CIS Benchmarks

CIS Microsoft 365 Foundations Benchmark

v1.1.0 - 12-20-2019

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

This document, Security Configuration Benchmark for Microsoft 365, provides prescriptive guidance for establishing a secure configuration posture for Microsoft 365 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 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.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. 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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **E3 Level 1**
- **E3 Level 2**
- **E5 Level 1**
- **E5 Level 2**

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
Jordan Rakoske
Gururaj Pandurangi
Shamir Charania
Sean Sweeney
Karen Scarfone
Jon Wall
Himalay Kondekar
Phil White

Editor
Dan Menicucci
Brandon Cox

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 (Scored)

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 Administrator
- User Management 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.

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 `Conditional Access` on the left side navigation.
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 `Conditional Access` on the left side navigation.
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:

Version 7

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 (Scored)

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 each day. 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.

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 `Conditional Access` on the left side navigation.
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) 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 all users` policy 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 `Conditional Access` on the left side navigation.
4. Click `New policy`
5. Select `Cloud apps or actions` > `All cloud apps` (and don't exclude any apps)
6. `Access Controls` > `Grant` > `Require multi-factor authentication` (and nothing else)
7. `Conditions` > `Client Apps` > `Configure` (Yes) > Explicitly select `Browser`, `Mobile apps and desktop clients`, `Modern authentication clients`, `Exchange ActiveSync clients`, and `Other clients`
8. Leave all other conditions blank
9. Make sure the policy is enabled
10. Create

Default Value:

Disabled

CIS Controls:

Version 7

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 (Scored)

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.

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.

Audit:

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

1. Select `Users` > `Active Users`.
2. Set `Views` to `Global Admins`.
3. 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:

```
$role = Get-MsolRole -RoleName "Company Administrator"
Get-MsolRoleMember -RoleObjectId $role.objectid
```

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. Select `Users` > `Active Users`.
2. Set `Views` to `Global Admins`.
3. To create a new Global Admin:
    1. Select `Add Users`.
    2. Enter User Information.
    3. Select `Roles`.
    4. Select `Global Administrator`.
    5. Click `Add`.
4. To remove Global Admins:
    1. Select User.
    2. Select `Edit` under `Roles`.
    3. Select `Customized administrator` and chose appropriate role.
    4. Click `Save`.

CIS Controls:

Version 7

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 (Scored)

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.

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.

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` under `Users - All users`.
4. On the Properties page, ensure that `All` is selected under `Self service password reset enabled`.

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

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

Remediation:

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

1. Choose `Settings` > `Security & privacy`.
2. Choose the link to go to the `Azure admin center`.
3. Choose `Users and groups` > `Password reset`.
4. On the Properties page, set the value to `All` is selected under `Self service password reset enabled`, and then choose `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

1.1.5 (L1) Ensure that password protection is enabled for Active Directory in hybrid environments (Scored)

Profile Applicability:

- E3 Level 1

Description:

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

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.

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 `Authentication methods` under `Security` on the left side navigation.
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

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 `Authentication methods` under `Security` on the left side navigation.
5. Select `Password protection` and toggle `Enable password protection on Windows Server Active Directory` to `Yes` and `Mode` to `Enforced`

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

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.

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 `Conditional Access` under `Security` on the left side navigation.
4. Verify that either the policy `Baseline policy: Block legacy authentication (Preview)` is enabled or find another with the following settings enabled:
    - Under `Client apps (preview)` ensure that `Mobile apps and desktop clients` and `Other clients` are checked
    - Under `Access controls` the `Grant` is set to `Block access`
    - Under `Assignments` that `All users` and `All cloud apps` are selected

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 `Conditional Access` under `Security` on the left side navigation.
4. Create a new policy by selecting `New policy`.
5. Set the following conditions within the policy.
    - Under `Client apps (preview)` enable the settings for `Mobile apps and desktop clients` and `Other clients`
    - Under `Access controls` set the `Grant` section to `Block access`
    - Under `Assignments` enable `All users` and `All cloud apps`
    - 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.

Impact:

Enabling this setting will prevent users from connecting with older versions of Office, ActiveSync or using protocols like IMAP, POP or SMTP.

Default Value:

Legacy authentication is enabled by default.

1.1.7 (L1) Ensure that password hash sync is enabled for resiliency and leaked credential detection (Not Scored)

Profile Applicability:

- E3 Level 1

Description:

Ensure that password hash sync is enabled for resiliency and leaked credential detection.

Rationale:

Password hash synchronization is one of the sign-in methods used to accomplish hybrid identity. 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. Password hash synchronization helps by reducing the number of passwords your users need to maintain to just one. Enabling password hash synchronization also allows for leaked credential reporting. It can also be used as a backup authentication method when federation is used, if the federation provider fails.

Audit:

To verify if Password Hash Sync is enabled, use 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
```

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`.

Impact:

Enabling this setting will prevent users from connecting with older versions of Office, ActiveSync or using protocols like IMAP, POP or SMTP.

1.1.8 (L1) Enabled Identity Protection to identify anomalous logon behavior (Not Scored)

Profile Applicability:

- E5 Level 1

Description:

Azure Active Directory Identity Protection monitors account behaviors and enables organizations to configure automated responses to detected suspicious actions related to user identities.

Rationale:

Azure Active Directory Identity Protection helps to discover at risk or compromised accounts in your environment. Identity based attacks continue to be a top source for breaches. Enabling Identity Protection not only helps to monitor and provide reporting, but also helps to automatically respond to identity based risks.

Audit:

To verify if Azure Active Directory Identity Protection is enabled, 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 `Marketplace`.
3. In the applications list, click `Identity`.
4. Click `Azure AD Identity Protection`.
5. On the `Azure AD Identity Protection` blade, validate that the feature has been enabled.

Remediation:

To setup Azure Active Directory Identity Protection, 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 `Marketplace`.
3. In the applications list, click `Identity`.
4. Click `Azure AD Identity Protection`.
5. On the `Azure AD Identity Protection` blade, click `Create`.

1.1.9 (L2) Enable Azure AD Identity Protection sign-in risk policies (Not Scored)

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.

Audit:

To verify if a Sign-In risk policy is enabled, 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 Identity Protection`.
3. Under `Configure` click on `Sign-in risk policy`.
4. Review the settings and ensure that `Enforce Policy` is set to `On`

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

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

Remediation:

To configure a Sign-In risk policy, 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 Identity Protection`.
3. Under `Configure` click on `Sign-in risk policy`.
4. Under `Assignments` ensure that policy is applied to `All users` or the scope of users appropriate
5. Under `Assignments` choose `Conditions` and the appropriate `Sign-in risk` level
6. Under `Controls`, select `Access` and choose `Allow access` and `Require multi-factor authentication`
7. Ensure that `Enforce Policy` is set to `On`

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.

1.1.10 (L2) Enable Azure AD Identity Protection user risk policies (Not Scored)

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.

Audit:

To verify if a User Risk policy is enabled, 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 Identity Protection`.
3. Under `Configure` click on `User risk policy`.
4. Review the settings and ensure that `Enforce Policy` is set to `On`

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

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

Remediation:

To configure a User risk policy, 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 Identity Protection`.
3. Under `Configure` click on `User risk policy`.
4. Under `Assignments` ensure that policy is applied to `All users` or the scope of users appropriate
5. Under `Assignments` choose `Conditions` and the appropriate `User risk` level
6. Under `Controls`, select `Access` and choose `Allow access` and `Require password change`
7. Ensure that `Enforce Policy` is set to `On`

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. Thus, it is important to configure the MFA registration policy for all users who are a part of the user risk policy to ensure that they have registered MFA.

1.1.11 (L2) Use Just In Time privileged access to Office 365 roles (Not Scored)

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.

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
```

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. Thus, it is important to configure the MFA registration policy for all users who are a part of the user risk policy to ensure that they have registered MFA.

