Microsoft 365 Defender

Microsoft 365 Minimum Viable Secure Configuration Baseline

Draft Version 0.1

October 2022
Cybersecurity and Infrastructure Security Agency
Secure Cloud Business Applications (SCuBA)

Record of Changes

No.	Date	Reference	A=Add
			M=Modify
			D=Delete
				Description of Change

V0.1	17 October 2022	Entire document	M	Initial Draft w/Edit

Microsoft 365
Minimum Viable Secure Configuration Baseline

Table of Contents

This page is intentionally blank.

Microsoft 365
Minimum Viable Secure Configuration Baseline

1. Introduction

Microsoft 365 Defender is a cloud-based enterprise defense suite that coordinates prevention, detection, investigation and response. This set of tools and features is used to detect many types of attacks.

This baseline focuses on the features of Defender for Office 365 and some settings are in fact configured in the Microsoft 365 compliance admin center. However, for simplicity, both the Microsoft 365 Defender and Microsoft 365 compliance admin center items are contained in this baseline.

Generally, use of Microsoft Defender is not required by the baselines of core Microsoft 365 products (Exchange Online, Teams, etc.); however, some of the controls in the core baselines require the use of a dedicated security tool, such as Defender. This baseline should not be considered a requirement to use Defender, but instead used as guidance for how these requirements could be met using Defender, should an agency elect to use Defender as their tool of choice.

In addition to these controls, agencies should consider using a Cloud Access Security Broker to secure their environments as they adopt zero trust principles.

1.1 *Assumptions*

The **License Requirements** sections of this document assume the organization is using a Microsoft 365 E3 or G3 license level. Therefore, only licenses not included in E3/G3 are listed.

1.2 *Resources*

License Compliance and Copyright
Portions of this document are adapted from documents in Microsoft's Microsoft 365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Source documents are linked throughout this document. The United States Government has adapted selections of these documents to develop innovative and scalable configuration standards to strengthen the security of widely used cloud-based software services.

2. Baseline

2.1 *Preset Security Profiles SHOULD NOT Be Used*

Microsoft Defender defines two preset security profiles: standard and strict. While most of the settings in this baseline mirror the settings of the standard profile, this baseline recommends against the use of preset profiles. Instead, it enumerates all relevant settings, as the preset security profiles are inflexible and take precedence over all other present policies.

2.1.1 Policy

- Preset security profiles SHOULD NOT be used.

2.1.2 Resources

- Recommended settings for EOP [Exchange Online Protection] and Microsoft Defender for Office 365 security | Microsoft Docs

2.1.3 License Requirements

- N/A

2.2 *Data Loss Prevention SHALL Be Enabled*

There are multiple ways to secure sensitive information, such as warning users, encryption, or blocking attempts to share. The agency's data loss prevention (DLP) policy will dictate what agency information is sensitive and how that information is handled.

2.2.1 Policy

- A custom policy SHALL be configured to protect personally identifiable information (PII) and sensitive information, as defined by the agency. At a minimum, credit card numbers, Taxpayer Identification Numbers (TIN), and Social Security Numbers (SSN) SHALL be blocked.
- The custom policy SHOULD be applied in Exchange, OneDrive, Teams Chat, and Microsoft Defender.
- The action for the DLP policy SHOULD be set to block sharing sensitive information with everyone when DLP conditions are met.
- Notifications to inform users and help educate them on the proper use of sensitive information SHOULD be enabled.
- A list of apps that are not allowed to access files protected by DLP policy SHOULD be defined.
- A list of browsers that are not allowed to access files protected by DLP policy SHOULD be defined.

2.2.2 Resources

- Plan for data loss prevention (DLP) | Microsoft Docs
- Data loss prevention in Exchange Online | Microsoft Docs
- Personally identifiable information (PII) | National Institute of Standards and Technology (NIST)
- Sensitive information | NIST

2.2.3 License Requirements

- DLP for Teams requires an E5 or G5 license. See Information Protection: Data Loss Prevention for Teams | Microsoft Docs for more information.
- DLP for Endpoint requires an E5 or G5 license. See Get started with Endpoint data loss prevention - Microsoft Purview (compliance) | Microsoft Docs for more information.

