GOOGLE DRIVE AND DOCS

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.01

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

REVISION HISTORY

Version	Summary of revisions	Edited By	Date
1.0	- Entire Document – Initial Draft Change	CISA SCuBA	06/07/2023
1.01	- Added OCC provided statement to Section 1.1 Assumptions. - Incorporated comment from OCC making grammatical change to Section 1.1 Assumptions (brevity).	CISA SCuBA	12/2/2023

CONTENTS

1. CISA GOOGLE WORKSPACE SECURE CONFIGURATION BASELINE FOR GOOGLE DRIVE AND DOCS

Google Drive and Docs are collaboration tools in Google Workspace that support document management and storage, access, and sharing of files. Drive and Docs allow administrators to control and manage their files and documents. This Secure Configuration Baseline (SCB) provides specific policies to strengthen Drive and Docs security.

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

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

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

This baseline is based on Google documentation available at Google Workspace Admin Help: Overview: Manage Drive for an organization and addresses the following:

- Sharing Outside the Organization
- Shared Drive Creation
- Security Updates for Files
- Drive SDK
- Installation of Drive and Doc Add-Ons
- Drive for Desktop
- DLP Rules

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

1.1 ASSUMPTIONS

This document assumes the organization is using GWS Enterprise Plus.

This document does not address, ensure compliance with, or supersede any law, regulation, or other authority. Entities are responsible for complying with any recordkeeping, privacy, and other laws that may apply to the use of technology. This document is not intended to, and does not, create any right or benefit for anyone against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

1.2 KEY TERMINOLOGY

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

2. BASELINE POLICIES

2.1 SHARING OUTSIDE THE ORGANIZATION'S DOMAIN

This section covers whether users can share files outside of the organization, whether Google checks a shared file to ensure that recipients have access, and which users have permission to distribute content outside of the organization to include uploading or moving content to shared drives owned by another organization. These files include Google Docs, Sheets, Slides, My Maps, folders, and anything else stored in Drive.

2.2 POLICIES

2.2.1 GWS.DRIVEDOCS.1.1v0.1

Agencies SHOULD disable sharing outside of the organization's domain.

- Rationale: To have the tightest control over access to documents created within the organization, agencies should disable sharing from outside the organization. Disabling external sharing will block any collaboration from outside the organization and will prevent disseminating documents outside the organization.
- Last Modified: July 10, 2023
- Note:
  - This policy restricts information sharing
  - This policy prevents data leakage outside of the organization
  - If this policy is enforced, then follow Policy 1.2 v1.0
  - If this policy is not enforced, then follow Policies 1.3 v1.0 and 1.4 v1.0
  - Regardless, policies 1.5 through 1.8 must be followed

2.2.2 GWS.DRIVEDOCS.1.2v0.1

If disabling sharing outside of the organization's domain, then agencies SHOULD also disable users' receiving files from outside of the organization's domain.

- Rationale: If the agency decides that external sharing should be disabled, users should not be able to receive files from outside the organization as well. Disabling external sharing ensures that all communication stays within the organization, which helps mitigate risk from malicious files from an external source.
- Last Modified: July 10, 2023
- Note:
  - This policy only applies if sharing outside was disabled in Policy 1.1

2.2.3 GWS.DRIVEDOCS.1.3v0.1

When a user is going to share something outside the domain, a warning should be given. The warning alerts the user that they are intentionally sharing something externally.

- Rationale: In the case that a user is going to share something outside the domain, a warning should be given. The warning ensures that the user is aware that they are sharing something externally, and doing so purposefully.
- Last Modified: July 10, 2023
- Note:
  - This policy only applies if external sharing was allowed in Policy 1.1

2.2.4 GWS.DRIVEDOCS.1.4v0.1

If sharing outside of the organization, then agencies SHALL disable sharing of files with individuals who are not using a Google account.

- Rationale: To ensure that all shared documents are secured, and that agencies are able to control dissemination of the files, agencies shall only share files with individuals using a google account.
- Last Modified: July 10, 2023
- Note:
  - This policy only applies if external sharing is allowed in Policy 1.1

2.2.5 GWS.DRIVEDOCS.1.5v0.1

Agencies SHALL disable making files and published web content visible to anyone with the link.

- Rationale: We want to ensure that only approved individuals are able to access and view the document. If content was visible to anyone with a link, that link could be forwarded to anyone, and agencies would no longer have control over who can view the specific document. By disabling file access to anyone with a link, agencies and individuals will have tighter control over who can view files and published web content.
- Last Modified: July 10, 2023

2.2.6 GWS.DRIVEDOCS.1.6v0.1

Agencies SHALL enable access checking for file sharing outside of Docs or Drive.

