CIS Google Workspace Foundations Benchmark

v1.2.0 - 05-29-2024

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

Overview

All CIS Benchmarks™ focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches.
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches.

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

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 CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. 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, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

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

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) '4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

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:

Recommendations

1 Directory

The Directory section of the Google Workspace Admin Console.

1.1 Users

User defined in this domain and their permissions.

1.1.1 (L1) Ensure more than one Super Admin account exists (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Having more than one Super Admin account is needed primarily so that a single point of failure can be avoided. Also, for larger organizations, having multiple Super Admins can be useful for workload balancing purposes.

Rationale:

From a security point of view, having only a single Super Admin Account can be problematic if this user were unavailable for an extended period of time. Also, Super Admin accounts should never be shared amongst multiple users.

Impact:

There should be no user impact, but Administrators should have a normal (low privilege) and an Administrative (high privilege) account.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Go to `Directory` and click on `Users`, this will show a list of all users
3. Click on `+ Add a filter`, select `Admin role`, check the `Super admin` box, and then select `Apply`
4. The list of Users displayed will only be those with the `Super Admin` role
5. Make sure more than one (1) user is listed

Remediation:

Create at least one additional account with a Super Admin role.
NOTE: A new account should be created vs adding this role to an existing account since Administration tasks should be done through separate Admin accounts.

Default Value:

All Google Workspace tenants will have one Super Admin initially.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.1 <u>Establish and Maintain an Inventory of Accounts</u>** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	🟢	🟠	🔵
v7	**4.1 <u>Maintain Inventory of Administrative Accounts</u>** Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		🟠	🔵

1.1.2 (L1) Ensure no more than 4 Super Admin accounts exist (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Having more than one Super Admin account is needed primarily so that a single point of failure can be avoided, but having too many should be avoided.

Rationale:

From a security point of view, having a large number of Super Admin accounts is a bad practice. In general, all users should be assigned the least privileges needed to do their job. This includes Administrators since not everyone that needs to "Administer Something" needs to be a Super Admin. Google Workspaces provides many predefined Administration Roles and also allows the creation of Custom Roles with very granular permission selection.

Impact:

There should be no user impact, but Administrators should have a normal (low privilege) and an Administrative (high privilege) account.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Go to `Directory` and click on `Users`, this will show a list of all users
3. Click on `+ Add a filter`, select `Admin role`, check the `Super admin` box, and then select `Apply`
4. The list of Users displayed will only be those with the `Super Admin` role
5. Make sure no more than four (4) users are listed

Remediation:

Reduce the number of accounts with a "Super Admin" role.

Default Value:

All Google Workspace tenants will have one Super Admin initially.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.1 Establish and Maintain an Inventory of Accounts** Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	**4.1 Maintain Inventory of Administrative Accounts** Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.1.3 (L1) Ensure super admin accounts are used only for super admin activities (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Super admin accounts have access to all features in the Google Admin console and Admin API and can manage every aspect of your organization's account. Super admins also have full access to all users' calendars and event details.

It is recommended to give each super administrator two accounts. One for their super admin account and a second account for daily activities. Users should only sign in to a super admin account to perform super admin tasks, such as setting up 2-Step Verification (2SV), managing billing and user licenses, or helping another admin recover their account. Super administrators should use a separate, non-admin account for day-to-day activities.

Super admins should sign in as needed to do specific tasks and then sign out. Leaving super admin accounts sign-in can increase exposure to phishing attacks.

Rationale:

Use the super admin account only when needed. Delegate administrator tasks to user accounts with limited admin roles. Use the least privilege approach, where each user has access to the resources and tools needed for their typical tasks. For example, you could grant an admin permissions to create user accounts and reset passwords, but not let them delete user accounts.

Impact:

Super admin users will have to switch accounts as well as utilize login/logout functionality when performing administrative tasks.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Go to `Directory` and click on `Users`, this will show a list of all users
3. Click on `+ Add a filter`, select `Admin role`, check the `Super admin` box, and then select `Apply`
4. The list of Users displayed will only be those with the `Super Admin` role
5. Click on `+ Add a filter`, select `Admin role`, check the `Delegated admin` box, and then select `Apply`
6. Verify that there are no users in both the `Super admin` and `Delegated admin` roles

Remediation:

For every `Super admin` that is also a `Delegated admin` account, either create a `Delegated admin` account for the user of elevate or their existing non-admin account to a `Delegated admin` account.

Default Value:

N/A

References:

1. https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/add-users?view=o365-worldwide
2. https://learn.microsoft.com/en-us/microsoft-365/enterprise/protect-your-global-administrator-accounts?view=o365-worldwide
3. https://learn.microsoft.com/en-us/azure/active-directory/roles/best-practices#9-use-cloud-native-accounts-for-azure-ad-roles
4. https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/whatis

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

1.2 Directory Settings

The Directory section of the Google Workspace Admin Console.

1.2.1 Sharing Settings

Decide how users can share contacts, both within your organization and externally.

1.2.1.1 (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 this setting via 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`
6. Select `Save`

Remediation:

To configure this setting via 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`

2 Devices

The Devices section of the Google Workspace Admin Console is outside the scope of this Benchmark. The Chrome settings are currently covered in the CIS Chrome Benchmark. The Mobile & endpoint settings will be covered in a future Benchmark.

3 Apps

The Apps section of the Google Workspace Admin Console.

3.1 Google Workspace

The Google Workspace sub-section of the Google Workspace Admin Console.

3.1.1 Calendar

Calendar settings.

3.1.1.1 Sharing Settings

Set global sharing policies for user's primary calendars.

3.1.1.1.1 (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 this setting via 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 this setting via 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)`
7. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.1.1.2 (L2) Ensure internal sharing options for primary calendars are configured (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

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

Rationale:

In general, not everyone in the organization needs to know the schedule details of everyone else (operational security). Free/busy indication is enough for most people.

Impact:

This will be the default for the user's primary calendar. The user can override this setting to allow other specific users greater visibility of their calendar.

Audit:

To verify this setting via 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 `Internal sharing options for primary calendars`
6. Ensure `Only free/busy information (hide event details)` is `selected`

Remediation:

To configure this setting via 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 `Internal sharing options for primary calendars`
6. Select `Only free/busy information (hide event details)`
7. Select `Save`

Default Value:

Internal sharing options for primary calendars is Share all information

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 <u>Protect Information through Access Control Lists</u> 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.	●	●	●

3.1.1.1.3 (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 this setting via 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 this setting via 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. Set `Warn users when inviting guests outside of the domain` to `checked`
7. Select `Save`

Default Value:

`Warn users when inviting guests outside of the domain` is `checked`

3.1.1.2 General Settings

Configure external sharing policies.

3.1.1.2.1 (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 this setting via 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 this setting via 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)`
7. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.1.2.2 (L2) Ensure internal sharing options for secondary calendars are configured (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

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

Rationale:

In general, not everyone in the organization needs to know the schedule details of everyone else (operational security). Free/busy indication is enough for most people.

Impact:

This will be the default for the user's secondary calendars. The user can override this setting to allow other specific users greater visibility of their calendars.

Audit:

To verify this setting via 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 `Internal sharing options for secondary calendars`
6. Ensure `Only free/busy information (hide event details)` is `selected`

Remediation:

To configure this setting via 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 `Internal sharing options for secondary calendars`
6. Select `Only free/busy information (hide event details)`
7. Select `Save`

Default Value:

Internal sharing options for secondary calendars is Share all information

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.1.3 Advanced Settings

Enable Google Calendar features for your users.

3.1.1.3.1 (L2) Ensure calendar web offline is disabled (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Limit who is allowed offline calendar access.

Rationale:

When enabled, users can turn on offline use for each computer they use. Data is stored on the computer until offline use is turned off by the user. In this case, the organization can lose control of where its data is stored (for this user). Care should be taken regarding which users and groups have this capability enabled.

Impact:

Users will not be able to access their calendars offline.

Audit:

To verify this setting via 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 `Advanced settings`, select `Calendar web offline`
6. Ensure `Allow using Calendar on the web when offline` is `unchecked`

Remediation:

To configure this setting via 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 `Advanced settings`, select `Calendar web offline`
6. Set `Allow using Calendar on the web when offline` to `unchecked`
7. Select `Save`

Default Value:

`Allow using Calendar on the web when offline` is `checked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.1.2 Drive and Docs

Drive and Docs settings.

3.1.2.1 Sharing Settings

Set global policies for sharing files outside your organization, and define the default link sharing visibility of new files.

Google has added Trust rules to create granular polices for access to Google Drive. Trust rules should be used based on organizational decisions. You can find out more here: [Create and manage trust rules for Drive sharing](#)

3.1.2.1.1 Sharing Options

Sharing outside of organization.

3.1.2.1.1.1 (L1) Ensure users are warned when they share a file outside their domain (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Warn the user when they try and share a file and/or shared drive externally.

Rationale:

The user may not realize the potential account is external to the organization. Providing a warning allows the user an opportunity to know this and possibly reassess this sharing.

Impact:

None, except an additional warning. Sharing can still occur.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Drive and Docs`
4. Select `Sharing Settings`
5. Select `Sharing Options`
6. Under `Sharing outside of <Company>`
7. Ensure `ON - Files owned by users in <Company> can be shared outside of <Company>. This applies to files in all shared drives as well.` is `checked`. Also, ensure the sub-setting `For files owned by users in <Company> warn when sharing outside of <Company>` is `checked`.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Drive and Docs`
4. Select `Sharing Settings`
5. Select `Sharing Options`
6. Under `Sharing outside of <Company>`
7. Set `ON - Files owned by users in <Company> can be shared outside of <Company>. This applies to files in all shared drives as well.` to `checked`. Also, set the sub-setting `For files owned by users in <Company> warn when sharing outside of <Company>` to `checked`.
8. Select `Save`

Default Value:

`For files owned by users in <Company> warn when sharing outside of <Company>` is `checked`

3.1.2.1.1.2 (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 this setting via 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 `When sharing outside of <Company> is allowed, users in <Company> can make files and published web content visible to anyone with the link` is `unchecked`

Remediation:

To configure this setting via 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`, set `When sharing outside of <Company> is allowed, users in <Company> can make files and published web content visible to anyone with the link` to `unchecked`
7. Select `Save`

Default Value:

`When sharing outside of <Company> is allowed, users in <Company> can make files and published web content visible to anyone with the link` is `Checked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 <u>Configure Data Access Control Lists</u>** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 <u>Protect Information through Access Control Lists</u>** 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.	●	●	●

3.1.2.1.1.3 (L2) Ensure document sharing is being controlled by domain with allowlists (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 this setting via 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 `ALLOWLISTED DOMAINS - Files owned by users in <Company> can be shared with Google Accounts in compatible allowlisted domains.` is `selected`
7. Ensure `Warn when files owned by users or shared drives in <Company> are shared with users in allowlisted domains` is `checked`

Remediation:

To configure this setting via 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 `ALLOWLISTED DOMAINS - Files owned by users in <Company> can be shared with Google Accounts in compatible allowlisted domains.`
7. Set `Warn when files owned by users or shared drives in <Company> are shared with users in allowlisted domains` to `checked`
8. Select `Save`

Default Value:

`Sharing outside of <Company>` is `ON - Files owned by users in <Company> can be shared outside of <Company>. This applies to files in all shared drives as well.`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	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.	●	●	●

3.1.2.1.1.4 (L2) Ensure users are warned when they share a file with users in an allowlisted domain (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Warn the user when they try and share a file and/or shared drive with users in an allowlisted domain.

Rationale:

The user may not realize the potential account is external to the organization. Providing a warning allows the user an opportunity to know this and possibly reassess this sharing.

Impact:

None, except an additional warning. Sharing can still occur.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Drive and Docs`
4. Select `Sharing Settings`
5. Select `Sharing Options`
6. Under `Sharing outside of <Company>`
7. Ensure `ALLOWLISTED DOMAINS - Files owned by users or shared drives in BMDT-Group can be shared with Google accounts in compatible allowlisted domains` is `checked`. Also, ensure the sub-setting `Warn when files owned by users or shared drives in <Company> are shared with users in allowlisted domains` is `checked`.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Drive and Docs`
4. Select `Sharing Settings`
5. Select `Sharing Options`
6. Under `Sharing outside of <Company>`
7. Set `ALLOWLISTED DOMAINS - Files owned by users or shared drives in BMDT-Group can be shared with Google accounts in compatible allowlisted domains.` to `checked`. Also, set the sub-setting `Warn when files owned by users or shared drives in <Company> are shared with users in allowlisted domains` to `checked`.
8. Select `Save`

Default Value:

`For files owned by users in <Company> warn when sharing outside of <Company>` is `checked`

3.1.2.1.1.5 (L1) Ensure Access Checker is configured to limit file access (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

When a user shares a file via a Google product other than Docs or Drive (e.g. by pasting a link in Gmail), Google can check that the recipients have access. If not, when possible, Google will ask the user to pick how they want to share the file.

Rationale:

In general, access should be restricted to the smallest group possible. In this case recipients only.

Impact:

Only recipients can access files. Recipients cannot share access with others by forwarding the email/link.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Drive and Docs`
4. Select `Sharing Settings`
5. Select `Sharing Options`
6. Under `Access Checker`
7. Ensure `Recipients only.` is `checked`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Drive and Docs`
4. Select `Sharing Settings`
5. Select `Sharing Options`
6. Under `Access Checker`
7. Set `Recipients only.` to `checked`
8. Select `Save`

Default Value:

Recipients only, suggested target audience, or public (no Google account required). is checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 <u>Configure Data Access Control Lists</u>** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 <u>Protect Information through Access Control Lists</u>** 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.	●	●	●

3.1.2.1.1.6 (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 this setting via 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 configure this setting via 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>`
7. Select `Save`

Default Value:

`Distributing content outside of <Company>` is `Anyone`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.2.1.2 Shared Drive Creation

Default settings for new shared drives.

3.1.2.1.2.1 (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 this setting via 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 `Shared drive creation`
6. Ensure `Prevent users in <Company> from creating new shared drives` is `un-checked`

Remediation:

To verify this setting via 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 `Shared drive creation`
6. Set `Prevent users in <Company> from creating new shared drives` to `unchecked`
7. Select `Save`

Default Value:

`Prevent users in <Company> from creating new shared drives` is `unchecked`

Internal Only - General

3.1.2.1.2.2 (L1) Ensure manager 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 manager access members to override or modify shared drive settings can allow intentional and unintentional data access by unauthorized users.

Impact:

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

Audit:

To verify this setting via 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. Select `Sharing settings`
6. Under `Shared drive creation`, ensure `Allow members with manager access to override the settings below` is `unchecked`

Remediation:

To configure this setting via 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. Select `Sharing settings`
6. Under `Shared drive creation`, set `Allow members with manager access to override the settings below` to `unchecked`
7. Select `Save`

Default Value:

Allow members with manager access to override the settings below is
checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.2.1.2.3 (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:

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

Audit:

To verify this setting via 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. Select `Sharing settings`
6. Under `Shared drive creation`, ensure `Allow people who aren't shared drive members to be added to files` is `unchecked`

Remediation:

To configure this setting via 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. Select `Sharing settings`
6. Under `Shared drive creation`, set `Allow people who aren't shared drive members to be added to files` to `unchecked`
7. Select `Save`

Default Value:

Allow people who aren't shared drive members to be added to files is checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.2.1.2.4 (L2) Ensure viewers and commenters ability to download, print, and copy files is disabled (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

limit what viewers/commenters on a shared document can do with it.

Rationale:

In many cases when sharing a document it might be fine for the users to do what they want with the document on the shared drive (Download, Print, etc.). In more restricted environments these capabilities may need to be prevented (Protected Intellectual property, Personally Identifiable Information, etc.).

Impact:

Users of this shared drive will be restricted to only reading and commenting on the existing files.

Audit:

To verify this setting via 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. Select `Sharing settings`
6. Under `Shared drive creation`, ensure `Allow viewers and commenters to download, print, and copy files` is `unchecked`

Remediation:

To verify this setting via 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. Select `Sharing settings`
6. Under `Shared drive creation`, set `Allow viewers and commenters to download, print, and copy files` to `unchecked`
7. Select `Save`

Default Value:

Allow viewers and commenters to download, print, and copy files is
unchecked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.2.2 Features and Applications

Manage which features and applications are available to users in your organization.

3.1.2.2.1 (L1) Ensure offline access to documents is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Prevent documents from being locally accessible on an unconnected device.

Rationale:

This setting prevents an organization's files from being stored locally, thus limiting data loss issues if the device is lost or stolen.

Impact:

Copies of recent files are only synced and saved on devices if you've defined a managed policy to do so.

NOTE: All users will lose access to offline documents on all devices if managed devices policies are not set.

