Recommendations

1 Microsoft 365 admin center

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

https://admin.microsoft.com/

1.1 Users

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

Profile Applicability:

- E3 Level 1

Description:

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

Ensure administrative accounts are `licensed without attached applications` and `cloud-only`.

Rationale:

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

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

Impact:

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

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

Audit:

Ensure Administrative accounts are separate and cloud-only:

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com.
2. Click to expand `Users` select `Active users`.
3. Sort by the `Licenses` column.
4. For each user account in an administrative role verify the following:
   - The account is Cloud only (not synced)
   - The account is assigned a license that is not associated with applications i.e. (Microsoft Entra ID P1, Microsoft Entra ID P2)

Remediation:

To created licensed, separate Administrative accounts for Administrative users:

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

Default Value:

N/A

References:

1. https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/add-users?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/enterprise/protect-your-global-administrator-accounts?view=o365-worldwide
3. https://learn.microsoft.com/en-us/azure/active-directory/roles/best-practices#9-use-cloud-native-accounts-for-azure-ad-roles
4. https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/whatis

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

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

Ensure two `Emergency Access` accounts have been defined.

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

Rationale:

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

Impact:

If care is not taken in properly implementing an emergency access account this could weaken security posture. Microsoft recommends to exclude at least one of these accounts from all conditional access rules therefore passwords must have sufficient entropy and length to protect against random guesses. FIDO2 security keys may be used instead of a password for secure passwordless solution.

Audit:

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

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

Step 2 - Ensure two emergency access accounts are defined:

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com
2. Expand `Users` > `Active Users`
3. Inspect the designated emergency access accounts and ensure the following:

   - The accounts are named correctly, and do NOT identify with a particular person.
   - The accounts use the default `.onmicrosoft.com` domain and not the organization's.
   - The accounts are cloud-only.
   - The accounts are unlicensed.
   - The accounts are assigned the `Global Administrator` directory role.

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

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

Remediation:

Step 1 - Create two emergency access accounts:

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com
2. Expand `Users` > `Active Users`
3. Click `Add user` and create a new user with this criteria:

   - Name the account in a way that does NOT identify it with a particular person.
   - Assign the account to the default `.onmicrosoft.com` domain and not the organization's.
   - The password must be at least 16 characters and generated randomly.
   - Do not assign a license.
   - Assign the user the `Global Administrator` role.

4. Repeat the above steps for the second account.

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

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

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

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

NOTE: Microsoft's documentation contains in depth information on securing break glass accounts, please refer to the references section.

Default Value:

Not defined.

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/roles/security-planning#stage-1-critical-items-to-do-right-now
2. https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access

Additional Information:

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

https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access#monitor-sign-in-and-audit-logs

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

If there is only one global tenant administrator, he or she can perform malicious activity without the possibility of being discovered by another admin. If there are numerous global tenant administrators, the more likely it is that one of their accounts will be successfully breached by an external attacker.

Impact:

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

Audit:

Ensure that between two and four global admins are designated:

1. Navigate to the `Microsoft 365 admin center` https://admin.microsoft.com
2. Select `Users` > `Active Users`.
3. Select `Filter` then select `Global Admins`.
4. Review the list of `Global Admins` to confirm there are from two to four such accounts.

To verify the number of global tenant administrators using PowerShell:

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

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

Write-Host "*** There are" $globalAdmins.AdditionalProperties.Count "Global
Administrators assigned."
```

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:

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

References:

1. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.directorymanagement/get-mgdirectoryrole?view=graph-powershell-1.0
2. https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#role-template-ids

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

Ensure Guest Users are reviewed no less frequently than biweekly.

NOTE: With the E5 license an access review can be configured to review guest accounts automatically on a reoccurring basis. This is the preferred method if the licensing is available.

Rationale:

Periodic review of guest users ensures proper access to resources.

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 guest users in the UI:

1. Navigate to `Microsoft 365 admin center` https://admin.microsoft.com/.
2. Click to expand `Users` and select `Guest Users`.
3. Review the list of users.

To verify Microsoft 365 audit log search is enabled using Microsoft Graph PowerShell:

1. Connect using `Connect-MgGraph -Scopes "User.Read.All"`
2. Run the following PowerShell command:

```
Get-MgUser -All -Property UserType,UserPrincipalName |
    Where {$_.UserType -ne "Member"} |
    Format-Table UserPrincipalName, UserType
```

3. Review the list of users. If nothing is returned then there are no guest users.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

1.2 Teams & groups

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

Profile Applicability:

- E3 Level 2

Description:

Microsoft 365 Groups is the foundational membership service that drives all teamwork across Microsoft 365. With Microsoft 365 Groups, you can give a group of people access to a collection of shared resources. While there are several different group types this recommendation concerns **Microsoft 365 Groups**.

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

Rationale:

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

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

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

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

Impact:

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

Audit:

Ensure only organizationally managed/approved public groups exist:

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

Using the Microsoft Graph PowerShell module:

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

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

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

Remediation:

To enable only organizationally managed/approved public groups exist:

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

Default Value:

Public when create from the Administration portal; private otherwise.

References:

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

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

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

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

Rationale:

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

Audit:

Review Shared mailboxes in the UI:

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

Note: If sign-in is not blocked it will read `Block sign-in`.
In PowerShell connect using 2 modules:

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

```
$MBX = Get-EXOMailbox -RecipientTypeDetails SharedMailbox
$MBX | ForEach {Get-AzureADUser -ObjectId $_.ExternalDirectoryObjectId} |
    Format-Table DisplayName,UserPrincipalName,AccountEnabled
```

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

Both are functionally identical.

Remediation:

Block sign-in to shared mailboxes in the UI:

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

Using PowerShell connect with 2 modules:

1. Connect using `Connect-AzureAD`.
2. To disable sign-in for a single account:

```
Set-AzureADUser -ObjectId TestUser@example.com -AccountEnabled $false
```

3. Or, the following script will block sign-in to all Shared Mailboxes.
4. Connect using `Connect-ExchangeOnline`.

```
$MBX = Get-EXOMailbox -RecipientTypeDetails SharedMailbox
$MBX | ForEach {Set-AzureADUser -ObjectId $_.ExternalDirectoryObjectId -
AccountEnabled $false}
```

Default Value:

AccountEnabled: `True`

References:

1. https://learn.microsoft.com/en-us/microsoft-365/admin/email/about-shared-mailboxes?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/admin/email/create-a-shared-mailbox?view=o365-worldwide#block-sign-in-for-the-shared-mailbox-account
3. https://learn.microsoft.com/en-us/microsoft-365/enterprise/block-user-accounts-with-microsoft-365-powershell?view=o365-worldwide#block-individual-user-accounts
4. https://learn.microsoft.com/en-us/powershell/module/azuread/set-azureaduser?view=azureadps-2.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

1.3 Settings

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

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

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

Audit:

Ensure that Office 365 passwords are set to never expire:

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

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

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

```
Get-MgDomain -DomainId <Domain Name> | ft PasswordValidityPeriodInDays
```

Remediation:

To set Office 365 passwords are set to never expire:

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

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

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

```
Update-MgDomain -DomainId <Domain> -PasswordValidityPeriodInDays 2147483647 -
PasswordNotificationWindowInDays 30
```

Default Value:

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

References:

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

CIS Controls:

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

1.3.2 (L1) Ensure 'Idle session timeout' is set to '3 hours (or less)' for unmanaged devices (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

The following Microsoft 365 web apps are supported.

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

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

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

Rationale:

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

Impact:

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

Audit:

Step 1 - Ensure Idle session timeout is configured:

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

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

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Expand `Azure Active Directory` > `Protect & secure` > `Conditional Access`
3. Inspect existing conditional access rules for one that meets the below conditions:

- `Users` is set to `All users`
- `Cloud apps or actions` > `Select apps` is set to `Office 365`.
- `Conditions` > `Client apps` is `Browser` and nothing else.
- `Session` is set to `Use app enforced restrictions`.
- `Enable Policy` is set to `On`

NOTE: To ensure that idle timeouts affect only unmanaged devices, both steps must be completed.

Remediation:

To configure Idle session timeout:

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

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

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

NOTE: To ensure that idle timeouts affect only unmanaged devices, both steps must be completed.

Default Value:

Not configured. (Idle sessions will not timeout.)

References:

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

Additional Information:

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 2

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure calendar details sharing with external users is disabled:

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

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

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

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

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

Remediation:

To disable calendar details sharing with external users:

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

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

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

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

Default Value:

Enabled (True)

References:

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

Additional Information:

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

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

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

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

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

CIS Controls:

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

1.3.4 (L1) Ensure 'User owned apps and services' is restricted (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

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

Rationale:

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

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

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

Impact:

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

Audit:

Ensure users installing Office Store add-ins, and enabling 365 trials is not allowed:

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

Remediation:

To prohibit users installing Office Store add-ins and starting 365 trials:

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

Default Value:

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

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure internal phishing protection for Forms is enabled:

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

Remediation:

To enable internal phishing protection for Forms:

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

Default Value:

Internal Phishing Protection is enabled.

References:

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

CIS Controls:

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

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

Profile Applicability:

- E5 Level 2

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure the customer lockbox feature is enabled:

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

To verify the Customer Lockbox feature is enabled using the SecureScore Portal:

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

To verify the Customer Lockbox feature is enabled using the REST API:

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

To verify the Customer Lockbox feature is enabled using PowerShell:

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

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

3. Verify the value is set to `True`

Remediation:

To enable the Customer Lockbox feature:

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

To set the Customer Lockbox feature to enabled using PowerShell:

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

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

Default Value:

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

`CustomerLockboxEnabled` - `False`

References:

1. https://learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- E3 Level 2

Description:

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

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

Rationale:

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

Impact:

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

Audit:

Ensure Microsoft 365 on the web is restricted:

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

Remediation:

To restrict Microsoft 365 on the web:

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

Default Value:

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

References:

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 2

Description:

Sway is a new app from Microsoft Office that allows users to create and share interactive reports, personal stories, presentations, and more.

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

Rationale:

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

Impact:

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

Audit:

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

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

Remediation:

To ensure Sways cannot be viewed outside of your organization:

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

Default Value:

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

References:

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

CIS Controls:

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

2 Microsoft 365 Defender

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

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

2.1 Email & collaboration

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

Profile Applicability:

- E5 Level 2

Description:

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

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

Rationale:

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

Impact:

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

Audit:

Ensure Safe Links for Office Applications is Enabled:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com
2. Under `Email & collaboration` select `Policies & rules`
3. Select `Threat policies` then `Safe Links`
4. Inspect each policy and attempt to identify one that matches the parameters outlined below.
5. Scroll down the pane and click on `Edit Protection settings` (Global Readers will look for on or off values)
6. Ensure the following protection settings are set as outlined:
   Email
   - Checked `On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default`
   - Checked `Apply Safe Links to email messages sent within the organization`
   - Checked `Apply real-time URL scanning for suspicious links and links that point to files`
   - Checked `Wait for URL scanning to complete before delivering the message`
   - Unchecked `Do not rewrite URLs, do checks via Safe Links API only.`

   Teams

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

   Office 365 Apps

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

   Click protection settings

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

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

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

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

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

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

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

Remediation:

To create a Safe Links policy:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com
2. Under `Email & collaboration` select `Policies & rules`
3. Select `Threat policies` then `Safe Links`
4. Click on `+Create`
5. Name the policy then click `Next`
6. In `Domains` select all valid domains for the organization and `Next`
7. Ensure the following `URL & click protection settings` are defined:
   Email
   - Checked `On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default`
   - Checked `Apply Safe Links to email messages sent within the organization`
   - Checked `Apply real-time URL scanning for suspicious links and links that point to files`
   - Checked `Wait for URL scanning to complete before delivering the message`
   - Unchecked `Do not rewrite URLs, do checks via Safe Links API only.`

   Teams

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

   Office 365 Apps

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

   Click protection settings

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

To create a Safe Links policy using the Exchange Online PowerShell Module:

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

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

}

New-SafeLinksPolicy @params

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

References:

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure the Common Attachment Types Filter is enabled:

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

To verify the Common Attachment Types Filter is enabled using PowerShell:

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

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

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

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

Remediation:

To enable the Common Attachment Types Filter:

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

To enable the Common Attachment Types Filter using PowerShell:

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

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

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

Default Value:

Always on

References:

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

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

Rationale:

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

Impact:

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

Audit:

Ensure notifications for internal users sending malware is Enabled:

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

To audit using PowerShell:

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

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

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

Remediation:

To enable notifications for internal users sending malware:

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

To remediate using PowerShell:

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

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

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

Default Value:

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

CIS Controls:

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

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

Profile Applicability:

- E5 Level 2

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure Safe Attachments policy is enabled:

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

To verify the Safe Attachments policy is enabled using PowerShell:

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

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

Remediation:

To enable the Safe Attachments policy:

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

Default Value:

disabled

CIS Controls:

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

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

Profile Applicability:

- E5 Level 2

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure Safe Attachments for SharePoint, OneDrive, and Microsoft Teams is Enabled:

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

To audit using PowerShell:

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

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

Verify the values for each parameter as below:

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

Remediation:

To enable Safe Attachments for SharePoint, OneDrive, and Microsoft Teams:

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

To remediate using PowerShell:

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

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

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

Rationale:

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

Impact:

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

Audit:

Ensure Exchange Online Spam Policies are set to notify administrators:

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

To verify the Exchange Online Spam Policies are set correctly using PowerShell:

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

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

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

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

Remediation:

To set the Exchange Online Spam Policies:

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

To set the Exchange Online Spam Policies correctly using PowerShell:

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

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

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

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

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

Default Value:

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

CIS Controls:

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

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

Profile Applicability:

- E5 Level 1

Description:

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

Rationale:

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

Impact:

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

Audit:

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

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules`
3. Select `Threat policies`.
4. Under Policies select `Anti-phishing`.
5. Verify the `Office365 AntiPhish Default (Default)` policy exists and is `Always on`.
6. Verify that `Phishing email threshold` is set to at least `2 - Aggressive`
7. Verify the following features are enabled: `Mailbox intelligence` - `Mailbox intelligence for impersonations` and `Spoof intelligence`.

To verify the anti-phishing policy using PowerShell:

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

```
Get-AntiPhishPolicy | Format-Table -AutoSize `
    name, enabled, PhishThresholdLevel, `
    EnableMailboxIntelligenceProtection, `
    EnableMailboxIntelligence, EnableSpoofIntelligence
```

3. Verify values for `Office365 AntiPhish Default` and custom policies are:

- `Enabled` - `True`
- `PhishThresholdLevel` - at least `2`
- `EnableMailboxIntelligenceProtection` - `True`
- `EnableMailboxIntelligence` - `True`
- `EnableSpoofIntelligence` - `True`

Remediation:

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

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Policies & rules`
3. Select `Threat policies`.
4. Under Policies select `Anti-phishing`.
5. Select the `Office365 AntiPhish Default (Default)` policy and click `Edit protection settings`.
6. Set the `Phishing email threshold` to at least `2 - Aggressive`.

Under **Impersonation**

- Check `Enable mailbox intelligence (Recommended)`
- Check `Enable Intelligence for impersonation protection (Recommended)`.

Under **Spoof**

- Check `Enable spoof intelligence (Recommended)`.

7. Click Save.

To create an anti-phishing policy using PowerShell:

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

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure that SPF records are published for all Exchange Domains:

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]/serviceConfigurationRec
ords
```

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

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

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

Rationale:

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

Impact:

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

Audit:

To ensure DKIM is enabled:

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

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

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

```
Get-DkimSigningConfig
```

3. Verify `Enabled` is set to True

Remediation:

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

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

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

For Office 365, the selectors will always be `selector1` or `selector2`. domainGUID is the same as the domainGUID in the customized MX record for your custom domain that appears before mail.protection.outlook.com. For example, in the following MX record for the domain contoso.com, the domainGUID is contoso-com:

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

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

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

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

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

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

References:

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

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure DMARC Records for all Exchange Online domains are published:

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

CIS Controls:

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

2.1.11 (L1) Ensure the spoofed domains report is reviewed weekly (Manual)

Profile Applicability:

- E5 Level 1

Description:

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

Rationale:

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

Audit:

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

Remediation:

To review the spoofed domains report:

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

To view spoofed senders that were allowed or blocked by spoof intelligence in the last 7 days:

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

```
Get-SpoofIntelligenceInsight
```

3. Review.

References:

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

CIS Controls:

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

2.1.12 (L1) Ensure the 'Restricted entities' report is reviewed weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Audit:

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

Remediation:

To review the report of users who have had their email privileges restricted due to spamming:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Under `Email & collaboration` navigate to `Review`.
3. Click `Restricted Entities`.
4. Review alerts and take appropriate action (unblocking) after account has been remediated.

Review a list of users blocked from sending messages using PowerShell:

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

```
Get-BlockedSenderAddress
```

3. Review.

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/responding-to-a-compromised-email-account?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-users-portal-after-spam?view=o365-worldwide
3. https://learn.microsoft.com/en-us/powershell/module/exchange/get-blockedsenderaddress?view=exchange-ps

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

The Threat protection status report shows specific instances of Microsoft blocking a malware attachment from reaching users, phishing being blocked, impersonation attempts, etc. The Threat protection status report should be reviewed at least weekly.

Rationale:

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

Audit:

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

Remediation:

To review the Threat protection status report:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click to expand `Email & collaboration` select `Review`.
3. Select `Malware trends`.
4. On the Threat Explorer page, select `All email` and review statistics.

References:

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

CIS Controls:

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

2.2 Cloud apps

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

2.3 Audit

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

If the organization doesn't usually use a third party provider to manage accounts, any entry on the list is likely illicit. However, if the organization uses a third party provider, it is recommended to monitor transaction volumes and look for new or unusual third party applications that may be managing users. If anything unusual is observed, the provider should be contacted to determine the legitimacy of the action.

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 Account Provisioning Activity report:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click on `Audit`.
3. Set `Activities` to `Added user` for `User administration activities`.
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

To review Account Provisioning Activity report using PowerShell:

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

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

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

3. Review the output

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

Non-global administrator role group assignments should be reviewed 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 unusual activity is detected, 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:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Click on `Audit`.
3. Set `Added member to Role` and `Removed a user from a directory role` for `Activities`.
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

CIS Controls:

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

2.4 Settings

2.4.1 (L1) Ensure Priority account protection is enabled and configured (Manual)

Profile Applicability:

- E5 Level 1

Description:

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

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

Rationale:

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

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

Audit:

Audit with a 3-step process
Step 1: Verify Priority account protection is enabled:

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

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

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

Step 3: Ensure alerts are configured:

8. Expand `E-mail & Collaboration` on the left column.
9. Select `Policies & rules` > `Alert policy`
10. Ensure alert policies are configured for priority accounts, enabled and have a valid recipient. The tags column can be used to identify policies using a specific tag.

Remediation:

Remediate with a 3-step process
Step 1: Enable Priority account protection in Microsoft 365 Defender:

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

Step 2: Tag priority accounts:

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

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

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

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

Default Value:

By default, priority accounts are undefined.

References:

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

CIS Controls:

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

2.4.2 (L1) Ensure Priority accounts have 'Strict protection' presets applied (Manual)

Profile Applicability:

- E5 Level 1

Description:

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

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

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

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

Rationale:

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

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

Impact:

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

Audit:

Verify strict preset security policies have been applied to Priority accounts:

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

Remediation:

Enable strict preset security policies for Priority accounts:

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

Default Value:

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

References:

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

CIS Controls:

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

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

Profile Applicability:

- E5 Level 2

Description:

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

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

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

Rationale:

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

Audit:

Ensure Microsoft Defender for Cloud Apps is enabled and configured:

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

Remediation:

Configure Information Protection and Cloud Discovery:

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

Note: Defender for Endpoint requires a Defender for Endpoint license.
Configure App Connectors:

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

Default Value:

Disabled

References:

1. https://learn.microsoft.com/en-us/defender-cloud-apps/connect-office-365
2. https://learn.microsoft.com/en-us/defender-cloud-apps/connect-azure
3. https://learn.microsoft.com/en-us/defender-cloud-apps/best-practices
4. https://learn.microsoft.com/en-us/defender-cloud-apps/get-started
5. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

Additional Information:

Additional Microsoft 365 Defender features include:

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

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

CIS Controls:

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

3 Microsoft Purview

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

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

3.1 Audit

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

Profile Applicability:

- E3 Level 1

Description:

When audit log search is enabled in the Microsoft Purview compliance portal, user and admin activity within the organization is recorded in the audit log and retained for 90 days. However, some organizations may prefer to use a third-party security information and event management (SIEM) application to access their auditing data. In this scenario, a global admin can choose to turn off audit log search in Microsoft 365.

