



GROUPS FOR BUSINESS

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	<ul style="list-style-type: none">Entire Document - Initial Draft Change	CISA SCuBA	06/07/2023
1.01	<ul style="list-style-type: none">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 Groups for Business 6
 - 1.1 Assumptions 6
 - 1.2 Key Terminology 7
- 2. Baseline Policies 7
 - 2.1 Group Access from Outside the Organization 7
 - 2.2 Baseline Policies 7
 - 2.2.1 GWS.GROUPS.1.1v0.1 7
 - 2.3 Resources 7
 - 2.4 Prerequisites 7
 - 2.5 Implementation 7
 - 2.5.1 GWS.GROUPS.1.1v0.1 instructions: 7
- 3. Group Owners' Ability to Add External Members to Groups 8
 - 3.1 Policies 8
 - 3.1.1 GWS.GROUPS.2.1v0.1 8
 - 3.2 Resources 8
 - 3.3 Prerequisites 8
 - 3.4 Implementation 8
 - 3.4.1 GWS.GROUPS.2.1v0.1 instructions: 8
- 4. Group Owners' Ability to Allow Posting to a Group by an External, Non-Group Member 8
 - 4.1 Policies 9
 - 4.1.1 GWS.GROUPS.3.1v0.1 9
 - 4.2 Resources 9
 - 4.3 Prerequisites 9
 - 4.4 Implementation 9
 - 4.4.1 GWS.GROUPS.3.1v0.1 instructions: 9
- 5. Group Creation 9
 - 5.1 Policies 9

5.1.1 GWS.GROUPS.4.1v0.1 9

5.2 Resources 9

5.3 Prerequisites..... 10

5.4 Implementation 10

 5.4.1 GWS.GROUPS.4.1v0.1 instructions: 10

6. The Default Permission to View Conversations 10

 6.1 Policies..... 10

 6.1.1 GWS.GROUPS.5.1v0.1..... 10

 6.2 Resources 10

 6.3 Prerequisites..... 10

 6.4 Implementation 10

 6.4.1 GWS.GROUPS.5.1v0.1 instructions: 10

7. Group Owners’ Ability to Hide Groups from the Directory 11

 7.1 Policies..... 11

 7.1.1 GWS.GROUPS.6.1v0.1..... 11

 7.2 Resources 11

 7.3 Prerequisites..... 11

 7.4 Implementation 11

 7.4.1 GWS.GROUPS.6.1v0.1 instructions: 11

8. The Ability for Newly Created Groups to be Hidden from the Directory 12

 8.1 Policies..... 12

 8.1.1 GWS.GROUPS.7.1v0.1..... 12

 8.2 Resources 12

 8.3 Prerequisites..... 12

 8.4 Implementation 12

 8.4.1 GWS.GROUPS.7.1v0.1 instructions: 12

9. New Groups 12

 9.1 Policies..... 12

 9.1.1 GWS.GROUPS.8.1v0.1..... 12

9.2 Resources 13

9.3 Prerequisites..... 13

9.4 Implementation 13

 9.4.1 GWS.GROUPS.8.1v0.1 instructions: 13

1. CISA GOOGLE WORKSPACE SECURITY CONFIGURATION BASELINE FOR GROUPS FOR BUSINESS

Groups for Business is a Google Workspace collaboration tool that supports storage, access, and sharing of files, document management, and email. Groups for Business allows administrators to control and manage collaboration efforts among groups within their organizations. This Secure Configuration Baseline (SCB) provides specific policies to strengthen Groups 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 being 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 baseline is based on Google documentation available at [Google Workspace Admin Help: Set up and manage Groups for Business](#) and addresses the following:

- [External Group Access](#)
- [Owner's Adding External Members](#)
- [Owner's Allowing Posting by External Members](#)
- [Group Creation](#)
- [Default Permissions for Viewing Conversations](#)
- [Owners Ability to Hide Groups from the Directory](#)
- [Ability for New Groups to be Hidden from the Directory](#)
- [New Groups](#)

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 GROUP ACCESS FROM OUTSIDE THE ORGANIZATION

This control determines whether users outside of an agency's organization can view, search for, or post to groups internal to an agency.

Note: Even with this setting configured, group owners can still explicitly add external POCs to a group ([Owner's Adding External Members](#)), or explicitly allow posting to a group by an external POC who has not been added to said group ([Owner's Allowing Posting by External Members](#)).