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

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.

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-EXOPSSession`.
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-EXOPSSession`.
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:

Version 7

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.

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 Skype for Business Online is enabled (Scored)

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 Skype for Business, the Skype for Business client uses modern authentication to log in to Skype for Business Online.

Rationale:

Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by Skype for Business Online clients. Enabling modern authentication for Skype for Business Online ensures strong authentication mechanisms are used when establishing sessions between clients and Skype for Business Online.

Audit:

To verify modern authentication is enabled, use the Skype for Business Online PowerShell Module:

1. Connect to Skype for Business Online using the following Powershell commands:

```
Import-Module SkypeOnlineConnector
$sfbSession = New-CsOnlineSession
Import-PSSession $sfbSession
```

2. Run the following PowerShell command to verify that modern authentication is enabled:

```
Get-CsOAuthConfiguration |fl ClientAdalAuthOverride
```

3. Verify that `ClientAdalAuthOverride` is set to `Allowed`.

Remediation:

To enable modern authentication, use the Skype for Business Online PowerShell Module:

1. Connect to Skype for Business Online using the following Powershell commands:

```
Import-Module SkypeOnlineConnector
$sfbSession = New-CsOnlineSession
Import-PSSession $sfbSession
```

2. Run the following PowerShell command to verify that modern authentication is enabled:

```
Set-CsOAuthConfiguration -ClientAdalAuthOverride Allowed
```

References:

1. https://social.technet.microsoft.com/wiki/contents/articles/34339.skype-for-business-online-enable-your-tenant-for-modern-authentication.aspx

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

1.4 (L1) Ensure modern authentication for SharePoint applications is required (Scored)

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.

Audit:

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

1. Select `SharePoint` under `Admin centers`.
2. In the `SharePoint Admin Center`, select `Access Control`.
3. Verify that `Apps that don't use modern authentication` is set to `Block`.

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. Select `SharePoint` under `Admin centers`.
2. In the `SharePoint Admin Center`, select `Access Control`.
3. Set `Apps that don't use modern authentication` to `Block`.
4. Click `OK`.

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
```

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access

Use multi-factor authentication and encrypted channels for all administrative account access.

1.5 (L1) Ensure that Office 365 Passwords Are Not Set to Expire (Scored)

Profile Applicability:

- E3 Level 1

Description:

Review the password expiration policy, to ensure that user passwords in Office 365 are not set to expire.

Rationale:

NIST has updated their recommendation 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.

Audit:

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

1. Go to `Settings` > `Security & Privacy`.
2. Under the `Password Policy` section, ensure that `Days before passwords expire` is `Never`

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. Go to `Settings` > `Security & Privacy`.
2. Click `Edit` next to `Password Policy`.
3. Ensure that `Set user passwords to never expire` is set to `On`.

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
```

2 Application Permissions

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

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.

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`.

Default Value:

Yes

CIS Controls:

Version 7

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 (Scored)

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.

Audit:

To verify calendar details sharing with external users is disabled, use the Microsoft 365 Admin Center:

1. Select `Admin Center` and Click `Settings`.
2. Click `Services and add-ins`.
3. Click `Calendar`.
4. Verify `Let your users share their calendars with external users who have O365 or Exchange` is set to `Off`.

To verify calendar details sharing with external users is disabled, use the Exchange Online PowerShell Module:

1. Connect to Exchange Online using `Connect-EXOPSSession`.
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 `Settings`.
2. Click `Services and add-ins`.
3. Click `Calendar`.
4. Set `Let your users share their calendars with external users who have O365 or Exchange` to `Off`.
5. Click `Save`.

To disabled calendar details sharing with external users policy, use the Exchange Online PowerShell Module:

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

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

Default Value:

On

2.3 (L2) Ensure O365 ATP SafeLinks for Office Applications is Enabled (Scored)

Profile Applicability:

- E5 Level 2

Description:

Enabling the Advanced Threat Protection (ATP) Safe Links policy for Office applications allows URL's that existing inside of Office documents opened by Office, Office Online and Office mobile to be processed against ATP time-of-click verification.

Rationale:

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

Audit:

To verify the ATP Safe Links policy for Office is enabled, use the Microsoft 365 Admin Center:

1. Click `Security` under `Admin centers` to open the `Microsoft 365 Security Center`.
2. Navigate to `Policies` and select `ATP safe links (Office 365)`.
3. Navigate to `Threat management` and select `Policy`
4. Select `ATP Safe Links`
5. Under `Policies that apply to the entire organization`, click on the `Default` policy and click `Edit`.
6. Under `Settings that apply to content except email`:
    1. Verify that `Office 365 ProPlus, Office for iOS and Android` is `checked` under `Use safe links in:`.
    2. Verify that `Do not let users click through safe links to original URL` is `checked`.

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

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

```
Get-AtpPolicyForO365 | fl
Name,AllowClickThrough,EnableSafeLinksForClients,EnableSafeLinksForWebAccessC
ompanion,EnableSafeLinksForO365Clients
```

3. Verify the value for `AllowClickThrough` is set to `False` and the rest are set for `True`.

Remediation:

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

1. Click `Security` under `Admin centers` to open the `Microsoft 365 Security Center`.
2. Navigate to `Policies` and select `ATP safe links (Office 365)`.
3. Navigate to `Threat management` and select `Policy`
4. Select `ATP Safe Links`
5. Under `Policies that apply to the entire organization`, click on the `Default` policy and click `Edit`.
6. Under `Settings that apply to content except email`:
    1. Ensure that `Office 365 ProPlus, Office for iOS and Android` is `checked`.
    2. Ensure that `Do not let users click through safe links to original URL` is `checked`.

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

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

```
Set-AtpPolicyForO365 -AllowClickThrough $False -EnableSafeLinksForClients
$true
```

CIS Controls:

Version 7

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 Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams is Enabled (Scored)

Profile Applicability:

- E5 Level 2

Description:

Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams scans these services for malicious files.

Rationale:

Office 365 ATP 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.

Audit:

To verify that O365 ATP is enabled for SharePoint, OneDrive, and Microsoft Teams, use the Microsoft 365 Admin Center:

1. Click `Security` under `Admin centers` to open the `Microsoft 365 Security Center`.
2. Navigate to `Policies` and select `ATP safe attachments (Office 365)`.
3. Verify that `Turn on ATP` for `SharePoint`, `OneDrive`, and `Microsoft Teams` is `checked`.

To verify that O365 ATP is enabled for SharePoint, OneDrive, and Microsoft Teams, use the Exchange Online PowerShell Module:

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

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

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

Remediation:

To enable O365 ATP for SharePoint, OneDrive, and Microsoft Teams, use the Microsoft 365 Admin Center:

1. Click `Security` under `Admin centers` to open the `Microsoft 365 Security Center`.
2. Navigate to `Policies` and select `ATP safe attachments (Office 365)`.
3. Ensure that `Turn on ATP` for `SharePoint`, `OneDrive`, and `Microsoft Teams` is `checked`.

