Microsoft Exchange Online

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

This page is intentionally blank.

1. Introduction

Microsoft Exchange Online provides users easy access to their email and supports organizational meetings, contacts, and calendars.

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 or the Microsoft 365 compliance admin centers. Generally speaking, the use of Microsoft Defender is not strictly required for this baseline. When noted, alternative products may be used in lieu of Microsoft Defender, on the condition that they fulfill the required baseline settings.

1.1 Assumptions

The **License Requirements** sections of this document assume the organization is using an Microsoft 365 E3 or G3 license level. Therefore, only licenses not included in E3 or 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 Automatic Forwarding to External Domains SHALL Be Disabled

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

2.1.1 Policy

- Automatic forwarding to external domains SHALL be disabled.

2.1.2 Resources

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

2.1.3 License Requirements

- N/A

2.1.4 Implementation

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**.

2.2 Sender Policy Framework SHALL Be Enabled

The Sender Policy Framework (SPF) is a mechanism that allows domain administrators to specify which Internet Protocol (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 the Domain Name Service (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.

2.2.1 Policy

- A list of approved IP addresses for sending mail SHALL be maintained.
- An SPF policy(s) that designates only these addresses as approved senders SHALL be published.

2.2.2 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 Docs
- How Microsoft 365 uses Sender Policy Framework (SPF) to prevent spoofing | Microsoft Docs

2.2.3 License Requirements

- N/A

2.2.4 Implementation

SPF is not configured through the Exchange admin center, but rather via the DNS records hosted by the agency's domain. Thus, the exact steps needed to set up SPF vary from agency to agency.

To test your SPF configuration, SPF records can be requested using the PowerShell tool Resolve-DnsName. For example:

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

2.3 DomainKeys Identified Mail SHOULD Be Enabled

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. DKIM is enabled for the tenant's default domain (e.g., on microsoft.com domains), but it must be manually enabled for custom domains.

2.3.1 Policy

- DKIM SHOULD be enabled for any custom domain.

2.3.2 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 Docs
- Support for validation of DKIM signed messages | Microsoft Docs
- What is EOP? | Microsoft Docs

2.3.3 License Requirements

- DKIM signing is included with Exchange Online Protection (EOP), which is included in all Microsoft 365 subscriptions that contain Exchange Online mailboxes.

2.3.4 Implementation

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

1. Navigate to the Microsoft 365 Defender admin center.
   a. Go to Policies & Rules.
      i. Go to Threat Policies.
2. Select **DKIM**.
3. Select your domain.
4. Switch **Sign messages for this domain with DKIM signatures** to **Enabled**.
5. If you are enabling DKIM for the first time, a pop-up window listing Canonical Name (CNAME) records displays. Publish these records to your DNS service provider.
6. Return to the DKIM page on the Defender admin center to finish enabling DKIM.

2.4 Domain-Based Message Authentication, Reporting, and Conformance SHALL Be Enabled

Domain-based Message Authentication, Reporting, and Conformance (DMARC) works with SPF and DKIM to authenticate mail senders and ensure that 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 or DKIM checks.

2.4.1 Policy

- A DMARC policy SHALL be published for every second-level domain.
- The DMARC message rejection option SHALL be "p=reject."
- The DMARC point of contact for aggregate reports SHALL include reports@dmarc.cyber.dhs.gov.
- An agency point of contact SHOULD be included for aggregate and/or failure reports.

2.4.2 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 Docs
- How Office 365 handles outbound email that fails DMARC | Microsoft Docs

2.4.3 License Requirements

- N/A

2.4.4 Implementation

DMARC implementation varies depending on how an agency manages its DNS records. See Form the DMARC TXT record for your domain | Microsoft Docs for Microsoft guidance.

DMARC records can be requested using the Powershell tool Resolve-DnsName. For example:

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

Replace "example.com" in the example with the domain(s) used for your agency's emails. Ensure that (1) the DNS record exists, (2) "p=reject;" is included in the policy returned from the query, and that (3) reports@dmarc.cyber.dhs.gov is included as a point for contact for aggregate feedback.

2.5 Simple Mail Transfer Protocol Authentication SHALL Be Disabled

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.

2.5.1 Policy

- SMTP AUTH SHALL be disabled in Exchange Online.
- SMTP AUTH MAY be enabled on a per-mailbox basis.

2.5.2 Resources

- Enable or disable authenticated client SMTP submission (SMTP AUTH) in Exchange Online | Microsoft Docs
- Use the Microsoft 365 admin center to enable or disable SMTP AUTH on specific mailboxes | Microsoft Docs

2.5.3 License Requirements

- N/A

2.5.4 Implementation

SMTP AUTH can only be disabled tenant-wide using Exchange Online PowerShell. To do so, follow the instructions listed at Disable SMTP AUTH in your organization | Microsoft Docs.