- Rationale: Enabling access checking for sharing files outside of Drive/Docs helps ensure that the documents are shared with approved individuals, organizations, or external domains only.
- Last Modified: July 10, 2023

2.2.7 GWS.DRIVEDOCS.1.7v0.1

Agencies SHALL NOT allow any users to distribute content from an organization-owned shared drive to shared drives owned by another organizations.

- Rationale: To control access to content owned by the organization, users should not be able to distribute content to a shared drive owned by another organization. Once a document is moved outside the organization's drives, it no longer has control over the dissemination of the document. By not allowing users to distribute content to external shared drives, the organization maintains more control over the document.
- Last Modified: July 10, 2023

2.2.8 GWS.DRIVEDOCS.1.8v0.1

Agencies SHALL set newly created items to have Private to the Owner as the default level of access.

- Rationale: All newly created items should default to private. Any sharing of the document needs to be explicitly applied by the owner of the document.
- Last Modified: November 14, 2023

2.3 RESOURCES

- Google Workspace Admin Help: Set Drive users' sharing permissions
- CIS Google Workspace Foundations Benchmark

2.4 PREREQUISITES

- None

2.5 IMPLEMENTATION

To configure the settings for Sharing options:

2.5.1 Policy Group 1 Common instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Drive and Docs**.
3. Follow implementation for each individual policy
4. Select **Save**

2.5.2 GWS.DRIVEDOCS.1.1v0.1 instructions:

1. Select **Sharing settings** -> **Sharing options**.
2. Select **Sharing outside of your domain** -> **OFF – Files owned by users in your domain cannot be shared outside of your domain** OR

2.5.3 GWS.DRIVEDOCS.1.2v0.1 instructions:

1. Select **Sharing settings** -> **Sharing options**.
2. Deselect **Allow users to receive files from users or shared drives outside of the organization**

2.5.4 GWS.DRIVEDOCS.1.3v0.1 instructions:

1. Select **Sharing settings** -> **Sharing options**.
2. Select **Warn when files owned by users or shared drives in your organization are shared outside of your organization.**

2.5.5 GWS.DRIVEDOCS.1.4v0.1 instructions:

1. Select **Sharing settings** -> **Sharing options**.
2. Deselect **Allow users or shared drives in your organization to share items with people outside of your organization who aren't using a Google account.**

2.5.6 GWS.DRIVEDOCS.1.5v0.1 instructions:

1. Select **Sharing settings** -> **Sharing options**.
2. Deselect **When sharing outside of your organization is allowed, users in your organization can make files and published web content visible to anyone with the link.**

2.5.7 GWS.DRIVEDOCS.1.6v0.1 instructions:

1. Select **Sharing settings** -> **Sharing options**.
2. Select **Access Checker** -> **Recipients only, or suggested target audience.**

2.5.8 GWS.DRIVEDOCS.1.7v0.1 instructions:

1. Select **Sharing settings** -> **Sharing options**.
2. Select **Distributing content outside of your domain** -> **Only users in your organization.**

2.5.9 GWS.DRIVEDOCS.1.8v0.1 instructions:

1. Select **Sharing settings -> General access default.**
2. Select **When users in your organization create items, the default access will be -> Private to the owner.**

3. SHARED DRIVE CREATION

This section covers whether users can create new shared drives to share with other users, including those external to their organization. Even if users cannot create new shared drives, they can still be added to shared drives owned by other users. This control also determines which users, both internal and external to the organization, can access files in shared drives.

3.1 POLICIES

3.2 GWS.DRIVEDOCS.2.1V0.1

Agencies SHOULD enable shared drive creation to allow for effective collaboration.

- Rationale: Disabling shared drives would make collaboration difficult. Shared drives allow users in the organization to work together on one or multiple documents concurrently.
- Last Modified: July 10, 2023

3.2.1 GWS.DRIVEDOCS.2.2v0.1

Agencies SHOULD NOT allow members with manager access to override shared drive creation settings.

- Rationale: The settings outlined in the SCBs should not be able to be overwritten by anyone, even those with manager access. Not allowing anyone to change shared drive creation settings ensures that security best practices are being followed.
- Last Modified: July 10, 2023

3.2.2 GWS.DRIVEDOCS.2.3v0.1

Agencies SHOULD NOT allow users outside of their organization to access files in shared drives.

- Rationale: To control access to documents within the organization, agencies should not allow users outside the organization to access files in shared drives. Blocking external access to shared drives helps prevent documents shared within the organization from being shared outside the organization without explicit knowledge and approvals.
- Last Modified: July 10, 2023

3.2.3. GWS.DRIVEDOCS.2.4v0.1

Agencies SHALL allow users who are not shared drive members to be added to files.