Rationale:

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

Audit:

Ensure Microsoft 365 audit log search is Enabled:

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

To verify audit log search is enabled using PowerShell:

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

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

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

Remediation:

To enable Microsoft 365 audit log search:

1. Navigate to `Microsoft Purview` https://compliance.microsoft.com.
2. Select `Audit` to open the audit search.
3. Click `Start recording user and admin activity` next to the information warning at the top.
4. Click `Yes` on the dialog box to confirm.

To enable Microsoft 365 audit log search using PowerShell:

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

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

References:

1. https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-log-enable-disable?view=o365-worldwide
2. https://learn.microsoft.com/en-us/powershell/module/exchange/set-adminauditlogconfig?view=exchange-ps

CIS Controls:

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

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

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

Audit:

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

Remediation:

To review user role group changes:

1. Navigate to `Microsoft Purview` https://compliance.microsoft.com/.
2. Under Solutions click on `Audit` then select `New Search`.
3. In `Activities` find `Added member to Role` under the **Role administration activities** section and select it.
4. Set a valid `Start Date` and `End Date` within the last week.
5. Click `Search`.
6. Review once the search is completed.

To review user role group changes using PowerShell:

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

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

Search-UnifiedAuditLog -StartDate $startDate -EndDate $endDate -RecordType
AzureActiveDirectory -Operations "Add member to role."
```

3. Review the output

References:

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

CIS Controls:

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

3.2 Data loss protection

3.2.1 (L1) Ensure DLP policies are enabled (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure DLP policies are enabled:

1. Navigate to `Microsoft Purview` https://compliance.microsoft.com.
2. Under `Solutions` select `Data loss prevention` then `Policies`.
3. Verify that policies exist and are enabled.

Remediation:

To enable DLP policies:

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

References:

1. https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

CIS Controls:

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

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

Profile Applicability:

- E5 Level 1

Description:

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

By default, the rule includes sensitive information types, such as credit card numbers and social security numbers, and applies to all users in the organization.

Rationale:

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

Impact:

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

Audit:

Ensure DLP policies are enabled for Microsoft Teams:

1. Navigate to `Microsoft Purview` compliance portal https://compliance.microsoft.com.
2. Under `Solutions` select `Data loss prevention` then `Policies`.
3. Click `Policies` tab.
4. Verify `Default policy for Teams` Status is On.

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

1. Connect using `Connect-ExchangeOnline`, then run the following

```
Import-Module ExchangeOnlineManagement
```

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

```
Get-DlpCompliancePolicy
```

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

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

NOTE: Connect-IPPSSession still requires Basic authentication to be enabled in WinRM on the local computer. Depending on your configuration this might be disabled. To turn on basic authentication see the supporting Microsoft document in the references section.

Remediation:

To enable DLP policies:

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

Default Value:

Enabled (On)

References:

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

CIS Controls:

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

3.3 Information Protection

3.3.1 (L1) Ensure SharePoint Online Information Protection policies are set up and used (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

The creation of data classification policies is unlikely to have a significant impact on an organization. However, maintaining long-term adherence to policies may require ongoing training and compliance efforts across the organization. Therefore, organizations should include training and compliance planning as part of the data classification policy creation process.

Audit:

Ensure SharePoint Online Information Protection policies are set up and used:

1. Navigate to `Microsoft Purview` compliance portal https://compliance.microsoft.com.
2. Under `Solutions` select `Information protection`.
3. Click on the `Label policies` tab.
4. Ensure that a Label policy exists and is published accordingly.

Remediation:

To set up SharePoint Online Information Protection:

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

References:

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

CIS Controls:

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

4 Microsoft Intune admin center

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

CIS has platform specific benchmarks for InTune endpoints not covered here. Those are located in the following WorkBench communities:

CIS Microsoft Intune for Windows:

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

CIS Intune Apple iOS and iPadOS Benchmarks:

https://workbench.cisecurity.org/communities/179

5 Microsoft Entra admin center

Microsoft Entra, also known as Identity, contains settings related to identity, conditional access, and was formerly named Azure AD.

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

5.1 Identity

5.1.1 Overview

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

Profile Applicability:

- E3 Level 1

Description:

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

By default, Microsoft enables security defaults. The goal is to ensure that all organizations have a basic level of security enabled. The security default setting is manipulated in the Azure Portal.

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

Rationale:

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

For example, doing the following:

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

Impact:

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

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

Audit:

Ensure security defaults is disabled:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click to expand `Identity` select `Overview`
3. Click `Properties`.
4. Review the section **Security Defaults** near the bottom
5. If `Manage security defaults` appears clickable then proceed to the remediation section, otherwise read the note below.

NOTE: If `Manage Conditional Access` appears in blue then Security defaults are already disabled, and CA is in use. The audit can be considered a Pass.

To verify security defaults is disabled using Microsoft Graph PowerShell:

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

```
Get-MgPolicyIdentitySecurityDefaultEnforcementPolicy | ft IsEnabled
```

3. If the value is false then Security Defaults is disabled.

Remediation:

To disable security defaults:

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

To configure security defaults using Microsoft Graph PowerShell:

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

```
$params = @{ IsEnabled = $false }
Update-MgPolicyIdentitySecurityDefaultEnforcementPolicy -BodyParameter
$params
```

WARNING: It is recommended not to disable security defaults until you are ready to implement conditional access rules in the benchmark. Rules such as requiring MFA for all users and blocking legacy protocols are required in CA in order to make up the gap by disabling defaults. Plan accordingly. See the reference section for more details on what coverage Security Defaults provide.

Default Value:

Enabled.

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

5.1.2 Users

5.1.2.1 (L1) Ensure 'Per-user MFA' is disabled (Manual)

Profile Applicability:

- E3 Level 1

Description:

Legacy per-user Multi-Factor Authentication (MFA) can be configured to require individual users to provide multiple authentication factors, such as passwords and additional verification codes, to access their accounts. It was introduced in earlier versions of Office 365, prior to the more comprehensive implementation of Conditional Access (CA).

Rationale:

Both security defaults and conditional access with security defaults turned off are not compatible with per-user multi-factor authentication (MFA), which can lead to undesirable user authentication states. The CIS Microsoft 365 Benchmark explicitly employs Conditional Access for MFA as an enhancement over security defaults and as a replacement for the outdated per-user MFA. To ensure a consistent authentication state disable per-user MFA on all accounts.

Impact:

Accounts using per-user MFA will need to be migrated to use CA.

Prior to disabling per-user MFA the organization must be prepared to implement conditional access MFA to avoid security gaps and allow for a smooth transition. This will help ensure relevant accounts are covered by MFA during the change phase from disabling per-user MFA to enabling CA MFA. Section 5.2.2 in this document covers creating of a CA rule for both administrators and all users in the tenant.

Microsoft has detailed documentation on migrating from per-user MFA including a PowerShell script titled Convert users from per-user MFA to Conditional Access based MFA

Audit:

To audit per-user MFA using the UI:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Users` select `All users`.
3. Click on `Per-user MFA` on the top row.
4. Ensure under the column `Multi-factor Auth Status` that each account is set to `Disabled`

To audit per-user MFA using PowerShell:

1. Connect to MSOnline using `Connect-MsolService`.
2. Run the following script:

```
$UserList = Get-MsolUser -All | Where-Object {$_.UserType -eq 'Member'}
$Report = @()

foreach ($user in $UserList) {
    $PerUserMFAState = $null
    if ($user.StrongAuthenticationRequirements) {
        $PerUserMFAState = $user.StrongAuthenticationRequirements.State
    } else {
        $PerUserMFAState = 'Disabled'
    }
    $obj = [pscustomobject][ordered]@{
        UserPrincipalName     = $User.UserPrincipalName
        DisplayName           = $User.DisplayName
        PerUserMFAState       = $PerUserMFAState
    }
    $Report += $obj
}
$Report
```

3. Ensure `PerUserMfaState` is `Disabled` for all users.

Remediation:

Disable per-user MFA using the UI:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Users` select `All users`.
3. Click on `Per-user MFA` on the top row.
4. Click the empty box next to `Display Name` to select all accounts.
5. On the far right under *quick steps* click `Disable`.

Default Value:

Disabled

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#convert-users-from-per-user-mfa-to-conditional-access
2. https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide#use-conditional-access-policies
3. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#convert-per-user-mfa-enabled-and-enforced-users-to-disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●

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

Profile Applicability:

- E3 Level 2

Description:

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

Rationale:

Third party integrated applications connection to services should be disabled, unless there is a very clear value and robust security controls are in place. While there are legitimate uses, attackers can grant access from breached accounts to third party applications to exfiltrate data from your tenancy without having to maintain the breached account.

Impact:

Implementation of this change will impact both end users and administrators. End users will not be able to integrate third-party applications that they may wish to use. Administrators are likely to receive requests from end users to grant them permission to necessary third-party applications.

Audit:

Ensure third party integrated applications are not allowed:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Users` select `Users settings`.
3. Verify `Users can register applications` is set to `No`.

Remediation:

To prohibit third party integrated applications:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Users` select `Users settings`.
3. Set `Users can register applications` to `No`.
4. Click Save.

Default Value:

Yes (Users can register applications.)

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	18.4 Only Use Up-to-date And Trusted Third-Party Components Only use up-to-date and trusted third-party components for the software developed by the organization.		●	●

5.1.2.3 (L1) Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated)

Profile Applicability:

- E3 Level 1

Description:

Non-privileged users can create tenants in the Azure AD and Entra administration portal under Manage tenant. The creation of a tenant is recorded in the Audit log as category “DirectoryManagement” and activity “Create Company”. Anyone who creates a tenant becomes the Global Administrator of that tenant. The newly created tenant doesn't inherit any settings or configurations.

Rationale:

Restricting tenant creation prevents unauthorized or uncontrolled deployment of resources and ensures that the organization retains control over its infrastructure. User generation of shadow IT could lead to multiple, disjointed environments that can make it difficult for IT to manage and secure the organization's data, especially if other users in the organization began using these tenants for business purposes under the misunderstanding that they were secured by the organization's security team.

Impact:

Non-admin users will need to contact I.T. if they have a valid reason to create a tenant.

Audit:

Verify access to the Azure AD portal is restricted:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity`> `Users` > `User settings`.
3. Ensure `Restrict non-admin users from creating tenants` is set to `Yes`

To audit using PowerShell:

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

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions |
    Select-Object AllowedToCreateTenants
```

3. Ensure the returned value is `False`

Remediation:

Restrict access to the Azure AD portal:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity`> `Users` > `User settings`.
3. Set `Restrict non-admin users from creating tenants` to `Yes` then `Save`.

To remediate using PowerShell:

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Policy.ReadWrite.Authorization"`
2. Run the following commands.

```
# Create hashtable and update the auth policy
$params = @{ AllowedToCreateTenants = $false }
Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions $params
```

Default Value:

No - Non-administrators can create tenants.

`AllowedToCreateTenants` is `True`

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

5.1.2.4 (L1) Ensure 'Restrict access to the Azure AD administration portal' is set to 'Yes' (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

Note: This recommendation only affects access to the Azure AD web portal. It does not prevent privileged users from using other methods such as Rest API or PowerShell to obtain information. Those channels are addressed elsewhere in this document.

Rationale:

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

Note: Users will still be able to sign into `Azure Active directory admin center` but will be unable to see directory information.

Audit:

Verify access to the Azure AD portal is restricted:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity`> `Users` > `User settings`.
3. Verify under the **Administration portal** section that `Restrict access to Microsoft Entra ID administration portal` is set to `Yes`

Remediation:

Ensure access to the Azure AD portal is restricted:

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

Default Value:

No - Non-administrators can access the Azure AD administration portal.

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- E3 Level 2

Description:

The option for the user to `Stay signed in` or the `Keep me signed in` option will prompt a user after a successful login, when the user selects this option a persistent refresh token is created. Typically this lasts for 90 days and does not prompt for sign-in or Multi-Factor.

Rationale:

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

Impact:

Once this setting is hidden users will no longer be prompted upon sign-in with the message `Stay signed in?`. This may mean users will be forced to sign in more frequently. Important: some features of SharePoint Online and Office 2010 have a dependency on users remaining signed in. If you hide this option, users may get additional and unexpected sign in prompts.

Audit:

Ensure the option to remain signed in is hidden:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity`> `Users` > `User settings`.
3. Ensure `Show keep user signed in` is highlighted `No`.

Remediation:

To disable the option to remain signed in:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity`> `Users` > `User settings`.
3. Set `Show keep user signed in` to `No`.
4. Click `Save`.

Default Value:

Users may select `stay signed in`

CIS Controls:

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

5.1.2.6 (L2) Ensure 'LinkedIn account connections' is disabled (Manual)

Profile Applicability:

- E3 Level 2

Description:

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

Rationale:

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

Impact:

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

Audit:

Ensure that LinkedIn account connections is disabled:

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

Remediation:

To disable LinkedIn account connections:

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

Default Value:

LinkedIn integration is enabled by default.

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

5.1.3 Groups

5.1.3.1 (L1) Ensure a dynamic group for guest users is created (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

The recommended state is to create a dynamic group that includes guest accounts.

Rationale:

Dynamic groups allow for an automated method to assign group membership.

Guest user accounts will be automatically added to this group and through this existing conditional access rules, access controls and other security measures will ensure that new guest accounts are restricted in the same manner as existing guest accounts.

Audit:

Ensure a dynamic guest group is created:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Groups` select `All groups`.
3. On the right of the search field click `Add filter`.
4. Set `Filter` to `Membership type` and `Value` to `Dynamic` then apply.
5. Identify a dynamic group and select it.
6. Under manage, select `Dynamic membership rules` and ensure the rule syntax contains `(user.userType -eq "Guest")`
7. If necessary, inspect other dynamic groups for the value above.

Using PowerShell:

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

```
$groups = Get-MgGroup | Where-Object { $_.GroupTypes -contains
"DynamicMembership" }
$groups | ft DisplayName,GroupTypes,MembershipRule
```

3. Look for a dynamic group containing the rule `(user.userType -eq "Guest")`

Remediation:

Create a dynamic guest group:

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

```
(user.userType -eq "Guest")
```

7. Select `OK` and `Save`

Using PowerShell:

1. Connect to Microsoft Graph using `Connect-MgGraph -Scopes "Group.ReadWrite.All"`
2. In the script below edit `DisplayName` and `MailNickname` as needed and run:

```
$params = @{
     DisplayName                     = "Dynamic Test Group"
     MailNickname                    = "DynGuestUsers"
     MailEnabled                     = $false
     SecurityEnabled                 = $true
     GroupTypes                      = "DynamicMembership"
     MembershipRule                  = '(user.userType -eq "Guest")'
     MembershipRuleProcessingState = "On"
}

New-MgGroup @params
```

Default Value:

Undefined

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

5.1.4 Devices

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

5.1.5 Applications

5.1.5.1 (L1) Ensure the Application Usage report is reviewed at least weekly (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

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 Application Usage report:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Applications` select `Enterprise applications`.
3. Under Activity select `Usage & insights`.
4. Review the information.

CIS Controls:

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

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

Profile Applicability:

- E3 Level 2

Description:

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive but can represent a risk in some situations if it's not monitored and controlled carefully.

Rationale:

Attackers commonly use custom applications to trick users into granting them access to company data. Disabling future user consent operations setting mitigates this risk, and helps to reduce the threat-surface. If user consent is disabled previous consent grants will still be honored but all future consent operations must be performed by an administrator.

Impact:

If user consent is disabled, previous consent grants will still be honored but all future consent operations must be performed by an administrator. Tenant-wide admin consent can be requested by users through an integrated administrator consent request workflow or through organizational support processes.

Audit:

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

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Applications` select `Enterprise applications`.
3. Under `Security` select `Consent and permissions` > `User consent settings`.
4. Verify `User consent for applications` is set to `Do not allow user consent`.

Remediation:

To prohibit user consent to apps accessing company data on their behalf:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Applications` select `Enterprise applications`.
3. Under `Security` select `Consent and permissions` > `User consent settings`.
4. Under `User consent for applications` select `Do not allow user consent`.
5. Click the `Save` option at the top of the window.

Default Value:

UI - `Allow user consent for apps`

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

5.1.5.3 (L1) Ensure the admin consent workflow is enabled (Manual)

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges.

Audit:

Ensure the admin consent workflow is enabled:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Applications` select `Enterprise applications`.
3. Under Security select `Consent and permissions`.
4. Under Manage select `Admin consent settings`.
5. Verify that `Users can request admin consent to apps they are unable to consent to` is set to `Yes`.

Remediation:

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

1. Navigate to Microsoft Entra admin center https://entra.microsoft.com/.
2. Click to expand Identity > Applications select Enterprise applications.
3. Under Security select Consent and permissions.
4. Under Manage select Admin consent settings.
5. Set Users can request admin consent to apps they are unable to consent to to Yes under Admin consent requests.
6. Under the Reviewers choose the Roles and Groups that will review user generated app consent requests.
7. Set Selected users will receive email notifications for requests to Yes
8. Select Save at the top of the window.

Default Value:

- Users can request admin consent to apps they are unable to consent to: No
- Selected users to review admin consent requests: None
- Selected users will receive email notifications for requests: Yes
- Selected users will receive request expiration reminders: Yes
- Consent request expires after (days): 30

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	18.3 Verify That Acquired Software is Still Supported Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.		●	●

5.1.6 External Identities

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

Profile Applicability:

- E3 Level 2

Description:

Azure Active Directory (Azure AD) B2B collaboration is a feature within External Identities allows for guest invitations to an organization.

Ensure users can only send invitations to `specified domains`.

NOTE: This list works independently from OneDrive for Business and SharePoint Online allow/block lists. To restrict individual file sharing in SharePoint Online, set up an allow or blocklist for OneDrive for Business and SharePoint Online. For instance, in SharePoint or OneDrive users can still share with external users from prohibited domains by using Anyone links if they haven't been disabled.

Rationale:

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

Impact:

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

Audit:

Ensure that collaboration invitations are sent to allowed domains only:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `External Identities` select `External collaboration settings`.
3. Under `Collaboration restrictions`, make sure that `Allow invitations only to the specified domains (most restrictive)` is selected. Then make sure that `Target domains` is checked and that allowed domains are specified.

Remediation:

To restrict collaboration invitations only to the specified domains:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `External Identities` select `External collaboration settings`.
3. Under `Collaboration restrictions`, select `Allow invitations only to the specified domains (most restrictive)`, check the `Target domains` setting, and specify the domains allowed to collaborate.

Default Value:

Allow invitations to be sent to any domain (most inclusive)

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/external-identities/allow-deny-list
2. https://learn.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v7	13.1 Maintain an Inventory Sensitive Information Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.	●	●	●

5.1.7 User experiences

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

5.1.8 Hybrid management

5.1.8.1 (L1) Ensure that password hash sync is enabled for hybrid deployments (Automated)

Profile Applicability:

- E3 Level 1

Description:

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

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

Rationale:

Password hash synchronization helps by reducing the number of passwords your users need to maintain to just one and enables leaked credential detection for your hybrid accounts. Leaked credential protection is leveraged through Azure AD Identity Protection and is a subset of that feature which can help identify if an organization's user account passwords have appeared on the dark web or public spaces.

Using other options for your directory synchronization may be less resilient as Microsoft can still process sign-ins to 365 with Hash Sync even if a network connection to your on-premises environment is not available.

Impact:

Compliance or regulatory restrictions may exist, depending on the organization's business sector, that preclude hashed versions of passwords from being securely transmitted to cloud data centers.

Audit:

Ensure that password hash sync is enabled for hybrid deployments:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity` > `Hybrid management` > `Microsoft Entra Connect`.
3. Select `Connect Sync`
4. Under **Azure AD Connect Sync**, verify Password Hash Sync is `Enabled`.

To ensure Password Hash Sync is enabled using the Azure AD Connect tool:

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

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

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

To verify if Password Hash Sync is enabled utilizing Microsoft Graph PowerShell:

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

```
Get-MgOrganization | ft OnPremisesSyncEnabled
```

3. If nothing returns then password sync is not enabled for the on premises AD.

Remediation:

To setup Password Hash Sync, use the following steps:

1. Log in to the on premises server that hosts the Azure AD Connect tool
2. Double-click the `Azure AD Connect` icon that was created on the desktop
3. Click `Configure`.
4. On the `Additional tasks` page, select `Customize synchronization options` and click `Next`.
5. Enter the username and password for your global administrator.
6. On the `Connect your directories` screen, click `Next`.
7. On the `Domain and OU filtering` screen, click `Next`.
8. On the `Optional features` screen, check `Password hash synchronization` and click `Next`.
9. On the `Ready to configure` screen click `Configure`.
10. Once the configuration completes, click `Exit`.

