EXCHANGE ONLINE

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.0

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

REVISION HISTORY

Version	Summary of revisions	Edited By	Date
1.0	• Creation	CISA	08/13/2023

CONTENTS

1. CISA M365 SECURITY CONFIGURATION BASELINE FOR EXCHANGE ONLINE

Microsoft 365 (M365) Exchange Online is a cloud-based messaging platform that gives users easy access to their email and supports organizational meetings, contacts, and calendars. This Secure Configuration Baseline (SCB) provides specific policies to strengthen Exchange Online security.

Many admin controls for Exchange Online are found in the **Exchange admin center**. However, several of the security features for Exchange Online are shared between Microsoft products and are configured in either the **Microsoft 365 Defender portal** or **Microsoft Purview compliance portal**. Generally speaking, the use of Microsoft Defender is not strictly required for this baseline. When noted, alternative products may be used in lieu of Defender, on the condition that they fulfill these required baseline settings.

The Secure Cloud Business Applications (SCuBA) project run by the Cybersecurity and Infrastructure Security Agency (CISA) provides guidance and capabilities to secure federal civilian executive branch (FCEB) agencies' cloud business application environments and protect federal information that is created, accessed, shared, and stored in those environments.

The CISA SCuBA SCBs for M365 help secure federal information assets stored within M365 cloud business application environments through consistent, effective, and manageable security configurations. CISA created baselines tailored to the federal government's threats and risk tolerance with the knowledge that every organization has different threat models and risk tolerance. Non-governmental organizations may also find value in applying these baselines to reduce risks.

The information in this document is provided "as is" for INFORMATIONAL PURPOSES ONLY. CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial entities or commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA. This document does not address, ensure compliance with, or supersede any law, regulation, or other authority. Entities are responsible for complying with any recordkeeping, privacy, and other laws that may apply to the use of technology. This document is not intended to, and does not, create any right or benefit for anyone against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

1.1 LICENSE COMPLIANCE AND COPYRIGHT

Portions of this document are adapted from documents in Microsoft's M365 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. Sources 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.

1.2 ASSUMPTIONS

The **License Requirements** sections of this document assume the organization is using an M365 E3 or G3 license level at a minimum. Therefore, only licenses not included in E3/G3 are listed.

1.3 KEY TERMINOLOGY

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. BASELINE POLICIES

2.1 AUTOMATIC FORWARDING TO EXTERNAL DOMAINS

This control is intended to prevent bad actors from using client-side forwarding rules to exfiltrate data to external recipients.

2.2 POLICIES

2.2.1 MS.EXO.1.1v1

Automatic forwarding to external domains SHALL be disabled.

- *Rationale:* Adversaries can use automatic forwarding to gain persistent access to a victim's email. Disabling forwarding to external domains prevents this technique when the adversary is external to the organization but does not impede legitimate internal forwarding.
- *Last modified:* June 2023

2.3 RESOURCES

- Reducing or increasing information flow to another company | Microsoft Learn

2.4 LICENSE REQUIREMENTS

- N/A

2.5 IMPLEMENTATION

2.5.1 MS.EXO.1.1v1 Instructions

To disallow automatic forwarding to external domains:

1. Sign in to the **Exchange admin center**.
2. Select **Mail flow**, then **Remote domains**.
3. Select **Default**.
4. Under Email reply types, select **Edit reply types**.
5. Clear the checkbox next to **Allow automatic forwarding**, then click **Save**.
6. Return to **Remote domains** and repeat steps 4 and 5 for each additional remote domain in the list.

3. SENDER POLICY FRAMEWORK

The Sender Policy Framework (SPF) is a mechanism allowing domain administrators to specify which IP addresses are explicitly approved to send email on behalf of the domain, facilitating detection of spoofed emails. SPF is not configured through the Exchange admin center, but rather via Domain Name System (DNS) records hosted by the agency's domain. Thus, the exact steps needed to set up SPF vary from agency to agency, but Microsoft's documentation provides some helpful starting points.

3.1 POLICIES

3.1.1 MS.EXO.2.1v1

A list of approved IP addresses for sending mail SHALL be maintained.

- *Rationale:* Failing to maintain an accurate list of authorized IP addresses may result in spoofed email messages or failure to deliver legitimate messages when SPF is enabled. Maintaining such a list helps ensure unauthorized servers sending spoofed messages can be detected and permits message delivery from legitimate senders.

- *Last modified*: June 2023

3.1.2 MS.EXO.2.2v1

An SPF policy SHALL be published for each domain, designating only these addresses as approved senders.

- *Rationale:* An adversary may modify the FROM field of an email such that it appears to be a legitimate email sent by an agency, facilitating phishing attacks. Publishing an SPF policy for each agency domain mitigates forged FROM fields by providing a means for recipients to detect emails spoofed in this way. SPF is required for FCEB departments and agencies by Binding Operational Directive (BOD) 18-01, "Enhance Email and Web Security."
- *Last modified:* June 2023

3.2 RESOURCES

- Binding Operational Directive 18-01 – Enhance Email and Web Security | DHS
- Trustworthy Email | NIST 800-177 Rev. 1
- Set up SPF to help prevent spoofing | Microsoft Learn
- How Microsoft 365 uses Sender Policy Framework (SPF) to prevent spoofing | Microsoft Learn

3.3 LICENSE REQUIREMENTS

- N/A

3.4 IMPLEMENTATION

3.4.1 MS.EXO.2.1v1 Instructions

Identify any approved senders specific to your agency. Additionally, see External DNS records required for SPF for inclusions required for Microsoft to send email on behalf of your domain.

