GOOGLE MAIL

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.01

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

REVISION HISTORY

Version	Summary of revisions	Edited By	Date
2.0	• Entire Document – Initial Draft Change	CISA SCuBA	06/07/2023
2.01	• Incorporated comment from OCC making grammatical change to Section 1.1 Assumptions (brevity). • Added OCC provided statement to Section 1.1 Assumptions. • Incorporated comment from OCC making grammatical change to Rationale for GWS.GMAIL.3.1v0.1 (helps ensure). • Incorporated comment from OCC making grammatical change to Rationale for GWS.GMAIL.5.5v0.1 (helps warn). • Incorporated comment from OCC making grammatical change to Rationale for GWS.GMAIL.6.2v0.1 (active voice). • Incorporated comment from OCC making grammatical change to Rationale for GWS.GMAIL.7.6v0.1 (“reduced” vs. “greatly reduced”) • Incorporated comment from OCC replacing (4) instances of “whitelist” with “allowlist” in introductory section and policy statement for GWS.GMAIL.12.1v0.1. • Incorporated comment from OCC making grammatical change to Rationale for GWS.GMAIL.22.1v0.1 (“helps ensure” and “help prevent”).	CISA SCuBA	12/3/2023

CONTENTS

1. CISA GOOGLE WORKSPACE SECURITY CONFIGURATION BASELINE FOR GMAIL

Gmail is the Google Workspace offering for sending and receiving email. Users can upload attachments to emails and send them to a given email address. Additional Gmail features include integrating with other Google applications, such as Meet and Chat. This Secure Configuration Baseline (SCB) provides specific policies to strengthen Gmail security.

The Secure Cloud Business Applications (SCuBA) project provides guidance and capabilities to secure agencies' cloud business application environments and protect federal information that is created, accessed, shared, and stored in those environments. The SCuBA Secure Configuration Baselines (SCB) for Google Workspace (GWS) will help secure federal civilian executive branch (FCEB) information assets stored within GWS cloud environments through consistent, effective, modern, and manageable security configurations.

The CISA SCuBA SCBs for GWS help secure federal information assets stored within GWS 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.

This baseline is based on Google documentation available at the Gmail Google Workspace Admin Help Center and addresses the following:.

- Mail Delegation
- Domain Keys Identified Mail
- SPF Policies
- Domain Based Authentication
- Attachment Protections
- Links and External Images Protections
- Spoofing and Authentication Protection
- User Email Uploads
- POP and IMAP Access
- Workspace Sync
- Automatic Forwarding

- Image URL Proxy Whitelists
- Per User Outbound Gateways
- Unintended External Reply Warning
- Email Allowlist
- Enhanced Pre-Delivery Message Scanning
- Security Sandbox
- Spam Approved Senders List
- Blocked Senders List
- Comprehensive Mail Storage
- Content Compliance Filtering
- Objective Content Filtering
- Attachment Compliance Filtering

Within Google Workspace, settings can be assigned to users through organizational units, configuration groups, or individually. Before changing a setting, the user can select the organizational unit, configuration group, or individual users to which they want to apply changes.

1.1 ASSUMPTIONS

This document assumes the organization is using GWS Enterprise Plus.

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.

1.2 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 MAIL DELEGATION

This section determines whether users can delegate access to their mailbox to others within the same domain. This delegation includes access to read, send, and delete messages on the account owner's behalf. This delegation can be done via a command line tool (GAM) if enabled in the admin console.

2.2 POLICIES

2.2.1 GWS.GMAIL.1.1v0.1

Mail Delegation SHOULD be disabled.

- Rationale: Mail delegation can be a useful tool for delegating email management tasks to trusted individuals. However, it does pose the potential for risks such as unintentional disclosure of sensitive information, impersonation of delegated accounts, and malicious deletion or modification of emails.
- Last Modified: October 4, 2023
- Notes
  - Exceptions should be limited to individuals authorized by existing Agency policy, such as SES or Politically Appointed staff. Other considerations include ensuring that delegated accounts require Phishing-Resistant Multi-Factor Authentication (MFA), limiting delegated account permissions (ex. allowing view/reply but not delete), monitoring delegated accounts regularly, and disabling them if no longer required.

2.3 RESOURCES

- Google Workspace Admin Help: Turn Gmail delegation on or off
- GAM: Example Email Settings - Creating a Gmail delegate
- CIS Google Workspace Foundations Benchmark

2.4 PREREQUISITES

- None

2.5 IMPLEMENTATION

2.5.1 GWS.GMAIL.1.1v0.1 instructions:

To configure the settings for Mail Delegation:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **User Settings -> Mail delegation**.
4. Ensure that the **Let users delegate access to their mailbox to other users in the domain** checkbox is unchecked.
5. Select **Save**.

3. DOMAINKEYS IDENTIFIED MAIL

This section enables DomainKeys Identified Mail (DKIM) to help prevent spoofing on outgoing messages sent from a specific domain. DKIM allows digital signatures to be added to email messages in the message header, providing a layer of both authenticity and integrity to emails. Without DKIM, messages that are sent from a specific domain are more likely to be marked as spam by receiving mail servers. DKIM relies on Domain Name System (DNS) records, thus, its deployment depends on how an agency manages its DNS.

3.1 POLICIES

3.1.1 GWS.GMAIL.2.1v0.1

DKIM SHOULD be enabled for agencies' mail enabled domain.