To enable SMTP AUTH on a per-mailbox basis, follow the instructions listed at Use the Microsoft 365 admin center to enable or disable SMTP AUTH on specific mailboxes | Microsoft Docs.

2.6 Calendar and Contact Sharing SHALL Be Restricted

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

2.6.1 Policy

- Contact folders SHALL NOT be shared with all domains, although they MAY be shared with specific domains.
- Calendar details SHALL NOT be shared with all domains, although they MAY be shared with specific domains.

2.6.2 Resources

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

2.6.3 License Requirements

- N/A

2.6.4 Implementation

To restrict sharing with all domains:

1. Sign in to the Exchange admin center.
2. Under **Organization**, select **Sharing**.
3. Under **Individual Sharing**, for all existing policies, ensure that for all sharing rules, **Sharing with all domains** is not selected.

2.7 External Sender Warnings SHALL Be Implemented

Mail flow rules allow the modification of incoming mail such that mail from external users can be easily identified, for example, by prepending the subject line with "[External]."

2.7.1 Policy

- External sender warnings SHALL be implemented.

2.7.2 Resources

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

2.7.3 License Requirements

- N/A

2.7.4 Implementation

To enable 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 located…**.
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. Under **Choose a mode for this rule**, select **Enforce**.
11. Click **Save**.

2.8 Data Loss Prevention Solutions SHALL Be Enabled

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 a several commercial DLP solutions available that document support for Microsoft 365. Agencies may select any service that fits their needs and meets the requirements outlined in this baseline setting.

Microsoft offers DLP services, controlled within the Microsoft 365 compliance admin center. Though use of Microsoft's DLP solution is not strictly required, guidance for configuring Microsoft's DLP solution can be found in the "Data Loss Prevention SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*. The

DLP solution selected by an agency should offer services comparable to those offered by Microsoft.

2.8.1 Policy

- A DLP solution SHALL be used. The selected DLP solution SHOULD offer services comparable to the native DLP solution offered by Microsoft.
- The DLP solution SHALL protect personally identifiable information (PII) and sensitive information, as defined by the agency. At a minimum, the sharing of credit card numbers, Taxpayer Identification Numbers (TIN), and Social Security Numbers (SSN) via email SHALL be restricted.

2.8.2 Resources

- The "Data Loss Prevention SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.9 Emails SHALL Be Filtered by Attachment File Type

For some types of files (e.g., executable files), the dangers of allowing them to be sent over email outweigh any potential benefits. Some services, such as the Common Attachment Filter of Microsoft Defender, filter emails based on the attachment file types. Use of Microsoft Defender for this purpose is not strictly required; instead, equivalent products that fulfill the requirements outlined in this baseline setting may be used.

Though use of 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 "Common Attachments Filter SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*. The solution selected by an agency should offer services comparable to those offered by Microsoft.

2.9.1 Policy

- Emails SHALL be filtered by the file types of included attachments. The selected filtering solution SHOULD offer services comparable to Microsoft Defender's Common Attachment Filter.
- The attachment filter SHOULD attempt to determine the true file type and assess the file extension.
- Disallowed file types SHALL be determined and set. At a minimum, click-to-run files SHOULD be blocked (e.g., .exe, .cmd, and .vbe).

2.9.2 Resources

- The "Common Attachments Filter SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.10 Emails SHALL Be Scanned for Malware

Though any product that fills the requirements outlined in this baseline setting may be used, for guidance on implementing malware scanning using Microsoft Defender, see the following sections of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*:

- The "Safe-Attachments SHALL Be Enabled"

- "Zero-hour Auto Purge for Malware SHALL Be Enabled"

2.10.1 Policy

- Emails SHALL be scanned for malware.
- Emails identified as containing malware SHALL be quarantined or dropped.
- Email scanning SHOULD be capable of reviewing emails after delivery.

2.10.2 Resources

- The "Safe-Attachments SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline.*
- The "Zero-hour Auto Purge for Malware SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline.*

2.11 Phishing Protections SHOULD Be Enabled

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

- Impersonation protection checks, wherein a tool compares the sender's address to the addresses of known senders to flag look-alike addresses, like 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.

Microsoft Defender has capabilities for all these phishing protections. Except for impersonation protection, these features are available with EOP, which is included in all Microsoft 365 subscriptions that contain Exchange Online mailboxes. For more guidance on configuring phishing protections with Microsoft's native solutions, see the "Phishing Protections SHOULD Be Enabled," section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.11.1 Policy

- Impersonation protection checks SHOULD be used.
- User warnings, comparable to the user safety tips included with EOP, SHOULD be displayed.
- The phishing protection solution SHOULD include an AI-based phishing detection tool comparable to EOP Mailbox Intelligence.