- Rationale: When users who are not shared drive members are not allowed to be added to file, administrators would need to add them as drive members in order to facilitate access which would provide access to all files within the drive, not just the file intended to be shared.
  - Last Modified: July 10, 2023

3.2.4 GWS.DRIVEDOCS.2.5v0.1

Agencies SHALL NOT allow viewers and commenters to download, print, and copy files.

- Rationale: All existing access control settings are circumvented once a file is downloaded and taken out of the GWS tenant which creates the possibility for data leakage.
- Last Modified: July 10, 2023

3.3 RESOURCES

- Google Workspace Admin Help: Set Drive users' sharing permissions
- CIS Google Workspace Foundations Benchmark

3.4 PREREQUISITES

- None

3.5 IMPLEMENTATION

To configure the settings for Shared drive creation:

3.5.1 Policy Group 2 common instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Drive and Docs**.
3. Select **Sharing settings -> Shared drive creation.**
4. Follow the implementation for each individual policy.
5. Select **Save**

2.5.2 GWS.DRIVEDOCS.2.1v0.1 instructions:

1. Uncheck the **Prevent users in organization from creating new shared drives** checkbox.

2.5.3 GWS.DRIVEDOCS.2.2v0.1 instructions:

1. Uncheck the **Allow members with manager access to override the settings below** checkbox.

2.5.4 GWS.DRIVEDOCS.2.3v0.1 instructions:

1. Uncheck the **Allow users outside organization to access files in shared drives** checkbox.

2.5.5 GWS.DRIVEDOCS.2.4v0.1 instructions:

1. Check the **Allow people who aren't shared drive members to be added to files** checkbox.

2.5.6 GWS.DRIVEDOCS.2.5v0.1 instructions:

1. Check the **Allow viewers and commenters to download, print, and copy files** checkbox.

3. SECURITY UPDATES FOR FILES

This section covers whether a security update issued by Google will be applied to make file links more secure. When sharing files using a link, users must not remove the resource key parameter, as doing so may result in unexpected file access requests.

3.1 POLICIES

3.1.1 GWS.DRIVEDOCS.3.1v0.1

Agencies SHALL enable security updates for Drive files.

- Rationale: Allowing security updates to be applied to all affected files will help keep the GWS tenant secure from potential security risks.
- Last Modified: July 10, 2023

3.2 RESOURCES

- Google Workspace Admin Help: Security update for Google Drive

3.3 PREREQUISITES

- None

3.4 IMPLEMENTATION

To configure the settings for Security update for files:

3.4.1 GWS.DRIVEDOCS.3.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Drive and Docs.**
3. Select **Sharing settings -> Security update for files.**
4. Select **Apply security update to all impacted files.**
5. Uncheck the **Allow users to remove/apply the security update for files they own or manage** checkbox.
6. Select **Save.**

4. DRIVE SDK

This section covers whether users have access to Google Drive with the Drive SDK API, which allows third party applications to work on the files that are stored in Google Drive. The Drive SDK API is used by developers to access Google Drive through third party applications that they have created.

4.1 POLICIES

4.1.1 GWS.DRIVEDOCS.4.1v0.1

Agencies SHOULD disable Drive SDK access to restrict information sharing and prevent data leakage.

- Rationale: The Drive SDK allows third-party external applications to access data and files from within Drive. Disabling the Drive SDK prevents third party applications from accessing the files and data from within the organization, which protects against data leakage and unintentional information sharing.
- Last Modified: July 10, 2023

4.2 RESOURCES

- Google Drive for Developers
- CIS Google Workspace Foundations Benchmark

4.3 PREREQUISITES

- None

4.4 IMPLEMENTATION

To configure the settings for Drive SDK:

4.4.1 GWS.DRIVEDOCS.4.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Drive and Docs.**
3. Select **Features and Applications -> Drive SDK.**
4. Uncheck the **Allow users to access Google Drive with the Drive SDK API** checkbox.
5. Select **Save.**

5. USER INSTALLATION OF GOOGLE DOCS ADD-ONS FROM THE ADD-ONS STORE

This section covers whether users can use add-ons in file editors within Google Drive, such as Docs, Sheets, Slides, and Forms. These add-ons include those available through Google Workspace Marketplace that have been built by other developers.

5.1 POLICIES

5.1.1 GWS.DRIVEDOCS.5.1v0.1

Agencies SHALL disable Add-Ons with the exception of those that are approved within the organization.

- Rationale: Google Docs Add-Ons can pose a great security risk based on the permissions the add-on is given. Add-ons can be given full access to the google drive, permission to add or edit existing documents, share documents, connect to external services, and more. Any add-on needs to be fully vetted before given access to the google workspace. Therefore, unapproved add-ons need to be disabled.