- Rationale: Spoofing is a common unauthorized use of email, so some email servers require DKIM to prevent email spoofing.
- Last Modified: July 10, 2023

3.2 RESOURCES

- Binding Operational Directive 18-01 - Enhance Email and Web Security | DHS
- Trustworthy Email | NIST 800-177 Rev. 1
- Google Workspace Admin Help: Help prevent spoofing and spam with DKIM
- CIS Google Workspace Foundations Benchmark

3.3 PREREQUISITES

- None

3.4 IMPLEMENTATION

3.4.1 GWS.GMAIL.2.1v0.1 instructions:

To configure the settings for DKIM:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Authenticate email -> DKIM authentication**.
4. Select a domain listed in the **Selected** domain drop-down menu.
5. Select **START AUTHENTICATION**. Note that it can take up to 48 hours for DNS changes to fully propagate.
6. Select **Save**.

4. SENDER POLICY FRAMEWORK

The Sender Policy Framework (SPF) is a mechanism that allows domain administrators to specify which IP addresses are explicitly approved to send email on behalf of the domain, facilitating detection of spoofed emails. SPF isn't configured through the Google Admin Console, 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, but Google's documentation provides some helpful starting points.

4.1 POLICIES

4.1.1 GWS.GMAIL.3.1v0.1

Agencies SHALL determine which IP addresses are approved senders for their domain(s).

- 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 that unauthorized servers sending spoofed messages can be detected and permits message delivery from legitimate senders.
- Last Modified: July 10, 2023

4.1.2 GWS.GMAIL.3.2v0.1

Agencies SHALL publish SPF policy(s) that designate these (and only these) addresses as approved senders for their domain(s).

- Rationale: These policies help to ensure that messages are only allowed to come from the addresses on the allow list.
- Last Modified: July 10, 2023

4.2 RESOURCES

- Binding Operational Directive 18-01 - Enhance Email and Web Security | DHS
- Trustworthy Email | NIST 800-177 Rev. 1
- Google Workspace Admin Help: Help prevent spoofing and spam with SPF

4.3 PREREQUISITES

- None

4.4 IMPLEMENTATION

4.1.1 GWS.GMAIL.3.1v0.1 - GWS.GMAIL.3.2v0.1 instructions:

SPF is not configured through the Google Workspace 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 Google Workspace Admin Help: Help prevent spoofing and spam with SPF for the guidance offered by Google.

5. DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING, AND CONFORMANCE

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.

5.1 POLICIES

5.1.1 GWS.GMAIL.4.1v0.1

Agencies SHALL publish a DMARC policy.

- Rationale: DMARC works with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) to authenticate mail senders and ensure that destination email systems trust messages sent from your domain. Spammers can spoof your domain or organization to send fake messages that impersonate your organization. DMARC tells receiving mail servers what to do when they get a message that appears to be from your organization, but doesn't pass authentication checks, or doesn't meet the authentication requirements in your DMARC policy record. Messages that aren't authenticated might be impersonating your organization or might be sent from unauthorized servers.

- Last Modified: July 10, 2023

5.1.2 GWS.GMAIL.4.2v0.1

Agencies SHALL set their policy to message rejection (i.e., “p=reject”).

- Rationale: This helps ensure that unauthenticated emails are not delivered to keep the agency secure from potential attacks.
- Last Modified: July 10, 2023

5.1.3 GWS.GMAIL.4.3v0.1

Agencies SHALL include reports@dmarc.cyber.dhs.gov as a point of contact for aggregate reports.

- Rationale: This complies with requirements in DHS Binding Operational Directive 18-01: Enhance Email and Web Security. Information derived from reports can inform additional protection mechanisms.
- Last Modified: July 10, 2023

5.1.4 GWS.GMAIL.4.4v0.1

Agencies SHOULD include an agency point of contact for aggregate and/or failure reports in their policy.

- Rationale: Having an agency point of contact can help inform additional protection mechanisms.
- Last Modified: July 10, 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
- Google Workspace Admin Help: Help prevent spoofing and spam with DMARC

5.3 PREREQUISITES

- DKIM or SPF must be enabled.

5.4 IMPLEMENTATION

5.4.1 GWS.GMAIL.4.1v0.1 - GWS.GMAIL.4.4v0.1 instructions:

DMARC implementation varies depending on how an agency manages its DNS records.

See Google Workspace Admin Help: Help prevent spoofing and spam with DMARC for the guidance offered by Google.

6. ATTACHMENT PROTECTIONS

This section enables protections against suspicious attachments and scripts from untrusted senders, to include encrypted attachments, documents with malicious scripts, and attachment file types that are

uncommon and/or archaic. Through these attachments malware can be spread. These messages can be kept in the inbox with a warning label (default), moved to spam, or quarantined.

A Google Workspace solution is not strictly required to satisfy this baseline control, but the solution selected by an agency should offer services comparable to those offered by Google.

6.1 POLICIES

6.1.1 GWS.GMAIL.5.1v0.1

Protect against encrypted attachments from untrusted senders SHALL be enabled.

- Rationale: Protect users from potentially malicious attachments.
- Last Modified: July 10, 2023

6.1.2 GWS.GMAIL.5.2v0.1

Protect against attachments with scripts from untrusted senders SHALL be enabled.

- Rationale: Protect users from potentially malicious attachments.
- Last Modified: July 10, 2023

6.1.3 GWS.GMAIL.5.3v0.1

Protect against anomalous attachment types in emails SHALL be enabled.

- Rationale: Protect users from potentially malicious attachments.
- Last Modified: July 10, 2023

6.1.4 GWS.GMAIL.5.4v0.1

Google SHOULD be allowed to automatically apply future recommended settings.