NOTE: Setting up policies to control offline access on individual devices is outside the scope of this Benchmark. Additional information om doing this for various device types can be found **[here](#)**.

Audit:

To verify this setting via 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. Select `Features and Applications`
6. Select `Offline`
7. Ensure `Control offline access using device policies` is `checked`

Remediation:

To configure this setting via 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. Select `Features and Applications`
6. Select `Offline`
7. Set `Control offline access using device policies.` to `checked`
8. Select `Save`

Default Value:

`Control offline access using device policies` is `unchecked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

3.1.2.2.2 (L1) Ensure desktop access to Drive is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Prevent documents from being locally accessible on an unconnected device.

Rationale:

This setting prevents an organization's files from being stored locally, thus limiting data loss issues if the device is lost or stolen.

NOTE: The Google Drive desktop application has its own way of handling "Offline" files and does not obey the `Drive and Doc` > `Offline` > `Control offline access using divide policies` setting. Not allowing Google Drive for desktop on the device will prevent this channel.

Impact:

The end user will not be able to use Google Drive for desktop and its convenient integration into the Windows file explorer.

Audit:

To verify this setting via 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. Select `Features and Applications`
6. Select `Google Drive for desktop`
7. Ensure `Allow Google Drive for desktop in your organization` is `unchecked`

Remediation:

To verify this setting via 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. Select `Features and Applications`
6. Select `Google Drive for desktop`
7. Set `Allow Google Drive for desktop in your organization` to `unchecked`
8. Select `Save`

Default Value:

`Allow Google Drive for desktop in your organization` is `checked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.1.2.2.3 (L1) Ensure Add-Ons is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Prevent users to install Google Docs add-ons from add-ons store.

NOTE: This setting controls add-on access from outside your organization.

Rationale:

Allowing uses to install unapproved Add-Ons puts the organization at risk. If users need a specific Add-On this can be handled on a case by case basis as the need, and the add-on, is approved.

Impact:

The end user will not be able to use Google Drive for desktop and its convenient integration into the Windows file explorer.

Audit:

To verify this setting via 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. Select `Features and Applications`
6. Select `Add-Ons`
7. Ensure `Allow users to install Google Docs add-ons from add-ons store.` is `unchecked`

Remediation:

To verify this setting via 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. Select `Features and Applications`
6. Select `Add-Ons`
7. Set `Allow users to install Google Docs add-ons from add-ons store.` to `unchecked`
8. Select `Save`

Default Value:

Allow users to install Google Docs add-ons from add-ons store. is checked

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F4530135&assistant_id=generic-unu&product_context=4530135&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.1.3 Gmail

Gmail settings.

3.1.3.1 User Settings

Set name formats. Enable user preferences such as themes, read receipts, and email delegation.

3.1.3.1.1 (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 this setting via 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 `unchecked`

Remediation:

To configure this setting via 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`, set `Let users delegate access to their mailbox to other users in the domain` to `unchecked`
6. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.3.1.2 (L1) Ensure offline access to Gmail is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Disables the user's ability to utilize various Gmail functions (read, write, search, delete, and label email messages) while not connected to the internet.

Rationale:

Prevents the organization's data (user's email) from being copied to remote computers.

Impact:

Users will need internet access to use Gmail.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Gmail`
4. Select `User Settings`
5. Under `Gmail web offline`
6. Ensure `Enable Gmail web offline` is `unchecked`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Gmail`
4. Select `User Settings`
5. Select `Gmail web offline`
6. Set `Enable Gmail web offline` to `unchecked`
7. Select `Save`

Default Value:

`Enable Gmail web offline` is `unchecked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.1.3.2 Authenticate email

Set up email authentication (DKIM).

3.1.3.2.1 (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 this setting via 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 configure this setting via 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:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.5 Implement DMARC** To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		●	●
v7	**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.		●	●

3.1.3.2.2 (L1) Ensure the SPF record is configured for all mail enabled domains (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

For all the email domains configured in Google Workspace, a corresponding Sender Policy Framework (SPF) record should be created.

NOTE: There are a number of ways SPF can be configured, this document presents a most basic method. For more information on setting up SPF for Google Workspace please refer to the Google documentation.

- **How SPF protects against spoofing and spam**
- **Define your SPF record—Basic setup**

Rationale:

SPF records allow Gmail and other mail systems to know where messages from your domains are allowed to originate. This information can be used by that system to determine how to treat the message based on if it is being spoofed or is valid.

Impact:

There should be minimal impact of setting up SPF records however, organizations should ensure proper SPF record setup as email could be flagged as spam if SPF is not set up appropriately.

Audit:

Check the DNS records for each domain.

1. Use a Domain Name System (DNS) lookup tool to review the current configuration for your domain (DNS Records). This information can be discovered in a variety of ways:
   - Reviewing the DNS Record information at your domain registrar (GoDaddy, etc.)
   - Using an OS based `nslookup` tool on your workstation OS
   - Using Google **Dig** tool available from the Google Admin Toolbox site (Link: **Dig**)
2. Using the chosen tool, enter your email domain name (ex. domain1.com)
3. In the results displayed, ensure that a TXT Record with the value of `v=spf1 include:_spf.google.com ~all` exists and designates Google Gmail as a authorized sender.

Remediation:

Configure the DNS record for each domain.

- If all email in your domain is sent from and received by Google Gmail, add the following TXT record for each domain:

```
v=spf1 include:_spf.google.com ~all
```

NOTE: This will likely need to be configured at your domain registrar (Godaddy, etc.).

Default Value:

None

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.5 <u>Implement DMARC</u> To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		●	●
v7	7.8 <u>Implement DMARC and Enable Receiver-Side Verification</u> 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.		●	●

3.1.3.2.3 (L1) Ensure the DMARC record is configured for all mail enabled domains (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

For all email domains configured in Google Workspace, a corresponding Domain-Based Message Authentication, Reporting and Conformance (DMARC) record should be created.

NOTE: There are a number of ways DMARC can be configured, this document presents a most basic method. For more information on setting up DMARC for Google Workspace please refer to the Google documentation.

- **Help prevent spoofing and spam with DMARC**
- **Tutorial: Recommended DMARC rollout**

Rationale:

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

Impact:

There should be minimal impact of setting up DMARC records however, organizations should ensure proper DMARC record setup as email could be flagged as spam if DMARC is not set up appropriately.

Audit:

Check the DNS records for each domain.

1. Use a Domain Name System (DNS) lookup tool to review the current configuration for your domain (DNS Records). This information can be discovered in a variety of ways:
    -   Reviewing the DNS Record information at your domain registrar (GoDaddy, etc.)
    -   Using an OS based `nslookup` tool on your workstation OS
    -
        Preferred: Using Google **Dig** tool available from the Google Admin Toolbox site (Link: **Dig**)
2. Using the chosen tool, enter your email domain name (ex. domain1.com)
3. In the results displayed, ensure that a TXT Record with the value of `v=DMARC1; p=none; rua=mailto:<report@domain1.com>` exists. This designates Google Gmail as an authorized sender.

NOTE: The **p=none** sets DMARC to non-enforcing. This is a relaxed DMARC policy that lets you start getting reports without risking messages from your domain being rejected or marked as spam by receiving servers. Start with a none policy that only monitors email flow, and then eventually change to a policy that rejects all unauthenticated messages (`p=reject`).

NOTE: The **rua=mailto:_report@domain1.com** entry is optional but setting it to a valid email address is recommended. RUA reports provide a comprehensive view of all of a domain's traffic. At a minimum, organizations should configure their DMARC record to receive RUA reports.

-
    The Difference in DMARC Reports: RUA and RUF

Remediation:

Configure the DNS record for each domain.

1. If all email in your domain is sent from and received by Google Gmail, add the following TXT record for the domain:

```
v=DMARC1; p=none; rua=mailto:<report@domain1.com>
```

NOTE: This will likely need to be configured at your domain registrar (Godaddy, etc.).

Default Value:

None

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.5 <u>Implement DMARC</u>** To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		🟠	🔵
v7	**7.8 <u>Implement DMARC and Enable Receiver-Side Verification</u>** 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.		🟠	🔵

3.1.3.3 Manage Quarantines

Create, modify, or remove email quarantines.

3.1.3.3.1 (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 this setting via 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` is `checked`

Remediation:

To configure this setting via 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, set Notify periodically when messages are quarantined to checked

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

Default Value:

Notify periodically when messages are quarantined is unchecked

3.1.3.4 Safety

Configure email and spam safety features.

3.1.3.4.1 Attachments

Additional policies to protect against malware in emails.

3.1.3.4.1.1 (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 this setting via 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 this setting via 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`, set `Protect against encrypted attachments from untrusted senders` to `checked`
6. Select `Save`

Default Value:

`Protect against encrypted attachments from untrusted senders` is `checked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.6 <u>Block Unnecessary File Types</u> Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●
v7	7.9 <u>Block Unnecessary File Types</u> Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.		●	●

3.1.3.4.1.2 (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 this setting via 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 verify this setting via 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`, set `Protect against attachments with scripts from untrusted senders` to `checked`
6. Select `Save`

Default Value:

Protect against attachments with scripts from untrusted senders is enabled is checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.6 Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.		🟠	🔵
v7	**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.		🟠	🔵

3.1.3.4.1.3 (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 this setting via 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 this setting via 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`, set `Protect against anomalous attachment types in emails` to `checked`
6. Select `Save`

Default Value:

`Protect against anomalous attachment types in emails` is `Unchecked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.6 Block Unnecessary File Types** Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●
v7	**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.		●	●

3.1.3.4.2 Links and external images

Additional settings to prevent email phishing due to links and external images.

3.1.3.4.2.1 (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 this setting via 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 verify this setting via 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`, set `Identify links behind shortened URLs` to `checked`
6. Select `Save`

Default Value:

`Identify links behind shortened URLs` is `checked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	**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.		●	●

3.1.3.4.2.2 (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 this setting via 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 this setting via 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`, set `Scan linked images` to `checked`
6. Select `Save`

Default Value:

`Scan linked images` is `checked`

3.1.3.4.2.3 (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 this setting via 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 this setting via 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`, set `Show warning prompt for any click on links to untrusted domains` is `checked`
6. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.3 <u>Maintain and Enforce Network-Based URL Filters</u>** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	**7.4 <u>Maintain and Enforce Network-Based URL Filters</u>** 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.		●	●

3.1.3.4.3 Spoofing and authentication

Additional settings to reduce phishing attacks due to spoofing and unauthenticated emails.

3.1.3.4.3.1 (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 this setting via 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 verify this setting via 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`, set `Protect against domain spoofing based on similar domain names` to `checked`
6. Set `Action` to `Move email to spam`
7. Select `Save`

Default Value:

- Protect against domain spoofing based on similar domain names is checked
- Action is Keep email in inbox and show warning (default)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		🟠	🔵
v7	**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.		🟠	🔵

3.1.3.4.3.2 (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 this setting via 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 verify this setting via 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`, set `Protect against spoofing of employee names` to `checked`
6. Set `Action` to `Move email to spam`
7. Select `Save`

Default Value:

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

3.1.3.4.3.3 (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 this setting via 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 this setting via 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`, set `Protect against inbound emails spoofing your domain` to `checked`
6. Set `Action` to `Move email to spam`
7. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	**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.		●	●

3.1.3.4.3.4 (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 this setting via 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 verify this setting via 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`, set `Protect against any unauthenticated emails` to `checked`
6. Select `Save`

Default Value:

`Protect against any unauthenticated emails` = `unchecked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.5 <u>Implement DMARC</u> To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.		🟠	🔵
v7	7.8 <u>Implement DMARC and Enable Receiver-Side Verification</u> 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.		🟠	🔵

3.1.3.4.3.5 (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 this setting via 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 configure this setting via 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`, set `Protect your Groups from inbound emails spoofing your domain` to `checked`
6. Set `Action` to `Move email to spam`
7. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**9.3 Maintain and Enforce Network-Based URL Filters** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	**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.		●	●

3.1.3.5 End User Access

Configure end user access features.

3.1.3.5.1 (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 this setting via 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`
6. Ensure `Enable IMAP access for all users` is `unchecked`
7. Ensure `Enable POP access for all users` is `unchecked`

Remediation:

To configure this setting via 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`
6. Set `Enable IMAP access for all users` to `unchecked`
7. Set `Enable POP access for all users` to `unchecked`
8. Select `Save`

Default Value:

- `Enable IMAP access for all users` is `checked`
- `Enable POP access for all users` is `checked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		🟠	🔵
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		🟠	🔵

3.1.3.5.2 (L1) Ensure automatic forwarding options are disabled (Manual)

Profile Applicability:

- Enterprise Level 1

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 this setting via 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 `unchecked`

Remediation:

To verify this setting via 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`, set `Allow users to automatically forward incoming email to another address` to `unchecked`
6. Select `Save`

Default Value:

Allow users to automatically forward incoming email to another address is checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.1.3.5.3 (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 this setting via 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 `unchecked`

Remediation:

To configure this setting via 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`, set `Allow users to send mail through an external SMTP server when configuring a "from" address hosted outside your email domain` to `unchecked`
6. Select `Save`

Default Value:

`Allow users to send mail through an external SMTP server when configuring a "from" address hosted outside your email domain` is `unchecked`

3.1.3.5.4 (L1) Ensure external recipient warnings are enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Gmail adds an image or colored border to external addresses.

Rationale:

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

Impact:

When this setting is on, Gmail shows warnings (colored boarder) when:

- An email thread includes external recipients (not available on iOS).
- Replying to a message from an external recipient.
- Composing a new message to an external recipient (not available on iOS).

Gmail doesn't show a warning if the external recipient is in your organization's Directory, personal Contacts, or other Contacts. Warnings aren't displayed for secondary domain or domain alias addresses.

Audit:

To verify Ensure external recipient warnings are 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. Select `End User Access`
6. Under `Warn for external recipients`, ensure `Highlight any external recipients in a conversation. Warn users before they reply to email with external recipients who aren't in their contacts.` is `ON`

Remediation:

To configure external recipient warnings are 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. Select End User Access
6. Select Warn for external recipients
7. Set Highlight any external recipients in a conversation. Warn users before they reply to email with external recipients who aren't in their contacts. to checked
8. Select Save

Default Value:

Highlight any external recipients in a conversation. Warn users before they reply to email with external recipients who aren't in their contacts. is ON

3.1.3.6 Spam, Phishing and Malware

Configure spam, phishing and malware features.

3.1.3.6.1 (L1) Ensure enhanced pre-delivery message scanning is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Enables improved detection of suspicious content prior to delivery.

Rationale:

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

Impact:

With the Enhanced pre-delivery message scanning option, when Gmail detects suspicious content, message delivery is slightly delayed so that Gmail can do additional security checks on the message.

Audit:

To verify this setting via 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. Select `Spam, phishing, and malware`
6. Ensure `Enhanced pre-delivery message scanning.` is `ON`

Remediation:

To configure this setting via 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. Select `Spam, phishing, and malware`
6. Select `Enhanced pre-delivery message scanning.`
7. Set `Enables improved detection of suspicious content prior to delivery` to `checked`
8. Select `Save`

Default Value:

Enhanced pre-delivery message scanning. is ON

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.7 Deploy and Maintain Email Server Anti-Malware Protections Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.			●
v7	7.10 Sandbox All Email Attachments Use sandboxing to analyze and block inbound email attachments with malicious behavior.			●

3.1.3.6.2 (L1) Ensure spam filters are not bypased for internal senders (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

You can configure your advanced Gmail settings to bypass, or not bypass, spam filters for messages received from internal senders.

Rationale:

Turning off this setting reduces the risk of spoofing and phishing/whaling.

Impact:

Your users will be better protected by filtering their email for spam and minimizing the chances for spoofing and phishing/whaling attacks.

Audit:

To verify this setting via 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. Select `Spam, phishing, and malware`
6. Under `Spam`, select `Configure`
7. Ensure `Bypass spam filters for messages received from internal senders.` is `unchecked`

Remediation:

To configure this setting via 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. Select `Spam, phishing, and malware`
6. Under `Spam`, select `Configure`
7. Set `Bypass spam filters for messages received from internal senders.` to `unchecked`
8. Select `Save`

Default Value:

`Bypass spam filters for messages received from internal senders.` is `checked`

3.1.3.7 Compliance

Configure compliance features.

Note on Content Compliance

Google Workspace has extensive capabilities for monitoring Gmail content compliance (incoming and outgoing mail). The use of these capabilities is very organizationally specific, but admins are encouraged to review the capabilities in this area and setup appropriate checks for your organization.

Google documentation for setting up rules for advanced email content filtering is **here**.

