CIS Benchmarks

CIS Microsoft 365 Foundations Benchmark

v1.0.0 - 12-06-2018

Terms of Use

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

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

Table of Contents

Overview

This document, Security Configuration Benchmark for Microsoft 365, provides prescriptive guidance for establishing a secure configuration posture for Microsoft 365 running on any OS. This guide was tested against Microsoft 365. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft 365.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

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

Scored

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

Not Scored

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile apply to Microsoft 365 and are intend to:

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

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

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

Acknowledgements

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

Editor
Sean Sweeney
Jonathan Trull
Dan Menicucci
Gururaj Pandurangi
Shamir Charania
Dan Menicucci
Karen Scarfone

Contributor
Jordan Rakoske GSEC, GCWN

Recommendations

1 Account / Authentication

1.1 (L1) Ensure multifactor authentication is enabled for all users in administrative roles (Scored)

Profile Applicability:

- Level 1

Description:

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

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

Rationale:

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

Audit:

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

1. Log in as a `Global Administrator`.

2. Go to `Users` > `Active Users`.
3. Click on `More` > `Multifactor Authentication Setup`.
4. Using the `View` Option, select the appropriate administrator role to review.
5. Review Users for Multifactor authentication status.

To verify the multifactor authentication configuration for administrators, use the Office 365 PowerShell MSOL:

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

```
Get-MsolRole | Where-Object {$_.Name -like "*Administrator*"} | ForEach-
Object { Get-MsolRoleMember -RoleObjectId $_.ObjectId } | Select-Object
EmailAddress, @{N="MFA Status";
e={$_.StrongAuthenticationRequirements.state}} -Unique
```

3. Ensure that `MFA Status` equals `Enforced`.

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

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

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

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

Remediation:

To enable multifactor authentication for administrators, use the Azure Portal:

1. Sign in to the Azure Portal as a Global Administrator, Security Administrator, or Conditional Access Administrator.
2. In the Azure Portal, on the left navbar, click `Azure Active Directory`.
3. On the Azure Active Directory page, in the Security section, click `Conditional access`.
4. In the list of policies, click the policy named `Baseline policy: Require MFA for admins`.
5. To enable the policy, select `Use policy immediately`.
6. Click `Save`.

To enable multifactor authentication for administrators, use the Office 365 PowerShell MSOL:

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

```
$Auth = New-Object -TypeName
Microsoft.Online.Administration.StrongAuthenticationRequirement -Property
@{RelyingParty = "*"; State = "Enabled"}

Get-MsolRole | Where-Object {$_.Name -like "*Administrator*"} | ForEach-
Object { Get-MsolRoleMember -RoleObjectId $_.ObjectId } | Select-Object -
Unique | ForEach-Object { Set-MsolUser -ObjectId $_.ObjectId -
StrongAuthenticationRequirements $Auth }
```

References:

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

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

1.2 (L2) Ensure multifactor authentication is enabled for all users in all roles (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

1. Log in as a `Global Administrator`.
2. Go to `Users` > `Active Users`.
3. Click on `More` > `Multifactor Authentication Setup`.
4. Using the `View` Option, select `Sign-in allowed users`.
5. Confirm there are no users with an MFA Status set to `Disabled`.

To verify the multifactor authentication configuration for all users, use the Office 365 PowerShell MSOL:

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

```
Get-MsolUser –All | Select-Object UserPrincipalName, @{N="MFA Status";
e={$_.StrongAuthenticationRequirements.State}}
```

3. Ensure that `MFA Status` equals `Enforced`.

Remediation:

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

1. Log in as a `Global Administrator`.
2. Go to `Users` > `Active Users`.
3. Click on `More` > `Multifactor Authentication Setup`.
4. Using the `View` Option, select `Sign-in allowed users`.
5. Select all users with MFA Status set to `Disabled`.
6. Click `Enable`.

To enable multifactor authentication for all users, use the Office 365 PowerShell MSOL:

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

```
$Auth = New-Object -TypeName
Microsoft.Online.Administration.StrongAuthenticationRequirement -Property
@{RelyingParty = "*"; State = "Enabled"}

Get-MsolUser –All | ForEach-Object { Set-MsolUser -UserPrincipalName
$_.UserPrincipalName -StrongAuthenticationRequirements $Auth }
```

Default Value:

Disabled

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

1.3 (L1) Ensure that between two and four global admins are designated (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

1. Select `Users` > `Active Users`.
2. Set `Views` to `Global Admins`.
3. Review the list of `Global Admins` to confirm there are from two to four such accounts.