To enable O365 ATP for SharePoint, OneDrive, and Microsoft Teams, use the Exchange Online PowerShell Module:

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

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

CIS Controls:

Version 7

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.

3 Data Management

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

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.

Audit:

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

1. Browse to the `Microsoft 365 admin center`.
2. Under `Settings` choose `Security & privacy`.
3. Click `Edit` next to `Customer Lockbox`.
4. Check that the value of `Require approval for all data access requests` is set to `On`.

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 Microsoft Online PowerShell Module:

1. Run Microsoft Online PowerShell Module.
2. Connect using `Connect-MSOnline`.
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. Under `Settings` choose `Security & privacy`.
3. Click `Edit` next to `Customer Lockbox`.
4. Click the box next to `Require approval for all data access requests` to enable the feature and then click `Save`.

Default Value:

Disabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

13.4 Only Allow Access to Authorized Cloud Storage or Email Providers
Only allow access to authorized cloud storage or email providers.

3.2 (L2) Ensure SharePoint Online data classification policies are set up and used (Not Scored)

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.

Audit:

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

1. Select `Compliance` under `Admin centers` to open the `Microsoft 365 Compliance Center`.
2. Under `Classification` choose `Labels`
3. Choose `Sensitivity labels`
4. Ensure Labels exist.

Remediation:

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

1. Select `Compliance` under `Admin centers` to open the `Microsoft 365 Compliance Center`.
2. Under `Classification` choose `Labels`
3. Choose `Retention labels`
4. Click `Create` to create a label.

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

Profile Applicability:

- E3 Level 2

Description:

Disable the ability of your users to communicate via Skype or Teams with users outside your organization.

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. Attackers may be able to pretend to be someone your user knows and then send malicious links or attachments, resulting in an account breach or leaked information.

Audit:

To verify Skype for Business and Teams access with external users is disabled, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` choose `Teams`.
2. Select `Org Wide Settings` and `External Access`.
3. Verify that `Users can communicate with Skype for Business and Teams users` is set to `Off`.
4. Verify that `Skype for Business users can communicate with Skype users` is set to `Off`.

Remediation:

To disable Skype for Business and Teams access with external users, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` choose `Teams`.
2. Select `Org Wide Settings` and `External Access`.
3. Set `Users can communicate with Skype for Business and Teams users` to `Off`.
4. Set `Skype for Business users can communicate with Skype users` to `Off`.

Default Value:

On

CIS Controls:

Version 7

12.4 Deny Communication over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

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

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.

Audit:

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

1. Select `Compliance` under `Admin centers`.
2. From the `Microsoft 365 compliance center` choose `Policies` select `Data loss prevention`
3. Select `Data loss prevention`.
4. Click `Policy`.
5. Verify that policies exist and are enabled

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

1. Login to 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. Click on `Apply Data Loss Prevention policies` policy to check if policies are being applied.
3. Check the number of data loss prevention policy applied

To verify the DLP feature is enabled, use the REST API:

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

Remediation:

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

1. Select `Compliance` under `Admin centers`.
2. From the `Microsoft 365 compliance center` choose `Policies` select `Data loss prevention`
3. Select `Data loss prevention`.
4. Click `Policy`.
5. Click `Create a policy`.

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

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.

Audit:

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

1. Select `Compliance` under `Admin centers`.
2. From the `Microsoft 365 compliance center` choose `Policies` select `Data loss prevention`
3. Select `Data loss prevention`.
4. Click `Policy`.
5. Verify that policies exist and are enabled
6. Ensure that the policies include the location `Teams chat and channel messages`

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

1. Login to 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. Click on `Apply Data Loss Prevention policies` policy to check if policies are being applied.
3. Check the number of data loss prevention policy applied

To verify the DLP feature is enabled, use the REST API:

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

Remediation:

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

1. Select `Compliance` under `Admin centers`.
2. From the `Microsoft 365 compliance center` choose `Policies` select `Data loss prevention`
3. Select `Data loss prevention`.
4. Click `Policy`.
5. Click `Create a policy`.
6. Either start with a template or create a custom policy.
7. Provide a `Name` for your policy
8. 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.
9. Ensure that the proper DLP rules are created for the type of content to be detected and what actions should be taken.

Impact:

Enabling a Teams DLP policy will allow sensitive data in Teams channels or chat messages to be detected or blocked.

Default Value:

This is not enabled by default.

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

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.

Audit:

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

1. Select `SharePoint` under `Admin centers`.
2. Select `Sharing` under `Policies`.
3. Under `Advanced settings for external sharing`, 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. Select `SharePoint` under `Admin centers`.
2. Select `Sharing` under `Policies`.
3. Set `Allow guests to share items they don't own` to `Enabled`.
4. Click `OK`.

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-MSOLService`.
2. Run the following SharePoint Online PowerShell command:

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

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.7 (L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services (Not Scored)

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.

Rationale:

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

Audit:

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

1. Under `Admin Centers` choose `Teams`.
2. Under `Org-wide settings` select `Teams settings`.
3. Verify `Files` is set to `On` for only authorized cloud storage options.

Remediation:

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

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

Default Value:

On

CIS Controls:

Version 7

13 Data Protection
Data Protection

3.8 (L1) Ensure that Cloud App Security is enabled (Not Scored)

Profile Applicability:

- E5 Level 1

Description:

Ensure that the Microsoft Cloud App Security console is enabled and collecting data from Office 365.

Rationale:

Cloud App Security Console gives you insights into suspicious activity so you can investigate situations that are potentially problematic and take action to address security issues. With Cloud App Security Console, you can set up alerts by using policies to notify you about anomalous and suspicious activity. You also have access to productivity app discovery, which lets you use the information from your organization's log files to understand and act on your users' app usage in Office 365 and other cloud apps.

Audit:

To verify that Cloud App Security is enabled, use the Microsoft 365 Admin Center:

1. Under `Admin Centers` choose `Security`.
2. Under `More Resources` select `Microsoft Cloud App Security`.
3. Under `General Dashboard` verify that activities are being monitored

This information is also available via the Microsoft Graph Security API, by looking at the `CloudApplicationSecurityEnabled` controlName:

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

Remediation:

To setup Cloud App Security, use the Security & Compliance Center:

1. Go to the `Security & Compliance Center` (protection.office.com)
2. Expand `Alerts` and choose `Manage advanced alerts`
3. Ensure that `Turn on Office 365 Cloud App Security` is checked and click `Go to Office 365 Cloud App Security`

Impact:

Enabling this tool will provide administrators insights about how cloud services are being used. Users will not be impacted by enabling the service.

Default Value:

On

CIS Controls:

Version 7

13 Data Protection
Data Protection

4 Email Security / Exchange Online

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

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.