- Rationale: Apply the latest recommended settings.
- Last Modified: July 10, 2023

6.1.5 GWS.GMAIL.5.5v0.1

Emails flagged by the above attachment protection controls SHALL NOT be kept in inbox.

- Rationale: Helps warn users about the risks of opening a suspicious attachment.
- Last Modified: September 8, 2023
- Notes
  - Agencies and Organizations can choose whether to send email to spam or quarantine.
  - Applies to Policies 5.1 - 5.3

6.1.6 GWS.GMAIL.5.6v0.1

Any third-party or outside application selected for attachment protection SHOULD offer services comparable to those offered by Google Workspace.

- Rationale: A third-party system should provide the same minimum functionality provided by Google.
- Last Modified: July 10, 2023

6.1.7 Resources

- Google Workspace Admin Help: Advanced phishing and malware protection

6.2 PREREQUISITES

- N/A

6.3 IMPLEMENTATION

To configure the settings for Attachment Protections:

6.3.1Policies Group 5 Common Instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Safety -> Attachments**.
4. Follow implementation for each individual policy
5. Select **Save**.

6.3.2 GWS.GMAIL.5.1v0.1 instructions:

1. Check the **Protect against encrypted attachments from untrusted senders'** checkbox.

6.3.3 GWS.GMAIL.5.2v0.1 instructions:

1. Check the **Protect against attachments with scripts from untrusted senders'** checkbox.

6.3.4 GWS.GMAIL.5.3v0.1 instructions:

10k. Check the **Protect against anomalous attachment types in emails** checkbox

6.3.5 GWS.GMAIL.5.4v0.1 instructions:

1. Check the **Apply future recommended settings automatically** checkbox.

6.3.6 GWS.GMAIL.5.5v0.1 instructions:

1. Under the setting for Policy 5.1 through Policy 5.3, ensure either "Move email to spam" or "Quarantine" is selected.

6.3.7 GWS.GMAIL.5.6v0.1 instructions:

1. No implementation steps for this policy

7. LINKS AND EXTERNAL IMAGES PROTECTION

This section enables extra protections to prevent email phishing due to links and external images. Specific settings for this control include identifying hidden malicious links behind shortened URLs, scanning linked images to find hidden malicious content, showing a warning prompt when clicking links to untrusted domains, and applying future recommended settings automatically.

A Google Workspace solution is not strictly required to satisfy this baseline control, but the solution selected by an agency should offer services comparable to those offered by Google.

7.1 POLICIES

7.1.1 GWS.GMAIL.6.1v0.1

Identify links behind shortened URLs SHALL be Enabled.

- Rationale: By allowing the identification of links that are behind shortened URLs provided protection against potential phishing attacks as the true links would be known.
- Last Modified: July 10, 2023

7.1.2 GWS.GMAIL.6.2v0.1

Scan linked images SHALL be enabled.

- Rationale: Scanning linked images provides additional protections for potential malware that may be sent via email through an image.
- Last Modified: July 10, 2023

7.1.3 GWS.GMAIL.6.3v0.1

Show warning prompt for any click on links to untrusted domains SHALL be enabled.

- Rationale: This will provide awareness to users about the risks associated with clicking an unknown link
- Last Modified: July 10, 2023

7.1.4 GWS.GMAIL.6.4v0.1

Google SHALL be allowed to automatically apply future recommended settings.

- Rationale: This ensures that the recommended settings are always the settings in place.
- Last Modified: July 10, 2023

7.1.5 GWS.GMAIL.6.5v0.1

Any third-party or outside application selected for links and external images protection SHOULD offer services comparable to those offered by Google Workspace.

- Rationale: A third-party system should provide the same minimum functionality provided by Google.
- Last Modified: July 10, 2023

7.2 RESOURCES

- Google Workspace Admin Help: Advanced phishing and malware protection
- Google Workspace Admin Help: Set up rules to detect harmful attachments
- Google Workspace Admin Help: Monitor the health of your Gmail settings
- CIS Google Workspace Foundations Benchmark

7.3 PREREQUISITES

- N/A

7.4 IMPLEMENTATION

To configure the settings for Links and External Images Protection:

7.4.1 Policies Group 6 common instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Safety -> Links and external images**.
4. Follow implementation for each individual policy.
5. Select **Save**

7.4.2 GWS.GMAIL.6.1v0.1 instructions:

1. Check the **Identify links behind shortened URLs** checkbox.

7.4.3 GWS.GMAIL.6.2v0.1 instructions:

1. Check the **Scan linked images** checkbox.

7.4.4 GWS.GMAIL.6.3v0.1 instructions:

1. Check the **Show warning prompt for any click on links to untrusted domains** checkbox.

7.4.5 GWS.GMAIL.6.4v0.1 instructions:

1. Check the **Apply future recommended settings automatically** checkbox.

7.4.6 GWS.GMAIL.6.5v0.1 instructions:

1. No implementation steps for this policy

8. SPOOFING AND AUTHENTICATION PROTECTION

This control enables extra protections to prevent spoofing of a domain name, employee names, email pretending to be from a specific domain, and unauthenticated email from any domain. These messages can be kept in the inbox with a warning label (default), moved to spam, or quarantined.

A Google Workspace solution is not strictly required to satisfy this baseline control, but the solution selected by an agency should offer services comparable to those offered by Google.

8.1 POLICIES

8.1.1 GWS.GMAIL.7.1v0.1

Protect against domain spoofing based on similar domain names SHALL be enabled.