2.2.4 Implementation

1. Sign in to the Microsoft 365 compliance admin center.
2. Under **Solutions**, select **Data loss prevention**.
3. Select **Policies** from the top of the page.
4. Select **Default Office 365 DLP policy**.
5. Select **Edit policy**.
6. Edit the name and description of the policy if desired, then click **Next**.
7. Under **Locations to apply the policy**, set **Status** to **On** for all products except Power BI (preview).
8. Click **Create rule**. Assign the rule an appropriate name and description.
9. Click **Add condition**, then **Content contains**.
10. Click **Add**, then **Sensitive info types**.
11. Create policies that protect information that is sensitive to the agency. At a minimum, the agency should protect:
    a. Credit card numbers.
    b. U.S. Individual Taxpayer Identification Numbers (TIN).
    c. U.S. Social Security Numbers (SSN).
    d. All agency defined PII and sensitive information.
12. Click **Add**.
13. Under **Actions**, click **Add an action**.
14. Click **Restrict access of encrypt the content in Microsoft 365 locations**.
15. Check **Restrict Access or encrypt the content in Microsoft 365 locations**.
16. Select **Block Everyone**.
17. Turn on **Use notifications to inform your users and help educate them on the proper use of sensitive info**.
18. Click **Save**, then **Next**.
19. Select **Turn it on right away**, then click **Next**.
20. Click **Submit**.
21. Go to **Endpoint DLP Settings.**
    a. Go to **Unallowed Apps.**
    b. Click **Add** or **Edit Unallowed Apps.**
    c. Enter an app and executable name to disallow said app from accessing protected files and to log the incident.
    d. Return and click **Unallowed Bluetooth Apps**.
    e. Enter an app and executable name to disallow said app from accessing protected files and to log the incident.

f. Return and click **Browser and domain restrictions to sensitive data**.

g. Under **Unallowed Browsers**, enter and select needed browsers to prevent that browser from accessing protected files

h. Switch **Always audit file activity for devices** to **ON**.

2.3 *Common Attachments Filter SHALL Be Enabled*

Filtering emails by attachment file types will flag emails as malware if the file type has been put in a predefined list of disallowed file types. The Common Attachments Filter also attempts to look beyond just the file extension and automatically detect the file type using true typing.

2.3.1 Policy

- The common attachments filter SHALL be enabled in the default anti-malware policy and in all existing policies.
- Disallowed file types SHALL be determined and set. At a minimum, click-to-run files SHOULD be blocked (e.g., .exe, .cmd, and .vbe).

2.3.2 Resources

- Configure anti-malware policies in EOP | Microsoft Docs
- Anti-malware policies | Microsoft Docs

2.3.3 License Requirements

- Requires Defender for Office 365 Plan 1 or 2. These are included with E5 and G5 and are available as add-ons for E3 and G3.

2.3.4 Implementation

To enable common attachments filter in the default policy:

1. Sign in to Microsoft 365 Defender.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies**.
4. Under **Policies**, select **Anti-malware**.
5. Select the **Default (Default)** policy.
6. Click **Edit protection settings.**
7. Check **Enable the common attachments filter**.
8. Click **Customize file types** as needed.
9. Click **Save**.

To create a new, custom policy, follow the instructions on Use the Microsoft 365 Defender portal to create anti-malware policies.

2.4 *Zero-Hour Auto Purge for Malware SHOULD Be Enabled*

This setting determines whether emails can be quarantined automatically after delivery to a user’s mailbox (e.g., in the case of a match with an updated malware classification rule).

2.4.1 Policy

- Zero-hour auto purge (ZAP) for malware SHOULD be enabled in the default anti-malware policy and in all existing custom policies.

