TLP:CLEAR

# GOOGLE COMMON CONTROLS

## 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.<br>• Incorporated comment from OCC making grammatical change to Section 1.1 Assumptions (brevity).<br>• Incorporated comment from OCC making grammatical change to Rationale in Section 7.1.1 (clarity).<br>• Incorporated comment from OCC making wording change to Section 8.1.1 (replacing “never” with “not”).<br>• Incorporated statement from OCC to Rationale in section 9.1.1 regarding unmanaged accounts and federal records.<br>• Incorporated comment from OCC making grammatical change to Rationale in Section 10.1.3 (clarity).<br>• Incorporated comment from OCC making grammatical change to Rationale in Section 10.1.4 (clarity).<br>• Incorporated comment from OCC making wording change to Rationale in Section 11.1.1 (adding “even”).<br>• Incorporated comment from OCC making wording change to Rationale in Section 11.1.2 (adding “even”).<br>• Incorporated comment from OCC making grammatical change to Rationale in Section 12.1.5 (clarity).<br>• Incorporated comment from OCC making grammatical change to Rationale in Section 13.1.1 (clarity).<br>• Incorporated comment from OCC making grammatical change to Rationale in Section 13.1.2 (clarity).<br>• Incorporated comment from OCC making grammatical change to Rationale in Section 15.3 (clarity).<br>• Incorporated comment from OCC making grammatical change to Intro in Section 16 (clarity). | CISA SCuBA | 12/2/2023 |

# CONTENTS

# 1. CISA GOOGLE WORKSPACE SECURITY CONFIGURATION BASELINE FOR COMMON CONTROLS

The Google Workspace (GWS) Admin console is the primary configuration hub for configuring and setting up the subscription. The scope of this document is to provide recommendations for setting up the subscription's security controls. This Secure Configuration Baseline (SCB) provides specific policies to strengthen the security of a GWS tenant.

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 and addresses the following:

- Phishing-Resistant Multi-Factor Authentication
- Context Aware Access
- Login Challenges
- User Session Duration
- Secure Passwords
- Highly Privileged Accounts
- Super Admin Accounts
- Conflicting Account Management
- Catastrophic Recovery Options
- Advanced Protection Program
- App Access to Google APIs
- Authorized Marketplace Apps
- Less Secure Apps
- Google Takeout Service
- System-Defined Rules
- Workspace Logs

## 1.2 ASSUMPTIONS

This document assumes the organization is using GWS Enterprise Plus. The Google Workspace (GWS) Common Controls Secure Configuration Baseline is unique among the GWS configuration baseline documents released by CISA in that it does not align to one specific GWS app. Implementers should be aware of this when cross-referencing the baseline statements to the live GWS admin console. Therefore, this document serves an enterprise-level compendium of implementable and testable configuration settings across the entire GWS admin console. The configurations specified herein correlate to the Security, Account, Directory, Rules, and Marketplace apps sections of the GWS admin console.

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 Common Controls baseline document:

- Assumes users are familiar with overarching Federal cyber guidance and cloud security fundamentals such as the shared responsibility model;
- Accounts for recent direction from Executive Order 14028, the Federal Zero Trust Strategy (published as Office of Management & Budget Memo M-22-09 *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*), CISA's Zero Trust Maturity Model, and the Federal Cloud Security Technical Reference Architecture;
- Observes industry guidance such as the Center for Internet Security's Google Workspace Foundations benchmark and Google official documentation and white papers; and
- Was developed with input from both the Office of Management & Budget (OMB) and Google product managers and security engineers.

## 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 PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA), particularly phishing-resistant MFA, is a critical security control against attacks such as password spraying, password theft, and phishing. Adopting phishing-resistant MFA may take time, especially on mobile devices. Organizations must upgrade to a phishing-resistant MFA method as soon as possible to be compliant with OMB M-22-09 and this policy to address the critical security threat posed by modern phishing attacks. In the intermediate period before phishing-resistant MFA is fully adopted, organizations should adopt an MFA method from the list in GWS.COMMONCONTROLS.1.4v0.1 below.

This control recognizes federation as a viable option for phishing-resistant MFA and includes architectural considerations around on-premises and cloud-native identity federation in established Federal Civilian Executive Branch (FCEB) environments. Federation for GWS can be implemented via a cloud-native identity provider (IdP). Google's documentation acknowledges that on-premises Active Directory implementations may be predominant in environments that adopt GWS and provides guidance on the use of Google Cloud Directory Sync (GCDS) to synchronize Google Account data with an established Microsoft Active Directory or LDAP server.

The following graphic illustrates the spectrum of MFA options and their relative strength, with phishing resistant MFA (per OMB Memo 22-09) being the mandated method. Please note there is a distinction between Google 2 Step Verification (2SV) and MFA as a general term. While FIDO Security Key and Phone as a Security Key are acceptable forms of Phishing-Resistant MFA which rely on Google 2SV as the underlying mechanism, the other forms listed in the "strongest" column do not use Google 2SV but are still acceptable forms of Phishing-Resistant MFA.

## 2.2 POLICIES

### 2.2.1 GWS.COMMONCONTROLS.1.1v0.1

Phishing-Resistant MFA SHALL be required for all users.

```
    > Phishing-resistant methods:

        - FIDO2 Security Key (directly in Google Workspace)

        - Phone as Security Key

        - FIDO2 Security Key (Federated from Identity Provider)

        - Federal Personal Identity Verification (PIV) card (Federated from
agency Active Directory or other identity provider).

        - Google Passkeys
```

- Rationale
  - Required by Office of Management and Budget Memo M-22-09.
  - Add an extra layer of security to user accounts by asking users to verify their identity when they enter a username and password. MFA (including methods using 2-Step Verification) requires an individual to present a minimum of two separate forms of authentication before access is granted. MFA provides additional assurance that the individual attempting to gain access is who they claim to be. With MFA, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.
- Last Modified: August 17, 2023
- Notes
  - Policy 1.1 applies if Phishing-Resistant MFA is available. Otherwise, Policy 1.4 applies.

### 2.2.2 GWS.COMMONCONTROLS.1.2v0.1

Google 2SV new user enrollment period SHALL be set to 1 week.

- Rationale: This allows enough time for new personnel to log into their account and configure MFA prior to getting locked out of their account. However, does not give an excessive amount of time in order to limit security risks.
- Last Modified: August 17, 2023
- Notes
  - This setting and policy only applies when the means of Phishing-Resistant MFA in use relies on Google 2SV.