3.4.2 MS.EXO.2.2v1 Instructions

SPF is not configured through the Exchange admin center, but rather via DNS records hosted by the agency's domain. Thus, the exact steps needed to set up SPF varies from agency to agency. See Add or edit an SPF TXT record to help prevent email spam (Outlook, Exchange Online) | Microsoft Learn for more details.

To test your SPF configuration, consider using a web-based tool, such as those listed under How can I validate SPF records for my domain? | Microsoft Learn. Additionally, SPF records can be requested using the PowerShell tool **Resolve-DnsName**. For example:

```
Resolve-DnsName example.onmicrosoft.com txt
```

If SPF is configured, you will see a response resembling v=spf1 include:spf.protection.outlook.com -all returned; though by necessity, the contents of the SPF policy may vary by agency. In this example, the SPF policy indicates the IP addresses listed by the policy for "spf.protection.outlook.com" are the only approved senders for "example.onmicrosoft.com." These IPs can be determined via an additional SPF lookup, this time for "spf.protection.outlook.com." Ensure the IP addresses listed as approved senders for your domain are those identified for MS.EXO.2.1v1. See SPF TXT record syntax for Microsoft 365 | Microsoft Learn for a more in-depth discussion of SPF record syntax.

4. DOMAINKEYS IDENTIFIED MAIL

DomainKeys Identified Mail (DKIM) allows digital signatures to be added to email messages in the message header, providing a layer of both authenticity and integrity to emails. As with SPF, DKIM relies on DNS records; thus, its deployment depends on how an agency manages its DNS. Exchange Online Protection (EOP) features include DKIM signing capabilities.

4.1 POLICIES

4.1.1 MS.EXO.3.1v1

DKIM SHOULD be enabled for all domains.

- *Rationale:* An adversary may modify the FROM field of an email such that it appears to be a legitimate email sent by an agency, facilitating phishing attacks. Enabling DKIM is another means for recipients to detect spoofed emails and verify the integrity of email content.
- *Last modified:* June 2023

4.2 RESOURCES

- Binding Operational Directive 18-01 – Enhance Email and Web Security | DHS
- Trustworthy Email | NIST 800-177 Rev. 1
- Use DKIM to validate outbound email sent from your custom domain | Microsoft Learn
- Support for validation of DKIM signed messages | Microsoft Learn
- What is EOP? | Microsoft Learn

4.3 LICENSE REQUIREMENTS

- N/A

4.4 IMPLEMENTATION

4.1.1 MS.EXO.3.1v1 Instructions

To enable DKIM, follow the instructions listed on Steps to Create, enable and disable DKIM from Microsoft 365 Defender portal | Microsoft Learn.

5. DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE (DMARC)

Domain-based Message Authentication, Reporting, and Conformance (DMARC) works with SPF and DKIM to authenticate mail senders and helps ensure destination email systems can validate messages sent from your domain. DMARC helps receiving mail systems determine what to do with messages sent from your domain that fail SPF and DKIM checks.

5.1 POLICIES

5.1.1 MS.EXO.4.1v1

A DMARC policy SHALL be published for every second-level domain.

- *Rationale:* Without a DMARC policy available for each domain, recipients may improperly handle SPF and DKIM failures, possibly enabling spoofed emails to reach end users' mailboxes. Publishing DMARC records at the second-level domain protects the second-level domains and all subdomains.
- *Last modified:* June 2023

5.1.2 MS.EXO.4.2v1

The DMARC message rejection option SHALL be p=reject.

- *Rationale:* Of the three policy options (i.e., none, quarantine, and reject), reject provides the strongest protection. Reject is the level of protection required by BOD 18-01 for FCEB departments and agencies.
- *Last modified:* June 2023

5.1.3 MS.EXO.4.3v1

The DMARC point of contact for aggregate reports SHALL include reports@dmarc.cyber.dhs.gov.

- *Rationale:* Email spoofing attempts are not inherently visible to domain owners. DMARC provides a mechanism to receive reports of spoofing attempts. Including reports@dmarc.cyber.dhs.gov as a point of contact for these reports gives CISA insight into spoofing attempts and is required by BOD 18-01 for FCEB departments and agencies.
- *Last modified:* June 2023
- *Note:* Only FCEB departments and agencies should include this email address in their DMARC record.

5.1.4 MS.EXO.4.4v1

An agency point of contact SHOULD be included for aggregate and failure reports.

- *Rationale:* Email spoofing attempts are not inherently visible to domain owners. DMARC provides a mechanism to receive reports of spoofing attempts. Including an agency point of contact gives the agency insight into attempts to spoof their domains.
- *Last modified:* June 2023

5.2 RESOURCES

- Binding Operational Directive 18-01 - Enhance Email and Web Security | DHS
- Trustworthy Email | NIST 800-177 Rev. 1
- Domain-based Message Authentication, Reporting, and Conformance (DMARC) | RFC 7489
- Best practices for implementing DMARC in Office 365 | Microsoft Learn
- How Office 365 handles outbound email that fails DMARC | Microsoft Learn

5.3 LICENSE REQUIREMENTS

- N/A

5.4 IMPLEMENTATION

5.4.1 MS.EXO.4.1v1 Instructions

DMARC is not configured through the Exchange admin center, but rather via DNS records hosted by the agency's domain. As such, implementation varies depending on how an agency manages its DNS records. See Form the DMARC TXT record for your domain | Microsoft Learn for Microsoft guidance.