3.1.3.7.1 (L1) Ensure comprehensive mail storage is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Comprehensive mail storage ensures messages sent by other core services appear in users' sent folders and are therefore accessible to Vault.

Rationale:

As an administrator, you can ensure that a copy of all sent or received messages in your domain—including messages sent or received by non-Gmail mailboxes—is stored in the associated users' Gmail mailboxes.

Impact:

There are some important considerations to carefully review before enabling comprehensive mail storage:

- You should not enable comprehensive mail storage if you have compliance routing rules that change the recipient (and don't want the original recipient to receive a copy of the email).
- When you have the SMTP Relay service enabled, user mailboxes will keep a copy of the message in the sent folder (for example, when sending mail from a scanner) if comprehensive mail storage is enabled. This might cause accounts to exceed storage limits if your account's edition has storage limits. Compare editions.
- You should enable comprehensive mail storage if you only use Gmail for the Vault feature and forward email to your on-premise mail server or other email provider.

Audit:

To verify this setting via 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. Select `Compliance`
6. Under `Comprehensive mail storage`, ensure `Ensure that a copy of all sent and received mail is stored in associated users' mailboxes` is `ON`

Remediation:

To configure this setting via 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. Select `Compliance`
6. Select `Comprehensive mail storage`
7. Set `Ensure that a copy of all sent and received mail is stored in associated users' mailboxes` to `checked`
8. Select `Save`

Default Value:

`Copy of all sent and received mail is stored in associated users' mailboxes` is `OFF`

3.1.3.7.2 (L1) Ensure 'Send email over a secure TLS connection' Is Enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

The default is that Gmail always tries to send messages over a secure TLS connection. If the receiving server doesn't use TLS, Gmail still sends messages with TLS but the connection isn't secure.

This setting allows the option to require a CA-signed certificate, verify the hostname associated with the certificate, and test the TLS connection.

A padlock image will appear next to the recipient address if the message will be sent with TLS. The padlock shows only for accounts with a Google Workspace subscription that supports S/MIME encryption.

Google Workspace supports TLS versions 1.0, 1.1, 1.2, and 1.3.

Rationale:

Transport Layer Security (TLS) encrypts email messages for security and privacy and prevents unauthorized access of messages when they're sent over internet connections.

Impact:

This should not have an impact on the usage of Gmail.

Audit:

To verify this setting via 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. Select `Compliance`
6. Under `Secure transport (TLS) compliance`, select `Configure`
7. Under `Email messages to affect` ensure `Inbound - all messages` and `Outbound - all messages` are `ON`

Remediation:

To configure this setting via 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. Select `Compliance`
6. Select `Secure transport (TLS) compliance`
7. Select `Configure`
8. Set `Inbound - all messages` and `Outbound - all messages` to `checked`
9. Select `Save`

Note: Enabling the `Inbound - all messages` and `Outbound - all messages` configurations will also, by default, enable `Require CA-signed certificate when delivering outbound messages to the TLS-enabled domains specified above`. This is not a required configuration, but it is recommended.

References:

1. https://support.google.com/a/answer/2520500

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		🟠	🔵
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		🟠	🔵

3.1.4 Google Chat

Google Chat

3.1.4.1 Chat File Sharing

Control how users can share files to people inside and outside of the domain.

3.1.4.1.1 (L1) Ensure external filesharing in Google Chat and Hangouts is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Control how files are shared externally in Google Chat and Hangouts.

Rationale:

Files often contain confidential information, and some organizations, particularly in regulated industries, need to control the flow of this information within and outside of their organization.

Impact:

Users will not be able to share files via chat externally.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `Chat File Sharing`
5. Under `Setting`, verify `External filesharing` is set to `No files`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `Chat File Sharing`
5. Under `Setting`, set `External filesharing` to `No files`
6. Select `Save`

Default Value:

`External filesharing` is `Allow all files`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

3.1.4.1.2 (L2) Ensure internal filesharing in Google Chat and Hangouts is disabled (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

Control how files are shared internally in Google Chat and Hangouts.

Rationale:

Files often contain confidential information, and some organizations, particularly in regulated industries, need to control the flow of this information within and outside of their organization.

Impact:

Users will not be able to share files via chat internally.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `Chat File Sharing`
5. Under `Setting`, verify `Internal filesharing` is set to `No files`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `Chat File Sharing`
5. Under `Setting`, set `Internal filesharing` to `No files`
6. Select `Save`

Default Value:

`Internal filesharing` is `Allow all files`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

3.1.4.2 External Chat Settings

Control how users can chat with people outside the domain.

3.1.4.2.1 (L1) Ensure Google Chat externally is restricted to allowed domains (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Control how users chat with people outside of your organization. If you allow your users to chat externally, you can also allow them to create and join spaces with people outside your organization.

Rationale:

Restricting external chat to only approved domains potentially limits the spread of company information.

Impact:

Users will not be able to chat with users in any external domain, only approved domains. This will require some admin-level approval and allowlist maintenance.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `External Chat Settings`
5. Select `Chat externally`
6. Verify `Allow users to send messages outside <company>` is `ON`
7. Verify `Only allow this for allowlisted domains` is `checked`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `External Chat Settings`
5. Select `Chat externally`
6. Set `Allow users to send messages outside <company>` to `ON`
7. Set `Only allow this for allowlisted domains` to `checked`
8. Select `Save`

Default Value:

- Allow users to send messages outside <company> is set to ON
- Only allow this for allowlisted domains is unchecked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.4.3 External Spaces

Settings for External Spaces.

3.1.4.3.1 (L1) Ensure external spaces in Google Chat and Hangouts are restricted (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Control whether users can create or join spaces within your organization that include external people outside of your organization.

Rationale:

Restricting external spaces to only approved domains potentially limits the spread of company information.

Impact:

Users with this setting turned off or who have editions that don't support external spaces can't create these spaces, but they can join existing spaces with external people

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `External Spaces`
5. Under `Setting`, verify `Allow users at <domain> to create and join spaces with people outside their organization` is `ON`
6. Verify `Only allow users to add people from allowlisted domains` is `checked`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `External Spaces`
5. Under `Setting`, set `Allow users at <domain> to create and join spaces with people outside their organization` to `ON`
6. Set `Only allow users to add people from allowlisted domains` to `checked`
7. Select `Save`

Default Value:

- Allow users at <company> to create and join spaces with people outside their organization is ON
- Only allow users to add people from allowlisted domains is unchecked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.4.4 Chat Apps

Settings for Chat Apps.

3.1.4.4.1 (L1) Ensure allow users to install Chat apps is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Control the use of Chat apps in spaces or direct messages to connect to services in Google Chat and look up information, schedule meetings, or complete tasks. Apps are accounts created by Google, users in your organization, or third parties.

Rationale:

When a user interacts with an app in Chat, the app can see the user's email address, avatar, other basic user information, user locale, timezone, and interaction information. The app can also see the basic user information of other people in the chat, but it can't see their email address or avatar unless they also interact directly with the app.

Chat apps that you install from the Google Workspace Marketplace can be made by developers from outside of your organization.

Using these Chat app need to be carefully controlled (vetted and approved) since a malicious Chat app could allow the exfiltration of company proprietary information.

Impact:

By default users will not be able to install Chat apps.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `Chat apps`
5. Under `Chat apps access settings`, verify `Allow users to install Chat apps` is `OFF`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `Chat apps`
5. Under `Chat apps access settings`, set `Allow users to install Chat apps` to `OFF`
6. Select `Save`

Default Value:

`Allow users to install Chat apps` is `ON`

References:

1. https://developers.google.com/chat/concepts/apps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.1.4.4.2 (L1) Ensure allow users to add and use incoming webhooks is disabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Allow users to configure incoming webhooks and developers to call incoming webhooks to post content. Incoming webhooks let you send asynchronous messages into Google Chat from applications that aren't Chat apps.

Rationale:

Webhook usage should be carefully controlled (vetted and approved) since a malicious application could send bogus information to exposed webhooks and ultimately these users.

Impact:

By default users will have exposed webhooks.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `Chat apps`
5. Under `Chat apps access settings`, verify `Allow users to add and use incoming webhooks` is `OFF`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Chat and classic Hangouts`
4. Select `Chat apps`
5. Under `Chat apps access settings`, set `Allow users to add and use incoming webhooks` to `OFF`

Default Value:

`Allow users to add and use incoming webhooks` is `ON`

References:

1. https://developers.google.com/chat/concepts/apps

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		🟠	🔵
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		🟠	🔵

3.1.5 Google Meet

The CIS Google Workspace Community does not have any specific security recommendations with regard to Google Meet, due to its usage being very organizationally specific.

That being said, are some items that Admins should consider when deploying Google Meet:

- Who should be allowed to create meetings?
- Example: In an education environment possibly configure that only Teachers can be allowed to create a meeting and Students only attend.
- Who can join a meeting?
- Example: In an education environment possibly Teachers can attend any meeting (internally or externally created) and Students can only attend internally created meetings.

Settings you may want to review are:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Google Workspace`
3. Select `Apps`
4. Select `Google Meet`
5. Select `Meet video settings`
   - Select `Recording`- `Let people record their meetings.`
   - Select `Stream`- `Let people stream their meetings.`
6. Select `Meet safety settings`
   - Select `Domain`- `Who can join meetings created by your organization`
   - Select `Access`- `Which meetings users in the organization can join`
   - Select `Joining`- `How users join a meeting (quick access)`
   - Select `Chat`- `Who can send in-call chat messages`
   - Select `Present`- `Who can share their screens in calls`
   - Select `Host management`- `Default host management`

NOTE: To configure this properly will likely require creating different Organizational Units (OUs) to segment users properly and allow different configuration settings to be applied. An informative video on this topic can be found **here**.

3.1.6 Groups for Business

Settings for Groups for Business.

3.1.6.1 (L1) Ensure accessing groups from outside this organization is set to private (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Choose whether people outside your organization can access your groups. Group owners can further restrict access as needed.

Rationale:

Who can externally view groups internal to the organization should be carefully controlled and their access vetted as needed.

Impact:

No one outside your organization can view or search for your groups. External users can email the group if group settings allow.

Audit:

To verify this setting via 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 `Groups for Business`
5. Select `Sharing options`
6. Verify `Accessing groups from outside this organization` is `Private`

Remediation:

To configure this setting via 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 `Groups for Business`
5. Select `Sharing options`
6. Set `Accessing groups from outside this organization` to `Private`
7. Select `Save`

Default Value:

`Accessing groups from outside this organization` is `Private`

References:

1. https://apps.google.com/supportwidget/articlehome?hl=en&article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F10308022%3Fhl%3Den&product_context=10308022&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.6.2 (L1) Ensure creating groups is restricted (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Control who is allowed to create Groups in your organization and if they can have external members.

Rationale:

The organization should have some control over the organizational groups created and the purpose they are for.

Impact:

In a large organization, this may cause too much burden on administrators.

Audit:

To verify this setting via 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 `Groups for Business`
5. Select `Creating groups`
6. Verify `Only organization admins can create groups` is `selected`
7. Verify `Group owners can allow external members Organization admins can always add external members` is `unchecked`
8. Verify `Group owners can allow incoming email from outside the organization` is `unchecked`

Remediation:

To configure this setting via 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 `Groups for Business`
5. Select `Creating groups`
6. Select `Only organization admins can create groups`
7. Set `Group owners can allow external members Organization admins can always add external members` to `unchecked`
8. Set `Group owners can allow incoming email from outside the organization` to `unchecked`
9. Select `Save`

Default Value:

- `Anyone in the organization can create groups` is `selected`
- `Group owners can allow external members Organization admins can always add external members` is `unchecked`
- `Group owners can allow incoming email from outside the organization` is `unchecked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.6.3 (L1) Ensure default for permission to view conversations is restricted (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

By default, only allow group members to view group conversations.

Rationale:

Conversation viewing can always be expanded by exception for certain groups as needed (Need to know), but by default be restricted.

Impact:

No practical impact, since Group members can view conversations in the Group.

Audit:

To verify this setting via 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 `Groups for Business`
5. Select `Sharing options`
6. Verify `Default for permission to view conversations` is `All group members`

Remediation:

To configure this setting via 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 `Groups for Business`
5. Select `Sharing options`
6. Set `Default for permission to view conversations` to `All group members`
7. Select `Save`

Default Value:

`Default for permission to view conversations` is `All organization users`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

3.1.7 Sites

Settings for Sites.

3.1.7.1 (L1) Ensure service status for Google Sites is set to off (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

By default turn off Google Sites for all users.

Rationale:

There is really no reason for every user within an organization to have access to Google Sites. If this capability is needed, it can be enabled and configured for those users and groups by exception as required by the organization to meet specific needs.

Impact:

Users will not be have access to Google Sites.

Audit:

To verify this setting via 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 `Sites`
5. Select `Service status`
6. Verify `Service status` is `OFF for everyone`

Remediation:

To configure this setting via 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 `Sites`
5. Select `Service status`
6. Set `Service status` to `OFF for everyone`
7. Select `Save`

Default Value:

`Service status` is `ON for everyone`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.1.8 Additional Google services

Settings for Additional Google services.

3.1.8.1 (L1) Ensure access to external Google Groups is OFF for Everyone (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Control whether users in your organization can access external groups from their Google Workspace account. External groups are created outside your organization and might include a public community group or a group for a club a user belongs to.

Control access to external groups by turning on or off the Google Groups additional service — a legacy service in your Admin console that does only one thing: It allows or blocks users from accessing external groups from their Google Workspace account.

NOTE: This service has no effect on your organization's internal groups.

Rationale:

In general, most of the organization's personnel do not need to assess external groups. They can be allowed by exception as needed by the business.

Impact:

Users can't access external groups from their Google Workspace account. However, they do continue to receive email digests from groups they're already subscribed to when you turn off the service.

Audit:

To verify this setting via 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 `Additional Google services
5. Scroll down to `Google Groups`
6. Verify it is `OFF for everyone`

Remediation:

To configure this setting via 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 `Additional Google services
5. Scroll down to `Google Groups`
6. Set it to `OFF for everyone`
7. Select `Save`

Default Value:

`Google Groups` is `ON for Everyone`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.1.9 Google Workspace Marketplace

Settings for Google Workspace Marketplace.

3.1.9.1 Settings

Manage access to apps.

3.1.9.1.1 (L1) Ensure users access to Google Workspace Marketplace apps is restricted (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Restrict what Google Marketplace apps a user can install.

Rationale:

Users should only be allowed to install approved and vetted apps. This will limit the overall attack surface for the organization.

Impact:

Users can only install approved Google Marketplace apps. This list will have to be created and maintained.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace Marketplace apps`
4. Select `Settings`
5. Under `Manage Google Workspace Marketplace allowlist access`, verify `Settings to install third-party Google Workspace Marketplace apps:` is set to `Allow users to install and run only selected apps from the Marketplace`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Apps`
3. Select `Google Workspace Marketplace apps`
4. Select `Settings`
5. Under `Manage Google Workspace Marketplace allowlist access`, set `Settings to install third-party Google Workspace Marketplace apps:` to `Allow users to install and run only selected apps from the Marketplace`
6. Select `Save`

Default Value:

Settings to install third-party Google Workspace Marketplace apps: is
Allow users to install and run any app from the Marketplace

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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 Security

The Security section of the Google Workspace Admin Console.

4.1 Authentication

Authentication settings.

4.1.1 2-Step Verification

Configure 2-Step Verification policies.

4.1.1.1 (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 this setting via 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 `unchecked`
8. Under `Methods`, ensure `Any except verification codes via text, phone call` is `selected`

Remediation:

To verify this setting via 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 `unchecked`
8. Under `Methods`, set `Any except verification codes via text, phone call` to `selected`
9. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

4.1.1.2 (L2) Ensure hardware security keys are used for all users in administrative roles and other high-value accounts (Manual)

Profile Applicability:

- Enterprise Level 2

Description:

A hardware security key connects to a user's device using USB (A & C), Lightning, NFC, or Bluetooth connection. Also, many Android phones and Apple iPhones have built-in security keys accessible via Bluetooth and that can be assigned to a Google Workspace account.

The purpose of a physical security key is to provide an additional security layer to high value accounts; in the event of a compromise of a user's credentials (username and password) without the associated security key, the authentication process cannot be successfully completed.

Rationale:

The purpose of a physical security key is to provide an additional security layer to high value accounts; in the event of a compromise of a user's credentials (username and password) without the associated security key, the authentication process cannot be successfully completed.

Hardware security keys help to protect high value accounts from targeted attacks, including phishing attempts.

Adding a hardware security key requirement to your Google privileged accounts adds another layer of depth of protection greater than any other form of two-factor authentication.

Impact:

Users with hardware security keys enabled will need to have physical access to the hardware key in order complete the authentication process and this will force users to adopt a practice of making sure that the physical key is available to them at any point in time that they need to be able to log in.