### 2.2.3 GWS.COMMONCONTROLS.1.3v0.1

Allow users to trust the device SHALL be disabled.

- Rationale: This ensures that Google 2SV must be used each time to prevent unauthorized access to accounts.
- Last Modified: August 17, 2023
- Notes
  - This setting and policy only applies when the means of Phishing-Resistant MFA in use relies on Google 2SV.

### 2.2.4 GWS.COMMONCONTROLS.1.4v0.1

If phishing-resistant MFA is not yet tenable, an MFA method from the following list SHALL be used in the interim.

  - Google Prompt
  - Google Authenticator
  - Backup Codes
  - Software Tokens One-Time Password (OTP): This option is commonly implemented using mobile phone authenticator apps
  - Hardware Tokens OTP

- Rationale: Some agencies do not have capability for phishing-resistant MFA at this time, therefore an alternative is provided.
- Last Modified: August 17, 2023
- Notes
  - ONLY to be enforced if Policy 1.1 is not possible for the agency.
  - SMS or Voice as the MFA method SHALL NOT be used.

## 2.3 RESOURCES

- GWS Admin Help | Set up 2-Step Verification (Deploy)
- GWS Admin Help | Set up 2-Step Verification (Protect your business)
- GWS Admin Help | Set up SSO via a third-party Identity provider
- Google Cloud Architecture Center | Federating Google Cloud with Active Directory
- Google Cloud Architecture Center | Federating Google Cloud with Azure Active Directory

- Google Workspace Updates /| Simplify and Strengthen Sign-In by Enabling Passkeys for Your Users

- Google Security Blog /| So Long Passwords, Thanks for all the Phish
- Allow Users to Skip Passwords at Sign-In (Beta)
- CIS Google Workspace Foundations Benchmark

## 2.4 PREREQUISITES

- FIDO2-compliant security keys

## 2.5 IMPLEMENTATION

Note: If using a third-party IdP with GWS, refer to Google documentation on setting up third-party single sign-on (SSO). If using GWS as the IdP, refer to Google documentation on setting up SSO.

To enforce 2-Step Verification (MFA) for all users, use the Google Workspace Admin Console:

### 2.5.1 Policy 1 common instructions:

1. Sign in to Google Admin console as an administrator.
2. Select **Security** -> **Authentication.**
3. Select **2-Step Verification.**
4. Follow implementation for individual policy implementations
5. Select **Save**

### 2.5.2 GWS.COMMONCONTROLS.1.1v0.1 instructions:

1. Under Authentication, look for the, **Allow users to turn on 2-Step Verification.**
2. Set **Enforcement** to **On.**
3. Select **Save**

### 2.5.3 GWS.COMMONCONTROLS.1.2v0.1 instructions:

1. Set **New user enrollment** period to **1 Week**.
2. Select **Save**

### 2.5.4 GWS.COMMONCONTROLS.1.3v0.1 instructions:

1. Under Frequency, deselect the **Allow user to trust device** checkbox.
2. Select **Save**

### 2.5.5 GWS.COMMONCONTROLS.1.4v0.1 instructions:

If using security keys:

1. Under **Methods**, select **Only security Key**. Next, select **Don't allow users to select security codes**.
2. Select **Save**

If security keys are not yet available for your organization:

1. Under **Methods**, select **Any except verification codes via text, phone call**.
2. Select **Save**

If using Passkeys, use the Google Workspace Admin Console:

1. Sign in to Google Admin console as an administrator.
2. Select **Security** -> **Authentication** -> **Passwordless.**
3. Select **Skip passwords.**
4. Select the **Allow users to skip passwords at sign-in by using passkeys** box.
5. Select **Save.**

# 3. CONTEXT-AWARE ACCESS FOR ALL DEVICES THAT CONNECT TO GWS

Device-based context-aware access provides access control policies based on device disposition attributes such as compliance with organizational secure configuration policies for devices (e.g., managed by Unified

Endpoint Management). GWS also provides other context-aware access policies based on authentication and network information. These can be used to implement more targeted access policies. For advanced use cases, custom context aware access rules can be authored using the Common Expressions Language (CEL).

Device-based context-aware access can be used in several ways depending on agency business requirements. The following options are all acceptable approaches:

- Properties of the device as reported by Google (encryption, screen lock, OS version, etc.)
- Device inventory status (corporate-issued versus BYOD)
- Use of Managed Chrome Browser
- Data based on integration with certain third-party device management tools

It is extremely important to know how context-aware access policies affect one another, for example:

- At a given scope (e.g., Organizational Unit [OU] or Group), each context aware access rule is evaluated separately. If any rule grants access, then access is allowed to the given application.
- If rules are applied to OUs and Groups, which allow an action that may be denied after evaluating a policy at a higher level, then access will be allowed.

To enforce a device policy that requires company-owned devices, Google needs a list of serial numbers for company-owned devices.

## 3.1 POLICIES

### 3.1.1 GWS.COMMONCONTROLS.2.1v0.1

Policies restricting access to GWS based on signals about enterprise devices SHOULD be implemented.

- Rationale: Granular device access control afforded by context-aware access is in alignment with Federal zero trust strategy and principles. Context-aware access can help to increase the security of your GWS data by allowing you to restrict access to certain applications or services based on the user's context.
- Last Modified: July 10, 2023

### 3.1.2 GWS.COMMONCONTROLS.2.2v0.1

Use of context-aware access for more granular controls, including using Advanced Mode (CEL), MAY be maximized and tailored if necessary.

