CIS Benchmarks

CIS Google Workspace Foundations

v1.0.0 - 01-29-2021

Terms of Use

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

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

Table of Contents

Terms of Use ... 1

Overview ... 5

Intended Audience ... 5

Consensus Guidance ... 5

Typographical Conventions ... 6

Assessment Status ... 6

Profile Definitions ... 7

Acknowledgements ... 8

Recommendations ... 9

1 Account / Authentication ... 9

1.1 (L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles (Manual) ... 9

1.2 (L2) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users (Manual) ... 12

1.3 (L2) Ensure Advanced Protection Program is configured (Manual) ... 14

1.4 (L1) Ensure password policy is configured for enhanced security (Manual) .. 17

1.5 (L2) Ensure login challenges are enforced (Manual) ... 20

1.6 (L1) Ensure Google session control is configured (Manual) ... 22

1.7 (L2) Ensure Google Cloud session control (Beta) is configured (Manual) ... 24

2 Application Permissions ... 26

2.1 (L1) Ensure less secure app access is disabled (Manual) ... 26

2.2 (L1) Ensure directory data access is externally restricted (Manual) ... 28

2.3 (L2) Ensure application access to Google services is restricted (Manual) ... 31

2.4 (L2) Review third-party applications periodically (Manual) ... 33

2.5 (L2) Review domain-wide delegation for applications periodically (Manual) 35

3 Calendar ... 37

3.1 (L1) Ensure external sharing options for primary calendars are configured (Manual) ... 37

3.2 (L1) Ensure external invitation warnings for Google Calendar are configured (Manual) ... 39

3.3 (L1) Ensure external sharing options for secondary calendars are configured (Manual) 41

4 Drive and Docs 43

4.1 (L1) Ensure DLP policies for Google Drive are configured (Manual) 43

4.2 (L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted (Manual) 46

4.3 (L1) Ensure only users inside your organization can distribute content externally (Manual) 48

4.4 (L2) Ensure document sharing is being controlled by domain with allow-lists (Manual) 50

4.5 (L1) Ensure users can create new shared drives (Manual) 52

4.6 (L1) Ensure full-access members cannot modify shared drive settings (Manual) 54

4.7 (L1) Ensure shared drive file access is restricted to members only (Manual) 56

4.8 (L1) Ensure link sharing default settings are configured (Manual) 58

5 Gmail 60

5.1 (L1) Ensure users cannot delegate access to their mailbox (Manual) 60

5.2 (L1) Ensure Gmail labs is not enabled (Manual) 62

5.3 (L1) Ensure that DKIM is enabled for all mail enabled domains (Manual) 64

5.4 (L1) Enable quarantine admin notifications for Gmail (Manual) 66

5.5 (L1) Ensure protection against encrypted attachments from untrusted senders is enabled (Manual) 68

5.6 (L1) Ensure protection against attachments with scripts from untrusted senders is enabled (Manual) 70

5.7 (L1) Ensure protection against anomalous attachment types in emails is enabled (Manual) 72

5.8 (L1) Ensure link identification behind shortened URLs is enabled (Manual) . 74

5.9 (L1) Ensure scan linked images for malicious content is enabled (Manual) ... 76

5.10 (L1) Ensure warning prompt is shown for any click on links to untrusted domains (Manual) 78

5.11 (L1) Ensure protection against domain spoofing based on similar domain names is enabled (Manual) 80

5.12 (L1) Ensure protection against spoofing of employee names is enabled (Manual) 82
5.13 (L1) Ensure protection against inbound emails spoofing your domain is enabled (Manual) 84
5.14 (L1) Ensure protection against any unauthenticated emails is enabled (Manual) 86
5.15 (L1) Ensure groups are protected from inbound emails spoofing your domain (Manual) 88
5.16 (L2) Ensure POP and IMAP access is disabled for all users (Manual) 90
5.17 (L2) Ensure automatic forwarding options are disabled (Manual) 92
5.18 (L1) Ensure per-user outbound gateways is disabled (Manual) 94
Appendix: Summary Table 96
Appendix: Change History 99

Overview

This document, Security Configuration Benchmark for Google Workspace, provides prescriptive guidance for establishing a secure configuration posture for Google Workspace running on any OS. This guide was tested against Google Workspace Enterprise, and includes recommendations for Gmail, Drive and Docs, Calendar, Accounts, and Applications. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

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

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Enterprise Level 1**

  Items in this profile apply to customer deployments of Google Workspace with an Enterprise license and intend to:

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

- **Enterprise Level 2**

  This profile extends the "Enterprise Level 1" profile. Items in this profile exhibit one or more of the following characteristics and is focused on customer deployments of Google Workspace Enterprise:

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

Acknowledgements

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

Author
Wacey Lanier, SecureSky

Contributor
Iulia Ion, Google

Editor
Phil White, Center for Internet Security

Recommendations

1 Account / Authentication

1.1 (L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Enforce 2-Step Verification (Multi-Factor Authentication) for all users assigned administrative roles. These include roles such as:

- Help Desk Admin
- Groups Admin
- Super Admin
- Services Admin
- User Management Admin
- Mobile Admin
- Android Admin
- Custom Admin Roles

Rationale:

Add an extra layer of security to users accounts by asking users to verify their identity when they enter a username and password. 2-Step Verification (Multi-factor authentication) requires an individual to present a minimum of two separate forms of authentication before access is granted. 2-Step Verification provides additional assurance that the individual attempting to gain access is who they claim to be. With 2-Step Verification, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact:

Implementation of 2-Step Verification (multi-factor authentication) for all users in administrative roles will necessitate a change to user routine. All users in administrative roles will be required to enroll in 2-Step Verification using using phone, SMS, or an authentication application. After enrollment, use of 2-Step Verification will be required for future access to the environment.

Audit:

To verify the 2-Step Verification (multi-factor authentication) configuration for administrators, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Go to `Security` and click on `2-Step Verification`
3. Select the appropriate group with `ALL ADMIN ROLES` -- Create this group if needed
4. Under `Authentication`, ensure `Allow users to turn on 2-Step Verification` is `checked`
5. Ensure `Enforcement` is set to `On`
6. Ensure `New user enrollment period` is set to `2 weeks`
7. Under `Frequency`, ensure `Allow user to trust device` is `not checked`
8. Under `Methods`, ensure `Any except verification codes via text, phone call` is `selected`

Remediation:

To enforce 2-Step Verification (multi-factor authentication) configuration for administrators, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Go to `Security` and click on `2-Step Verification`
3. Select the appropriate group with `ALL ADMIN ROLES` -- Create this group if needed
4. Under `Authentication`, set `Allow users to turn on 2-Step Verification` to `checked`
5. Set `Enforcement` to `On`
6. Set `New user enrollment period` is set to `2 weeks`
7. Under `Frequency`, set `Allow user to trust device` to `not checked`
8. Under `Methods`, set `Any except verification codes via text, phone call` to `selected`

Default Value:

- `Allow users to turn on 2-Step Verification` = `checked`
- `Enforcement` = `Off`
- `New user enrollment period` = `None`
- `Frequency`, `Allow user to trust device` = `checked`
- `Methods` = `Any`

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

1.2 (L2) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Enforce 2-Step Verification (Multi-Factor Authentication) for all users.