A DMARC record published at the second-level domain will protect all subdomains. In other words, a DMARC record published for example.com will protect both a.example.com and b.example.com, but a separate record would need to be published for c.example.gov.

To test your DMARC configuration, consider using one of many publicly available web-based tools. Additionally, DMARC records can be requested using the PowerShell tool Resolve-DnsName. For example:

```
Resolve-DnsName _dmarc.example.com txt
```

If DMARC is configured, a response resembling v=DMARC1; p=reject; pct=100; rua=mailto:reports@dmarc.cyber.dhs.gov, mailto:reports@example.com; ruf=mailto:reports@example.com will be returned, though by necessity, the contents of the record will vary by agency. In this example, the policy indicates all emails failing the SPF/DKIM checks are to be rejected and aggregate reports sent to reports@dmarc.cyber.dhs.gov and reports@example.com. Failure reports will be sent to reports@example.com.

5.4.2 MS.EXO.4.2v1 Instructions

See MS.EXO.1.1v1 instructions for an overview of how to publish **and** check a DMARC record. Ensure the record published includes p=reject.

5.4.3 MS.EXO.4.3v1 Instructions

See MS.EXO.1.1v1 instructions for an overview of how to publish and check a DMARC record. Ensure the record published includes reports@dmarc.cyber.dhs.gov as one of the emails for the RUA field.

5.4.4 MS.EXO.4.4v1 Instructions

See MS.EXO.1.1v1 instructions for an overview of how to publish and check a DMARC record. Ensure the record published includes:

- A point of contact specific to your agency in the RUA field.
- reports@dmarc.cyber.dhs.gov as one of the emails in the RUA field.
- One or more agency-defined points of contact in the RUF field.

6. SIMPLE MAIL TRANSFER PROTOCOL AUTHENTICATION

Modern email clients that connect to Exchange Online mailboxes—including Outlook, Outlook on the web, iOS Mail, and Outlook for iOS and Android—do not use Simple Mail Transfer Protocol Authentication (SMTP AUTH) to send email messages. SMTP AUTH is only needed for applications outside of Outlook that send email messages. Multifactor authentication (MFA) cannot be enforced while using SMTP Auth. Proceed with caution if SMTP Auth needs to be enabled for any use case.

6.1 POLICIES

6.1.1 MS.EXO.5.1v1

SMTP AUTH SHALL be disabled.

- *Rationale:* SMTP AUTH is not used or needed by modern email clients. Therefore, disabling it as the global default conforms to the principle of least functionality.
- *Last modified:* June 2023

6.2 RESOURCES

- Enable or disable authenticated client SMTP submission (SMTP AUTH) in Exchange Online | Microsoft Learn

6.3 LICENSE REQUIREMENTS

- N/A

6.4 IMPLEMENTATION

6.4.1 MS.EXO.5.1v1 Instructions

To disable SMTP AUTH for the organization:

1. Sign in to the **Exchange admin center**.
2. On the left-hand pane, select **Settings**; then from the Settings list, select **Mail Flow**.
3. Make sure the setting **Turn off SMTP AUTH protocol for your organization** is checked.

7. CALENDAR AND CONTACT SHARING

Exchange Online allows creation of sharing polices that soften default restrictions on contact and calendar details sharing. These policies should be enabled with caution and only after considering the following policies.

7.1 Policies

7.1.1 MS.EXO.6.1v1

Contact folders SHALL NOT be shared with all domains.

- *Rationale:* Contact folders may contain information that should not be shared by default with all domains. Disabling sharing with all domains closes an avenue for data exfiltration while still allowing for specific legitimate use as needed.
- *Last modified:* June 2023
- *Note:* Contact folders MAY be shared with specific domains.

7.1.2 MS.EXO.6.2v1

Calendar details SHALL NOT be shared with all domains.

- *Rationale:* Calendar details may contain information that should not be shared by default with all domains. Disabling sharing with all domains closes an avenue for data exfiltration while still allowing for legitimate use as needed.
- *Last modified:* June 2023
- *Note:* Calendar details MAY be shared with specific domains.

7.2 RESOURCES

- Sharing in Exchange Online | Microsoft Learn
- Organization relationships in Exchange Online | Microsoft Learn
- Sharing policies in Exchange Online | Microsoft Learn

7.3 LICENSE REQUIREMENTS

- N/A

7.4 IMPLEMENTATION

7.4.1 MS.EXO.6.1v1 Instructions

To restrict sharing with all domains:

1. Sign in to the **Exchange admin center**.
2. On the left-hand pane under **Organization**, select **Sharing**.
3. Select **Individual Sharing**.
4. For all existing policies, select the policy, then select **Manage domains.**
5. For all sharing rules under all existing policies, ensure **Sharing with all domains** is not selected.

7.4.2 MS.EXO.6.2v1 Instructions

To restrict calendar sharing with all domains:

1. Refer to step 5 in MS.EXO.6.1v1 instructions to implement this policy.

8. EXTERNAL SENDER WARNINGS

Mail flow rules allow incoming email modification such that email from external users can be easily identified (e.g., by prepending the subject line with “[External]”).