Default Value:

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

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs
2. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#user-linked-detections
3. https://www.microsoft.com/en-us/download/details.aspx?id=47594

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

5.2 Protection

5.2.1 Identity Protection

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

5.2.2 Conditional Access

5.2.2.1 (L1) Ensure multifactor authentication is enabled for all users in administrative roles (Manual)

Profile Applicability:

- E3 Level 1

Description:

Multi-factor authentication is a process that requires an additional form of identification during the sign-in process, such as a code from a mobile device or a fingerprint scan, to enhance security.

Ensure users in administrator roles have MFA capabilities enabled.

Rationale:

Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact:

Implementation of multifactor authentication for all users in administrative roles will necessitate a change to user routine. All users in administrative roles will be required to enroll in multifactor authentication using phone, SMS, or an authentication application. After enrollment, use of multifactor authentication will be required for future access to the environment.

Audit:

Ensure the multifactor authentication configuration for administrators:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. 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`.
4. The minimum list of `Directory roles` can be found in the Remediation section.

To verify the multifactor authentication configuration for administrators using SecureScore:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Select `Secure score`.
3. Select `Recommended actions`.
4. Click on `Require multifactor authentication for administrative roles`.
5. Review 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:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Click `New policy`.
4. Go to `Assignments` > `Users and groups` > `Include` > `Select users and groups` > check `Directory roles`.
5. At a minimum, select the `Directory roles listed` below in this section of the document.
6. Go to `Cloud apps or actions` > `Cloud apps` > `Include` > select `All cloud apps (and don't exclude any apps)`.
7. Under `Access controls` > `Grant` > select `Grant access` > check `Require multi-factor authentication` (and nothing else).
8. Leave all other conditions blank.
9. Make sure the policy is enabled.
10. Create.

At minimum these directory roles should be included for MFA:

- Application administrator
- Authentication administrator
- Billing administrator
- Cloud application administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Global reader
- Helpdesk administrator
- Password administrator
- Privileged authentication administrator
- Privileged role administrator
- Security administrator
- SharePoint administrator
- User administrator

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.2.2.2 (L1) Ensure multifactor authentication is enabled for all users (Manual)

Profile Applicability:

- E3 Level 1

Description:

Enable multifactor authentication for all users in the Microsoft 365 tenant. Users will be prompted to authenticate with a second factor upon logging in to Microsoft 365 services. The second factor is most commonly a text message to a registered mobile phone number where they type in an authorization code, or with a mobile application like Microsoft Authenticator.

Rationale:

Multifactor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multifactor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multifactor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact:

Implementation of multifactor authentication for all users will necessitate a change to user routine. All users will be required to enroll in multifactor authentication using phone, SMS, or an authentication application. After enrollment, use of multifactor authentication will be required for future authentication to the environment.

NOTE: Organizations that have difficulty enforcing MFA globally due lack of the budget to provide company owned mobile devices to every user, or equally are unable to force end users to use their personal devices due to regulations, unions, or policy have another option. FIDO2 Security keys may be used as a stand in for this recommendation. They are more secure, phishing resistant, and are affordable for an organization to issue to every end user.

Audit:

Ensure multifactor authentication is enabled for all users in all roles:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. 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 Audit using SecureScore:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com.
2. Select `Secure score`.
3. Select `Recommended actions`.
4. Click on `Require multifactor authentication for administrative roles`.
5. Review 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 all users:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Click `New policy`.
4. Go to `Assignments` > `Users and groups` > `Include` > select `All users` (and do not exclude any user).
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. Leave all other conditions blank.
8. Make sure the policy is Enabled/On.
9. Create.

Default Value:

Disabled

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa
2. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa
3. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.reports/update-mgreportauthenticationmethoduserregistrationdetail?view=graph-powershell-1.0#-isadmin

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.2.2.3 (L1) Enable Conditional Access policies to block legacy authentication (Manual)

Profile Applicability:

- E3 Level 1

Description:

Entra ID supports the most widely used authentication and authorization protocols including legacy authentication. This authentication pattern includes basic authentication, a widely used industry-standard method for collecting username and password information.

The following messaging protocols support legacy authentication:

- Authenticated SMTP - Used to send authenticated email messages.
- Autodiscover - Used by Outlook and EAS clients to find and connect to mailboxes in Exchange Online.
- Exchange ActiveSync (EAS) - Used to connect to mailboxes in Exchange Online.
- Exchange Online PowerShell - Used to connect to Exchange Online with remote PowerShell. If you block Basic authentication for Exchange Online PowerShell, you need to use the Exchange Online PowerShell Module to connect. For instructions, see Connect to Exchange Online PowerShell using multifactor authentication.
- Exchange Web Services (EWS) - A programming interface that's used by Outlook, Outlook for Mac, and third-party apps.
- IMAP4 - Used by IMAP email clients.
- MAPI over HTTP (MAPI/HTTP) - Primary mailbox access protocol used by Outlook 2010 SP2 and later.
- Offline Address Book (OAB) - A copy of address list collections that are downloaded and used by Outlook.
- Outlook Anywhere (RPC over HTTP) - Legacy mailbox access protocol supported by all current Outlook versions.
- POP3 - Used by POP email clients.
- Reporting Web Services - Used to retrieve report data in Exchange Online.
- Universal Outlook - Used by the Mail and Calendar app for Windows 10.
- Other clients - Other protocols identified as utilizing legacy authentication.

Rationale:

Legacy authentication protocols do not support multi-factor authentication. These protocols are often used by attackers because of this deficiency. Blocking legacy authentication makes it harder for attackers to gain access.

NOTE: As of October 2022 Microsoft began disabling basic authentication in all tenants, except for those who requested special exceptions it should no longer be available in most tenants beyond Dec 31, 2022. Despite this CIS recommends the CA policy to remain in place to act as a defense in depth measure.

Impact:

Enabling this setting will prevent users from connecting with older versions of Office, ActiveSync or using protocols like IMAP, POP or SMTP and may require upgrades to older versions of Office, and use of mobile mail clients that support modern authentication.

This will also cause multifunction devices such as printers from using scan to e-mail function if they are using a legacy authentication method. Microsoft has mail flow best practices in the link below which can be used to configure a MFP to work with modern authentication:

https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365

Audit:

Ensure a Conditional Access policy to block legacy authentication is enabled:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Verify that either the policy `Baseline policy: Block legacy authentication` is set to `On` or find another with the following settings enabled:
   - Under `Conditions` then `Client apps` ensure the settings are enabled for and `Exchange ActiveSync clients` and `other clients`.
   - Under `Access controls` ensure the `Grant` is set to `Block access`
   - Under `Assignments` ensure `All users` is enabled
   - Under `Assignments` and `Users and groups` ensure the `Exclude` is set to least one low risk account or directory role. This is required as a best practice.

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

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

Remediation:

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

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Create a new policy by selecting `New policy`.
4. Set the following conditions within the policy.
    - Select `Conditions` then `Client apps` enable the settings for and `Exchange ActiveSync clients` and `other clients`.
    - Under `Access controls` set the `Grant` section to `Block access`
    - Under `Assignments` enable `All users`
    - Under `Assignments` and `Users and groups` set the `Exclude` to be at least one low risk account or directory role. This is required as a best practice.

Default Value:

Basic authentication is disabled by default as of January 2023.

References:

1. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online
2. https://learn.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365
3. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online

Additional Information:

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

AUDIT

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

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

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

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

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

REMEDIATION

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

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

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

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

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

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

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

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

Profile Applicability:

- E3 Level 1

Description:

In complex deployments, organizations might have a need to restrict authentication sessions. Conditional Access policies allow for the targeting of specific user accounts. Some scenarios might include:

- Resource access from an unmanaged or shared device
- Access to sensitive information from an external network
- High-privileged users
- Business-critical applications

Ensure Sign-in frequency does not exceed `4 hours` for E3 tenants, or `24 hours` for E5 tenants using Privileged Identity Management.

Ensure `Persistent browser session` is set to `Never persist`

NOTE: This CA policy can be added to the previous CA policy in this benchmark "Ensure multifactor authentication is enabled for all users in administrative roles"

Rationale:

Forcing a time out for MFA will help ensure that sessions are not kept alive for an indefinite period of time, ensuring that browser sessions are not persistent will help in prevention of drive-by attacks in web browsers, this also prevents creation and saving of session cookies leaving nothing for an attacker to take.

Impact:

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

Audit:

Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Protection` > `Conditional Access` Select `Policies`.
3. Review the list of policies and ensure that there is a policy that have `Sign-in frequency` set to the time determined by your organization and that `Persistent browser session` is set to `Never persistent`.
4. Ensure `Sign-in frequency` does not exceed `4 hours` for E3 tenants. E5 tenants using PIM may be set to a maximum of `24 hours`.

- A list of directory role applying to Administrators can be found in the remediation section.

Remediation:

To configure Sign-in frequency and browser sessions persistence for Administrative users:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Protection` > `Conditional Access` Select `Policies`.
3. Click `New policy`
4. Click `Users and groups`
5. Under **Include** select `Select users and groups` and then select `Directory roles`.
6. At a minimum, select the roles in the section below.
7. Go to `Cloud apps or actions` > `Cloud apps` > `Include` > select `All cloud apps (and don't exclude any apps)`.
8. Under `Access controls` > `Grant` > select `Grant access` > check `Require multi-factor authentication` (and nothing else).
9. Under `Session` select `Sign-in frequency` and set to at most `4 hours` for E3 tenants. E5 tenants with PIM can be set to a maximum value of `24 hours`.
10. Check `Persistent browser session` then select `Never persistent` in the drop-down menu.
11. For `Enable Policy` select `On` and click `Save`

At minimum these directory roles should be included for MFA:

- Application administrator
- Authentication administrator
- Billing administrator
- Cloud application administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Global reader
- Helpdesk administrator
- Password administrator
- Privileged authentication administrator
- Privileged role administrator
- Security administrator
- SharePoint administrator
- User administrator

Default Value:

The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.2.2.5 (L2) Ensure 'Phishing-resistant MFA strength' is required for Administrators (Manual)

Profile Applicability:

- E3 Level 2

Description:

Authentication strength is a Conditional Access control that allows administrators to specify which combination of authentication methods can be used to access a resource. For example, they can make only phishing-resistant authentication methods available to access a sensitive resource. But to access a non-sensitive resource, they can allow less secure multifactor authentication (MFA) combinations, such as password + SMS.

Microsoft has 3 built-in authentication strengths. MFA strength, Passwordless MFA strength, and Phishing-resistant MFA strength. Ensure administrator roles are using a CA policy with `Phishing-resistant MFA strength`.

Administrators can then enroll using one of 3 methods:

- FIDO2 Security Key
- Windows Hello for Business
- Certificate-based authentication (Multi-Factor)

NOTE: Additional steps to configure methods such as FIDO2 keys are not covered here but can be found in related MS articles in the references section. The Conditional Access policy only ensures 1 of the 3 methods is used.

WARNING: Administrators should be pre-registered for a strong authentication mechanism before this Conditional Access Policy is enforced. Additionally, as stated elsewhere in the CIS Benchmark a break-glass administrator account should be excluded from this policy to ensure unfettered access in the case of an emergency.

Rationale:

Sophisticated attacks targeting MFA are more prevalent as the use of it becomes more widespread. These 3 methods are considered phishing-resistant as they remove passwords from the login workflow. It also ensures that public/private key exchange can only happen between the devices and a registered provider which prevents login to fake or phishing websites.

Impact:

If administrators aren't pre-registered for a strong authentication method prior to a conditional access policy being created, then a condition could occur where a user can't register for strong authentication because they don't meet the conditional access policy requirements and therefore are prevented from signing in.

Audit:

Ensure phishing-resistant MFA is enabled for users in administrative roles:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Review the list of policies and ensure that there is a policy with the `Grant` access control set to `Require authentication strength (Preview)`: `Phishing-resistant MFA`
4. Ensure the above policy conforms to these settings:
   - `Users` > `Include` > `Select users and groups` > `Directory Roles` to include at minimum the roles listed in the remediation section.
   - `Cloud apps or actions` > `All cloud apps`
   - `Grant` > `Grant Access` with `Require authentication strength (Preview)`: `Phishing-resistant MFA` set.
5. The policy is set to `On`.

Remediation:

To create a phishing-resistant MFA CA policy for users in administrative roles:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Click `New policy`.
4. Go to `Users` > `Users and groups` > `Include` > `Select users and groups` > `Directory roles`
5. Add at least the `Directory roles` listed after these steps.
6. Select `Cloud apps or actions` > `All cloud apps` (and don't exclude any apps).
7. `Grant` > `Grant Access` with `Require authentication strength (Preview)`: `Phishing-resistant MFA`
8. Click `Select'
9. Set `Enable policy` to `Report-only` and click `Create`

At minimum these directory roles should be included for the policy:

- Application administrator
- Authentication administrator
- Billing administrator
- Cloud application administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Global reader
- Helpdesk administrator
- Password administrator
- Privileged authentication administrator
- Privileged role administrator
- Security administrator
- SharePoint administrator
- User administrator

WARNING: Ensure administrators are pre-registered with strong authentication before enforcing the policy. After which the policy must be set to `On`.

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless#fido2-security-keys
2. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key
3. https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths
4. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●

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

Profile Applicability:

- E5 Level 2

Description:

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

Note: While Identity Protection also provides two risk policies with limited conditions, Microsoft highly recommends setting up risk-based policies in Conditional Access as opposed to the "legacy method" for the following benefits:

- Enhanced diagnostic data
- Report-only mode integration
- Graph API support
- Use more Conditional Access attributes like sign-in frequency in the policy

Rationale:

With the user risk policy turned on, Azure AD detects the probability that a user account has been compromised. Administrators can configure a user risk conditional access policy to automatically respond to a specific user risk level.

Impact:

Upon policy activation, account access will be either blocked or the user will be required to use multi-factor authentication (MFA) and change their password. Users without registered MFA will be denied access, necessitating an admin to recover the account. To avoid inconvenience, it is advised to configure the MFA registration policy for all users under the User Risk policy.

Additionally, users identified in the Risky Users section will be affected by this policy. To gain a better understanding of the impact on the organization's environment, the list of Risky Users should be reviewed before enforcing the policy.

Audit:

Ensure a user risk policy is enabled:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Ensure that a policy exist with the following characteristics and is set to `On`:
    - Under `Users or workload identities` choose `All users`
    - Under `Cloud apps or actions` choose `All cloud apps`
    - Under `Conditions` choose `User risk` then `Yes` is set to `High`.
    - Under `Access Controls` select `Grant` then in the right pane click `Grant access`, then select `Require multifactor authentication` and `Require password change`.
    - Under `Session` ensure `Sign-in frequency` is set to `Every time`.

Remediation:

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

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Create a new policy by selecting `New policy`.
4. Set the following conditions within the policy:
    - Under `Users or workload identities` choose `All users`
    - Under `Cloud apps or actions` choose `All cloud apps`
    - Under `Conditions` choose `User risk` then `Yes` and select the user risk level `High`.
    - Under `Access Controls` select `Grant` then in the right pane click `Grant access` then select `Require multifactor authentication` and `Require password change`.
    - Under `Session` ensure `Sign-in frequency` is set to `Every time`.
5. Click `Select`.
6. You may opt to begin in a state of `Report Only` as you step through implementation however, the policy will need to be set to `On` to be in effect.
7. Click `Create`.

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

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback
2. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.3 Deploy a Network Intrusion Detection Solution Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

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

Profile Applicability:

- E5 Level 2

Description:

Azure Active Directory Identity Protection sign-in risk detects risks in real-time and offline. A risky sign-in is an indicator for a sign-in attempt that might not have been performed by the legitimate owner of a user account.

Note: While Identity Protection also provides two risk policies with limited conditions, Microsoft highly recommends setting up risk-based policies in Conditional Access as opposed to the "legacy method" for the following benefits:

- Enhanced diagnostic data
- Report-only mode integration
- Graph API support
- Use more Conditional Access attributes like sign-in frequency in the policy

Rationale:

Turning on the sign-in risk policy ensures that suspicious sign-ins are challenged for multi-factor authentication.

Impact:

When the policy triggers, the user will need MFA to access the account. In the case of a user who hasn't registered MFA on their account, they would be blocked from accessing their account. It is therefore recommended that the MFA registration policy be configured for all users who are a part of the Sign-in Risk policy.

Audit:

To ensure Sign-In a risk policy is enabled:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Ensure that a policy exist with the following characteristics and is set to `On`:
    - Under `Users or workload identities` choose `All users`
    - Under `Cloud apps or actions` choose `All cloud apps`
    - Under `Conditions` choose `Sign-in risk` then `Yes` ensuring `High` and `Medium` are selected.
    - Under `Access Controls` select `Grant` then in the right pane click `Grant access` then select `Require multifactor authentication`.
    - Under `Session` select `Sign-in Frequency` is set to `Every time`.

Remediation:

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

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Create a new policy by selecting `New policy`.
4. Set the following conditions within the policy.
    - Under `Users or workload identities` choose `All users`
    - Under `Cloud apps or actions` choose `All cloud apps`
    - Under `Conditions` choose `Sign-in risk` then `Yes` and check the risk level boxes `High` and `Medium`
    - Under `Access Controls` select `Grant` then in the right pane click `Grant access` then select `Require multifactor authentication`.
    - Under `Session` select `Sign-in Frequency` and set to `Every time`.
5. Click `Select`
6. You may opt to begin in a state of `Report Only` as you step through implementation however, the policy will need to be set to `On` to be in effect.
7. Click `Create`.

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

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback
2. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.3 Deploy a Network Intrusion Detection Solution Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

5.2.2.8 (L1) Ensure 'Microsoft Azure Management' is limited to administrative roles (Manual)

Profile Applicability:

- E3 Level 1

Description:

The Microsoft Azure Management application governs various Azure services and can be secured through the implementation of a Conditional Access policy. This policy can restrict specific user accounts from accessing the related portals and applications.

When Conditional Access policy is targeted to the Microsoft Azure Management application, within the Conditional Access policy app picker the policy will be enforced for tokens issued to application IDs of a set of services closely bound to the portal.

- Azure Resource Manager
- Azure portal, which also covers the Microsoft Entra admin center
- Azure Data Lake
- Application Insights API
- Log Analytics API

`Microsoft Azure Management` should be restricted to specific pre-determined administrative roles.

NOTE: Blocking Microsoft Azure Management will prevent non-privileged users from signing into most portals other than Microsoft 365 Defender and Microsoft Purview.

Rationale:

Blocking sign-in to Azure Management applications and portals enhances security of sensitive data by restricting access to privileged users. This mitigates potential exposure due to administrative errors or software vulnerabilities, as well as acting as a defense in depth measure against security breaches.

Impact:

PIM functionality will be impacted unless non-privileged users are first assigned to a permanent group or role that is excluded from this policy. When attempting to checkout a role in the Entra ID PIM area they will receive the message "You don't have access to this Your sign-in was successful but you don't have permission to access this resource."

Because the policy is applied to the Azure management portal and API, services, or clients with an Azure API service dependency, can indirectly be impacted:

```
Classic deployment model APIs
Azure PowerShell
Azure CLI
Azure DevOps
Azure Data Factory portal
Azure Event Hubs
Azure Service Bus
Azure SQL Database
SQL Managed Instance
Azure Synapse
Visual Studio subscriptions administrator portal
Microsoft IoT Central
```

Audit:

Ensure Microsoft Azure Management is restricted:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Inspect and identify existing policies for the parameters below:
   - `Users` set to `Include All Users`
   - `Users` > `Exclude` Verify `Guest or external users` and `Users and groups` are unchecked.
   - `Users` > `Exclude` Verify `Directory Roles` only contains administrative roles. See below for details on roles.
   - `Cloud apps or actions` `Select` `Microsoft Azure Management`
   - `Grant` is equal to `Block Access`
   - `Enable policy` is set to `On`
4. If any of these conditions are not met, then the audit fails.

Directory Roles and Exclusions

In `Directory roles` > `Exclude` the role `Global Administrator` at a minimum should be selected to avoid I.T. being locked out. The organization should pre-determine roles in the exclusion list as there is not a one size fits all. Auditors and system administrators should exercise due diligence balancing operation while exercising least privilege. As the size of the organization increases so will the number of roles being utilized.
A an example starting list of Administrator roles can be found under **Additional Information**

Remediation:

To enable Microsoft Azure Management restrictions:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` > `Conditional Access` select `Policies`.
3. Click `New Policy` and then name the policy.
4. Select `Users` > `Include` > `All Users`
5. Select `Users` > `Exclude` > `Directory roles` and select only administrative roles. See audit section for more information.
6. Select `Cloud apps or actions` > `Select apps` > `Select` then click the box next to `Microsoft Azure Management`.
7. Click `Select`.
8. Select `Grant` > `Block access` and click `Select`.
9. Ensure `Enable Policy` is `On` then click `Create`.