Rationale:

Add an extra layer of security to users accounts by asking users to verify their identity when they enter a username and password. 2-Step Verification (Multi-factor authentication) requires an individual to present a minimum of two separate forms of authentication before access is granted. 2-Step Verification provides additional assurance that the individual attempting to gain access is who they claim to be. With 2-Step Verification, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact:

Implementation of 2-Step Verification (multi-factor authentication) for all users will necessitate a change to user routine. All users will be required to enroll in 2-Step Verification using using phone, SMS, or an authentication application. After enrollment, use of 2-Step Verification will be required for future access to the environment.

Audit:

To verify the 2-Step Verification (multi-factor authentication) configuration for all users, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `2-Step Verification`
4. Under `Authentication`, ensure `Allow users to turn on 2-Step Verification` is `checked`
5. Ensure `Enforcement` is set to `On`
6. Ensure `New user enrollment period` is set to `2 weeks`
7. Under `Frequency`, ensure `Allow user to trust device` is `not checked`
8. Under `Methods`, ensure `Any except verification codes via text, phone call` is `selected`

Remediation:

To enforce 2-Step Verification (multi-factor authentication) configuration for all users, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `2-Step Verification`
4. Under `Authentication`, check - `Allow users to turn on 2-Step Verification`
5. Set `Enforcement` to `On`
6. Set `New user enrollment period` to `2 weeks`
7. Under `Frequency`, uncheck - `Allow user to trust device`
8. Under `Methods`, select - `Any except verification codes via text, phone call`

Default Value:

- `Allow users to turn on 2-Step Verification` = `checked`
- `Enforcement` = `Off`
- `New user enrollment period` = `None`
- `Frequency`, `Allow user to trust device` = `checked`
- `Methods` = `Any`

CIS Controls:

Version 7

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

1.3 (L2) Ensure Advanced Protection Program is configured (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Enable Google's Advanced Protection Platform for all users and prevent the use of security codes where applicable.

Rationale:

Sophisticated phishing tactics can trick the most savvy users into giving their sign-in credentials to attackers. Advanced Protection requires you to use a security key, which is a hardware device or special software on your phone used to verify your identity, to sign in to your Google Account. Unauthorized users won't be able to sign in without your security key, even if they have your username and password.

The Advanced Protection Program includes a curated group of high-security policies that are applied to enrolled accounts. Additional policies may be added to the Advanced Protection Program to ensure the protections are current.

Advanced Protection allows you to apply all of these protections at once, and override similar settings you may have configured manually. These policies include:

- Strong authentication with security keys
- Use of security codes with security keys (as needed)
- Restrictions on third-party access to account data
- Deep Gmail scans
- Google Safe Browsing protections in Chrome (when users are signed into Chrome using the same identity as their Advanced Protection Program identity)
- Account recovery through admin

Impact:

User Impact

- You need your security key when you sign in for the first time on a computer, browser, or device. If you stay signed in, you may not be asked to use your security key the next time you log in.
- Limits third-party app access to your data, puts stronger checks on suspicious downloads, and tightens account recovery security to help prevent unauthorized access.

Security Keys - 2 Required

- Android: With an Android 7.0+ phone, you can enroll in a few taps by registering your phone's built-in security key.
- iPhone: If you have an iPhone running iOS 10.0+, install the `Google Smart Lock` app to register your security key first, then enroll.
- Two security keys are required for added assurance. If one key is lost or damaged, users can use the second key to regain account access.

Third-Party iDP You can use the Advanced Protection Program with accounts that federate from an IdP using SAML. When users with these accounts enroll in the Advanced Protection Program, we'll require security key use after the user signs in on the IdP. Note that SAML users can select Remember the device to avoid challenges on a browser or device.

Security Codes

- Before allowing users to generate security codes, carefully evaluate if your organization needs them. Using security keys with security codes increases the risk of phishing. However, if your organization has important workflows where security keys can't be used directly, enabling security codes for those situations may help improve your security posture overall.

Using 'Sign in with Google' with other apps and services

- You can still sign into apps and services with Google. If they request access to your Gmail or Drive data, access is denied.

Audit:

To verify Google's Advanced Protection Program is configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Advanced Protection Program`
4. Under `Enrollment - Allow users to enroll in the Advanced Protection Program`, ensure `Enable user enrollment` is `selected` for the desired organizational unit or group
5. Under `Security Codes`, ensure `Do not allow users to generate security codes` is `selected` for the desired organizational unit or group

Remediation:

To configure Google's Advanced Protection Program, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Advanced Protection Program`
4. Under `Enrollment - Allow users to enroll in the Advanced Protection Program`, `select` - `Enable user enrollment` for the desired organizational unit or group
5. Under `Security Codes`, `select` - `Do not allow users to generate security codes` for the desired organizational unit or group

Default Value:

- `Allow users to enroll in the Advanced Protection Platform` = `selected`
- `Security codes` = `Allow security codes without remote access`

CIS Controls:

Version 7

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

1.4 (L1) Ensure password policy is configured for enhanced security (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configure Google Workspace Password Policy with a more secure length and is enforced upon next sign-in to protect against the use of common password attacks.

Rationale:

Strong password policies protect an organization by prohibiting the use of weak passwords.

Impact:

The potential impact associated with implementation of this setting is dependent upon the existing password policies in place in the environment. For environments that have strong password policies in place, the impact will be minimal. For organizations that do not have strong password policies in place, enhancing the password policy may require users to change passwords, and adhere to more stringent requirements than they have been accustomed to.

Audit:

To verify a strong password policy is configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Password management`
4. Under `Strength`, ensure `Enforce strong passwords` is `checked`
5. Under `Length`, ensure `Minimum Length` is set to `12`+
6. Under `Strength and Length enforcement`, ensure `Enforce password policy at next sign-in` is set to `checked`
7. Under `Reuse`, ensure `Allow password reuse` is `not checked`

Optional:
Setting passwords to never expire is recommended ONLY if 2-Step Verification (Multi-Factor Authentication) is ENFORCED

8. Under `Expiration`, ensure `Password reset frequency` is set to `Never expires`

Remediation:

To confiure a strong password policy is configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Password management`
4. Under `Strength`, `check` - `Enforce strong passwords`
5. Under `Length`, set `Minimum Length` to `12`+
6. Under `Strength and Length enforcement`, `check` - `Enforce password policy at next sign-in`
7. Under `Reuse`, `uncheck` - `Allow password reuse`

Optional:
Setting passwords to never expire is recommended ONLY if 2-Step Verification (Multi-Factor Authentication) is ENFORCED

8. Under `Expiration`, set `Password reset frequency` to `Never expires`

Default Value:

- `Enforce strong password` = `checked`
- `Minimum length` = `8`
- `Maximum length` = `100`
- `Enforce password policy at next sign-in` = `not checked`
- `Allow password reuse` = `not checked`
- `Expiration` = `Never expires`

CIS Controls:

Version 7

4.4 Use Unique Passwords

Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.