Remediation:

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

1. Select `Users` > `Active Users`.
2. Set `Views` to `Global Admins`.
3. To create a new Global Admin:
    1. Select `Add Users`.
    2. Enter User Information.
    3. Select `Roles`.
    4. Select `Global Administrator`.
    5. Click `Add`.
4. To remove Global Admins:

1. Select User.
2. Select `Edit` under `Roles`.
3. Select `Customized administrator` and chose appropriate role.
4. Click `Save`.

CIS Controls:

Version 7

4.1 Maintain Inventory of Administrative Accounts
Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.

1.4 (L1) Ensure self-service password reset is enabled (Scored)

Profile Applicability:

- Level 1

Description:

Enabling self-service password reset allows users to reset their own passwords in Azure AD. When your users sign in to Microsoft 365, they will be prompted to enter additional contact information that will help them reset their password in the future.

Self-service password reset is free for cloud users with Microsoft 365 business, non-profit or education plans. It doesn't work with trial subscriptions. If you are using On-premise AD and syncing your users, it requires a paid subscription to Azure AD Premium.

Rationale:

Users will no longer need to engage the helpdesk for password resets, and the password reset mechanism will automatically block common, easily guessable passwords.

Audit:

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

1. Choose `Settings` > `Security & privacy`.
2. Choose the link to go to the `Azure admin center`.
3. Choose `Users and groups` > `Password reset`.
4. On the Properties page, check the selected option.

Remediation:

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

1. Choose `Settings` > `Security & privacy`.
2. Choose the link to go to the `Azure admin center`.
3. Choose `Users and groups` > `Password reset`.
4. On the Properties page, choose `All` to enable it for everyone in your business, and then choose `Save`.

References:

1. https://support.office.com/en-us/article/let-users-reset-their-own-passwords-in-office-365-5bc3f460-13cc-48c0-abd6-b80bae72d04a
2. https://gallery.technet.microsoft.com/office/Enable-Self-Service-59846d88

3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr

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

Profile Applicability:

- Level 1

Description:

Modern authentication in Microsoft 365 enables authentication features like multifactor authentication (MFA) using smart cards, certificate-based authentication (CBA), and third-party SAML identity providers. When you enable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use modern authentication to log in to Microsoft 365 mailboxes. When you disable modern authentication in Exchange Online, Outlook 2016 and Outlook 2013 use basic authentication to log in to Microsoft 365 mailboxes.

When users initially configure certain email clients, like Outlook 2013 and Outlook 2016, they may be required to authenticate using enhanced authentication mechanisms, such as multifactor authentication. Other Outlook clients that are available in Microsoft 365 (for example, Outlook Mobile and Outlook for Mac 2016) always use modern authentication to log in to Microsoft 365 mailboxes.

Rationale:

Strong authentication controls, such as the use of multifactor authentication, may be circumvented if basic authentication is used by Exchange Online email clients such as Outlook 2016 and Outlook 2013. Enabling modern authentication for Exchange Online ensures strong authentication mechanisms are used when establishing sessions between email clients and Exchange Online.

Audit:

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

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

```
Get-OrganizationConfig | Format-Table -Auto Name, OAuth*
```

4. Verify `OAuth2ClientProfileEnabled` is `True`.

Remediation:

To enable modern authentication, use the Exchange Online PowerShell Module:

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

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $True
```

Default Value:

True

References:

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

CIS Controls:

Version 7

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

2 Application Permissions

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

Profile Applicability:

- Level 2

Description:

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

Rationale:

You should not allow third party integrated applications to connect to your services unless there is a very clear value and you have robust security controls in place. While there are legitimate uses, attackers can grant access from breached accounts to third party applications to exfiltrate data from your tenancy without having to maintain the breached account.

Audit:

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

1. Click `Security and Compliance`.
2. Select `Admin Centers` and `Azure Active Directory`.
3. Select `Users Settings`.
4. Verify `App Registrations` is set to `No`.

Remediation:

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

1. Click `Security and Compliance`.
2. Select `Admin Centers` and `Azure Active Directory`.
3. Select `Users Settings`.
4. Set `App Registrations` to `No`.

Default Value:

Yes

CIS Controls:

Version 7

18.4 Only Use Up-to-date And Trusted Third-Party Components

Only use up-to-date and trusted third-party components for the software developed by the organization.

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

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

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

Remediation:

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

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

Default Value:

On

3 Data Management

3.1 (L2) Ensure the customer lockbox feature is enabled (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

1. Browse to https://portal.office.com/AdminPortal/Home?switchtomoderndefault=true#/settings/security.
2. Click `Edit` next to `Customer Lockbox`.
3. Check that the value of `Require approval for all data access requests` is set to `On`.

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

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

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

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

Remediation:

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

1. Browse to https://portal.office.com/AdminPortal/Home?switchtomoderndefault=true#/settings/security.
2. Click `Edit` next to `Customer Lockbox`.
3. Click the box next to `Require approval for all data access requests` to enable the feature and then click `Save`.

Default Value:

Disabled

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

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

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

1. Select `Security and Compliance`.
2. Select `Data Governance` and then `Retention`.
3. Click 'Labels'.
4. Ensure Labels exist.

Remediation:

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

1. Select `Security and Compliance`.
2. Select `Data Governance` and then `Retention`.
3. Select 'Labels'.
4. Click `Create` to create a label.

References:

1. https://msdn.microsoft.com/en-us/library/mt718319.aspx

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

Profile Applicability:

- Level 2

Description:

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

Rationale:

You should not allow your users to communicate with Skype users outside your organization. While there are legitimate, productivity-improving scenarios for this, it also represents a potential security threat because those external users will be able to interact with your users over Skype for Business. Attackers may be able to pretend to be someone your user knows and then send malicious links or attachments, resulting in an account breach or leaked information.

Audit:

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

1. Select `Admin Centers` and `Teams and Skype`.
2. Select `Org Wide Settings` and `External Access`.
3. Verify `External Access` and `Users can communicate with external Skype users` are set to `Off`.

Remediation:

To disable Skype access with external users, use the Microsoft 365 Admin Center:

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

Default Value:

On

CIS Controls:

Version 7

12.4 Deny Communication over Unauthorized Ports

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

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

1. Select `Security and Compliance`.
2. Select `Data loss prevention`.
3. Click `Policy`.
4. Click `Create a policy`.

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

1. Login to Microsoft 365 SecureScore portal (https://securescore.microsoft.com) using admin permissions (global admin or a custom admin role) for an Office 365 Enterprise, Microsoft 365 Business, or Office 365 Business Premium subscription.
2. Click on `Apply Data Loss Prevention policies` policy to check customer lockbox feature.
3. Check the number of data loss prevention policy applied

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

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

Remediation:

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

1. Select `Security and Compliance`.
2. Select `Data loss prevention`.

3. Click `Policy`.
4. Click `Create a policy`.

CIS Controls:

Version 7

13 Data Protection
Data Protection

4 Email Security / Exchange Online

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

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

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

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

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

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

Remediation:

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

1. Navigate to the Exchange Admin Center and click `Protection` > `Malware Filter`.

2. Edit the `Default` profile.
3. Click on the Edit tab under `Settings`. Ensure that the `Common Attachment Types Filter` has the value of `On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).`

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

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

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

Default Value:

off

References:

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

CIS Controls:

Version 7

8.1 Utilize Centrally Managed Anti-malware Software
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

4.2 (L1) Ensure Exchange Online Spam Policies are set correctly (Scored)

Profile Applicability:

- Level 1

Description:

You should set your Exchange Online Spam Policies to copy emails and notify someone when a sender in your tenant has been blocked for sending spam emails.

Rationale:

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

Audit:

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

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

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

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

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

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

Remediation:

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

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

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

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

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

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

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

Default Value:

disabled

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

To verify the mail transport rules do not forward email to external domains, use the Microsoft 365 Admin Center:

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

Remediation:

To alter the mail transport rules so they do not forward email to external domains, use the Microsoft 365 Admin Center:

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

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

Whitelisting domains in transport rules bypasses regular malware and phishing scanning, which can enable an attacker to launch attacks against your users from a safe haven domain.

Audit:

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

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

Remediation:

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

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

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

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

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

To verify the Client Rules Forwarding Block is enabled, use the Microsoft 365 Admin Center:

1. Go to `Exchange`.
2. Select `Rules`.
3. Verify that 'Client Rules To External Block' exists.

Remediation:

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

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

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.6 (L2) Ensure the Advanced Threat Protection Safe Links policy is enabled (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

1. Click `Security & Compliance` to open the Security & Compliance portal.
2. Navigate to `Threat management` > `Policy` > `ATP Safe Links`.
3. Under `Policies that apply to specific recipients`, verify that at least one policy exists and click `Edit`.
4. Select `Settings`.
5. Verify `Select the action for unknown potentially malicious URLs in messages` is set to `On`.
6. Verify that at least both `Use safe attachments to scan downloadable content` and `Apply safe links to messages sent within the organization` are checked.

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

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

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

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

Remediation:

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

1. Click `Security & Compliance` to open the Security & Compliance portal.
2. Navigate to `Threat management` > `Policy` > `ATP Safe Links`.
3. Under `Policies that apply to specific recipients`, verify that at least one policy exists and click `Edit`, or create a new policy.
4. Select `Settings`.
5. Select `On` for `Select the action for unknown potentially malicious URLs in messages`.
6. Check `Use safe attachments to scan downloadable content`.
7. Check `Apply safe links to messages sent within the organization`.
8. Click `Save`.

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

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

