

Disable external sharing of Sway items such as reports, newsletters, presentations etc that could contain sensitive information.

Rationale:

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

Impact:

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

Audit:

To verify Sways cannot be viewed outside of your organization use the Microsoft 365 Admin Center:

1. Expand `Settings` then select `Org settings`.
2. Under Services select `Sway`.
3. Confirm that under `Sharing` the following are not checked

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

Remediation:

To ensure Sways cannot be viewed outside of your organization use the Microsoft 365 Admin Center:

1. Expand `Settings` then select `Org settings`.
2. Under Services select `Sway`.
3. Under `Sharing` uncheck the following

- `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#:~:text=Navigate%20to%20Settings%20%3E%20Settings.,options%2C%20uncheck%20the%20check%20boxes.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software 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 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.	●	●	●

3 Data Management

3.1 (L2) Ensure the customer lockbox feature is enabled (Automated)

Profile Applicability:

- E5 Level 2

Description:

You should enable the Customer Lockbox feature. It requires Microsoft to get your approval for any datacenter operation that grants a Microsoft support engineer or other employee direct access to any of your data. For example, in some cases a Microsoft support engineer might need access to your Microsoft 365 content in order to help troubleshoot and fix an issue for you. Customer lockbox requests also have an expiration time, and content access is removed after the support engineer has fixed the issue.

Rationale:

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

Impact:

The impact associated with this setting is a requirement to grant Microsoft access to the tenant environment prior to a Microsoft engineer accessing the environment for support or troubleshooting.

Audit:

To verify the Customer Lockbox feature is enabled, use the Microsoft 365 Admin Portal:

1. Browse to the `Microsoft 365 admin center`.
2. Expand `Settings` then select `Org settings`
3. Choose `Security & privacy` in the right pane.
4. Click `Customer lockbox`.
5. Ensure the box labeled `Require approval for all data access requests` is checked.

To verify the Customer Lockbox feature is enabled, use the Microsoft 365 SecureScore Portal:

1. Log in to the Microsoft 365 SecureScore portal (https://securescore.microsoft.com) using admin permissions (global admin or a custom admin role) for an Office 365 Enterprise, Microsoft 365 Business, or Office 365 Business Premium subscription.
2. Search for `Turn on customer lockbox feature` under `Improvement actions`

To verify the Customer Lockbox feature is enabled, use the REST API:

```
GET https://graph.microsoft.com/beta/security/secureScores
```

To verify the Customer Lockbox feature is enabled, use the Exchange Online PowerShell Module:

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

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

4. Verify the value is set to `True`

Remediation:

To enable the Customer Lockbox feature, use the Microsoft 365 Admin Portal:

1. Browse to the `Microsoft 365 admin center`.
2. Expand `Settings` then select `Org settings`
3. Choose `Security & privacy` in the right pane.
4. Click `Customer Lockbox`.
5. Check the box `Require approval for all data access requests`.
6. Click `Save`.

To set the Customer Lockbox feature to enabled, use the Exchange Online PowerShell Module:

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

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

Default Value:

Disabled

3.2 (L2) Ensure SharePoint Online Information Protection policies are set up and used (Manual)

Profile Applicability:

- E3 Level 2

Description:

You should set up and use SharePoint Online data classification policies on data stored in your SharePoint Online sites.

Rationale:

The policies will help categorize your most important data so you can effectively protect it from illicit access, and will help make it easier to investigate discovered breaches.

Impact:

Creation of data classification policies will not cause a significant impact to an organization. However, ensuring long term adherence with policies can potentially be a significant training and ongoing compliance effort across an organization. Organizations should ensure that training and compliance planning is part of the classification policy creation process.

Audit:

To verify data classification policies are set up, use the Microsoft 365 Admin Center:

1. Under `Admin centers` select `Compliance` to open the `Microsoft Purview compliance portal`.
2. Under `Solutions` click `Information protection`
3. Ensure Labels exist.
4. Click on the `Label policies` tab
5. Ensure that a Label policy exists and is published accordingly.

Remediation:

To set up data classification policies, use the Microsoft 365 Admin Center:

1. Under `Admin centers` select `Compliance` to open the `Microsoft Purview compliance portal`.
2. Under `Solutions` click `Information protection`
3. Select `Labels` tab
4. Click `Create a label` to create a label.
5. Select the label and click on the `Publish label`
6. Fill out the forms to create the policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.7 Establish and Maintain a Data Classification Scheme 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 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 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.	●	●	●

3.3 (L2) Ensure external domains are not allowed in Skype or Teams (Manual)

Profile Applicability:

- E3 Level 2

Description:

As of December 2021 the default for Teams external communication is set to 'People in my organization can communicate with Teams users whose accounts aren't managed by an organization.' This means that users can communicate with personal Microsoft accounts (e.g. Hotmail, Outlook etc.), which presents data loss / phishing / social engineering risks.

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 reference for more information.

Rationale:

You should not allow your users to communicate with Skype or Teams users outside your organization. While there are legitimate, productivity-improving scenarios for this, it also represents a potential security threat because those external users will be able to interact with your users over Skype for Business or Teams. Users are prone to data loss / phishing / social engineering attacks via Teams.

Impact:

Impact associated with this change is highly dependent upon current practices in the tenant. If users do not regularly communicate with external parties using Skype or Teams channels, then minimal impact is likely. However, if users do regularly utilize Teams and Skype for client communication, potentially significant impacts could occur, and users should be contacts, and if necessary, alternate mechanisms to continue this communication should be identified prior to disabling external access to Teams and Skype.

Audit:

To review user communication with external Teams organizations, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` select `Teams`.
2. Under `Users` select `External access`
3. Under `Teams and Skype for Business users in external organizations` ensure that `Block all external domains`
    - **Note:** If organizational policy allows select any allowed external domains.
4. Under `Teams accounts not managed by an organization` ensure the slider is set to `Off`.
5. Under `Skype users` ensure the slider is set to `Off`.

Remediation:

To prohibit user communication with external Teams organizations, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `Teams`.
2. Under `Users` select `External access`
3. Under `Teams and Skype for Business users in external organizations` Select `Block all external domains`
    - **Note:** If organizational policy allows select any allowed external domains.
4. Under `Teams accounts not managed by an organization` move the slider to `Off`.
5. Under `Skype users` move the slider is to `Off`.
6. Click `Save`.

Default Value:

On

References:

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

3.4 (L1) Ensure DLP policies are enabled (Automated)

Profile Applicability:

- E3 Level 1

Description:

Enabling Data Loss Prevention (DLP) policies allows 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 in regards to testing and implementation of DLP policies based on your organizational standards.

Audit:

To verify DLP policies are enabled, use the Microsoft 365 Admin Center:

1. Under `Admin centers` Select `Compliance` to open `Microsoft Purview`.
2. Under `Solutions` select `Data loss prevention` then `Policies`.

- Alternatively you may visit `https://compliance.microsoft.com/datalossprevention`

3. Verify that policies exist and are enabled

Remediation:

To enable DLP policies, use the Microsoft 365 Admin Center:

1. Under `Admin centers` Select `Compliance` to open `Microsoft Purview`
2. Under `Solutions` select `Data loss prevention` then `Policies`.
3. Click `Create policy`.

References:

1. https://docs.microsoft.com/en-us/microsoft-365/compliance/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 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 Data Protection			
v7	14.7 Enforce Access Control to Data through Automated Tools 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.			●

3.5 (L1) Ensure DLP policies are enabled for Microsoft Teams (Manual)

Profile Applicability:

- E5 Level 1

Description:

Enabling Data Loss Prevention (DLP) policies for Microsoft Teams, blocks sensitive content when shared in teams or channels. 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 Teams channels or chat messages to be detected or blocked.

Audit:

To verify DLP policies are enabled, use the Microsoft 365 Admin Center:

1. Select `Compliance` under `Admin centers` to open `Microsoft Purview compliance portal`.
2. Under `Solutions` select `Data loss prevention`
3. Click `Policies`.
4. Verify that policies exist and are enabled
5. Ensure that under `Locations to apply the policy` the policies include `Teams chat and channel messages`

To verify DLP for Microsoft Teams is enabled for all users, use the Exchange Online / Compliance PowerShell Module:

1. Run Exchange Online PowerShell Module.
2. Connect using `Connect-ExchangeOnline`, then run the following

```
Import-Module ExchangeOnlineManagement
```

3. Then connect to the Security and Compliance Center via the following `Connect-IPPSSession`
4. Run the following PowerShell command to see what DLP Policies are created:

```
Get-DlpCompliancePolicy
```

5. Next you will run the following to look at the policy details to ensure the required users are included `TeamsLocation` and that no undesired users are excluded `TeamsLocationException`

```
Get-DlpCompliancePolicy -Identity "POLICYNAME FROM ABOVE" | Select-Object
TeamsLocation*
```

Remediation:

To enable DLP policies, use the Microsoft 365 Admin Center:

1. Select `Compliance` under `Admin centers` to open `Microsoft 365 Purview compliance portal`.
2. Under `Solutions` select `Data loss prevention`
3. Click `Policies`.
4. Click `Create policy`.
5. Either start with a template or create a custom policy.
6. Provide a `Name` for your policy
7. At the `Choose locations` step, either choose `Protect content in Exchange email, Teams chats and channel messages and OneDrive and SharePoint documents` or select `Let me choose specific locations`. If you select `Let me choose specific locations`, ensure that `Teams chat and channel messages` is selected.
8. Ensure that the proper DLP rules are created for the type of content to be detected and what actions should be taken.

Default Value:

This is not enabled by default.