2.4.2 Resources

- Configure anti-malware policies in EOP | Microsoft Docs
- Anti-malware policies | Microsoft Docs

2.4.3 License Requirements

- Requires Defender for Office 365 Plan 1 or 2. These are included with E5 and G5 and are available as add-ons for E3 and G3.

2.4.4 Implementation

To enable ZAP:

1. Sign in to Microsoft 365 Defender.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies**.
4. Under **Policies**, select **Anti-malware**.
5. Select the **Default (Default)** policy.
6. Click **Edit protection settings**.
7. Check **Enable zero-hour auto purge for malware (Recommended)**.
8. Click **Save**.

2.5 *Phishing Protections SHOULD Be Enabled*

There are multiple ways to protect against phishing, including impersonation protection, mailbox intelligence and safety tips. Impersonation protection checks incoming emails to see if the sender address is similar to the users or domains on an agency-defined list. If the sender address is significantly similar, as to indicate an impersonation attempt, the email is quarantined. Mailbox intelligence is an artificial intelligence (AI)-based tool for identifying potential impersonation attempts.

2.5.1 Policy

- User impersonation protection SHOULD be enabled for key agency leaders.
- Domain impersonation protection SHOULD be enabled for domains owned by the agency.
- Domain impersonation protection SHOULD be added for frequent partners.
- Trusted senders and domains MAY be added in the event of false positives.
- Intelligence for impersonation protection SHALL be enabled.
- Message action SHALL be set to quarantine if the message is detected as impersonated.

- Mail classified as spoofed SHALL be quarantined.
- All safety tips SHALL be enabled, including:
  - first contact.
  - user impersonation.
  - domain impersonation.
  - user impersonation unusual characters.
  - "?" for unauthenticated senders for spoof.
  - "via" tag.
- The above configurations SHALL be set in the default policy and SHOULD be set in all existing custom policies.

2.5.2 Resources

- Configure anti-phishing policies in EOP | Microsoft Docs
- EOP anti-phishing policy settings | Microsoft Docs

2.5.3 License Requirements

- Impersonation protection and advanced phishing thresholds require Defender for Office 365 Plan 1 or 2. These are included with E5 and G5 and are available as add-ons for E3 and G3. As of September 1, 2022, anti-phishing for user and domain impersonation and spoof intelligence are not yet available in GCC High [Government Community] and DoD [Department of Defense] (see Platform features | Microsoft Docs for current offerings).

2.5.4 Implementation

1. Sign in to Microsoft 365 Defender.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies**.
4. Under **Policies**, select **Anti-phishing**.
5. Select the **Office365 AntiPhish Default (Default)** policy.
6. Click **Edit protection settings**.
7. Check **Enable users to protect**.
8. Click **Manage sender(s)**, then add users that merit impersonation protection.
9. Check **Enable domains to protect**.
10. Check **Include domains I own**.
11. Check **Include custom domains**.
12. Click **Manage custom domains(s)** to add the domains of frequent partners.
13. Check **Enable mailbox intelligence (Recommended)**.
14. Check **Enable Intelligence for impersonation protection (Recommended)**.

15. Click **Save**.
16. Click **Edit actions**.
17. Set **If message is detected as an impersonated user** to **Quarantine the message**.
18. Set **If message is detected as an impersonated domain** to **Quarantine the message**.
19. Set **If Mailbox Intelligence detects an impersonated user** to **Quarantine the message**.
20. Set **If message is detected as spoof** to **Quarantine the message**.
21. Under **Safety tips & indicators**, check:
    a. **Show first contact safety tip (Recommended).**
    b. **Show user impersonation safety tip.**
    c. **Show domain impersonation safety tip.**
    d. **Show user impersonation unusual characters safety tip.**
    e. **Show (?) for unauthenticated senders for spoof.**
    f. **Show "via" tag.**
22. Click **Save**.