```
$SafeLinksPolicy = Get-SafeLinksPolicy

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

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

Default Value:

disabled

References:

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

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.7 (L2) Ensure the Advanced Threat Protection Safe Attachments policy is enabled (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

1. Click `Security & Compliance` to open the Security & Compliance portal.
2. Navigate to `Threat management` > `Policy` > `ATP Safe Attach`.
3. Under `Policies that apply to specific recipients`, verify that at least one policy exists.

Remediation:

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

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

Impact:

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

Default Value:

disabled

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

4.8 (L2) Ensure basic authentication for Exchange Online is disabled (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

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

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

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

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

Remediation:

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

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

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

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

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

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

Impact:

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

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

Default Value:

false

References:

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

online?redirectSourcePath=%252fen-us%252farticle%252fdisable-basic-authentication-in-exchange-online-bba2059a-7242-41d0-bb3f-baaf7ec1abd7

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

16.3 Require Multi-factor Authentication
Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.

5 Auditing

5.1 (L1) Enable Microsoft 365 audit log search (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

1. Log in as an administrator.
2. Click `Security & Compliance`.
3. In the Security & Compliance Center, navigate to `Search & investigation` > `Audit log search`.
4. Verify that you are able to do searches (e.g. try searching for Activities as `Accessed file` and results should be displayed).

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

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

```
Set-AdminAuditLogConfig | Select-Object -ExpandProperty
UnifiedAuditLogIngestionEnabled
```

4. Verify the resulting value is `true`.

Remediation:

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

1. Log in as an administrator.
2. Click `Security & Compliance`.
3. In the Security & Compliance Center, navigate to `Search & investigation` > `Audit log search`.
4. Click `Turn on auditing` next to the information warning at the top.
5. Click `Yes` on the dialog box to confirm.

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

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

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

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

Default Value:

disabled

References:

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

CIS Controls:

Version 7

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

5.2 (L1) Enable mailbox auditing for all users (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

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

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

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

Remediation:

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

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

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

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

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

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

Default Value:

disabled

References:

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

CIS Controls:

Version 7

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

5.3 (L1) Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly (Not Scored)

Profile Applicability:

- Level 1

Description:

This report contains records of accounts that have had activity that could indicate they are compromised, such as accounts that have: -successfully signed in after multiple failures, which is an indication that the accounts have cracked passwords -signed in to your tenancy from a client IP address that has been recognized by Microsoft as an anonymous proxy IP address (such as a TOR network) -successful signins from users where two signins appeared to originate from different regions and the time between signins makes it impossible for the user to have traveled between those regions

Rationale:

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

Audit:

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

Remediation:

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

1. Go to portal.azure.com.
2. Click `Azure Active Directory`.
3. Select `Risky Sign-ins`.
4. Review by `Detection Type`.

References:

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

CIS Controls:

Version 7

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

5.4 (L2) Ensure the Application Usage report is reviewed at least weekly (Not Scored)

Profile Applicability:

- Level 2

Description:

You should review the Application Usage report at least weekly. This report includes a usage summary for all Software As A Service (SaaS) applications that are integrated with your directory.