References:

1. https://docs.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process 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 Data Protection			
v7	14.7 Enforce Access Control to Data through Automated Tools 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.			●

3.6 (L2) Ensure that external users cannot share files, folders, and sites they do not own (Automated)

Profile Applicability:

- E3 Level 2

Description:

SharePoint gives users the ability to share files, folder, and site collections. Internal users can share with external collaborators, who with the right permissions, could share those to another external party.

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:

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 verify SharePoint sharing settings, use the Microsoft 365 Admin Center:

1. Under `Admin centers` select `SharePoint`.
2. 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 verify Prevent external users from sharing files, folders, and sites that they don’t own, use the SharePoint Online PowerShell Module:

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

```
Get-SPOTenant | ft PreventExternalUsersFromResharing
```

3. Verify `PreventExternalUsersFromResharing` is set True

Remediation:

To set SharePoint sharing settings, use the Microsoft 365 Admin Center:

1. Under `Admin centers` select `SharePoint`.
2. 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 Set Prevent external users from sharing files, folders, and sites that they don't own, use the SharePoint Online PowerShell Module:

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

```
Set-SPOTenant -PreventExternalUsersFromResharing $True
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists 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 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.	●	●	●

3.7 (L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services (Manual)

Profile Applicability:

- E3 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 the link in the reference 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:

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 verify external file sharing in Teams, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` choose `Teams`.
2. Expand `Teams` select `Teams settings`.
3. Under `Files` verify that only authorized cloud storage options are set `On`.

** To verify external file sharing in Teams you may also utilize PowerShell. Ensure that the Skype for business online, Windows PowerShell module and Microsoft Teams module are both installed. **

1. Connect to Microsoft Teams using Connect-MicrosoftTeams
2. Run the following command to verify which cloud storage providers are enabled for Teams

```
Get-CsTeamsClientConfiguration | select allow*
```

3. Verify that only allowed authorized providers are set to 'True'.

Remediation:

To Set external file sharing in Teams, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` choose `Teams`.
2. Expand `Teams` select `Teams settings`.
3. Set each cloud storage service under `Files` to `On` if it is authorized.

** To verify external file sharing in Teams you may also utilize PowerShell. Ensure that the Skype for business online, Windows PowerShell module and Microsoft Teams module are both installed. **

1. Install the PowerShell module for teams. Skype module will need downloaded from Microsoft.

```
Install-Module MicrosoftTeams
Import-Module SkypeOnlineConnector
```

2. Connect to your tenant as a Global Administrator, methods will differ based on whether 2FA is enabled. See the following article for more information - https://docs.microsoft.com/en-us/office365/enterprise/powershell/manage-skype-for-business-online-with-office-365-powershell
3. Run the following command to verify which cloud storage providers are enabled for Teams

```
Get-CsTeamsClientConfiguration | select allow*
```

4. Run the following PowerShell command to disable external providers that are not authorized. (the example disables ShareFile, GoogleDrive, Box, and DropBox

```
Set-CsTeamsClientConfiguration -AllowGoogleDrive $false -AllowShareFile
$false -AllowBox $false -AllowDropBox $false -AllowEgnyte $false
```

5. You may verify this worked by running the following PowerShell command again.

```
Get-CsTeamsClientConfiguration | select allow*
```

Default Value:

On

References:

1. https://docs.microsoft.com/en-us/skypeforbusiness/set-up-skype-for-business-online/set-up-skype-for-business-online

Additional Information:

Skype Online Connector - https://www.microsoft.com/en-us/download/details.aspx?id=39366

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists 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 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.			●

4 Email Security / Exchange Online

4.1 (L1) Ensure the Common Attachment Types Filter is enabled (Automated)

Profile Applicability:

- E3 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 verify the Common Attachment Types Filter is enabled, use the Microsoft 365 Admin Portal:

1. Navigate to the Microsoft Admin Center and click `Security`.
2. Under `Email & collaboration` > `Policies & rules` > `Threat policies`.
3. Select `Anti-malware` and click on the highest priority policy.
4. In the Edit tab under `Protection settings`, verify that the `Enable the common attachments filter` has the value of 'On`

To verify the Common Attachment Types Filter is enabled, use the Exchange Online PowerShell Module:

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`.

Remediation:

To enable the Common Attachment Types Filter, use the Microsoft 365 Admin Portal:

1. Navigate to the Microsoft Admin Center and click `Security`.
2. Under `Email & collaboration` > `Policies & rules` > `Threat policies`.
3. Select `Anti-malware` and click on the highest priority policy.
4. In the Edit tab under at the bottom click on `Edit protection settings`, check the `Enable the common attachments filter`

To enable the Common Attachment Types Filter, use the Exchange Online PowerShell Module:

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

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

Default Value:

off

References:

1. https://docs.microsoft.com/en-us/powershell/module/exchange/antispam-antimalware/Get-MalwareFilterPolicy?view=exchange-ps
2. https://docs.microsoft.com/en-us/office365/SecurityCompliance/configure-anti-malware-policies#use-remote-powershell-to-configure-anti-malware-policies

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●
v7	7.9 Block Unnecessary File Types 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 Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

4.2 (L1) Ensure Exchange Online Spam Policies are set to notify administrators (Automated)

Profile Applicability:

- E3 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 your tenant 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.

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.

Impact:

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

Audit:

To verify the Exchange Online Spam Policies are set correctly, use the Microsoft 365 Admin Center:

1. Navigate to the Microsoft Admin Center and click `Security`
2. Under `Email & collaboration` > `Policies & rules` > `Threat policies` > `Anti-spam policies`
3. Click on the `Anti-spam outbound policy (default)`.
4. Verify that `Send a copy of outbound messages that exceed these limits to these users and groups` is set to `On`, ensure the email address is correct.
5. 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 verify the Exchange Online Spam Policies are set correctly, use the Exchange Online PowerShell Module:

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.

Remediation:

To set the Exchange Online Spam Policies correctly, use the Microsoft 365 Admin Center:

1. Navigate to the Microsoft Admin Center and click `Security`
2. Under `Email & collaboration` > `Policies & rules` > `Threat policies` > `Anti-spam policies`
3. Click on the `Anti-spam outbound policy (default)`.
4. Select `Edit protection settings` then under `Notifications`
5. Check `Send a copy of outbound messages that exceed these limits to these users and groups` then enter the desired email addresses.
6. Check `Notify these users and groups if a sender is blocked due to sending outbound spam` then enter the desired email addresses.
7. Click `Save`.

To set the Exchange Online Spam Policies correctly, use the Exchange Online PowerShell Module:

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
```

Default Value:

disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	17.5 Assign Key Roles and Responsibilities 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 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 Use sandboxing to analyze and block inbound email attachments with malicious behavior.			●

4.3 (L1) Ensure all forms of mail forwarding are blocked and/or disabled (Automated)

Profile Applicability:

- E3 Level 1

Description:

You should set your Exchange Online mail transport rules to not forward email to domains outside of your organization. Automatic forwarding to prevent users from auto-forwarding mail via Outlook or Outlook on the web should also be disabled. Alongside this Client Rules Forwarding Block, which prevents the use of any client-side rules that forward email to an external domain, should also be enabled.

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.

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 three step procedure as follows:*
STEP 1: Transport rules
To verify the mail transport rules do not forward email to external domains, use the Microsoft 365 Admin Center:

1. Select `Exchange`.
2. Select `Mail Flow` and `Rules`.
3. Review the rules and verify that none of them are forwards to external domains.

To verify that no rules are forwarding the email to external domains, you can also use the Exchange Online PowerShell module:

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 are going to external domains

STEP 2: Automatic forwarding
To verify automatic forwarding is disabled using the Microsoft 365 Admin Center:

1. Select `Exchange` under Admin centers
2. Under `Mail flow` select `Remote domains`
3. Click on the `default` policy.
4. Click `Edit reply types` in the pane on the right
5. Ensure `Allow automatic forwarding` is not checked.

To verify that automatic forwarding is disabled, you may use the Exchange Online PowerShell:

1. Connect to Exchange online using `Connect-ExchangeOnline`.
2. Run the following PowerShell to find if auto-forwarding is enabled to remote domains:

```
Get-RemoteDomain Default | fl AllowedOOFType, AutoForwardEnabled
```

3. Review the `AutoForwardEnabled` parameter, and verify it is set to `False`.

STEP 3: Block client rules for forwarding
To verify the Client Rules Forwarding Block is enabled, use the Microsoft 365 Admin Center:

1. Go to `Exchange Admin Center`.
2. Select `mail flow`.
3. Select `Rules`.
4. Verify that 'Client Rules To External Block' exists.

To verify the Client Rules Forwarding Block is enabled, use the Exchange Online PowerShell Module:

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

```
Get-TransportRule | where { $_.Identity -like '*Client Rules To External Block*' }
```

- Note that `Client Rules To External Block` is a placeholder for the name of said rule.

3. Verify that 'Client Rules To External Block' state is set to Enabled.

Remediation:

NOTE: *Remediation is a three step procedure as follows:*
STEP 1: Transport rules
To alter the mail transport rules so they do not forward email to external domains, use the Microsoft 365 Admin Center:

1. Select `Exchange`.
2. Select `Mail Flow` and `Rules`.
3. For each rule that forwards email to external domains, select the rule and click the 'Delete' icon.

To perform remediation you may also use the Exchange Online PowerShell Module:

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

```
Remove-TransportRule {RuleName}
```

3. To verify this worked you may re-run the audit command as follows:

```
Get-TransportRule | Where-Object {$_.RedirectMessageTo -ne $null} | ft
Name,RedirectMessageTo
```

STEP 2: Automatic forwarding
To verify disable automatic forwarding using the Microsoft 365 Admin Center:

1. Select `Exchange` under Admin centers
2. Under `Mail flow` select `Remote domains`
3. Click on the `default` policy.
4. Click `Edit reply types` in the pane on the right
5. Ensure `Allow automatic forwarding` is not checked.