If a hardware security key is lost or stolen, the impacted user can gain access to their Google account by using a backup MFA process and then remove the lost/stolen key and add another one.

If a hardware security key is stolen, the user's account is not automatically compromised as the hardware key works in conjunction with the user's account credentials (username & password).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Go to `Security` and click on `Authentication`
3. Under `Authentication`, select `2-Step Verification`
4. Ensure the option to `Allow users to turn on 2-Step Verification` is checked
5. Ensure that the `Enforcement` option is set to either `'On'` or `'On from'` with a valid date present
6. Under `Methods` ensure that `Only security key` is selected
7. Under `2-Step Verification policy suspension grace period` ensure that `1 day` is selected
8. Under `Security codes` ensure that `Don't allow users to generate security codes` is selected

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Go to `Security` and click on `Authentication`
3. Under `Authentication`, select `2-Step Verification`
4. Select the option to `Allow users to turn on 2-Step Verification`
5. Under `Enforcement`, enable either `'On'` or else `'On from'` and configure a valid date
6. Under `Methods`, select `Only security key` to force the use of a security key
7. Under `2-Step Verification policy suspension grace period`, select `1 day`
8. Under `Security codes`, select `Don't allow users to generate security codes`
9. Select `Save`

Default Value:

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

References:

1. https://support.google.com/accounts/answer/6103523?hl=En

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 <u>Use Multifactor Authentication For All Administrative Access</u> Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

4.1.1.3 (L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users (Manual)

Profile Applicability:

- Enterprise Level 1

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 this setting via 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 configure this setting via 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`
9. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.3 Require MFA for Externally-Exposed Applications** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		🟠	🔵
v7	**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.		🟠	🔵

4.1.2 Account Recovery

Configure account-recovery policies.

4.1.2.1 (L1) Ensure Super Admin account recovery is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

This option allows Super Admin users to recover access to their accounts if their password has been forgotten.

The option is not available if either *Single Sign On* or *Password Sync* is in use.

Rationale:

Allowing Super Admins to recover access to their accounts when they have forgotten their passwords reduces the number of support tickets generated by users, and reduces the amount of down time spent waiting on the account recovery process to initiate and complete.

Impact:

The potential impact to Super Admins being allowed to recover their accounts includes:

1. The Super Admins are now empowered to reset their passwords.
2. The Super Admins will no longer need to call a helpdesk or open a support ticket to regain access to their account.

An organization that allows users to recover their account will realize less time spent by administrative staff working on these tasks.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Security`.
3. Under `Account recovery` select `Super admin account recovery`.
4. Ensure `Allow super admins to recover their account` is `checked`.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Security`.
3. Under `Account recovery` select `Super admin account recovery`.
4. Set `Allow super admins to recover their account` to `checked`
5. Click `Save`

Default Value:

`Allow super admins to recover their account` is `OFF`

4.1.2.2 (L1) Ensure User account recovery is enabled (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

This option allows non-Super Admin users to recover access to their accounts if their password has been forgotten.

The option is not available if either *Single Sign On* or *Password Sync* is in use.

Rationale:

Allowing users to recover access to their accounts when they have forgotten their passwords reduces the number of support tickets generated by users, and reduces the amount of down time spent waiting on the account recovery process to initiate and complete.

Impact:

The potential impact to users being allowed to recover their accounts includes:

1. The user is now empowered to reset their passwords.
2. The user will no longer need to call a helpdesk or open a support ticket to regain access to their account.

An organization that allows users to recover their account will realize less time spent by administrative staff working on these tasks.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Security`.
3. Select `User account recovery`
4. Verify `Allow users and non-super admins to recover their account` is checked.

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Security`.
3. Select `User account recovery`
4. Select either the pencil icon or the setting itself.
5. Set `Allow users and non-super admins to recover their account` to checked.
6. Select `Save`.

Default Value:

`Allow users and non-super admins to recover their account` is `OFF`

Internal Only - General

4.1.3 Advanced Protection Program

Configure the strongest security settings for those who need it most.

4.1.3.1 (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 this setting via 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 verify this setting via 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`, set `Enable user enrollment` to `selected` for the desired organizational unit or group
5. Under `Security Codes`, set `Do not allow users to generate security codes` to `selected` for the desired organizational unit or group
6. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	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.		●	●

4.1.4 Login Challenges

Manage the information used during login to protect users.

4.1.4.1 (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 this setting via 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 `unchecked`

Remediation:

To configure this setting via 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`, set `Logins using SSO are subject to additional verifications (if appropriate) and 2-Step Verification (if configured)` is `checked`
5. Select `Save`
6. Under `Login challenges`, set `Use employee ID to keep my users more secure` to `unchecked`
7. Select `Save`

Default Value:

- `Post-SSO verification` is `Logins using SSO bypass additional verifications`
- `Use employee ID to keep my users more secure` is `unchecked`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	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.		●	●

4.1.5 Password Management

Configure password policies.

4.1.5.1 (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.

Configuring passwords to expire at a 1 year mark ensures that users are not forced to change passwords so often that easily discerned patterns are used in the creation of the passwords. The day-to-day impact on users will be that they have to manage fewer passwords changing on a frequent basis.

NOTE: Password should be changed immediately on any indication of system compromise, when a user role changes, and when a user leaves the organization.

Audit:

To verify this setting via 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 `14`+
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 `unchecked`
8. Under `Expiration`, ensure `Password reset frequency` is set to `365 Days`

Remediation:

To configure this setting via 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`, set `Enforce strong passwords` to `checked`
5. Under `Length`, set `Minimum Length` to `14` or greater
6. Under `Strength and Length enforcement`, set `Enforce password policy at next sign-in` is `checked`
7. Under `Reuse`, set `Allow password reuse` to `unchecked`
8. Under `Expiration`, set `Password reset frequency` to `365 Days`
9. Select `Save`

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2 Use Unique Passwords** Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**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.		●	●

4.2 Access and Data Control

Access and Data Control settings.

4.2.1 API Controls

Manage OAuth access to third party apps, and manage Domain wide delegation.

4.2.1.1 (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 this setting via the Google Workspace Admin Console:

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

Remediation:

To configure this setting via the Google Workspace Admin Console:

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

Default Value:

Access is Unrestricted

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

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

Profile Applicability:

- Enterprise Level 2

Description:

Weekly 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 verify this setting via the Google Workspace Admin Console:

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

Remediation:

To configure this setting via the Google Workspace Admin Console:

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

Default Value:

None

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**2.1 Establish and Maintain a Software Inventory** Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	●	●	●
v8	**2.3 Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	**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.	●	●	●
v7	**2.6 Address unapproved software** Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

4.2.1.3 (L1) Ensure internal apps can access Google Workspace APIs (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Enable access to Google Workspace APIs for customer-owned / developed applications.

Rationale:

All organization-built internal apps (owned by your organization), can be trusted to access restricted Google Workspace APIs. That way, the organization does not have to trust them all individually.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `API Controls`, then select `App access control`
5. Under `Settings`, verify `Trust internal, domain-owned apps` is `selected`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `API Controls`, then select `App access control`
5. Under `Settings`, select `Trust internal, domain-owned apps`
6. Select `Save`

Default Value:

`Trust internal, domain-owned apps` is `selected`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 <u>Configure Data Access Control Lists</u>** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 <u>Protect Information through Access Control Lists</u>** 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.	●	●	●

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

Profile Applicability:

- Enterprise Level 2

Description:

Weekly review domain-wide delegations for applications for potentially 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 verify this setting via the Google Workspace Admin Console:

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

Remediation:

To configure this setting via the Google Workspace Admin Console:

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

Default Value:

None

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**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.	●	●	●

4.2.2 Context-Aware Access

Use device and user identification to manage access levels and enforce access policies for Google Workspace applications.

4.2.2.1 (L1) Ensure blocking access from unapproved geographic locations (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Restrict access to selected Google applications by geographic location.

Rationale:

Restricting access to known/approved geographic locations is a simple way to limit where attacks can originate from. Especially for smaller organizations that do not need global access to applications.

Impact:

Valid/approved users traveling to a geographic region outside of those defined in the Access Level will not be able to access their applications.

Audit:

To verify this setting via the Google Workspace Admin Console:
Verify an appropriate Access Level has been defined

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `Context-Aware Access`
5. Select `Access levels`
6. Review the list of Access Levels displayed and determine if there is an appropriate restriction on geographic access

Verify the appropriate Access Level has been assigned to the application(s) that need the restriction

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `Context-Aware Access`
5. Select `Assign access levels`
6. Review the list of Google Applications displayed and make sure the appropriate access level for geographic access is assigned to each

NOTE: CIS recommends geographically restricting access to the following Google applications at minimum:

1. Admin Console
2. Drives and Docs
3. Gmail
4. Google Vault

Remediation:

To configure this setting via the Google Workspace Admin Console:
Create an appropriate Access Level

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `Context-Aware Access`
5. Select `Access levels`
6. Select `Create Access Level`
7. Under Details - Name the Access Level (Suggested using a clear name - ex. "Restrict to USA")
8. Under Conditions - Select `Basic`
9. Under Condition 1 - Select `Meet attributes`
10. Under Condition 1 - Select `Add Attribute`
11. Click on the `Add Attribute` drop-down box and select `Geographic origin`
12. Click on the far right drop-down box and select the region, or regions, to be allowed (ex. United States)
13. Click `Save`

Assign the defined Access Level has been assigned to the application(s) that need the restriction

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `Context-Aware Access`
5. Select `Assign access levels`
6. For each application listed that needs this restriction, select `Assign`
7. Under, `Access is granted when a user meets conditions in at least one of the selected access levels`, ensure the previously named Access Level (ex. "Restrict to USA") is `checked`
8. Also, ensure `Apply to Google desktop and mobile apps` is `checked`

NOTE: CIS recommends geographically restricting assess to the following Google applications at minimum:

1. Admin Console
2. Drives and Docs
3. Gmail
4. Google Vault

Default Value:

None

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.2.3 Data Protection

Google Workspace has extensive Data Leak Protection (DLP) capabilities built in based on the licensing level. These capabilities allow admins to confidently secure your company's sensitive data from being leaked to unauthorized parties and manage third-party app access to your Google Services. CIS considers using these capabilities extremely important, but they are also extremely organization dependent. What is considered protected information varies significantly from company to company and region to region.

For example, Google provides a wide variety of detectors organized by type (Credentials and Secrets, Documents, etc.) and region (United States, United Kingdom, Australia, etc.) For the United States alone here are some options for detectors:

- Social Security Number (SSN)
- Driver's License Number
- Drug Enforcement Administration (DEA) Number
- American Bankers Association (ABA) Routing Number
- National Provider Identifier (NPI)
- Committee on Uniform Security Identification Procedures (CUSIP)
- Food and Drug Administration (FDA) Approved Prescription Drugs
- Passport
- State Names
- Adoption Taxpayer Identification Number (ATIN)
- Employer Identification Number (EIN)
- Individual Taxpayer Identification Number (ITIN)
- Toll Free Phone Number
- Vehicle Identification Number (VIN)
- Preparer Taxpayer Identification Number (PTIN)

Admins are encouraged learn more about the DLP capabilities of Google Workspace and setup appropriate DLP rules for their organization.

- An overview of DLP in Google documentation is **here**.
- Details on predefined detectors Google documentation is **here**.
- Details on Regular Expression use in Google documentation is **here**.

Some good videos on Google Workspace usage:

- Detectors Overview is **here**.
- Rules Overview is **here**.
- General demo is **here**.

4.2.3.1 (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 this setting via the Google Workspace Admin Console:

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

Remediation:

To configure this setting via the Google Workspace Admin Console:

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

New rule
Examples can be found **here**.

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

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F10846568%3Fvisit_id%3D638058685723082013-4065283876&product_context=10846568&product_name=UnuFlow&trigger_context=a
2. https://workspaceupdates.googleblog.com/2020/10/data-protection-dlp-reports.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.13 Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v7	**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.			●

4.2.4 Google Session Control

Set session duration for Google core and additional services, such as Gmail and Docs.

4.2.4.1 (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 this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `Google session control`
5. Verify `Web session duration`, is `12 hours` or less

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `Google session control`
5. Set `Web session duration` to `12 hours` or less
6. Select `Save`

Default Value:

`Web session duration` is `14 days`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●

4.2.5 Google Cloud Session Control

Set session duration for Google Cloud Platform console and Google Cloud SDK.

4.2.5.1 (L2) Ensure Google Cloud session control 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 console and Cloud SDK without having to re-authenticate. For example, you might want users with elevated privileges, like project owners, billing administrators, or others with administrator roles, to re-authenticate more frequently than regular users. 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 re-authenticate using their password, they're redirected to the identity provider (IdP). The IdP might not require the user to re-enter their password to start another console session, if the user already has a session active with the IdP—because they are using another application that caused the session to remain active. If a user must re-authenticate by touching their security key, they can do this while using the console. They will not be redirected to the IdP.
- With the Cloud SDK—If a password is required for re-authentication, gcloud will require the user to execute the gcloud auth login command to renew the session. This will bring up a browser window, and the user will be taken to the IdP, where they may be prompted for credentials if there's no active session with the IdP. If a user must reauthenticate by touching their security key, they can do this on the Cloud SDK. They will not be redirected to the IdP.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `Google Cloud session control`
5. Under `Reauthentication policy`, ensure `Require reauthentication` is `selected` and `Exempt Trusted apps` is `unchecked`
6. Verify `Reauthentication frequency`, is `16 hours (recommended)`
7. Verify `Reauthentication method` is `Security key`

Remediation:

To configure this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator
2. Select `Security`
3. Select `Access and Data Control`
4. Select `Google Cloud session control`
5. Under `Reauthentication policy`, set `Require reauthentication` to selected and `Exempt Trusted apps` is `unchecked`
6. Set `Reauthentication frequency` to `16 hours (recommended)`
7. Set `Reauthentication method` to `Security key`
8. Select `Override`

Default Value:

`Reauthentication policy` is `Never require reauthentication`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●

4.2.6 Less Secure Apps

Configure policies to manage access to less-secure apps.

4.2.6.1 (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 this setting via the Google Workspace Admin Console:

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

Remediation:

To configure this setting via the Google Workspace Admin Console:

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

Default Value:

`Disable access to less secure apps (Recommended)` is `selected`

Page 223

4.3 Security Center

Security Reports.

A note on the Investigation tool

The Investigation tool found in the Security center portion of the Google Workspace Admin UI is a powerful tool for investigating various incidents. It is basically a flexible search that has access to essentially all the various logs in Google Workspace. How this tool would be used is very organization-specific and possibly event specific, so CIS does not have any specific recommendations for its use in this Benchmark.

That being said, admins should be aware of this tool and it capabilities, since it will be very useful in detecting and resolving various incidents, so we urge admins to get familiar with the tool. For example, you can use the investigation tool to:

- Access data about devices.
- Access device log data to get a clear view of the devices and applications being used to access your data.
- Access data about Gmail messages, including email content.
- Access Gmail log data to find and erase malicious emails, mark emails as spam or phishing, or send emails to users' inboxes.
- View search results that list suspended users.
- Access Drive log data to investigate file sharing in your organization, investigate the creation and deletion of documents, investigate who accessed documents, and more.

For more information:

- Google Documentation is **here**.
- A useful overview video is **here**.

4.3.1 (L1) Ensure the Dashboard is reviewed regularly for anomalies (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

As an administrator, you can use the security dashboard to see an overview of different security reports. By default, each security report panel displays data from the last 7 days. You can customize the dashboard to view data from Today, Yesterday, This week, Last week, This month, Last month, or Days ago (up to 180 days).

Charts/reports available (Minimum, but could be many more depending on account type):

- DLP incidents
- Top policy incidents
- Failed device password attempts
- Compromised device events
- Suspicious device activities
- OAuth scope grants by product (beta customers only)
- OAuth grant activity
- OAuth grants to new apps
- User login attempts – Challenge method
- User login attempts – Failed
- User login attempts – Suspicious

Details on what each of these charts/reports mean can be found **here**. This report should be reviewed weekly.

NOTE: The availability of each individual report on the security dashboard depends on your Google Workspace edition. See Google documentation for more details.

NOTE: In larger organizations reviewing this entire report weekly may not be possible. At a minimum, all Administrator and Super Administrator users should be reviewed, since they are a higher risk. These can be filtered from the overall user list.

Rationale:

The Security report provides a comprehensive view of how people share and access data and whether they take appropriate security precautions. For example, you can review who installs external apps, shares numerous files, skips 2-Step Verification, and uses security keys.