Rationale:

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

Audit:

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

Remediation:

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

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

CIS Controls:

Version 7

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

5.5 (L1) Ensure the self-service password reset activity report is reviewed at least weekly (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

Remediation:

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

1. Go to portal.azure.com.
2. Go to 'Azure Active Directory'.
3. Click on 'Password Reset'.
4. Select 'Audit Logs'.
5. Review the list of users who have reset their passwords in the last seven days.

CIS Controls:

Version 7

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

5.6 (L1) Ensure user role group changes are reviewed at least weekly (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

Remediation:

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

1. Go to `Security and Compliance Center`.
2. Select `Search and Investigation` and then `Audit Log Search`.
3. Set `Activities` to `Added member to role`.
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

CIS Controls:

Version 7

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

5.7 (L1) Ensure mail forwarding rules are reviewed at least weekly (Not Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

Remediation:

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

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

To review mail forwarding rules, use the following Powershell script:
Uses the administrator user credential to export Mail forwarding rules, User Delegates and SMTP Forwarding policies to multiple csv files

```
import-module MSOnline

#Let's get us an admin cred!
$userCredential = Get-Credential

#This connects to Azure Active Directory
Connect-MsolService -Credential $userCredential

$ExoSession = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri  https://outlook.office365.com/powershell-liveid/ -Credential
$userCredential -Authentication Basic -AllowRedirection
Import-PSSession $ExoSession
```

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


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


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


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

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

CIS Controls:

Version 7

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

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

Remediation:

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

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

CIS Controls:

Version 7

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

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

While this report isn't strictly actionable, reviewing it will give you a sense of the overall volume of malware being targeted at your users, which may prompt you to adopt more aggressive malware mitigations.

Audit:

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

Remediation:

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

1. Select `Security and Compliance`.
2. Select `Report` and `Dashboard`.
3. Review the `Malware Detected in Email` report.

CIS Controls:

Version 7

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

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

Remediation:

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

1. Go to `Security and Compliance Center`.
2. Select `Search and Investigation` and then `Audit Log Search`.
3. Set `Activities` to `Added user`.
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

CIS Controls:

Version 7

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

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

Remediation:

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

1. Go to `Security and Compliance Center`.
2. Select `Search and Investigation` and then `Audit Log Search`.
3. Set `Initiated by (Actor)` to the name of a non-global admin.
4. Set `Start Date` and `End Date`.
5. Click `Search`.
6. Review.

CIS Controls:

Version 7

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

5.12 (L2) Enable Microsoft 365 Cloud App Security (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

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

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

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

1. Login to Microsoft 365 SecureScore portal (https://securescore.microsoft.com) using admin permissions (global admin or a custom admin role) for an Office 365 Enterprise, Microsoft 365 Business, or Office 365 Business Premium subscription.
2. Click on “Enable Cloud App Security Console” policy to see the status of the Microsoft 365 Cloud App Security console.

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

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

Remediation:

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

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

6 Storage

6.1 (L2) Ensure document sharing is being controlled by domains with whitelist or blacklist (Not Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

Attackers will often attempt to expose sensitive information to external entities through sharing, and restricting the domains that your users can share documents with will reduce that surface area.

Audit:

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

1. Select `Admin Centers` and `SharePoint`.
2. Click `Sharing`.
3. Confirm that `Limit external sharing using domains` is checked.
4. Verify that `Allow sharing only with users from these domains` or `Don't allow sharing with users from these blocked domains` is set correctly along with an accurate list of approved or disallowed domains.

Remediation:

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

1. Select `Admin Centers` and `SharePoint`.
2. Click `Sharing`.
3. Check `Limit external sharing using domains`.
4. Toggle `Allow sharing only with users from these domains` or `Don't allow sharing with users from these blocked domains`.
5. Enter list of approved or disallowed domains.