- Rationale: Attackers commonly try to trick users into going to a malicious site by using similar domain names. This policy helps protect the organization and users from this type of attempted compromise.
- Last Modified: July 10, 2023

8.1.2 GWS.GMAIL.7.2v0.1

Protect against spoofing of employee names SHALL be enabled.

- Rationale: Attackers will try to phish individuals by spoofing the email/identity of another employee (e.g., CEO and IT staff). Therefore, this provides additional protection against this type of attempted compromise.
- Last Modified: July 10, 2023

8.1.3 GWS.GMAIL.7.3v0.1

Protect against inbound emails spoofing your domain SHALL be enabled.

- Rationale: Attackers will try to phish individuals by spoofing the domain name of your organization. This policy provides additional protection against this type of attempted compromise.
- Last Modified: July 10, 2023

8.1.4 GWS.GMAIL.7.4v0.1

Protect against any unauthenticated emails SHALL be enabled.

- Rationale: This policy provides extra protection from potentially malicious emails, helping safeguard the organization from data leakage and other malware.
- Last Modified: July 10, 2023

8.1.5 GWS.GMAIL.7.5v0.1

Protect your Groups from inbound emails spoofing your domain SHALL be enabled.

- Rationale: This provides protections against phishing attacks using an email address within your domain.
- Last Modified: July 10, 2023

8.1.6 GWS.GMAIL.7.6v0.1

Emails flagged by the above spoofing and authentication controls SHALL NOT be kept in inbox.

- Rationale: Emails that fail Gmail's spoofing and authentication checks may pose a significant risk to users. By moving these emails to either spam or quarantine, the risk of a user inadvertently interacting with these emails is reduced.
- Last Modified: September 8, 2023
- Notes
  - Agencies and organizations can choose whether to send to spam or quarantine
  - This policy applies to Policy 7.1 - Policy 7.5

8.1.7 GWS.GMAIL.7.7v0.1

Google SHALL be allowed to automatically apply future recommended settings.

- Rationale: This allows automatic application of recommended settings from Google.
- Last Modified: July 10, 2023

8.1.8 GWS.GMAIL.7.8v0.1

Any third-party or outside application selected for spoofing and authentication protection SHOULD offer services comparable to those offered by Google Workspace.

- Rationale: A third-party system should provide the same minimum functionality provided by Google.
- Last Modified: July 10, 2023

8.2 RESOURCES

- Google Workspace Admin Help: Advanced phishing and malware protection

8.3 PREREQUISITES

- N/A

8.4 IMPLEMENTATION

To configure the settings for Spoofing and Authentication Protection:

8.4.1 Policies Group 7 common instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Safety -> Spoofing and authentication**.
4. Follow steps for individual policies below.
5. Select **Save**

8.4.2 GWS.GMAIL.7.1v0.1 instructions:

1. Check the **Protect against domain spoofing based on similar domain names** checkbox.

8.4.3 GWS.GMAIL.7.2v0.1 instructions:

1. Check the **Protect against spoofing of employee names** checkbox.

8.4.4 GWS.GMAIL.7.3v0.1 instructions:

1. Check the **Protect against inbound emails spoofing your domain** checkbox.

8.4.5 GWS.GMAIL.7.4v0.1 instructions:

1. Check the **Protect against any unauthenticated emails** checkbox.

8.4.6 GWS.GMAIL.7.5v0.1 instructions:

1. Check the **Protect your groups from inbound emails spoofing your domain** checkbox.

8.4.7 GWS.GMAIL.7.6v0.1 instructions:

1. Under each setting from Policy 7.1 through Policy 7.5, make sure either "Move email to spam" or "Quarantine" is selected.

8.4.8 GWS.GMAIL.7.7v0.1 instructions:

1. Check the **Apply future recommended settings automatically** checkbox.

8.4.9 GWS.GMAIL.7.8v0.1 instructions:

1. There is no implementation for this policy.

9. USER EMAIL UPLOADS

This section enables users to import their email and contacts from non-Google webmail accounts such as Yahoo!, Hotmail, or AOL.

9.1 POLICIES

9.1.1 GWS.GMAIL.8.1v0.1

User email uploads SHALL be disabled to protect against unauthorized files being introduced into the secured environment.

- Rationale: This helps ensure that unauthorized files from other webmail providers are not introduced into the secure Gmail environment.
- Last Modified: July 10, 2023

9.2 RESOURCES

- Google Workspace Admin Help: Advanced Gmail settings reference for admins
- Google Workspace Admin Help: Turn imports from webmail hosts on or off

9.3 PREREQUISITES

- N/A

9.4 IMPLEMENTATION

To configure the settings for User Email Uploads:

9.4.1 GWS.GMAIL.8.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Setup -> User email uploads**.
4. Uncheck the **Show users the option to import mail and contacts from Yahoo!, Hotmail, AOL, or other webmail or POP3 accounts from the Gmail settings page** checkbox.
5. Select **Save**.

10. POP AND IMAP ACCESS FOR USERS

This section determines whether users have POP3 and IMAP access. Doing so allows the user to access Gmail emails from outside the context of protected/hardened environments and from older versions of Gmail applications or other third-party mail applications.

10.1 POLICIES

10.1.1 GWS.GMAIL.9.1v0.1

POP and IMAP access SHALL be disabled to protect sensitive agency or organization emails from being accessed through legacy applications or other third-party mail clients.