To perform remediation you may use the Exchange Online PowerShell Module:

1. Connect to Exchange online using `Connect-ExchangeOnline`.
2. Run the following PowerShell to disable auto-forwarding to remote domains:

```
Set-RemoteDomain Default -AutoForwardEnabled $false
```

3. Run the following PowerShell to verify `AutoForwardEnabled` is now set to `False`.

```
Get-RemoteDomain Default | fl AllowedOOFType, AutoForwardEnabled
```

STEP 3: Block client rules for forwarding
To create the Client Rules Forwarding Block, use the Exchange Online PowerShell Module:

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

```
$rejectMessageText = "To improve security, auto-forwarding rules to external
addresses have been disabled. Please contact your Microsoft Partner if you'd
like to set up an exception."

New-TransportRule -name "Client Rules To External Block" -Priority 0 -
SentToScope NotInOrganization -FromScope InOrganization -MessageTypeMatches
AutoForward -RejectMessageEnhancedStatusCode 5.7.1 -RejectMessageReasonText
$rejectMessageText
```

- Note that `Client Rules To External Block` is a placeholder name, this may be named based on preference.

3. Verify that `Client Rules To External Block` or other named preference rule is created.

References:

1. https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/mail-flow-rule-procedures?view=exchserver-2019
2. https://docs.microsoft.com/en-us/archive/blogs/exovoice/disable-automatic-forwarding-in-office-365-and-exchange-server-to-prevent-information-leakage
3. https://docs.microsoft.com/en-us/powershell/module/exchange/mail-flow/set-remotedomain?view=exchange-ps
4. 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,%

4.4 (L1) Ensure mail transport rules do not whitelist specific domains (Automated)

Profile Applicability:

- E3 Level 1

Description:

You should set your Exchange Online mail transport rules so they do not whitelist any specific domains.

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.

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 verify the mail transport rules do not whitelist any specific domains, use the Microsoft 365 Admin Center:

1. Select `Exchange`.
2. Select `Mail Flow` and `Rules`.
3. Review the rules and verify that none of them whitelist any specific domains.

To verify that mail transport rules do not whitelist any domains, you can also use the Exchange Online 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
```

Remediation:

To alter the mail transport rules so they do not whitelist any specific domains, use the Microsoft 365 Admin Center:

1. Select `Exchange`.
2. Select `Mail Flow` and `Rules`.
3. For each rule that whitelists specific domains, select the rule and click the 'Delete' icon.

To remove mail transport rules you may also use the Exchange Online PowerShell:

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

```
Remove-TransportRule {RuleName}
```

3. Verify the rules no longer exists.

```
Get-TransportRule | Where-Object {($_.setscl -eq -1 -and $_.SenderDomainIs -
ne $null)}  | ft Name,SenderDomainIs
```

4.5 (L2) Ensure Safe Attachments policy is enabled (Automated)

Profile Applicability:

- E5 Level 2

Description:

Enabling the Safe Attachments policy extends malware protections to include routing all messages and attachments without a known malware signature to a special hypervisor environment. In that environment, a behavior analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent.

Rationale:

This policy increases the likelihood of identifying and stopping previously unknown malware.

Impact:

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

Audit:

To verify the Safe Attachments policy is enabled, use the Microsoft 365 Admin Center:

1. Click `Security` to open the Microsoft 365 Defender portal.
2. Under `E-mail & Collaboration` navigate to `Policies & rules` > `Threat policies`
3. Under `Policies` select `Safe Attachments`.
4. Verify that at least one policy exists.

To verify the Safe Attachments policy is enabled, you can also use the Exchange Online PowerShell:

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

```
Get-SafeAttachmentPolicy | where-object {$_.Enable -eq "True"}
```

Remediation:

To enable the Safe Attachments policy, use the Microsoft 365 Admin Center:

1. Click `Security` to open the Microsoft 365 Defender portal.
2. Under `E-mail & Collaboration` navigate to `Policies & rules` > `Threat policies`
3. Under `Policies` select `Safe Attachments`.
4. Click `+ Create`.
5. Enter Policy Name and Description.
6. Select `Block`, `Monitor`, `Replace` or `Dynamic Delivery`.
7. Select `Save`.

Default Value:

disabled

CIS Controls:

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

4.6 (L1) Ensure that an anti-phishing policy has been created (Automated)

Profile Applicability:

- E5 Level 1

Description:

By default, Office 365 includes built-in features that help protect your 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 where you can 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:

Turning on Anti-Phishing should not cause an impact, messages will be displayed when applicable.

Audit:

To review the anti-phishing policy, use the Microsoft 365 Admin Center:

1. Click `Security` to open the Security portal.
2. Under `Email & collaboration` navigate to `Policies & rules` > `Threat policies`.
3. Select `Anti-phishing`.
4. Verify the `Office365 AntiPhish Default (Default)` policy exists.

To verify anti-phishing policy, use the Exchange Online PowerShell Module:

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

```
Get-AntiPhishPolicy | ft Name
```

3. Verify `Office365 Antiphish Default` policy exists

Remediation:

To set the anti-phishing policy, use the Microsoft 365 Admin Center:

1. Click `Security` to open the Security portal.
2. Under `Email & collaboration` navigate to `Policies & rules` > `Threat policies`.
3. Select `Anti-phishing`.
4. Click `Create` to create an anti-phishing policy.

To create an anti-phishing policy, use the Exchange Online PowerShell Module:

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

```
New-AntiPhishPolicy -Name "Office365 AntiPhish Policy"
```

CIS Controls:

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

4.7 (L1) Ensure that DKIM is enabled for all Exchange Online Domains (Automated)

Profile Applicability:

- E3 Level 1

Description:

You should use DKIM in addition to SPF and DMARC to help prevent spoofers 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 review if DKIM is enabled, use the Microsoft 365 Admin Center:

1. Click `Security` to open the Security portal.
2. Under `Email & collaboration` navigate to `Policies & rules` > `Threat policies`.
3. Under `Rules` click `DKIM`
4. Click on each domain and confirm that `Sign messages for this domain with DKIM signatures` is `Enabled`.

To verify DKIM is enabled, use the Exchange Online PowerShell Module:

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

```
Get-DkimSigningConfig
```

3. Verify `Enabled` is set to True

Remediation:

To setup DKIM records, first add the following records to your DNS system, for each domain in Exchange Online that you plan to use to send email with:

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 in on microsoft.com.

1. After the DNS records are created, enable DKIM signing in the Office 365 Admin Portal
2. Launch the `Security` Admin Center.
3. Under `Email & collaboration` navigate to `Policies & rules` > `Threat policies`.
4. Under `Rules` click `DKIM`
5. Click on each domain and click `Enable` next to `Sign messages for this domain with DKIM signature`.

To set DKIM is enabled, use 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://docs.microsoft.com/en-us/office365/SecurityCompliance/use-dkim-to-validate-outbound-email

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.5 Implement DMARC 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 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.		●	●

4.8 (L1) Ensure that SPF records are published for all Exchange Domains (Manual)

Profile Applicability:

- E3 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 know where messages from your domains are allowed to originate. This information can be used to 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 verify that SPF records are published for each Exchange Online Domain, do the following:

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

```
nslookup -type=txt domain1.com
```

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

Remediation:

To setup SPF records for Exchange Online accepted domains, perform the following steps:

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://docs.microsoft.com/en-us/office365/SecurityCompliance/set-up-spf-in-office-365-to-help-prevent-spoofing

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.5 Implement DMARC 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 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.		●	●

4.9 (L1) Ensure DMARC Records for all Exchange Online domains are published (Manual)

Profile Applicability:

- E3 Level 1

Description:

Publish Domain-Based Message Authentication, Reporting and Conformance (DMARC) records for each Exchange Online Accepted Domain.

Rationale:

Domain-based Message Authentication, Reporting and Conformance (DMARC) work with Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to authenticate mail senders and ensure that destination email systems trust messages sent from your domain.

Impact:

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

Audit:

To verify that DMARC records are published, perform the following steps:

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

```
nslookup -type=txt _dmarc.domain1.com
```

3. Ensure that a policy exists that starts with `v=DMARC1;`.

Remediation:

To add DMARC records, use the following steps:

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

```
Record:   _dmarc.domain1.com
Type:  TXT
Value:  v=DMARC1; p=none;
```

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

References:

1. https://docs.microsoft.com/en-us/office365/SecurityCompliance/use-dmarc-to-validate-email#CreateDMARCRecord

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.5 Implement DMARC 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 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.		●	●

4.10 (L1) Ensure notifications for internal users sending malware is Enabled (Automated)

Profile Applicability:

- E3 Level 1

Description:

Exchange Online Protection (EOP) is the cloud-based filtering service that protects your organization 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.

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.

Impact:

Notification of account with potential issues should not cause an impact to the user.

Audit:

To verify notifications for internal users sending malware is enabled, use the Microsoft 365 Admin Center:

1. Click `Security` to open the Security portal.
2. Under `Email & collaboration` navigate to `Policies & rules` > `Threat policies`.
3. Select `Anti-malware`.
4. Click on the Default policy.
5. 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 check the setting from PowerShell, use the Exchange Online Module for PowerShell

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

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

Remediation:

To enable notifications for internal users sending malware, use the Microsoft 365 Admin Center:

1. Click `Security` to open the Security portal.
2. Under `Email & collaboration` navigate to `Policies & rules` > `Threat policies`.
3. Select `Anti-malware`.
4. Click on the Default policy.
5. 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`.

To check the setting from PowerShell, use the Exchange Online Module for PowerShell

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

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	17.5 Assign Key Roles and Responsibilities 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 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 Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

4.11 (L2) Ensure MailTips are enabled for end users (Automated)

Profile Applicability:

- E3 Level 2

Description:

MailTips assist end users with identifying strange patterns to emails they send

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.

Audit:

To verify MailTips are enabled, use the Exchange Online PowerShell Module:

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