- Rationale: Granular device access control afforded by context-aware access is in alignment with Federal zero trust strategy and principles. Context-aware access can help to increase the security of your GWS data by allowing you to restrict access to certain applications or services based on the user and/or device context. Advanced Mode's Common Expressions Language (CEL) gives administrators the ability to tailor access policies for devices, time-based use cases, authentication, and to combine multiple conditions into tailored controls.
- Last Modified: July 11, 2023

## 3.2 RESOURCES

- GWS Admin Help | Context-Aware Access overview
- GWS Admin Help | Context-Aware Access examples for Basic mode

- GWS Admin Help | Context-Aware Access examples for Advanced mode
- GWS Admin Help | Device management security checklist
- GWS Admin Help | Set up guide: Deploy company-owned devices in Google endpoint management
- GWS Admin Help | Turn endpoint verification on or off
- GWS Admin Help | Set up guide: Deploy company-owned devices in Google endpoint management—Steps 1 and 2
- GitHub | Google | Google Common Expressions Language (CEL)
- Google Cloud Access Context Manager | Macros for CEL expressions
- Google Cloud Access Context Manager | Custom access level specification
- GWS Blog | Enable advanced context-aware access to Google Workspace in the Admin console
- GWS Admin Help | Google Workspace Device management security checklist
- GWS Admin Help | Deploy Context-Aware Access

## 3.3 PREREQUISITES

- One or more of the following user roles should have been configured to set context-aware policies:

```
> Super admin

> Delegated admin with each of these privileges:

        - Data Security -\> Access level management

        - Data Security -\> Rule management

        - Admin API Privileges -\> Groups\>Read

        - Admin API Privileges -\> Users\>Read
```

- Serial numbers may be required to enforce a policy for company-owned devices. Refer to Google documentation on device management for additional guidance.

## 3.4 IMPLEMENTATION

### 3.4.1 GWS.COMMONCONTROLS.2.1v0.1 instructions:

To turn on Context-Aware Access:

1. Access the Google Admin console.
2. From the menu, go to **Security** -> **Access and data control** -> **Context-Aware Access**.
3. Verify **Context-Aware Access** is **ON for everyone**. If not, click **Turn On**.

### 3.4.2 GWS.COMMONCONTROLS.2.2v0.1 instructions:

Note that the implementation details of context-aware access use cases will vary per agency. Refer to Google's documentation on implementing context-aware access for your specific use cases. Common use cases include:

- Require company-owned on desktop but not on mobile device
- Require basic device security
- Allow access to contractors only through the corporate network
- Block access from known hijacker IP addresses
- Allow or disallow access from specific locations
- Use nested access levels instead of selecting multiple access levels during assignment

# 4. LOGIN CHALLENGES

Login challenges are additional security measures used to verify a user's identity. For example, Google might ask the user to confirm their recovery email before logging in as part of a challenge.

## 4.1 POLICIES

### 4.1.1 GWS.COMMONCONTROLS.3.1v0.1

Login Challenges SHALL be enabled when third party SAML SSO is in use.

- Rationale
  - Many organizations use third-party identity providers (IdPs) to authenticate users who use single sign on (SSO) through SAML. The third-party IdP authenticates users and no additional risk-based challenges are presented to them. Any Google 2-Step Verification (2SV) configuration is ignored. This is the default behavior. You can set a policy to allow additional risk-based authentication challenges and 2SV if it's configured. If Google receives a valid SAML assertion (authentication information about the user) from the IdP during user sign-in, Google can present additional challenges to the user.
  - Login challenges requires users have a recovery phone number or email account associated with their organizational account. If not previously configured, users will be prompted to enter this information periodically until provided.
  - One login challenge option prompts users to enter their employee ID. This method is susceptible to information gathering attacks, should a list of employee IDs ever be leaked.
- Last Modified: July 10, 2023

## 4.2 RESOURCES

- GWS Admin Help | Protect Google Workspace accounts with security challenges
- CIS Google Workspace Foundations Benchmark

## 4.3 PREREQUISITES

- When using Employee ID challenge, the Employee ID must be uploaded to Google Workspace through the Agency's Identity Management infrastructure (e.g., via GCDS).

## 4.4 IMPLEMENTATION

### 4.4.1 GWS.COMMONCONTROLS.3.1v0.1 instructions:

1. Sign in to Google Admin console as an administrator.
2. Select **Security**->**Authentication**->**Login challenges.**
3. Under **Organizational units**, ensure that the name for the entire organization is selected.
4. Click **Post-SSO verification**, then select **Ask users for additional verifications from Google if a sign-in looks suspicious, and always apply 2-Step Verification policies (if configured)**. Click **SAVE**.
5. Optionally, if employee IDs are known to agency employees (or accessible to the employee outside of Google Workspace), they may be used.
6. Click **Login challenges**.
7. Select the **Use employee ID to keep my users more secure** checkbox**.**
8. Click **SAVE**.

# 5. USER SESSION DURATION SHALL BE LIMITED

This control allows configuring of limits on how long a GWS session can be active before being prompted for authentication credentials.

Note: If using a third-party IdP, and agency-set web session lengths for its users, then there will be a need to set the IdP session length parameter to expire before the Google session expires to ensure users are forced to sign in again. See GWS documentation for additional details.

## 5.1 POLICIES

### 5.1.1 GWS.COMMONCONTROLS.4.1v0.1

Users SHALL be forced to re-authenticate after an established 12-hour GWS login session has expired.

- Rationale
  - This is to ensure that a session is not active without needing to reauthenticate for a longer period of time as this creates a higher potential for unauthorized access.
- Last Modified: July 10, 2023

## 5.2 RESOURCES

- GWS Admin Help | Set session length for Google services

## 5.3 PREREQUISITES

- None

## 5.4 IMPLEMENTATION

### 5.4.1 GWS.COMMONCONTROLS.4.1v0.1 instructions:

To configure Google session control:

1. Sign in to the Google Admin console as an administrator.
2. Select **Security.**
3. Select **Access and data control** -> **Google session control.**

4. Look for the **Web session duration** heading.
5. Set the duration to **12 hours.**

# 6. SECURE PASSWORDS

Per NIST 800-63 and OMB M-22-09, ensure that user passwords do not expire and that long passwords are chosen. Research indicates that frequent password rotation breeds poor password choice and encourages password reuse. Ensure that passwords are strong to defend against brute-force attacks. Ensure that passwords are not reused to defend against credential theft.

## 6.1 POLICIES

### 6.1.1 GWS.COMMONCONTROLS.5.1v0.1

User password strength SHALL be enforced.

- Rationale: Strong password policies protect an organization by prohibiting the use of weak passwords.
- Last Modified: July 10, 2023

### 6.1.2 GWS.COMMONCONTROLS.5.2v0.1

User password length SHALL be at least 12 characters.

- Rationale: Strong password policies protect an organization by prohibiting the use of weak passwords.
- Last Modified: July 10, 2023

### 6.1.3 GWS.COMMONCONTROLS.5.3v0.1

Password policy SHALL be enforced at next sign-in.

- Rationale: Strong password policies protect an organization by prohibiting the use of weak passwords.
- Last Modified: July 10, 2023

### 6.1.4 GWS.COMMONCONTROLS.5.4v0.1

User passwords SHALL NOT be reused.