Audit:

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

1. Navigate to the Exchange Admin Center and click `Protection` > `Malware Filter`.
2. Edit the `Default` profile.
3. In the Edit tab under `Settings`, verify that the `Common Attachment Types Filter` has the value of 'On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).`

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

1. Connect to Exchange Online using `Connect-EXOPSSession`.
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 Exchange Admin Center and click `Protection` > `Malware Filter`.
2. Edit the `Default` profile.
3. Click on the Edit tab under `Settings`. Ensure that the `Common Attachment Types Filter` has the value of `On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).`

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

1. Connect to Exchange Online using `Connect-EXOPSSession`.
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:

Version 7

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 correctly (Scored)

Profile Applicability:

- E3 Level 1

Description:

You should set your 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.

Audit:

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

1. Select `Exchange`.
2. Navigate to `Protection` > `Outbound Spam`.
3. Edit the `Default` profile.
4. Select `Outbound spam preferences`.
5. Verify both `Send a copy of all suspicious outbound email messages to the following email address or addresses` and `Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam` are checked and the email addresses to be notified are correct.

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

1. Connect to Exchange Online using `Connect-EXOPSSession`.
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. Select `Exchange`.
2. Navigate to `Protection` > `Outbound Spam`.
3. Edit the `Default` profile.
4. Select `Outbound spam preferences`.
5. Check `Send a copy of all suspicious outbound email messages to the following email address or addresses` and enter the email address(es).
6. Check `Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam` and enter the email address(es).
7. Click `Save`.

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

1. Connect to Exchange Online using `Connect-EXOPSSession`.
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:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.3 (L1) Ensure mail transport rules do not forward email to external domains (Scored)

Profile Applicability:

- E3 Level 1

Description:

You should set your Exchange Online mail transport rules to not forward email to domains not registered in your tenancy.

Rationale:

Attackers often create these rules to exfiltrate data from your tenancy.

Audit:

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 are forwarding email to external domains, you can also use the Exchange Online PowerShell module:

1. Connect to Exchange online using Connect-EXOPSSession
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

Remediation:

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.

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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

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.

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-EXOPSSession
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.

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.5 (L2) Ensure the Client Rules Forwarding Block is enabled (Scored)

Profile Applicability:

- E3 Level 2

Description:

You should enable the Client Rules Forwarding Block, which prevents the use of any client-side rules that forward email to an external domain.

Rationale:

The use of client-side forwarding rules to exfiltrate data to external recipients is an increasingly used vector for data exfiltration by bad actors.

Audit:

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-EXOPSSession`.
2. Run the following Exchange Online PowerShell command:

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

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

Remediation:

To enable the Client Rules Forwarding Block, use the Microsoft 365 Admin Center

1. Go to `Security and Compliance`.
2. Go to `Secure Score`.
3. Select `Client Rules Forwarding Block`.
4. Select `Learn More`.
5. Select `Apply`.

To create the Client Rules Forwarding Block, use the Exchange Online PowerShell Module:

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

```
$rejectMessageText = "To improve security, auto-forwarding rules to external
addresses has 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 1 -
SentToScope NotInOrganization -FromScope InOrganization -MessageTypeMatches
AutoForward -RejectMessageEnhancedStatusCode 5.7.1 -RejectMessageReasonText
$rejectMessageText
```

3. Verify that `Client Rules To External Block` gets created.

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.6 (L2) Ensure the Advanced Threat Protection Safe Links policy is enabled (Scored)

Profile Applicability:

- E5 Level 2

Description:

Enabling the Advanced Threat Protection (ATP) Safe Links policy allows email messages that include URLs to be processed and rewritten if required. ATP Safe Links provides time-of-click verification of web addresses in email messages and Office documents.

Rationale:

ATP Safe Links extends phishing protection to include redirecting all email hyperlinks through a forwarding service which will block malicious ones even after the email has been delivered to the end user.

Audit:

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

1. Click `Security & Compliance` to open the Security & Compliance portal.
2. Navigate to `Threat management` > `Policy` > `ATP Safe Links`.
3. Under `Policies that apply to specific recipients`, verify that at least one policy exists and click `Edit`.
4. Select `Settings`.
5. Verify `Select the action for unknown potentially malicious URLs in messages` is set to `On`.
6. Verify that at least both `Do not let users click through safe links to original URL` and `Apply safe links to messages sent within the organization` are checked.

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

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

```
Get-SafeLinksPolicy | Select-Object Name, IsEnabled, ScanUrls,
EnableForInternalSenders, AllowClickThrough
```

3. Verify the values for `IsEnabled` and `ScanUrls` are set to `True`, and `AllowClickThrough` is set to `False`.

Remediation:

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

1. Click `Security & Compliance` to open the Security & Compliance portal.
2. Navigate to `Threat management` > `Policy` > `ATP Safe Links`.
3. Under `Policies that apply to specific recipients`, verify that at least one policy exists and click `Edit`, or create a new policy.
4. Select `Settings`.
5. Select `On` for `Select the action for unknown potentially malicious URLs in messages`.
6. Check `Use safe attachments to scan downloadable content`.
7. Check `Apply safe links to messages sent within the organization`.
8. Check `Do not let users click through safe links to original URL`
9. Click `Save`.

To enable the ATP Safe Links policy, use the Exchange Online PowerShell Module:

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

```
$SafeLinksPolicy = Get-SafeLinksPolicy

If (-not $SafeLinksPolicy.Identity) {
  $SafeLinksPolicy = New-SafeLinksPolicy -Name "Safe Links"
}

Set-SafeLinksPolicy -Identity $SafeLinksPolicy.Identity -IsEnabled $True -
ScanUrls $True -EnableForInternalSenders $True -AllowClickThrough $False
```

Default Value:

disabled

References:

1. https://docs.microsoft.com/en-us/office365/securitycompliance/atp-safe-links
2. https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies

Notes:

ATP Safe Links features are part of Advanced Threat Protection, which is included in Office 365 Enterprise E5, Microsoft 365 Business, and Microsoft 365 Enterprise.

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.7 (L2) Ensure the Advanced Threat Protection Safe Attachments policy is enabled (Scored)

Profile Applicability:

- E5 Level 2

Description:

Enabling the Advanced Threat Protection 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.

Audit:

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

1. Click `Security & Compliance` to open the Security & Compliance portal.
2. Navigate to `Threat management` > `Policy` > `ATP Safe Attachments`.
3. Verify that at least one policy exists.

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

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

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

Remediation:

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

1. Click `Security & Compliance` to open the Security & Compliance portal.
2. Navigate to `Threat management` > `Policy` > `ATP Safe Attach`.
3. Click `+`.
4. Enter Policy Name and Description.
5. Select `Block`, `Monitor` or `Dynamic Delivery`.
6. Select `Save`.

Impact:

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

Default Value:

disabled

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.8 (L2) Ensure basic authentication for Exchange Online is disabled (Scored)

Profile Applicability:

- E3 Level 2

Description:

Basic authentication may allow users to access Exchange Online using legacy or unapproved email clients that do not support modern authentication mechanisms, such as multifactor authentication.

Rationale:

Disabling basic authentication prevents use of legacy and unapproved email clients with weaker authentication mechanisms that would increase the risk of email account credential compromise.