8.1 POLICIES

8.1.1 MS.EXO.7.1v1

External sender warnings SHALL be implemented.

- *Rationale:* Phishing is an ever-present threat. Alerting users when email originates from outside their organization can encourage them to exercise increased caution, especially if an email is one they expected from an internal sender.
- *Last modified:* June 2023

8.2 RESOURCES

- Mail flow rules (transport rules) in Exchange Online | Microsoft Learn
- Capacity Enhancement Guide: Counter-Phishing Recommendations for Federal Agencies | CISA
- Actions To Counter Email-Based Attacks On Election-Related Entities | CISA

8.3 LICENSE REQUIREMENTS

- N/A

8.4 IMPLEMENTATION

8.4.1 MS.EXO.7.1v1 Instructions

To create a mail flow rule to produce external sender warnings:

1. Sign in to the **Exchange admin center.**
2. Under **Mail flow**, select **Rules**.
3. Click the plus (**+**) button to create a new rule.
4. Select **Modify messages….**
5. Give the rule an appropriate name.
6. Under **Apply this rule if…**, select **The sender is external/internal.**
7. Under **select sender location**, select **Outside the organization**, then click **OK**.
8. Under **Do the following…**, select **Prepend the subject of the message with….**
9. Under **specify subject prefix**, enter a message such as “[External]” (without the quotation marks), then click **OK**.
10. Click **Next**.

11. Under **Choose a mode for this rule**, select **Enforce**.
12. Leave the **Severity** as **Not Specified**.
13. Leave the **Match sender address in message** as **Header** and click **Next**.
14. Click **Finish** and then **Done**.
15. The new rule will be disabled. Re-select the new rule to show its settings and slide the **Enable or disable rule** slider to the right until it shows as **Enabled**.

9. DATA LOSS PREVENTION SOLUTIONS

Data loss prevention (DLP) helps prevent both accidental leakage of sensitive information as well as intentional exfiltration of data. DLP forms an integral part of securing Microsoft Exchange Online. There are several commercial DLP solutions available that document support for M365. Microsoft itself offers DLP services, controlled within the Microsoft Purview compliance portal. Agencies may select any service that fits their needs and meets the requirements outlined in this baseline setting. The DLP solution selected by an agency should offer services comparable to those offered by Microsoft.

Though use of Microsoft's DLP solution is not strictly required, guidance for configuring Microsoft's DLP solution can be found in the following section of the CISA M365 Security Configuration Baseline for Defender for Office 365.

- Data Loss Prevention | CISA M365 Security Configuration Baseline for Defender for Office 365

9.1 POLICIES

9.1.1 MS.EXO.8.1v1

A DLP solution SHALL be used. The selected DLP solution SHOULD offer services comparable to the native DLP solution offered by Microsoft.

- *Rationale:* Users may inadvertently disclose sensitive information to unauthorized individuals. A capable DLP solution should detect the presence of sensitive information in Exchange Online and block access to authorized entities.
- *Last modified:* June 2023

9.1.2 MS.EXO.8.2v1

The DLP solution SHALL protect personally identifiable information (PII) and sensitive information, as defined by the agency. At a minimum, sharing credit card numbers, Taxpayer Identification Numbers (TIN), and Social Security numbers (SSN) via email SHALL be restricted.

- *Rationale:* Users may inadvertently share sensitive information with others who should not have access to it. DLP policies provide a way for agencies to detect and prevent unauthorized disclosures.
- *Last modified:* June 2023

9.2 RESOURCES

- None

9.3 LICENSE REQUIREMENTS

- N/A

9.4 IMPLEMENTATION

9.4.1 MS.EXO.8.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for DLP for additional guidance.

9.4.2 MS.EXO.8.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency is using Microsoft Defender, see the following implementation steps for protecting PII for additional guidance.

10. ATTACHMENT FILE TYPE

For some types of files (e.g., executable files), the dangers of allowing them to be sent via email outweigh any potential benefits. Some services, such as the Common Attachment Filter of Microsoft Defender, filter emails based on the attachment file types. Using Microsoft Defender for this purpose is not required. However, the solution selected by an agency should offer services comparable to those offered by Microsoft.

Though using Microsoft Defender's solution is not strictly required for this purpose, guidance for configuring the Common Attachment Filter in Microsoft Defender can be found in the follow section of the CISA M365 Security Configuration Baseline for Defender for Office 365.

- Preset Security Policies | CISA M365 Security Configuration Baseline for Defender for Office 365

10.1 POLICIES

10.1.1 MS.EXO.9.1v1

Emails SHALL be filtered by attachment file types. The selected filtering solution SHOULD offer services comparable to Microsoft Defender's Common Attachment Filter.

- *Rationale:* Malicious attachments often take the form of click-to-run files. Sharing high-risk file types, when necessary, is better left to a means other than email; the dangers of allowing them to be sent over email outweigh any potential benefits. Filtering email attachments based on file types can prevent spread of malware distributed via click-to-run email attachments.
- *Last modified:* June 2023

10.1.2 MS.EXO.9.2v1

The attachment filter SHOULD attempt to determine the true file type and assess the file extension.

- *Rationale:* Users can change a file extension at the end of a file name (e.g., notepad.exe to notepad.txt) to obscure the actual file type. Verifying the file type and checking that this matches the designated file extension can help detect instances where the file extension was changed.
- *Last modified:* June 2023

10.1.3 MS.EXO.9.3V1

Disallowed file types SHALL be determined and set. At a minimum, click-to-run files SHOULD be blocked (e.g., .exe, .cmd, and .vbe).