2.2 BASELINE POLICIES

2.2.1 GWS.GROUPS.1.1v0.1

Group access from outside the organization SHALL be disabled unless explicitly granted by the group owner.

- Rationale: Who can externally view groups internal to the organization should be carefully controlled and their access vetted as needed.
- Last Modified: July 10, 2023

2.3 RESOURCES

- [Google Workspace Admin Help: Set organization-wide policies for using groups](#)
- [CIS Google Workspace Foundations Benchmark](#)

2.4 PREREQUISITES

- None

2.5 IMPLEMENTATION

2.5.1 GWS.GROUPS.1.1v0.1 instructions:

To configure the settings for Sharing options:

1. Sign in to the [Google Admin Console](#).
2. Select **Apps** -> **Google Workspace** -> **Groups for Business**.
3. Select **Sharing settings** -> **Sharing options**.
4. Select **Accessing groups from outside this organization** -> **Private**.

5. Select **Save**.

3. GROUP OWNERS' ABILITY TO ADD EXTERNAL MEMBERS TO GROUPS

This section covers whether or not the owner of the group has the ability to add external members to the group.

3.1 POLICIES

3.1.1 GWS.GROUPS.2.1v0.1

Group owners' ability to add external members to groups SHOULD be disabled unless necessary for agency mission fulfillment.

- Rationale: The ability to add external members should be left to the organization/agency to protect the agency from potential data leakage.
- Last Modified: July 10, 2023

3.2 RESOURCES

- [Google Workspace Admin Help: Set organization-wide policies for using groups](#)

3.3 PREREQUISITES

- None

3.4 IMPLEMENTATION

3.4.1 GWS.GROUPS.2.1v0.1 instructions:

To configure the settings for Sharing options:

1. Sign in to the [Google Admin Console](#).
2. Select **Apps** -> **Google Workspace** -> **Groups for Business**.
3. Select **Sharing settings** -> **Sharing options**.
4. **Uncheck** the **Group owners can allow external members** checkbox.
5. Select **Save**.

4. GROUP OWNERS' ABILITY TO ALLOW POSTING TO A GROUP BY AN EXTERNAL, NON-GROUP MEMBER

This section covers whether or not an owner of a group has the ability to allow an external non-member to post to the group.

4.1 POLICIES

4.1.1 GWS.GROUPS.3.1v0.1

Group owners' ability to allow posting to a group by an external, non-group member SHOULD be disabled unless necessary for agency mission fulfillment.

- Rationale: External member posting would create unnecessary security risks.
- Last Modified: July 10, 2023

4.2 RESOURCES

- [Google Workspace Admin Help: Set organization-wide policies for using groups](#)

4.3 PREREQUISITES

- None

4.4 IMPLEMENTATION

4.4.1 GWS.GROUPS.3.1v0.1 instructions:

To configure the settings for Sharing options:

1. Sign in to the [Google Admin Console](#).
2. Select **Apps** -> **Google Workspace** -> **Groups for Business**.
3. Select **Sharing settings** -> **Sharing options**.
4. **Uncheck** the **Group owners can allow incoming mail from outside the organization** checkbox.
5. Select **Save**.

5. GROUP CREATION

This section covers who has the ability to create a new group within the organization.

5.1 POLICIES

5.1.1 GWS.GROUPS.4.1v0.1

Group creation SHOULD be restricted to admins within the organization unless necessary for agency mission fulfillment.

- Rationale: The organization should have some control over the organizational groups created and the purpose they are for.
- Last Modified: July 10, 2023

5.2 RESOURCES

- [Google Workspace Admin Help: Set organization-wide policies for using groups](#)

- [CIS Google Workspace Foundations Benchmark](#)

5.3 PREREQUISITES

- None

5.4 IMPLEMENTATION

5.4.1 GWS.GROUPS.4.1v0.1 instructions:

To configure the settings for Sharing options:

1. Sign in to the [Google Admin Console](#).
2. Select **Apps** -> **Google Workspace** -> **Groups for Business**.
3. Select **Sharing settings** -> **Sharing options**.
4. Select **Creating groups** -> **Only organization admins can create groups**.
5. Select **Save**.

6. THE DEFAULT PERMISSION TO VIEW CONVERSATIONS

This section covers the default permissions assigned to the viewing of conversations within a group.