- Rationale: Strong password policies protect an organization by prohibiting the use of weak passwords.
- Last Modified: July 10, 2023

### 6.1.5 GWS.COMMONCONTROLS.5.5v0.1

User passwords SHALL NOT expire.

- Rationale: Strong password policies protect an organization by prohibiting the use of weak passwords.
- Last Modified: July 10, 2023

## 6.2 RESOURCES

- GWS Admin Help | Enforce and monitor password requirements for users
- CIS Google Workspace Foundations Benchmark

## 6.3 PREREQUISITES

- None

## 6.4 IMPLEMENTATION

To configure a strong password policy is configured, use the Google Workspace Admin Console:

### 6.4.1 Policy Group 5 common instructions:

1. Sign in to the Google Admin console as an administrator.
2. Select **Security** -> **Authentication.**
3. Locate **Password management.**
4. Follow implementation for each individual policy.
5. Select **Save**.

### 6.4.2 GWS.COMMONCONTROLS.5.1v0.1 instructions:

1. Under **Strength**, select the **Enforce strong password** checkbox**.**

### 6.4.3 GWS.COMMONCONTROLS.5.2v0.1 instructions:

1. Under **Length**, set **Minimum Length** to 12+.

### 6.4.4 GWS.COMMONCONTROLS.5.3v0.1 instructions:

1. Under **Strength and Length enforcement**, select the **Enforce password policy at next sign-in** checkbox**.**

### 6.4.5 GWS.COMMONCONTROLS.5.4v0.1 instructions:

1. Under **Reuse**, deselect the **Allow password reuse** checkbox**.**

### 6.4.6 GWS.COMMONCONTROLS.5.5v0.1 instructions:

1. Under **Expiration**, select **Never Expires.**

# 7. HIGHLY PRIVILEGED ACCOUNTS

Highly privileged accounts represent significant risk to an agency if compromised or if insiders use them in an unauthorized way. Highly privileged accounts share the same risk factors related to the catastrophic impacts on GWS services, user community and agency data, if compromised. This section supports the definition of highly privileged accounts and the controls necessary to protect them.

Pre-Built GWS Admin Roles considered highly privileged:

Super Admin: This role possesses critical control over the entire GWS structure. It has access to all features in the Admin Console and Admin API and can manage every aspect of agency GWS accounts.

User Management Admin: This account has rights to add, remove, and delete normal users in addition to managing all user passwords, security settings, and other management tasks that make it potentially crucial if compromised.

Services Admin: This admin has full rights to turn on or off GWS services and security settings for these services (Gmail, Drive, Voice, etc.). Given that most GWS features are premised on these services being secure, compromise of this account would be critical.

Mobile Admin: This admin has full rights to manage all the agency mobile devices including authorizing their use and controlling the apps that can be downloaded and used on them. This admin can also set the security policies on all agency mobile devices connected to GWS.

Groups Admin: This admin has full rights to view profiles in the organizational and OU structures and can manage all rights for those members in the group.

## 7.1 POLICIES

### 7.1.1 GWS.COMMONCONTROLS.6.1v0.1

Agencies SHALL ensure that all accounts with highly privileged roles are separate administrative accounts, distinct from the ordinary day to day accounts of those personnel.

- Rationale: This helps ensure that the accounts with admin privileges are only used when performing admin tasks and that for ordinary tasks personnel use a lower-privileged account.
- Last Modified: July 11, 2023

### 7.1.2 GWS.COMMONCONTROLS.6.2v0.1

All highly privileged accounts SHALL leverage Google Account authentication with phishing-resistant MFA and not the agency's authoritative on-premises or federated identity system.

- Rationale: Provides a stronger and more centralized form of authentication which provides stronger protections against compromises.
- Last Modified: July 10, 2023

## 7.2 RESOURCES

- Google Cloud Architecture Center | Best practices for planning accounts and organizations
- GWS Admin Help | Create, edit, and delete custom admin roles
- GWA Admin Help | Assign Specific Admin Roles
- GWA Admin Help | Pre-Built Admin Roles

## 7.3 PREREQUISITES

- Super admin users cannot log in to admin.google.com with a 3rd party IdP when using Super Admin level accounts—they must use Google Login as the authentication mechanism. This policy extends this rule to other Admin types.
- Delegated accounts, including the ones defined as highly privileged above, can by default, use a third-party IdP to access admin.google.com: however, this policy prohibits that practice. All highly privileged accounts must use phishing resistant Google Authentication.

## 7.4 IMPLEMENTATION

### 7.4.1 GWS.COMMONCONTROLS.6.1v0.1 instructions:

1. The implementation process for this can be located here.

### 7.4.2 GWS.COMMONCONTROLS.6.2v0.1 instructions:

1. The implementation process for this can be located here.

# 8. SUPER ADMIN ACCOUNTS

Super Admin is the highest privileged role in GWS because it provides unfettered access to the organization. Therefore, if a user's credential with these permissions were to be compromised, it would present significant risks to the security of the organization. Limit the number of users that are assigned the role of Super Administrator. Assign users to finer-grained administrative roles that they need to perform their duties instead of being assigned the Super Administrator role.

## 8.1 POLICIES

### 8.1.1 GWS.COMMONCONTROLS.7.1v0.1

A minimum of **two** and maximum of **four** separate and distinct Super Admin users SHALL be configured.

- Rationale: Having only a single Super Admin Account can be problematic if this user were unavailable for an extended period of time. Also, Super Admin accounts should not be shared amongst multiple users.
  - In addition, having too many super admins could be problematic as then there are many users with those privileges which creates a larger security risk
- Last Modified: July 10, 2023
- Note: Admin count does not include "break-glass" Super Admin accounts.

## 8.2 RESOURCES

- Google Cloud Architecture Center | Best practices for planning accounts and organizations
- GWS Admin Help | Create, edit, and delete custom admin roles
- GWS Admin Help | Assign Specific Admin Roles
- GWS Admin Help | Pre-Built Admin Roles
- GWS Admin SDK Documentation | Make User Super Admin
- CIS Google Workspace Foundations Benchmark

## 8.3 PREREQUISITES

- None

## 8.4 IMPLEMENTATION

### 8.4.1 GWS.COMMONCONTROLS.7.1v0.1 instructions:

To obtain a list of all GWS Super Admins:

1. Sign in to the Google Admin console as an administrator.
2. Navigate to **Account** -> **Admin Roles**.
3. Click the **Super Admin** role in the list of roles
4. The subsequent dialog provides a list of Super Admins.