- Rationale: Disabling POP and IMAP helps prevent use of legacy and unapproved email clients with weaker authentication mechanisms that would increase the risk of email account credential compromise.
- Last Modified: July 10, 2023

10.1.2 GWS.GMAIL.9.2v0.1

POP and IMAP access MAY be enabled on a per-user and per-application basis as needed.

- Rationale: To allow access to users and applications which made need access to these protocols.
- Last Modified: July 10, 2023

10.2 RESOURCES

- Google Workspace Admin Help: Turn POP and IMAP on and off for users

10.3 PREREQUISITES

- N/A

10.4 IMPLEMENTATION

To configure the settings for POP and IMAP access:

10.4.1 Policies Group 9 common instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **End User Access -> POP and IMAP access**.
4. Follow the implementation for each policy.
5. Select **Save**.

10.4.2 GWS.GMAIL.9.1v0.1 instructions:

1. Uncheck the **Enable IMAP access for all users** checkboxes.

10.4.3 GWS.GMAIL.9.2v0.1 instructions:

1. Uncheck the **Enable POP access for all users** checkboxes.

11. GOOGLE WORKSPACE SYNC

This section determines whether Google Workspace Sync allows data synchronization between Google Workspace and Microsoft Outlook. The data includes email, calendar, and contacts. Data synchronizes each time users start Outlook. This is an additional plugin that must be downloaded.

11.1 POLICIES

11.1.1 GWS.GMAIL.10.1v0.1

Google Workspace Sync SHOULD be disabled.

- Rationale: By allowing this would allow users to use less secure methods of accessing email.
- Last Modified: July 10, 2023

11.1.2 GWS.GMAIL.10.2v0.1

Google Workspace Sync MAY be enabled on a per-user basis as needed.

- Rationale: Some users might need access to this feature for organizational needs/tasks.
- Last Modified: July 10, 2023

11.2 RESOURCES

- Google Workspace Sync for Microsoft Outlook

11.3 PREREQUISITES

- N/A

11.4 IMPLEMENTATION

To configure the settings for Google Workspace Sync:

11.4.1 Policy Group 10 Common instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **End User Access -> Google Workspace Sync**.

11.4.2 GWS.GMAIL.10.1v0.1 instructions:

1. Uncheck the **Enable Google Workspace Sync for Microsoft Outlook for my users** checkbox.
2. Select **Save**.

11.4.3 GWS.GMAIL.10.2v0.1 instructions:

1. There are no implementation steps for this policy.
2. Select **Save**.

12. AUTOMATIC FORWARDING

This section determines whether emails can be automatically forwarded from a user's inbox to another of their choosing, possibly to external domains.

12.1 POLICIES

12.1.1 GWS.GMAIL.11.1v0.1

Automatic forwarding SHOULD be disabled, especially to external domains.

- Rationale: In the event that an attacker gains control of an end-user account, they could create rules to ex-filtrate data from your environment.
- Last Modified: July 10, 2023

12.1.2 GWS.GMAIL.11.2v0.1

Automatic forwarding MAY be enabled on a per-user basis as needed.

- Rationale: Some users may need access to this feature based on organization needs
- Last Modified: July 10, 2023

12.2 RESOURCES

- Google Workspace Admin Help: Disable automatic forwarding

12.3 PREREQUISITES

- N/A

12.4 IMPLEMENTATION

To configure the settings for Automatic Forwarding:

12.4.1 Policy Group 11 Common instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **End User Access -> Automatic forwarding**.

12.4.2 GWS.GMAIL.11.1v0.1 instructions:

1. Uncheck the **Allow users to automatically forward incoming email to another address** checkbox.
2. Select **Save**.

12.4.3 GWS.GMAIL.11.2v0.1 instructions:

1. There are no implementation steps for this policy
2. Select **Save**

13. IMAGE URL PROXY ALLOWLISTS

This section determines whether image URL proxy allowlists can be used within a domain. These lists allow for a set of domains and a path prefix to be specified for a large group of URLs. In doing so, those URLs will be able to bypass proxy protection to keep links to images intact while protecting users and the domain against image-based security vulnerabilities.

13.1 POLICIES

13.1.1 GWS.GMAIL.12.1v0.1

Image URL proxy allowlists SHOULD be enabled to avoid broken links to images that are dependent on internal IP addresses within an organization's domain.

- Rationale: To avoid attacks based on image-based vulnerabilities as well as preventing broken image links.
- Last Modified: July 10, 2023

13.2 RESOURCES

- Google Workspace Admin Help: Set up an image URL proxy whitelist

13.3 PREREQUISITES

- N/A

13.4 IMPLEMENTATION

To configure the settings for Image URL Proxy Whitelists:

13.4.1 GWS.GMAIL.12.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **End User Access -> Image URL proxy allowlist**.
4. In the **Enter image URL patterns** field, enter **image URL proxy whitelist patterns**.
    1. A pattern can contain the scheme, the domain, and a path.
    2. The pattern must always have a forward slash (/) between the domain and path.
    3. If the URL pattern specifies a scheme, then the scheme and the domain must fully match. Otherwise, the domain can partially match the URL suffix.
    4. For example, the pattern /google.com matches www.google.com, but not gle.com. The URL pattern can specify a path that's matched against the path prefix.
5. Select **Save**.

14. PER-USER OUTBOUND GATEWAYS

This section determines whether outgoing mail is delivered only through the Google Workspace mail servers, or another specified external SMTP server. With this setting, a user can choose which email address displays in the "From" field.