- *Rationale:* Malicious attachments often take the form of click-to-run files, though other file types can contain malicious content as well. As such, determining the full list of file types to block is left to each organization, to be made in accordance with their risk tolerance.
- *Last modified:* June 2023

10.2 RESOURCES

- None

10.3 LICENSE REQUIREMENTS

- N/A

10.4 IMPLEMENTATION

10.4.1 MS.EXO.9.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which include email filtering based on attachment file type.

10.4.2 MS.EXO.9.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which attempt to determine the true file type and assess the file extension.

10.4.3 MS.EXO.9.3v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which disallow click-to-run file types.

11. MALWARE SCANNING

Email messages may include attachments that contain malware. Therefore, email messages should be scanned for malware to prevent infections. Once malware has been identified, the scanner should drop or quarantine the associated messages. Because malware detections may be updated, it is also important that emails that were already delivered to users are also scanned and removed.

Using Microsoft Defender for this purpose is not required. However, the solution selected by an agency should offer services comparable to those offered by Microsoft. If the agency uses Microsoft Defender to implement malware scanning, see the following policies of the CISA M365 Security Configuration Baseline for Defender for Office 365 for additional guidance.

- MS.DEFENDER.1.2v1 | CISA M365 Security Configuration Baseline for Defender for Office 365
  - All users SHALL be added to Exchange Online Protection in either the standard or strict preset security policy.
- MS.DEFENDER.1.3v1 | CISA M365 Security Configuration Baseline for Defender for Office 365
  - All users SHALL be added to Defender for Office 365 Protection in either the standard or strict preset security policy.

11.1 POLICIES

11.1.1 MS.EXO.10.1v1

Emails SHALL be scanned for malware.

- *Rationale:* Email can be used as a mechanism for delivering malware. In many cases, malware can be detected through scanning, reducing the risk for end users.

- *Last modified:* June 2023

11.1.2 MS.EXO.10.2v1

Emails identified as containing malware SHALL be quarantined or dropped.

- *Rationale:* Email can be used as a mechanism for delivering malware. Preventing emails with known malware from reaching user mailboxes helps ensure users cannot interact with those emails.
- *Last modified:* June 2023

11.1.3 MS.EXO.10.3v1

Email scanning SHALL be capable of reviewing emails after delivery.

- *Rationale:* As known malware signatures are updated, it is possible for an email to be retroactively identified as containing malware after delivery. By scanning emails, the number of malware-infected in users' mailboxes can be reduced.
- *Last modified:* June 2023

11.2 RESOURCES

- None

11.3 LICENSE REQUIREMENTS

- N/A

11.4 IMPLEMENTATION

11.4.1 MS.EXO.10.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which include anti-malware protection.

11.4.2 MS.EXO.10.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which include anti-malware protection to quarantine malware in email.

11.4.3 MS.EXO.10.3v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which include zero-hour auto purge (ZAP) to retroactively detect malware in messages already delivered to mailboxes and removes them.

12. PHISHING PROTECTIONS

Several techniques exist for protecting against phishing attacks, including the following:

- Impersonation protection checks, wherein a tool compares the sender's address to the addresses of known senders to flag look-alike addresses, such as user@exmple.com and user@example.com.
- User warnings, such as displaying a notice the first time a user receives an email from a new sender.
- Artificial intelligence (AI)-based tools.

Any product meeting the requirements outlined in this baseline policy group may be used. If the agency uses Exchange Online Protection (EOP), which is included in all Microsoft 365 subscriptions containing Exchange Online mailboxes, see the following policy and section of the CISA M365 Security Configuration Baseline for Defender for Office 365.

- MS.DEFENDER.1.2v1 | CISA M365 Security Configuration Baseline for Defender for Office 365
  - All users SHALL be added to Exchange Online Protection in either the standard or strict preset security policy.

EOP alone does not support impersonation protection, but this is provided through Defender for Office 365. If using Defender for Office 365 for impersonation protection, see the following policy and section of the CISA M365 Security Configuration Baseline for Defender for Office 365.

- Impersonation Protection | CISA M365 Security Configuration Baseline for Defender for Office 365

12.1 POLICIES

12.1.1 MS.EXO.11.1v1

Impersonation protection checks SHOULD be used.

- *Rationale:* Users might not be able to reliably identify phishing emails, especially if the FROM address is nearly indistinguishable from that of a known entity. By automatically identifying senders who appear to be impersonating known senders, the risk of a successful phishing attempt can be reduced.
- *Last modified:* June 2023

12.1.2 MS.EXO.11.2v1

User warnings, comparable to the user safety tips included with EOP, SHOULD be displayed.

- *Rationale:* Many tasks are better suited for automated processes, such as identifying unusual characters in the FROM address or identifying a first-time sender. User warnings can handle these tasks, reducing the burden on end users and the risk of successful phishing attempts.
- *Last modified:* June 2023

12.1.3 MS.EXO.11.3v1

The phishing protection solution SHOULD include an AI-based phishing detection tool comparable to EOP Mailbox Intelligence.