# 9. CONFLICTING ACCOUNT MANAGEMENT

It is possible for employees of an organization to create conflicting, unmanaged accounts that are unmanaged by an enterprise's Google Workspace tenant. Unmanaged accounts are defined as users who independently created a Google account using the organization's domain. For example, a user with an enterprise/corporate email of user@company.com could create a personal, unmanaged Google account using that email address. This would create an account conflict in a GWS tenant licensed to company.com since email addresses are unique.

Creating a conflicting account can also happen unintentionally. After signing up for Google Cloud Identity or Google Workspace, admins might decide to set up single sign-on with an external identity provider (IdP) such as Azure Active Directory (AD) or Active Directory. When configured, the external IdP might automatically create accounts in Cloud Identity or Google Workspace for all users for which single sign-on was enabled, inadvertently creating conflicting accounts.

Unmanaged accounts carry significant risk, as they cannot be managed by admins, rendering them outside of the scope of protection admins can apply to keep work data secure. Significantly, two-step verification (2SV) cannot be enforced. Even if access is revoked, these accounts can carry a social engineering risk. Further, reconciling conflicting accounts creates churn for admins and adds to the workload of onboarding users to Google Workspace & Google Cloud.

The GWS admin console provides several administrative options for handling conflicting, unmanaged accounts:

- Automatically invite users to transfer unmanaged accounts.
- Replace unmanaged accounts with managed ones.
- Don't create new accounts if unmanaged accounts exist.

This policy requires replacing unmanaged accounts with managed ones. When this option is configured, data owned by the account will not be imported; the user will receive a temporary account address, which they'll need to manually replace with a @gmail.com address of their choice; the user will receive an email notification of this and are informed they cannot use the original email any longer.

By changing the email address, the user resolves the conflict by ensuring that the managed account and consumer account have different identities. The result remains that they have one consumer account that has all their original data, and one managed account that doesn't have access to the original data.

## 9.1 POLICIES

### 9.1.1 GWS.COMMONCONTROLS.8.1v0.1

Account conflict management SHALL be configured to replace conflicting unmanaged accounts with managed ones.

- Rationale
  - As per Google, if employees of an organization use unmanaged accounts, then the premise of having a single place to manage user identities is compromised. Unmanaged accounts aren't managed by Google Workspace or Cloud Identity. Therefore, the ideal security course of action for government agencies is to replace conflicting unmanaged accounts with managed ones, rather than allowing a grace period or doing nothing with such accounts.
  - Per Google, unmanaged personal accounts that use a business email address carry multiple risks, including the following:

- You can't control the lifecycle of an unmanaged user account. An employee who leaves the company might continue to use the unmanaged account to access corporate resources or to generate corporate expenses.
- Even if you revoke access to all resources, the unmanaged account might still pose a social engineering risk. Because the user account uses a seemingly trustworthy identity with your company's domain name, the former employee might be able to convince current employees or business partners to grant access to resources again—for example, a sensitive Drive file.
- A former employee with an unmanaged account might use the user account to perform activities that aren't in line with your organization's policies, which could put your company's reputation at risk.
- You can't enforce security policies like 2-step verification or password complexity rules.
- You can't restrict which geographic location Docs and Drive data is stored in, which might be a compliance risk.
- You can't restrict which Google services can be accessed by an unmanaged user account.

  – Reconciling conflicting accounts creates churn for admins and adds to the workload of onboarding users to Google Workspace & Google Cloud.
  – Note that if unmanaged accounts are used for official federal government business, they may be subject to record-keeping requirements under the Federal Records Act, 44 U.S.C. Chapter 31 *et seq*.

- Last Modified: September 14, 2023

## 9.2 RESOURCES

- GWS Admin Help | Use the transfer tool to migrate unmanaged users

- GWS Admin Help | Find and add unmanaged users

- Google Workspace Updates Blog | Resolve conflict accounts faster with the new Conflict Accounts Management tool

- Google Cloud Architecture Center | Migrating consumer accounts

- Google Cloud Architecture Center | Best practices for planning accounts and organizations

## 9.3 PREREQUISITES

- Super Admin privileges

## 9.4 IMPLEMENTATION

### 9.4.1 GWS.COMMONCONTROLS.8.1v0.1 instructions:

To configure account conflict management per the policy:

1. Sign in to the Google Admin console as an administrator.
2. Navigate to **Account** -> **Account settings.**
3. Click the **Conflicting accounts management** card.
4. Select the radio button option: **"Replace conflicting unmanaged accounts with managed ones."**

5. Click **Save.**

# 10. CATASTROPHIC RECOVERY OPTIONS FOR SUPER ADMINS

If a catastrophic event occurs in which the GWS Super Admin credentials are lost or stolen, this control is in place to require “break-glass” Super Admin accounts. These accounts are to be physically secured in a highly secure location as a recovery option, with the account self-recovery feature disabled in GWS.

## 10.1 POLICIES

### 10.1.1 GWS.COMMONCONTROLS.9.1v0.1

A second, “break-glass” Super Admin account SHALL be created and physically secured for each individual Super Admin user to mitigate account access issues resulting from catastrophic credential loss or compromise.

- Rationale
  - Having a "break-glass" account for each super admin is important in case the super admin loses access to their account and needs to recover it.
  - Only using this account for recovery provides a benefit of being able to track when they recover their account as the access to the "break-glass" account would indicate a recovery.
  - Keeping it physically secure ensures there is no unauthorized access to the account.
- Last Modified: July 10, 2023

### 10.1.2 GWS.COMMONCONTROLS.9.2v0.1

Account self-recovery for Super Admins SHALL be disabled, forcing Super Admin users who have lost their login credentials to contact another Super Admin to recover their account.

- Rationale: This makes it more difficult for a potential adversary from being able to attempt to gain access to a super admin account through the method of account recovery.
- Last Modified: July 10, 2023

### 10.1.3 GWS.COMMONCONTROLS.9.3v0.1

“Break-glass” account credentials SHALL be used only if all Super Admins have lost their credentials.

- Rationale: This helps ensure that there is limited access to the "break-glass" account keeping the credentials to those accounts secure and not exposing them to potentially being leaked.
- Last Modified: July 10, 2023

### 10.1.4 GWS.COMMONCONTROLS.9.4v0.1

A geographically separate and secure location SHOULD be planned and implemented to store “break-glass” account credentials for Super Admins.