14.1 POLICIES

14.1.1 GWS.GMAIL.13.1v0.1

Using a per-user outbound gateway that is a mail server other than the Google Workspace mail servers SHALL be disabled.

- Rationale: Mail sent via external SMTP will circumvent your outbound gateway
- Last Modified: July 10, 2023

14.2 RESOURCES

- Google Workspace Admin Help: Allow per-user outbound gateways

14.3 PREREQUISITES

- N/A

14.4 IMPLEMENTATION

To configure the settings for Per-user Outbound Gateways:

14.1.1 GWS.GMAIL.13.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **End User Access -> Allow per-user outbound gateways**.
4. Uncheck the **Allow users to send mail through an external SMTP server when configuring a "from" address hosted outside your email domain** checkbox.
5. Select **Save**.

15. UNINTENDED EXTERNAL REPLY WARNING

This section determines whether users are prompted with a warning for messages that include external recipients (users with emails addresses that are outside of your organization). However, the warning is not shown if the external recipient is in the organization's Directory, personal Contacts, or other Contacts; or if a secondary domain or domain alias address is used.

15.1 POLICIES

15.1.1 GWS.GMAIL.14.1v0.1

Unintended external reply warnings SHALL be enabled to avoid unintentional replies and remind users to treat external messages with caution.

- Rationale: As an admin for your organization, you can turn alerts on or off for messages that include external recipients (people with email addresses outside of your organization). These alerts help people avoid unintentional replies and remind them to treat external messages with caution.
- Last Modified: July 10, 2023

15.2 RESOURCES

- Google Workspace Admin Help: Control Gmail external recipient warnings
- Capacity Enhancement Guide Counter-Phishing Recommendations for Federal Agencies | CISA
- Actions to Counter Email-Based Attacks on Election-Related Entities | CISA

15.3 PREREQUISITES

- N/A

15.4 IMPLEMENTATION

To configure the settings to warn users of external recipients:

15.4.1 GWS.GMAIL.14.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **End User Access -> Warn for external recipients.**
4. Check the **Highlight any external recipients in a conversation. Warn users before they reply to email with external recipients who aren't in their contacts** checkbox.
5. Select **Save**.

16. EMAIL ALLOWLIST

This section determines whether an email allowlist allows for messages from certain IP addresses to not be marked as spam by Gmail. However, if implemented, emails from these senders will bypass important security mechanisms, such as SPF, DKIM, and DMARC.

16.1 POLICIES

16.1.1 GWS.GMAIL.15.1v0.1

An email allowlist SHOULD not be implemented.

- Rationale: This marks suspected spam email and helps allow spam policies to protect organization from potential attacks.

- Last Modified: July 10, 2023

16.1.2 GWS.GMAIL.15.2v0.1

A connection filter policy to create a Blocked Senders list MAY be implemented.

- Rationale: This ensures that measure blocks known malicious senders.
- Last Modified: July 10, 2023

16.2 RESOURCES

- Google Workspace Admin Help: Add IP addresses to allowlists in Gmail

16.3 PREREQUISITES

- N/A

16.4 IMPLEMENTATION

To configure the settings for Email Allowlists:

16.4.1 GWS.GMAIL.15.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Spam, phishing, and malware -> Email allowlist**.
4. Under the **Enter the IP addresses for your email allowlist** field, ensure **no IP addresses** are listed.
5. Select **Save**.

16.4.2 GWS.GMAIL.15.2v0.1 instructions:

1. There are no implementation steps for this policy

17. ENHANCED PRE-DELIVERY MESSAGE SCANNING

This section determines whether Gmail can screen and identify suspicious content that may be phishing attempts. In doing so, Google can either show a warning or move the email to Spam, but email delivery will experience a short delay due to the additional checks.

A Google Workspace solution is not strictly required to satisfy this baseline control, but the solution selected by an agency should offer services comparable to those offered by Google.

17.1 POLICIES

17.1.1 GWS.GMAIL.16.1v0.1

Enhanced pre-delivery message scanning SHALL be enabled to prevent phishing.

- Rationale: As an administrator, you can increase Gmail's ability to identify suspicious content with enhanced pre-delivery message scanning. Typically, when Gmail identifies a possible phishing message, a warning is displayed, and the message might be moved to spam.

- Last Modified: July 10, 2023

17.1.2 GWS.GMAIL.16.2v0.1

Any third-party or outside application selected for enhanced pre-delivery message scanning SHOULD offer services comparable to those offered by Google Workspace.

- Rationale: A third-party system should provide the same minimum functionality provided by Google.
- Last Modified: July 10, 2023

17.2 RESOURCES

- Google Workspace Admin Help: Help prevent phishing with pre-delivery message scanning

17.3 PREREQUISITES

- N/A

17.4 IMPLEMENTATION

To configure the settings for Enhanced Pre-Delivery Message Scanning:

17.4.1 GWS.GMAIL.16.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Spam, phishing, and malware -> Enhanced pre-delivery message scanning**.
4. Check the **Enables improved detection of suspicious content prior to delivery** checkbox.
5. Select **Save**.

17.4.2 GWS.GMAIL.16.2v0.1 instructions:

1. There are no implementation steps for this policy

18. SECURITY SANDBOX

This section determines whether certain messages and their associated attachments are executed in a sandbox environment for protection against malware, ransomware, and zero-day threats. Malicious software may be missed by traditional antivirus programs. However, this may cause some messages to get delayed before final delivery. Some of the file types scanned include Microsoft executables, Microsoft Office, PDF, and archives (zip, rar).