1.5 (L2) Ensure login challenges are enforced (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Configure Google Workspace to verify a user's identity post-sso.

Rationale:

Many organizations use third-party identity providers (IdPs) to authenticate users who use single sign on (SSO) through SAML. The third-party IdP authenticates users and no additional risk-based challenges are presented to them. Any Google 2-Step Verification (2SV) configuration is ignored. This is the default behavior. You can set a policy to allow additional risk-based authentication challenges and 2SV if it's configured. If Google receives a valid SAML assertion (authentication information about the user) from the IdP during user sign-in, Google can present additional challenges to the user.

Login challenges requires users have a recovery phone number or email account associated with their organizational account. If not previously configured, users will be prompted to enter this information periodically until provided.

One login challenge option prompts users to enter their employee ID. This method is susceptible to information gathering attacks, should a list of employee IDs ever be leaked.

Impact:

The potential impact associated with implementation of this setting is dependent upon the existing 2-Step Verification (2SV) polices.

- If you have existing 2SV policies, such as 2SV enforcement, those policies apply immediately.
- Users affected by the new policy and who are enrolled in 2SV get a 2SV challenge at sign-in.
- Based on Google sign-in risk analysis, users might see risk-based challenges at sign-in.

Audit:

To verify login challenges are configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Login Challenges`
4. Under `Post-SSO verification`, ensure `Logins using SSO are subject to additional verifications (if appropriate) and 2-Step Verification (if configured)` is `checked`
5. Under `Login challenges`, ensure `Use employee ID to keep my users more secure` is `Not-Checked`

Remediation:

To configure login challenges, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Login Challenges`
4. Under `Post-SSO verification`, `Select` - `Logins using SSO are subject to additional verifications (if appropriate) and 2-Step Verification (if configured)`
5. Under `Login challenges`, `Un-Check` - `Use employee ID to keep my users more secure`

Default Value:

- `Post-SSO verification` = `Logins using SSO bypass additional verifications`
- `Use employee ID to keep my users more secure` = `Not-Checked`

CIS Controls:

Version 7

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

1.6 (L1) Ensure Google session control is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configure Google Workspace's session control to strengthen session expiration.

Rationale:

As an administrator, you can control how long users can access Google services, such as Gmail on the web, without having to sign in again. For example, for users that work remotely or from untrusted locations, you might want to limit the time that they can access sensitive resources by applying a shorter web session length. If users want to continue accessing a resource when a session ends, they're prompted to sign in again and start a new session.

How the settings work on mobile devices varies by device and app.

Impact:

The potential impact associated with implementation of this setting are:

- When a web session expires for a user, they see the Verify it's you page and must sign in again.
- When you change the session length, users need to sign out and in again for settings to take effect.
- If you set the session to never expire, users never have to sign in again.
- If you need some users to sign in more frequently than others, place them in different organizational units. Then, apply different session lengths to them. That way, certain users won't be interrupted to sign in when it isn't necessary.
- If a Google Meet meeting starts within 2 hours of a session's scheduled expiration, the user is forced to sign in again before the start of the meeting. This helps avoid an interruption to the meeting while in-progress.
- If you're using a third-party identity provider (IdP), such as Okta or Ping, and you set web session lengths for your users, you need to set the IdP session length parameter to expire before the Google session expires. That way, your users will be forced to sign in again. If the third-party IdP session is still valid when the Google session expires, the Google session might be renewed automatically without the user signing in again.

Audit:

To verify Google session control is configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Google session control`
4. Under `Web session duration`, ensure the duration is set to less than or equal to `12 hours`

Remediation:

To configure Google session control, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Google session control`
4. Under `Web session duration`, set the duration to less than or Equal to `12 hours`

Default Value:

- `Web session duration` = `14 days`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.7 (L2) Ensure Google Cloud session control (Beta) is configured (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Configure Google cloud session control to strengthen session expiration.

Rationale:

As an administrator, you can control how long different users can access the Google Cloud Platform (GCP) Console and Cloud SDK without having to sign in again. For example, for users that work remotely, you might want to limit the time that they can access sensitive resources. If you set a session length, they're prompted to sign in again to start a new session.

Impact:

The potential impact associated with implementation of this setting are:

- When a Google cloud session expires for a user, they see the Verify it's you page and must sign in again.
- If you require a security key, users who do not have one cannot use the GCP Console or Cloud SDK until they set it up. Once they have a security key, they can switch to using their password instead if they want. **If you're using a third-party identity provider (IdP):**
- With the GCP Console—If you require a user to sign in again using their password, they're redirected to the IdP for signing in.The IdP might not require the user to re-enter their password to start another GCP Console session. Therefore, we recommend that you set short session lengths when you use a third-party IdP. If a user must sign in again by touching their security key, they can do this in the GCP Console. They will not be redirected to the IdP.
- With the Cloud SDK—If you require a user to sign in again using their password, they will not be redirected to the IdP. To sign in again, they enter the gcloud auth login command and then complete the authentication with the IdP. If a user must sign in again by touching their security key, they can do this on the Cloud SDK. They will not be redirected to the IdP.

Audit:

To verify Google Cloud session control (Beta) is configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Google Cloud session control (Beta)`
4. Under `Session duration`, ensure `Set session duration` is `Selected` and set to `12 hours`

Remediation:

To configure Google Cloud session control (Beta), use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Google Cloud session control (Beta)`
4. Under `Session duration`, `Select` - `Set session duration`
5. Under `Set session duration`, set the timeout to `12 hours`

Default Value:

- `Session duration` = `Session never expires`
- `Set session duration` = `1 hour` *(if \ when selected)*
- `Re-authentication method` = `Password`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2 Application Permissions

2.1 (L1) Ensure less secure app access is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configure Google Workspace security settings to prevent access to less secure apps.

Rationale:

You can block sign-in attempts from some apps or devices that are less secure. Apps that are less secure don't use modern security standards, such as OAuth. Using apps and devices that don't use modern security standards increases the risk of accounts being compromised. Blocking these apps and devices helps keep your users and data safe.

Impact:

The potential impact associated with implementation of this setting is that users won't be able to turn on access to less secure apps. When you disable access to less secure apps while a less secure app has an open connection with a user account, the app will time out when it tries to refresh the connection. Timeout periods vary per app.

Audit:

To verify less secure app access is disabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Less secure apps`
4. Ensure `Disable access to less secure apps (Recommended)` is `selected`

Remediation:

To disable less secure app access, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Less secure apps`
4. Select `Disable access to less secure apps (Recommended)`
5. Click `Save` to commit this configuration change.

Default Value:

- `Disable access to less secure apps (Recommended)` = `Selected`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.2 (L1) Ensure directory data access is externally restricted (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configure Google Workspace's external directory sharing to prevent unrestricted directory data access.

Rationale:

If your organization uses third-party apps that integrate with your Google services, you control how much Directory information the external apps can access.

If you allow directory access, your users have a better experience with external apps. For example, when they use a third-party mail app, they want to find domain contacts and have email addresses automatically complete. The app needs access to Directory data to make this happen. However, this has the ability to share ALL domain AND public data with the connected third-party app.