```
Get-OrganizationConfig |Select-Object MailTipsAllTipsEnabled,
MailTipsExternalRecipientsTipsEnabled, MailTipsGroupMetricsEnabled,
MailTipsLargeAudienceThreshold
```

4. 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 enable MailTips, use the Exchange Online PowerShell Module:

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

```
Set-OrganizationConfig -MailTipsAllTipsEnabled $true -
MailTipsExternalRecipientsTipsEnabled $true -MailTipsGroupMetricsEnabled
$true -MailTipsLargeAudienceThreshold '25'
```

Default Value:

MailTipsAllTipsEnabled: True MailTipsExternalRecipientsTipsEnabled: False MailTipsGroupMetricsEnabled: True MailTipsLargeAudienceThreshold: 25

5 Auditing

5.1 (L1) Ensure Microsoft 365 audit log search is Enabled (Automated)

Profile Applicability:

- E3 Level 1

Description:

When audit log search in the Microsoft Purview compliance portal is enabled, user and admin activity from your organization is recorded in the audit log and retained for 90 days. However, your organization might be using a third-party security information and event management (SIEM) application to access your auditing data. In that case, a global admin can turn off audit log search in Microsoft 365.

Rationale:

Enabling Microsoft Purview audit log search helps Office 365 back office teams to investigate activities for regular security operational or forensic purposes.

Audit:

To verify audit log search is enabled, use the Microsoft 365 Admin Center:

1. Log in as an administrator.
2. Navigate to the `Microsoft Purview compliance portal` by going to https://compliance.office.com
3. Under Solutions, select `Audit` then select an applicable time frame.
4. Verify that you are able to do searches (e.g. try searching for Activities as `Accessed file` and results should be displayed).

To verify audit log search is enabled, use the Exchange Online PowerShell Module:

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

```
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
```

3. Verify the resulting value is `UnifiedAuditLogIngestionEnabled : True`.

Remediation:

To enable Microsoft 365 audit log search, use the Microsoft 365 Admin Center:

1. Log in as an administrator.
2. Navigate to the `Microsoft Purview compliance portal` by going to https://compliance.office.com
3. Under Solutions, select `Audit`.
4. Click `Start recording user and admin activity` next to the information warning at the top.
5. Click `Yes` on the dialog box to confirm.

To enable Microsoft 365 audit log search via Exchange Online PowerShell:

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

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

Default Value:

disabled

References:

1. https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off
2. https://docs.microsoft.com/en-us/powershell/module/exchange/set-adminauditlogconfig?view=exchange-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs 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 Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.2 (L1) Ensure mailbox auditing for all users is Enabled (Automated)

Profile Applicability:

- E3 Level 1

Description:

By turning on mailbox auditing, Microsoft 365 back office teams can track logons to a mailbox as well as what actions are taken while the user is logged on. After you turn on mailbox audit logging for a mailbox, you can search the audit log for mailbox activity. Additionally, when mailbox audit logging is turned on, some actions performed by administrators, delegates, and owners are logged by default.

Rationale:

Starting in January 2019, Microsoft is turning on mailbox audit logging by default for all organizations. This means that certain actions performed by mailbox owners, delegates, and admins are automatically logged, and the corresponding mailbox audit records will be available when you search for them in the mailbox audit log. When mailbox auditing on by default is turned on for the organization, the AuditEnabled property for affected mailboxes won't be changed from False to True. In other words, mailbox auditing on by default ignores the AuditEnabled property on mailboxes. However, only certain mailbox types support default auditing `On`

- User Mailboxes
- Shared Mailboxes
- Microsoft 365 Group Mailboxes

The remaining mailbox types require auditing be turned on at the mailbox level:

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

Whether it is for regulatory compliance or for tracking unauthorized configuration changes in Microsoft 365, enabling mailbox auditing allows for Microsoft 365 back office teams to run security operations, forensics or general investigations on mailbox activities.

NOTE: Without advanced auditing (E5 function) the logs are limited to 90 days.

Audit:

To verify mailbox auditing is enabled by default, use the Exchange Online PowerShell Module:

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

```
Get-OrganizationConfig | Format-List AuditDisabled
```

4. Verify `AuditDisabled` is set to `False`.

To verify mailbox auditing is enabled for all mailboxes that don't support default auditing, use the Exchange Online PowerShell Module:

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

```
Get-Mailbox -ResultSize Unlimited | Where-Object {$_.AuditEnabled -ne $true -
and ($_.RecipientTypeDetails -ne "UserMailbox" -or $_.RecipientTypeDetails -
ne "SharedMailbox")}
```

Alternatively you may run the following command:

```
Get-mailbox | Where AuditEnabled -Match 'False' | select UserPrincipalName,
auditenabled
```

4. Verify `AuditEnabled` is set to `True` for all mailboxes that are not a user, shared, or group mailbox.

Remediation:

To enable mailbox auditing for all users, use the Exchange Online PowerShell Module:

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

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

$AuditDelegate =
@("Create", "FolderBind", "HardDelete", "Move", "MoveToDeletedItems", "SendAs
", "SendOnBehalf", "SoftDelete", "Update", "UpdateFolderPermissions", "Update
InboxRules")

$AdminOwner =
@("Create", "HardDelete", "MailboxLogin", "Move", "MoveToDeletedItems", "Soft
Delete", "Update", "UpdateCalendarDelegation",
"UpdateFolderPermissions", "UpdateInboxRules")

Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditEnabled $true -
AuditLogAgeLimit 180 -AuditAdmin $AuditAdmin -AuditDelegate $AuditDelegate -
AuditOwner $AuditOwner
```

Default Value:

Only certain mailbox types support default auditing `On`:

- User Mailboxes
- Shared Mailboxes
- Microsoft 365 Group Mailboxes

The remaining mailbox types require auditing be turned on at the mailbox level:

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

References:

1. https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-mailbox-auditing?view=o365-worldwide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs 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 Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.3 (L1) Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

This report contains records of accounts that have had activity that could indicate they are compromised, such as accounts that have:

- successfully signed in after multiple failures, which is an indication that the accounts have cracked passwords
- signed in to your tenant from a client IP address that has been recognized by Microsoft as an anonymous proxy IP address (such as a TOR network)
- successful sign-ins from users where two sign-ins appeared to originate from different regions and the time between sign-ins makes it impossible for the user to have traveled between those regions

Rationale:

Reviewing this report on a regular basis allows for identification and remediation of compromised accounts.

Audit:

To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review the report, perform the following steps using the Azure Portal:

1. Go to portal.azure.com.
2. Click `Azure Active Directory`.
3. Under `Manage` click on `Security`
4. Under `Report` click on `Risky sign-ins`
5. Review by `Risk level (aggregate)`.

To get risky sign-ins event report programmatically, use following graph API:

```
https://graph.microsoft.com/beta/identityRiskEvents?$filter=riskEventDateTime
gt < 7 days older datetime > and riskEventStatus eq 'active'
```

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-user-at-risk
2. https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-remediate-users-flagged-for-risk

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.4 (L2) Ensure the Application Usage report is reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 2

Description:

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

Rationale:

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

Audit:

To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review the report, perform the following steps using the Azure Portal:

1. Go to portal.azure.com.
2. Click `Azure Active Directory`.
3. Select `Enterprise applications`.
4. Review the information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.5 (L1) Ensure the self-service password reset activity report is reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

The Microsoft 365 platforms allow a user to reset their password in the event they forget it. The self-service password reset activity report logs each time a user successfully resets their password this way. You should review the self-service password reset activity report at least weekly.

Rationale:

An attacker will commonly compromise an account, then change the password to something they control and can manage.

Audit:

To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review the report, perform the following steps using the Azure Portal:

1. Go to portal.azure.com.
2. Go to 'Azure Active Directory'.
3. Click on 'Usage & insights' under 'Monitoring'.
4. Select 'Authentication methods activity' and the 'Usage' tab.
5. Review the list of users who have reset their passwords in the last seven days by clicking 'Self-service password resets and account unlocks by method'.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.6 (L1) Ensure user role group changes are reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

Role-Based Access Control allows for permissions to be assigned to users based on their roles within an organization. It is more manageable form of access control that is less prone to errors. These user roles can be audited inside of Microsoft Purview to provide a security auditor insight into user privilege change.

Rationale:

Weekly reviews provide an opportunity to identify rights changes in an organization and is a large part of maintaining Least Privilege and preventing Privilege creep. Insider Threats, either intentional or unintentional can occur when a user has higher than needed privileges. Maintaining accountability of role membership will keep Insiders and malicious actors limited in the scope of potential damaging activities.

Impact:

By performing regular reviews the Administrators assigning rights to users will need to inevitably provide justification for those changes to security auditors. Documentation that includes detailed policies, procedures, and change requests will need to be considered in order to keep a secure organization functioning within it's planned operational level.

Audit:

To verify user role group changes are being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review user role group changes, perform the following steps using the Microsoft 365 Admin Center:

1. Beneath **Admin centers** Click on `Compliance` to be redirected to Microsoft Purview.
2. Click on `Audit` then select `Search`.
3. In `Activities` find `Added member to Role` under the **Role administration activities** section.
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

To review user role group changes, perform the following steps using Exchange Online PowerShell Module:

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

```
$startDate = ((Get-date).AddDays(-7)).ToShortDateString()
$endDate = (Get-date).ToShortDateString()

Search-UnifiedAuditLog -StartDate $startDate -EndDate $endDate | Where-Object
{ $_.Operations -eq "Add member to role." }
```

3. Review the output

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.7 (L1) Ensure mail forwarding rules are reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

There is no impacting to reviewing these reports.