- *Rationale:* Phishing attacks can result in unauthorized data disclosure and unauthorized access. Using AI-based phishing detection tools to improve the detection rate of phishing attempts helps reduce the risk of successful phishing attacks.
- *Last modified:* June 2023

12.2 RESOURCES

- None

12.3 LICENSE REQUIREMENTS

- If using Defender for Office 365 for impersonation protection and advanced phishing thresholds, Defender for Office 365 Plan 1 or 2 is required. These are included with E5 and G5 and are available as add-ons for E3 and G3. As of November 14, 2023, anti-phishing for user and domain impersonation and spoof intelligence are not yet available in M365 Government Community Cloud High (GCC High) and M365 Department of Defense (DOD). See Platform features | Microsoft Docs for current offerings.

12.4 IMPLEMENTATION

12.4.1 MS.EXO.11.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling impersonation protection.

12.4.2 MS.EXO.11.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which include user safety tips to warn users.

12.4.3 MS.EXO.11.3v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which include mailbox intelligence for detecting phishing attacks using AI.

13. IP ALLOW LISTS

Microsoft Defender supports creating IP allow lists intended to prevent blocking emails from *specific* senders. However, as a result, emails from these senders bypass important security mechanisms, such as spam filtering, SPF, DKIM, DMARC, and FROM address enforcement.

IP block lists block email from listed IP addresses. Although we have no specific guidance on which IP addresses to add, blocklists can be used to block mail from known spammers.

IP safe lists are dynamic lists of “known, good senders,” which Microsoft sources from various third-party subscriptions. As with senders in the allowlist, emails from these senders bypass important security mechanisms.

13.1 POLICIES

13.1.1 MS.EXO.12.1v1

IP allow lists SHOULD NOT be created.

- *Rationale:* Messages sent from IP addresses on an allowlist bypass important security mechanisms, including spam filtering and sender authentication checks. Avoiding use of IP allow lists prevents potential threats from circumventing security mechanisms.
- Last modified: June 2023

13.1.2 MS.EXO.12.2v1

Safelists SHOULD NOT be enabled.

- *Rationale:* Messages sent from allowed safelist addresses bypass important security mechanisms, including spam filtering and sender authentication checks. Avoiding use of safelists prevents potential threats from circumventing security mechanisms. While blocking all malicious senders is not feasible, blocking specific known malicious IP addresses may reduce the threat from specific senders.
- *Last modified:* June 2023
- *Note:* A connection filter MAY be implemented to create an IP block list.

13.2 RESOURCES

- Use the IP Allow List | Microsoft Learn
- Configure connection filtering | Microsoft Learn
- Use the Microsoft 365 Defender portal to modify the default connection filter policy | Microsoft Learn

13.3 LICENSE REQUIREMENTS

- N/A

13.4 IMPLEMENTATION

13.4.1 MS.EXO.12.1v1 Instructions

To modify the connection filters, follow the instructions found in Use the Microsoft 365 Defender portal to modify the default connection filter policy.

1. Sign in to **Microsoft 365 Defender portal**.
2. From the left-hand menu, find **Email & collaboration** and select **Policies and Rules.**
3. Select **Threat Policies** from the list of policy names.
4. Under **Policies**, select **Anti-spam**.
5. Select **Connection filter policy (Default)**.
6. Click **Edit connection filter policy**.
7. Ensure no addresses are specified under **Always allow messages from the following IP addresses or address range**.
8. Ensure **Turn on safe list** is not selected.

13.4.2 MS.EXO.12.2v1 Instructions

1. Sign in to **Microsoft 365 Defender portal**.
2. From the left-hand menu, find **Email & collaboration** and select **Policies and Rules**
3. Select **Threat Policies** from the list of policy names.
4. Under **Policies**, select **Anti-spam**.
5. Select **Connection filter policy (Default)**.
6. Click **Edit connection filter policy**.
7. (Optional) Enter addresses under **Always block messages from the following IP addresses or address range** as needed.
8. Ensure **Turn on safe list** is not selected.

14. MAILBOX AUDITING

Mailbox auditing helps users investigate compromised accounts or discover illicit access to Exchange Online. As a feature of Exchange Online, mailbox auditing is enabled by default for all organizations. Microsoft defines a default audit policy that logs certain actions performed by administrators, delegates, and owners. While mailbox auditing is enabled by default, this policy helps avoid inadvertent disabling.

14.1 POLICIES

14.1.1 MS.EXO.13.1v1

Mailbox auditing SHALL be enabled.

- *Rationale:* Exchange Online user accounts can be compromised or misused. Enabling mailbox auditing provides a valuable source of information to detect and respond to mailbox misuse.
- *Last modified*: June 2023

14.2 RESOURCES

- Manage mailbox auditing in Office 365 | Microsoft Learn
- Supported mailbox types | Microsoft Learn
- Microsoft Purview Compliance Manager - Microsoft 365 Compliance |Microsoft Learn

14.3 LICENSE REQUIREMENTS

- N/A

14.4 IMPLEMENTATION

14.4.1 MS.EXO.13.1v1 Instructions

Mailbox auditing can be managed from the Exchange Online PowerShell. Follow the instructions listed on Manage mailbox auditing in Office 365.

To check the current mailbox auditing status for your organization via PowerShell:

1. Connect to the Exchange Online PowerShell.
2. Run the following command: `Get-OrganizationConfig | Format-List AuditDisabled`
3. An `AuditDisabled : False` result indicates mailbox auditing is enabled.