- Public data and authenticated user basic profile fields — Share publicly visible domain profile data with external apps and APIs. Also share the authenticated user's name, photo, and email address to enable Google Sign-In if the appropriate scopes are granted. Other non-public profile fields for the authenticated user aren't shared. All the non-public profile information of other users in the domain aren't shared.
- Domain and public data — (Default) Share all Directory information that's shared with your domain and public data. This information includes profile information for users in your domain, shared external contacts, and Google+ profile names and photos.

Impact:

The External directory sharing setting applies only to the following APIs and the Apps Scripts or third-party Marketplace apps that use those APIs:

- Google People API
- Google CardDAV API
- Google Contacts API v3

The setting applies only to third-party apps, such as iOS Mail and iOS Contacts (when enrolled on an iOS device via Add Account and then Google), third-party Contacts apps (on Android).

The setting doesn't apply to Google products, including mobile apps, such as the following

- Gmail, Contacts (on Android), Inbox, Meet, and other Google mobile apps
- iOS Mail and iOS Contacts using Google Sync (when enrolled on an iOS device through Add Account and then Exchange)
- Workspace Sync for Microsoft Outlook

Audit:

To verify directory data access is externally restricted, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Open the collapsed menu via "hamburger button \ 3 horizontal lines"
3. Under `Directory`, select `Directory settings`
4. Under `Sharing settings`, select `External Directory sharing`
5. Ensure `Domain and public data` is `not selected`

Remediation:

To externally restrict directory data access, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Open the collapsed menu via "hamburger button \ 3 horizontal lines"
3. Under `Directory`, select `Directory settings`
4. Under `Sharing settings`, select `External Directory sharing`
5. Select `Public data and authenticated user basic profile fields`

Default Value:

- `External Directory sharing` = `Domain and public data`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.3 (L2) Ensure application access to Google services is restricted (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Prevent unrestricted application access to Google services.

Rationale:

You can restrict (or leave unrestricted) access to most Workspace services, including Google Cloud Platform services such as Machine Learning. For Gmail and Google Drive, you can specifically restrict access to high-risk scopes (for example, sending Gmail or deleting files in Drive). While users are prompted to consent to apps, if an app uses restricted scopes and you haven't specifically trusted it, users can't add it.

Impact:

The potential impact associated with implementation of this setting is that any previously installed apps that you haven't trusted stop working and tokens are revoked. When a user tries to install an app that has a restricted scope, they're notified that it's blocked.

Audit:

To verify application access to Google services is restricted, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `API Controls`, then select `App access control`
4. Under `Overview`, select `MANAGE GOOGLE SERVICES`
5. Ensure `ALL` applicable Google Services have `Restricted` in the `Access` column

Remediation:

To restrict application access to Google services, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `API Controls`, then select `App access control`
4. Under `Overview`, select `MANAGE GOOGLE SERVICES`
5. Select `ALL` applicable Google Services
6. Click `Change access`
7. Select `Restricted: Only trusted apps can access a service`

Default Value:

- `Access` = `Unrestricted`

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

2.4 (L2) Review third-party applications periodically (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Periodically review connected applications for potential malicious or unintended access or connections.

Rationale:

Performing a periodic review of connected applications and their permission scopes ensures only permitted and required applications can access organizational data or resources. Attackers commonly attempt to persuade or trick users to grant their application access to organizational data resources by asking for their consent.

Audit:

To view third-party application connections, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `API Controls`, then select `App access control`
4. Under `Overview`, select `MANAGE THIRD-PARTY APP ACCESS`
5. Ensure all listed applications have been properly vetted and authorized by the appropriate personnel

Remediation:

To remove third-party application connections, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `API Controls`, then select `App access control`
4. Under `Overview`, select `MANAGE THIRD-PARTY APP ACCESS`
5. Select `Change Access` for the application you wish to remove
6. Select `Blocked: Can't access any Google service`
7. Log in to the Google Clout Platform - Resource Manager `https://console.cloud.google.com/cloud-resource-manager` as an administrator
8. Now `Delete` the desired application

CIS Controls:

Version 7

2.1 Maintain Inventory of Authorized Software
Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.

2.6 Address unapproved software
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

2.5 (L2) Review domain-wide delegation for applications periodically (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Periodically review domain-wide delegations for applications for potential malicious or unintended access or connections.

Rationale:

Domain-wide delegation is a powerful feature that allows apps to access users' data across your organization's entire Workspace account. Performing a periodic review of domain-wide delegations for applications and their permission scopes ensures only permitted and required applications can access organizational data or resources.

Audit:

To view domain-wide delegation for applications, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `API Controls`, then select `App access control`
4. Under `Domain wide delegation`, select `MANAGE DOMAIN WIDE DELEGATION`
5. Ensure all listed applications have been properly vetted and authorized by the appropriate personnel

Remediation:

To remove third-party application connections, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `API Controls`, then select `App access control`
4. Under `Domain wide delegation`, select `MANAGE DOMAIN WIDE DELEGATION`
5. Select `Change Access` for the application you wish to remove
6. Now `Delete` the desired application

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3 Calendar

3.1 (L1) Ensure external sharing options for primary calendars are configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Control how much calendar information users in your organization can share externally.

Rationale:

Prevent data leakage by restricting the amount of information that is externally viewable when a user shares their calendar with someone external to your organization.

Impact:

- Once you limit external sharing for your organization, users can't exceed these limits when sharing individual events. For example, if you limit your organization's external sharing to Free/Busy, events with Public visibility are only shared as Free/Busy.
- External mobile users who previously synced events may keep seeing restricted details. That access stops when their device is wiped and re-synced.
- If you lower the external sharing level, people outside your organization may lose access to calendars they could previously see.

Audit:

To verify external sharing options for primary calendars are configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Calendar`
5. Under `Sharing settings`, select `External sharing options for primary calendars`
6. Ensure `Only free/busy information (hide event details)` is `selected`

Remediation:

To configure external sharing options for primary calendars, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Calendar`
5. Under `Sharing settings`, select `External sharing options for primary calendars`
6. Select `Only free/busy information (hide event details)`

Default Value:

- `External sharing options for primary calendars` = `Only free/busy information (hide event details)`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.2 (L1) Ensure external invitation warnings for Google Calendar are configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configure Google Calendar to warn users when inviting guest outside your domain.

Rationale:

When your users create a Google Calendar event that includes one or more guests from outside of your domain, they are prompted to confirm whether it's OK to include external guests in the event invitation, assisting in the prevention of unintentional data leakage.

Impact:

Users will be prompted to allow the inclusion of external guests in an event invitation.

Audit:

To verify external invitation warnings for Google Calendar are configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Calendar`
5. Under `Sharing settings`, select `External invitations`
6. Ensure `Warn users when inviting guests outside of the domain` is `checked`

Remediation:

To configure external invitation warnings for Google Calendar, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Calendar`
5. Under `Sharing settings`, select `External Invitations`
6. Check `Warn users when inviting guests outside of the domain`

Default Value:

- `Warn users when inviting guests outside of the domain` = `Checked`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.3 (L1) Ensure external sharing options for secondary calendars are configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Control how much calendar information users in your organization can share externally.