Audit:

To verify mail forwarding rules are being reviewed at least weekly, confirm that the necessary procedures are in place and being followed by the assigned employee.

Remediation:

To review mail forwarding rules, use the Microsoft 365 Admin Center:

1. Go to `Exchange admin center`.
2. Expand `Reports` then select `Mail flow`.
3. Click on `Auto forwarded messages report`.
4. Review

Note: Mail flow reports cannot be viewed from the Classic Exchange Admin Center

To review mail forwarding rules, use the following PowerShell script:
Uses the administrator user credential to export Mail forwarding rules, User Delegates and SMTP Forwarding policies to multiple csv files. First connect to Exchange Online and Azure Active Directory by using both `Connect-ExchangeOnline` and `Connect-MsolService`

```
$allUsers = @()
$AllUsers = Get-MsolUser -All -EnabledFilter EnabledOnly | select ObjectID,
UserPrincipalName, FirstName, LastName, StrongAuthenticationRequirements,
StsRefreshTokensValidFrom, StrongPasswordRequired,
LastPasswordChangeTimestamp | Where-Object {($_.UserPrincipalName -notlike
"*#EXT#*")}


$UserInboxRules = @()
$UserDelegates = @()


foreach ($User in $allUsers)
{
    Write-Host "Checking inbox rules and delegates for user: "
$User.UserPrincipalName;
    $UserInboxRules += Get-InboxRule -Mailbox $User.UserPrincipalname |
Select Name, Description, Enabled, Priority, ForwardTo,
ForwardAsAttachmentTo, RedirectTo, DeleteMessage | Where-Object
{($_.ForwardTo -ne $null) -or ($_.ForwardAsAttachmentTo -ne $null) -or
($_.RedirectsTo -ne $null)}
    $UserDelegates += Get-MailboxPermission -Identity $User.UserPrincipalName
| Where-Object {($_.IsInherited -ne "True") -and ($_.User -notlike "*SELF*")}
}


$SMTPForwarding = Get-Mailbox -ResultSize Unlimited | select
DisplayName,ForwardingAddress,ForwardingSMTPAddress,DeliverToMailboxandForwar
d | where {$_.ForwardingSMTPAddress -ne $null}

# Export list of inboxRules, Delegates and SMTP Forwards
$UserInboxRules | Export-Csv MailForwardingRulesToExternalDomains.csv
$UserDelegates | Export-Csv MailboxDelegatePermissions.csv
$SMTPForwarding | Export-Csv Mailboxsmtpforwarding.csv
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.8 (L1) Ensure all security threats in the Threat protection status report are reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should review all the security threats in the Threat protection status report at least weekly. This report shows specific instances of Microsoft blocking a malware attachment from reaching your users, phishing being blocked, impersonation attempts, etc.

Rationale:

While this report isn't strictly actionable, reviewing it will give you a sense of the overall volume of various security threats targeting your users, which may prompt you to adopt more aggressive threat mitigations.

Audit:

To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review the report, use the Microsoft 365 Admin Center:

1. Select `Security`.
2. Click on `Reports` and under `Email & collaboration` select `Email & collaboration reports`.
3. Under `Threat protection status` click on `View details`
4. Review the chart and look for `Email Malware` statistics.

References:

1. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-email-security-reports?view=o365-worldwide#threat-protection-status-report

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.9 (L1) Ensure the Account Provisioning Activity report is reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

The Account Provisioning Activity report details any account provisioning that was attempted by an external application.

Rationale:

If you don't usually use a third party provider to manage accounts, any entry on the list is likely illicit. If you do, this is a great way to monitor transaction volumes and look for new or unusual third party applications that are managing users. If you see something unusual, contact the provider to determine if the action is legitimate.

Audit:

To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review the report, use the Microsoft 365 Admin Center:

1. Go to `Security`.
2. Click on `Audit` then select `Search`.
3. Set `Activities` to `Added user` for `User administration activities`.
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

To review Account Provisioning Activity report, use the Exchange Online PowerShell Module:

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

```
$startDate = ((Get-date).AddDays(-7)).ToShortDateString()
$endDate = (Get-date).ToShortDateString()

Search-UnifiedAuditLog -StartDate $startDate -EndDate $endDate | Where-Object
{ $_.Operations -eq "add user." }
```

3. Review the output

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.10 (L1) Ensure non-global administrator role group assignments are reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should review non-global administrator role group assignments at least every week.

Rationale:

While these roles are less powerful than a global admin, they do grant special privileges that can be used illicitly. If you see something unusual, contact the user to confirm it is a legitimate need.

Audit:

To verify non-global administrator role group assignments are being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review non-global administrator role group assignments, use the Microsoft 365 Admin Center:

1. Go to `Security`.
2. Click on `Audit` then select `Search`.
3. Set `Added member to Role` and `Removed a user from a directory role` for `Activities`
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.11 (L1) Ensure the spoofed domains report is reviewed weekly (Automated)

Profile Applicability:

- E5 Level 1

Description:

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

Rationale:

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

Audit:

To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review the report, use the Microsoft 365 Admin Center:

1. Go to `Security`.
2. Under `Email & collaboration` click on `Policies & rules` then select `Threat policies`.
3. Under `Rules` click on `Tenant Allow / Block Lists` then select `Spoofing`.
4. Review.

To view spoofed senders that were allowed or blocked by spoof intelligence using the Exchange Online PowerShell module:

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

```
Get-SpoofIntelligenceInsight
```

3. Review.

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.12 (L2) Ensure Microsoft Defender for Cloud Apps is Enabled (Manual)

Profile Applicability:

- E5 Level 2

Description:

Enabling Microsoft Defender for Cloud Apps gives you insight into suspicious activity in Microsoft 365 so you can investigate situations that are potentially problematic and, if needed, take action to address security issues.

Rationale:

You can receive notifications of triggered alerts for atypical or suspicious activities, see how your 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 verify Microsoft Defender for Cloud Apps is enabled, use the Microsoft 365 Admin Center:

1. Select `Security`.
2. Select `More Resources`.
3. Select `Open` under `Microsoft Defender for Cloud App Security`.
4. Ensure the dashboard opens and the feature is enabled.

Remediation:

To enable Microsoft Defender for Cloud Apps, use the Microsoft 365 Admin Center:

1. Select `Security`.
2. Select `More Resources`.
3. Select `Open` under `Microsoft Defender for Cloud App Security`.
4. Ensure the dashboard opens and the feature is enabled.

Additional Information:

https://docs.microsoft.com/en-us/defender-cloud-apps/get-started

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	10.5 Enable Anti-Exploitation Features 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 Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

5.13 (L1) Ensure the report of users who have had their email privileges restricted due to spamming is reviewed (Manual)

Profile Applicability:

- E3 Level 1

Description:

Microsoft 365 Defender reviews of Restricted Entities will provide a list of user accounts restricted from sending e-mail. If a user exceeds one of the outbound sending limits as specified in the service limits or in outbound spam policies, the user is restricted from sending email, but they can still receive email.

Rationale:

Users who are found on the restricted users list have a high probability of having been compromised. Review of this list will allow an organization to remediate these user accounts, and then unblock them.

Audit:

To verify the report is being reviewed at least weekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To review the report, use the Microsoft 365 Admin Center:

1. Click `Security` to open the Security portal.
2. Under `Email & collaboration` navigate to `Review`.
3. Click `Restricted Entities`.
4. Review alerts and take appropriate action (unblocking) after account has been remediated.

References:

1. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account?view=o365-worldwide
2. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 Conduct Audit Log Reviews Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.14 (L1) Ensure Guest Users are reviewed at least biweekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

Guest users can be set up for those users not in your tenant to still be granted access to resources. It is important to maintain visibility for what guest users are established in the tenant.

Rationale:

Periodic review of guest users ensures proper access to resources in your tenant.

Audit:

To verify the report is being reviewed at least biweekly, confirm that the necessary procedures are in place and being followed.

Remediation:

To view guest users, use the Microsoft 365 Admin Center:

1. Log in as an administrator
2. Navigate to the `Users` and `Guest Users`
3. Review the list of users

To verify Microsoft 365 audit log search is enabled, use the Microsoft Online PowerShell Module:

1. Run Microsoft Online PowerShell Module
2. Connect using `Connect-MsolService`
3. Run the following PowerShell command:

```
Get-MsolUser -all |Where-Object {$_.UserType -ne "Member"} |Select-Object
UserPrincipalName, UserType, CreatedDate
```

4. Review the list of users

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts 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 Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

6 Storage

6.1 (L2) Ensure document sharing is being controlled by domains with whitelist or blacklist (Automated)

Profile Applicability:

- E3 Level 2

Description:

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

Rationale:

Attackers will often attempt to expose sensitive information to external entities through sharing, and restricting the domains that your 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 verify document sharing settings, use the Microsoft 365 Admin Center:

1. Navigate to Microsoft 365 administration portal (`https://admin.microsoft.com`), Click on `Admin Centers` and then `SharePoint`.
2. Expand `Policies` then click `Sharing`.
3. Expand `More external sharing settings` and confirm that `Limit external sharing by domain` is checked.
4. Verify that an accurate list of allowed domains is listed.

To verify document sharing setting, you can also use SharePoint Online PowerShell:

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