6.1 POLICIES

6.1.1 GWS.GROUPS.5.1v0.1

The default permission to view conversations SHOULD be set to All Group Members.

- Rationale: Conversation viewing by default should be restricted as a security best practice but can be expanded by exception for certain groups on a need-to-know basis.
- Last Modified: July 10, 2023
- Note: This setting can be changed by group owners and group managers.

6.2 RESOURCES

- [Google Workspace Admin Help: Set organization-wide policies for using groups](#)
- [CIS Google Workspace Foundations Benchmark](#)

6.3 PREREQUISITES

- None

6.4 IMPLEMENTATION

6.4.1 GWS.GROUPS.5.1v0.1 instructions:

To configure the settings for Sharing options:

1. Sign in to the [Google Admin Console](#).
2. Select **Apps** -> **Google Workspace** -> **Groups for Business**.
3. Select **Sharing settings** -> **Sharing options**.
4. Select **Default for permission to view conversations** -> **All group members**.
5. Select **Save**.

7. GROUP OWNERS' ABILITY TO HIDE GROUPS FROM THE DIRECTORY

This section covers whether or not the owner of a group can hide the group from the directory.

7.1 POLICIES

7.1.1 GWS.GROUPS.6.1v0.1

Group owners' ability to hide groups from the directory SHOULD be disabled unless necessary for agency mission fulfillment.

- Rationale: Provide group visibility at the directory level and restrict group owners from changing the setting unless required for agency mission fulfillment.
- Last Modified: July 10, 2023

7.2 RESOURCES

- [Google Workspace Admin Help: Set organization-wide policies for using groups](#)

7.3 PREREQUISITES

- None

7.4 IMPLEMENTATION

7.4.1 GWS.GROUPS.6.1v0.1 instructions:

To configure the settings for Sharing options:

1. Sign in to the [Google Admin Console](#).
2. Select **Apps** -> **Google Workspace** -> **Groups for Business**.
3. Select **Sharing settings** -> **Sharing options**.
4. **Uncheck** the **Group owners can hide groups from the directory** checkbox.
5. Select **Save**.

8. THE ABILITY FOR NEWLY CREATED GROUPS TO BE HIDDEN FROM THE DIRECTORY

This section covers whether or not a new group can be hidden from the directory.

8.1 POLICIES

8.1.1 GWS.GROUPS.7.1v0.1

The ability for newly created groups to be hidden from the directory SHOULD be disabled unless necessary for agency mission fulfillment.

- Rationale: Provide group visibility for newly created groups at the directory level and restrict group owners from changing the setting unless required for agency mission fulfillment.
- Last Modified: July 10, 2023

8.2 RESOURCES

- [Google Workspace Admin Help: Set organization-wide policies for using groups](#)

8.3 PREREQUISITES

- The ability for group owners to hide groups from the directory must be enabled for this setting to be selectable.

8.4 IMPLEMENTATION

8.4.1 GWS.GROUPS.7.1v0.1 instructions:

To configure the settings for Sharing options:

1. Sign in to the [Google Admin Console](#).
2. Select **Apps** -> **Google Workspace** -> **Groups for Business**.
3. Select **Sharing settings** -> **Sharing options**.
4. **Ensure** that the **hide newly created groups from the directory** checkbox is not selected.
5. Select **Save**.

9. NEW GROUPS

This section covers the access type setting for new groups that are created.

9.1 POLICIES

9.1.1 GWS.GROUPS.8.1v0.1

New Groups SHOULD be created with an Access type of Restricted unless necessary for agency mission fulfillment.

- Rationale: This helps protect against unauthorized access to groups
- Last Modified: July 10, 2023

9.2 RESOURCES

- [Google Workspace Admin Help: Create a group in your organization](#)

9.3 PREREQUISITES

- This control only applies to agencies with Google Groups for Business enabled.

9.4 IMPLEMENTATION

9.4.1 GWS.GROUPS.8.1v0.1 instructions:

To configure Access type for a Google Group:

1. Sign in to the [Google Admin Console](#).
2. Select **Directory** -> **Groups**.
3. Select **Create group**.
4. Fill in the details for the new group and click **Next**.
5. In the **Access type** section, select the **Restricted** radio button.
6. If the group needs to receive messages from non-members, select the appropriate checkboxes in the **Who can post** row.
7. Select **Next**.
8. Select **Create Group**.