- Last Modified: July 10, 2023

5.2 RESOURCES

- Google Workspace Admin Help: Allow or restrict add-ons in Docs editors

- CIS Google Workspace Foundations Benchmark

5.3 PREREQUISITES

- None

5.4 IMPLEMENTATION

To configure the settings for add-ons:

5.4.1 GWS.DRIVEDOCS.5.1v0.1 instructions:

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

3. Select **Features and Applications -> Add-Ons.**
4. Uncheck the **Allow users to install Google Docs add-ons from add-ons stor**e checkbox.
5. Select **Save.**

6. DRIVE FOR DESKTOP

This section covers that Google Drive for Desktop, if not disabled entirely, should only be allowed on authorized devices.

6.1 POLICIES

6.1.1 GWS.DRIVEDOCS.6.1v0.1

Agencies SHOULD either disable Google Drive for Desktop or only allow Google Drive for Desktop on authorized devices.

- Rationale: Saving directly to the cloud reduces the risk of potentially losing data, which is beneficial when dealing with sensitive information and when trying to retain certain files.
- Last Modified: July 10, 2023

6.2 RESOURCES

- Use Google Drive for desktop - Google Drive Help
- CIS Google Workspace Foundations Benchmark

6.3 PREREQUISITES

- None

6.4 IMPLEMENTATION

6.4.1 GWS.DRIVEDOCS.6.1v0.1 instructions:

To Disable Google Drive for Desktop:

1. Sign in to the Google Admin Console.
2. Select **Menu->Apps->Google Workspace->Drive and Docs->Google Drive for Desktop.**
3. Uncheck the **Allow Google Drive for desktop in your organization box** checkbox or
4. Ensure **Allow Google Drive for desktop in your organization box** and **Only allow Google Drive for desktop on authorized devices** is checked.
5. Select **Save.**

To limit Google Drive for Desktop to authorized devices:

1. Sign in to the Google Admin Console.
2. Select Menu->Apps->Google Workspace->Drive and Docs->Features and Applications.
3. Uncheck the Allow Google Drive for desktop in your organization checkbox.
4. Check the Only allow Google Drive for desktop on authorized devices checkbox.
5. Ensure authorized devices are added to company-owned inventory.
6. Select Save.

Alternatively, Context-Aware access policies can be configured for more granular controls around authorized devices. The access level applied to Google Drive must have the "Apply to Google desktop and mobile apps" enabled to meet this requirement. For additional guidance, see the *Common Controls Minimum Viable Secure Baseline*, section "Context-Aware Access for All Devices that Connect to GWS SHOULD be Implemented."

7. DLP RULES

This recommendation applies only to agencies that allow external sharing (see Sharing Outside the Organization).

Using data loss prevention (DLP), you can create and apply rules to control the content that users can share in files outside the organization. DLP gives you control over what users can share and prevents unintended exposure of sensitive information.

DLP rules can use predefined content detectors to match PII (e.g., SSN), credentials (e.g., API keys), or specific document types (e.g., source code). Custom rules can also be applied based upon regex match or document labels.

7.1 POLICIES

7.1.1 GWS.DRIVEDOCS.7.1v0.1

Agencies SHOULD configure DLP rules to block or warn on sharing files with sensitive data.

- Rationale: Data Loss Prevention (DLP) rules trigger scans of files to look for sensitive content and restrict sharing of documents that may contain sensitive content. Configuring DLP rules helps agencies protect their information, by determining what data and/or phrasing might be sensitive, and restricting the dissemination of the documents containing that data. Examples include PII, PHI, portion markings, etc.
- Last Modified: July 10, 2023

7.2 RESOURCES

- How to use predefined content detectors - Google Workspace Admin Help
- Get started as a Drive labels admin - Google Workspace Admin Help
- CIS Google Workspace Foundations Benchmark

7.3 PREREQUISITES

- None

7.4 IMPLEMENTATION

7.4.1 GWS.DRIVEDOCS.7.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Menu -> Security -> Access and data control -> Data protection.**
3. Click **Manage Rules.** Then click **Add rule** -> **New rule** or click **Add rule** -> **New rule from template.** For templates, select a template from the Templates page.
4. In the **Name** section, add the name and description of the rule.

5. In the **Scope** section, apply this rule only to the entire domain or to selected organizational units or groups, and click **Continue**. If there's a conflict between organizational units and groups in terms of inclusion or exclusion, the group takes precedence.
6. In the **Apps** section, choose the trigger for **Google Drive, File created, modified, uploaded or shared**, and click **Continue**.
7. In the **Conditions** section, click **Add Condition**.
8. Configure appropriate content definition(s) based upon the agency's individual requirements and click **Continue**.
9. Select the appropriate action to warn or block sharing, based upon the agency's individual requirements.
10. In the **Alerting** section, choose a severity level, and optionally, check **Send to alert center to trigger notifications**.
11. Review the rule details, mark the rule as **Active**, and click **Create.**