A Google Workspace solution is not strictly required to satisfy this baseline control, but the solution selected by an agency should offer services comparable to those offered by Google.

18.1 POLICIES

18.1.1 GWS.GMAIL.17.1v0.1

Security sandbox SHOULD be enabled to provide additional protections for their email messages.

- Rationale: This allows potentially malicious messages to be quarantined to be analyzed to see if it malicious.
- Last Modified: July 10, 2023

18.1.2 GWS.GMAIL.17.2v0.1

Any third-party or outside application selected for security sandbox SHOULD offer services comparable to those offered by Google Workspace.

- Rationale: A third-party system should provide the same minimum functionality provided by Google.
- Last Modified: July 10, 2023

18.2 RESOURCES

- Google Workspace Admin Help: Set up rules to detect harmful attachments

18.3 PREREQUISITES

- N/A

18.4 IMPLEMENTATION

To configure the settings for Security sandbox or Security sandbox rules:

18.4.1 GWS.GMAIL.17.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Spam, phishing, and malware -> Security sandbox**.
4. Check the **Enable virtual execution of attachments in a sandbox environment for all the users of the Organizational Unit for protection against malware, ransomware, and zero-day threats** checkbox.
5. Either **Security sandbox** or **Security sandbox rules** may be enabled but enabling **Security sandbox** takes precedence.
6. If **Security sandbox** rules are enabled, then the configuration needs to be completed and consists of the following fields **:**
    1. A short description.
    2. Email messages to affect.
    3. Expressions to describe the content to search for in each message.
    4. Action to take if expressions match.
7. Select **Save**.

18.4.2 GWS.GMAIL.17.2v0.1 instructions:

1. There are no implementation steps for this policy.

19. SPAM PROTECTION

This section covers the spam protection features in Gmail.

19.1 POLICIES

19.1.1 GWS.GMAIL.18.1v0.1

Aggressive spam filtering SHALL be enabled.

- Rationale: This helps ensure that all available protections are being implemented to help prevent risks associated with spam emails.
- Last Modified: December 1, 2023

19.1.2 GWS.GMAIL.18.2v0.1

Agencies allowing spam filter bypass for known senders SHALL enable warnings.

- Rationale: Warnings when bypassing spam filters can help provide administrators with situational awareness regarding the tenant's security posture.
- Last Modified: December 1, 2023

19.1.3 19.1.4 GWS.GMAIL.18.3v0.1

Addresses added to the Allowed Senders List SHALL be set to require authentication.

- Rationale: Authentication of delivered mail helps provide extra security for the agency.
- Last Modified: November 14, 2023

19.2 RESOURCES

- Google Workspace Admin Help: Help prevent spoofing, phishing, and spam

19.3 PREREQUISITES

- N/A

19.4 IMPLEMENTATION

To configure the settings for spam protection::

19.4.1 Policy Group 18 Common Instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Spam, phishing, and malware -> Spam**.

19.4.2 GWS.GMAIL.18.1v0.1 instructions:

1. Ensurethe **Be more aggressive when filtering spam** checkbox is checked.
2. Select **save**.

•

19.4.2 GWS.GMAIL.18.2v0.1 instructions:

1. Ensure the **bypass spam filters and hide warnings for messages from senders or domains in selected lists** is unchecked.
2. Ensure the **bypass spam filters and hide warnings for all messages from internal and external senders (not recommended)** is unchecked.
3. Select **save**.

19.4.3 GWS.GMAIL.18.3v0.1 instructions:

☐ 1. Select **Create or Edit List.**
☐ 2. Select **Add Address List** or **Edit** an existing list.
☐ 3. For each domain or sender added, ensure **Authentication required** is enabled.
☐

20. 21. COMPREHENSIVE MAIL STORAGE

This section allows for email messages sent through other Google Workspace applications, (i.e., Calendar, Drive, Docs, Sheets, Slides, Drawings, Forms, and Keep) to be stored in the associated users' Gmail mailboxes. This includes a copy of all sent or received messages within a specified domain (including messages sent or received by non-Gmail mailboxes).

21.1 POLICIES

21.1.1 GWS.GMAIL.20.1v0.1

Comprehensive mail storage SHOULD be enabled to allow tracking of information across applications.

- Rationale: This allows for tracking shared information from emails between GWS applications for traceability and security purposes.
- Last Modified: November 14, 2023

21.2 RESOURCES

- Google Workspace Admin Help: Set up comprehensive mail storage

21.3 PREREQUISITES

- N/A

21.4 IMPLEMENTATION

To configure the settings for Comprehensive Mail Storage:

21.4.1 GWS.GMAIL.20.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Compliance -> Comprehensive mail storage**.

4. Check the **Ensure that a copy of all sent and received mail is stored in associated users' mailboxes** checkbox.
5. Select **Save**.

22. CONTENT COMPLIANCE FILTERING SHOULD BE ENABLED

This section determines whether Gmail content is filtered based upon specified expressions, such as keyword, strings or patterns, and metadata. The compliance actions based upon the word lists are reject, quarantine, or deliver with modifications.

A Google Workspace solution is not strictly required to satisfy this baseline control, but the solution selected by an agency should offer services comparable to those offered by Google.

22.1 POLICIES

22.1.1 GWS.GMAIL.21.1v0.1

Content filtering SHOULD be enabled within Gmail messages.

- Rationale: Protects the agency against malicious content from entering the agencies systems.
- Last Modified: July 10, 2023

22.1.2 GWS.GMAIL.21.2v0.1

Any third-party or outside application selected for advanced email content filtering SHOULD offer services comparable to those offered by Google Workspace.