WARNING: Exclude `Global Administrator` at a minimum to avoid being locked out. Report-only is a good option to use when testing any Conditional Access policy for the first time.

Default Value:

No - Non-administrators can access the Azure AD administration portal.

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-cloud-apps

Additional Information:

Below is an example list of Administrator roles that could be excluded

- Application administrator
- Authentication administrator
- Billing administrator
- Cloud application administrator
- Conditional Access administrator
- Exchange administrator
- Global administrator
- Global reader
- Helpdesk administrator
- Password administrator
- Privileged authentication administrator
- Privileged role administrator
- Security administrator
- SharePoint administrator
- User administrator

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

5.2.3 Authentication Methods

5.2.3.1 (L1) Ensure Microsoft Authenticator is configured to protect against MFA fatigue (Manual)

Profile Applicability:

- E3 Level 1

Description:

Microsoft has released additional settings to enhance the configuration of the Microsoft Authenticator application. These settings provide additional information and context to users who receive MFA passwordless and push requests, such as geographic location the request came from, the requesting application and requiring a number match.

Ensure the following are `Enabled`.

- `Require number matching for push notifications`
- `Show application name in push and passwordless notifications`
- `Show geographic location in push and passwordless notifications`

NOTE: On February 27, 2023 Microsoft started enforcing number matching tenant-wide for all users using Microsoft Authenticator.

Rationale:

As the use of strong authentication has become more widespread, attackers have started to exploit the tendency of users to experience "MFA fatigue." This occurs when users are repeatedly asked to provide additional forms of identification, leading them to eventually approve requests without fully verifying the source. To counteract this, number matching can be employed to ensure the security of the authentication process. With this method, users are prompted to confirm a number displayed on their original device and enter it into the device being used for MFA. Additionally, other information such as geolocation and application details are displayed to enhance the end user's awareness. Among these 3 options, number matching provides the strongest net security gain.

Impact:

Additional interaction will be required by end users using number matching as opposed to simply pressing "Approve" for login attempts.

Audit:

To ensure Microsoft Authenticator is configured to be resistant to MFA fatigue:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click to expand `Protection` > `Authentication methods` select `Policies`.
3. Under **Method** select `Microsoft Authenticator`.
4. Under `Enable and Target` verify the setting is set to `Enable`.
5. Select `Configure`
6. Verify the following Microsoft Authenticator settings:
    - `Require number matching for push notifications` Status is set to `Enabled`, Target `All users`
    - `Show application name in push and passwordless notifications` is set to `Enabled`, Target `All users`
    - `Show geographic location in push and passwordless notifications` is set to `Enabled`, Target `All users`

Remediation:

To configure Microsoft Authenticator to protect against MFA fatigue:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click to expand `Protection` > `Authentication methods` select `Policies`.
3. Select `Microsoft Authenticator`
4. Under `Enable and Target` ensure the setting is set to `Enable`.
5. Select `Configure`
6. Set the following Microsoft Authenticator settings:
    - `Require number matching for push notifications` Status is set to `Enabled`, Target `All users`
    - `Show application name in push and passwordless notifications` is set to `Enabled`, Target `All users`
    - `Show geographic location in push and passwordless notifications` is set to `Enabled`, Target `All users`

Default Value:

Microsoft-managed

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-default-enablement
2. https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677
3. https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●

5.2.3.2 (L1) Ensure custom banned passwords lists are used (Manual)

Profile Applicability:

- E3 Level 1

Description:

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support business and security needs, custom banned password lists can be defined. When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords.

A custom banned password list should include some of the following examples:

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific internal terms
- Abbreviations that have specific company meaning

Rationale:

Creating a new password can be difficult regardless of one's technical background. It is common to look around one's environment for suggestions when building a password, however, this may include picking words specific to the organization as inspiration for a password. An adversary may employ what is called a 'mangler' to create permutations of these specific words in an attempt to crack passwords or hashes making it easier to reach their goal.

Impact:

If a custom banned password list includes too many common dictionary words, or short words that are part of compound words, then perfectly secure passwords may be blocked. The organization should consider a balance between security and usability when creating a list.

Audit:

Ensure a custom banned password list is in place:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Protection` > `Authentication methods`
3. Select `Password protection`
4. Verify `Enforce custom list` is set to `Yes`
5. Verify `Custom banned password list` contains entries specific to the organization, or matches a pre-determined list.

Remediation:

Create a custom banned password list:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Protection` > `Authentication methods`
3. Select `Password protection`
4. Set `Enforce custom list` to `Yes`
5. In `Custom banned password list` create a list using suggestions outlined in this document.
6. Click `Save`

NOTE: Below is a list of examples that can be used as a starting place. The references section contains more suggestions.

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific internal terms
- Abbreviations that have specific company meaning

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#custom-banned-password-list
2. https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

5.2.3.3 (L1) Ensure password protection is enabled for on-prem Active Directory (Manual)

Profile Applicability:

- E3 Level 1

Description:

Azure Active Directory (Azure AD) Password Protection provides a global and custom banned password list. A password change request fails if there's a match in these banned password list. To protect on-premises Active Directory Domain Services (AD DS) environment, install and configure Azure AD Password Protection.

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

Rationale:

Azure Active Directory protects an organization by prohibiting the use of weak or leaked passwords. In addition, organizations can create custom banned password lists to prevent their users from using easily guessed passwords that are specific to their industry. Deploying this feature to Active Directory will strengthen the passwords that are used in the environment.

Impact:

The potential impact associated with implementation of this setting is dependent upon the existing password policies in place in the environment. For environments that have strong password policies in place, the impact will be minimal. For organizations that do not have strong password policies in place, implementation of Azure Active Directory Password Protection may require users to change passwords, and adhere to more stringent requirements than they have been accustomed to.

Audit:

Ensure that password protection is enabled for Active Directory:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Protection` select `Authentication methods`.
3. Select `Password protection` and ensure that `Enable password protection on Windows Server Active Directory` is set to `Yes` and that `Mode` is set to `Enforced`.

Remediation:

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

- Download and install the `Azure AD Password Proxies` and `DC Agents` from the following location: https://www.microsoft.com/download/details.aspx?id=57071 After installed follow the steps below.

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Protection` select `Authentication methods`.
3. Select `Password protection` and set `Enable password protection on Windows Server Active Directory` to `Yes` and `Mode` to `Enforced`.

Default Value:

Enable - Yes

Mode - Audit

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations

CIS Controls:

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

5.2.4 Password reset

5.2.4.1 (L1) Ensure 'Self service password reset enabled' is set to 'All' (Manual)

Profile Applicability:

- E3 Level 1

Description:

Enabling self-service password reset allows users to reset their own passwords in Azure AD. When users sign in to Microsoft 365, they will be prompted to enter additional contact information that will help them reset their password in the future. If combined registration is enabled additional information, outside of multi-factor, will not be needed.

NOTE: Effective Oct. 1st, 2022, Microsoft will begin to enable combined registration for all users in Azure AD tenants created before August 15th, 2020. Tenants created after this date are enabled with combined registration by default.

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.

Impact:

Users will be required to provide additional contact information to enroll in self-service password reset. Additionally, minor user education may be required for users that are used to calling a help desk for assistance with password resets.

NOTE: This is unavailable if using Azure AD Connect / Sync in a hybrid environment.

Audit:

Ensure self-service password reset is enabled:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Protection` > `Password reset` select `Properties`.
3. Ensure `Self service password reset enabled` is set to `All`

Remediation:

To enable self-service password reset:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Protection` > `Password reset` select `Properties`.
3. Set `Self service password reset enabled` to `All`

References:

1. https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/let-users-reset-passwords?view=o365-worldwide
2. https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr
3. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-registration-mfa-sspr-combined

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- E3 Level 1

Description:

The Microsoft 365 platform allows users 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. The self-service password reset activity report should be review 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 self-service password reset activity report:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Protection` > `Password reset` select `Audit logs`.
3. Review the list of users who have reset their passwords by setting the `Date` to `Last 7 days` and `Service` to `Self-service Password Management`

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-reporting
2. https://learn.microsoft.com/en-us/azure/active-directory/authentication/troubleshoot-sspr

CIS Controls:

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

5.2.5 Custom security attributes

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

5.2.6 Risky activities

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

Profile Applicability:

- E5 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 tenant from a client IP address that has been recognized by Microsoft as an anonymous proxy IP address (such as a TOR network)
- successful sign-ins from users where two sign-ins appeared to originate from different regions and the time between sign-ins makes it impossible for the user to have traveled between those regions

Rationale:

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

Audit:

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

Remediation:

To review the Azure AD 'Risky sign-ins' report:

1. Navigate to the `Microsoft Entra admin center` https://entra.microsoft.com.
2. Click expand `Protection` select `Risky activities`.
3. Under `Report` click on `Risky sign-ins`.
4. Review by `Risk level (aggregate)`.

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
2. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock

CIS Controls:

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

5.3 Identity Governance

5.3.1 (L2) Ensure 'Privileged Identity Management' is used to manage roles (Manual)

Profile Applicability:

- E5 Level 2

Description:

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

Rationale:

Organizations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of a malicious actor getting that access, or an authorized user inadvertently impacting a sensitive resource. However, users still need to carry out privileged operations in Azure AD and Office 365. Organizations can give users just-in-time (JIT) privileged access to roles. There is a need for oversight for what those users are doing with their administrator privileges. PIM helps to mitigate the risk of excessive, unnecessary, or misused access rights.

Impact:

Implementation of Just in Time privileged access is likely to necessitate changes to administrator routine. Administrators will only be granted access to administrative roles when required. When administrators request role activation, they will need to document the reason for requiring role access, anticipated time required to have the access, and to reauthenticate to enable role access.

Audit:

Ensure Use Just In Time privileged access to Office 365 roles:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity Governance` select `Privileged Identity Management`.
3. Select `Azure AD Roles`.
4. Select `Roles` beneath **Manage**.
5. Inspect at a minimum the following sensitive roles to ensure 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 Use Just In Time privileged access to Office 365 roles, use the following steps:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/.
2. Click to expand `Identity Governance` select `Privileged Identity Management`.
3. Select `Azure AD Roles`.
4. Select `Roles` beneath **Manage**.
5. Inspect at a minimum the following sensitive roles. For each of the members that have an `ASSIGNMENT TYPE` of `Permanent`, click on the `...` and choose `Make eligible`:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

5.3.2 (L1) Ensure 'Access reviews' for Guest Users are configured (Manual)

Profile Applicability:

- E5 Level 1

Description:

Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organization.

Ensure `Access reviews` for Guest Users are configured to be performed no less frequently than `monthly`.

Rationale:

Access to groups and applications for guests can change over time. If a guest user's access to a particular folder goes unnoticed, they may unintentionally gain access to sensitive data if a member adds new files or data to the folder or application. Access reviews can help reduce the risks associated with outdated assignments by requiring a member of the organization to conduct the reviews. Furthermore, these reviews can enable a fail-closed mechanism to remove access to the subject if the reviewer does not respond to the review.

Impact:

Access reviews that are ignored may cause guest users to lose access to resources temporarily.

Audit:

Verify an access review for Guest Users is in place:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity Governance` and select `Access reviews`
3. Inspect the access reviews, and ensure an access review is created with the following criteria:
    - `Overview`: `Scope` is set to `Guest users only` and status is `Active`
    - `Reviewers`: Ensure appropriate reviewer(s) are designated.
    - `Settings` > `General`: `Mail notifications` and `Reminders` are set to `Enable`
    - `Reviewers`: `Require reason on approval` is set to `Enable`
    - `Scheduling`: `Frequency` is `Monthly` or more frequent.
    - `When completed`: `Auto apply results to resource` is set to `Enable`
    - `When completed`: `If reviewers don't respond` is set to `Remove access`

Remediation:

Create an access review for Guest Users:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity Governance` and select `Access reviews`
3. Click `New access review`.
4. `Select what to review` choose `Teams + Groups`.
5. `Review Scope` set to `All Microsoft 365 groups with guest users`, do not exclude groups.
6. `Scope` set to `Guest users only` then click `Next: Reviews`.
7. `Select reviewers` an appropriate user that is NOT the guest user themselves.
8. `Duration (in days)` at most `3`.
9. `Review recurrence` is `Monthly` or more frequent.
10. `End` is set to `Never`, then click `Next: Settings`.
11. Check `Auto apply results to resource`.
12. Set `If reviewers don't respond` to `Remove access`.
13. Check the following: `Justification required`, `E-mail notifications`, `Reminders`.
14. Click `Next: Review + Create` and finally click `Create`.

Default Value:

By default access reviews are not configured.

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review
2. https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person’s name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●

5.3.3 (L1) Ensure 'Access reviews' for high privileged Azure AD roles are configured (Manual)

Profile Applicability:

- E5 Level 1

Description:

Access reviews enable administrators to establish an efficient automated process for reviewing group memberships, access to enterprise applications, and role assignments. These reviews can be scheduled to recur regularly, with flexible options for delegating the task of reviewing membership to different members of the organization.

Ensure `Access reviews` for high privileged Azure AD roles are done no less frequently than `weekly`. These reviews should include **at a minimum** the roles listed below:

- Global Administrator
- Exchange Administrator
- SharePoint Administrator
- Teams Administrator
- Security Administrator

NOTE: An access review is created for each role selected after completing the process.

Rationale:

Regular review of critical high privileged roles in Azure AD will help identify role drift, or potential malicious activity. This will enable the practice and application of "separation of duties" where even non-privileged users like security auditors can be assigned to review assigned roles in an organization. Furthermore, if configured these reviews can enable a fail-closed mechanism to remove access to the subject if the reviewer does not respond to the review.

Audit:

Verify access reviews for high privileged roles is in place:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity Governance` and select `Privileged Identity Management`
3. Select `Azure AD Roles` under Manage
4. Select `Access reviews`
5. Ensure there are access reviews configured for each high privileged roles and each meets the criteria laid out below:
   - `Scope` - `Everyone`
   - `Status` - `Active`
   - `Reviewers` - Role reviewers should be designated personnel. Preferably not a self-review.
   - `Mail notifications` - `Enable`
   - `Reminders` - `Enable`
   - `Require reason on approval` - `Enable`
   - `Frequency` - `Monthly` or more frequent
   - `Duration (in days)` - `4` at most
   - `Auto apply results to resource` - `Enable`
   - `If reviewers don't respond` - `No change`

Any remaining settings are discretionary.

NOTE: Reviewers will have the ability to revoke roles should be trusted individuals who understand the impact of the access reviews. The principal of separation of duties should be considered so that no one administrator is reviewing their own access levels.

NOTE2: The setting `If reviewers don't respond` is recommended to be set to `Remove access` due to the potential of all Global Administrators being unassigned if the review is not addressed.

Remediation:

Create an access review for high privileged roles:

1. Navigate to `Microsoft Entra admin center` https://entra.microsoft.com/
2. Click to expand `Identity Governance` and select `Privileged Identity Management`
3. Select `Azure AD Roles` under Manage
4. Select `Access reviews` and click `New access review`.
5. Provide a name and description.
6. `Frequency` set to `Weekly` or more frequent.
7. `Duration (in days)` is set to at most `3`.
8. `End` set to `Never`.
9. `Role` select these roles: `Global Administrator`,`Exchange Administrator`,`SharePoint Administrator`,`Teams Administrator`,`Security Administrator`
10. `Assignment type` set to `All active and eligible assignments`.
11. `Reviewers` set to `Selected user(s) or group(s)`
12. `Select reviewers` are member(s) responsible for this type of review.
13. `Auto apply results to resource` set to `Enable`
14. `If reviewers don't respond` is set to `No change`
15. `Show recommendations` set to `Enable`
16. `Require reason or approval` set to `Enable`
17. `Mail notifications` set to `Enable`
18. `Reminders` set to `Enable`
19. Click `Start` to save the review.

NOTE: Reviewers will have the ability to revoke roles should be trusted individuals who understand the impact of the access reviews. The principal of separation of duties should be considered so that no one administrator is reviewing their own access levels.

Default Value:

By default access reviews are not configured.

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review
2. https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●

6 Exchange admin center

The Exchange admin center contains settings related to everything Exchange Online.

Direct link: https://admin.exchange.microsoft.com/

The PowerShell module most commonly used in this section is `ExchangeOnlineManagement` and uses `Connect-ExchangeOnline` as the connection cmdlet.

The latest version of the module can be downloaded here: https://www.powershellgallery.com/packages/ExchangeOnlineManagement/

6.1 Audit

6.1.1 (L1) Ensure 'AuditDisabled' organizationally is set to 'False' (Automated)

Profile Applicability:

- E3 Level 1

Description:

The value False indicates that mailbox auditing on by default is turned on for the organization. Mailbox auditing on by default in the organization overrides the mailbox auditing settings on individual mailboxes. For example, if mailbox auditing is turned off for a mailbox (the AuditEnabled property on the mailbox is False), the default mailbox actions are still audited for the mailbox, because mailbox auditing on by default is turned on for the organization.

Turning off mailbox auditing on by default ($true) has the following results:

- Mailbox auditing is turned off for your organization.
- From the time you turn off mailbox auditing on by default, no mailbox actions are audited, even if mailbox auditing is enabled on a mailbox (the AuditEnabled property on the mailbox is True).
- Mailbox auditing isn't turned on for new mailboxes and setting the AuditEnabled property on a new or existing mailbox to True is ignored.
- Any mailbox audit bypass association settings (configured by using the Set-MailboxAuditBypassAssociation cmdlet) are ignored.
- Existing mailbox audit records are retained until the audit log age limit for the record expires.

The recommended state for this setting is `False` at the organization level. This will enable auditing and enforce the default.

Rationale:

Enforcing the default ensures auditing was not turned off intentionally or accidentally. Auditing mailbox actions will allow forensics and IR teams to trace various malicious activities that can generate TTPs caused by inbox access and tampering.

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

Impact:

None - this is the default behavior as of 2019.

Audit:

Ensure mailbox auditing is enabled by default at the organizational level:

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

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

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

Remediation:

Enable mailbox auditing at the organizational level:

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

```
Set-OrganizationConfig -AuditDisabled $false
```

Default Value:

False

References:

1. https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-mailboxes?view=o365-worldwide
2. https://learn.microsoft.com/en-us/powershell/module/exchange/set-organizationconfig?view=exchange-ps#-auditdisabled

CIS Controls:

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

6.1.2 (L1) Ensure mailbox auditing for E3 users is Enabled (Automated)

Profile Applicability:

- E3 Level 1

Description:

Mailbox audit logging is turned on by default in all organizations. This effort started in January 2019, and means that certain actions performed by mailbox owners, delegates, and admins are automatically logged. The corresponding mailbox audit records are available for admins to search in the mailbox audit log.

Mailboxes and shared mailboxes have actions assigned to them individually in order to audit the data the organization determines valuable at the mailbox level.

The recommended state is `AuditEnabled` to `True` on all user mailboxes along with additional audit actions beyond the Microsoft defaults.

Note: Due to some differences in defaults for audit actions this recommendation is specific to users assigned an E3 license only.

Rationale:

Whether it is for regulatory compliance or for tracking unauthorized configuration changes in Microsoft 365, enabling mailbox auditing, and ensuring the proper mailbox actions are accounted for allows for Microsoft 365 teams to run security operations, forensics or general investigations on mailbox activities.

The following mailbox types ignore the organizational default and must have `AuditEnabled` set to `True` at the mailbox level in order to capture relevant audit data.

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

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

Impact:

None - this is the default behavior.

Audit:

To manually verify mailbox auditing is enabled and configured for all mailboxes:

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

```
$MailAudit = Get-EXOMailbox -PropertySets Audit -ResultSize Unlimited |
    Select-Object UserPrincipalName, AuditEnabled, AuditAdmin, AuditDelegate,
AuditOwner

$MailAudit | Export-Csv -Path C:\CIS\AuditSettings.csv -NoTypeInformation
```

3. Analyze the output and verify `AuditEnabled` is set to `True` and all audit actions are included in what is defined in the script in the remediation section.