Default Value:

off

CIS Controls:

Version 7

13 Data Protection
Data Protection

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

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

1. Select `Admin Centers` and `SharePoint`.
2. Click `Sharing`.
3. Click `Anonymous access links expire in this many days`.
4. Confirm the number of days is set to the desired value, such as `30`.

Remediation:

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

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

Default Value:

off

CIS Controls:

Version 7

13 Data Protection

Data Protection

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Account / Authentication**		
1.1	(L1) Ensure multifactor authentication is enabled for all users in administrative roles (Scored)	☐	☐
1.2	(L2) Ensure multifactor authentication is enabled for all users in all roles (Scored)	☐	☐
1.3	(L1) Ensure that between two and four global admins are designated (Not Scored)	☐	☐
1.4	(L1) Ensure self-service password reset is enabled (Scored)	☐	☐
1.5	(L1) Ensure modern authentication for Exchange Online is enabled (Scored)	☐	☐
2	**Application Permissions**		
2.1	(L2) Ensure third party integrated applications are not allowed (Scored)	☐	☐
2.2	(L2) Ensure calendar details sharing with external users is disabled (Scored)	☐	☐
3	**Data Management**		
3.1	(L2) Ensure the customer lockbox feature is enabled (Not Scored)	☐	☐
3.2	(L2) Ensure SharePoint Online data classification policies are set up and used (Not Scored)	☐	☐
3.3	(L2) Ensure external domains are not allowed in Skype or Teams (Not Scored)	☐	☐
3.4	(L1) Ensure DLP policies are enabled (Scored)	☐	☐
4	**Email Security / Exchange Online**		
4.1	(L1) Ensure the Common Attachment Types Filter is enabled (Scored)	☐	☐
4.2	(L1) Ensure Exchange Online Spam Policies are set correctly (Scored)	☐	☐
4.3	(L1) Ensure mail transport rules do not forward email to external domains (Not Scored)	☐	☐
4.4	(L1) Ensure mail transport rules do not whitelist specific domains (Not Scored)	☐	☐
4.5	(L2) Ensure the Client Rules Forwarding Block is enabled (Scored)	☐	☐
4.6	(L2) Ensure the Advanced Threat Protection Safe Links policy is enabled (Not Scored)	☐	☐
4.7	(L2) Ensure the Advanced Threat Protection Safe Attachments policy is enabled (Not Scored)	☐	☐

4.8	(L2) Ensure basic authentication for Exchange Online is disabled (Not Scored)	□	□
5	**Auditing**		
5.1	(L1) Enable Microsoft 365 audit log search (Scored)	□	□
5.2	(L1) Enable mailbox auditing for all users (Scored)	□	□
5.3	(L1) Ensure the Azure AD 'Risky sign-ins' report is reviewed at least weekly (Not Scored)	□	□
5.4	(L2) Ensure the Application Usage report is reviewed at least weekly (Not Scored)	□	□
5.5	(L1) Ensure the self-service password reset activity report is reviewed at least weekly (Not Scored)	□	□
5.6	(L1) Ensure user role group changes are reviewed at least weekly (Not Scored)	□	□
5.7	(L1) Ensure mail forwarding rules are reviewed at least weekly (Not Scored)	□	□
5.8	(L1) Ensure the Mailbox Access by Non-Owners Report is reviewed at least biweekly (Not Scored)	□	□
5.9	(L1) Ensure the Malware Detections report is reviewed at least weekly (Not Scored)	□	□
5.10	(L1) Ensure the Account Provisioning Activity report is reviewed at least weekly (Not Scored)	□	□
5.11	(L1) Ensure non-global administrator role group assignments are reviewed at least weekly (Not Scored)	□	□
5.12	(L2) Enable Microsoft 365 Cloud App Security (Not Scored)	□	□
6	**Storage**		
6.1	(L2) Ensure document sharing is being controlled by domains with whitelist or blacklist (Not Scored)	□	□
6.2	(L1) Ensure expiration time for external sharing links is set (Scored)	□	□

Appendix: Change History

Date	Version	Changes for this version
12/6/2018	1.0.0	Initial Release