- Rationale: A third-party system should provide the same minimum functionality provided by Google.
- Last Modified: July 10, 2023

21.1.3 GWS.GMAIL.21.3v0.1

Gmail or third-party applications SHALL be configured to protect 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.

- Rationale: This helps protect against PII data leakage.
- Last Modified: July 10, 2023

21.2 RESOURCES

- Google Workspace Admin Help: Set up rules for advanced email content filtering
- Personally identifiable information (PII) | NIST
- Sensitive information | NIST

21.3 PREREQUISITES

- N/A

21.4 IMPLEMENTATION

To configure the settings for Objectionable content:

21.4.1 GWS.GMAIL.21.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Compliance -> Content Compliance**.
4. If **Content compliance** filtering is enabled, then the configuration needs to be completed and consists of the following fields:
    1. A short description.
    2. Email messages to affect.
    3. Expressions for content to search for in messages.
    4. Compliance action options.
5. Select **Save**.

21.4.2 GWS.GMAIL.21.2v0.1 instructions:

1. There are no implementation steps for this policy.

21.4.3 GWS.GMAIL.21.3v0.1 instructions:

1. There are no implementation steps for this policy.

22. OBJECTIONABLE CONTENT FILTERING

This section determines whether Gmail content is filtered based upon word lists, for example, obscenities or "confidential" words. The compliance actions based upon the word lists are reject, quarantine, or deliver with modifications.

A Google Workspace solution is not strictly required to satisfy this baseline control, but the solution selected by an agency should offer services comparable to those offered by Google.

22.1 POLICIES

22.1.1 GWS.GMAIL.22.1v0.1

Word lists SHOULD be enabled to filter objectionable content within Gmail messages.

- Rationale: This helps ensure that confidential/sensitive information can be filtered from Gmail messages to help prevent unauthorized or accidental sharing.
- Last Modified: July 10, 2023

22.1.2 GWS.GMAIL.22.2v0.1

Any third-party or outside application selected for objectionable content filtering SHOULD offer services comparable to those offered by Google Workspace.

- Rationale: A third-party system should provide the same minimum functionality provided by Google.
- Last Modified: July 10, 2023

22.2 RESOURCES

- Google Workspace Admin Help: Set up rules for objectionable content
- Personally identifiable information (PII) | NIST
- Sensitive information | NIST

22.3 PREREQUISITES

- N/A

22.4 IMPLEMENTATION

To configure the settings for objectionable content:

22.4.1 GWS.GMAIL.22.1v0.1 instructions:

1. Sign into the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.
3. Select **Compliance -> Objectionable content**.
4. If **Objectionable content** filtering is enabled, then the configuration needs to be completed and consists of the following fields:
    1. A short description.
    2. Email messages to affect.
    3. Custom objectionable words.
    4. Compliance action options.
5. Select **Save**.

22.4.2 GWS.GMAIL.22.2v0.1 instructions:

1. This has no implementation steps for this policy.

23. ATTACHMENT COMPLIANCE FILTERING

This section determines whether attachments are filtered based on file type, file name, and message size. The compliance actions based upon the word lists are reject, quarantine, or deliver with modifications.

A Google Workspace solution is not strictly required to satisfy this baseline control, but the solution selected by an agency should offer services comparable to those offered by Google.

23.1 POLICIES

23.1.1 GWS.GMAIL.23.1v0.1

Attachment compliance SHOULD be enabled to filter specific attachments within Gmail messages.

- Rationale: This allows filtering of confidential/sensitive information from Gmail messages stored within specific file attachments to help prevent unauthorized or accidental sharing.
- Last Modified: July 10, 2023

23.1.2 GWS.GMAIL.23.2v0.1

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

- Rationale: This allows filtering of confidential/sensitive information from Gmail messages stored within specific file attachments to help prevent unauthorized or accidental sharing.
- Last Modified: July 10, 2023

23.1.3 GWS.GMAIL.23.3v0.1

The set of disallowed file types SHALL be determined.

- Rationale: This allows filtering of confidential/sensitive information from Gmail messages stored within specific file attachments to help prevent unauthorized or accidental sharing. This also helps protect the organization from attacks based on specific file types.
- Last Modified: July 10, 2023

23.1.4 GWS.GMAIL.23.4v0.1

Any third-party or outside application selected for attachment compliance filtering SHOULD offer services comparable to those offered by Google Workspace.

- Rationale: A third-party system should provide the same minimum functionality provided by Google.
- Last Modified: July 10, 2023

23.2 RESOURCES

- Google Workspace Admin Help: Content filtering with rules

23.3 PREREQUISITES

- N/A

23.4 IMPLEMENTATION

To configure the settings for Attachment Compliance:

23.4.1 GWS.GMAIL.23.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Gmail**.

3. Select **Compliance -> Attachment compliance**.
4. If **Attachment compliance** filtering is enabled, then the configuration needs to be completed and consists of the following fields:
    1. A short description.
    2. Email messages to affect.
    3. Expressions for content to search for in messages.
    4. Compliance action options.
5. Select **Save**.

23.4.2 GWS.GMAIL.23.2v0.1 instructions:

1. There are no implementation steps for this policy

23.4.3 GWS.GMAIL.23.3v0.1 instructions:

1. There are no implementation steps for this policy

23.4.4 GWS.GMAIL.23.4v0.1 instructions:

1. There are no implementation steps for this policy