Impact:

No user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Reporting`
3. Select `Reports`
4. Select `User Reports`
5. Select `Security`, and a table of results will be displayed with the fields listed in the Recommendation description above.
6. Review the displayed users and values for anomalies

Remediation:

The remediation for any anomalies in the various fields varies widely (different sections of the Google Workspace Admin UI). Please refer to Google's documentation for specifics (**here**).
NOTE: Many of these settings will be remedied by implementing other sections of this Benchmark. For example, an Admin not enrolled in 2-Step Verification can be remedied by implementing the Remediation procedure for the recommendation ***Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles***.

Default Value:

The report will display all users and fields.

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F7492330&assistant_id=generic-unu&product_context=7492330&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.11 Conduct Audit Log Reviews** Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	**6.7 Regularly Review Logs** On a regular basis, review logs to identify anomalies or abnormal events.		●	●

4.3.2 (L1) Ensure the Security health is reviewed regularly for anomalies (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

As an administrator, the security health page enables you to monitor the configuration of your Admin console settings from one location. For example, you can check the status of settings like automatic email forwarding, device encryption, Drive sharing settings, and much more.

Settings reported (Minimum, but could be many more depending on account type):

- Blocking of compromised mobile devices
- Mobile management
- Mobile password requirements
- Device encryption
- Mobile inactivity reports
- Auto account wipe
- Application verification
- Installation of mobile applications from unknown sources
- External media storage
- Two-step verification for users
- Two-step verification for admins
- Security key enforcement for admins

Details on what each of these report entries mean can be found **here**. This report should be reviewed weekly.

NOTE: The availability of each individual report on the security dashboard depends on your Google Workspace edition. See Google documentation for more details.

Rationale:

The security health page provides visibility into your Admin console settings to help you better understand and manage security risks. If needed, you can make adjustments to your domain's settings based on general security guidelines and best practices, while balancing these guidelines with your organization's business needs and risk management policy.

Impact:

No user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Security`
3. Select `Security center`
4. Select `Security health`, and a table of results will be displayed with the settings listed in the Recommendation description above.
5. Review the displayed values for anomalies

Remediation:

The remediation for any anomalies in the various settings varies widely (different sections of the Google Workspace Admin UI). Please refer to Google's documentation for specifics (**here**).
NOTE: Many of these settings will be remedied by implementing other sections of this Benchmark. For example, an Admin not enrolled in 2-Step Verification can be remedied by implementing the Remediation procedure for the recommendation *Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles*.

Default Value:

The report will display the status of a predefined group of settings based on your Google Workspace license.

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F7491656&assistant_id=generic-unu&product_context=7491656&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.11 <u>Conduct Audit Log Reviews</u> Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	6.7 <u>Regularly Review Logs</u> On a regular basis, review logs to identify anomalies or abnormal events.		●	●

5 Reporting

The Reporting section of the Google Workspace Admin Console.

This area is quite diverse and there is a wide variety of existing reports available and even more, that can be developed by users. The usefulness of these reports are very organizationally specific and CIS urges companies to explore the various reporting capabilities and tailor them to the organization's needs.

This section will cover a few specific security-related reports that CIS feels are applicable to all organizations and that should be reviewed on a regular basis.

NOTE: Some of the reports will ultimately go to other sections of the UI and these same reports can be accessed there. The "Reports" section just is just a way to consolidate them into one area of the Google Workspace admin UI.

5.1 Reports

The Reports sub-section.

5.1.1 User Reports

User Reports sub-section.

5.1.1.1 (L1) Ensure the App Usage Report is reviewed regularly for anomalies (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

As an administrator, you can use Apps usage reports to get an in-depth understanding of how your users use Google Workspace apps.

Fields Available:

- User
- Gmail storage used (MB)
- Drive storage used (MB)
- Photos storage used (MB)
- Total storage used (MB)
- Storage used (%)
- Classroom - last used time
- Classes created
- Posts created
- Total emails
- Emails sent
- Emails received
- Gmail (IMAP) - last used time
- Gmail (POP) - last used time
- Gmail (Web) - last used time
- Files edited
- Files viewed
- Drive - last active time
- Files added
- Other types added
- Google Docs added
- Google Sheets added
- Google Slides added
- Google Forms added
- Google Drawings added
- Posts
- +1s
- +1s received
- Comments
- Comments received
- Reshares
- Reshares received
- Search queries

- Search queries from web
- Search queries from Android
- Search queries from iOS

Details on what each of these fields mean can be found **here**. This report should be reviewed weekly.

NOTE: In larger organizations reviewing this entire report weekly may not be possible. At a minimum, all Administrator and Super Administrator users should be reviewed, since they are a higher risk. These can be filtered from the overall user list.

Rationale:

The App usage report can allow administrator to discover user that are potentially using application that they do not have access to and/or using in atypical ways.

Impact:

No user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Reporting`
3. Select `Reports`
4. Select `User Reports`
5. Select `App usage`, and a table of results will be displayed with the fields listed in the Recommendation description above.
6. Review the displayed users and values for anomalies

Remediation:

The remediation for any anomalies in the various fields varies widely (different sections of the Google Workspace Admin UI). Please refer to Google's documentation for specifics (**here**).
NOTE: Many of these settings will be remedied by implementing other sections of this Benchmark. For example, an Admin showing recent Gmail (IMAP) - last used time and/or Gmail (POP) - last used time can be remedied by implementing the Remediation procedure for the recommendation ***Ensure POP and IMAP access is disabled for all users***.

Default Value:

The report will display all users and fields.

References:

1. https://apps.google.com/supportwidget/articlehome?hl=en&article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F4579578%3Fhl%3Den&assistant_id=generic-unu&product_context=4579578&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.11 Conduct Audit Log Reviews** Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	**6.7 Regularly Review Logs** On a regular basis, review logs to identify anomalies or abnormal events.		●	●

5.1.1.2 (L1) Ensure the Security Report is reviewed regularly for anomalies (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

As your organization's administrator, you can monitor your users' exposure to data compromise by reviewing the security report.

Fields Available:

- User
- External apps
- 2-Step verification enrollment
- 2-Step verification enforcement
- Password length compliance
- Password strength
- User account status
- Admin status
- Security keys enrolled
- Less secure apps access
- Gmail (IMAP) - last used time
- Gmail (POP) - last used time
- Gmail (Web) - last used time
- External shares
- Internal shares
- Public
- Anyone with link
- Outside domain
- Anyone in domain shares
- Anyone in domain with link shares
- Within domain shares
- Private shares

Details on what each of these fields mean can be found **here**. This report should be reviewed weekly.

NOTE: In larger organizations reviewing this entire report weekly may not be possible. At a minimum, all Administrator and Super Administrator users should be reviewed, since they are a higher risk. These can be filtered from the overall user list.

Rationale:

The Security report provides a comprehensive view of how people share and access data and whether they take appropriate security precautions. For example, you can review who installs external apps, shares numerous files, skips 2-Step Verification, and uses security keys.

Impact:

No user impact.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Reporting`
3. Select `Reports`
4. Select `User Reports`
5. Select `Security`, and a table of results will be displayed with the fields listed in the Recommendation description above.
6. Review the displayed users and values for anomalies

Remediation:

The remediation for any anomalies in the various fields varies widely (different sections of the Google Workspace Admin UI). Please refer to Google's documentation for specifics (**here**).
NOTE: Many of these settings will be remedied by implementing other sections of this Benchmark. For example, an Admin not enrolled in 2-Step Verification can be remedied by implementing the Remediation procedure for the recommendation ***Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles***.

Default Value:

The report will display all users and fields.

References:

1. https://apps.google.com/supportwidget/articlehome?hl=en&article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F6000269%3Fhl%3Den&assistant_id=generic-unu&product_context=6000269&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.11 Conduct Audit Log Reviews** Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.		●	●
v7	**6.7 Regularly Review Logs** On a regular basis, review logs to identify anomalies or abnormal events.		●	●

6 Rules

The Rules section of the UI.

Note on the Rules section

Google Workspace has a powerful notification capability consolidated in the Rules
section of the admin UI. A given organization may want to define a wide variety of rules
to notify key people of various security-related events. This section will provide some
specific recommendations that CIS feels that should be monitored universally, but it only
scratches the surface of possibilities. Admins are encouraged to learn more about how
to define new rules specific to their organization's needs and threats and use them to
their advantage.

- Google documentation on System defined rules is **here**.
- Google documentation on create and manage trust rules for drive sharing rules is
  here.
- Google documentation on admin access to reporting rules & activity rules is
  here.

6.1 (L1) Ensure User's password changed is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configuring and enabling the setting that an alert will be generated when a user's password has changed.

Rationale:

Ensuring that administrators are alerted when user passwords are changed provides organizations with the ability to detect and halt potential attacks involving credential compromise and account takeover.

Impact:

This setting should have no impact on the end user but will send emails to super administrators when triggered.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `User's password changed` and select it.
5. Ensure that `Alerts` is set to `On`.
6. Ensure the `Severity` is set to `Medium`
7. Ensure that `Email Notifications` is set to `On`
8. Ensure that `Email notification recipients` is set to `All super administrators`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `User's password changed` and select it.
5. Within the `Actions` pane, click the edit pencil on the right side of the pane.
6. Select `Send to alert center` (This will result in the alert being set to On).
7. Set the alert severity to `Medium`
8. To enable emails when this alert condition is met, select `Send email notifications`. Once enabled, the `All super administrators` option is selected by default.
9. Click `Review` to confirm the values.
10. Click `Update Rule`.
11. Confirm that the `User's password changed` shows an Alert status of `On` in the list.

Default Value:

`User's password changed` is `OFF`

6.2 (L1) Ensure Government-backed attacks is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configuring and enabling the setting that an alert will be generated when Google believes your users are being targeted by a government-backed attack.

Rationale:

Ensuring that administrators are alerted that they may be being targeted by a government-backed entity allows them time to check their defenses and potentially up their sensitivity for anomalies.

NOTE: Google sends these out of an abundance of caution — the notice does not necessarily mean that the account has been compromised or that there is a widespread attack. Rather, the notice reflects Goggle's assessment that a government-backed attacker has likely attempted to access the user's account or computer through phishing or malware, for example.

Impact:

This setting should have no impact on the end user but will send emails to super administrators when triggered.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Government-backed attacks` and select it.
5. Ensure that `Alerts` is set to `On`.
6. Ensure the `Severity` is set to `High`
7. Ensure that `Email Notifications` is set to `On`
8. Ensure that `Email notification recipients` is set to `All super administrators`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Government-backed attacks` and select it.
5. Within the `Actions` pane, click the edit pencil on the right side of the pane.
6. Select `Send to alert center` (This will result in the alert being set to On).
7. Set the alert severity to `High`
8. To enable emails when this alert condition is met, select `Send email notifications`. Once enabled, the `All super administrators` option is selected by default.
9. Click `Review` to confirm the values.
10. Click `Update Rule`.
11. Confirm that the `Government-backed attacks` shows an Alert status of `On` in the list.

Default Value:

`Government-backed attacks` is `ON`

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F3230421&assistant_id=generic-unu&product_context=3230421&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

6.3 (L1) Ensure User suspended due to suspicious activity is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configuring and enabling the setting that an alert will be generated when Google suspended a user's account due to a potential compromise detected.

Rationale:

Ensuring that administrators are alerted when the account was suspended by Google. The reason for this should be investigated ASAP, since it could be a possible indication of malicious activity. In any case, the user's account was suspended and something will need to be done to allow the user to resume work.

Impact:

Emails will be sent to all super administrators when triggered. Also, the user's account will be suspended and something will need to be done about that based on company policy (investigated, re-enabled, etc.).

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `User suspended due to suspicious activity` and select it.
5. Ensure that `Alerts` is set to `On`.
6. Ensure the `Severity` is set to `High`
7. Ensure that `Email Notifications` is set to `On`
8. Ensure that `Email notification recipients` is set to `All super administrators`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `User suspended due to suspicious activity` and select it.
5. Within the `Actions` pane, click the edit pencil on the right side of the pane.
6. Select `Send to alert center` (This will result in the alert being set to On).
7. Set the alert severity to `High`
8. To enable emails when this alert condition is met, select `Send email notifications`. Once enabled, the `All super administrators` option is selected by default.
9. Click `Review` to confirm the values.
10. Click `Update Rule`.
11. Confirm that the `User suspended due to suspicious activity` shows an Alert status of `On` in the list.

Default Value:

`User suspended due to suspicious activity` is `ON`

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F3230421&assistant_id=generic-unu&product_context=3230421&product_name=UnuFlow&trigger_context=a

6.4 (L1) Ensure User granted Admin privilege is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configuring and enabling the setting that an alert will be generated when a user has been granted an admin privilege.

Rationale:

Ensuring that administrators are alerted when a user is given increased privileges could be an indication of compromise unless this access has been approved.

Impact:

This setting should have no impact on the end user but will send emails to super administrators when triggered.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `User granted Admin privilege` and select it.
5. Ensure that `Alerts` is set to `On`.
6. Ensure the `Severity` is set to `Medium`
7. Ensure that `Email Notifications` is set to `On`
8. Ensure that `Email notification recipients` is set to `All super administrators`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `User granted Admin privilege` and select it.
5. Within the `Actions` pane, click the edit pencil on the right side of the pane.
6. Select `Send to alert center` (This will result in the alert being set to On).
7. Set the alert severity to `Medium`
8. To enable emails when this alert condition is met, select `Send email notifications`. Once enabled, the `All super administrators` option is selected by default.
9. Click `Review` to confirm the values.
10. Click `Update Rule`.
11. Confirm that the `User granted Admin privilege` shows an Alert status of `On` in the list.

Default Value:

`User granted Admin privilege` is `OFF`

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F3230421&assistant_id=generic-unu&product_context=3230421&product_name=UnuFlow&trigger_context=a

6.5 (L1) Ensure Suspicious programmatic login is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configuring and enabling the setting that an alert will be generated when Google detects suspicious login attempts from applications or computer programs.

Rationale:

Ensuring that administrators are alerted when suspicious login attempts occur. This could be an indication of an active attack on the company by an adversary using previously obtained credentials.

Impact:

This setting should have no impact on the end user but will send emails to super administrators when triggered.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Suspicious programmatic login` and select it.
5. Ensure that `Alerts` is set to `On`.
6. Ensure the `Severity` is set to `Low`
7. Ensure that `Email Notifications` is set to `On`
8. Ensure that `Email notification recipients` is set to `All super administrators`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Suspicious programmatic login` and select it.
5. Within the `Actions` pane, click the edit pencil on the right side of the pane.
6. Select `Send to alert center` (This will result in the alert being set to On).
7. Set the alert severity to `Low`
8. To enable emails when this alert condition is met, select `Send email notifications`. Once enabled, the `All super administrators` option is selected by default.
9. Click `Review` to confirm the values.
10. Click `Update Rule`.
11. Confirm that the `Suspicious programmatic login` shows an Alert status of `On` in the list.

Default Value:

`Suspicious programmatic login` is `ON`

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F3230421&assistant_id=generic-unu&product_context=3230421&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

6.6 (L1) Ensure Suspicious login is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configuring and enabling the setting that an alert will be generated when Google detects a sign-in attempt that doesn't match a user's normal behavior, such as a sign-in from an unusual location.

Rationale:

Ensuring that administrators are alerted when suspicious login attempts occur. This could be an indication of an active attack on the company by an adversary using previously obtained credentials.

Impact:

This setting should have no impact on the end user but will send emails to super administrators when triggered.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Suspicious login` and select it.
5. Ensure that `Alerts` is set to `On`.
6. Ensure the `Severity` is set to `Low`
7. Ensure that `Email Notifications` is set to `On`
8. Ensure that `Email notification recipients` is set to `All super administrators`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Suspicious login` and select it.
5. Within the `Actions` pane, click the edit pencil on the right side of the pane.
6. Select `Send to alert center` (This will result in the alert being set to On).
7. Set the alert severity to `Low`
8. To enable emails when this alert condition is met, select `Send email notifications`. Once enabled, the `All super administrators` option is selected by default.
9. Click `Review` to confirm the values.
10. Click `Update Rule`.
11. Confirm that the `Suspicious login` shows an Alert status of `On` in the list.

Default Value:

`Suspicious login` is `ON`

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F3230421&assistant_id=generic-unu&product_context=3230421&product_name=UnuFlow&trigger_context=a

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

6.7 (L1) Ensure Leaked password is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configuring and enabling the setting that an alert will be generated when Google detects compromised credentials requiring a reset of a user's password.

Rationale:

Ensuring that administrators are alerted when Google detects that a user's credentials have been compromised due to a publicized breach. This is usually because the user has reused their credentials at another site that was breached.