- Rationale
  - Keeping break glass credentials in a separate and secure location helps prevent against losing the credentials if something happens to the primary location.

  - In addition, provides extra security as the credentials are kept separate from where an attacker would most likely look.

- Last Modified: July 10, 2023

## 10.2 RESOURCES

- GWS Admin Help | Allow super administrators to recover their password
- GWS Admin Help | Recover an account protected by 2-Step Verification

## 10.3 PREREQUISITES

- None

## 10.4 IMPLEMENTATION

### 10.4.1 GWS.COMMONCONTROLS.9.1v0.1 instructions:

To configure break glass Super Admin account:

1. Follow standard instructions for setting up a GWS normal user
2. Follow these instructions for upgrading user to a Super Admin
3. Link: https://support.google.com/a/answer/172176
4. Follow the guidance in this document for setting up phishing resistant MFA for the Super Admin
5. Store the MFA credentials for this account in a highly protected safe or secured room
6. Set up multi-factor and/or multi-person access to the secured area

### 10.4.2 GWS.COMMONCONTROLS.9.2v0.1 instructions:

To disable Super Admin account self-recovery:

1. Sign in to https://admin.google.com as an administrator.
2. Select **Security** -> **Authentication.**
3. Select **Account Recovery**.
4. Click **Super admin account recovery**.
5. To apply the setting to all your Super Admins, leave the top OU selected. Otherwise, select a child OU or a configuration group.
6. Deselect the **Allow Super Admins to recover their account** checkbox.
7. Click **Save**.
8. Ask your Super Admins to set up a recovery phone number or email address for receiving password recovery instructions.

### 10.4.3 GWS.COMMONCONTROLS.9.3v0.1 instructions:

1. There are no implementation steps for this policy.

### 10.4.4 GWS.COMMONCONTROLS.9.4v0.1 instructions:

1. There are no implementation steps for this policy.

# 11. GWS ADVANCED PROTECTION PROGRAM

This control enforces more secure protection of highly privileged, senior executive and sensitive users accounts from targeted attacks. It enforces optional GWS user security features like:

- Strong authentication with security keys
- Use of security codes with security keys
- Restrictions on third-party access to account data
- Deep Gmail scans
- Google Safe Browsing protections in Chrome
- Account recovery through admin

## 11.1 POLICIES

### 11.1.1 GWS.COMMONCONTROLS.10.1v0.1

Highly privileged accounts SHALL be enrolled in the GWS Advanced Protection Program.

- Rationale
  - Sophisticated phishing tactics can trick even the most savvy users into giving their sign-in credentials to attackers. Advanced Protection requires you to use a security key, which is a hardware device or special software on your phone used to verify your identity, to sign in to your Google Account. Unauthorized users won't be able to sign in without your security key, even if they have your username and password.
  - The Advanced Protection Program includes a curated group of high-security policies that are applied to enrolled accounts. Additional policies may be added to the Advanced Protection Program to ensure the protections are current.
- Last Modified: July 10, 2023

### 11.1.2 GWS.COMMONCONTROLS.10.2v0.1

All sensitive user accounts SHOULD be enrolled into the GWS Advanced Protection Program. This control enforces more secure protection of sensitive user accounts from targeted attacks. Sensitive user accounts include political appointees, Senior Executive Service (SES) officials, or other senior officials whose account compromise would pose a level of risk prohibitive to agency mission fulfillment.

- Rationale
  - Sophisticated phishing tactics can trick even the most savvy users into giving their sign-in credentials to attackers. Advanced Protection requires you to use a security key, which is a hardware device or special software on your phone used to verify your identity, to sign in to your Google Account. Unauthorized users won't be able to sign in without your security key, even if they have your username and password.
  - The Advanced Protection Program includes a curated group of high-security policies that are applied to enrolled accounts. Additional policies may be added to the Advanced Protection Program to ensure the protections are current.
- Last Modified: July 10, 2023

## 11.2 RESOURCES

- GWS Admin Help | Protect users with the Advanced Protection Program
- GWS Admin Help | Advanced Protection Program FAQ

- CIS Google Workspace Foundations Benchmark

## 11.3 PREREQUISITES

- Two security keys are required for added assurance. If one key is lost or damaged, users can use the second key to regain account access.

## 11.4 IMPLEMENTATION

### 11.4.1 Policy Group 10 instructions:

To allow all users to enroll:

1. Sign in to the Google Admin console as an administrator.
2. Select **Security** -> **Authentication** -> **Advanced Protection Program.**
3. On the right, locate the **Advanced Protection** header.
4. Locate the **Allow users to enroll in the Advanced Protection Program** header.
5. Select **Enable user enrollment.**
6. Click **SAVE.**

# 12. APP ACCESS TO GOOGLE APIS

Agencies need to have a process in place to manage and control application access to GWS data. This control enables the ability to restrict access to Google Workspace APIs from other applications and is aimed at mitigating the significant cybersecurity risk posed by the potential compromise of OAuth tokens. The baseline policy statements are written to allow implementers to balance operational need with risk posed by granting app access.

## 12.1 POLICIES

### 12.1.1 GWS.COMMONCONTROLS.11.1v0.1

Agencies SHALL develop and implement a process to explicitly allow-list (trust) third-party app access to GWS services.

- Rationale
  - Prevents unauthorized access to GWS through the GWS API which provides additional protection against cyber attacks.
- Last Modified: July 10, 2023

### 12.1.2 GWS.COMMONCONTROLS.11.2v0.1

Agencies SHALL use GWS application access control policies to restrict access to all GWS services by third party apps.

- Rationale: You can restrict (or leave unrestricted) access to most Workspace services, including Google Cloud Platform services such as Machine Learning. For Gmail and Google Drive, you can specifically restrict access to high-risk scopes (for example, sending Gmail or deleting files in Drive). While users are prompted to consent to apps, if an app uses restricted scopes and you haven't specifically trusted it, users can't add it.
- Last Modified: July 10, 2023

### 12.1.3 GWS.COMMONCONTROLS.11.3v0.1

Agencies SHALL NOT allow users to consent to access to low-risk scopes.