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-EXOPSSession`.
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 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-EXOPSSession`.
3. Run the following PowerShell command:

```
$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 -AllowBasicAuthRest:$false -
AllowBasicAuthRpc:$false -AllowBasicAuthSmtp:$false -
AllowBasicAuthWebServices:$false

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

Impact:

Blocking basic authentication will block the following legacy Exchange Online features:

- App passwords: An app password is a code that gives an app or device permission to access your Microsoft 365 account. If multi-factor authentication is enabled for your organization and you're using apps that connect to your Microsoft 365 account, you'll need to generate an app password so the app can connect to Microsoft 365. For example, if you're using Outlook 2016 or earlier with Microsoft 365, an app password is required.
- Availability address spaces: These contain a service account that's used to share calendar free/busy information in hybrid and federated deployments. The service account authenticates with a username and password, so blocking Basic authentication blocks the authentication flow.

Default Value:

false

References:

1. https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online?redirectSourcePath=%252fen-us%252farticle%252fdisable-basic-authentication-in-exchange-online-bba2059a-7242-41d0-bb3f-baaf7ec1abd7

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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.

4.9 (L1) Ensure that an anti-phishing policy has been created (Scored)

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.

Audit:

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

1. Select `Security and Compliance`.
2. Select `Threat Management` and `Policy`.
3. Select `ATP Anti-phishing`.
4. Verify a policy exists.

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

1. Connect to Exchange Online service using `Connect-EXOPSSession`.
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. Select `Security and Compliance`.
2. Select `Threat Management` and `Policy`.
3. Select `ATP Anti-phishing`.
4. Click `Create` to create a anti-phishing policy.

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

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

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

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.10 (L1) Ensure that DKIM is enabled for all Exchange Online Domains (Scored)

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 by 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.

Audit:

To review if DKIM is enabled, use the Microsoft 365 Admin Center:

1. Launch the `Security & Compliance` Admin Center
2. Click `Threat Management` > `Policy`
3. 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-EXOPSSession`.
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
```

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

2. After the DNS records are created, enable DKIM signing in the Office 365 Admin Portal
3. Launch the `Security & Compliance` Admin Center.
4. Click `Threat Management` > `Policy`.
5. Click `DKIM`.
6. 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-EXOPSSession`.
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

4.11 (L1) Ensure that SPF records are published for all Exchange Domains (Not Scored)

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.

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:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.12 (L1) Ensure DMARC Records for all Exchange Online domains are published (Not Scored)

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.

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:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.13 (L1) Ensure notifications for internal users sending malware is Enabled (Scored)

Profile Applicability:

- E3 Level 1

Description:

Setup the EOP malware filter to notify administrators if internal senders are blocked for sending malware.

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.

Audit:

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

1. Launch the `Security & Compliance Admin Center`.
2. Go to `Threat Management` > `Policy` > `Anti-malware`.
3. Ensure the setting `Notify administrator about undelivered messages from internal senders` is `checked` 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-exopssession commandlet`.
2. Run the following command:

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

Remediation:

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

1. Launch the `Security & Compliance Admin Center`.
2. Go to `Threat Management` > `Policy` > `Anti-malware`.
3. Check the setting `Notify administrator about undelivered messages from internal senders` 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-exopssession commandlet`.
2. Run the following command:

```
set-MalwareFilterPolicy -EnableInternalSenderAdminNotifications $True -
InternalSenderAdminAddress admin@domain1.com
```

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

4.14 (L2) Ensure MailTips are enabled for end users (Scored)

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-EXOPSSession`
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-MSOnline`
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 (Scored)

Profile Applicability:

- E3 Level 1

Description:

When audit log search in the Microsoft 365 Security & Compliance Center 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 365 audit log search helps Office 365 back office teams to investigate activities for regular security operational or forensic purposes.

Audit:

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

1. Log in as an administrator.
2. Navigate to the `Office 365 security & compliance center` by going to https://protection.office.com
3. In the Security & Compliance Center, navigate to `Search` > `Audit log search`.
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 Microsoft 365 audit log search is enabled, use the Exchange Online PowerShell Module:

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

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

4. Verify the resulting values are `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 `Office 365 security & compliance center` by going to https://protection.office.com
3. In the Security & Compliance Center, navigate to `Search` > `Audit log search`.
4. Click `Start recording user and admin activities` next to the information warning at the top.
5. Click `Yes` on the dialog box to confirm.

To enable Microsoft 365 audit log search, use the Exchange Online PowerShell Module:

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

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

A message is displayed saying that it might take up to 60 minutes for the change to take effect. If an error appears, you may need to run `Enable-OrganizationCustomization` before disconnecting and trying the command again.

Default Value:

disabled

References:

1. https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off

CIS Controls:

Version 7

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 (Scored)

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 user 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:

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

Audit:

To verify mailbox auditing is enabled for all users, use the Exchange Online PowerShell Module:

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

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq
"UserMailbox"} | Format-Table Name, AuditEnabled
```

4. Verify `AuditEnabled` is set to `True` for all mailboxes.

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-EXOPSSession`.
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 -Filter {RecipientTypeDetails -eq
"UserMailbox" -or RecipientTypeDetails -eq "SharedMailbox" -or
RecipientTypeDetails -eq "RoomMailbox" -or RecipientTypeDetails -eq
"DiscoveryMailbox"} | Set-Mailbox -AuditEnabled $true -AuditLogAgeLimit 180 -
AuditAdmin $AuditAdmin -AuditDelegate $AuditDelegate -AuditOwner $AuditOwner
```

Default Value:

disabled

References:

1. https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing

CIS Controls:

Version 7

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 (Not Scored)

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 tenancy from a client IP address that has been recognized by Microsoft as an anonymous proxy IP address (such as a TOR network) -successful signins from users where two signins appeared to originate from different regions and the time between signins 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. Select `Risk events`.
4. Review by `Detection Type`.

To get risky sign-ins event report programatically, 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:

Version 7

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 (Not Scored)

Profile Applicability:

- E3 Level 2

Description:

You should review the Application Usage report at least weekly. This 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:

Version 7

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 (Not Scored)

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:

Version 7

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 (Not Scored)

Profile Applicability:

- E3 Level 1

Description:

User role group changes should be reviewed on a weekly basis to ensure no one has been improperly added to an administrative role.

Rationale:

Illicit role group changes could give an attacker elevated privileges to perform more dangerous and impactful things in your tenancy.

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. Go to `Security and Compliance Center`.
2. Select `Search` and then `Audit Log Search`.
3. Set `Activities` to `Added member to role`.
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-EXOPSSession`.
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

CIS Controls:

Version 7

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 (Not Scored)

Profile Applicability:

- E3 Level 1

Description:

You should review mail forwarding rules to external domains at least every week.

Rationale:

While there are lots of legitimate uses of mail forwarding rules, they are also a popular data exfiltration tactic for attackers. You should review them regularly to ensure your users' email is not being exfiltrated.

Audit:

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

Remediation:

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

1. Go to `Security and Compliance Center`.
2. Select `Mail Flow` and then `Dashboard`.
3. Review `Auto Forwarded Messages` on the dashboard.