2.6 *Inbound Anti-Spam Protections SHALL Be Enabled*

There are several features that protect against inbound spam: bulk compliant level, quarantines, safety tips, and zero-hour auto purge.

2.6.1 Policy

- The bulk complaint level (BCL) threshold SHOULD be set to six or lower.
- Spam and high confidence spam SHALL be moved to either the junk email folder or the quarantine folder.
- Phishing and high confidence phishing SHALL be quarantined.
- Bulk email SHOULD be moved to either the junk email folder or the quarantine folder.
- Spam in quarantine SHOULD be retained for at least 30 days.
- Spam safety tips SHOULD be turned on.
- Zero-hour auto purge (ZAP) SHALL be enabled for both phishing and spam messages.
- Allowed senders MAY be added, but allowed domains SHALL NOT be added.
- The previously listed configurations SHALL be set in the default policy and SHOULD be set in all existing custom policies.

2.6.2 Resources

- Bulk complaint level (BCL) in EOP | Microsoft Docs
- EOP anti-spam policy settings | Microsoft Docs

- Configure anti-spam policies in EOP | Microsoft Docs

2.6.3 License Requirements

- N/A

2.6.4 Implementation

1. Sign in to Microsoft 365 Defender.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies**.
4. Under Policies, select **Anti-spam**.
5. Select **Anti-spam inbound policy (Default)**.
6. Under **Bulk email threshold & spam properties**, click **Edit spam threshold and properties**.
7. Set **Bulk email threshold** to six or lower.
8. Click **Save**.
9. Under **Actions**, click **Edit actions**.
10. In the **Message actions** section:
    a. For **Spam, High confidence spam**, and **Bulk**, set the action to either **Move message to Junk Email folder** or **Quarantine message**.
    b. Set the action for both **Phishing** and **High confidence phishing** to **Quarantine message**.
    c. Set **Retain spam in quarantine for this many days** to “30.”
    d. Check **Enable spam safety tips**.
    e. Check **Enable zero-hour auto purge (ZAP)**, **Enable for phishing messages,** and **Enable for spam messages**.
11. Click **Save.**

2.7 *Safe Link Policies SHOULD Be Enabled*

When enabled, URLs in emails are rewritten by prepending

https://*.safelinks.protection.outlook.com/?url=

to the original URL. This change can only be seen by either clicking the URL or copying and pasting it; the end-user, even when hovering over the URL in their email, will still only see the original URL. By prepending the safe links URL, Microsoft can proxy the initial URL through their scanning service. Their proxy can perform the following:

- Compare the URL with a block list.
- Compare the URL with a list of know malicious sites.
- If the URL points to a downloadable file, apply real-time file scanning.

If all checks pass, the user is redirected to the original URL.

2.7.1 Policy

- The Safe Links Policy SHALL include all agency domains—and by extension—all users.
- URL rewriting and malicious link click checking SHALL be enabled.
- Malicious link click checking SHALL be enabled with Microsoft Teams.
- Real-time suspicious URL and file-link scanning SHALL be enabled.
- URLs SHALL be scanned completely before message delivery.
- Internal agency email messages SHALL have safe links enabled.
- User click tracking SHALL be enabled.
- Safe Links in Office 365 apps SHALL be turned on.
- Users SHALL NOT be enabled to click through to the original URL.

2.7.2 Resources

- Safe Links in Microsoft Defender for Office 365 | Microsoft Docs
- Set up Safe Links policies in Microsoft Defender for Office 365 | Microsoft Docs

2.7.3 License Requirements

- Requires Defender for Office 365 Plan 1 or 2. These are included with E5 and G5 and are available as add-ons for E3 and G3.

2.7.4 Implementation

For more information about recommended Safe Links settings, see Safe Links settings.

