GOOGLE SITES

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 Title • Added Sub-Title • Corrected TLP Designation on P.1 • Updated ToC • Added OCC provided statement to Section 1.1 Assumptions. • Incorporated comment from OCC making grammatical change to Section 1.1 Assumptions (brevity). • Revised Rationale for Section 2.2.1 GWS.SITES.1.1v0.1	CISA SCuBA	12/2/2023

CONTENTS

1. CISA GOOGLE WORKSPACE SECURITY CONFIGURATION BASELINE FOR GOOGLE SITES

Google Sites is a collaborative tool in Google Workspace that supports the creation of websites (i.e., internal project hubs, team sites, and public-facing websites) without the need of a designer, programmer, or IT help. Sites allow administrators to control and manage their files and documents. Google Drive manages sharing and publishing settings for new Sites. This Secure Configuration Baseline (SCB) provides specific policies to strengthen Sites 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: Sites](#) and addresses the following:

- [Sites Service Status](#)

Google is currently transitioning from classic Sites to new Sites, [Google Workspace Admin Help: Transition from classic Sites to new Sites](#). Starting December 1, 2022, classic Sites will no longer be editable. And starting January 1, 2023, classic Sites will no longer be viewable unless converted to new Google Sites. All remaining classic Sites will be automatically archived as HTML files, saved to the site owner's Google Drive, and replaced with a draft in new Sites to be reviewed and published.

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.

1.2 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.

1.3 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 GOOGLE SITES SERVICE STATUS

This section covers whether users are able to access Google Sites.

2.2 POLICY

2.2.1 GWS.SITES.1.1v0.1

Sites Service SHOULD be disabled for all users.

- Rationale: This helps to minimize attack surface. Not every user within an organization needs access to Google Sites. If this capability is needed, it can be enabled and configured for those users based on user's assigned organizational unit (OU) and by exception as required by the organization to meet specific needs.
- Last Modified: July 10, 2023

2.3 RESOURCES

- Google Workspace Admin Help: Manage users' access in Sites

- CIS Google Workspace Foundations Benchmark

2.4 PREREQUISITES

- None

2.5 IMPLEMENTATION

To configure the settings for Site creation and editing:

2.5.1 GWS.SITES.1.1v0.1 instructions:

1. Sign in to the Google Admin Console.

2. Select **Apps** -> **Google Workspace** -> **Sites**.

3. Select **Service Status**

4. Select **OFF for everyone**.

5. Select **Save**.