```
Get-SPOTenant | fl SharingDomainRestrictionMode,SharingAllowedDomainList
```

Remediation:

To configure document sharing restrictions, use the Microsoft 365 Admin Center:

1. Navigate to Microsoft 365 administration portal (`https://admin.microsoft.com`), Click on `Admin Centers` and then `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 configure document sharing restrictions, you can also use SharePoint Online 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:

off

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists 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 Only allow access to authorized cloud storage or email providers.		●	●
v7	14.6 Protect Information through Access Control Lists 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.	●	●	●

6.2 (L2) Block OneDrive for Business sync from unmanaged devices (Automated)

Profile Applicability:

- E3 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 or not it is Azure Domain Joined or Active Directory Domain joined.

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 Azure AD domains. If you have devices which are only Azure AD 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 verify sync settings on unmanaged devices, use the Microsoft 365 Admin Center:

1. Navigate to Microsoft 365 administration portal (`https://admin.microsoft.com`), Click on `All Admin Centers` and then `Show All`, then `SharePoint`.
2. Now 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 to obtain the GUID for each on-premises domain

To verify sync settings on unmanaged devices, you can also use SharePoint Online PowerShell:

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

```
Get-SPOTenantSyncClientRestriction | fl
TenantRestrictionEnabled,AllowedDomainList
```

3. Verify `TenantRestrictionEnabled` is set to `True` and `AllowedDomainList` is populated and valid.

Remediation:

To block the sync client on unmanaged devices, use the Microsoft 365 Admin Center:

1. Navigate to Microsoft 365 administration portal (`https://admin.microsoft.com`), Click on `All Admin Centers` and then `Show All`, then `SharePoint`.
2. Now click `Settings` followed by `OneDrive - Sync`
3. Check the `Allow syncing only on computers joined to specific domains`
4. Use the `Get-ADDomain` PowerShell command to obtain the GUID from each domain then add them to the box.
5. Click `Save`

To block the sync client on unmanaged devices, you can also use SharePoint Online 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 is no domain restriction applied to the syncing of OneDrive.

References:

1. https://docs.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenantsyncclientrestriction?view=sharepoint-ps
2. https://docs.microsoft.com/en-US/onedrive/allow-syncing-only-on-specific-domains?WT.mc_id=365AdminCSH_spo

6.3 (L1) Ensure expiration time for external sharing links is set (Automated)

Profile Applicability:

- E3 Level 1

Description:

The external sharing features of Microsoft SharePoint let users in your organization share content with people outside the organization (such as partners, vendors, clients, or customers). External sharing in SharePoint is part of secure collaboration with Microsoft 365.

Rationale:

An attacker can compromise a user account for a short period of time, send anonymous sharing links to an external account, then take their time accessing the data. They can also compromise external accounts and steal the anonymous sharing links sent to those external entities well after the data has been shared. Restricting how long the links are valid can reduce the window of opportunity for attackers.

Impact:

Enabling this feature will ensure that link expire within the defined number of days. This will have an affect on links that were previously not set with an expiration.

Audit:

To verify anonymous access links are correctly set to expire, use the Microsoft 365 Admin Center:

1. Select `Admin Centers` and `SharePoint`.
2. Expand `Polices` then click `Sharing`.
3. Under `Choose expiration and permissions options for Anyone links`. verify if `These links must expire within this many days` is checked.
4. Confirm the number of days is set to the desired value, such as `30`.

To verify anonymous links are correctly set to expire, you can also use SharePoint Online PowerShell:

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

```
Get-SPOTenant | fl RequireAnonymousLinksExpireInDays
```

3. Verify that the returned value is at most `30 days` but is not set to **-1**

Remediation:

To set expiration for anonymous access links, use the Microsoft 365 Admin Center

1. Select `Admin Centers` and `SharePoint`
2. Expand `Polices` then click `Sharing`
3. Under `Choose expiration and permissions options for Anyone links.` check the `These links must expire within this many days`
4. Set to the desired number of days, such as `30`
5. Click `Save`

To set expiration for anonymous access links, you can also use SharePoint Online PowerShell:

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

```
set-SPOTenant -RequireAnonymousLinksExpireInDays 30
```

Default Value:

Anonymous Sharing - `On`

Sharing Links Expiration - `Off`

References:

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

Additional Information:

Setting links to expire in X number of days only applies in the most permissive sharing mode which is the default setting. Organizations should decide on an organizational level whether to allow external sharing and to what level.

6.4 (L2) Ensure external storage providers available in Outlook on the Web are restricted (Automated)

Profile Applicability:

- E3 Level 2

Description:

You should restrict storage providers that are integrated with Outlook on the Web.

Rationale:

By default additional storage providers are allowed in Outlook 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:

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 verify external storage providers are disabled, use the Exchange Online PowerShell Module:

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

```
Get-OwaMailboxPolicy | Format-Table Name, AdditionalStorageProvidersAvailable
```

3. Verify that the value returned is `False`.

Remediation:

To disable external storage providers, use the Exchange Online PowerShell Module:

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

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

3. Run the following Powershell command to verify that the value is now `False`:

```
Get-OwaMailboxPolicy | Format-Table Name, AdditionalStorageProvidersAvailable
```

Default Value:

Additional Storage Providers - True

References:

1. https://docs.microsoft.com/en-us/powershell/module/exchange/client-access/set-owamailboxpolicy?view=exchange-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists 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 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 Only allow access to authorized cloud storage or email providers.		●	●

7 Mobile Device Management

7.1 (L1) Ensure mobile device management policies are set to require advanced security configurations (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should configure your mobile device management policies to require advanced security configurations. If you do not require this, users will be able to connect from devices that are vulnerable to basic exploits, leading to potential breaches of accounts and data.

Rationale:

Managing mobile devices in your organization, helps provide a basic level of security to protect against attacks from these platforms. For example ensure that the device is up to date on patches or is not rooted. These configurations open those devices to vulnerabilities that are addressed in patched versions of the mobile OS.

Impact:

The impact associated with this change is dependent upon the settings specified in the mobile device configuration profile.

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Ensure that profiles exist and are assigned for relevant mobile device types

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create profile` to create a new profile. Select the appropriate Platform and settings from the configuration screens.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

7.2 (L1) Ensure that mobile device password reuse is prohibited (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should not allow your users to reuse the same password on their mobile devices.

Rationale:

Devices without this protection are vulnerable to being accessed by attackers who can then steal account credentials, data, or install malware on the device. Choosing unique and unused passwords every time a password changes on mobile devices lessens the likelihood that the password can be guessed by an attacker.

Impact:

This change will have a moderate user impact

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Device restrictions` section under `Password` and verify `Prevent reuse of previous passwords` is set to `5`.

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create profile`
4. Set a `Name` for the policy, choose the appropriate `Platform` and select `Device restrictions`
5. In the `Password` section, ensure that `Prevent reuse of previous passwords` is set to `5`.

Default Value:

Password reuse is not enforced by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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 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.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

7.3 (L1) Ensure that mobile devices are set to never expire passwords (Manual)

Profile Applicability:

- E3 Level 1

Description:

Ensure that users passwords on their mobile devices, never expire.

Rationale:

While this is not the most intuitive recommendation, research has found that when periodic password resets are enforced, passwords become weaker as users tend to pick something weaker and then use a pattern of it for rotation. If a user creates a strong password: long, complex and without any pragmatic words present, it should remain just as strong is 60 days as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason.

Impact:

This setting should not cause a noticeable impact to users

Audit:

To verify mobile device management profile, use the Microsoft 365 Admin Center:

1. Select `Device Management` under `Admin Centers`.
2. Select `Devices`, then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Device restrictions` section and under `Password` verify that passwords are not configured to expire.

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Select `Device Management` under `Admin Centers`.
2. Select `Devices`, then under `Policy` select `Configuration profiles`
3. Review the list of profiles.
4. From there, go to the device policies page to remove any device security policies that expire passwords.

Default Value:

Password changes are not required by default

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

7.4 (L1) Ensure that users cannot connect from devices that are jail broken or rooted (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should not allow your users to use to connect with mobile devices that have been jail broken or rooted.

Rationale:

These devices have had basic protections disabled to run software that is often malicious and could very easily lead to an account or data breach.

Impact:

Impact should be minimal however, in the event that a device is Jailbroken or running a developer build of a mobile Operating System it will be blocked from connecting.

Audit:

To verify mobile device management policies, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Device Health` section under `Settings` and verify `Jailbroken devices` or `Rooted devices` is set to `Block`.

Remediation:

To set mobile device management policies, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create Policy`
4. Set a `Name` for the policy, choose the appropriate `Platform`
5. Under `Settings` and `Device Health` ensure that `Jailbroken devices` or `Rooted devices` is set to `Block`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.2 Address Unauthorized Assets Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	●	●	●
v7	18.3 Verify That Acquired Software is Still Supported 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.		●	●
v7	18.4 Only Use Up-to-date And Trusted Third-Party Components Only use up-to-date and trusted third-party components for the software developed by the organization.		●	●

7.5 (L2) Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise (Manual)

Profile Applicability:

- E3 Level 2

Description:

Require mobile devices to wipe on multiple sign-in failures

Rationale:

Devices without this protection are vulnerable to being accessed physically by attackers who can then steal account credentials, data, or install malware on the device.

Impact:

This setting has no impact, unless a user mistypes their password multiple times and causes their device to wipe. In that case, it will have a high user impact.

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Password` section under `Device restrictions` and verify `Number of sign-in failures before wiping device` is set to `10`.

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create profile`
4. Set a `Name` for the policy, choose the appropriate `Platform` and select `Device restrictions`
5. In the `Password` section, ensure that `Number of sign-in failures before wiping device` is set to `10`.

Default Value:

The default is to not wipe the device on multiple failed attempts.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

7.6 (L1) Ensure that mobile devices require a minimum password length to prevent brute force attacks (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should require your users to use a minimum password length of at least six characters to unlock their mobile devices.

Rationale:

Devices without this protection are vulnerable to being accessed physically by attackers who can then steal account credentials, data, or install malware on the device.

Impact:

This change has potentially high user impact depending on the willingness and awareness of the end-user.

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Password` section under `Device restrictions` and verify `Minimum password length` is set to `6`.

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create profile`
4. Set a `Name` for the policy, choose the appropriate `Platform` and select `Device restrictions`
5. In the `Password` section, ensure that `Minimum password length` is set to `6`.

Default Value:

Minimum password lengths are not enforced by default

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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 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.		●	●

7.7 (L1) Ensure devices lock after a period of inactivity to prevent unauthorized access (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should require your users to configure their mobile devices to lock on inactivity.

Rationale:

Attackers can steal unlocked devices and access data and account information.

Impact:

This setting has a low impact on users.

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Password` section under `Device restrictions`
5. Verify `Maximum minutes of inactivity until screen lock` is set to `5` and `Maximum minutes after screen lock before password is required` is set to `Immediately`

Remediation:

To set mobile device management policies, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create profile`
4. Set a `Name` for the policy, choose the appropriate `Platform` and select `Device restrictions`
5. In the `Password` section, ensure that `Maximum minutes of inactivity until screen lock` is set to `5` and `Maximum minutes after screen lock before password is required` is set to `Immediately`

Default Value:

Screen locking is not enabled by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets 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	5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers			
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

7.8 (L1) Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should require your users to use encryption on their mobile devices.

Rationale:

Unencrypted devices can be stolen and their data extracted by an attacker very easily.

Impact:

This setting should have no user impact, provided the device supports the feature.

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for `Android`.
4. Review the `Password` section under `Device restrictions` and verify `Encryption` is set to `Require`.

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create profile`
4. Set a `Name` for the policy, choose `Android` as the `Platform` and select `Device restrictions`
5. In the `Password` section, ensure that `Encryption` is set to `Require`.

Default Value:

Device encryption is not required by the O365 platform by default, although some mobile platforms are encrypted by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.6 Encrypt Data on End-User Devices Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	●	●	●
v7	5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers			
v7	13.6 Encrypt the Hard Drive of All Mobile Devices. Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	●	●	●

7.9 (L1) Ensure that mobile devices require complex passwords (Type = Alphanumeric) (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should require your users to use a complex password with a at least two character sets (letters and numbers, for example) to unlock their mobile devices.

Rationale:

Devices without this protection are vulnerable to being accessed physically by attackers who can then steal account credentials, data, or install malware on the device.

Impact:

This setting will have a moderate user impact

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Password` section under `Device restrictions` and verify `Required password type` is set to `Alphanumeric`.

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create profile`
4. Set a `Name` for the policy, choose the appropriate `Platform` and select `Device restrictions`
5. In the `Password` section, ensure that `Required password type` is set to `Alphanumeric`.

Default Value:

This setting is not enabled by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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 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.		●	●
v7	5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers			

7.10 (L1) Ensure that mobile devices require complex passwords (Simple Passwords = Blocked) (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should require your users to use a complex password to unlock their mobile devices.

Rationale:

Devices without this protection are vulnerable to being accessed physically by attackers who can then steal account credentials, data, or install malware on the device.

Impact:

This has a moderate impact on users

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Password` section under `Device restrictions` and verify `Simple Passwords` is set to `Blocked`.

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Configuration profiles`
3. Select `Create profile`
4. Set a `Name` for the policy, choose the appropriate `Platform` and select `Device restrictions`
5. In the `Password` section, ensure that `Simple Passwords` is set to `Blocked`.

Default Value:

This setting is not enabled by default

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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 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.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

7.11 (L1) Ensure that devices connecting have AV and a local firewall enabled (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should configure your mobile device management policies to require the PC to have anti-virus and have a firewall enabled.

Rationale:

If you do not require this, users will be able to connect from devices that are vulnerable to basic internet attacks, leading to potential breaches of accounts and data.

Impact:

Impact should be minimal however, in the event that a device is not running appropriate protection it will be blocked from connecting.

Audit:

To verify mobile device management policies, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Compliance policies`
3. Review the list of policies. Ensure that a policy exists for each `Platform`.
4. Review the `Properties` section of each policy. Under `Settings` and `System Security` verify the value for `Firewall`, `Antivirus`, and `Antispyware` are all set to `Require`.

Remediation:

To set mobile device management policies, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` select `Endpoint Management`.
2. Select `Devices` and then under `Policy` select `Compliance policies`
3. Select `Create Policy`
4. Set a `Name` for the policy, choose the appropriate PC `Platform`
5. Select `System Security` under `Settings`.
6. Under `Device Security` set the values for `Firewall`, `Antivirus`, and `Antispyware` all to `Require`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

7.12 (L2) Ensure mobile device management policies are required for email profiles (Manual)

Profile Applicability:

- E3 Level 2

Description:

You should configure your mobile device management policies to require the policy to manage the email profile of the user.

Rationale:

If you do not require this, users will be able to setup and configure email accounts without the protections of the mobile device management policy, leading to potential breaches of accounts and data.

Impact:

This setting will have a moderate impact on users

Audit:

To verify mobile device management policies, use the Microsoft 365 Admin Center:

1. Select `Device Management` under `Admin Centers`.
2. Select `Device compliance` and then under `Policy` select `Compliance policies`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Email` section under `Settings` and verify `Require mobile devices to have a managed email profile` is set to `Require`.

Remediation:

To set mobile device management policies, use the Microsoft 365 Admin Center:

1. Select `Device Management` under `Admin Centers`.
2. Select `Device compliance` and then under `Policy` select `Compliance policies`
3. Select `Create Policy`
4. Set a `Name` for the policy, choose the appropriate `Platform`
5. Under `Settings` and `Email` ensure that `Require mobile devices to have a managed email profile` is set to `Require`.

Default Value:

This setting is not enabled by default

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	7 Email and Web Browser Protections Email and Web Browser Protections			
v7	7.1 Ensure Use of Only Fully Supported Browsers and Email Clients 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.	●	●	●

7.13 (L1) Ensure mobile devices require the use of a password (Manual)

Profile Applicability:

- E3 Level 1

Description:

You should require your users to use a password to unlock their mobile devices.

Rationale:

Devices without this protection are vulnerable to being accessed physically by attackers who can then steal account credentials, data, or install malware on the device.

Impact:

This change will require users to provide a password to unlock their mobile device after the timeout period expires

Audit:

To verify mobile device management profiles, use the Microsoft 365 Admin Center:

1. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then under `Policy` select `Configuration profiles`
3. Review the list of profiles. Ensure that a profile exists for each `Platform`.
4. Review the `Password` section under `Device restrictions` and verify `Password` is set to `Require`.

Remediation:

To set mobile device management profiles, use the Microsoft 365 Admin Center:

1. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then under `Policy` select `Configuration profiles`
3. Select `Create profile`
4. Set a `Name` for the policy, choose the appropriate `Platform` and select `Device restrictions`
5. In the `Password` section, ensure that `Password` is set to `Require`.

Default Value:

This setting is not enabled by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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 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.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Account / Authentication**		
1.1	**Azure Active Directory**		
1.1.1	(L1) Ensure multifactor authentication is enabled for all users in administrative roles (Automated)	☐	☐
1.1.2	(L2) Ensure multifactor authentication is enabled for all users in all roles (Manual)	☐	☐
1.1.3	(L1) Ensure that between two and four global admins are designated (Automated)	☐	☐
1.1.4	(L1) Ensure self-service password reset is enabled (Manual)	☐	☐
1.1.5	(L1) Ensure that password protection is enabled for Active Directory (Manual)	☐	☐
1.1.6	(L1) Enable Conditional Access policies to block legacy authentication (Automated)	☐	☐
1.1.7	(L1) Ensure that password hash sync is enabled for hybrid deployments (Manual)	☐	☐
1.1.8	(L2) Enable Azure AD Identity Protection sign-in risk policies (Manual)	☐	☐
1.1.9	(L2) Enable Azure AD Identity Protection user risk policies (Manual)	☐	☐
1.1.10	(L2) Use Just In Time privileged access to Office 365 roles (Manual)	☐	☐
1.1.11	(L1) Ensure Security Defaults is disabled on Azure Active Directory (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.1.12	(L2) Ensure that only organizationally managed/approved public groups exist (Manual)	☐	☐
1.1.13	(L2) Ensure that collaboration invitations are sent to allowed domains only (Manual)	☐	☐
1.1.14	(L2) Ensure that LinkedIn contact synchronization is disabled. (Manual)	☐	☐
1.1.15	(L1) Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users. (Manual)	☐	☐
1.1.16	(L2) Ensure the option to remain signed in is hidden (Manual)	☐	☐
1.2	(L1) Ensure modern authentication for Exchange Online is enabled (Automated)	☐	☐
1.3	(L1) Ensure modern authentication for SharePoint applications is required (Automated)	☐	☐
1.4	(L1) Ensure that Office 365 Passwords Are Not Set to Expire (Automated)	☐	☐
1.5	(L1) Ensure Administrative accounts are separate and cloud-only (Manual)	☐	☐
2	**Application Permissions**		
2.1	(L2) Ensure third party integrated applications are not allowed (Manual)	☐	☐
2.2	(L2) Ensure calendar details sharing with external users is disabled (Automated)	☐	☐
2.3	(L2) Ensure Safe Links for Office Applications is Enabled (Automated)	☐	☐
2.4	(L2) Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5	(L2) Ensure Office 365 SharePoint infected files are disallowed for download (Automated)	☐	☐
2.6	(L2) Ensure user consent to apps accessing company data on their behalf is not allowed (Automated)	☐	☐
2.7	(L2) Ensure the admin consent workflow is enabled (Automated)	☐	☐
2.8	(L2) - Ensure users installing Outlook add-ins is not allowed (Automated)	☐	☐
2.9	(L1) - Ensure users installing Word, Excel, and PowerPoint add-ins is not allowed (Manual)	☐	☐
2.10	(L1) Ensure internal phishing protection for Forms is enabled (Manual)	☐	☐
2.11	(L1) Ensure that Sways cannot be shared with people outside of your organization (Manual)	☐	☐
3	**Data Management**		
3.1	(L2) Ensure the customer lockbox feature is enabled (Automated)	☐	☐
3.2	(L2) Ensure SharePoint Online Information Protection policies are set up and used (Manual)	☐	☐
3.3	(L2) Ensure external domains are not allowed in Skype or Teams (Manual)	☐	☐
3.4	(L1) Ensure DLP policies are enabled (Automated)	☐	☐
3.5	(L1) Ensure DLP policies are enabled for Microsoft Teams (Manual)	☐	☐
3.6	(L2) Ensure that external users cannot share files, folders, and sites they do not own (Automated)	☐	☐
3.7	(L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4	**Email Security / Exchange Online**		
4.1	(L1) Ensure the Common Attachment Types Filter is enabled (Automated)	☐	☐
4.2	(L1) Ensure Exchange Online Spam Policies are set to notify administrators (Automated)	☐	☐
4.3	(L1) Ensure all forms of mail forwarding are blocked and/or disabled (Automated)	☐	☐
4.4	(L1) Ensure mail transport rules do not whitelist specific domains (Automated)	☐	☐
4.5	(L2) Ensure Safe Attachments policy is enabled (Automated)	☐	☐
4.6	(L1) Ensure that an anti-phishing policy has been created (Automated)	☐	☐
4.7	(L1) Ensure that DKIM is enabled for all Exchange Online Domains (Automated)	☐	☐
4.8	(L1) Ensure that SPF records are published for all Exchange Domains (Manual)	☐	☐
4.9	(L1) Ensure DMARC Records for all Exchange Online domains are published (Manual)	☐	☐
4.10	(L1) Ensure notifications for internal users sending malware is Enabled (Automated)	☐	☐
4.11	(L2) Ensure MailTips are enabled for end users (Automated)	☐	☐
5	**Auditing**		
5.1	(L1) Ensure Microsoft 365 audit log search is Enabled (Automated)	☐	☐
5.2	(L1) Ensure mailbox auditing for all users is Enabled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.3	(L1) Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly (Manual)	☐	☐
5.4	(L2) Ensure the Application Usage report is reviewed at least weekly (Manual)	☐	☐
5.5	(L1) Ensure the self-service password reset activity report is reviewed at least weekly (Manual)	☐	☐
5.6	(L1) Ensure user role group changes are reviewed at least weekly (Manual)	☐	☐
5.7	(L1) Ensure mail forwarding rules are reviewed at least weekly (Manual)	☐	☐
5.8	(L1) Ensure all security threats in the Threat protection status report are reviewed at least weekly (Manual)	☐	☐
5.9	(L1) Ensure the Account Provisioning Activity report is reviewed at least weekly (Manual)	☐	☐
5.10	(L1) Ensure non-global administrator role group assignments are reviewed at least weekly (Manual)	☐	☐
5.11	(L1) Ensure the spoofed domains report is reviewed weekly (Automated)	☐	☐
5.12	(L2) Ensure Microsoft Defender for Cloud Apps is Enabled (Manual)	☐	☐
5.13	(L1) Ensure the report of users who have had their email privileges restricted due to spamming is reviewed (Manual)	☐	☐
5.14	(L1) Ensure Guest Users are reviewed at least biweekly (Manual)	☐	☐
6	**Storage**		
6.1	(L2) Ensure document sharing is being controlled by domains with whitelist or blacklist (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2	(L2) Block OneDrive for Business sync from unmanaged devices (Automated)	☐	☐
6.3	(L1) Ensure expiration time for external sharing links is set (Automated)	☐	☐
6.4	(L2) Ensure external storage providers available in Outlook on the Web are restricted (Automated)	☐	☐
7	**Mobile Device Management**		
7.1	(L1) Ensure mobile device management policies are set to require advanced security configurations (Manual)	☐	☐
7.2	(L1) Ensure that mobile device password reuse is prohibited (Manual)	☐	☐
7.3	(L1) Ensure that mobile devices are set to never expire passwords (Manual)	☐	☐
7.4	(L1) Ensure that users cannot connect from devices that are jail broken or rooted (Manual)	☐	☐
7.5	(L2) Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise (Manual)	☐	☐
7.6	(L1) Ensure that mobile devices require a minimum password length to prevent brute force attacks (Manual)	☐	☐
7.7	(L1) Ensure devices lock after a period of inactivity to prevent unauthorized access (Manual)	☐	☐
7.8	(L1) Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data (Manual)	☐	☐
7.9	(L1) Ensure that mobile devices require complex passwords (Type = Alphanumeric) (Manual)	☐	☐
7.10	(L1) Ensure that mobile devices require complex passwords (Simple Passwords = Blocked) (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.11	(L1) Ensure that devices connecting have AV and a local firewall enabled (Manual)	☐	☐
7.12	(L2) Ensure mobile device management policies are required for email profiles (Manual)	☐	☐
7.13	(L1) Ensure mobile devices require the use of a password (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
3/15/2022	1.5.0	UPDATE - Cannot audit LinkedIn Contact sync programmatically - Make Manual Ticket #15139
3/22/2022	1.5.0	UPDATE - API is available to assess Password Protection Ticket #14800
3/24/2022	1.5.0	UPDATE - Audit Procedure Wording for skype/teams Ticket #15103
3/24/2022	1.5.0	MOVED - Ensure Safe Links for Office Applications is Enabled moved under section 2 - ensure safe links for office apps. Ticket #15026
3/24/2022	1.5.0	MOVED - What is difference between the checks 4.5 and 2.3 ? (Safe Links for Exchange and Office Apps) Ticket #14991
5/17/2022	1.5.0	UPDATE - Safe Links Policy cmdlet: the parameter 'IsEnabled' is no longer supported. Ticket #15493
5/17/2022	1.5.0	UPDATE - Remove AdminAuditLogEnabled - ON-PREM only command Ticket #15109
5/20/2022	1.5.0	UPDATE - Audit DLP for Teams via PowerShell Ticket #14990
6/27/2022	1.5.0	UPDATE - Parameter AllowClickThrough is deprecated for SafeLinksPolicy Ticket #14992
7/25/2022	1.5.0	UPDATE - PowerShell cmdlet for assessing password hash sync Ticket #15022

Date	Version	Changes for this version
7/28/2022	1.5.0	UPDATE - Only works in the new Exchange Admin center, Fixed PS remediation Ticket #15972
8/2/2022	1.5.0	UPDATE - Clarify breadth of report Ticket #16097
8/4/2022	1.5.0	UPDATE - PowerShell guidance, Role Name to Role Object ID Ticket #16125
8/4/2022	1.5.0	UPDATE - Missing a step Ticket #15967
8/4/2022	1.5.0	REMOVE - Ensure modern authentication for Skype for Business Online is enabled Ticket #15719
8/5/2022	1.5.0	UPDATE - Improve PowerShell Audit Procedure guidance Ticket #15970
8/5/2022	1.5.0	UPDATE - Block OneDrive, clarify scope and accuracy of recommendation Ticket #16147
8/5/2022	1.5.0	UPDATE - PS cmdlet correction Ticket #16140
8/8/2022	1.5.0	UPDATE - DLP settings found in SecureScore Portal/API Ticket #13747
8/8/2022	1.5.0	UPDATE - 'Ensure the option to stay signed in' Audit and Remediation steps Ticket #16016
8/12/2022	1.5.0	UPDATE - Provide more detailed path for audit Ticket #15968
8/12/2022	1.5.0	UPDATE - Safe Links Audit+Remediation Ticket #16025

Date	Version	Changes for this version
8/12/2022	1.5.0	UPDATE - Connect-EXOPSSession V1 cmdlet replaced with V2 Connect-ExchangeOnline Ticket #15942
8/12/2022	1.5.0	UPDATE - Ensure the spoofed domains report is reviewed weekly Ticket #15317
8/12/2022	1.5.0	UPDATE - Microsoft Compliance became Microsoft Purview Ticket #15432
8/12/2022	1.5.0	UPDATE - Fix rationale Ticket #16107
8/15/2022	1.5.0	UPDATE - Role group changes procedures Ticket #16037
8/15/2022	1.5.0	UPDATE - Password hash sync audit procedure Ticket #16184
8/15/2022	1.5.0	UPDATE - change 'unlicensed' to 'un-assigned' to clarify the point that 'apps' are not assigned. Ticket #15015
8/15/2022	1.5.0	UPDATE - Implement Spam Filter Policy w/transport rule to simplify Ticket #14642
8/15/2022	1.5.0	UPDATE - Modern Authentication Clients option no longer listed Ticket #15318
8/15/2022	1.5.0	REMOVE - Non-Owners Report is deprecated Ticket #16195
8/16/2022	1.5.0	UPDATE - Ensure notifications for internal users sending malware is Enabled should be check for Default Policy or for all polices Ticket #15725
8/18/2022	1.5.0	UPDATE - Ensure Safe Links for Office Applications is Enabled Ticket #15482