- Rationale: Allowing users to give access to OAuth scopes that aren't classified as high-risk could still allow for apps that are not trusted to be granted access by non-administrator personnel and without having to be allowlisted in accordance with 11.1.
- Last Modified: July 10, 2023

### 12.1.4 GWS.COMMONCONTROLS.11.4v0.1

Agencies SHALL NOT trust unconfigured internal apps.

- Rationale: By not trusting unconfigured apps it is ensuring the platform remains secure as unconfigured apps could be unsecure and create vulnerabilities within the whole system.
- Last Modified: July 10, 2023

### 12.1.5 GWS.COMMONCONTROLS.11.5v0.1

Agencies SHALL NOT allow users to access unconfigured third-party apps.

- Rationale: Not allowing access to unconfigured apps helps ensure the platform remains secure as unconfigured apps could be unsecure and create vulnerabilities within the whole system.
- Last Modified: July 10, 2023

## 12.2 RESOURCES

- RFC 6819
- RFC 6749
- OMB M-22-09
- GWS Admin Help | Control which third-party & internal apps access GWS data
- CIS Google Workspace Foundations Benchmark

## 12.3 PREREQUISITES

- None

## 12.4 IMPLEMENTATION

### 12.4.1 Policy Group 11 common instructions:

1. Sign in to Google Admin console.
2. Go to **Security** -> **Access and Data Control** -> **API controls.**

### 12.4.2 GWS.COMMONCONTROLS.11.1v0.1 instructions:

1. Select **Manage Google Services.**
2. Select the **Services box** to check all services boxes.
3. Once this box is selected, then the **Change access** link at the top of console will be available; select it.
4. Select **Restricted: Only trusted apps can access a service.**
5. Select **Change** then **confirm** if prompted.

### 12.4.3 GWS.COMMONCONTROLS.11.2v0.1 instructions:

1. There are no implementation steps for this policy

### 12.4.4 GWS.COMMONCONTROLS.11.3v0.1 instructions:

1. Select **Manage Google Services.**
2. Select the **Services box** to check all services boxes.
3. Once this box is selected, then the **Change access** link at the top of console will be available; select it.
4. Ensure to uncheck the check box next to **For apps that are not trusted, allow users to give access to OAuth scopes that aren't classified as high-risk.**
5. Select **Change** then **confirm** if prompted.

### 12.4.5 GWS.COMMONCONTROLS.11.4v0.1 instructions:

1. Select **Settings.**
2. Select **Unconfigured third-party apps** and select **Don't allow users to access any third-party apps**
3. Select **SAVE.**

### 12.4.6 GWS.COMMONCONTROLS.11.5v0.1 instructions:

1. Select **Settings.**
2. Select **Internal apps** and uncheck the box next to **Trust internal apps.**
3. Select **SAVE.**

It should be noted that admins will have to manually approve each trusted app. The implementation steps for this activity are outlined in Google's documentation on controlling which third-party & internal apps access GWS data (also listed under Resources).

# 13. AUTHORIZED GOOGLE MARKETPLACE APPS

This section enables the ability to restrict the installation of Google Workspace Marketplace apps to a defined list provided and configured in the app allowlist.

## 13.1 POLICIES

### 13.1.1 GWS.COMMONCONTROLS.12.1v0.1

Policy SHOULD be established dictating the app review and approval process.

- Rationale: Helps ensure a standardized procedure for approving apps for marketplace and ensures it is documented.
- Last Modified: July 10, 2023

### 13.1.2 GWS.COMMONCONTROLS.12.2v0.1

Only approved Google Workspace Marketplace applications SHOULD be allowed for installation.

- Rationale: Users should only be allowed to install approved and vetted apps. This will help limit the overall attack surface for the organization.
- Last Modified: July 10, 2023

## 13.2 RESOURCES

- GWS Admin Help | Manage Google Workspace Marketplace apps on your allowlist

- CIS Google Workspace Foundations Benchmark

## 13.3 PREREQUISITES

- None

## 13.4 IMPLEMENTATION

### 13.4.1 GWS.COMMONCONTROLS.12.1v0.1 instructions:

1. There are no implementation steps for this policy

### 13.4.2 GWS.COMMONCONTROLS.12.2v0.1 instructions:

1. Sign in to the Google Admin console as an administrator.
2. Select **Apps** -> **Google Workspace Marketplace apps** -> **Settings.**
3. Select **Allow users to install and run only selected apps from the Marketplace.**
4. Click **Save.**

To add an app to the allowlist:

1. On the left-hand side above **Setting,** click **Apps lists.**
2. Click the **ALLOWLIST APP** to add an app to the allow list.
   or
3. Click **Allowlisted Apps** to manage the allow list.

# 14. LESS SECURE APPS

This control disables legacy authentication and requires the use of modern authentication protocols based on federation for access from applications.

Some older versions of common software may break when this control is implemented. Examples of these apps include:

- Mails configured with POP3
- Older versions of Outlook

## 14.1 POLICIES

### 14.1.1 GWS.COMMONCONTROLS.13.1v0.1

Access to Google Workspace applications by less secure apps that do not meet security standards for authentication SHALL be prevented.

- Rationale: You can block sign-in attempts from some apps or devices that are less secure. Apps that are less secure don't use modern security standards, such as OAuth. Using apps and devices that don't use modern security standards increases the risk of accounts being compromised. Blocking these apps and devices helps keep your users and data safe.
- Last Modified: July 10, 2023

## 14.2 RESOURCES

- GWS Admin Help | Control access to less secure apps

- CIS Google Workspace Foundations Benchmark

## 14.3 PREREQUISITES

- None

## 14.4 IMPLEMENTATION

### 14.4.1 GWS.COMMONCONTROLS.13.1v0.1 instructions:

1. Sign in to the Google Admin console as an administrator.
2. Select **Security.**
3. Select **Access and data control** -> **Less secure apps.**
4. Select **Disable access to less secure apps (Recommended).**
5. Click **Save** to commit this configuration change.

# 15. GOOGLE TAKEOUT SERVICES FOR USERS

This section prevents users from downloading a copy of the Google Takeout service's data to their user accounts. Services include Google Blogger, Books, Maps, Pay, Photos, Play, Play Console, Location History and YouTube, among numerous others.

## 15.1 POLICIES

### 15.1.1 GWS.COMMONCONTROLS.14.1v0.1

Google Takeout services SHALL be disabled for users.