Rationale:

Prevent data leakage by restricting the amount of information is externally viewable when a user shares their calendar with someone external to your organization.

Impact:

- Once you limit external sharing for your organization, users can't exceed these limits when sharing individual events. For example, if you limit your organization's external sharing to Free/Busy, events with Public visibility are only shared as Free/Busy.
- External mobile users who previously synced events may keep seeing restricted details. That access stops when their device is wiped and re-synced. -If you lower the external sharing level, people outside your organization may lose access to calendars they could previously see.

Audit:

To verify external sharing options for secondary calendars are configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Calendar`
5. Under `General settings`, select `External sharing options for secondary calendars`
6. Ensure `Only free/busy information (hide event details)` is `selected`

Remediation:

To configure external sharing options for secondary calendars, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Calendar`
5. Under `General settings`, select `External sharing options for secondary calendars`
6. Select `Only free/busy information (hide event details)`

Default Value:

- `External sharing options for secondary calendars` = `Share all information, but outsiders cannot change calendars`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4 Drive and Docs

4.1 (L1) Ensure DLP policies for Google Drive are configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Enabling Data Loss Prevention (DLP) policies for Google Drive allows organizations to control the content that users can share in Google Drive files outside the organization.

Rationale:

Enabling DLP policies alerts users and administrators that specific types of data should not be exposed, helping to protect the data from accidental exposure. DLP gives you control over what users can share, and prevents unintended exposure of sensitive information such as credit card numbers or identity numbers

Impact:

Configuring a DLP policy for Google Drive will detect or block sensitive information.

Audit:

To verify DLP policies for Google Drive are configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Data protection`
4. Select `Manage Rules`
5. Ensure data protection rules `exist` and are `enabled`

Remediation:

To configure DLP policies for Google Drive, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Data protection`
4. Select `Manage Rules`
5. Select `ADD RULE`, then select either `New rule` or `New rule from template`

New rule

Examples can be found at *`https://support.google.com/a/answer/9655387?hl=en&ref_topic=9646660#zippy=%2Cplan-and-then-create-rules%2Cexample-protect-social-security-numbers-using-a-predefined-classifier`*

1. Set the rule `Name`
2. Optionally - Set the rule `Description`
3. Set the `Scope` as appropriate
4. Select `Continue`
5. Set `Triggers` by `checking` - `File modified` under `Google Drive`
6. Select `ADD CONDITION` and configure values (`Field`, `Comparison Operator`, `Content to match`) - *Repeat as appropriate*
7. Select `Continue`
8. Under `Actions`, select the desired action to take for each incident
9. Under `Alerting`, select the desired severity level
10. Under `Alerting`, `Select` - `Send to alert center`
11. Select `Continue`
12. Select `Create`

New rule from template

1. Select the desired rule template
2. Optionally set the `Name` as desired
3. Optionally set the `Description as desired
4. Set the `Scope` as appropriate
5. Select `Continue`
6. Modify preconfigured `Conditions` as desired, or add additional conditions
7. Select `Continue`
8. Under `Alerting`, `Select` - `Send to alert center`
9. Select `Continue`
10. Select `Create`

Default Value:

No DLP policies for Google Drive are configured by default

CIS Controls:

Version 7

13 Data Protection
Data Protection

14.7 Enforce Access Control to Data through Automated Tools
Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.

4.2 (L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

You should control the publishing of documents to the web or making them visable to the world as public or unlisted.

Rationale:

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

This setting is only applicable if `ON - Files owned by users in <Company> can be shared outside of <Company>. This applies to files in all shared drives as well` is `selected`, but should be configured as described below to prevent unintentional document publishing.

Impact:

Enabling this feature will prevent users from publishing documents on the web or making them visible to the world as public or unlisted files.

Audit:

To verify users cannot publish files to the web or make visible to the world as public or unlisted, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Sharing settings`, select `Sharing options`
6. Under `Sharing outside of <Company>` - `ON - Files owned by users in <Company> can be shared outside of <Company>. This applies to files in all shared drives as well`, ensure `Allow users in <Company> to publish files on the web or make them visible to the world as public or unlisted files` is `unchecked`

Remediation:

To control how users publish files to the web or make visible to the world as public or unlisted, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Sharing settings`, select `Sharing options`
6. Under `Sharing outside of <Company>` - `ON - Files owned by users in <Company> can be shared outside of <Company>. This applies to files in all shared drives as well`, uncheck - `Allow users in <Company> to publish files on the web or make them visible to the world as public or unlisted files`

Default Value:

- `Allow users in <Company> to publish files on the web or make them visible to the world as public or unlisted files` = `Checked`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.3 (L1) Ensure only users inside your organization can distribute content externally (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

You should control who is allowed to distribute organizational content to shared drives owned by another organization.

Rationale:

Sharing and collaboration are key; however, only your users should have the authority over where company content is shared with to prevent unauthorized disclosures of information.

Impact:

Only people in your organization with Manager access to a shared drive can move files from that shared drive to a Drive location in a different organization.

In addition, users in the selected organizational unit or group can copy content from their My Drive to a shared drive owned by a different organization.

Audit:

To verify users cannot publish files to the web or make visible to the world as public or unlisted, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Sharing settings`, select `Sharing options`
6. Under `Distributing content outside of <Company>`, ensure `Only users in <Company>` is `selected`

Remediation:

To control how users publish files to the web or make visible to the world as public or unlisted, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Sharing settings`, select `Sharing options`
6. Under `Distributing content outside of <Company>`, `select` - `Only users in <Company>`

Default Value:

- `Distributing content outside of <Company>` = `Anyone`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.4 (L2) Ensure document sharing is being controlled by domain with allow-lists (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

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

Rationale:

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

Impact:

Enabling this feature will prevent users from sharing documents with domains outside of the organization unless allowed.

Audit:

To verify document sharing is being controlled by domain with allow-lists, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Sharing settings`, select `Sharing options`
6. Under `Sharing outside of <Company>`, ensure `WHITELISTED DOMAINS - Files owned by users in <Company> can be shared with Google accounts in compatible whitelisted domains. This applies to files in all shared drives as well` is `selected`
7. Ensure `For files owned by users in <Company>, warn when sharing with users in whitelisted domains` is `checked`

All other options under `Sharing outside of <Company>` are `Optional`

Remediation:

To control document sharing by domain with allow-lists, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Sharing settings`, select `Sharing options`
6. Under `Sharing outside of <Company>`, `select` - `WHITELISTED DOMAINS - Files owned by users in <Company> can be shared with Google accounts in compatible whitelisted domains. This applies to files in all shared drives as well`
7. Check `For files owned by users in <Company>, warn when sharing with users in whitelisted domains`

All other options under `Sharing outside of <Company>` are `Optional`

Default Value:

- `Sharing outside of <Company>` = `WHITELISTED DOMAINS - Files owned by users in <Company> can be shared with Google accounts in compatible whitelisted domains. This applies to files in all shared drives as well`
- `For files owned by users in <Company>, warn when sharing with users in whitelisted domains` = `Checked`

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

4.5 (L1) Ensure users can create new shared drives (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

All users should have the ability to create new shared drives.