1. Sign in to Microsoft 365 Defender.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies**.
4. Under **Policies**, select **Safe Links**.
5. Create a Safe Links Policy.
   a. Assign the new policy an appropriate name and description.
   b. Include all tenant domains. All users under those domains will be added.
   c. On the **URL & click protection settings** page:
      i. Select **On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.**
      ii. Select **Apply Safe Links to email messages sent within the organization.**
      iii. Select **Apply real-time URL scanning for suspicious links and links that point to files.**
      iv. Select **Wait for URL scanning to complete before delivering the message.**
   d. On the **URL & click protection settings** page, under **Teams**, select **On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten.**

e. On the **URL & click protection settings** page, under **Office 365 Apps**, select **On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office Apps. URLs are not rewritten.**

f. On the **URL & click protection settings** page, under **Click protection settings**:

i. Select **Track User Clicks.**

ii. Do not select **Let users click through to the original URL**.

g. Review the new policy, then click **Submit.**

2.8 *Safe Attachments SHALL Be Enabled*

The Safe Attachments will scan messages for attachments with malicious content. It routes all messages and attachments that do not have a virus/malware signature to a special environment. The process then uses machine learning and analysis techniques to detect malicious intent. Enabling this feature may slow down message delivery to the user due to the scanning.

2.8.1 Policy

- At least one Safe Attachments Policy SHALL include all agency domains—and by extension—all users.
- The action for malware in email attachments SHALL be set to block.
- Redirect emails with detected attachments to an agency-specified email SHOULD be enabled.
- Safe attachments SHOULD be enabled for SharePoint, OneDrive, and Microsoft Teams.

2.8.2 Resources

- Safe Attachments in Microsoft Defender for Office 365 | Microsoft Docs
- Safe Attachments Policy Settings | Microsoft Docs
- Use the Microsoft 365 Defender portal to create Safe Attachments policies | Microsoft Docs
- Turn on Safe Attachments for SharePoint, OneDrive, and Microsoft Teams | Microsoft Docs

2.8.3 License Requirements

- Requires Defender for Office 365 Plan 1 or 2. These are included with E5 and G5 and are available as add-ons for E3 and G3.

2.8.4 Implementation

To configure safe attachments for Exchange Online, follow the instructions listed on Use the Microsoft 365 Defender portal to create Safe Attachments policies.

1. Sign in to Microsoft 365 Defender.
2. Under **Email & collaboration**, select **Policies & rules**.

3. Select **Threat policies.**
4. Under **Policies**, select **Safe Attachments.**
5. Click **Create** to start a new policy.
6. Give the new policy an appropriate name and description.
7. Under domains, enter all agency tenant domains. All users under these domains will be added to the policy.
8. Under **Safe Attachments unknown malware response**, select **Block**.
9. Set the **Quarantine policy** to **AdminOnlyAccessPolicy.**
10. Click **Next**, then **Submit.**

To enable Safe Attachments for SharePoint, OneDrive, and Microsoft Teams, follow the instructions listed at Turn on Safe Attachments for SharePoint, OneDrive, and Microsoft Teams | Microsoft Docs.

1. Sign in to Microsoft 365 Defender.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies.**
4. Under **Policies**, select **Safe Attachments**.
5. Select **Global settings.**
6. Set **Turn on Defender for Office 365 for SharePoint, OneDrive, and Microsoft Teams** to on.

2.9 *Alerts SHALL Be Enabled*

There are several pre-built alert policies available pertaining to various apps in the Microsoft 365 suite. These alerts give admins better real-time insight into possible security incidents.

2.9.1 Policy

- At a minimum, the alerts required by the *Exchange Online Minimum Viable Secure Configuration Baseline* SHALL be enabled.
- The alerts SHOULD be sent to a monitored address or incorporated into a SIEM.

2.9.2 Resources

- Alert policies in Microsoft 365 | Microsoft Docs

2.9.3 License Requirements

- N/A

2.9.4 Implementation

1. Sign in to Microsoft 365 Defender.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Alert Policy.**
4. Click the policy name.

a. Ensure **Status** is set to **On**.

b. Ensure **Email recipients** includes at least one monitored address.

