GOOGLE MEET

Secure Cloud Business Applications Minimum Viable Secure Configuration Baselines

Version: 1.01

Publication: 12/2023

Cybersecurity and Infrastructure Security Agency

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp

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 SECURITY CONFIGURATION BASELINE FOR GOOGLE MEET

Google Meet is a video conferencing service in Google Workspace that supports real-time video, desktop, and presentation sharing. Meet allows administrators to control and manage their video meetings. This Secure Configuration Baseline (SCB) provides specific policies to strengthen Meet 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 Meet settings reference for admins and addresses the following:

- Meeting Access
- Internal Access to External Meetings
- Host Management Features
- External Participants

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 MEETING ACCESS

This control limits safe meeting access to users with a Google Account or Dialing in using a phone.

2.2 POLICIES

2.2.1 GWS.MEET.1.1v0.1

Meeting access SHALL be restricted to users signed in with a Google Account or Dialing in using a phone.

- Rationale: This protects against unauthorized access to a Google meeting and helps ensures the user has been authenticated prior to joining.
- Last Modified: June 29, 2023

2.3 RESOURCES

- Google Meet security & privacy for admins
- Google Meet settings reference for admins

2.4 PREREQUISITES

- None

2.5 IMPLEMENTATION

To configure the settings for Domain Meet safety settings:

2.5.1 GWS.MEET.1.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Meet**.
3. Select **Meet safety settings** -> **Domain**.
4. Select **Only users from your organization or users dialing in using a phone** or **Users signed in with a Google account or dialing in using a phone**.
5. Select **Save**.

3. INTERNAL USER ACCESS TO EXTERNALLY CREATED MEETINGS

This control determines which meetings users within the agency's organization can join.

3.1 POLICIES

3.1.1 GWS.MEET.2.1v0.1

Meeting access SHALL be disabled for meetings created by users who are not members of any Google Workspace tenant or organization.

- Rationale: This helps ensure that organization members are not able to join meetings created externally to avoid potential data leakage or other security risks.
- Last Modified: September 26, 2023

3.2 RESOURCES

- Google Meet security & privacy for admins
- Google Meet settings reference for admins

3.3 PREREQUISITES

- None

3.4 IMPLEMENTATION

To configure the settings for Access within Meet safety settings:

3.4.1 GWS.MEET.2.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Meet**.
3. Select **Meet safety settings** -> **Access**.
4. Select **Meetings created in your organization only** or **Meetings created in any Workspace organization**.
5. Select **Save**.

4. HOST MANAGEMENT MEETING FEATURES

This control enables the following features for a host to implement during their meeting: prevent participants from sharing their screen, turn chat messages on or off, end the meeting for all, and mute all. By default, this control is disabled.

Note: When this feature is not enabled, any attendee that is a member of the host’s organization can record the meeting.

4.1 POLICIES

4.1.1 GWS.MEET.3.1v0.1

Host Management meeting features SHALL be enabled so that they are available by default when a host starts their meeting.

- Rationale: Enabling these features does not pose any security risk and provides better collaboration features to users. If this setting was disabled then any participant could take control of the meeting.
- Last Modified: July 3, 2023

4.2 RESOURCES

- Google Meet security & privacy for admins
- Google Meet settings reference for admins
- Record a Video Meeting

4.3 PREREQUISITES

- None

4.4 IMPLEMENTATION

To enable Host Management meeting features:

4.4.1 GWS.MEET.3.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Meet**.
3. Select **Meet safety settings** -> **Host management**.
4. Check the **Start video calls with host management turned on** checkbox.
5. Select **Save**.

5. EXTERNAL PARTICIPANT WARNING

This control provides a warning label for any participating a meeting who is not a member of the organization or whose identity is unconfirmed.

5.1 POLICIES

5.1.1 GWS.MEET.4.1v0.1

Warn for external participants SHALL be enabled.

- Rationale: When enabled, external or unidentified participants in a meeting are given a label. This increases situational awareness amongst meeting participants and can help prevent inadvertent data leakage.
- Last Modified: September 26, 2023

5.2 RESOURCES

- Manage Meet settings (for admins)

5.3 PREREQUISITES

- None

5.4 IMPLEMENTATION

To enable Host Management meeting features:

5.4.1 GWS.MEET.4.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Google Meet.**
3. Select **Meet safety settings** -> **Warn for external participants.**
4. Check the **External or unidentified participants in a meeting are given a label** checkbox.
5. Select **Save.**