GOOGLE CALENDAR

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	• Updated Table of Contents • 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 Section 5 Calendar Interop Management (clarity). • Incorporated comment from OCC making grammatical change to Rationale in Section 6.1.1 (clarity).	CISA SCuBA	12/2/2023

CONTENTS

1. CISA GOOGLE WORKSPACE SECURITY CONFIGURATION BASELINE FOR GOOGLE CALENDAR

Google Calendar is a calendar service in Google Workspace used for creating and editing events that enables collaboration amongst users. Calendar allows administrators to control and manage their sharing settings for both internal and external use. This Secure Configuration Baseline (SCB) provides specific policies to strengthen Calendar 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: Set Calendar sharing options and addresses the following:

- External Sharing for Primary Calendars
- External Invitations Warnings
- External Sharing for Secondary Calendars
- Calendar Interop
- Paid Appointments

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 EXTERNAL SHARING OPTIONS FOR PRIMARY CALENDARS

This section determines what information is shared from primary calendars with external entities.

2.2 POLICIES

2.2.1 GWS.CALENDAR.1.1v0.1

External Sharing Options for Primary Calendars SHALL be configured to "Only free/busy information (hide event details)" to restrict information sharing and prevent data leakage.

- 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.
- Last Modified: July 10, 2023

2.2.2 GWS.CALENDAR.1.2v0.1

External sharing options for primary calendars between multiple components within an organization MAY be configured to "Only free/busy information (hide event details)."

- Rationale: Prevent data leakage by restricting the information viewable by internal users when a user shares their calendar by configuring additional settings on shared information between components.
- Last Modified: November 14, 2023

2.3 RESOURCES

- Google Workspace Admin Help: Set Calendar sharing options
- CIS Google Workspace Foundations Benchmark

2.4 PREREQUISITES

- None

2.5 IMPLEMENTATION

To configure the settings for External Sharing in Primary Calendar:

2.5.1 GWS.CALENDAR.1.1v0.1 Instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Calendar**.
3. Select **Sharing settings** -> **External sharing options for primary calendars**.
4. Select **Only free/busy information (hide event details)**.
5. Select **Save**.

2.5.2 GWS.CALENDAR.1.2v0.1 instructions:

1. There is no implementation for this policy.

3. EXTERNAL INVITATIONS WARNINGS

This section determines whether users are warned when inviting one or more guests from outside of their domain.

3.1 POLICIES

3.1.1 GWS.CALENDAR.2.1v0.1

External invitations warnings SHALL be enabled to prompt users before sending invitations.

- 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.
- Last Modified: July 10, 2023

3.2 RESOURCES

- Google Workspace Admin Help: Allow external invitations in Google Calendar events
- CIS Google Workspace Foundations Benchmark

3.3 PREREQUISITES

- None

3.4 IMPLEMENTATION

3.4.1 GWS.CALENDAR.2.1v0.1 instructions:

To configure the settings for Confidential Mode:

1. Sign in to the Google Admin Console.
2. Select **Apps** -> **Google Workspace** -> **Calendar**.
3. Select **Sharing settings** -> **External Invitations**.
4. Check the **Warn users when inviting guests outside of the domain** checkbox.
5. Select **Save**.

4. EXTERNAL SHARING OPTIONS FOR SECONDARY CALENDARS

This section determines what information is shared from secondary calendars with external entities.

4.1 POLICIES

4.1.1 GWS.CALENDAR.3.1v0.1

External sharing options for secondary calendars SHALL be configured to "Only free/busy information (hide event details)" to restrict information sharing and prevent data leakage.

- 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.
- Last Modified: July 10, 2023

4.1.2 GWS.CALENDAR.3.2v0.1

External sharing options for secondary calendars between multiple components within an organization MAY be configured.

- Rationale: Prevent data leakage by restricting the information viewable by internal users when a user shares their calendar by configuring additional settings on shared information between components.
- Last Modified: July 10, 2023

4.2 RESOURCES

- Google Workspace Admin Help: Set Calendar sharing options
- CIS Google Workspace Foundations Benchmark

4.3 PREREQUISITES

- N/A

4.4 IMPLEMENTATION

4.4.1 GWS.CALENDAR.3.1v0.1 instructions:

To configure the settings for External Sharing in secondary calendars:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Calendar**.
3. Select **General settings -> External sharing options for secondary calendars**.
4. Select **Only free/busy information (hide event details)**.
5. Select **Save**.

4.4.2 GWS.CALENDAR.3.2v0.1 instructions:

1. There is no implementation for this policy

5. CALENDAR INTEROP MANAGEMENT

This section determines whether Microsoft Exchange and Google Calendar can be configured to work together to allow users in both systems to share their availability status so they can view each other's schedules. The availability and event information that will be shared between Exchange and Calendar include availability for users, group or team calendars, and calendar resources (such as meeting rooms). Calendar Interop respects event-level privacy settings from either Exchange or Calendar.

Due to the added complexity and attack surface associated with configuring Calendar Interop, it should be disabled in environments for which this capability is not necessary for agency mission fulfillment.

5.1 POLICIES

5.1.1 GWS.CALENDAR.4.1v0.1

Calendar Interop SHOULD be disabled unless agency mission fulfillment requires collaboration between users internal and external to an organization who use both Microsoft Exchange and Google Calendar.

- Rationale: Prevent information exchange between Microsoft and Google calendars for users using both services unless it is required by the organization.
- Last Modified: July 10, 2023

5.1.2 GWS.CALENDAR.4.2v0.1

OAuth 2.0 SHALL be used in lieu of basic authentication to establish connectivity between tenants or organizations in cases where Calendar Interop is deemed necessary for agency mission fulfillment.

- Rationale: When required by organizational requirements, for user's to exchange information between Google and Microsoft calendars, users will be authenticated using OAuth 2.0 to prevent unauthorized access.
- Last Modified: July 10, 2023

5.2 RESOURCES

- Google Workspace Admin Help: About Calendar Interop

5.3 PREREQUISITES

- None

5.4 IMPLEMENTATION

5.4.1 GWS.CALENDAR.4.1v0.1 instructions:

To configure the settings for Calendar Interop:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Calendar**.
3. Select **Calendar Interop management**.
4. Check the **Disable Interoperability for Calendar** checkbox.
5. Select **Save**.

5.4.2 GWS.CALENDAR.4.2v0.1 instructions:

To configure the settings for Calendar Interop:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Calendar**.
3. Select **Calendar Interop management**.
4. Select **OAuth 2.0 client credentials**
5. Select **Save**.

6. PAID APPOINTMENTS

This section covers whether or not the paid appointment booking feature is enabled.

6.1 POLICIES

6.1.1 GWS.CALENDAR.5.1v0.1

Appointment Schedule with Payments SHALL be disabled.

- Rationale
    - This helps avoid unnecessary interconnectivity with third-party services that can create a greater chance of additional vulnerabilities in the platform.
    - There is no obvious need for agencies to have this feature enabled.

- Last Modified: July 10, 2023

6.2 RESOURCES

- [Google Workspace Help: Allow paid appointment schedules in Calendar](#)

6.3 PREREQUISITES

- None

6.4 IMPLEMENTATION

6.4.1 GWS.CALENDAR.5.1v0.1 instructions:

1. Sign in to the Google Admin Console.
2. Select **Apps -> Google Workspace -> Calendar**.
3. Select **Advanced Settings -> Appointment schedules with payments**
4. Select **OFF- Blocks users' from adding required payments to their Calendar appointment schedules**
5. Select **Save**