To enable mailbox auditing by default for your organization via PowerShell:

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

```
Set-OrganizationConfig –AuditDisabled $false
```

15. INBOUND ANTI-SPAM PROTECTIONS

Junk email, or spam, can clutter user mailboxes and hamper communications across an agency. Implementing a spam filter helps to identify inbound spam and quarantine or move those messages. Microsoft Defender includes several capabilities for protecting against inbound spam emails. Using Microsoft Defender is not strictly required for this purpose; any product that fulfills the requirements outlined in this baseline policy group may be used. If the agency uses Microsoft Defender to meet this baseline policy group, see the following policy of the CISA M365 Security Configuration Baseline for Defender for Office 365.

- MS.DEFENDER.1.2v1 | CISA M365 Security Configuration Baseline for Defender for Office 365
- All users SHALL be added to Exchange Online Protection in either the standard or strict preset security policy.

15.1 POLICIES

15.1.1 MS.EXO.14.1v1

A spam filter SHALL be enabled. The filtering solution selected SHOULD offer services comparable to the native spam filtering offered by Microsoft.

- *Rationale:* Spam is a constant threat as junk mail can reduce user productivity, fill up mailboxes unnecessarily, and in some cases include malicious links or attachments. Filtering out spam reduces user workload burden, prevents junk mail congestion, and reduces potentially malicious content exposure.
- *Last modified*: June 2023

15.1.2 MS.EXO.14.2v1

Spam and high confidence spam SHALL be moved to either the junk email folder or the quarantine folder.

- *Rationale:* Spam is a constant threat as junk mail can reduce user productivity, fill up mailboxes unnecessarily, and in some cases include malicious links or attachments. Moving spam messages to a separate junk or quarantine folder helps users filter out spam while still giving them the ability to review messages, as needed, in case a message is filtered incorrectly.
- *Last modified*: June 2023

15.1.3 MS.EXO.14.3v1

Allowed domains SHALL NOT be added to inbound anti-spam protection policies.

- *Rationale:* Legitimate emails may be incorrectly filtered by spam protections. Adding allowed senders is an acceptable method of combating these false positives. Allowing an entire domain, especially a common domain like office.com, however, provides for a large number of potentially unknown users to bypass spam protections.
- Last modified: June 2023
- *Note:* Allowed senders MAY be added.

15.2 RESOURCES

- None

15.3 LICENSE REQUIREMENTS

- N/A

15.4 IMPLEMENTATION

15.4.1 MS.EXO.14.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which include spam filtering.

15.4.2 MS.EXO.14.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which include spam filtering that moves high-confidence spam to either the junk or quarantine folder.

15.4.3 MS.EXO.14.3v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender, see the following implementation steps for enabling preset security policies, which do not include any allowed sender domains by default.

16. LINK PROTECTION

Several technologies exist for protecting users from malicious links included in emails. For example, Microsoft Defender accomplishes this by prepending:

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

to any URLs included in emails. By prepending the safe links URL, Microsoft can proxy the initial URL through their scanning service. Their proxy can perform the following actions:

- Compare the URL with a blocklist.
- 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.

Microsoft Defender for Office 365 includes link-scanning capabilities. Using Microsoft Defender is not strictly required for this purpose; any product fulfilling the requirements outlined in this baseline policy group may be used. If the agency uses Microsoft Defender for Office 365 to meet this baseline policy group, see the following policy of the CISA M365 Security Configuration Baseline for Defender for Office 365 for additional guidance.

- MS.DEFENDER.1.3v1 | CISA M365 Security Configuration Baseline for Defender for Office 365
- All users SHALL be added to Defender for Office 365 Protection in either the standard or strict preset security policy.

16.1 POLICIES

16.1.1 MS.EXO.15.1v1

URL comparison with a blocklist SHOULD be enabled.

- *Rationale:* Users may be directed to malicious websites via links in email. Blocking access to known malicious URLs can prevent users from accessing known malicious websites.
- *Last modified*: June 2023

16.1.2 MS.EXO.15.2v1

Direct-download links SHOULD be scanned for malware.

- *Rationale:* URLs in emails may direct users to download and run malware. Scanning direct-download links in real time for known malware and blocking access can prevent users from infecting their devices.
- *Last modified*: June 2023

16.1.3 MS.EXO.15.3v1

User click tracking SHOULD be enabled.

- *Rationale:* Users may click on malicious links in emails, leading to compromise or unauthorized data disclosure. Enabling user click tracking lets agencies know if a malicious link may have been visited after the fact to help tailor a response to a potential incident.
- *Last modified*: June 2023

16.2 RESOURCES

- None

16.3 LICENSE REQUIREMENTS

- N/A

16.4 IMPLEMENTATION

16.4.1 MS.EXO.15.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender for Office] 365, see the following implementation steps for enabling preset security policies, which include Safe Links protections to scan URLs in email messages against a list of known malicious links.

16.4.2 MS.EXO.15.2v1 Instructions

Any product that meets the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender for Office 365, see the following implementation steps for enabling preset security policies, which include Safe Links protections to scan links to files for malware.

16.4.3 MS.EXO.15.3v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft Defender for Office 365, see the following implementation steps for enabling preset security policies, which include Safe Links click protections to track user clicks on links in email.

17. ALERTS

Managing and monitoring Exchange mailboxes and user activity requires a means to define activity of concern and notify administrators. Alerts can be generated to help identify suspicious or malicious activity in Exchange Online. These alerts give administrators better real-time insight into possible security incidents.