Impact:

Emails will be sent to super administrators when triggered and in these cases, the user's password will need to be changed.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Leaked password` and select it.
5. Ensure that `Alerts` is set to `On`.
6. Ensure the `Severity` is set to `Medium`
7. Ensure that `Email Notifications` is set to `On`
8. Ensure that `Email notification recipients` is set to `All super administrators`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Leaked password` and select it.
5. Within the `Actions` pane, click the edit pencil on the right side of the pane.
6. Select `Send to alert center` (This will result in the alert being set to On).
7. Set the alert severity to `High`
8. To enable emails when this alert condition is met, select `Send email notifications`. Once enabled, the `All super administrators` option is selected by default.
9. Click `Review` to confirm the values.
10. Click `Update Rule`.
11. Confirm that the `Leaked password` shows an Alert status of `On` in the list.

Default Value:

`Leaked password` is `ON`

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F3230421&assistant_id=generic-unu&product_context=3230421&product_name=UnuFlow&trigger_context=a

6.8 (L1) Ensure Gmail potential employee spoofing is configured (Manual)

Profile Applicability:

- Enterprise Level 1

Description:

Configuring and enabling the setting that an alert will be generated when Google detects incoming messages are received where a sender's name is in your Google Workspace directory, but the mail is not from your company's domains or domain aliases.

Rationale:

Ensuring that administrators are alerted when the email is being spoofed since this could be an indication of a phishing attempt.

Impact:

This setting should have no impact on the end user but will send emails to super administrators when triggered.

Audit:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Gmail potential employee spoofing` and select it.
5. Ensure that `Alerts` is set to `On`.
6. Ensure the `Severity` is set to `Medium`
7. Ensure that `Email Notifications` is set to `On`
8. Ensure that `Email notification recipients` is set to `All super administrators`

Remediation:

To verify this setting via the Google Workspace Admin Console:

1. Log in to `https://admin.google.com` as an administrator.
2. Select `Rules`
3. Under `Google protects you by default` select `View list`.
4. Scroll to `Gmail potential employee spoofing` and select it.
5. Within the `Actions` pane, click the edit pencil on the right side of the pane.
6. Select `Send to alert center` (This will result in the alert being set to On).
7. Set the alert severity to `Medium`
8. To enable emails when this alert condition is met, select `Send email notifications`. Once enabled, the `All super administrators` option is selected by default.
9. Click `Review` to confirm the values.
10. Click `Update Rule`.
11. Confirm that the `Gmail potential employee spoofing` shows an Alert status of `On` in the list.

Default Value:

`Gmail potential employee spoofing` is `ON`

References:

1. https://apps.google.com/supportwidget/articlehome?article_url=https%3A%2F%2Fsupport.google.com%2Fa%2Fanswer%2F3230421&assistant_id=generic-unu&product_context=3230421&product_name=UnuFlow&trigger_context=a