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 by using `connect-exopssession`

```
$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:

Version 7

6.2 Activate audit logging

Ensure that local logging has been enabled on all systems and networking devices.

5.8 (L1) Ensure the Mailbox Access by Non-Owners Report is reviewed at least biweekly (Not Scored)

Profile Applicability:

- E3 Level 1

Description:

You should review the Mailbox Access by Non-Owners report at least every other week. This report shows which mailboxes have been accessed by someone other than the mailbox owner.

Rationale:

While there are many legitimate uses of delegate permissions, regularly reviewing that access can help prevent an external attacker from maintaining access for a long time, and can help discover malicious insider activity sooner.

Audit:

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

Remediation:

To review the report, perform the following steps using the Microsoft 365 Admin Center:

1. Click `Exchange`.
2. Click `Compliance Management` and `auditing`.
3. Select `Run a non-owner mailbox access report`.
4. Enter `Start Date` and `End Date`.
5. Change `Search for access by` field to `all non-owners`.
6. Select `Search`.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

5.9 (L1) Ensure the Malware Detections report is reviewed at least weekly (Not Scored)

Profile Applicability:

- E3 Level 1

Description:

You should review the Malware Detections report at least weekly. This report shows specific instances of Microsoft blocking a malware attachment from reaching your users.

Rationale:

While this report isn't strictly actionable, reviewing it will give you a sense of the overall volume of malware being targeted at your users, which may prompt you to adopt more aggressive malware 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 and Compliance`.
2. Select `Report` and `Dashboard`.
3. Review the `Malware Detected in Email` report.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

5.10 (L1) Ensure the Account Provisioning Activity report is reviewed at least weekly (Not Scored)

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 and Compliance Center`.
2. Select `Search` and then `Audit Log Search`.
3. Set `Activities` to `Added user`.
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-EXOPSSession`.
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:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

5.11 (L1) Ensure non-global administrator role group assignments are reviewed at least weekly (Not Scored)

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 and Compliance Center`.
2. Select `Search` and then `Audit Log Search`.
3. Set `Added member to Role` and `Removed a user from a directory role`
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

5.12 (L1) Ensure the spoofed domains report is review weekly (Not Scored)

Profile Applicability:

- E5 Level 1

Description:

Use spoof intelligence in the Security & Compliance 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 Advanced Threat Protection (ATP) 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.

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 and Compliance Center`.
2. Select `Threat Management` and then `Dashboard`.
3. Click `Spoofed domains that failed authentication over the past 30 days`.
4. Review.

To verify mailbox auditing is enabled for all users, use the Exchange Online PowerShell Module:

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

```
Get-PhishFilterPolicy -Detailed -SpoofAllowBlockList -SpoofType Internal
```

3. Review.

5.13 (L2) Ensure Microsoft 365 Cloud App Security is Enabled (Not Scored)

Profile Applicability:

- E3 Level 1

Description:

Enabling Microsoft 365 Cloud App Security 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 365 Cloud App Security is enabled, use the Microsoft 365 Admin Center:

1. Select `Security and Compliance`.
2. Select `Alerts`.
3. Select `Manage advanced alerts`.
4. Verify that `Turn on Microsoft 365 Cloud App Security` is selected.

To verify Microsoft 365 Cloud App Security is enabled, use the Microsoft 365 SecureScore Portal:

1. Login to 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. Click on `Enable Cloud App Security Console` policy to see the status of the Microsoft 365 Cloud App Security console.

To verify Microsoft 365 Cloud App Security is enabled, use the Microsoft 365 SecureScore REST API:

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

Remediation:

To enable Microsoft 365 Cloud App Security, use the Microsoft 365 Admin Center:

1. Select `Security and Compliance`.
2. Select `Alerts`.
3. Select `Manage advanced alerts`.
4. Check `Turn on Microsoft 365 Cloud App Security`.
5. Click `Go to Microsoft 365 Cloud App Security`.

5.14 (L1) Ensure the report of users who have had their email privileges restricted due to spamming is reviewed (Not Scored)

Profile Applicability:

- E3 Level 1

Description:

Review and unblock users who have been blocked for sending too many messages marked as spam/bulk.

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. Select `Security and Compliance`.
2. Select `Threat Management` and `Review`.
3. Click `Restricted Users`.
4. Review alerts and take appropriate action (unblocking) after account has been remediated.

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

5.15 (L1) Ensure Guest Users are reviewed at least biweekly (Not Scored)

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-MSOnline`
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

6 Storage

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

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.

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. Click `Sharing`.
3. Expand `Advanced external sharing by domain` and confirm that `Limit external sharing using domains` is checked.
4. Verify that `Allow sharing only with users from these domains` or `Don't allow sharing with users from these blocked domains` is set correctly along with an accurate list of approved or disallowed domains.

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. Select `Admin Centers` and `SharePoint`.
2. Click `Sharing`.
3. Expand `Advanced external sharing by domain` and confirm that `Limit external sharing using domains` is checked.
4. Toggle `Allow sharing only with users from these domains` or `Don't allow sharing with users from these blocked domains`.
5. Enter list of approved or disallowed domains.

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:

Version 7

13 Data Protection
Data Protection

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

Profile Applicability:

- E3 Level 2

Description:

You should prevent company data from OneDrive for Business from being synchronized to non-corporate managed devices.

Rationale:

Unmanaged devices pose a risk, since their security cannot be verified. 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.

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 `Admin Centers` and then `OneDrive`.
2. Click `Sync`.
3. Verify that `Allow syncing only on PCs joined to specific domains` is checked.
4. Verify that Domain GUIDs are listed in the box. Use the `Get-ADDomain` PowerShell command to obtain the GUID from each 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
TenantRestrictionsEnabled,AllowedDomainDomainList
```

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 `Admin Centers` and then `OneDrive`.
2. Click `Sync`.
3. Ensure that `Allow syncing only on PCs joined to specific domains` is checked.
4. Use the `Get-ADDomain` PowerShell command to obtain the GUID from each domain in your environment and add them to the box below.
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"
```

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.

Default Value:

This feature is not enabled by default.

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

Profile Applicability:

- E3 Level 1

Description:

You should restrict the length of time that anonymous access links are valid.

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.

Audit:

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

1. Select `Admin Centers` and `SharePoint`.
2. Click `Sharing`.
3. Click `These links must expire within this many days`.
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
```

Remediation:

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

1. Select `Admin Centers` and `SharePoint`.
2. Click `Sharing`.
3. Check `These links must expire within this many days`.
4. Set to the desired number of days, such as `30`.
5. Click `OK`.

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:

off

CIS Controls:

Version 7

13 Data Protection
Data Protection

7 Mobile Device Management

7.1 (L1) Ensure mobile device management polices are set to require advanced security configurations to protect from basic internet attacks (Not Scored)

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 internet attacks, 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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then select `Profiles`
3. Select `Create profile` to create a new profile. Select the appropriate Platform and settings from the configuration screens.

Impact:

This change will have a moderate impact on your users.

CIS Controls:

Version 7

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

7.2 (L1) Ensure that mobile device password reuse is prohibited (Not Scored)

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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then select `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`.

Impact:

This change will have a moderate user impact

Default Value:

Password reuse is not enforced by default.

CIS Controls:

Version 7

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

7.3 (L1) Ensure that mobile devices are set to never expire passwords (Not Scored)

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.

Audit:

To verify mobile device management profile, use the Microsoft 365 Admin Center:

1. Select `Device Management` under `Admin Centers`.
2. Select `Devices`, then `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 `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.

Impact:

This setting should not cause a noticeable impact to users

Default Value:

Password changes are not required by default

CIS Controls:

Version 7

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

7.4 (L1) Ensure that users cannot connect from devices that are jail broken or rooted (Not Scored)

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.