Optionally, this more comprehensive script can assess each user mailbox:

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

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

$DelegateActions = @(
    "ApplyRecord", "Create", "FolderBind", "HardDelete", "Move",
    "MoveToDeletedItems", "SendAs", "SendOnBehalf", "SoftDelete", "Update",
    "UpdateFolderPermissions", "UpdateInboxRules"
)

$OwnerActions = @(
    "ApplyRecord", "Create", "HardDelete", "MailboxLogin", "Move",
    "MoveToDeletedItems", "SoftDelete", "Update", "UpdateCalendarDelegation",
    "UpdateFolderPermissions", "UpdateInboxRules"
)

function VerifyActions {
    param (
        [string]$type,
        [array]$actions,
        [array]$auditProperty,
        [string]$mailboxName
    )

    $missingActions = @()
    $actionCount = 0

    foreach ($action in $actions) {
        if ($auditProperty -notcontains $action) {
            $missingActions += "    Failure: Audit action '$action' missing
from $type"
            $actionCount++
        }
    }

    if ($actionCount -eq 0) {
        Write-Host "[$mailboxName]: $type actions are verified." -
ForegroundColor Green
    } else {
        Write-Host "[$mailboxName]: $type actions are not all verified." -
ForegroundColor Red
        foreach ($missingAction in $missingActions) {
            Write-Host "    $missingAction" -ForegroundColor Red
        }
    }
}
```

```
$mailboxes = Get-EXOMailbox -PropertySets Audit,Minimum -ResultSize Unlimited
|
    Where-Object { $_.RecipientTypeDetails -eq "UserMailbox" }

foreach ($mailbox in $mailboxes) {
    Write-Host "--- Now assessing [$($mailbox.UserPrincipalName)] ---"

    if ($mailbox.AuditEnabled) {
        Write-Host "[$($mailbox.UserPrincipalName)]: AuditEnabled is true" -
ForegroundColor Green
    } else {
        Write-Host "[$($mailbox.UserPrincipalName)]: AuditEnabled is false" -
ForegroundColor Red
    }

    VerifyActions -type "AuditAdmin" -actions $AdminActions -auditProperty
$mailbox.AuditAdmin `
        -mailboxName $mailbox.UserPrincipalName
    VerifyActions -type "AuditDelegate" -actions $DelegateActions -
auditProperty $mailbox.AuditDelegate `
        -mailboxName $mailbox.UserPrincipalName
    VerifyActions -type "AuditOwner" -actions $OwnerActions -auditProperty
$mailbox.AuditOwner `
        -mailboxName $mailbox.UserPrincipalName

    Write-Host
}
```

Remediation:

To enable mailbox auditing for all user mailboxes using PowerShell:

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

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

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

$AuditOwner = @(
    "ApplyRecord", "Create", "HardDelete", "MailboxLogin", "Move",
    "MoveToDeletedItems", "SoftDelete", "Update", "UpdateCalendarDelegation",
    "UpdateFolderPermissions", "UpdateInboxRules"
)


$MBX = Get-EXOMailbox -ResultSize Unlimited | Where-Object {
$_.RecipientTypeDetails -eq "UserMailbox" }
$MBX | Set-Mailbox -AuditEnabled $true `
-AuditLogAgeLimit 90 -AuditAdmin $AuditAdmin -AuditDelegate $AuditDelegate `
-AuditOwner $AuditOwner
```

Default Value:

`AuditEnabled`: `True` for all mailboxes except below:

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

AuditAdmin: ApplyRecord, Create, HardDelete, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules

AuditDelegate: ApplyRecord, Create, HardDelete, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update, UpdateFolderPermissions, UpdateInboxRules

AuditOwner: ApplyRecord, HardDelete, MoveToDeletedItems, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules

References:

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

Additional Information:

Additional mailbox actions outside of the scope of this recommendations that can be audited for with an E5 license include:

- MailItemsAccessed
- SearchQueryInitiated
- Send

CIS Controls:

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

6.1.3 (L1) Ensure mailbox auditing for E5 users is Enabled (Automated)

Profile Applicability:

- E5 Level 1

Description:

Mailbox audit logging is turned on by default in all organizations. This effort started in January 2019, and means that certain actions performed by mailbox owners, delegates, and admins are automatically logged. The corresponding mailbox audit records are available for admins to search in the mailbox audit log.

Mailboxes and shared mailboxes have actions assigned to them individually in order to audit the data the organization determines valuable at the mailbox level.

The recommended state is `AuditEnabled` to `True` on all user mailboxes along with additional audit actions beyond the Microsoft defaults.

Note: Due to some differences in defaults for audit actions this recommendation is specific to users assigned an E5 license, or auditing addon license, only.

Rationale:

Whether it is for regulatory compliance or for tracking unauthorized configuration changes in Microsoft 365, enabling mailbox auditing and ensuring the proper mailbox actions are accounted for allows for Microsoft 365 teams to run security operations, forensics or general investigations on mailbox activities.

The following mailbox types ignore the organizational default and must have `AuditEnabled` set to `True` at the mailbox level in order to capture relevant audit data.

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

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

Impact:

None - this is the default behavior.

Audit:

To manually verify mailbox auditing is enabled and configured for all mailboxes:

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

```
$MailAudit = Get-EXOMailbox -PropertySets Audit -ResultSize Unlimited |
    Select-Object UserPrincipalName, AuditEnabled, AuditAdmin, AuditDelegate,
AuditOwner

$MailAudit | Export-Csv -Path C:\CIS\AuditSettings.csv -NoTypeInformation
```

3. Analyze the output and verify `AuditEnabled` is set to `True` and all audit actions are included in what is defined in the script in the remediation section.

Optionally, this more comprehensive script can assess each user mailbox:

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

```
$AdminActions = @(
    "ApplyRecord", "Copy", "Create", "FolderBind", "HardDelete",
    "MailItemsAccessed", "Move", "MoveToDeletedItems", "SendAs",
    "SendOnBehalf", "Send", "SoftDelete", "Update",
"UpdateCalendarDelegation",
    "UpdateFolderPermissions", "UpdateInboxRules"
    )

$DelegateActions = @(
    "ApplyRecord", "Create", "FolderBind", "HardDelete", "Move",
    "MailItemsAccessed", "MoveToDeletedItems", "SendAs", "SendOnBehalf",
    "SoftDelete", "Update", "UpdateFolderPermissions", "UpdateInboxRules"
)

$OwnerActions = @(
    "ApplyRecord", "Create", "HardDelete", "MailboxLogin", "Move",
    "MailItemsAccessed", "MoveToDeletedItems", "Send", "SoftDelete",
"Update",
    "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"
)

function VerifyActions {
    param (
        [string]$type,
        [array]$actions,
        [array]$auditProperty,
        [string]$mailboxName
    )

    $missingActions = @()
    $actionCount = 0

    foreach ($action in $actions) {
        if ($auditProperty -notcontains $action) {
            $missingActions += "    Failure: Audit action '$action' missing
from $type"
            $actionCount++
        }
    }

    if ($actionCount -eq 0) {
        Write-Host "[$mailboxName]: $type actions are verified." -
ForegroundColor Green
    } else {
        Write-Host "[$mailboxName]: $type actions are not all verified." -
ForegroundColor Red
        foreach ($missingAction in $missingActions) {
            Write-Host "    $missingAction" -ForegroundColor Red
        }
    }
}
```

```
$mailboxes = Get-EXOMailbox -PropertySets Audit,Minimum -ResultSize Unlimited
|
    Where-Object { $_.RecipientTypeDetails -eq "UserMailbox" }

foreach ($mailbox in $mailboxes) {
    Write-Host "--- Now assessing [$($mailbox.UserPrincipalName)] ---"

    if ($mailbox.AuditEnabled) {
        Write-Host "[$($mailbox.UserPrincipalName)]: AuditEnabled is true" -
ForegroundColor Green
    } else {
        Write-Host "[$($mailbox.UserPrincipalName)]: AuditEnabled is false" -
ForegroundColor Red
    }

    VerifyActions -type "AuditAdmin" -actions $AdminActions -auditProperty
$mailbox.AuditAdmin `
        -mailboxName $mailbox.UserPrincipalName
    VerifyActions -type "AuditDelegate" -actions $DelegateActions -
auditProperty $mailbox.AuditDelegate `
        -mailboxName $mailbox.UserPrincipalName
    VerifyActions -type "AuditOwner" -actions $OwnerActions -auditProperty
$mailbox.AuditOwner `
        -mailboxName $mailbox.UserPrincipalName

    Write-Host
}
```

Note: In order for a mailbox to pass the above it must have an E5 or Microsoft Purview Audit Premium addon license assigned to it. For the purposes of this recommendation shared mailboxes are ignored.

Remediation:

To enable mailbox auditing for all user mailboxes using PowerShell:

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

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

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

$AuditOwner = @(
    "ApplyRecord", "Create", "HardDelete", "MailboxLogin", "Move",
    "MailItemsAccessed", "MoveToDeletedItems", "Send", "SoftDelete",
"Update",
    "UpdateCalendarDelegation", "UpdateFolderPermissions", "UpdateInboxRules"
)


$MBX = Get-EXOMailbox -ResultSize Unlimited | Where-Object {
$_.RecipientTypeDetails -eq "UserMailbox" }
$MBX | Set-Mailbox -AuditEnabled $true `
-AuditLogAgeLimit 180 -AuditAdmin $AuditAdmin -AuditDelegate $AuditDelegate `
-AuditOwner $AuditOwner
```

Note: When running this script mailboxes without an E5 or Azure Audit Premium license applied will generate an error as they are not licensed for the additional actions which come default with E5.

Default Value:

`AuditEnabled`: `True` for all mailboxes except below:

- Resource Mailboxes
- Public Folder Mailboxes
- DiscoverySearch Mailbox

AuditAdmin: ApplyRecord, Create, HardDelete, MailItemsAccessed, MoveToDeletedItems, Send, SendAs, SendOnBehalf, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules

AuditDelegate: ApplyRecord, Create, HardDelete, MailItemsAccessed, MoveToDeletedItems, SendAs, SendOnBehalf, SoftDelete, Update, UpdateFolderPermissions, UpdateInboxRules

AuditOwner: ApplyRecord, HardDelete, MailItemsAccessed, MoveToDeletedItems, Send, SoftDelete, Update, UpdateCalendarDelegation, UpdateFolderPermissions, UpdateInboxRules

References:

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

CIS Controls:

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

6.1.4 (L1) Ensure 'AuditBypassEnabled' is not enabled on mailboxes (Manual)

Profile Applicability:

- E3 Level 1

Description:

When configuring a user or computer account to bypass mailbox audit logging, the system will not record any access or actions performed by the said user or computer account on any mailbox. Administratively this was introduced to reduce the volume of entries in the mailbox audit logs on trusted user or computer accounts.

Ensure `AuditBypassEnabled` is not enabled on accounts without a written exception.

Rationale:

If a mailbox audit bypass association is added for an account, the account can access any mailbox in the organization to which it has been assigned access permissions, without generating any mailbox audit logging entries for such access or recording any actions taken, such as message deletions.

Enabling this parameter, whether intentionally or unintentionally, could allow insiders or malicious actors to conceal their activity on specific mailboxes. Ensuring proper logging of user actions and mailbox operations in the audit log will enable comprehensive incident response and forensics.

Impact:

None - this is the default behavior.

Audit:

Ensure Audit Bypass is not enabled using PowerShell:

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

```
$MBX = Get-MailboxAuditBypassAssociation -ResultSize unlimited
$MBX | where {$_.AuditBypassEnabled -eq $true} | Format-Table
Name,AuditBypassEnabled
```

3. If nothing is returned then there are not accounts with Audit Bypass enabled.

Remediation:

Disable Audit Bypass on all mailboxes using PowerShell:

1. Connect to Exchange Online using `Connect-ExchangeOnline`.
2. The following example PowerShell script will disable AuditBypass for all mailboxes which currently have it enabled:

```
# Get mailboxes with AuditBypassEnabled set to $true
$MBXAudit = Get-MailboxAuditBypassAssociation -ResultSize unlimited | Where-
Object { $_.AuditBypassEnabled -eq $true }

foreach ($mailbox in $MBXAudit) {
    $mailboxName = $mailbox.Name
    Set-MailboxAuditBypassAssociation -Identity $mailboxName -
AuditBypassEnabled $false
    Write-Host "Audit Bypass disabled for mailbox Identity: $mailboxName" -
ForegroundColor Green
}
```

Default Value:

AuditBypassEnabled `False`

References:

1. https://learn.microsoft.com/en-us/powershell/module/exchange/get-mailboxauditbypassassociation?view=exchange-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●

6.2 Mail flow

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

Profile Applicability:

- E3 Level 1

Description:

Exchange Online offers several methods of managing the flow of email messages. These are Remote domain, Transport Rules, and Anti-spam outbound policies. These methods work together to provide comprehensive coverage for potential automatic forwarding channels:

- Outlook forwarding using inbox rules
- Outlook forwarding configured using OOF rule
- OWA forwarding setting (ForwardingSmtpAddress)
- Forwarding set by the admin using EAC (ForwardingAddress)
- Forwarding using Power Automate / Flow

Ensure a `Transport rule` and `Anti-spam outbound policy` are used to block mail forwarding.

NOTE: Any exclusions should be implemented based on organizational policy.

Rationale:

Attackers often create these rules to exfiltrate data from your tenancy, this could be accomplished via access to an end-user account or otherwise. An insider could also use one of these methods as a secondary channel to exfiltrate sensitive data.

Impact:

Care should be taken before implementation to ensure there is no business need for case-by-case auto-forwarding. Disabling auto-forwarding to remote domains will affect all users and in an organization. Any exclusions should be implemented based on organizational policy.

Audit:

NOTE: *Audit is a two step procedure as follows:*

STEP 1: Transport rules
To verify the mail transport rules do not forward email to external domains, use the Microsoft 365 Admin Center:

1. Select `Exchange` to open the Exchange admin center.
2. Select `Mail Flow` then `Rules`.
3. Review the rules and verify that none of them are forwards or redirects e-mail to external domains.

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

1. Connect to Exchange online using `Connect-ExchangeOnline`.
2. Run the following PowerShell command to review the Transport Rules that are redirecting email:

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

3. Verify that none of the addresses listed belong to external domains outside of the organization. If nothing returns then there are no transport rules set to redirect messages.

STEP 2: Anti-spam outbound policy
Ensure an anti-spam outbound policy is properly configured:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Expand `E-mail & collaboration` then select `Policies & rules`.
3. Select `Threat policies` > `Anti-spam`.
4. Inspect `Anti-spam outbound policy (default)` and ensure `Automatic forwarding` is set to `Off - Forwarding is disabled`
5. Inspect any additional custom outbound policies and ensure `Automatic forwarding` is set to `Off - Forwarding is disabled`, in accordance with the organization's exclusion policies.

NOTE: According to Microsoft if a recipient is defined in multiple policies of the same type (anti-spam, anti-phishing, etc.), only the policy with the highest priority is applied to the recipient. Any remaining policies of that type are not evaluated for the recipient (including the default policy). However, it is our recommendation to audit the default policy as well in the case a higher priority custom policy is removed. This will keep the organization's security posture strong.

Remediation:

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

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

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

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

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

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

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

STEP 2: Anti-spam outbound policy
Configure an anti-spam outbound policy:

1. Navigate to `Microsoft 365 Defender` https://security.microsoft.com/
2. Expand `E-mail & collaboration` then select `Policies & rules`.
3. Select `Threat policies` > `Anti-spam`.
4. Select `Anti-spam outbound policy (default)`
5. Click `Edit protection settings`
6. Set `Automatic forwarding rules` dropdown to `Off - Forwarding is disabled` and click `Save`
7. Repeat steps 4-6 for any additional higher priority, custom policies.

References:

1. https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/mail-flow-rule-procedures?view=exchserver-2019
2. https://techcommunity.microsoft.com/t5/exchange-team-blog/all-you-need-to-know-about-automatic-email-forwarding-in/ba-p/2074888#:~:text=%20%20%20Automatic%20forwarding%20option%20%20,%
3. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/outbound-spam-policies-external-email-forwarding?view=o365-worldwide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

Care should be taken before implementation to ensure there is no business need for case-by-case whitelisting. Removing all whitelisted domains could affect incoming mail flow to an organization although modern systems sending legitimate mail should have no issue with this.

Audit:

Ensure mail transport rules do not whitelist specific domains:

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

To verify that mail transport rules do not whitelist any domains using PowerShell:

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

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

Remediation:

To alter the mail transport rules so they do not whitelist any specific domains:

1. Navigate to `Exchange admin center` https://admin.exchange.microsoft.com..
2. Click to expand `Mail Flow` and then select `Rules`.
3. For each rule that whitelists specific domains, select the rule and click the 'Delete' icon.

To remove mail transport rules using PowerShell:

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

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

3. Verify the rules no longer exists.

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

References:

1. https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/configuration-best-practices
2. https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

6.2.3 (L1) Ensure email from external senders is identified (Automated)

Profile Applicability:

- E3 Level 1

Description:

External callouts provide a native experience to identify emails from senders outside the organization. This is achieved by presenting a new tag on emails called "External" (the string is localized based on the client language setting) and exposing related user interface at the top of the message reading view to see and verify the real sender's email address.

Once this feature is enabled via PowerShell, it might take 24-48 hours for users to start seeing the External sender tag in email messages received from external sources (outside of your organization), providing their Outlook version supports it.

The recommended state is `ExternalInOutlook` set to `Enabled True`

Note: Mail flow rules are often used by Exchange administrators to accomplish the External email tagging by appending a tag to the front of a subject line. There are limitations to this outlined here. The preferred method in the CIS Benchmark is to use the native experience.

Rationale:

Tagging emails from external senders helps to inform end users about the origin of the email. This can allow them to proceed with more caution and make informed decisions when it comes to identifying spam or phishing emails.

Note: Existing emails in a user's inbox from external senders are not tagged retroactively.

Impact:

Mail flow rules using external tagging will need to be disabled before enabling this to avoid duplicate [External] tags.

The Outlook desktop client is the last to receive this update and the feature is only available for certain versions see below:

Outlook for Windows: **Update 4/26/23:** *External Tag view in Outlook for Windows (matching other clients) released to production for Current Channel and Monthly Enterprise Channel in Version 2211 for builds 15831.20190 and higher. We anticipate the External tag to reach Semi-Annual Preview Channel with Version 2308 on the September 12th 2023 public update and reach Semi-Annual Enterprise Channel with Version 2308 with the January 9th 2024 public update.*

Audit:

To verify external sender tagging using PowerShell:

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

```
Get-ExternalInOutlook
```

3. For each identity verify `Enabled` is set to `True` and the `AllowList` only contains email addresses the organization has permitted to bypass external tagging.

Remediation:

To enable external tagging using PowerShell:

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

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

Default Value:

Disabled (False)

References:

1. https://techcommunity.microsoft.com/t5/exchange-team-blog/native-external-sender-callouts-on-email-in-outlook/ba-p/2250098
2. https://learn.microsoft.com/en-us/powershell/module/exchange/set-externalinoutlook?view=exchange-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

6.3 Roles

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

Profile Applicability:

- E3 Level 2

Description:

Specify the administrators and users who can install and manage add-ins for Outlook in Exchange Online

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

Rationale:

Attackers exploit vulnerable or custom add-ins to access user data. Disabling user-installed add-ins in Microsoft Outlook reduces this threat surface.

Impact:

Implementing this change will impact both end users and administrators. End users will be unable to integrate third-party applications they desire, and administrators may receive requests to grant permission for necessary third-party apps.

Audit:

Ensure user installation of Outlook add-ins is not allowed:

1. Navigate to `Exchange admin center` https://admin.exchange.microsoft.com.
2. Click to expand `Roles` select `User roles`.
3. Select `Default Role Assignment Policy`.
4. In the properties pane on the right click on `Manage permissions`.
5. Under *Other roles* verify `My Custom Apps`, `My Marketplace Apps` and `My ReadWriteMailboxApps` are **unchecked**.

To verify using PowerShell:

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

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

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

Remediation:

To prohibit users installing Outlook add-ins:

1. Navigate to `Exchange admin center` https://admin.exchange.microsoft.com.
2. Click to expand `Roles` select `User roles`.
3. Select `Default Role Assignment Policy`.
4. In the properties pane on the right click on `Manage permissions`.
5. Under *Other roles* uncheck `My Custom Apps`, `My Marketplace Apps` and `My ReadWriteMailboxApps`.
6. Click `Save changes`.

To remediate using PowerShell:

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

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

New-RoleAssignmentPolicy -Name $policy -Roles $roles
Set-RoleAssignmentPolicy -id $policy -IsDefault

# Assign new policy to all mailboxes
Get-EXOMailbox -ResultSize Unlimited | Set-Mailbox -RoleAssignmentPolicy
$policy
```

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

Default Value:

UI - `My Custom Apps`, `My Marketplace Apps`, and `My ReadWriteMailboxApps` are checked

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

References:

1. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/add-ins-for-outlook/specify-who-can-install-and-manage-add-ins?source=recommendations
2. https://learn.microsoft.com/en-us/exchange/permissions-exo/role-assignment-policies

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6.4 Reports

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

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

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

Impact:

There is no impact to reviewing these reports.