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Directory**		
1.1	**Users**		
1.1.1	(L1) Ensure more than one Super Admin account exists (Manual)	☐	☐
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist (Manual)	☐	☐
1.1.3	(L1) Ensure super admin accounts are used only for super admin activities (Manual)	☐	☐
1.2	**Directory Settings**		
1.2.1	**Sharing Settings**		
1.2.1.1	(L1) Ensure directory data access is externally restricted (Manual)	☐	☐
2	**Devices**		
3	**Apps**		
3.1	**Google Workspace**		
3.1.1	**Calendar**		
3.1.1.1	**Sharing Settings**		
3.1.1.1.1	(L1) Ensure external sharing options for primary calendars are configured (Manual)	☐	☐
3.1.1.1.2	(L2) Ensure internal sharing options for primary calendars are configured (Manual)	☐	☐
3.1.1.1.3	(L1) Ensure external invitation warnings for Google Calendar are configured (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.1.2	**General Settings**		
3.1.1.2.1	(L1) Ensure external sharing options for secondary calendars are configured (Manual)	☐	☐
3.1.1.2.2	(L2) Ensure internal sharing options for secondary calendars are configured (Manual)	☐	☐
3.1.1.3	**Advanced Settings**		
3.1.1.3.1	(L2) Ensure calendar web offline is disabled (Manual)	☐	☐
3.1.2	**Drive and Docs**		
3.1.2.1	**Sharing Settings**		
3.1.2.1.1	**Sharing Options**		
3.1.2.1.1.1	(L1) Ensure users are warned when they share a file outside their domain (Manual)	☐	☐
3.1.2.1.1.2	(L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted (Manual)	☐	☐
3.1.2.1.1.3	(L2) Ensure document sharing is being controlled by domain with allowlists (Manual)	☐	☐
3.1.2.1.1.4	(L2) Ensure users are warned when they share a file with users in an allowlisted domain (Manual)	☐	☐
3.1.2.1.1.5	(L1) Ensure Access Checker is configured to limit file access (Manual)	☐	☐
3.1.2.1.1.6	(L1) Ensure only users inside your organization can distribute content externally (Manual)	☐	☐
3.1.2.1.2	**Shared Drive Creation**		
3.1.2.1.2.1	(L1) Ensure users can create new shared drives (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.2.1.2.2	(L1) Ensure manager access members cannot modify shared drive settings (Manual)	☐	☐
3.1.2.1.2.3	(L1) Ensure shared drive file access is restricted to members only (Manual)	☐	☐
3.1.2.1.2.4	(L2) Ensure viewers and commenters ability to download, print, and copy files is disabled (Manual)	☐	☐
3.1.2.2	**Features and Applications**		
3.1.2.2.1	(L1) Ensure offline access to documents is disabled (Manual)	☐	☐
3.1.2.2.2	(L1) Ensure desktop access to Drive is disabled (Manual)	☐	☐
3.1.2.2.3	(L1) Ensure Add-Ons is disabled (Manual)	☐	☐
3.1.3	**Gmail**		
3.1.3.1	**User Settings**		
3.1.3.1.1	(L1) Ensure users cannot delegate access to their mailbox (Manual)	☐	☐
3.1.3.1.2	(L1) Ensure offline access to Gmail is disabled (Manual)	☐	☐
3.1.3.2	**Authenticate email**		
3.1.3.2.1	(L1) Ensure that DKIM is enabled for all mail enabled domains (Manual)	☐	☐
3.1.3.2.2	(L1) Ensure the SPF record is configured for all mail enabled domains (Manual)	☐	☐
3.1.3.2.3	(L1) Ensure the DMARC record is configured for all mail enabled domains (Manual)	☐	☐
3.1.3.3	**Manage Quarantines**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.3.3.1	(L1) Enable quarantine admin notifications for Gmail (Manual)	☐	☐
3.1.3.4	**Safety**		
3.1.3.4.1	**Attachments**		
3.1.3.4.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled (Manual)	☐	☐
3.1.3.4.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled (Manual)	☐	☐
3.1.3.4.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled (Manual)	☐	☐
3.1.3.4.2	**Links and external images**		
3.1.3.4.2.1	(L1) Ensure link identification behind shortened URLs is enabled (Manual)	☐	☐
3.1.3.4.2.2	(L1) Ensure scan linked images for malicious content is enabled (Manual)	☐	☐
3.1.3.4.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains (Manual)	☐	☐
3.1.3.4.3	**Spoofing and authentication**		
3.1.3.4.3.1	(L1) Ensure protection against domain spoofing based on similar domain names is enabled (Manual)	☐	☐
3.1.3.4.3.2	(L1) Ensure protection against spoofing of employee names is enabled (Manual)	☐	☐
3.1.3.4.3.3	(L1) Ensure protection against inbound emails spoofing your domain is enabled (Manual)	☐	☐
3.1.3.4.3.4	(L1) Ensure protection against any unauthenticated emails is enabled (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.3.4.3.5	(L1) Ensure groups are protected from inbound emails spoofing your domain (Manual)	☐	☐
3.1.3.5	**End User Access**		
3.1.3.5.1	(L2) Ensure POP and IMAP access is disabled for all users (Manual)	☐	☐
3.1.3.5.2	(L1) Ensure automatic forwarding options are disabled (Manual)	☐	☐
3.1.3.5.3	(L1) Ensure per-user outbound gateways is disabled (Manual)	☐	☐
3.1.3.5.4	(L1) Ensure external recipient warnings are enabled (Manual)	☐	☐
3.1.3.6	**Spam, Phishing and Malware**		
3.1.3.6.1	(L1) Ensure enhanced pre-delivery message scanning is enabled (Manual)	☐	☐
3.1.3.6.2	(L1) Ensure spam filters are not bypassed for internal senders (Manual)	☐	☐
3.1.3.7	**Compliance**		
3.1.3.7.1	(L1) Ensure comprehensive mail storage is enabled (Manual)	☐	☐
3.1.3.7.2	(L1) Ensure 'Send email over a secure TLS connection' Is Enabled (Manual)	☐	☐
3.1.4	**Google Chat**		
3.1.4.1	**Chat File Sharing**		
3.1.4.1.1	(L1) Ensure external filesharing in Google Chat and Hangouts is disabled (Manual)	☐	☐
3.1.4.1.2	(L2) Ensure internal filesharing in Google Chat and Hangouts is disabled (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.4.2	**External Chat Settings**		
3.1.4.2.1	(L1) Ensure Google Chat externally is restricted to allowed domains (Manual)	☐	☐
3.1.4.3	**External Spaces**		
3.1.4.3.1	(L1) Ensure external spaces in Google Chat and Hangouts are restricted (Manual)	☐	☐
3.1.4.4	**Chat Apps**		
3.1.4.4.1	(L1) Ensure allow users to install Chat apps is disabled (Manual)	☐	☐
3.1.4.4.2	(L1) Ensure allow users to add and use incoming webhooks is disabled (Manual)	☐	☐
3.1.5	**Google Meet**		
3.1.6	**Groups for Business**		
3.1.6.1	(L1) Ensure accessing groups from outside this organization is set to private (Manual)	☐	☐
3.1.6.2	(L1) Ensure creating groups is restricted (Manual)	☐	☐
3.1.6.3	(L1) Ensure default for permission to view conversations is restricted (Manual)	☐	☐
3.1.7	**Sites**		
3.1.7.1	(L1) Ensure service status for Google Sites is set to off (Manual)	☐	☐
3.1.8	**Additional Google services**		
3.1.8.1	(L1) Ensure access to external Google Groups is OFF for Everyone (Manual)	☐	☐
3.1.9	**Google Workspace Marketplace**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.9.1	**Settings**		
3.1.9.1.1	(L1) Ensure users access to Google Workspace Marketplace apps is restricted (Manual)	☐	☐
4	**Security**		
4.1	**Authentication**		
4.1.1	**2-Step Verification**		
4.1.1.1	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles (Manual)	☐	☐
4.1.1.2	(L2) Ensure hardware security keys are used for all users in administrative roles and other high-value accounts (Manual)	☐	☐
4.1.1.3	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users (Manual)	☐	☐
4.1.2	**Account Recovery**		
4.1.2.1	(L1) Ensure Super Admin account recovery is enabled (Manual)	☐	☐
4.1.2.2	(L1) Ensure User account recovery is enabled (Manual)	☐	☐
4.1.3	**Advanced Protection Program**		
4.1.3.1	(L2) Ensure Advanced Protection Program is configured (Manual)	☐	☐
4.1.4	**Login Challenges**		
4.1.4.1	(L2) Ensure login challenges are enforced (Manual)	☐	☐
4.1.5	**Password Management**		
4.1.5.1	(L1) Ensure password policy is configured for enhanced security (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2	**Access and Data Control**		
4.2.1	**API Controls**		
4.2.1.1	(L2) Ensure application access to Google services is restricted (Manual)	☐	☐
4.2.1.2	(L2) Review third-party applications periodically (Manual)	☐	☐
4.2.1.3	(L1) Ensure internal apps can access Google Workspace APIs (Manual)	☐	☐
4.2.1.4	(L2) Review domain-wide delegation for applications periodically (Manual)	☐	☐
4.2.2	**Context-Aware Access**		
4.2.2.1	(L1) Ensure blocking access from unapproved geographic locations (Manual)	☐	☐
4.2.3	**Data Protection**		
4.2.3.1	(L1) Ensure DLP policies for Google Drive are configured (Manual)	☐	☐
4.2.4	**Google Session Control**		
4.2.4.1	(L1) Ensure Google session control is configured (Manual)	☐	☐
4.2.5	**Google Cloud Session Control**		
4.2.5.1	(L2) Ensure Google Cloud session control is configured (Manual)	☐	☐
4.2.6	**Less Secure Apps**		
4.2.6.1	(L1) Ensure less secure app access is disabled (Manual)	☐	☐
4.3	**Security Center**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.3.1	(L1) Ensure the Dashboard is reviewed regularly for anomalies (Manual)	☐	☐
4.3.2	(L1) Ensure the Security health is reviewed regularly for anomalies (Manual)	☐	☐
5	**Reporting**		
5.1	**Reports**		
5.1.1	**User Reports**		
5.1.1.1	(L1) Ensure the App Usage Report is reviewed regularly for anomalies (Manual)	☐	☐
5.1.1.2	(L1) Ensure the Security Report is reviewed regularly for anomalies (Manual)	☐	☐
6	**Rules**		
6.1	(L1) Ensure User's password changed is configured (Manual)	☐	☐
6.2	(L1) Ensure Government-backed attacks is configured (Manual)	☐	☐
6.3	(L1) Ensure User suspended due to suspicious activity is configured (Manual)	☐	☐
6.4	(L1) Ensure User granted Admin privilege is configured (Manual)	☐	☐
6.5	(L1) Ensure Suspicious programmatic login is configured (Manual)	☐	☐
6.6	(L1) Ensure Suspicious login is configured (Manual)	☐	☐
6.7	(L1) Ensure Leaked password is configured (Manual)	☐	☐
6.8	(L1) Ensure Gmail potential employee spoofing is configured (Manual)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1.1.1.1	(L1) Ensure external sharing options for primary calendars are configured	☐	☐
3.1.1.1.2	(L2) Ensure internal sharing options for primary calendars are configured	☐	☐
3.1.1.2.1	(L1) Ensure external sharing options for secondary calendars are configured	☐	☐
3.1.1.2.2	(L2) Ensure internal sharing options for secondary calendars are configured	☐	☐
3.1.2.1.1.2	(L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted	☐	☐
3.1.2.1.1.3	(L2) Ensure document sharing is being controlled by domain with allowlists	☐	☐
3.1.2.1.1.5	(L1) Ensure Access Checker is configured to limit file access	☐	☐
3.1.2.1.1.6	(L1) Ensure only users inside your organization can distribute content externally	☐	☐
3.1.2.1.2.2	(L1) Ensure manager access members cannot modify shared drive settings	☐	☐
3.1.2.1.2.3	(L1) Ensure shared drive file access is restricted to members only	☐	☐
3.1.2.1.2.4	(L2) Ensure viewers and commenters ability to download, print, and copy files is disabled	☐	☐
3.1.3.1.1	(L1) Ensure users cannot delegate access to their mailbox	☐	☐
3.1.4.2.1	(L1) Ensure Google Chat externally is restricted to allowed domains	☐	☐
3.1.4.3.1	(L1) Ensure external spaces in Google Chat and Hangouts are restricted	☐	☐
3.1.6.1	(L1) Ensure accessing groups from outside this organization is set to private	☐	☐
3.1.6.2	(L1) Ensure creating groups is restricted	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.6.3	(L1) Ensure default for permission to view conversations is restricted	☐	☐
3.1.9.1.1	(L1) Ensure users access to Google Workspace Marketplace apps is restricted	☐	☐
4.2.1.1	(L2) Ensure application access to Google services is restricted	☐	☐
4.2.1.2	(L2) Review third-party applications periodically	☐	☐
4.2.1.3	(L1) Ensure internal apps can access Google Workspace APIs	☐	☐
4.2.1.4	(L2) Review domain-wide delegation for applications periodically	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	☐	☐
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	☐	☐
1.1.3	(L1) Ensure super admin accounts are used only for super admin activities	☐	☐
3.1.1.1.1	(L1) Ensure external sharing options for primary calendars are configured	☐	☐
3.1.1.1.2	(L2) Ensure internal sharing options for primary calendars are configured	☐	☐
3.1.1.2.1	(L1) Ensure external sharing options for secondary calendars are configured	☐	☐
3.1.1.2.2	(L2) Ensure internal sharing options for secondary calendars are configured	☐	☐
3.1.1.3.1	(L2) Ensure calendar web offline is disabled	☐	☐
3.1.2.1.1.2	(L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted	☐	☐
3.1.2.1.1.3	(L2) Ensure document sharing is being controlled by domain with allowlists	☐	☐
3.1.2.1.1.5	(L1) Ensure Access Checker is configured to limit file access	☐	☐
3.1.2.1.1.6	(L1) Ensure only users inside your organization can distribute content externally	☐	☐
3.1.2.1.2.2	(L1) Ensure manager access members cannot modify shared drive settings	☐	☐
3.1.2.1.2.3	(L1) Ensure shared drive file access is restricted to members only	☐	☐
3.1.2.1.2.4	(L2) Ensure viewers and commenters ability to download, print, and copy files is disabled	☐	☐
3.1.2.2.2	(L1) Ensure desktop access to Drive is disabled	☐	☐
3.1.2.2.3	(L1) Ensure Add-Ons is disabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.3.1.1	(L1) Ensure users cannot delegate access to their mailbox	☐	☐
3.1.3.1.2	(L1) Ensure offline access to Gmail is disabled	☐	☐
3.1.3.2.1	(L1) Ensure that DKIM is enabled for all mail enabled domains	☐	☐
3.1.3.2.2	(L1) Ensure the SPF record is configured for all mail enabled domains	☐	☐
3.1.3.2.3	(L1) Ensure the DMARC record is configured for all mail enabled domains	☐	☐
3.1.3.4.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled	☐	☐
3.1.3.4.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled	☐	☐
3.1.3.4.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled	☐	☐
3.1.3.4.2.1	(L1) Ensure link identification behind shortened URLs is enabled	☐	☐
3.1.3.4.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains	☐	☐
3.1.3.4.3.1	(L1) Ensure protection against domain spoofing based on similar domain names is enabled	☐	☐
3.1.3.4.3.3	(L1) Ensure protection against inbound emails spoofing your domain is enabled	☐	☐
3.1.3.4.3.4	(L1) Ensure protection against any unauthenticated emails is enabled	☐	☐
3.1.3.4.3.5	(L1) Ensure groups are protected from inbound emails spoofing your domain	☐	☐
3.1.3.5.1	(L2) Ensure POP and IMAP access is disabled for all users	☐	☐
3.1.3.5.2	(L1) Ensure automatic forwarding options are disabled	☐	☐
3.1.3.7.2	(L1) Ensure 'Send email over a secure TLS connection' Is Enabled	☐	☐
3.1.4.2.1	(L1) Ensure Google Chat externally is restricted to allowed domains	☐	☐
3.1.4.3.1	(L1) Ensure external spaces in Google Chat and Hangouts are restricted	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.4.4.1	(L1) Ensure allow users to install Chat apps is disabled	☐	☐
3.1.4.4.2	(L1) Ensure allow users to add and use incoming webhooks is disabled	☐	☐
3.1.6.1	(L1) Ensure accessing groups from outside this organization is set to private	☐	☐
3.1.6.2	(L1) Ensure creating groups is restricted	☐	☐
3.1.6.3	(L1) Ensure default for permission to view conversations is restricted	☐	☐
3.1.7.1	(L1) Ensure service status for Google Sites is set to off	☐	☐
3.1.8.1	(L1) Ensure access to external Google Groups is OFF for Everyone	☐	☐
3.1.9.1.1	(L1) Ensure users access to Google Workspace Marketplace apps is restricted	☐	☐
4.1.1.1	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles	☐	☐
4.1.1.2	(L2) Ensure hardware security keys are used for all users in administrative roles and other high-value accounts	☐	☐
4.1.1.3	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users	☐	☐
4.1.3.1	(L2) Ensure Advanced Protection Program is configured	☐	☐
4.1.4.1	(L2) Ensure login challenges are enforced	☐	☐
4.1.5.1	(L1) Ensure password policy is configured for enhanced security	☐	☐
4.2.1.1	(L2) Ensure application access to Google services is restricted	☐	☐
4.2.1.2	(L2) Review third-party applications periodically	☐	☐
4.2.1.3	(L1) Ensure internal apps can access Google Workspace APIs	☐	☐
4.2.1.4	(L2) Review domain-wide delegation for applications periodically	☐	☐
4.3.1	(L1) Ensure the Dashboard is reviewed regularly for anomalies	☐	☐
4.3.2	(L1) Ensure the Security health is reviewed regularly for anomalies	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.1	(L1) Ensure the App Usage Report is reviewed regularly for anomalies	☐	☐
5.1.1.2	(L1) Ensure the Security Report is reviewed regularly for anomalies	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	☐	☐
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	☐	☐
1.1.3	(L1) Ensure super admin accounts are used only for super admin activities	☐	☐
3.1.1.1.1	(L1) Ensure external sharing options for primary calendars are configured	☐	☐
3.1.1.1.2	(L2) Ensure internal sharing options for primary calendars are configured	☐	☐
3.1.1.2.1	(L1) Ensure external sharing options for secondary calendars are configured	☐	☐
3.1.1.2.2	(L2) Ensure internal sharing options for secondary calendars are configured	☐	☐
3.1.1.3.1	(L2) Ensure calendar web offline is disabled	☐	☐
3.1.2.1.1.2	(L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted	☐	☐
3.1.2.1.1.3	(L2) Ensure document sharing is being controlled by domain with allowlists	☐	☐
3.1.2.1.1.5	(L1) Ensure Access Checker is configured to limit file access	☐	☐
3.1.2.1.1.6	(L1) Ensure only users inside your organization can distribute content externally	☐	☐
3.1.2.1.2.2	(L1) Ensure manager access members cannot modify shared drive settings	☐	☐
3.1.2.1.2.3	(L1) Ensure shared drive file access is restricted to members only	☐	☐
3.1.2.1.2.4	(L2) Ensure viewers and commenters ability to download, print, and copy files is disabled	☐	☐
3.1.2.2.2	(L1) Ensure desktop access to Drive is disabled	☐	☐
3.1.2.2.3	(L1) Ensure Add-Ons is disabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.3.1.1	(L1) Ensure users cannot delegate access to their mailbox	☐	☐
3.1.3.1.2	(L1) Ensure offline access to Gmail is disabled	☐	☐
3.1.3.2.1	(L1) Ensure that DKIM is enabled for all mail enabled domains	☐	☐
3.1.3.2.2	(L1) Ensure the SPF record is configured for all mail enabled domains	☐	☐
3.1.3.2.3	(L1) Ensure the DMARC record is configured for all mail enabled domains	☐	☐
3.1.3.4.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled	☐	☐
3.1.3.4.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled	☐	☐
3.1.3.4.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled	☐	☐
3.1.3.4.2.1	(L1) Ensure link identification behind shortened URLs is enabled	☐	☐
3.1.3.4.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains	☐	☐
3.1.3.4.3.1	(L1) Ensure protection against domain spoofing based on similar domain names is enabled	☐	☐
3.1.3.4.3.3	(L1) Ensure protection against inbound emails spoofing your domain is enabled	☐	☐
3.1.3.4.3.4	(L1) Ensure protection against any unauthenticated emails is enabled	☐	☐
3.1.3.4.3.5	(L1) Ensure groups are protected from inbound emails spoofing your domain	☐	☐
3.1.3.5.1	(L2) Ensure POP and IMAP access is disabled for all users	☐	☐
3.1.3.5.2	(L1) Ensure automatic forwarding options are disabled	☐	☐
3.1.3.6.1	(L1) Ensure enhanced pre-delivery message scanning is enabled	☐	☐
3.1.3.7.2	(L1) Ensure 'Send email over a secure TLS connection' Is Enabled	☐	☐
3.1.4.2.1	(L1) Ensure Google Chat externally is restricted to allowed domains	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.4.3.1	(L1) Ensure external spaces in Google Chat and Hangouts are restricted	☐	☐
3.1.4.4.1	(L1) Ensure allow users to install Chat apps is disabled	☐	☐
3.1.4.4.2	(L1) Ensure allow users to add and use incoming webhooks is disabled	☐	☐
3.1.6.1	(L1) Ensure accessing groups from outside this organization is set to private	☐	☐
3.1.6.2	(L1) Ensure creating groups is restricted	☐	☐
3.1.6.3	(L1) Ensure default for permission to view conversations is restricted	☐	☐
3.1.7.1	(L1) Ensure service status for Google Sites is set to off	☐	☐
3.1.8.1	(L1) Ensure access to external Google Groups is OFF for Everyone	☐	☐
3.1.9.1.1	(L1) Ensure users access to Google Workspace Marketplace apps is restricted	☐	☐
4.1.1.1	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles	☐	☐
4.1.1.2	(L2) Ensure hardware security keys are used for all users in administrative roles and other high-value accounts	☐	☐
4.1.1.3	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users	☐	☐
4.1.3.1	(L2) Ensure Advanced Protection Program is configured	☐	☐
4.1.4.1	(L2) Ensure login challenges are enforced	☐	☐
4.1.5.1	(L1) Ensure password policy is configured for enhanced security	☐	☐
4.2.1.1	(L2) Ensure application access to Google services is restricted	☐	☐
4.2.1.2	(L2) Review third-party applications periodically	☐	☐
4.2.1.3	(L1) Ensure internal apps can access Google Workspace APIs	☐	☐
4.2.1.4	(L2) Review domain-wide delegation for applications periodically	☐	☐
4.2.2.1	(L1) Ensure blocking access from unapproved geographic locations	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.2.3.1	(L1) Ensure DLP policies for Google Drive are configured	☐	☐
4.3.1	(L1) Ensure the Dashboard is reviewed regularly for anomalies	☐	☐
4.3.2	(L1) Ensure the Security health is reviewed regularly for anomalies	☐	☐
5.1.1.1	(L1) Ensure the App Usage Report is reviewed regularly for anomalies	☐	☐
5.1.1.2	(L1) Ensure the Security Report is reviewed regularly for anomalies	☐	☐
6.2	(L1) Ensure Government-backed attacks is configured	☐	☐
6.5	(L1) Ensure Suspicious programmatic login is configured	☐	☐
6.6	(L1) Ensure Suspicious login is configured	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.2.1.1	(L1) Ensure directory data access is externally restricted	☐	☐
3.1.1.1.3	(L1) Ensure external invitation warnings for Google Calendar are configured	☐	☐
3.1.2.1.1.1	(L1) Ensure users are warned when they share a file outside their domain	☐	☐
3.1.2.1.1.4	(L2) Ensure users are warned when they share a file with users in an allowlisted domain	☐	☐
3.1.2.1.2.1	(L1) Ensure users can create new shared drives	☐	☐
3.1.2.2.1	(L1) Ensure offline access to documents is disabled	☐	☐
3.1.3.3.1	(L1) Enable quarantine admin notifications for Gmail	☐	☐
3.1.3.4.2.2	(L1) Ensure scan linked images for malicious content is enabled	☐	☐
3.1.3.4.3.2	(L1) Ensure protection against spoofing of employee names is enabled	☐	☐
3.1.3.5.3	(L1) Ensure per-user outbound gateways is disabled	☐	☐
3.1.3.5.4	(L1) Ensure external recipient warnings are enabled	☐	☐
3.1.3.6.2	(L1) Ensure spam filters are not bypassed for internal senders	☐	☐
3.1.3.7.1	(L1) Ensure comprehensive mail storage is enabled	☐	☐
3.1.4.1.1	(L1) Ensure external filesharing in Google Chat and Hangouts is disabled	☐	☐
3.1.4.1.2	(L2) Ensure internal filesharing in Google Chat and Hangouts is disabled	☐	☐
4.1.2.1	(L1) Ensure Super Admin account recovery is enabled	☐	☐
4.1.2.2	(L1) Ensure User account recovery is enabled	☐	☐
4.2.4.1	(L1) Ensure Google session control is configured	☐	☐
4.2.5.1	(L2) Ensure Google Cloud session control is configured	☐	☐
4.2.6.1	(L1) Ensure less secure app access is disabled	☐	☐
6.1	(L1) Ensure User's password changed is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.3	(L1) Ensure User suspended due to suspicious activity is configured	☐	☐
6.4	(L1) Ensure User granted Admin privilege is configured	☐	☐
6.7	(L1) Ensure Leaked password is configured	☐	☐
6.8	(L1) Ensure Gmail potential employee spoofing is configured	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	☐	☐
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	☐	☐
1.1.3	(L1) Ensure super admin accounts are used only for super admin activities	☐	☐
3.1.1.1.1	(L1) Ensure external sharing options for primary calendars are configured	☐	☐
3.1.1.1.2	(L2) Ensure internal sharing options for primary calendars are configured	☐	☐
3.1.1.2.1	(L1) Ensure external sharing options for secondary calendars are configured	☐	☐
3.1.1.2.2	(L2) Ensure internal sharing options for secondary calendars are configured	☐	☐
3.1.2.1.1.2	(L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted	☐	☐
3.1.2.1.1.3	(L2) Ensure document sharing is being controlled by domain with allowlists	☐	☐
3.1.2.1.1.5	(L1) Ensure Access Checker is configured to limit file access	☐	☐
3.1.2.1.1.6	(L1) Ensure only users inside your organization can distribute content externally	☐	☐
3.1.2.1.2.2	(L1) Ensure manager access members cannot modify shared drive settings	☐	☐
3.1.2.1.2.3	(L1) Ensure shared drive file access is restricted to members only	☐	☐
3.1.2.1.2.4	(L2) Ensure viewers and commenters ability to download, print, and copy files is disabled	☐	☐
3.1.3.1.1	(L1) Ensure users cannot delegate access to their mailbox	☐	☐
3.1.4.2.1	(L1) Ensure Google Chat externally is restricted to allowed domains	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.4.3.1	(L1) Ensure external spaces in Google Chat and Hangouts are restricted	☐	☐
3.1.6.1	(L1) Ensure accessing groups from outside this organization is set to private	☐	☐
3.1.6.2	(L1) Ensure creating groups is restricted	☐	☐
3.1.6.3	(L1) Ensure default for permission to view conversations is restricted	☐	☐
3.1.9.1.1	(L1) Ensure users access to Google Workspace Marketplace apps is restricted	☐	☐
4.1.1.1	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles	☐	☐
4.1.1.2	(L2) Ensure hardware security keys are used for all users in administrative roles and other high-value accounts	☐	☐
4.1.5.1	(L1) Ensure password policy is configured for enhanced security	☐	☐
4.2.1.1	(L2) Ensure application access to Google services is restricted	☐	☐
4.2.1.2	(L2) Review third-party applications periodically	☐	☐
4.2.1.3	(L1) Ensure internal apps can access Google Workspace APIs	☐	☐
4.2.1.4	(L2) Review domain-wide delegation for applications periodically	☐	☐
4.2.4.1	(L1) Ensure Google session control is configured	☐	☐
4.2.5.1	(L2) Ensure Google Cloud session control is configured	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	☐	☐
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	☐	☐
1.1.3	(L1) Ensure super admin accounts are used only for super admin activities	☐	☐
3.1.1.1.1	(L1) Ensure external sharing options for primary calendars are configured	☐	☐
3.1.1.1.2	(L2) Ensure internal sharing options for primary calendars are configured	☐	☐
3.1.1.2.1	(L1) Ensure external sharing options for secondary calendars are configured	☐	☐
3.1.1.2.2	(L2) Ensure internal sharing options for secondary calendars are configured	☐	☐
3.1.1.3.1	(L2) Ensure calendar web offline is disabled	☐	☐
3.1.2.1.1.2	(L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted	☐	☐
3.1.2.1.1.3	(L2) Ensure document sharing is being controlled by domain with allowlists	☐	☐
3.1.2.1.1.5	(L1) Ensure Access Checker is configured to limit file access	☐	☐
3.1.2.1.1.6	(L1) Ensure only users inside your organization can distribute content externally	☐	☐
3.1.2.1.2.2	(L1) Ensure manager access members cannot modify shared drive settings	☐	☐
3.1.2.1.2.3	(L1) Ensure shared drive file access is restricted to members only	☐	☐
3.1.2.1.2.4	(L2) Ensure viewers and commenters ability to download, print, and copy files is disabled	☐	☐
3.1.2.2.1	(L1) Ensure offline access to documents is disabled	☐	☐
3.1.2.2.2	(L1) Ensure desktop access to Drive is disabled	☐	☐
3.1.2.2.3	(L1) Ensure Add-Ons is disabled	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
3.1.3.1.1	(L1) Ensure users cannot delegate access to their mailbox	☐	☐
3.1.3.1.2	(L1) Ensure offline access to Gmail is disabled	☐	☐
3.1.3.2.1	(L1) Ensure that DKIM is enabled for all mail enabled domains	☐	☐
3.1.3.2.2	(L1) Ensure the SPF record is configured for all mail enabled domains	☐	☐
3.1.3.2.3	(L1) Ensure the DMARC record is configured for all mail enabled domains	☐	☐
3.1.3.4.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled	☐	☐
3.1.3.4.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled	☐	☐
3.1.3.4.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled	☐	☐
3.1.3.4.2.1	(L1) Ensure link identification behind shortened URLs is enabled	☐	☐
3.1.3.4.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains	☐	☐
3.1.3.4.3.1	(L1) Ensure protection against domain spoofing based on similar domain names is enabled	☐	☐
3.1.3.4.3.3	(L1) Ensure protection against inbound emails spoofing your domain is enabled	☐	☐
3.1.3.4.3.4	(L1) Ensure protection against any unauthenticated emails is enabled	☐	☐
3.1.3.4.3.5	(L1) Ensure groups are protected from inbound emails spoofing your domain	☐	☐
3.1.3.5.1	(L2) Ensure POP and IMAP access is disabled for all users	☐	☐
3.1.3.5.2	(L1) Ensure automatic forwarding options are disabled	☐	☐
3.1.3.7.2	(L1) Ensure 'Send email over a secure TLS connection' Is Enabled	☐	☐
3.1.4.1.1	(L1) Ensure external filesharing in Google Chat and Hangouts is disabled	☐	☐
3.1.4.1.2	(L2) Ensure internal filesharing in Google Chat and Hangouts is disabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.4.2.1	(L1) Ensure Google Chat externally is restricted to allowed domains	☐	☐
3.1.4.3.1	(L1) Ensure external spaces in Google Chat and Hangouts are restricted	☐	☐
3.1.4.4.1	(L1) Ensure allow users to install Chat apps is disabled	☐	☐
3.1.4.4.2	(L1) Ensure allow users to add and use incoming webhooks is disabled	☐	☐
3.1.6.1	(L1) Ensure accessing groups from outside this organization is set to private	☐	☐
3.1.6.2	(L1) Ensure creating groups is restricted	☐	☐
3.1.6.3	(L1) Ensure default for permission to view conversations is restricted	☐	☐
3.1.7.1	(L1) Ensure service status for Google Sites is set to off	☐	☐
3.1.8.1	(L1) Ensure access to external Google Groups is OFF for Everyone	☐	☐
3.1.9.1.1	(L1) Ensure users access to Google Workspace Marketplace apps is restricted	☐	☐
4.1.1.1	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles	☐	☐
4.1.1.2	(L2) Ensure hardware security keys are used for all users in administrative roles and other high-value accounts	☐	☐
4.1.1.3	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users	☐	☐
4.1.3.1	(L2) Ensure Advanced Protection Program is configured	☐	☐
4.1.4.1	(L2) Ensure login challenges are enforced	☐	☐
4.1.5.1	(L1) Ensure password policy is configured for enhanced security	☐	☐
4.2.1.1	(L2) Ensure application access to Google services is restricted	☐	☐
4.2.1.2	(L2) Review third-party applications periodically	☐	☐
4.2.1.3	(L1) Ensure internal apps can access Google Workspace APIs	☐	☐
4.2.1.4	(L2) Review domain-wide delegation for applications periodically	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.2.4.1	(L1) Ensure Google session control is configured	☐	☐
4.2.5.1	(L2) Ensure Google Cloud session control is configured	☐	☐
4.3.1	(L1) Ensure the Dashboard is reviewed regularly for anomalies	☐	☐
4.3.2	(L1) Ensure the Security health is reviewed regularly for anomalies	☐	☐
5.1.1.1	(L1) Ensure the App Usage Report is reviewed regularly for anomalies	☐	☐
5.1.1.2	(L1) Ensure the Security Report is reviewed regularly for anomalies	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1	(L1) Ensure more than one Super Admin account exists	☐	☐
1.1.2	(L1) Ensure no more than 4 Super Admin accounts exist	☐	☐
1.1.3	(L1) Ensure super admin accounts are used only for super admin activities	☐	☐
3.1.1.1.1	(L1) Ensure external sharing options for primary calendars are configured	☐	☐
3.1.1.1.2	(L2) Ensure internal sharing options for primary calendars are configured	☐	☐
3.1.1.2.1	(L1) Ensure external sharing options for secondary calendars are configured	☐	☐
3.1.1.2.2	(L2) Ensure internal sharing options for secondary calendars are configured	☐	☐
3.1.1.3.1	(L2) Ensure calendar web offline is disabled	☐	☐
3.1.2.1.1.2	(L1) Ensure users cannot publish files to the web or make visible to the world as public or unlisted	☐	☐
3.1.2.1.1.3	(L2) Ensure document sharing is being controlled by domain with allowlists	☐	☐
3.1.2.1.1.5	(L1) Ensure Access Checker is configured to limit file access	☐	☐
3.1.2.1.1.6	(L1) Ensure only users inside your organization can distribute content externally	☐	☐
3.1.2.1.2.2	(L1) Ensure manager access members cannot modify shared drive settings	☐	☐
3.1.2.1.2.3	(L1) Ensure shared drive file access is restricted to members only	☐	☐
3.1.2.1.2.4	(L2) Ensure viewers and commenters ability to download, print, and copy files is disabled	☐	☐
3.1.2.2.1	(L1) Ensure offline access to documents is disabled	☐	☐
3.1.2.2.2	(L1) Ensure desktop access to Drive is disabled	☐	☐
3.1.2.2.3	(L1) Ensure Add-Ons is disabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.3.1.1	(L1) Ensure users cannot delegate access to their mailbox	☐	☐
3.1.3.1.2	(L1) Ensure offline access to Gmail is disabled	☐	☐
3.1.3.2.1	(L1) Ensure that DKIM is enabled for all mail enabled domains	☐	☐
3.1.3.2.2	(L1) Ensure the SPF record is configured for all mail enabled domains	☐	☐
3.1.3.2.3	(L1) Ensure the DMARC record is configured for all mail enabled domains	☐	☐
3.1.3.4.1.1	(L1) Ensure protection against encrypted attachments from untrusted senders is enabled	☐	☐
3.1.3.4.1.2	(L1) Ensure protection against attachments with scripts from untrusted senders is enabled	☐	☐
3.1.3.4.1.3	(L1) Ensure protection against anomalous attachment types in emails is enabled	☐	☐
3.1.3.4.2.1	(L1) Ensure link identification behind shortened URLs is enabled	☐	☐
3.1.3.4.2.3	(L1) Ensure warning prompt is shown for any click on links to untrusted domains	☐	☐
3.1.3.4.3.1	(L1) Ensure protection against domain spoofing based on similar domain names is enabled	☐	☐
3.1.3.4.3.3	(L1) Ensure protection against inbound emails spoofing your domain is enabled	☐	☐
3.1.3.4.3.4	(L1) Ensure protection against any unauthenticated emails is enabled	☐	☐
3.1.3.4.3.5	(L1) Ensure groups are protected from inbound emails spoofing your domain	☐	☐
3.1.3.5.1	(L2) Ensure POP and IMAP access is disabled for all users	☐	☐
3.1.3.5.2	(L1) Ensure automatic forwarding options are disabled	☐	☐
3.1.3.6.1	(L1) Ensure enhanced pre-delivery message scanning is enabled	☐	☐
3.1.3.7.2	(L1) Ensure 'Send email over a secure TLS connection' Is Enabled	☐	☐
3.1.4.1.1	(L1) Ensure external filesharing in Google Chat and Hangouts is disabled	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.1.4.1.2	(L2) Ensure internal filesharing in Google Chat and Hangouts is disabled	☐	☐
3.1.4.2.1	(L1) Ensure Google Chat externally is restricted to allowed domains	☐	☐
3.1.4.3.1	(L1) Ensure external spaces in Google Chat and Hangouts are restricted	☐	☐
3.1.4.4.1	(L1) Ensure allow users to install Chat apps is disabled	☐	☐
3.1.4.4.2	(L1) Ensure allow users to add and use incoming webhooks is disabled	☐	☐
3.1.6.1	(L1) Ensure accessing groups from outside this organization is set to private	☐	☐
3.1.6.2	(L1) Ensure creating groups is restricted	☐	☐
3.1.6.3	(L1) Ensure default for permission to view conversations is restricted	☐	☐
3.1.7.1	(L1) Ensure service status for Google Sites is set to off	☐	☐
3.1.8.1	(L1) Ensure access to external Google Groups is OFF for Everyone	☐	☐
3.1.9.1.1	(L1) Ensure users access to Google Workspace Marketplace apps is restricted	☐	☐
4.1.1.1	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users in administrative roles	☐	☐
4.1.1.2	(L2) Ensure hardware security keys are used for all users in administrative roles and other high-value accounts	☐	☐
4.1.1.3	(L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users	☐	☐
4.1.3.1	(L2) Ensure Advanced Protection Program is configured	☐	☐
4.1.4.1	(L2) Ensure login challenges are enforced	☐	☐
4.1.5.1	(L1) Ensure password policy is configured for enhanced security	☐	☐
4.2.1.1	(L2) Ensure application access to Google services is restricted	☐	☐
4.2.1.2	(L2) Review third-party applications periodically	☐	☐
4.2.1.3	(L1) Ensure internal apps can access Google Workspace APIs	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.2.1.4	(L2) Review domain-wide delegation for applications periodically	☐	☐
4.2.3.1	(L1) Ensure DLP policies for Google Drive are configured	☐	☐
4.2.4.1	(L1) Ensure Google session control is configured	☐	☐
4.2.5.1	(L2) Ensure Google Cloud session control is configured	☐	☐
4.3.1	(L1) Ensure the Dashboard is reviewed regularly for anomalies	☐	☐
4.3.2	(L1) Ensure the Security health is reviewed regularly for anomalies	☐	☐
5.1.1.1	(L1) Ensure the App Usage Report is reviewed regularly for anomalies	☐	☐
5.1.1.2	(L1) Ensure the Security Report is reviewed regularly for anomalies	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.2.1.1	(L1) Ensure directory data access is externally restricted	☐	☐
3.1.1.1.3	(L1) Ensure external invitation warnings for Google Calendar are configured	☐	☐
3.1.2.1.1.1	(L1) Ensure users are warned when they share a file outside their domain	☐	☐
3.1.2.1.1.4	(L2) Ensure users are warned when they share a file with users in an allowlisted domain	☐	☐
3.1.2.1.2.1	(L1) Ensure users can create new shared drives	☐	☐
3.1.3.3.1	(L1) Enable quarantine admin notifications for Gmail	☐	☐
3.1.3.4.2.2	(L1) Ensure scan linked images for malicious content is enabled	☐	☐
3.1.3.4.3.2	(L1) Ensure protection against spoofing of employee names is enabled	☐	☐
3.1.3.5.3	(L1) Ensure per-user outbound gateways is disabled	☐	☐
3.1.3.5.4	(L1) Ensure external recipient warnings are enabled	☐	☐
3.1.3.6.2	(L1) Ensure spam filters are not bypassed for internal senders	☐	☐
3.1.3.7.1	(L1) Ensure comprehensive mail storage is enabled	☐	☐
4.1.2.1	(L1) Ensure Super Admin account recovery is enabled	☐	☐
4.1.2.2	(L1) Ensure User account recovery is enabled	☐	☐
4.2.2.1	(L1) Ensure blocking access from unapproved geographic locations	☐	☐
4.2.6.1	(L1) Ensure less secure app access is disabled	☐	☐
6.1	(L1) Ensure User's password changed is configured	☐	☐
6.2	(L1) Ensure Government-backed attacks is configured	☐	☐
6.3	(L1) Ensure User suspended due to suspicious activity is configured	☐	☐
6.4	(L1) Ensure User granted Admin privilege is configured	☐	☐
6.5	(L1) Ensure Suspicious programmatic login is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.6	(L1) Ensure Suspicious login is configured	☐	☐
6.7	(L1) Ensure Leaked password is configured	☐	☐
6.8	(L1) Ensure Gmail potential employee spoofing is configured	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Nov 27, 2022	1.1.0	NEW - (L1) Ensure users are warned when they share a file outside their domain (Ticket 17089)
Nov 27, 2022	1.1.0	NEW - (L1) Ensure Access Checker is configured to limit file access (Ticket 17091)
Nov 27, 2022	1.1.0	NEW - (L1) Ensure offline access to documents is disabled (Ticket 16316)
Nov 27, 2022	1.1.0	NEW - (L1) Ensure spam filters are not bypassed for internal senders (Ticket 16241)
Nov 27, 2022	1.1.0	NEW - (L1) Ensure comprehensive mail storage is enabled (Ticket 16240)
Nov 30, 2022	1.1.0	NEW - (L2) Ensure viewers and commenters ability to download, print, and copy files is disabled (Ticket 17084)
Nov 30, 2022	1.1.0	NEW - (L1) Ensure blocking access from unapproved locations (Ticket 16012)
Dec 5, 2022	1.1.0	NEW - (L1) Ensure external recipient warnings are enabled (Ticket 16243)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure more than one Super Admin account exists (Ticket 17283)
Jan 8, 2023	1.1.0	DELETE - (L1) Ensure link sharing default settings are configured (Ticket 17085)
Jan 8, 2023	1.1.0	UPDATE - (L1) Ensure manager access members cannot modify shared drive settings (Ticket 17302)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure desktop access to Drive is disabled (Ticket 17303)
Jan 8, 2023	1.1.0	UPDATE - (L2) Ensure Google Cloud session control is configured (Ticket 15977)