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 select `Policies`
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` is set to `Block`.

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 select `Policies`
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` is set to `Block`.

CIS Controls:

Version 7

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

7.5 (L2) Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise (Not Scored)

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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then select `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`.

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.

Default Value:

The default is to not wipe the device on multiple failed attempts.

CIS Controls:

Version 7

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

7.6 (L1) Ensure that mobile devices require a complex password to prevent brute force attacks (Not Scored)

Profile Applicability:

- E3 Level 1

Description:

You should require your users to use a complex password with 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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then select `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`.

Impact:

This change has a moderate user impact

Default Value:

Minimum password lengths are not enforced by default

CIS Controls:

Version 7

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

7.7 (L1) Ensure that settings are enable to lock devices after a period of inactivity to prevent unauthorized access (Not Scored)

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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then select `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`

Impact:

This setting has a low impact on users.

Default Value:

Screen locking is not enabled by default.

CIS Controls:

Version 7

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

7.8 (L1) Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data (Not Scored)

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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then select `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`.

Impact:

This setting should have no user impact, provided the device supports the feature.

Default Value:

Device encryption is not required by the O365 platform by default, although some mobile platforms are encrypted by default.

CIS Controls:

Version 7

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

7.9 (L1) Ensure that mobile devices require complex passwords to prevent brute force attacks (Not Scored)

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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then select `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`.

Impact:

This setting will have a moderate user impact

Default Value:

This setting is not enabled by default.

CIS Controls:

Version 7

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 to prevent brute force attacks (Not Scored)

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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device configuration` and then select `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`.

Impact:

This has a moderate impact on users

Default Value:

This setting is not enabled by default

CIS Controls:

Version 7

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

7.11 (L1) Ensure that devices connecting have AV and a local firewall enabled (Not Scored)

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.

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 select `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. Select `Device Management` under `Admin Centers`.
2. Select `Device compliance` and then select `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`.

7.12 (L2) Ensure mobile device management policies are required for email profiles (Not Scored)

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.

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 select `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 select `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`.

Impact:

This setting will have a moderate impact on users

Default Value:

This setting is not enabled by default

CIS Controls:

Version 7

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

7.13 (L1) Ensure mobile devices require the use of a password (Not Scored)

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.

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 select `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 select `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`.

Impact:

This change will require users to provide a password to unlock their mobile device after the timeout period expires

Default Value:

This setting is not enabled by default.

CIS Controls:

Version 7

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

Appendix: Summary Table

Control		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 (Scored)	☐	☐
1.1.2	(L2) Ensure multifactor authentication is enabled for all users in all roles (Scored)	☐	☐
1.1.3	(L1) Ensure that between two and four global admins are designated (Scored)	☐	☐
1.1.4	(L1) Ensure self-service password reset is enabled (Scored)	☐	☐
1.1.5	(L1) Ensure that password protection is enabled for Active Directory in hybrid environments (Scored)	☐	☐
1.1.6	(L1) Enable Conditional Access policies to block legacy authentication (Scored)	☐	☐
1.1.7	(L1) Ensure that password hash sync is enabled for resiliency and leaked credential detection (Not Scored)	☐	☐
1.1.8	(L1) Enabled Identity Protection to identify anomalous logon behavior (Not Scored)	☐	☐
1.1.9	(L2) Enable Azure AD Identity Protection sign-in risk policies (Not Scored)	☐	☐
1.1.10	(L2) Enable Azure AD Identity Protection user risk policies (Not Scored)	☐	☐
1.1.11	(L2) Use Just In Time privileged access to Office 365 roles (Not Scored)	☐	☐
1.2	(L1) Ensure modern authentication for Exchange Online is enabled (Scored)	☐	☐
1.3	(L1) Ensure modern authentication for Skype for Business Online is enabled (Scored)	☐	☐
1.4	(L1) Ensure modern authentication for SharePoint applications is required (Scored)	☐	☐
1.5	(L1) Ensure that Office 365 Passwords Are Not Set to Expire (Scored)	☐	☐
2	**Application Permissions**		
2.1	(L2) Ensure third party integrated applications are not allowed (Not Scored)	☐	☐
2.2	(L2) Ensure calendar details sharing with external users is disabled (Scored)	☐	☐
2.3	(L2) Ensure O365 ATP SafeLinks for Office Applications is Enabled (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
2.4	(L2) Ensure Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams is Enabled (Scored)	☐	☐
3	**Data Management**		
3.1	(L2) Ensure the customer lockbox feature is enabled (Scored)	☐	☐
3.2	(L2) Ensure SharePoint Online data classification policies are set up and used (Not Scored)	☐	☐
3.3	(L2) Ensure external domains are not allowed in Skype or Teams (Not Scored)	☐	☐
3.4	(L1) Ensure DLP policies are enabled (Scored)	☐	☐
3.5	(L1) Ensure DLP policies are enabled for Microsoft Teams (Scored)	☐	☐
3.6	(L2) Ensure that external users cannot share files, folders, and sites they do not own (Scored)	☐	☐
3.7	(L2) Ensure external file sharing in Teams is enabled for only approved cloud storage services (Not Scored)	☐	☐
3.8	(L1) Ensure that Cloud App Security is enabled (Not Scored)	☐	☐
4	**Email Security / Exchange Online**		
4.1	(L1) Ensure the Common Attachment Types Filter is enabled (Scored)	☐	☐
4.2	(L1) Ensure Exchange Online Spam Policies are set correctly (Scored)	☐	☐
4.3	(L1) Ensure mail transport rules do not forward email to external domains (Scored)	☐	☐
4.4	(L1) Ensure mail transport rules do not whitelist specific domains (Scored)	☐	☐
4.5	(L2) Ensure the Client Rules Forwarding Block is enabled (Scored)	☐	☐
4.6	(L2) Ensure the Advanced Threat Protection Safe Links policy is enabled (Scored)	☐	☐
4.7	(L2) Ensure the Advanced Threat Protection Safe Attachments policy is enabled (Scored)	☐	☐
4.8	(L2) Ensure basic authentication for Exchange Online is disabled (Scored)	☐	☐
4.9	(L1) Ensure that an anti-phishing policy has been created (Scored)	☐	☐
4.10	(L1) Ensure that DKIM is enabled for all Exchange Online Domains (Scored)	☐	☐
4.11	(L1) Ensure that SPF records are published for all Exchange Domains (Not Scored)	☐	☐
4.12	(L1) Ensure DMARC Records for all Exchange Online domains are published (Not Scored)	☐	☐