Audit:

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

Remediation:

To review mail forwarding rules:

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

Note: Mail flow reports cannot be viewed from the Classic Exchange Admin Center
To review mail forwarding rules using PowerShell:

1. Connect to Exchange Online PowerShell using `Connect-ExchangeOnline`

```
# Uses the administrator user credential to export Mail forwarding rules,
User Delegates
# and SMTP Forwarding policies to multiple csv files.

$allUsers = Get-User -ResultSize Unlimited -Filter {RecipientTypeDetails -eq
"UserMailbox" } |
  Where-Object {$_.AccountDisabled -like "False"}

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

foreach ($User in $allUsers) {
  Write-Host "Checking inbox rules and delegates for user: "
$User.UserPrincipalName
  $UserInboxRules += Get-InboxRule -Mailbox $User.UserPrincipalName |
    Select-Object Name, Description, Enabled, Priority, ForwardTo,
ForwardAsAttachmentTo, RedirectTo, DeleteMessage |
    Where-Object { ($_.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*") }
}

$SMTPForwarding = Get-Mailbox -ResultSize Unlimited |
  Select-Object DisplayName, ForwardingAddress, ForwardingSMTPAddress,
DeliverToMailboxandForward |
  Where-Object {$_.ForwardingSMTPAddress -ne $null}

# Export list of inbox rules, delegates, and SMTP forwards
$UserInboxRules | Export-Csv MailForwardingRulesToExternalDomains.csv -
NoTypeInformation
$UserDelegates | Export-Csv MailboxDelegatePermissions.csv -NoTypeInformation
$SMTPForwarding | Export-Csv Mailboxsmtpforwarding.csv -NoTypeInformation
```

CIS Controls:

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

6.5 Settings

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

Profile Applicability:

- E3 Level 1

Description:

Modern authentication in Microsoft 365 enables authentication features like multifactor authentication (MFA) using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers. When you enable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use modern authentication to log in to Microsoft 365 mailboxes. When you disable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use basic authentication to log in to Microsoft 365 mailboxes.

When users initially configure certain email clients, like Outlook 2013 and Outlook 2016, they may be required to authenticate using enhanced authentication mechanisms, such as multifactor authentication. Other Outlook clients that are available in Microsoft 365 (for example, Outlook Mobile and Outlook for Mac 2016) always use modern authentication to log in to Microsoft 365 mailboxes.

Rationale:

Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by Exchange Online email clients such as Outlook 2016 and Outlook 2013. Enabling modern authentication for Exchange Online ensures strong authentication mechanisms are used when establishing sessions between email clients and Exchange Online.

Impact:

Users of older email clients, such as Outlook 2013 and Outlook 2016, will no longer be able to authenticate to Exchange using Basic Authentication, which will necessitate migration to modern authentication practices.

Audit:

To audit using PowerShell:

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

```
Get-OrganizationConfig | Format-Table -Auto Name, OAuth*
```

4. Verify `OAuth2ClientProfileEnabled` is `True`.

Remediation:

To remediate using PowerShell:

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

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $True
```

Default Value:

True

References:

1. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

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

Profile Applicability:

- E3 Level 2

Description:

MailTips are informative messages displayed to users while they're composing a message. While a new message is open and being composed, Exchange analyzes the message (including recipients). If a potential problem is detected, the user is notified with a MailTip prior to sending the message. Using the information in the MailTip, the user can adjust the message to avoid undesirable situations or non-delivery reports (also known as NDRs or bounce messages).

Rationale:

Setting up MailTips gives a visual aid to users when they send emails to large groups of recipients or send emails to recipients not within the tenant.

Audit:

To audit using PowerShell:

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

```
Get-OrganizationConfig | fl MailTips*
```

3. Verify the values for `MailTipsAllTipsEnabled`, `MailTipsExternalRecipientsTipsEnabled`, and `MailTipsGroupMetricsEnabled` are set to `True` and `MailTipsLargeAudienceThreshold` is set to an acceptable value; `25` is the default value.

Remediation:

To remediate using PowerShell:

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

```
$TipsParams = @{
    MailTipsAllTipsEnabled                  = $true
    MailTipsExternalRecipientsTipsEnabled   = $true
    MailTipsGroupMetricsEnabled             = $true
    MailTipsLargeAudienceThreshold          = '25'
}

Set-OrganizationConfig @TipsParams
```

Default Value:

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

References:

1. https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/mailtips/mailtips
2. https://learn.microsoft.com/en-us/powershell/module/exchange/set-organizationconfig?view=exchange-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

6.5.3 (L2) Ensure additional storage providers are restricted in Outlook on the web (Automated)

Profile Applicability:

- E3 Level 2

Description:

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

Ensure `AdditionalStorageProvidersAvailable` are restricted.

Rationale:

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

Impact:

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

Audit:

To audit using PowerShell:

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

```
Get-OwaMailboxPolicy | Format-Table Name, AdditionalStorageProvidersAvailable
```

3. Verify that the value returned is `False`.

Remediation:

To remediate using PowerShell:

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

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

Default Value:

`Additional Storage Providers - True`

References:

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

CIS Controls:

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

7 SharePoint admin center

The SharePoint admin center contains settings related to SharePoint and OneDrive.

UI Direct link: https://admin.microsoft.com/sharepoint

The PowerShell module most commonly used in this section is `Microsoft.Online.SharePoint.PowerShell` and uses `Connect-SPOService -Url https://contoso-admin.sharepoint.com` as the connection cmdlet (replacing tenant name with your value).

The latest version of the module can be downloaded here: https://www.powershellgallery.com/packages/Microsoft.Online.SharePoint.PowerShell/

7.1 Sites

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

7.2 Policies

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

Profile Applicability:

- E3 Level 1

Description:

Modern authentication in Microsoft 365 enables authentication features like multifactor authentication (MFA) using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers.

Rationale:

Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by SharePoint applications. Requiring modern authentication for SharePoint applications ensures strong authentication mechanisms are used when establishing sessions between these applications, SharePoint, and connecting users.

Impact:

Implementation of modern authentication for SharePoint will require users to authenticate to SharePoint using modern authentication. This may cause a minor impact to typical user behavior.

This may also prevent third-party apps from accessing SharePoint Online resources. Also, this will also block apps using the SharePointOnlineCredentials class to access SharePoint Online resources.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint.
2. Click to expand `Policies` select `Access control`.
3. Select `Apps that don't use modern authentication` and ensure that it is set to `Block access`.

To audit using PowerShell:

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com` replacing tenant with your value.
2. Run the following SharePoint Online PowerShell command:

```
Get-SPOTenant | ft LegacyAuthProtocolsEnabled
```

3. Ensure the returned value is `False`.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint.
2. Click to expand `Policies` select `Access control`.
3. Select `Apps that don't use modern authentication`.
4. Select the radio button for `Block access`.
5. Click `Save`.

To remediate using PowerShell:

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com` replacing tenant with your value.
2. Run the following SharePoint Online PowerShell command:

```
Set-SPOTenant -LegacyAuthProtocolsEnabled $false
```

Default Value:

True (Apps that don't use modern authentication are allowed)

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

7.2.2 (L1) Ensure SharePoint and OneDrive integration with Azure AD B2B is enabled (Automated)

Profile Applicability:

- E3 Level 1

Description:

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

Note: Global Reader role currently can't access SharePoint using PowerShell.

Rationale:

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

Impact:

Azure B2B collaboration is used with other Azure services so should not be new or unusual. Microsoft also has made the experience seamless when turning on integration on SharePoint sites that already have active files shared with guest users. The referenced Microsoft article on the subject has more details on this.

Audit:

To audit using PowerShell:

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

```
Get-SPOTenant | ft EnableAzureADB2BIntegration
```

3. Ensure the returned value is `True`.

Remediation:

To remediate using PowerShell:

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

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

Default Value:

False

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

7.2.3 (L1) Ensure external content sharing is restricted (Automated)

Profile Applicability:

- E3 Level 1

Description:

The external sharing settings govern sharing for the organization overall. Each site has its own sharing setting that can be set independently, though it must be at the same or more restrictive setting as the organization.

The new and existing guests option requires people who have received invitations to sign in with their work or school account (if their organization uses Microsoft 365) or a Microsoft account, or to provide a code to verify their identity. Users can share with guests already in your organization's directory, and they can send invitations to people who will be added to the directory if they sign in.

The recommended state is `New and existing guests` or less permissive.

Rationale:

Forcing guest authentication on the organization's tenant enables the implementation of controls and oversight over external file sharing. When a guest is registered with the organization, they now have an identity which can be accounted for. This identity can also have other restrictions applied to it through group membership and conditional access rules.

Impact:

When using Azure AD B2B integration, Azure AD external collaboration settings, such as guest invite settings and collaboration restrictions apply.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Locate the `External sharing section`.
4. Under SharePoint, ensure the slider bar is set to `New and existing guests` or a less permissive level.

To audit using PowerShell:

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

```
Get-SPOTenant | fl SharingCapability
```

3. Ensure `SharingCapability` is set to one of the following values:
   - Value1: `ExternalUserSharingOnly`
   - Value2: `ExistingExternalUserSharingOnly`
   - Value3: `Disabled`

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Locate the `External sharing section`.
4. Under SharePoint, move the slider bar to `New and existing guests` or a less permissive level.
    - OneDrive will also be moved to the same level and can never be more permissive than SharePoint.

To remediate using PowerShell:

1. Connect to SharePoint Online service using `Connect-SPOService`.
2. Run the following cmdlet to establish the minimum recommended state:

```
Set-SPOTenant -SharingCapability ExternalUserSharingOnly
```

Note: Other acceptable values for this parameter that are more restrictive include: `Disabled` and `ExistingExternalUserSharingOnly`.

Default Value:

Anyone (ExternalUserAndGuestSharing)

References:

1. https://learn.microsoft.com/en-US/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo
2. https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-spotenant?view=sharepoint-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

7.2.4 (L2) Ensure OneDrive content sharing is restricted (Automated)

Profile Applicability:

- E3 Level 2

Description:

This setting governs the global permissiveness of OneDrive content sharing in the organization.

OneDrive content sharing can be restricted independent of SharePoint but can never be more permissive than the level established with SharePoint.

The recommended state is `Only people in your organization`.

Rationale:

OneDrive, designed for end-user cloud storage, inherently provides less oversight and control compared to SharePoint, which often involves additional content overseers or site administrators. This autonomy can lead to potential risks such as inadvertent sharing of privileged information by end users. Restricting external OneDrive sharing will require users to transfer content to SharePoint folders first which have those tighter controls.

Impact:

Users will be required to take additional steps to share OneDrive content or use other official channels.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Locate the `External sharing section`.
4. Under OneDrive, ensure the slider bar is set to `Only people in your organization`.

To audit using PowerShell:

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

```
Get-SPOTenant | fl OneDriveSharingCapability
```

3. Ensure the returned value is `Disabled`.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Locate the `External sharing section`.
4. Under OneDrive, set the slider bar to `Only people in your organization`.

To remediate using PowerShell:

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

```
Set-SPOTenant -OneDriveSharingCapability Disabled
```

Default Value:

Anyone (ExternalUserAndGuestSharing)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

7.2.5 (L2) Ensure that SharePoint guest users cannot share items they don't own (Automated)

Profile Applicability:

- E3 Level 2

Description:

SharePoint gives users the ability to share files, folders, and site collections. Internal users can share with external collaborators, and with the right permissions could share to other external parties.

Rationale:

Sharing and collaboration are key; however, file, folder, or site collection owners should have the authority over what external users get shared with to prevent unauthorized disclosures of information.

Impact:

The impact associated with this change is highly dependent upon current practices. If users do not regularly share with external parties, then minimal impact is likely. However, if users do regularly share with guests/externally, minimum impacts could occur as those external users will be unable to 're-share' content.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` then select `Sharing`.
3. Expand `More external sharing settings`, verify that `Allow guests to share items they don't own` is unchecked.

To audit using PowerShell:

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

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

3. Ensure the returned value is `True`.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` then select `Sharing`.
3. Expand `More external sharing settings`, uncheck `Allow guests to share items they don't own`.
4. Click `Save`.

To remediate using PowerShell:

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

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

Default Value:

Checked (False)

References:

1. https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off
2. https://learn.microsoft.com/en-us/sharepoint/external-sharing-overview

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

7.2.6 (L2) Ensure SharePoint external sharing is managed through domain whitelist/blacklists (Automated)

Profile Applicability:

- E3 Level 2

Description:

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 users can share documents with will reduce that surface area.

Impact:

Enabling this feature will prevent users from sharing documents with domains outside of the organization unless allowed.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Expand `Policies` then click `Sharing`.
3. Expand `More external sharing settings` and confirm that `Limit external sharing by domain` is checked.
4. Verify that an accurate list of allowed domains is listed.

To audit using PowerShell:

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

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

3. Ensure that `SharingDomainRestrictionMode` is set to `AllowList` and `SharingAllowedDomainList` contains domains trusted by the organization for external sharing.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint.
2. Expand `Policies` then click `Sharing`.
3. Expand `More external sharing settings` and check `Limit external sharing by domain`.
4. Select `Add domains` to add a list of approved domains.
5. Click `Save` at the bottom of the page.

To remediate using PowerShell:

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

```
Set-SPOTenant -SharingDomainRestrictionMode AllowList -
SharingAllowedDomainList "domain1.com domain2.com"
```

Default Value:

Limit external sharing by domain is unchecked

SharingDomainRestrictionMode: `None`

SharingDomainRestrictionMode: <Undefined>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.		●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

7.2.7 (L1) Ensure link sharing is restricted in SharePoint and OneDrive (Automated)

Profile Applicability:

- E3 Level 1

Description:

This setting sets the default link type that a user will see when sharing content in OneDrive or SharePoint. It does not restrict or exclude any other options.

The recommended state is `Specific people (only the people the user specifies)`

Rationale:

By defaulting to specific people, the user will first need to consider whether or not the content being shared should be accessible by the entire organization versus select individuals. This aids in reinforcing the concept of least privilege.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to `Filer and folder links`.
4. Ensure that the setting `Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive` is set to `Specific people (only the people the user specifies)`

To audit using PowerShell:

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

```
Get-SPOTenant | fl DefaultSharingLinkType
```

3. Ensure the returned value is `Direct`.

Remediation:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to `Filer and folder links`.
4. Set `Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive` to `Specific people (only the people the user specifies)`

To remediate using PowerShell:

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

```
Set-SPOTenant -DefaultSharingLinkType Direct
```

Default Value:

Only people in your organization (Internal)

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

7.2.8 (L2) Ensure external sharing is restricted by security group (Manual)

Profile Applicability:

- E3 Level 2

Description:

External sharing of content can be restricted to specific security groups. This setting is global, applies to sharing in both SharePoint and OneDrive and cannot be set at the site level in SharePoint.

The recommended state is `Enabled` or `Checked`.

Note: Users in these security groups must be allowed to invite guests in the Azure Active Directory guest invite settings in Microsoft Entra. Identity > External Identities > External collaboration settings

Rationale:

Organizations wishing to create tighter security controls for external sharing can set this to enforce role-based access control by using security groups already defined in Microsoft Entra.

Impact:

OneDrive will also be governed by this and there is no granular control at the SharePoint site level.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to and expand `More external sharing settings`.
4. Ensure the following:
   - Verify `Allow only users in specific security groups to share externally` is checked
   - Verify `Manage security groups` is defined and accordance with company procedure.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to and expand `More external sharing settings`.
4. Set the following:
   - Check `Allow only users in specific security groups to share externally`
   - Define `Manage security groups` in accordance with company procedure.

Default Value:

Unchecked/Undefined

References:

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

CIS Controls:

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

7.2.9 (L1) Ensure guest access to a site or OneDrive will expire automatically (Automated)

Profile Applicability:

- E3 Level 1

Description:

This policy setting configures the expiration time for each guest that is invited to the SharePoint site or with whom users share individual files and folders with.

The recommended state is `30` or less.

Rationale:

This setting ensures that guests who no longer need access to the site or link no longer have access after a set period of time. Allowing guest access for an indefinite amount of time could lead to loss of data confidentiality and oversight.

Note: Guest membership applies at the Microsoft 365 group level. Guests who have permission to view a SharePoint site or use a sharing link may also have access to a Microsoft Teams team or security group.

Impact:

Site collection administrators will have to renew access to guests who still need access after 30 days. They will receive an e-mail notification once per week about guest access that is about to expire.

Note: The guest expiration policy only applies to guests who use sharing links or guests who have direct permissions to a SharePoint site after the guest policy is enabled. The guest policy does not apply to guest users that have pre-existing permissions or access through a sharing link before the guest expiration policy is applied.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to and expand `More external sharing settings`.
4. Ensure `Guest access to a site or OneDrive will expire automatically after this many days` is checked and set to `30` or less.

To audit using PowerShell:

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

```
Get-SPOTenant | fl ExternalUserExpirationRequired,ExternalUserExpireInDays
```

3. Ensure the following values are returned:
   - ExternalUserExpirationRequired is `True`.
   - ExternalUserExpireInDays is `30` or less.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to and expand `More external sharing settings`.
4. Set `Guest access to a site or OneDrive will expire automatically after this many days` to `30`

To remediate using PowerShell:

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

```
Set-SPOTenant -ExternalUserExpireInDays 30 -ExternalUserExpirationRequired
$True
```

Default Value:

ExternalUserExpirationRequired `$false`

ExternalUserExpireInDays `60` days

References:

1. https://learn.microsoft.com/en-US/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo#change-the-organization-level-external-sharing-setting
2. https://learn.microsoft.com/en-us/microsoft-365/community/sharepoint-security-a-team-effort

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

7.2.10 (L1) Ensure reauthentication with verification code is restricted (Automated)

Profile Applicability:

- E3 Level 1

Description:

This setting configures if guests who use a verification code to access the site or links are required to reauthenticate after a set number of days.

The recommended state is `15` or less.

Rationale:

By increasing the frequency of times guests need to reauthenticate this ensures guest user access to data is not prolonged beyond an acceptable amount of time.

Impact:

Guests who use Microsoft 365 in their organization can sign in using their work or school account to access the site or document. After the one-time passcode for verification has been entered for the first time, guests will authenticate with their work or school account and have a guest account created in the host's organization.

Note: If OneDrive and SharePoint integration with Azure AD B2B is enabled as per the CIS Benchmark the one-time-passcode experience will be replaced. Please visit Secure external sharing in SharePoint - SharePoint in Microsoft 365 | Microsoft Learn for more information.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to and expand `More external sharing settings`.
4. Ensure `People who use a verification code must reauthenticate after this many days` is set to `15` or less.

To audit using PowerShell:

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

```
Get-SPOTenant | fl EmailAttestationRequired,EmailAttestationReAuthDays
```

3. Ensure the following values are returned:
   - EmailAttestationRequired `True`
   - EmailAttestationReAuthDays `15` or less days.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click to expand `Policies` > `Sharing`.
3. Scroll to and expand `More external sharing settings`.
4. Set `People who use a verification code must reauthenticate after this many days` to `15` or less.

To remediate using PowerShell:

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