Date	Version	Changes for this version
Jan 8, 2023	1.1.0	NEW - (L2) Ensure calendar web offline is disabled (Ticket 17083)
Jan 8, 2023	1.1.0	DELETE - (L1) Ensure Gmail labs is not enabled (Ticket 16165)
Jan 8, 2023	1.1.0	UPDATE - (L1) Ensure password policy is configured for enhanced security (Ticket 15975)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure enhanced pre-delivery message scanning is enabled (Ticket 16242)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure offline access to Gmail is disabled (Ticket 17129)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure no more than 4 Super Admin accounts exist (Ticket 17284)
Jan 8, 2023	1.1.0	NEW - (L2) Ensure hardware security keys are used for all users in administrative roles and other high-value accounts (Ticket 17285)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure Super Admin account recovery is enabled (Ticket 17286)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure User account recovery is enabled (Ticket 17287)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure internal apps can access Google Workspace APIs (Ticket 17288)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure the Dashboard is reviewed regularly for anomalies (Ticket 17289)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure Gmail potential employee spoofing is configured (Ticket 17300)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure Leaked password is configured (Ticket 17299)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure Suspicious login is configured (Ticket 17298)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure Suspicious programmatic login is configured (Ticket 17297)

Date	Version	Changes for this version
Jan 8, 2023	1.1.0	NEW - (L1) Ensure User granted Admin privilege is configured (Ticket 17296)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure User suspended due to suspicious activity is configured (Ticket 17295)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure Government-backed attacks is configured (Ticket 17294)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure User's password changed is configured (Ticket 17293)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure the Security Report is reviewed regularly for anomalies (Ticket 17292)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure the App Usage Report is reviewed regularly for anomalies (Ticket 17291)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure the Security health is reviewed regularly for anomalies (Ticket 17290)
Jan 8, 2023	1.1.0	NEW - (L2) Ensure users are warned when they share a file with users in an allowlisted domain (Ticket 17301)
Jan 8, 2023	1.1.0	NEW - (L1) Ensure Add-Ons is disabled (Ticket 17305)
Jan 30, 2023	1.1.0	UPDATE - (L2) Ensure document sharing is being controlled by domain with allowlists (Ticket 17090)
Jan 30, 2023	1.1.0	UPDATE - (L1) Ensure 2-Step Verification (Multi-Factor Authentication) is enforced for all users (Manual) (Ticket 17468)
Jan 30, 2023	1.1.0	UPDATE - (L1) Ensure automatic forwarding options are disabled (Manual) (Ticket 17467)
Feb 2, 2023	1.1.0	NEW - (L1) Ensure external filesharing in Google Chat and Hangouts is disabled (Ticket 17127)
Feb 2, 2023	1.1.0	NEW - (L2) Ensure internal filesharing in Google Chat and Hangouts is disabled (Ticket 17128)
May 3, 2024	1.2.0	Draft Released

Date	Version	Changes for this version
May 3, 2024	1.2.0	3.1.4.2.1 Warn Users ... cannot be found (Ticket 18293)
May 3, 2024	1.2.0	Removing superadmin rights from regularusers (Ticket 17790)
May 29, 2024	1.2.0	3.1.4.2.1 - Recommendation needs to be removed since it was only applicable to Hangouts and Hangouts is depricated (Ticket 21665)
May 29, 2024	1.2.0	Add information about using trust rules to the sub-header overview (Ticket 21666)
May 29, 2024	1.2.0	Create Recommendation for 'Send email over a secure TLS connection' (Ticket 21653)
May 29, 2024	1.2.0	Update recommendation to reflect updated setting in Google Workspace (Ticket 21793)
May 29, 2024	1.2.0	Updated Version Release