Rationale:

By default, when a user account is deleted all the data in their personal drive is deleted as well. By allowing any user to create new shared drives aids in preventing data loss when user accounts are deleted.

Impact:

Disabling this feature will prevent users from creating new shared drives.

Audit:

To verify users can create new shared drives, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Sharing settings`, select `Sharing options`
6. Under `Shared drive creation`, ensure `Prevent users in <Company> from creating new shared drives` is `un-checked`

Remediation:

To ensure users can create new shared drives, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Sharing settings`, select `Sharing options`
6. Under `Shared drive creation`, `un-check` - `Prevent users in <Company> from creating new shared drives`

Default Value:

- `Prevent users in <Company> from creating new shared drives` = `not-checked`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.6 (L1) Ensure full-access members cannot modify shared drive settings (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Only administrators should be able to modify shared drive settings.

Rationale:

Allowing full-access members to override or modify shared drive settings can allow intentional and unintentional data access by unauthorized users.

Impact:

Enabling this feature will prevent full-access members from modifying shared drive settings, requiring administrators to perform settings modifications as required.

Audit:

To verify full-access members cannot modify shared drive settings, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Shared drive creation`, ensure `Prevent full-access members from modifying shared drive settings` is `checked`

Remediation:

To prevent full-access members from modifying shared drive settings, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Shared drive creation`, `check` - `Prevent full-access members from modifying shared drive settings`

Default Value:

- `Prevent full-access members from modifying shared drive settings` = `Unchecked`

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.7 (L1) Ensure shared drive file access is restricted to members only (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Shared drive file access should be restricted to that shared drive's members

Rationale:

Preventing unauthorized users from access sensitive data is paramount in preventing unauthorized or unintentional information disclosures.

Impact:

Enabling this feature will prevent shared drive non-members from access content in shared drives where they are not a member.

Audit:

To verify shared drive file access is restricted to members only, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Shared drive creation`, ensure `Prevent non-members of the shared drive from accessing files in the shared drive` is `checked`

Remediation:

To restrict shared drive file access to members only, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Shared drive creation`, check - `Prevent non-members of the shared drive from accessing files in the shared drive`

Default Value:

- `Prevent non-members of the shared drive from accessing files in the shared drive` = `Unchecked`

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

4.8 (L1) Ensure link sharing default settings are configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Only the owner of a file should have access of a newly created file by default.

Rationale:

Preventing unauthorized users from access sensitive data is paramount in preventing unauthorized or unintentional information disclosures. If the default link sharing setting allows any user with or without the link to access the newly created file, there is a good chance an unauthorized users may access content of which they are not permitted.

Impact:

Enabling this feature will configured the default link sharing settings to prevent other users from accessing or seeing a newly created file until he or she shares it.

Audit:

To verify link sharing default settings are configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Link Sharing`, ensure `OFF` is `selected`

Remediation:

To configure link sharing default settings, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Drive and Docs`
5. Under `Link Sharing`, `select` - `OFF`

Default Value:

- `Link Sharing Defaults` = `OFF`

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists
Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

5 Gmail

5.1 (L1) Ensure users cannot delegate access to their mailbox (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Mail delegation allows the delegate to read, send, and delete messages on their behalf. For example, a manager can delegate Gmail access to another person in their organization, such as an administrative assistant.

Rationale:

Only administrators should be able to delegate access to a user's mailboxes.

Impact:

Existing delegations will be hidden, when this feature is disabled.

Audit:

To verify users cannot delegate access to their mailbox, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `User Settings` - `Mail delegation`, ensure `Let users delegate access to their mailbox to other users in the domain` is `not checked`

Remediation:

To prevent users from delegating access to their mailbox, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `User Settings` - `Mail delegation`, `uncheck` - `Let users delegate access to their mailbox to other users in the domain`

Default Value:

- `Let users delegate access to their mailbox to other users in the domain` = `unchecked`

CIS Controls:

Version 7

14.6 Protect Information through Access Control Lists

Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

5.2 (L1) Ensure Gmail labs is not enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Gmail Labs allows your users to try out experimental new features in Gmail.

Rationale:

Experimental features may contain undiscovered security flaws and can enable attackers to exploit these features.

Impact:

Users will no longer have "Alpha" or "Beta" features available to them in classic Gmail.

Audit:

To verify Gmail labs is not enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Labs`, ensure `Enable Gmail Labs for my users` is `not checked`

Remediation:

To disable Gmail labs, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Labs`, `uncheck` - `Enable Gmail Labs for my users`

Default Value:

- `Enable Gmail Labs for my users` = `checked`

CIS Controls:

Version 7

2.6 Address unapproved software
Ensure that unauthorized software is either removed or the inventory is updated in a timely manner

5.3 (L1) Ensure that DKIM is enabled for all mail enabled domains (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

DKIM adds an encrypted signature to the header of all outgoing messages. Email servers that get signed messages use DKIM to decrypt the message header, and verify the message was not changed after it was sent.

Rationale:

Spoofing is a common unauthorized use of email, so some email servers require DKIM to prevent email spoofing.

Impact:

There should be no impact of setting up DKIM however, organizations should ensure appropriate setup to ensure continuous mail-flow.

Audit:

To verify DKIM is enabled for all mail enabled domains, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Authenticate email`, ensure a DKIM record exists for each mail enabled domain

Remediation:

To enable DKIM for all mail enabled domains, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Authenticate email`, `select` - `Generate new record`
6. Under `Select DKIM key bit length`, select the appropriate `key bit length` *2048 is recommended if supported*
7. Under `Prefix selector (optional)`, enter the appropriate prefix selector
8. Use the text at TXT record value to update the DNS record at your domain host
9. Select `Start Authentication`

Default Value:

`None`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.4 (L1) Enable quarantine admin notifications for Gmail (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Quarantines can help prevent spam, minimize data loss, and protect confidential information. They can also help moderate message attachments so users don't send, open, or click something they shouldn't.

Rationale:

Admins should be notified periodically when messages are quarantined so they can take the appropriate actions.

Impact:

Admins will begin receiving quarantine notifications as emails are quarantined.

Audit:

To verify quarantine admin notifications for Gmail is configured, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Manage quarantines`, ensure each quarantine has `Notify periodically when messages are quarantined` - `checked`

Remediation:

To configure quarantine admin notifications for Gmail, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Manage quarantines`, check - `Notify periodically when messages are quarantined`

As required, give appropriate users the `Access Admin Quarantine` and\or `Access restricted quarantine` roles

Default Value:

- `Notify periodically when messages are quarantined` = `not-checked`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.5 (L1) Ensure protection against encrypted attachments from untrusted senders is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

As a Google Workspace administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected.

Rationale:

You should protect your users from potentially malicious attachments.

Impact:

Users will be warned when they receive an encrypted attachment from an untrusted sender.

