TLP:CLEAR

GOOGLE CHAT

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.01

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

TLP:CLEAR

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). • Incorporated comment from OCC making grammatical change to Rationale in Section 2.1.1 (clarity)	CISA SCuBA	12/2/2023

CONTENTS

1. CISA GOOGLE WORKSPACE SECURITY CONFIGURATION BASELINE FOR GOOGLE CHAT

Google Chat is a communication and collaboration tool in Google Workspace that supports direct messaging, group conversations, and content creation and sharing. Chat allows administrators to control and manage their messages and files. This Secure Configuration Baseline (SCB) provides specific policies to strengthen Chat 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: Google Chat settings and addresses the following:

- Chat History
- External File Sharing
- History for Spaces
- External Chat Messaging
- Installation of Chat Add-Ons
- 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 CHAT HISTORY

This section covers chat history retention for users within the organization and prevents users from changing their history setting. This control applies to both direct messages and group messages.

2.2 POLICIES

2.1.1 GWS.CHAT.1.1v0.1

Chat history SHOULD be enabled for information traceability.

- Rationale: Helps ensure there is a record of chats sent to receive in the case that it needs to be reviewed in the future for legal or compliance issues.
- Last Modified: July 10, 2023

2.1.2 GWS.CHAT.1.2v0.1

Users SHALL NOT be allowed to change their history setting.

- Rationale: This setting helps prevent changes by the user.
- Last Modified: July 10, 2023

2.2 RESOURCES

- Google Workspace Admin Help: Turn chat history on or off for users

2.3 PREREQUISITES

- None

2.4 IMPLEMENTATION

To configure the settings for History for chats:

2.4.1 GWS.CHAT.1.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Chat**.
3. Select **History for chats**.
4. Select **History is ON**.
5. Select **Save**

2.4.2 GWS.CHAT.1.2v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Chat**.
3. Uncheck the **Allow users to change their history setting** checkbox.
4. Select **Save**.

3. EXTERNAL FILE SHARING

This section covers what types of files users are allowed to share external to their organization.

3.1 POLICIES

3.1.1 GWS.CHAT.2.1v0.1

External file sharing SHALL be disabled to protect sensitive information from unauthorized or accidental sharing.

- Rationale: Protects against unintentional or intentional data leakage from the agency or organization.
- Last Modified: July 10, 2023

3.2 RESOURCES

- Google Workspace Admin Help: Control file sharing in Chat

3.3 PREREQUISITES

- None

3.4 IMPLEMENTATION

To configure the settings for External filesharing:

3.4.1 GWS.CHAT.2.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Chat**.
3. Select **Chat File Sharing**.
4. In the **External filesharing** dropdown menu, select **No files.**
5. Select **Save**.

4. HISTORY FOR SPACES

This section covers whether chat history is retained by default for users within the organization. This control does not apply for threaded chat spaces because those require that history be on, which cannot be changed. Chat spaces allow for multiple users to share files, assign tasks, and stay connected.

4.1 POLICIES

4.1.1 GWS.CHAT.3.1v0.1

Space history SHOULD be enabled for traceability of information.

- Rationale: This provides the ability to trace history when needed from an organizational level.
- Last Modified: July 10, 2023

4.2 RESOURCES

- Google Workspace Admin Help: Set a space history option for users

4.3 PREREQUISITES

- None

4.4 IMPLEMENTATION

To configure the settings for History for spaces:

4.4.1 GWS.CHAT.3.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Chat**.
3. Select **History for spaces**.
4. Select **History is ON by default** or **History is ALWAYS ON**.
5. Select **Save**.

5. EXTERNAL CHAT MESSAGING

This section covers that while users can send Chat messages outside of their organization, Chat must be restricted to allowlisted domains only.

5.1 POLICIES

5.1.1 GWS.CHAT.4.1v0.1

External Chat messaging SHALL be restricted to allowlisted domains only to limit data leakage.

- Rationale: Protects the organization from external risks and helps prevent data leakage outside the organization.
- Last Modified: November 14, 2023

5.1.2 GWS.CHAT.4.2v0.1

Only allow this for allowlisted domains SHALL be enabled.

- Rationale: This limits the security vulnerabilities present with allowing chatting outside of organization.
- Last Modified: August 1, 2023

5.2 RESOURCES

- Google Workspace Admin Help: Set external chat options
- Google Workspace Admin Help: Allow external sharing with only trusted domains
- CIS Google Workspace Benchmark v1.1.0 - 3.1.4.2.2 Ensure Google Chat Externally is Restricted to Allowlisted Domains

5.3 PREREQUISITES

- None

5.4 IMPLEMENTATION

To configure the settings for External Chat:

5.4.1 Policy Group 4 Common Instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Chat**.
3. Select **External Chat Settings** -> **Chat externally**

5.4.2 GWS.CHAT.4.1v0.1 instructions:

1. Select **ON**
2. Select **Save**

5.4.3 GWS.CHAT.4.2v0.1 instructions:

1. Select **Only allow this for allowlisted domains**
2. To add allowlisted domains select **Manage allowlisted domains**
3. Select **Save**

6. ALLOW USERS TO INSTALL CHAT APPS

This section permits users to send Chat messages outside of their organization, but such Chat messages must be restricted to allowlisted domains only.

6.1 POLICIES

6.1.1 GWS.CHAT.5.1v0.1

User-level ability to install Chat apps SHALL be disabled.

- Rationale: Protects against security risks associated with installing chat apps such as phishing, spyware, etc.
- Last Modified: July 10, 2023

6.2 RESOURCES

- Google Workspace Admin Help: Allow users to install Chat apps
- GWS Common Controls Minimum Viable Secure Configuration Baseline

6.3 PREREQUISITES

- None

6.4 IMPLEMENTATION

To configure the settings for Chat apps:

6.4.1 GWS.CHAT.5.1v0.1 instructions:

1. Sign in to the Google Admin Console
2. Select **Apps** -> **Google Workspace** -> **Google Chat**
3. Select **Chat apps** -> **Chat apps access settings**
4. Select **OFF** for **Allow users to install Chat apps**
5. Select **SAVE**

7. DLP RULES

This recommendation applies only to agencies that allow external sharing (see section 2.1).

Using data loss prevention (DLP), organizations 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.CHAT.6.1v0.1

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.CHAT.6.1v0.1 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 Chat, Message Sent or File Upload**, 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**