```
Set-SPOTenant -EmailAttestationRequired $true -EmailAttestationReAuthDays 15
```

Default Value:

EmailAttestationRequired : `False`

EmailAttestationReAuthDays : `30`

References:

1. https://learn.microsoft.com/en-US/sharepoint/what-s-new-in-sharing-in-targeted-release?WT.mc_id=365AdminCSH_spo
2. https://learn.microsoft.com/en-US/sharepoint/turn-external-sharing-on-or-off?WT.mc_id=365AdminCSH_spo#change-the-organization-level-external-sharing-setting
3. https://learn.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

7.3 Settings

7.3.1 (L2) Ensure Office 365 SharePoint infected files are disallowed for download (Automated)

Profile Applicability:

- E5 Level 2

Description:

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

Rationale:

Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams protects your organization from inadvertently sharing malicious files. When an infected file is detected that file is blocked so that no one can open, copy, move, or share it until further actions are taken by the organization's security team.

Impact:

The only potential impact associated with implementation of this setting is potential inconvenience associated with the small percentage of false positive detections that may occur.

Audit:

To audit using PowerShell:

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com`, replacing "tenant" with the appropriate value.
2. Run the following PowerShell command:

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

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

Note: According to Microsoft, SharePoint cannot be accessed through PowerShell by users with the Global Reader role. For further information, please refer to the reference section.

Remediation:

To remediate using PowerShell:

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com`, replacing "tenant" with the appropriate value.
2. Run the following PowerShell command to set the recommended value:

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

Note: The Global Reader role cannot access SharePoint using PowerShell according to Microsoft. See the reference section for more information.

Default Value:

False

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-configure?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection-for-spo-odfb-teams-about?view=o365-worldwide
3. https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#global-reader

CIS Controls:

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

7.3.2 (L2) Ensure OneDrive sync is restricted for unmanaged devices (Automated)

Profile Applicability:

- E3 Level 2

Description:

Microsoft OneDrive allows users to sign in their cloud tenant account and begin syncing select folders or the entire contents of OneDrive to a local computer. By default, this includes any computer with OneDrive already installed, whether or not it is Azure Domain Joined or Active Directory Domain joined.

The recommended state for this setting is `Allow syncing only on computers joined to specific domains` `Enabled: Specify the AD domain GUID(s)`

Rationale:

Unmanaged devices pose a risk, since their security cannot be verified through existing security policies, brokers or endpoint protection. Allowing users to sync data to these devices takes that data out of the control of the organization. This increases the risk of the data either being intentionally or accidentally leaked.

Note: This setting is only applicable to **Active Directory domains** when operating in a hybrid configuration. It does not apply to Azure AD domains. If there are devices which are only Azure AD joined, consider using a Conditional Access Policy instead.

Impact:

Enabling this feature will prevent users from using the OneDrive for Business Sync client on devices that are not joined to the domains that were defined.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click `Settings` followed by `OneDrive - Sync`
3. Verify that `Allow syncing only on computers joined to specific domains` is checked.
4. Verify that the Active Directory domain GUIDS are listed in the box.
   - Use the `Get-ADDomain` PowerShell command on the on-premises server to obtain the GUID for each on-premises domain.

To audit using PowerShell:

1. Connect to SharePoint Online using `Connect-SPOService -Url https://tenant-admin.sharepoint.com`, replacing "tenant" with the appropriate value.
2. Run the following PowerShell command:

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

3. Ensure `TenantRestrictionEnabled` is set to `True` and `AllowedDomainList` contains the trusted domains GUIDs from the on premises environment.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Click `Settings` then select `OneDrive - Sync`.
3. Check the `Allow syncing only on computers joined to specific domains`.
4. Use the `Get-ADDomain` PowerShell command on the on-premises server to obtain the GUID for each on-premises domain.
5. Click `Save`.

To remediate using PowerShell:

1. Connect to SharePoint Online using `Connect-SPOService`
2. Run the following PowerShell command and provide the DomainGuids from the Get-AADomain command:

```
Set-SPOTenantSyncClientRestriction -Enable -DomainGuids "786548DD-877B-4760-
A749-6B1EFBC1190A; 877564FF-877B-4760-A749-6B1EFBC1190A"
```

Note: Utilize the `-BlockMacSync:$true` parameter if you are not using conditional access to ensure Macs cannot sync.

Default Value:

By default there are no restrictions applied to the syncing of OneDrive.

TenantRestrictionEnabled : `False`

AllowedDomainList : `{}`

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

7.3.3 (L1) Ensure custom script execution is restricted on personal sites (Manual)

Profile Applicability:

- E3 Level 1

Description:

This setting controls custom script execution on OneDrive or user-created sites.

Custom scripts can allow users to change the look, feel and behavior of sites and pages. Every script that runs in a SharePoint page (whether it's an HTML page in a document library or a JavaScript in a Script Editor Web Part) always runs in the context of the user visiting the page and the SharePoint application. This means:

- Scripts have access to everything the user has access to.
- Scripts can access content across several Microsoft 365 services and even beyond with Microsoft Graph integration.

The recommended state is `Prevent users from running custom script on personal sites` and `Prevent users from running custom script on self-service created sites`

Rationale:

Custom scripts could contain malicious instructions unknown to the user or administrator. When users are allowed to run custom script, the organization can no longer enforce governance, scope the capabilities of inserted code, block specific parts of code, or block all custom code that has been deployed. If scripting is allowed the following things can't be audited:

- What code has been inserted
- Where the code has been inserted
- Who inserted the code

Note: Microsoft recommends using the SharePoint Framework instead of custom scripts.

Impact:

None - this is the default behavior.

Audit:

To audit using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Select `Settings`.
3. At the bottom of the page click the `classic settings page` hyperlink.
4. Scroll to locate the **Custom Script** section. On the right ensure the following:
   - Verify `Prevent users from running custom script on personal sites` is set.
   - Verify `Prevent users from running custom script on self-service created sites` is set.

Remediation:

To remediate using the UI:

1. Navigate to `SharePoint admin center` https://admin.microsoft.com/sharepoint
2. Select `Settings`.
3. At the bottom of the page click the `classic settings page` hyperlink.
4. Scroll to locate the **Custom Script** section. On the right set the following:
   - Select `Prevent users from running custom script on personal sites`.
   - Select `Prevent users from running custom script on self-service created sites`.

Default Value:

Selected `Prevent users from running custom script on personal sites`

Selected `Prevent users from running custom script on self-service created sites`

References:

1. https://learn.microsoft.com/en-us/sharepoint/allow-or-prevent-custom-script
2. https://learn.microsoft.com/en-us/sharepoint/security-considerations-of-allowing-custom-script
3. https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-sposite?view=sharepoint-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

7.3.4 (L1) Ensure custom script execution is restricted on site collections (Automated)

Profile Applicability:

- E3 Level 1

Description:

This setting controls custom script execution on a particulate site (previously called "site collection").

Custom scripts can allow users to change the look, feel and behavior of sites and pages. Every script that runs in a SharePoint page (whether it's an HTML page in a document library or a JavaScript in a Script Editor Web Part) always runs in the context of the user visiting the page and the SharePoint application. This means:

- Scripts have access to everything the user has access to.
- Scripts can access content across several Microsoft 365 services and even beyond with Microsoft Graph integration.

The recommended state is `DenyAddAndCustomizePages` set to `$true`.

Rationale:

Custom scripts could contain malicious instructions unknown to the user or administrator. When users are allowed to run custom script, the organization can no longer enforce governance, scope the capabilities of inserted code, block specific parts of code, or block all custom code that has been deployed. If scripting is allowed the following things can't be audited:

- What code has been inserted
- Where the code has been inserted
- Who inserted the code

Note: Microsoft recommends using the SharePoint Framework instead of custom scripts.

Impact:

None - this is the default behavior.

Audit:

To audit using PowerShell:

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

```
Get-SPOSite | ft Title,Url,DenyAddAndCustomizePages
```

3. Ensure the returned value is for `DenyAddAndCustomizePages` is `Enabled` for each site.

Note: The property `DenyAddAndCustomizePages` cannot be set on the MySite host, which is displayed with a URL like https://`tenant id`-my.sharepoint.com/

Remediation:

To remediate using PowerShell:

1. Connect to SharePoint Online using `Connect-SPOService`.
2. Edit the below and run for each site as neededed:

```
Set-SPOSite -Identity <SiteUrl> -DenyAddAndCustomizePages $true
```

Note: The property `DenyAddAndCustomizePages` cannot be set on the MySite host, which is displayed with a URL like https://`tenant id`-my.sharepoint.com/

Default Value:

DenyAddAndCustomizePages `$true` or `Enabled`

References:

1. https://learn.microsoft.com/en-us/sharepoint/allow-or-prevent-custom-script
2. https://learn.microsoft.com/en-us/sharepoint/security-considerations-of-allowing-custom-script
3. https://learn.microsoft.com/en-us/powershell/module/sharepoint-online/set-sposite?view=sharepoint-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

8 Microsoft Teams admin center

The Microsoft Teams admin center contains settings related to Microsoft Teams.

UI Direct link: https://admin.teams.microsoft.com/

The PowerShell module most commonly used in this section is `MicrosoftTeams` and uses `Connect-MicrosoftTeams` as the connection cmdlet.

The latest version of the module can be downloaded here:
https://www.powershellgallery.com/packages/MicrosoftTeams/

8.1 Teams

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

Profile Applicability:

- E3 Level 2

Description:

Microsoft Teams enables collaboration via file sharing. This file sharing is conducted within Teams, using SharePoint Online, by default; however, third-party cloud services are allowed as well.

Note: Skype for business is deprecated as of July 31, 2021 although these settings may still be valid for a period of time. See the link in the references section for more information.

Rationale:

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

Impact:

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

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Teams` select `Teams settings`.
3. Under files verify that only authorized cloud storage options are set to `On` and all others `Off`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following to verify the recommended state:

```
Get-CsTeamsClientConfiguration | fl
AllowDropbox,AllowBox,AllowGoogleDrive,AllowShareFile,AllowEgnyte
```

3. Verify that only authorized providers are set to `True` and all others `False`.

Remediation:

To set external file sharing in Teams:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Teams` select `Teams settings`.
3. Set any unauthorized providers to `Off`.

To set cloud sharing options using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following PowerShell command to disable external providers that are not authorized. (the example disables Citrix Files, DropBox, Box, Google Drive and Egnyte)

```
$storageParams = @{
    AllowGoogleDrive = $false
    AllowShareFile = $false
    AllowBox = $false
    AllowDropBox = $false
    AllowEgnyte = $false
}

Set-CsTeamsClientConfiguration @storageParams
```

Default Value:

AllowDropBox : `True`

AllowBox : `True`

AllowGoogleDrive : `True`

AllowShareFile : `True`

AllowEgnyte : `True`

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.7 Enforce Access Control to Data through Automated Tools Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			●

8.1.2 (L1) Ensure users can't send emails to a channel email address (Automated)

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

Channel email addresses are not under the tenant’s domain and organizations do not have control over the security settings for this email address. An attacker could email channels directly if they discover the channel email address.

Impact:

Users will not be able to email the channel directly.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Teams` select `Teams settings`.
3. Under email integration verify that `Users can send emails to a channel email address` is `Off`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsClientConfiguration -Identity Global | fl AllowEmailIntoChannel
```

3. Ensure the returned value is `False`.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Teams` select `Teams settings`.
3. Under email integration set `Users can send emails to a channel email address` to `Off`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsClientConfiguration -Identity Global -AllowEmailIntoChannel $false
```

Default Value:

On (True)

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#restricting-channel-email-messages-to-approved-domains
2. https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsclientconfiguration?view=skype-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

8.2 Users

8.2.1 (L1) Ensure 'external access' is restricted in the Teams admin center (Automated)

Profile Applicability:

- E3 Level 2

Description:

This policy setting controls chat with external unmanaged Skype and Teams users. Users in the organization will not be searchable by unmanaged Skype or Teams users and will have to initiate all communications with unmanaged users.

Note: As of December 2021, the default for Teams external communication is set to 'People in my organization can communicate with Teams users whose accounts aren't managed by an organization.'

Note #2: Skype for business is deprecated as of July 31, 2021, although these settings may still be valid for a period of time. See the link in the reference section for more information.

Rationale:

Allowing users to communicate with Skype or Teams users outside of an organization presents a potential security threat as external users can interact with organization users over Skype for Business or Teams. While legitimate, productivity-improving scenarios exist, they are outweighed by the risk of data loss, phishing, and social engineering attacks against organization users via Teams. Therefore, it is recommended to restrict external communications in order to minimize the risk of security incidents.

Impact:

The impact of disabling external access to Teams and Skype for an organization is highly dependent on current usage practices. If users infrequently communicate with external parties using these channels, the impact is likely to be minimal. However, if users regularly use Teams and Skype for client communication, the impact could be significant. Therefore, before disabling external access, users should be notified, and alternate communication mechanisms should be identified to ensure continuity of communication.

Note: Chat with external unmanaged Teams users isn't available in GCC, GCC High, or DOD deployments, or in private cloud environments.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Under `Teams and Skype for Business users in external organizations` ensure `Block all external domains`
    - **NOTE:** If the organization's policy allows select `Allow only specific external domains` and add the allowed domains domains.
4. Under `Teams accounts not managed by an organization` ensure the slider is set to `Off`.
5. Under `Skype users` ensure the slider is set to `Off`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command:

```
Get-CsTenantFederationConfiguration | fl
AllowTeamsConsumer,AllowPublicUsers,AllowFederatedUsers,AllowedDomains
```

- State: `AllowTeamsConsumer` is `False`
- State: `AllowPublicUsers` is `False`
- State: `AllowFederatedUsers` is `False` **OR**,
- If: `AllowFederatedUsers` is `True` then ensure `AllowedDomains` contains authorized domain names.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com/.
2. Click to expand `Users` select `External access`.
3. Under `Teams and Skype for Business users in external organizations` Select `Block all external domains`
   - **NOTE:** If the organization's policy allows select any allowed external domains.
4. Under `Teams accounts not managed by an organization` move the slider to `Off`.
5. Under `Skype users` move the slider is to `Off`.
6. Click `Save`.

To remediate using PowerShell:

- Connect to Teams PowerShell using `Connect-MicrosoftTeams`
- Run the following command:

```
Set-CsTenantFederationConfiguration -AllowTeamsConsumer False -
AllowPublicUsers False -AllowFederatedUsers $false
```

- To allow only specific external domains run these commands replacing the example domains with approved domains:

```
Set-CsTenantFederationConfiguration -AllowTeamsConsumer $false -
AllowPublicUsers $false -AllowFederatedUsers $true
$list = New-Object Collections.Generic.List[String]
$list.add("contoso.com")
$list.add("fabrikam.com")
Set-CsTenantFederationConfiguration -AllowedDomainsAsAList $list
```

Default Value:

- AllowTeamsConsumer : `True`
- AllowPublicUsers : `True`
- AllowFederatedUsers : `True`
- AllowedDomains : `AllowAllKnownDomains`

References:

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

Additional Information:

An additional audit method for this recommendation:

```
$passed = $true

$externalAccessConfig = Get-CsTenantFederationConfiguration
$externalAccessConfig | fl
AllowTeamsConsumer,AllowPublicUsers,AllowFederatedUsers

if ($externalAccessConfig.AllowTeamsConsumer) {
    $passed = $false
    Write-Host "*** Teams public users are allowed." -ForegroundColor Red
} else {
    Write-Host "*** Teams public users are forbidden."-ForegroundColor Green
}

if ($externalAccessConfig.AllowPublicUsers) {
    $passed = $false
    Write-Host "*** Skype public user are allowed." -ForegroundColor Red
} else {
    Write-Host "*** Skype public user are forbidden." -ForegroundColor Green
}

if ($externalAccessConfig.AllowFederatedUsers) {
    if ($externalAccessConfig.AllowedDomains.AllowedDomain.count -gt 0 ) {
        Write-Host ("*** External domains are allowed but limited ->
AllowedDomains = " +
            $($externalAccessConfig.AllowedDomains.AllowedDomain -join (",
"))) -ForegroundColor Green
    } elseif ($externalAccessConfig.BlockedDomains.count -gt 0 ) {
        Write-Host ("*** External domains are allowed but limited ->
BlockedDomains = " +
            $($externalAccessConfig.BlockedDomains.Domain -join (", "))) -
ForegroundColor Green
    } else {
        $passed = $false
        Write-Host "*** External domains are allowed and NOT limited" -
ForegroundColor Red
    }
} else {
    Write-Host "*** External domains are forbidden" -ForegroundColor Green
}
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

8.3 Teams devices

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

8.4 Teams apps

8.4.1 (L1) Ensure app permission policies are configured (Manual)

Profile Applicability:

- E3 Level 1

Description:

This policy setting controls which class of apps are available for users to install.

Rationale:

Allowing users to install third-party or unverified apps poses a potential risk of introducing malicious software to the environment.

Impact:

Users will only be able to install approved classes of apps.

Audit:

Ensure app permission policies are configured:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Teams apps` select `Permission policies`.
3. Click `Global (Org-wide default)`.
4. For `Microsoft apps` verify that app permission policies are set to `Allow all apps`.
5. For `Third-party apps` verify that app permission policies are set to `Block all apps` **OR** `Allow specific apps and block all others`.
6. For `Custom apps` verify that app permission policies are set to `Block all apps` **OR** `Allow specific apps and block all others`.

Remediation:

To set app permission policies:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Teams apps` select `Permission policies`.
3. Click `Global (Org-wide default)`.
4. For `Microsoft apps` set app permission policies to `Allow all apps`.
5. For `Third-party apps` set app permission policies to `Block all apps` **OR** `Allow specific apps and block all others`.
6. For `Custom apps` set app permission policies to `Block all apps` **OR** `Allow specific apps and block all others`.

Default Value:

Microsoft apps: Allow all apps

Third-party apps: Allow all apps

Custom apps: Allow all apps

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#disabling-third-party--custom-apps
2. https://learn.microsoft.com/en-us/microsoftteams/teams-app-permission-policies

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

8.5 Meetings

8.5.1 (L2) Ensure anonymous users can't join a meeting (Automated)

Profile Applicability:

- E3 Level 2

Description:

This policy setting can prevent anyone other than invited attendees (people directly invited by the organizer, or to whom an invitation was forwarded) from bypassing the lobby and entering the meeting.

For more information on how to setup a sensitive meeting, please visit: Configure Teams meetings with protection for sensitive data - Microsoft Teams | Microsoft Learn

Rationale:

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times.

Note: Those companies that don't normally operate at a Level 2 environment, but do deal with sensitive information, may want to consider this policy setting.

Impact:

Individuals who were not sent or forwarded a meeting invite will not be able to join the meeting automatically.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting join & lobby verify that `Anonymous users can join a meeting` is set to `Off`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl
AllowAnonymousUsersToJoinMeeting
```

3. Ensure the returned value is `False`.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`
4. Under meeting join & lobby set `Anonymous users can join a meeting` to `Off`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToJoinMeeting
$false
```

Default Value:

On (True)

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

8.5.2 (L1) Ensure anonymous users and dial-in callers can't start a meeting (Automated)

Profile Applicability:

- E3 Level 1

Description:

This policy setting controls if an anonymous participant can start a Microsoft Teams meeting without someone in attendance. Anonymous users and dial-in callers must wait in the lobby until the meeting is started by someone in the organization or an external user from a trusted organization.

Anonymous participants are classified as:

- Participants who are not logged in to Teams with a work or school account.
- Participants from non-trusted organizations (as configured in external access).
- Participants from organizations where there is not mutual trust.

Note: This setting only applies when `Who can bypass the lobby` is set to `Everyone`. If the `anonymous users can join a meeting` organization-level setting or meeting policy is `Off`, this setting only applies to dial-in callers.

Rationale:

Not allowing anonymous participants to automatically join a meeting reduces the risk of meeting spamming.

Impact:

Anonymous participants will not be able to start a Microsoft Teams meeting.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting join & lobby verify that `Anonymous users and dial-in callers can start a meeting` is set to `Off`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl
AllowAnonymousUsersToStartMeeting
```

3. Ensure the returned value is `False`.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting join & lobby set `Anonymous users and dial-in callers can start a meeting` to `Off`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowAnonymousUsersToStartMeeting
$false
```

Default Value:

Off (False)

References:

1. https://learn.microsoft.com/en-us/microsoftteams/anonymous-users-in-meetings
2. https://learn.microsoft.com/en-US/microsoftteams/who-can-bypass-meeting-lobby?WT.mc_id=TeamsAdminCenterCSH#overview-of-lobby-settings-and-policies

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

8.5.3 (L1) Ensure only people in my org can bypass the lobby (Automated)

Profile Applicability:

- E3 Level 1

Description:

This policy setting controls who can join a meeting directly and who must wait in the lobby until they're admitted by an organizer, co-organizer, or presenter of the meeting.

Rationale:

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly sent an invite before admitting them to the meeting. This will also prevent the anonymous user from using the meeting link to have meetings at unscheduled times.

Impact:

Individuals who were not part of the organization will have to wait in the lobby until they're admitted by an organizer, co-organizer, or presenter of the meeting.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting join & lobby verify `Who can bypass the lobby` is set to `People in my org`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl AutoAdmittedUsers
```

3. Ensure the returned value is `EveryoneInCompanyExcludingGuests`

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting join & lobby set `Who can bypass the lobby` to `People in my org`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AutoAdmittedUsers
"EveryoneInCompanyExcludingGuests"
```

Default Value:

People in my org and guests (EveryoneInCompany)

References:

1. https://learn.microsoft.com/en-US/microsoftteams/who-can-bypass-meeting-lobby?WT.mc_id=TeamsAdminCenterCSH
2. https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps

CIS Controls:

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

8.5.4 (L1) Ensure users dialing in can't bypass the lobby (Automated)

Profile Applicability:

- E3 Level 1

Description:

This policy setting controls if users who dial in by phone can join the meeting directly or must wait in the lobby. Admittance to the meeting from the lobby is authorized by the meeting organizer, co-organizer, or presenter of the meeting.

Rationale:

For meetings that could contain sensitive information, it is best to allow the meeting organizer to vet anyone not directly from the organization.

Impact:

Individuals who are dialing in to the meeting must wait in the lobby until a meeting organizer, co-organizer, or presenter admits them.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting join & lobby verify that `People dialing in can bypass the lobby` is set to `Off`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl AllowPSTNUsersToBypassLobby
```

3. Ensure the value is `False`.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting join & lobby set `People dialing in can't bypass the lobby` to `Off`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowPSTNUsersToBypassLobby $false
```

Default Value:

Off (False)

References:

1. https://learn.microsoft.com/en-US/microsoftteams/who-can-bypass-meeting-lobby?WT.mc_id=TeamsAdminCenterCSH#choose-who-can-bypass-the-lobby-in-meetings-hosted-by-your-organization
2. https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

8.5.5 (L2) Ensure meeting chat does not allow anonymous users (Automated)

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

Ensuring that only authorized individuals can read and write chat messages during a meeting reduces the risk that a malicious user can inadvertently show content that is not appropriate or view sensitive information.