Using Microsoft 365 alert policies is not strictly required for this purpose; any product fulfilling the requirements outlined in this baseline policy group may be used. If the agency uses Microsoft 365 alert policies, this includes several prebuilt alert policies, many of which pertain to Exchange Online. Guidance for configuring alerts in Microsoft 365 is given in the following section of the CISA M365 Security Configuration Baseline for Defender for Office 365.

- Alerts | CISA M365 Security Configuration Baseline for Defender for Office 365

17.1 POLICIES

17.1.1 MS.EXO.16.1v1

At a minimum, the following alerts SHALL be enabled:

a. **Suspicious email sending patterns detected.**
b. **Suspicious Connector Activity.**
c. **Suspicious Email Forwarding Activity.**
d. **Messages have been delayed.**
e. **Tenant restricted from sending unprovisioned email.**
f. **Tenant restricted from sending email.**
g. **A potentially malicious URL click was detected.**

- *Rationale:* Potentially malicious or service-impacting events may go undetected without a means of detecting these events. Setting up a mechanism to alert administrators to events listed above draws attention to them to help minimize impact to users and the agency.
- *Last modified:* June 2023

17.1.2 MS.EXO.16.2v1

The alerts SHOULD be sent to a monitored address or incorporated into a security information and event management (SIEM) system.

- *Rationale:* Suspicious or malicious events, if not resolved promptly, may have a greater impact to users and the agency. Sending alerts to a monitored email address or SIEM system helps ensure these suspicious or malicious events are acted upon in a timely manner to limit overall impact.
- *Last modified:* June 2023

17.2 RESOURCES

- None

17.3 LICENSE REQUIREMENTS

- N/A

17.4 IMPLEMENTATION

17.4.1 MS.EXO.16.1v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft 365 alert policies, see the following implementation steps for enabling alerts for additional guidance.

17.4.2 MS.EXO.16.2v1 Instructions

Any product meeting the requirements outlined in this baseline policy may be used. If the agency uses Microsoft 365 alert policies, see the following implementation steps to add email recipients to an alert for additional guidance.

18. AUDIT LOGGING

User activity from M365 services is captured in the organization's unified audit log. These logs are essential for conducting incident response and threat detection activity.

By default, Microsoft retains the audit logs for 180 days. Activity by users with E5 licenses assigned is retained for one year.

However, in accordance with Office of Management and Budget (OMB) Memorandum 21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, Microsoft 365 audit logs are to be retained at least 12 months in active storage and an additional 18 months in cold storage. This can be accomplished by offloading the logs out of the cloud environment or natively through Microsoft by creating an audit log retention policy.

OMB M-21-13 also requires Advanced Audit be configured in M365. Advanced Audit, now Microsoft Purview Audit (Premium), adds additional event types to the Unified Audit Log.

Audit logging is managed from the Microsoft Purview compliance portal. For implementation guidance for configuring audit logging, see the following section of the CISA M365 Security Configuration Baseline for Defender for Office 365.

- Audit Logging | CISA M365 Security Configuration Baseline for Defender for Office 365

18.1 POLICIES

18.1.1 MS.EXO.17.1v1

Microsoft Purview Audit (Standard) logging SHALL be enabled.

- *Rationale:* Responding to incidents without detailed information about activities that took place slows response actions. Enabling Microsoft Purview Audit (Standard) helps ensure agencies have visibility into user actions. Furthermore, Microsoft Purview Audit (Standard) is required for government agencies by OMB M-21-31 (referred to therein by its former name, Unified Audit Logs).
- *Last modified*: June 2023

18.1.2 MS.EXO.17.2v1

Microsoft Purview Audit (Premium) logging SHALL be enabled.

- *Rationale:* Standard logging may not include relevant details necessary for visibility into user actions during an incident. Enabling Microsoft Purview Audit (Premium) captures additional event types not included with Standard. Furthermore, it is required for government agencies by OMB M-21-13 (referred to therein by its former name, Unified Audit Logs w/Advanced Features).
- *Last modified*: June 2023

18.1.3MS.EXO.17.3v1

Audit logs SHALL be maintained for at least the minimum duration dictated by OMB M-21-31 (Appendix C).

- *Rationale:* Audit logs may no longer be available when needed if they are not retained for a sufficient time. Increased log retention time gives an agency the necessary visibility to investigate incidents that occurred some time ago. OMB M-21-13, Appendix C, Table 5 specifically calls out Unified Audit Logs in the Cloud Azure log category.
- *Last modified*: June 2023

18.2 RESOURCES

- Expanding cloud logging to give customers deeper security visibility | Microsoft Security Blog

18.3 LICENSE REQUIREMENTS

- Microsoft Purview Audit (Premium) logging capabilities, including creating a custom audit log retention policy, requires E5/G5 licenses or E3/G3 licenses with add-on compliance licenses.
- Additionally, maintaining logs in the M365 environment for longer than one year requires an add-on license. For more information, see Licensing requirements | Microsoft Docs.

18.4 IMPLEMENTATION

18.4.1 MS.EXO.17.1v1 Instructions

See the following implementation steps for enabling Microsoft Purview (Standard).

18.4.2 MS.EXO.17.1v2 Instructions

See the following implementation steps for enabling Microsoft Purview (Premium).

18.4.3 MS.EXO.17.1v3 Instructions

See the following implementation steps to create an audit retention policy.