2.11.2 Resources

- The "Phishing Protections SHOULD Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline.*

2.12 IP Allow Lists SHOULD NOT be Implemented

Microsoft Defender supports the creations of IP “allow lists,” which are intended to ensure that emails from *specific* senders are not blocked. 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” ensure that mail from these IP addresses is always blocked. Although we have no specific guidance on which IP addresses to add, block lists can be used to block mail from known spammers.

The IP “safe lists” group is a dynamic list of “known, good senders,” which Microsoft sources from various third-party subscriptions. As with senders in the allow list, emails from these senders bypass important security mechanisms.

2.12.1 Policy

- IP allow lists SHOULD NOT be created.
- Safe lists SHOULD NOT be enabled.
- A connection filter MAY be implemented to create an IP “block list.”

2.12.2 Resources

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

2.12.3 License Requirements

- Exchange Online Protection.

2.12.4 Implementation

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

1. Sign in to Microsoft 365 Defender**.**
2. Under **Email & collaboration**, select **Policies & rules**.
3. Under **Policies**, select **Anti-spam**.
4. Select **Connection filter policy (Default)**.
5. Click **Edit connection filter policy**.
6. Ensure no addresses are specified under **Always allow messages from the following IP addresses or address range**.
7. 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.

2.13 Mailbox Auditing SHALL Be Enabled

Mailbox auditing helps users investigate compromised accounts or discover illicit access to Exchange Online. Some actions performed by administrators, delegates, and owners are logged automatically. While mailbox auditing is enabled by default, agencies should ensure that it has not been inadvertently disabled.

2.13.1 Policy

- Mailbox auditing SHALL be enabled.

2.13.2 Resources

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

2.13.3 License Requirements

- N/A

2.13.4 Implementation

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

To check the current mailbox auditing status via PowerShell:

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

   Get-OrganizationConfig | Format-List AuditDisabled.

To enable mailbox auditing via PowerShell:

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

   Set-OrganizationConfig –AuditDisabled $false.

2.14 Inbound Anti-Spam Protections SHALL Be Enabled

Microsoft Defender includes several capabilities for protecting against inbound spam emails. Use of Microsoft Defender is not strictly required for this purpose, and any product that fulfills the requirements outlined in this baseline setting may be used. See the “Inbound Anti-Spam Protections SHALL Be Enabled” section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline* for additional guidance.

2.14.1 Policy

- A spam filter SHALL be enabled. The filtering solution selected SHOULD offer services comparable to the native spam filtering offered by Microsoft.
- Spam and high confidence spam SHALL be moved to either the junk email folder or the quarantine folder.

- Allowed senders MAY be added, but allowed domains SHALL NOT be added.

2.14.2 Resources

- The "Inbound Anti-Spam Protections SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.15 Link Protection SHOULD Be Enabled

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 then perform the following actions:

- 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.

Though Microsoft Defender's use is not strictly required for this purpose, guidance for enabling link scanning using Microsoft Defender is included in the "Safe Links Policies SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline.*

2.15.1 Policy

- URL comparison with a block-list SHOULD be enabled.
- Direct download links SHOULD be scanned for malware.
- User click tracking SHOULD be enabled.

2.15.2 Resources

- The "Safe Links Policies SHOULD Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.16 Alerts SHALL Be Enabled

Microsoft Defender includes several prebuilt alert policies, many of which pertain to Exchange Online. These alerts give admins better real-time insight into possible security incidents. Guidance for configuring alerts in Microsoft Defender is given in the "Alerts SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.16.1 Policy

- At a minimum, the following alerts SHALL be enabled:
  - Suspicious email sending patterns detected.
  - Suspicious connector activity.

  - Suspicious email forwarding activity.
  - Unusual increase in email reported as phish.
  - Messages have been delayed.
  - Tenant restricted from sending unprovisioned email.
  - Tenant restricted from sending email.
  - Malware campaign detected after delivery.
  - A potentially malicious URL click was detected.
- The alerts SHOULD be sent to a monitored address or incorporated into a security incident and event management (SIEM) tool.

2.16.2 Resources

- The "Alerts SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.17 Audit Logging SHALL Be Enabled

Viewing data in threat protection reports, email security reports, and Explorer requires turning on audit logging.

Audit logging is managed from the Microsoft compliance center. For guidance configuring audit logging, see the "Audit Logging SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

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 for 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.

2.17.1 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 (Appendix C).

2.17.2 Resources

- The "Audit Logging SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

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).