Impact:

Only authorized individuals will be able to read and write chat messages during a meeting.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting engagement verify that `Meeting chat` is set to `On for everyone but anonymous users`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl MeetingChatEnabledType
```

3. Ensure the returned value is `EnabledExceptAnonymous`.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under meeting engagement set `Meeting chat` to `On for everyone but anonymous users`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -MeetingChatEnabledType
"EnabledExceptAnonymous"
```

Default Value:

On for everyone (Enabled)

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

8.5.6 (L2) Ensure only organizers and co-organizers can present (Automated)

Profile Applicability:

- E3 Level 1

Description:

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

Note: Organizers and co-organizers can change this setting when the meeting is set up.

Rationale:

Ensuring that only authorized individuals are able to present reduces the risk that a malicious user can inadvertently show content that is not appropriate.

Impact:

Only organizers and co-organizers will be able to present without being granted permission.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under content sharing verify `Who can present` is set to `Only organizers and co-organizers`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl DesignatedPresenterRoleMode
```

3. Ensure the returned value is `OrganizerOnlyUserOverride`.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under content sharing set `Who can present` to `Only organizers and co-organizers`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -DesignatedPresenterRoleMode
"OrganizerOnlyUserOverride"
```

Default Value:

Everyone (EveryoneUserOverride)

References:

1. https://learn.microsoft.com/en-US/microsoftteams/meeting-who-present-request-control
2. https://learn.microsoft.com/en-us/microsoftteams/meeting-who-present-request-control#manage-who-can-present
3. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/step-by-step-guides/reducing-attack-surface-in-microsoft-teams?view=o365-worldwide#configure-meeting-settings-restrict-presenters
4. https://learn.microsoft.com/en-us/powershell/module/skype/set-csteamsmeetingpolicy?view=skype-ps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

8.5.7 (L1) Ensure external participants can't give or request control (Automated)

Profile Applicability:

- E3 Level 1

Description:

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

Rationale:

Ensuring that only authorized individuals and not external participants are able to present and request control reduces the risk that a malicious user can inadvertently show content that is not appropriate.

External participants are categorized as follows: external users, guests, and anonymous users.

Impact:

External participants will not be able to present or request control during the meeting.

Warning: This setting also affects webinars.

Note: At this time, to give and take control of shared content during a meeting, both parties must be using the Teams desktop client. Control isn't supported when either party is running Teams in a browser.

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under content sharing verify that `External participants can give or request control` is `Off`.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to verify the recommended state:

```
Get-CsTeamsMeetingPolicy -Identity Global | fl
AllowExternalParticipantGiveRequestControl
```

3. Ensure the returned value is `False`.

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Meetings` select `Meeting policies`.
3. Click `Global (Org-wide default)`.
4. Under content sharing set `External participants can give or request control` to `Off`.

To remediate using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Run the following command to set the recommended state:

```
Set-CsTeamsMeetingPolicy -Identity Global -
AllowExternalParticipantGiveRequestControl $false
```

Default Value:

Off (False)

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

8.6 Messaging

8.6.1 (L1) Ensure users can report security concerns in Teams (Automated)

Profile Applicability:

- E3 Level 1

Description:

User reporting settings allow a user to report a message as malicious for further analysis. This recommendation is composed of 3 different settings and all be configured to pass:

- **In the Teams admin center:** On by default and controls whether users are able to report messages from Teams. When this setting is turned off, users can't report messages within Teams, so the corresponding setting in the Microsoft 365 Defender portal is irrelevant.
- **In the Microsoft 365 Defender portal:** On by default for new tenants. Existing tenants need to enable it. If user reporting of messages is turned on in the Teams admin center, it also needs to be turned on the Defender portal for user reported messages to show up correctly on the User reported tab on the Submissions page.
- **Defender - Report message destinations:** This applies to more than just Microsoft Teams and allows for an organization to keep their reports contained. Due to how the parameters are configured on the backend it is included in this assessment as a requirement.

Rationale:

Users will be able to more quickly and systematically alert administrators of suspicious malicious messages within Teams. The content of these messages may be sensitive in nature and therefore should be kept within the organization and not shared with Microsoft without first consulting company policy.

Note:

- The reported message remains visible to the user in the Teams client.
- Users can report the same message multiple times.
- The message sender isn't notified that messages were reported.

Impact:

Enabling message reporting has an impact beyond just addressing security concerns. When users of the platform report a message the content could include messages that are threatening or harassing in nature, possibly stemming from colleagues.

Due to this security staff responsible for reviewing and acting on these reports should be equipped with the skills to discern and appropriately direct such messages to the relevant departments, such as Human Resources (HR).

Audit:

To audit using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Messaging` select `Messaging policies`.
3. Click `Global (Org-wide default)`.
4. Ensure `Report a security concern` is `On`.
5. Next, navigate to `Microsoft 365 Defender` https://security.microsoft.com/
6. Click on `Settings` > `Email & collaboration` > `User reported settings`.
7. Scroll to `Microsoft Teams`.
8. Ensure `Monitor reported messages in Microsoft Teams` is checked.
9. Ensure `Send reported messages to:` is set to `My reporting mailbox only` with report email addresses defined for authorized staff.

To audit using PowerShell:

1. Connect to Teams PowerShell using `Connect-MicrosoftTeams`.
2. Connect to Exchange Online PowerShell using `Connect-ExchangeOnline`.
3. Run the following cmdlet for to assess Teams:

```
Get-CsTeamsMessagingPolicy -Identity Global | fl
AllowSecurityEndUserReporting
```

4. Ensure the value returned is `True`.
5. Run this cmdlet to assess Defender:

```
Get-ReportSubmissionPolicy | fl Report*
```

6. Ensure the output matches the following values with organization specific email addresses:

```
ReportJunkToCustomizedAddress                 : True
ReportNotJunkToCustomizedAddress              : True
ReportPhishToCustomizedAddress                : True
ReportJunkAddresses                           : {SOC@contoso.com}
ReportNotJunkAddresses                        : {SOC@contoso.com}
ReportPhishAddresses                          : {SOC@contoso.com}
ReportChatMessageEnabled                      : False
ReportChatMessageToCustomizedAddressEnabled : True
```

Remediation:

To remediate using the UI:

1. Navigate to `Microsoft Teams admin center` https://admin.teams.microsoft.com.
2. Click to expand `Messaging` select `Messaging policies`.
3. Click `Global (Org-wide default)`.
4. Set `Report a security concern` to `On`.
5. Next, navigate to `Microsoft 365 Defender` https://security.microsoft.com/
6. Click on `Settings` > `Email & collaboration` > `User reported settings`.
7. Scroll to `Microsoft Teams`.
8. Check `Monitor reported messages in Microsoft Teams` and `Save`.
9. Set `Send reported messages to:` to `My reporting mailbox only` with reports configured to be sent to authorized staff.

To remediate using PowerShell:

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

```
Set-CsTeamsMessagingPolicy -Identity Global -AllowSecurityEndUserReporting
$true
```

4. To configure the Defender reporting policies, edit and run this script:

```
$usersub = "userreportedmessages@fabrikam.com" # Change this.

$params = @{
    Identity                              = "DefaultReportSubmissionPolicy"
    EnableReportToMicrosoft               = $false
    ReportChatMessageEnabled              = $false
    ReportChatMessageToCustomizedAddressEnabled = $true
    ReportJunkToCustomizedAddress         = $true
    ReportNotJunkToCustomizedAddress      = $true
    ReportPhishToCustomizedAddress        = $true
    ReportJunkAddresses                   = $usersub
    ReportNotJunkAddresses                = $usersub
    ReportPhishAddresses                  = $usersub
}

Set-ReportSubmissionPolicy @params

New-ReportSubmissionRule -Name DefaultReportSubmissionRule -
ReportSubmissionPolicy DefaultReportSubmissionPolicy -SentTo $usersub
```

Default Value:

On (`True`)

Report message destination: `Microsoft Only`

References:

1. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/submissions-teams?view=o365-worldwide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

9 Microsoft Fabric

Microsoft Fabric is Microsoft's new name for Power BI and contains settings for everything related to Power BI configuration.

Direct link: https://app.powerbi.com/admin-portal/

9.1 Tenant settings

9.1.1 (L1) Ensure guest user access is restricted (Manual)

Profile Applicability:

- E3 Level 1

Description:

This setting allows business-to-business (B2B) guests access to Microsoft Fabric, and contents that they have permissions to. With the setting turned off, B2B guest users receive an error when trying to access Power BI.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

Rationale:

Establishing and enforcing a dedicated security group prevents unauthorized access to Microsoft Fabric for guests collaborating in Azure that are new or assigned guest status from other applications. This upholds the principle of least privilege and uses role-based access control (RBAC). These security groups can also be used for tasks like conditional access, enhancing risk management and user accountability across the organization.

Impact:

Security groups will need to be more closely tended to and monitored.

Audit:

Ensure AAD guest user access is restricted:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Allow Azure Active Directory guest users to access Microsoft Fabric` adheres to one of these states:
   - State 1: `Disabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Remediation:

Restrict AAD guest user access:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Allow Azure Active Directory guest users to access Microsoft Fabric` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Default Value:

Enabled for Entire Organization

References:

1. https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

9.1.2 (L1) Ensure external user invitations are restricted (Manual)

Profile Applicability:

- E3 Level 1

Description:

The Invite external users setting helps organizations choose whether new external users can be invited to the organization through Power BI sharing, permissions, and subscription experiences. This setting only controls the ability to invite through Power BI.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

Note: To invite external users to the organization, the user must also have the Azure Active Directory Guest Inviter role.

Rationale:

Establishing and enforcing a dedicated security group prevents unauthorized access to Microsoft Fabric for guests collaborating in Azure that are new or assigned guest status from other applications. This upholds the principle of least privilege and uses role-based access control (RBAC). These security groups can also be used for tasks like conditional access, enhancing risk management and user accountability across the organization.

Impact:

Guest user invitations will be limited to only specific employees.

Audit:

Ensure external user invitations are restricted:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Invite external users to your organization` adheres to one of these states:
   - State 1: `Disabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Remediation:

Restrict external user invitations:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Invite external users to your organization` to one of these states:
   - State 1: `Disabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Default Value:

Enabled for the entire organization

References:

1. https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing
2. https://learn.microsoft.com/en-us/power-bi/enterprise/service-admin-azure-ad-b2b#invite-guest-users

CIS Controls:

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

9.1.3 (L1) Ensure guest access to content is restricted (Manual)

Profile Applicability:

- E3 Level 1

Description:

This setting allows Azure AD B2B guest users to have full access to the browsing experience using the left-hand navigation pane in the organization. Guest users who have been assigned workspace roles or specific item permissions will continue to have those roles and/or permissions, even if this setting is disabled.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

Rationale:

Establishing and enforcing a dedicated security group prevents unauthorized access to Microsoft Fabric for guests collaborating in Azure that are new or assigned guest status from other applications. This upholds the principle of least privilege and uses role-based access control (RBAC). These security groups can also be used for tasks like conditional access, enhancing risk management and user accountability across the organization.

Impact:

Security groups will need to be more closely tended to and monitored.

Audit:

Ensure AAD guest user content access is restricted:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Allow Azure Active Directory guest users to edit and manage content in the organization` adheres to one of these states:
   - State 1: `Disabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Remediation:

Restrict AAD guest user content access access:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Allow Azure Active Directory guest users to edit and manage content in the organization` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Default Value:

Disabled

References:

1. https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

9.1.4 (L1) Ensure 'Publish to web' is restricted (Manual)

Profile Applicability:

- E3 Level 1

Description:

Power BI enables users to share reports and materials directly on the internet from both the application's desktop version and its web user interface. This functionality generates a publicly reachable web link that doesn't necessitate authentication or the need to be an AAD user in order to access and view it.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

Rationale:

When using Publish to the Web anyone on the Internet can view a published report or visual. Viewing requires no authentication. It includes viewing detail-level data that your reports aggregate. By disabling the feature, restricting access to certain users and allowing existing embed codes organizations can mitigate the exposure of confidential or proprietary information.

Impact:

Depending on the organization's utilization administrators may experience more overhead managing embed codes, and requests.

Audit:

Ensure Publish to the web is restricted:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Publish to the web` adheres to one of these states:
   - State 1: `Disabled`
   - State 2: `Enabled` with `Choose how embed codes work` set to `Only allow existing codes` **AND** `Specific security groups` selected and defined

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Remediation:

Restrict Publish to the web:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Publish to the web` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Choose how embed codes work` set to `Only allow existing codes` **AND** `Specific security groups` selected and defined

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Default Value:

Enabled for the entire organization

Only allow existing codes

References:

1. https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-publish-to-web
2. https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing#publish-to-web

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	16.10 Apply Secure Design Principles in Application Architectures Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.		●	●

9.1.5 (L2) Ensure 'Interact with and share R and Python' visuals is 'Disabled' (Manual)

Profile Applicability:

- E3 Level 2

Description:

Power BI allows the integration of R and Python scripts directly into visuals. This feature allows data visualizations by incorporating custom calculations, statistical analyses, machine learning models, and more using R or Python scripts. Custom visuals can be created by embedding them directly into Power BI reports. Users can then interact with these visuals and see the results of the custom code within the Power BI interface.

Rationale:

Disabling this feature can reduce the attack surface by preventing potential malicious code execution leading to data breaches, or unauthorized access. The potential for sensitive or confidential data being leaked to unintended users is also increased with the use of scripts.

Impact:

Use of R and Python scripting will require exceptions for developers, along with more stringent code review.

Audit:

Ensure the recommended state is configured:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `R and Python visuals settings`.
4. Ensure that `Interact with and share R and Python visuals` is `Disabled`

Remediation:

Configure the recommended state:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `R and Python visuals settings`.
4. Set `Interact with and share R and Python visuals` to `Disabled`

Default Value:

Enabled

References:

1. https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-r-python-visuals
2. https://learn.microsoft.com/en-us/power-bi/visuals/service-r-visuals
3. https://www.r-project.org/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

9.1.6 (L1) Ensure 'Allow users to apply sensitivity labels for content' is 'Enabled' (Manual)

Profile Applicability:

- E3 Level 1

Description:

Information protection tenant settings help to protect sensitive information in the Power BI tenant. Allowing and applying sensitivity labels to content ensures that information is only seen and accessed by the appropriate users.

The recommended state is `Enabled` or `Enabled for a subset of the organization`.

Note: Sensitivity labels and protection are only applied to files exported to Excel, PowerPoint, or PDF files, that are controlled by "Export to Excel" and "Export reports as PowerPoint presentation or PDF documents" settings. All other export and sharing options do not support the application of sensitivity labels and protection.

Note 2: There are some prerequisite steps that need to be completed in order to fully utilize labeling. See here.

Rationale:

Establishing data classifications and affixing labels to data at creation enables organizations to discern the data's criticality, sensitivity, and value. This initial identification enables the implementation of appropriate protective measures, utilizing technologies like Data Loss Prevention (DLP) to avert inadvertent exposure and enforcing access controls to safeguard against unauthorized access.

This practice can also promote user awareness and responsibility in regard to the nature of the data they interact with. Which in turn can foster awareness in other areas of data management across the organization.

Impact:

Additional license requirements like Power BI Pro are required, as outlined in the Licensed and requirements page linked in the description and references sections.

Audit:

Ensure sensitivity labels are Enabled:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Information protection`.
4. Ensure that `Allow users to apply sensitivity labels for content` adheres to one of these states:
   - State 1: `Enabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

Remediation:

Enable sensitivity labels:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Information protection`.
4. Set `Allow users to apply sensitivity labels for content` to one of these states:
   - State 1: `Enabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

Default Value:

Disabled

References:

1. https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-enable-data-sensitivity-labels
2. https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-dlp-policies-for-power-bi-overview
3. https://learn.microsoft.com/en-us/power-bi/enterprise/service-security-enable-data-sensitivity-labels#licensing-and-requirements

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.2 Establish and Maintain a Data Inventory Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	●	●	●
v8	3.7 Establish and Maintain a Data Classification Scheme Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●

9.1.7 (L1) Ensure shareable links are restricted (Manual)

Profile Applicability:

- E3 Level 1

Description:

Creating a shareable link allows a user to create a link to a report or dashboard, then add that link to an email or another messaging application.

There are 3 options that can be selected when creating a shareable link:

- People in your organization
- People with existing access
- Specific people

This setting solely deals with restrictions to `People in the organization`. External users by default are not included in any of these categories, and therefore cannot use any of these links regardless of the state of this setting.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

Rationale:

While external users are unable to utilize shareable links, disabling or restricting this feature ensures that a user cannot generate a link accessible by individuals within the same organization who lack the necessary clearance to the shared data. For example, a member of Human Resources intends to share sensitive information with a particular employee or another colleague within their department. The owner would be prompted to specify either `People with existing access` or `Specific people` when generating the link requiring the person clicking the link to pass a first layer access control list. This measure along with proper file and folder permissions can help prevent unintended access and potential information leakage.

Impact:

If the setting is `Enabled` then only specific people in the organization would be allowed to create general links viewable by the entire organization.

Audit:

Ensure shareable links are restricted:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Allow shareable links to grant access to everyone in your organization` adheres to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Remediation:

Restrict shareable links:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Allow shareable links to grant access to everyone in your organization` to one of these states:
    - State 1: `Disabled`
    - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Default Value:

Enabled for Entire Organization

References:

1. https://learn.microsoft.com/en-us/power-bi/collaborate-share/service-share-dashboards?wt.mc_id=powerbi_inproduct_sharedialog#link-settings
2. https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●

9.1.8 (L1) Ensure enabling of external data sharing is restricted (Manual)

Profile Applicability:

- E3 Level 1

Description:

Power BI admins can specify which users or user groups can share datasets externally with guests from a different tenant through the in-place mechanism. Disabling this setting prevents any user from sharing datasets externally by restricting the ability of users to turn on external sharing for datasets they own or manage.

The recommended state is `Enabled for a subset of the organization` or `Disabled`.

Rationale:

Establishing and enforcing a dedicated security group prevents unauthorized access to Microsoft Fabric for guests collaborating in Azure that are new or from other applications. This upholds the principle of least privilege and uses role-based access control (RBAC). These security groups can also be used for tasks like conditional access, enhancing risk management and user accountability across the organization.

Impact:

Security groups will need to be more closely tended to and monitored.

Audit:

Ensure external data sharing is restricted:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Ensure that `Allow specific users to turn on external data sharing` adheres to one of these states:
   - State 1: `Disabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Remediation:

Restrict external data sharing:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Export and Sharing settings`.
4. Set `Allow specific users to turn on external data sharing` to one of these states:
   - State 1: `Disabled`
   - State 2: `Enabled` with `Specific security groups` selected and defined.

Important: If the organization doesn't actively use this feature it is recommended to keep it `Disabled`.

Default Value:

Enabled for the entire organization

References:

1. https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-export-sharing

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

9.1.9 (L1) Ensure 'Block ResourceKey Authentication' is 'Enabled' (Manual)

Profile Applicability:

- E3 Level 1

Description:

This setting blocks the use of resource key based authentication. The Block ResourceKey Authentication setting applies to streaming and PUSH datasets. If blocked users will not be allowed send data to streaming and PUSH datasets using the API with a resource key.

The recommended state is `Enabled`.

Rationale:

Resource keys are a form of authentication that allows users to access Power BI resources (such as reports, dashboards, and datasets) without requiring individual user accounts. While convenient, this method bypasses the organization's centralized identity and access management controls. Enabling ensures that access to Power BI resources is tied to the organization's authentication mechanisms, providing a more secure and controlled environment.

Impact:

Developers will need to request a special exception in order to use this feature.

Audit:

Ensure ResourceKey Authentication is Enabled:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Developer settings`.
4. Ensure that `Block ResourceKey Authentication` is `Enabled`

Remediation:

Ensure ResourceKey Authentication is Enabled:

1. Navigate to `Microsoft Fabric` https://app.powerbi.com/admin-portal
2. Select `Tenant settings`.
3. Scroll to `Developer settings`.
4. Set `Block ResourceKey Authentication` to `Enabled`

Default Value:

Disabled for the entire organization

References:

1. https://learn.microsoft.com/en-us/power-bi/admin/service-admin-portal-developer
2. https://learn.microsoft.com/en-us/power-bi/connect-data/service-real-time-streaming

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●