Audit:

To verify protection against encrypted attachments from untrusted senders in enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Attachments`, ensure `Protect against encrypted attachments from untrusted senders` is `checked`

Remediation:

To configure protection against encrypted attachments from untrusted senders, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Attachments`, check - `Protect against encrypted attachments from untrusted senders`

Default Value:

- `Protect against encrypted attachments from untrusted senders` = `checked`

CIS Controls:

Version 7

7.9 Block Unnecessary File Types
Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.

5.6 (L1) Ensure protection against attachments with scripts from untrusted senders is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

As a Google Workspace administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected.

Rationale:

You should protect your users from potentially malicious attachments.

Impact:

Users will be warned when they receive an attachments with scripts from an untrusted sender.

Audit:

To verify protection against attachments with scripts from untrusted senders is enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Attachments`, ensure `Protect against attachments with scripts from untrusted senders` is `checked`

Remediation:

To configure protection against attachments with scripts from untrusted senders, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Attachments`, check - `Protect against attachments with scripts from untrusted senders`

Default Value:

- `Protect against attachments with scripts from untrusted senders is enabled` = `checked`

CIS Controls:

Version 7

7.9 Block Unnecessary File Types
Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.

5.7 (L1) Ensure protection against anomalous attachment types in emails is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

As a Google Workspace administrator, you can protect incoming mail against phishing and harmful software (malware). You can also choose what action to take based on the type of threat detected.

Rationale:

You should protect your users from potentially malicious attachments.

Impact:

Users will be warned when they receive an anomalous attachment.

Audit:

To verify protection against anomalous attachment types in emails is enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Attachments`, ensure `Protect against anomalous attachment types in emails` is `checked`

Remediation:

To configure protection against anomalous attachment types in emails, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Attachments`, `check` - `Protect against anomalous attachment types in emails`

Default Value:

- `Protect against anomalous attachment types in emails` = `checked`

CIS Controls:

Version 7

7.9 Block Unnecessary File Types
Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.

5.8 (L1) Ensure link identification behind shortened URLs is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Identify links behind short URLs, and display a warning when you click links to untrusted domains.

Rationale:

You should protect your users from potentially malicious links.

Impact:

Users will be warned when they click links to untrusted domains.

Audit:

To verify link identification behind shortened URLs is enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Links and external images`, ensure `Identify links behind shortened URLs` is `checked`

Remediation:

To configure link identification behind shortened URLs, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Links and external images`, `check` - `Identify links behind shortened URLs`

Default Value:

- `Identify links behind shortened URLs` = `checked`

CIS Controls:

Version 7

7.4 Maintain and Enforce Network-Based URL Filters
Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

5.9 (L1) Ensure scan linked images for malicious content is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Scan linked images for malicious content, and display a warning when you click links to untrusted domains.

Rationale:

You should protect your users from potentially malicious links.

Impact:

Users will be warned when they click links to untrusted domains.

Audit:

To verify scan linked images is enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Links and external images`, ensure `Scan linked images` is `checked`

Remediation:

To configure scan linked images, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Links and external images`, `check` - `Scan linked images`

Default Value:

- `Scan linked images` = `checked`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.10 (L1) Ensure warning prompt is shown for any click on links to untrusted domains (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Display a warning when you click links to untrusted domains.

Rationale:

You should protect your users from potentially malicious links.

Impact:

Users will be warned when they click links to untrusted domains.

Audit:

To verify warning prompt is shown for any click on links to untrusted domains, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Links and external images`, ensure `Show warning prompt for any click on links to untrusted domains` is `checked`

Remediation:

To configure warning prompt for any click on links to untrusted domains, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Links and external images`, `check` - `Show warning prompt for any click on links to untrusted domains`

Default Value:

- `Show warning prompt for any click on links to untrusted domains` = `checked`

CIS Controls:

Version 7

7.4 Maintain and Enforce Network-Based URL Filters
Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

5.11 (L1) Ensure protection against domain spoofing based on similar domain names is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Moves domain spoofing emails to spam folder.

Rationale:

You should protect your users from domain spoofing emails.

Impact:

Domain spoofed emails will be moved to a user's spam folder.

Audit:

To verify protection against domain spoofing based on similar domain names is enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, ensure `Protect against domain spoofing based on similar domain names` is `checked`
6. Ensure `Action` is `Move email to spam`

Remediation:

To configure protection against domain spoofing based on similar domain names, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, `check` - `Protect against domain spoofing based on similar domain names`
6. Set `Action` to `Move email to spam`
7. Select `Save`

Default Value:

- `Protect against domain spoofing based on similar domain names` = `not-checked`
- `Action` = `Keep email in inbox and show warning (default)`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.12 (L1) Ensure protection against spoofing of employee names is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Moves employee spoofing emails to spam folder.

Rationale:

You should protect your users from employee spoofing emails.

Impact:

Employee spoofed emails will be moved to a user's spam folder.

Audit:

To verify protection against spoofing of employee names is enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, ensure `Protect against spoofing of employee names` is `checked`
6. Ensure `Action` is `Move email to spam`

Remediation:

To configure protection against spoofing of employee names, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, `check` - `Protect against spoofing of employee names`
6. Set `Action` to `Move email to spam`
7. Select `Save`

Default Value:

- `Protect against spoofing of employee names` = `un-checked`
- `Action` = `Keep email in inbox and show warning (default)`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.13 (L1) Ensure protection against inbound emails spoofing your domain is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Moves inbound emails spoofing your domain to spam folder.

Rationale:

You should protect your users from inbound company domain spoofing emails.

Impact:

Inbound company domain spoofed emails will be moved to a user's spam folder.

Audit:

To verify protection against inbound emails spoofing your domain is enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, ensure `Protect against inbound emails spoofing your domain` is `checked`
6. Ensure `Action` is `Move email to spam`

Remediation:

To configure protection against spoofing of employee names, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, `check` - `Protect against inbound emails spoofing your domain`
6. Set `Action` to `Move email to spam`
7. Select `Save`

Default Value:

- `Protect against inbound emails spoofing your domain` = `un-checked`
- `Action` = `Keep email in inbox and show warning (default)`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.14 (L1) Ensure protection against any unauthenticated emails is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Displays a warning when any message is not authenticated (SPF or DKIM).

Rationale:

You should protect your users from any emails that aren't authenticated (SPF or DKIM)

Impact:

Emails that aren't authenticated (SPF or DKIM) display a warning message to the recipient.

Audit:

To verify protection against any unauthenticated emails is enabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, ensure `Protect against any unauthenticated emails` is `checked`

Remediation:

To configure protection against any unauthenticated emails, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, `check` - `Protect against any unauthenticated emails`
6. Select `Save`

Default Value:

- `Protect against any unauthenticated emails` = `un-checked`

CIS Controls:

Version 7

7.8 Implement DMARC and Enable Receiver-Side Verification
To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.

5.15 (L1) Ensure groups are protected from inbound emails spoofing your domain (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

If a group receives an email that is spoofing your domain it is sent to the spam folder.

Rationale:

You should protect your groups from any emails that spoofing your domain.

Impact:

Emails that are spoofing your domain and are received by a group are sent to the spam folder.