Control		Set Correctly	
		Yes	No
4.13	(L1) Ensure notifications for internal users sending malware is Enabled (Scored)	☐	☐
4.14	(L2) Ensure MailTips are enabled for end users (Not Scored)	☐	☐
5	**Auditing**		
5.1	(L1) Ensure Microsoft 365 audit log search is Enabled (Scored)	☐	☐
5.2	(L1) Ensure mailbox auditing for all users is Enabled (Scored)	☐	☐
5.3	(L1) Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly (Not Scored)	☐	☐
5.4	(L2) Ensure the Application Usage report is reviewed at least weekly (Not Scored)	☐	☐
5.5	(L1) Ensure the self-service password reset activity report is reviewed at least weekly (Not Scored)	☐	☐
5.6	(L1) Ensure user role group changes are reviewed at least weekly (Not Scored)	☐	☐
5.7	(L1) Ensure mail forwarding rules are reviewed at least weekly (Not Scored)	☐	☐
5.8	(L1) Ensure the Mailbox Access by Non-Owners Report is reviewed at least biweekly (Not Scored)	☐	☐
5.9	(L1) Ensure the Malware Detections report is reviewed at least weekly (Not Scored)	☐	☐
5.10	(L1) Ensure the Account Provisioning Activity report is reviewed at least weekly (Not Scored)	☐	☐
5.11	(L1) Ensure non-global administrator role group assignments are reviewed at least weekly (Not Scored)	☐	☐
5.12	(L1) Ensure the spoofed domains report is review weekly (Not Scored)	☐	☐
5.13	(L2) Ensure Microsoft 365 Cloud App Security is Enabled (Not Scored)	☐	☐
5.14	(L1) Ensure the report of users who have had their email privileges restricted due to spamming is reviewed (Not Scored)	☐	☐
5.15	(L1) Ensure Guest Users are reviewed at least biweekly (Not Scored)	☐	☐
6	**Storage**		
6.1	(L2) Ensure document sharing is being controlled by domains with whitelist or blacklist (Scored)	☐	☐
6.2	(L2) Block OneDrive for Business sync from unmanaged devices (Scored)	☐	☐
6.3	(L1) Ensure expiration time for external sharing links is set (Scored)	☐	☐

Control		Set Correctly	
		Yes	No
7	**Mobile Device Management**		
7.1	(L1) Ensure mobile device management polices are set to require advanced security configurations to protect from basic internet attacks (Not Scored)	☐	☐
7.2	(L1) Ensure that mobile device password reuse is prohibited (Not Scored)	☐	☐
7.3	(L1) Ensure that mobile devices are set to never expire passwords (Not Scored)	☐	☐
7.4	(L1) Ensure that users cannot connect from devices that are jail broken or rooted (Not Scored)	☐	☐
7.5	(L2) Ensure mobile devices are set to wipe on multiple sign-in failures to prevent brute force compromise (Not Scored)	☐	☐
7.6	(L1) Ensure that mobile devices require a complex password to prevent brute force attacks (Not Scored)	☐	☐
7.7	(L1) Ensure that settings are enable to lock devices after a period of inactivity to prevent unauthorized access (Not Scored)	☐	☐
7.8	(L1) Ensure that mobile device encryption is enabled to prevent unauthorized access to mobile data (Not Scored)	☐	☐
7.9	(L1) Ensure that mobile devices require complex passwords to prevent brute force attacks (Not Scored)	☐	☐
7.10	(L1) Ensure that mobile devices require complex passwords to prevent brute force attacks (Not Scored)	☐	☐
7.11	(L1) Ensure that devices connecting have AV and a local firewall enabled (Not Scored)	☐	☐
7.12	(L2) Ensure mobile device management policies are required for email profiles (Not Scored)	☐	☐
7.13	(L1) Ensure mobile devices require the use of a password (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
12-20-2019	1.1.0	UPDATE - 3.1: (L2) Ensure the customer lockbox feature is enabled CIS Workbench Ticket #: 8939
12-20-2019	1.1.0	UPDATE - 4.11: (L1) Ensure that SPF records are published for all Exchange Domains CIS Workbench Ticket #: 8940
12-20-2019	1.1.0	UPDATE - 4.6: (L2) Ensure the Advanced Threat Protection Safe Links policy is enabled CIS Workbench Ticket #: 8890
12-20-2019	1.1.0	ADD - 5.15: (L1) Ensure Guest Users are reviewed at least biweekly CIS Workbench Ticket #: 8941
12-20-2019	1.1.0	ADD - 4.14: (L2) Ensure MailTips are enabled for end users CIS Workbench Ticket #: 8915
12-20-2019	1.1.0	UPDATE - 5.1: (L1) Ensure Microsoft 365 audit log search is Enabled CIS Workbench Ticket #: 8892
12-20-2019	1.1.0	UPDATE - 4.7: (L2) Ensure the Advanced Threat Protection Safe Attachments policy is enabled CIS Workbench Ticket #: 8891
12-20-2019	1.1.0	ADD - 1.1.5: (L1) Ensure that password protection is enabled for Active Directory in hybrid environments CIS Workbench Ticket #: 8933

Date	Version	Changes for this version
12-20-2019	1.1.0	ADD - 1.1.6: (L1) Enable Conditional Access policies to block legacy authentication CIS Workbench Ticket #: 9001
12-20-2019	1.1.0	ADD - 1.1.7: (L1) Ensure that password hash sync is enabled for resiliency and leaked credential detection CIS Workbench Ticket #: 9002
12-20-2019	1.1.0	ADD - 1.1.8: (L1) Enabled Identity Protection to identify anomalous logon behavior CIS Workbench Ticket #: 9033
12-20-2019	1.1.0	ADD - 1.1.9: (L2) Enable Azure AD Identity Protection sign-in risk policies CIS Workbench Ticket #: 9034
12-20-2019	1.1.0	ADD - 1.1.10: (L2) Enable Azure AD Identity Protection user risk policies CIS Workbench Ticket #: 9036
12-20-2019	1.1.0	ADD - 1.1.11: (L2) Use Just In Time privileged access to Office 365 roles CIS Workbench Ticket #: 9143
12-20-2019	1.1.0	ADD - 3.5: (L1) Ensure DLP policies are enabled for Microsoft Teams CIS Workbench Ticket #: 9141
12-20-2019	1.1.0	ADD - 3.8: (L1) Ensure that Cloud App Security is enabled CIS Workbench Ticket #: 9043
12-20-2019	1.1.0	ADD - 6.2: (L2) Block OneDrive for Business sync from unmanaged devices CIS Workbench Ticket #: 9039

Date	Version	Changes for this version
12-20-2019	1.1.0	ADD - 1.1: Azure Active Directory CIS Workbench Ticket #: 8414
12-20-2019	1.1.0	UPDATE - 7.3: (L1) Ensure that mobile devices are set to never expire passwords CIS Workbench Ticket #: 9181
12-20-2019	1.1.0	UPDATE - 1.1.3: (L1) Ensure that between two and four global admins are designated CIS Workbench Ticket #: 9037
12-20-2019	1.1.0	UPDATE - 1.1.4: (L1) Ensure self-service password reset is enabled CIS Workbench Ticket #: 9038
12-20-2019	1.1.0	5.10: (L1) Ensure the Account Provisioning Activity report is reviewed at least weekly CIS Workbench Ticket #: 8627
12-20-2019	1.1.0	UPDATE - 5.6: (L1) Ensure user role group changes are reviewed at least weekly CIS Workbench Ticket #: 8626
12-20-2019	1.1.0	UPDATE - 5.1: (L1) Ensure Microsoft 365 audit log search is Enabled CIS Workbench Ticket #: 9631
12-20-2019	1.1.0	UPDATE - 2.1 & 7.x: Scored (Automatic) Recommendations now Changed to Unscored (Manual) CIS Workbench Ticket #: 9632
12-20-2019	1.1.0	UPDATE - 2.3 (L2) Ensure O365 ATP SafeLinks for Office Applications is Enabled CIS Workbench Ticket #: 9490