- Rationale: Google Takeout is a service that allows you to download a copy of your data stored within 40+ Google products and services. This includes data from Gmail, Drive, Photos, Calendar, and many others. You can download your data in a variety of formats, including ZIP, TAR, and XML. While there may be a valid use case for individuals to backup their data in non-enterprise settings, this feature represents considerable attack surface as a mass data exfiltration mechanism, particularly in enterprise settings where other backup mechanisms are likely in use.
- Last Modified: July 10, 2023

## 15.2 RESOURCES

- GWS Admin Help | Security checklist for medium and large businesses
- GWS Admin Help | Allow or block Google Takeout

## 15.3 PREREQUISITES

- Determine which OU or access group will be affected by this policy and confirm that the right user and system accounts are in that OU or access group.

## 15.4 IMPLEMENTATION

### 15.4.1 GWS.COMMONCONTROLS.14.1v0.1 instructions:

1. Sign in to https://admin.google.com as an administrator.
2. Select **Account** then **Google Takeout.**

3. Select **User access to Takeout for Google services**.
4. For services without an individual admin control, select **Services without an individual admin control** then **Edit.**
5. Select **Don't allow for everyone**.
6. Click **Save**.
7. For services with an individual admin control, under **apps** select the checkbox next to **Service name** and select **Don't allow**.
8. Click **Save.**

## 16. SYSTEM-DEFINED RULES

GWS includes system-defined alerting rules that provide situational awareness into risky events and actions. A security best practice is to enable the following list of rules. Please note that some, but not all, of these rules may be set to "on" by default. Rules that are not listed may be useful but not security relevant. Review all system-defined rules to implement the appropriate configuration based on individual requirements.

- Google security checklist for medium and large businesses
- Government-backed attacks
- User-reported phishing
- User's Admin privilege revoked
- User suspended for spamming through relay
- User suspended for spamming
- User suspended due to suspicious activity
- User suspended (Google identity alert)
- User suspended (by admin)
- User granted Admin privilege
- User deleted
- Suspicious programmatic login
- Suspicious message reported
- Suspicious login
- Suspicious device activity
- Suspended user made active
- Spike in user-reported spam
- Rate limited recipient
- Phishing message detected post-delivery
- Phishing in inboxes due to bad allowlist
- New user added
- Mobile settings changed

- Malware message detected post-delivery
- Leaked password
- Google Operations
- Gmail potential employee spoofing
- Email settings changed
- Drive settings changed
- Domain data export initiated
- Device compromised
- Calendar settings changed
- Account suspension warning
- Client-side encryption service unavailable

## 16.1 POLICIES

### 16.1.1 GWS.COMMONCONTROLS.15.1v0.1

Required system-defined alerting rules, as listed in the Policy section, SHALL be active, with alerts enabled when available. Any system-defined rules not are considered optional but ought to be reviewed for consideration.

- Rationale: System-defined rules can allow an administrator to be notified of specific activity within a domain—such as a suspicious sign-in attempt, a compromised mobile device, or when another administrator changes settings.
- Last Modified: July 10, 2023

## 16.2 RESOURCES

- GWS Admin Help | Data sources for the security investigation tool
- GWS Admin Help | View and edit system-defined rules

## 16.3 PREREQUISITES

- None

## 16.4 IMPLEMENTATION

### 16.4.1 GWS.COMMONCONTROLS.15.1v0.1 instructions:

1. Sign in to Google Admin console.
2. On the left navigation pane, click the hamburger menu above **Home**->**Show more**.
3. Click **Rules**.
4. From the Rules page, click **Add a filter**.
5. From the drop-down menu, select **Type**.
6. Select the **System defined** check box.
7. Click **Apply**.

8. A list of system defined rules displays. Select one of the rules from the list by clicking the table row for that rule—for example, the Device compromised rule.
9. From the Rule details page, you can view the conditions and actions for the rule—for example, to confirm if email notifications are turned on, and to confirm the recipients for those email notifications.
10. Click **Edit Rule**.
11. Click **Next: View Conditions**.
12. Click **Next: Add Actions**.
13. From the Actions page, you can change the severity for the alert to High, Medium, or Low, send an alert to the alert center if the rule's conditions are met, set up admin email notifications, and specify recipients for those notifications.
14. Click **Next: Review**.
15. Review the updated rule details, and then click **Update Rule**.

# 17. GOOGLE WORKSPACE LOGS

Configure GWS to send critical logs to the agency's centralized SIEM so that they can be audited and queried. Configure GWS to send logs to a storage account and retain them for when incident response is needed.

## 17.1 POLICY

### 17.1.1 GWS.COMMONCONTROLS.16.1v0.1

The following critical logs SHALL be sent at a minimum.

```
> Admin Audit logs

> Enterprise Groups Audit logs

> Login Audit logs

> OAuth Token Audit logs

> SAML Audit log

> Context Aware Access logs
```

- Rationale
  - OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, provides guidance on log retention for federal agencies. The memorandum defines the types of logs that must be retained at each maturity level for log retention.
- Last Modified: July 10, 2023

### 17.1.2 GWS.COMMONCONTROLS.16.2v0.1

Audit logs SHALL be maintained for at least 6 months in active storage and an additional 18 months in cold storage, as dictated by OMB M-21-31. The logs SHALL be sent to the agency's Security Operations Center (SOC) for monitoring.

- Rationale: OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, provides guidance on log retention for federal agencies. The memorandum defines three maturity levels for log retention, with each level requiring different minimum retention periods.
- Last Modified: July 10, 2023

## 17.2 RESOURCES

- GWS Admin Help | Share data with Google Cloud Platform services
- Google Cloud Operations Suite | Audit logs for Google Workspace
- Google Cloud Operations Suite | View and manage audit logs for Google Workspace
- Google Cloud Operations Suite | Aggregate and store your organization's logs
- Google Cloud Architecture Center | Google Logging export scenarios
- GWS Admin Help | Data sources for GWS Audit and investigation page
- Google Cloud Operations Suite | Configure and Manage sinks – Google Cloud
- OMB M-21-31 | Office of Management and Budget

## 17.3 PREREQUISITES

- None

## 17.4 IMPLEMENTATION

### 17.4.1. GWS.COMMONCONTROLS.16.1v0.1 instructions:

1. Sign in to the Google Admin console as an administrator.
2. Go to Menu Account > Account settings > Legal and compliance.
3. Click **Sharing options.**
4. Select **Enabled.**
5. Click **Save**.

### 17.4.2 GWS.COMMONCONTROLS.16.2v0.1 instructions:

1. There is no implementation for this policy.