Audit:

To verify groups are protected from inbound emails spoofing your domain, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, ensure `Protect your Groups from inbound emails spoofing your domain` is `checked`
6. Ensure `Action` is set to `Move email to spam`

Remediation:

To protect groups from inbound emails spoofing your domain, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `Safety` - `Spoofing and authentication`, check - `Protect your Groups from inbound emails spoofing your domain`
6. Set `Action` to `Move email to spam`

Default Value:

- `Protect against any unauthenticated emails` = `checked`
- `Action` = `Keep email in inbox and display warning (default)`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.16 (L2) Ensure POP and IMAP access is disabled for all users (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

POP and IMAP may allow users to access Gmail using legacy or unapproved email clients that do not support modern authentication mechanisms, such as multifactor authentication.

Rationale:

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

Impact:

If you have Apple iOS or Android device users in your organization and you turn IMAP off, let them know that they're no longer syncing Google Workspace mail to the iOS or Android Mail app. They might not get a notification on their device. Additionally, new users can't manually add the Google Account they use for work or school to the device.

If your Google Workspace users want to use desktop clients, such as Microsoft Outlook and Apple Mail, to access their Google Workspace mail, you need to enable POP or IMAP access in the Google Admin console. You can enable access for everyone in your organization or only for users in specific organizational units.

Audit:

To verify POP and IMAP access is disabled for all users, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `End User Access` - `POP and IMAP Access`, ensure `Disable POP and IMAP access for all users` is `checked`

Remediation:

To disable POP and IMAP access for all users, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `End User Access` - `POP and IMAP Access`, check - `Disable POP and IMAP access for all users`

Default Value:

- `Disable POP and IMAP access for all users` = `un-checked`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.17 (L2) Ensure automatic forwarding options are disabled (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

You should disable automatic forwarding to prevent users from auto-forwarding mail.

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.

Impact:

Care should be taken before implementation to ensure there is no business need for case-by-case auto-forwarding. Disabling auto-forwarding to remote domains will affect all users and in an organization.

Audit:

To verify automatic email forwarding is disabled for all users, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `End User Access` - `Automatic forwarding`, ensure `Allow users to automatically forward incoming email to another address` is `not checked`

Remediation:

To disable automatic for all users, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `End User Access` - `Automatic forwarding`, `un-check` - `Allow users to automatically forward incoming email to another address`

Default Value:

- `Allow users to automatically forward incoming email to another address` = `checked`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

5.18 (L1) Ensure per-user outbound gateways is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

A per-user outbound gateway is a mail server, other than the Google Workspace mail servers, that delivers outgoing mail for a user in your domain.

Rationale:

Mail sent via external SMTP will circumvent your outbound gateway

Impact:

Care should be taken before implementation to ensure there is no business need for mail sent via external SMTP gateway.

Audit:

To verify per-user outbound gateways is disabled, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `End User Access` - `Allow per-user outbound gateways`, ensure `Allow users to send mail through an external SMTP server when configuring a "from" address hosted outside your email domain` is `not checked`

Remediation:

To disable per-user outbound gateways, use the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace`
4. Select `Gmail`
5. Under `End User Access` - `Allow per-user outbound gateways`, `un-check` - `Allow users to send mail through an external SMTP server when configuring a "from" address hosted outside your email domain`

Default Value:

- `Allow users to send mail through an external SMTP server when configuring a "from" address hosted outside your email domain` = `not checked`

CIS Controls:

Version 7

7 Email and Web Browser Protections
Email and Web Browser Protections

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Account / Authentication**		
1.1	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles (Manual)	□	□
1.2	(L2) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users (Manual)	□	□
1.3	(L2) Ensure Advanced Protection Program is configured (Manual)	□	□
1.4	(L1) Ensure password policy is configured for enhanced security (Manual)	□	□
1.5	(L2) Ensure login challenges are enforced (Manual)	□	□
1.6	(L1) Ensure Google session control is configured (Manual)	□	□
1.7	(L2) Ensure Google Cloud session control (Beta) is configured (Manual)	□	□
2	**Application Permissions**		
2.1	(L1) Ensure less secure app access is disabled (Manual)	□	□
2.2	(L1) Ensure directory data access is externally restricted (Manual)	□	□
2.3	(L2) Ensure application access to Google services is restricted (Manual)	□	□
2.4	(L2) Review third-party applications periodically (Manual)	□	□
2.5	(L2) Review domain-wide delegation for applications periodically (Manual)	□	□
3	**Calendar**		
3.1	(L1) Ensure external sharing options for primary calendars are configured (Manual)	□	□
3.2	(L1) Ensure external invitation warnings for Google Calendar are configured (Manual)	□	□
3.3	(L1) Ensure external sharing options for secondary calendars are configured (Manual)	□	□
4	**Drive and Docs**		
4.1	(L1) Ensure DLP policies for Google Drive are configured (Manual)	□	□
4.2	(L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted (Manual)	□	□
4.3	(L1) Ensure only users inside your organization can distribute content externally (Manual)	□	□

Control		Set Correctly	
		Yes	No
4.4	(L2) Ensure document sharing is being controlled by domain with allow-lists (Manual)	□	□
4.5	(L1) Ensure users can create new shared drives (Manual)	□	□
4.6	(L1) Ensure full-access members cannot modify shared drive settings (Manual)	□	□
4.7	(L1) Ensure shared drive file access is restricted to members only (Manual)	□	□
4.8	(L1) Ensure link sharing default settings are configured (Manual)	□	□
5	**Gmail**		
5.1	(L1) Ensure users cannot delegate access to their mailbox (Manual)	□	□
5.2	(L1) Ensure Gmail labs is not enabled (Manual)	□	□
5.3	(L1) Ensure that DKIM is enabled for all mail enabled domains (Manual)	□	□
5.4	(L1) Enable quarantine admin notifications for Gmail (Manual)	□	□
5.5	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled (Manual)	□	□
5.6	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled (Manual)	□	□
5.7	(L1) Ensure protection against anomalous attachment types in emails is enabled (Manual)	□	□
5.8	(L1) Ensure link identification behind shortened URLs is enabled (Manual)	□	□
5.9	(L1) Ensure scan linked images for malicious content is enabled (Manual)	□	□
5.10	(L1) Ensure warning prompt is shown for any click on links to untrusted domains (Manual)	□	□
5.11	(L1) Ensure protection against domain spoofing based on similar domain names is enabled (Manual)	□	□
5.12	(L1) Ensure protection against spoofing of employee names is enabled (Manual)	□	□
5.13	(L1) Ensure protection against inbound emails spoofing your domain is enabled (Manual)	□	□
5.14	(L1) Ensure protection against any unauthenticated emails is enabled (Manual)	□	□
5.15	(L1) Ensure groups are protected from inbound emails spoofing your domain (Manual)	□	□
5.16	(L2) Ensure POP and IMAP access is disabled for all users (Manual)	□	□

Control		Set Correctly	
		Yes	No
5.17	(L2) Ensure automatic forwarding options are disabled (Manual)	□	□
5.18	(L1) Ensure per-user outbound gateways is disabled (Manual)	□	□

Appendix: Change History

Date	Version	Changes for this version
1/29/2021	1.0.0	Initial Release