2.10 *Audit Logging SHALL Be Enabled*

To view data in threat protection reports, email security reports, and Explorer, audit logging must be turned on.

By default, Microsoft retains the audit logs for only 90 days. Activity by users with E5 licenses is logged for one year. However, per Office of Management and Budget (OMB) M-21-31, Microsoft audit logs are to be retained for at least 12 months in active storage and an additional 18 months in cold storage. This can be accomplished either by offloading the logs out of the cloud environment or natively through Microsoft by creating an audit log retention policy.

2.10.1 Policy

- Audit logging SHALL be enabled.
- Advanced audit SHALL be enabled.
- Audit logs SHALL be maintained for at least the minimum duration dictated by OMB M-21-31.

2.10.2 Resources

- OMB M-21-31 | Office of Management and Budget
- Turn auditing on or off | Microsoft Docs
- Create an audit log retention policy | Microsoft Docs
- Search the audit log in the compliance center | Microsoft Docs
- Audited Activities | Microsoft Docs

2.10.3 License Requirements

- Advanced audit capabilities, including the creation of a custom audit log retention policy, requires E5/G5 licenses or E3/G3 licenses with add-on compliance licenses.
- Additionally, maintaining logs in the Microsoft 365 environment for longer than one year requires an add-on license. For more information, see Licensing requirements | Microsoft Docs.

2.10.4 Implementation

Auditing can be enabled from the Microsoft 365 compliance admin center and the Exchange Online PowerShell. Follow the instructions listed on Turn on auditing.

1. Sign in to the Microsoft 365 compliance admin center.
2. Under **Solutions**, select **Audit**.
3. If auditing is not enabled, a banner displays and prompts that the user and admin activity start being recorded.
4. Click the **Start recording user and admin activity banner**.

To set up advanced audit, see Set up Advanced Audit in Microsoft 365 | Microsoft Docs.

To create an audit retention policy, follow the instructions listed on Create an audit log retention policy.

To check the current logging status via PowerShell:

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

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

To enable logging via PowerShell:

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

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

3. Acknowledgements

In addition to acknowledging the important contributions of a diverse team of Cybersecurity and Infrastructure Security Agency (CISA) experts, CISA thanks the following federal agencies and private sector organizations that provided input during the development of the Secure Business Cloud Application's security configuration baselines in response to Section 3 of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*:

- Consumer Financial Protection Bureau (CFPB)
- Department of the Interior (DOI)
- National Aeronautics and Space Administration (NASA)
- Sandia National Laboratories (Sandia)
- U.S. Census Bureau (USCB)
- U.S. Geological Survey (USGS)
- U.S. Office of Personnel Management (OPM)
- U.S. Small Business Administration (SBA)

The cross-agency collaboration and partnerships developed during this initiative serve as an example for solving complex problems faced by the federal government.

Cybersecurity Innovation Tiger Team (CITT) Leadership
Beau Houser (USCB), Sanjay Gupta (SBA), Michael Witt (NASA), James Saunders (OPM), Han Lin (Sandia), Andrew Havely (DOI).

CITT Authors
Trafenia Salzman (SBA), Benjamin McChesney (OPM), Robert Collier (USCB), Matthew Snitchler (Sandia), Darryl Purdy (USCB), Brandon Frankens (NASA), Brandon Goss (NASA), Nicole Bogeajis (DOI/USGS), Kevin Kelly (DOI), Adnan Ehsan (CFPB), Michael Griffin (CFPB), Vincent Urias (Sandia), Angela Calabaza (Sandia).

CITT Contributors
Dr. Mukesh Rohatgi (MITRE), Lee Szilagyi (MITRE), Nanda Katikaneni (MITRE), Ted Kolovos (MITRE), Thomas Comeau (MITRE), Karen Caraway (MITRE), Jackie Whieldon (MITRE), Jeanne Firey (MITRE), Kenneth Myers (General Services Administration).