Understanding Your Google Workspace Security Assessment: A Customer Guide

This guide will help you understand and interpret the information provided in your Google Workspace Security Assessment report. Our aim is to empower you with the knowledge to make informed decisions about your organisation's security posture.

Overview of the Security Assessment Tool

The Security Assessment Tool (SAT) provides a comprehensive analysis of your Google Workspace (GWS) environment against industry best practices and recommended security settings. We choose to interpret the Center for Internet Security (CIS) benchmarks in conjunction with our many years of experience managing GWS. The report highlights areas of compliance and identifies potential vulnerabilities, offering actionable insights to enhance your security.

Example alignment, prioritisation and benchmark mapping

(Note: Renders differently in an actual report, benchmarking is available in some tiers)

Setting name	Description	Recommendation	Priority	CIS benchmark alignment
User Settings - Mail delegation - Allow users to grant their mailbox access to a Google group	Controls whether the ability to delegate mailbox access can be extended to groups instead of just individual users	Disable automatic forwarding to prevent users from auto-forwarding mail.	High	3.1.3.1.1 (L1) Ensure users cannot delegate access to their mailbox (Manual)

Navigating the Report

Your security assessment report is divided into sections: **Summary** and **Policy Details** (potentially more dependent on your report type). You can switch between these sections using the tabs at the top of the report or Click on individual **Category Scores** buttons to jump to that section of the **Policy Details**.

Summary Tab

The Summary tab provides a high-level overview of your security posture:

- **Overall Compliance Score**: This score indicates your organisation's overall compliance with best practice settings, expressed as a percentage. A higher percentage signifies better adherence to recommended security configurations

- **High Priority Issues**: This number represents unique settings that are not fully compliant and pose a significant security risk. Addressing these issues should be your top priority
- **Fully Compliant Settings**: This shows the number of unique settings that perfectly match the recommended best practices, out of the total assessed settings
- **Category Scores:** Discussed below
- **Executive Summary:** textual interpretation of the information and calling out key concerns in your assessment. This is an AI generated synopsis of your review data.

Category Scores

This section breaks down your compliance score by different Google Workspace categories (e.g., Calendar, Chat, Drive and Docs). Each category displays:

- **Category Name**: The specific Google Workspace service or area being assessed
- **Score**: The compliance percentage for that specific category. The color of the score (e.g., red, yellow, green) indicates the level of compliance
- **High Priority Issues**: The number of high-priority non-compliant settings within that category

You can click on any category to jump directly to its detailed settings in the Policy Details tab.

AI Generated Executive Summary

This section gives a textual overview of your assessment and calls out critical items that need addressing urgently

Policy Details Tab

The Policy Details tab provides a granular view of each assessed security setting.

Email Security (DNS Records)

Reports the existence of SPF, DKIM and DMARC records. It does not underwrite the accuracy or health of those settings. It only reports on your primary domain that is linked to your GWS instance. We do offer a service to analyse and solidify your brand through correct configuration of your email reputation settings. Talk to us today to move forward with this essential service.

Policy Category Details

This section is a concertina by category and further each policy setting with fine-grained results of our investigation. You can control the focus of detail using the sliders at the top:

- **Show only non-compliant**: Use this toggle to filter the view and display only those settings that are not compliant with recommendations
- **Show only drifted** (report tier dependant): Use this toggle to see settings that were previously compliant but have “drifted” off track
- **Show only ADMIN defined**: Use this toggle to filter the view and display only settings that have been explicitly configured by an administrator
    - Settings marked as SYSTEM are still aligned to default.

When you click "View Details" for a specific setting, an expanded section will appear with the following information:

- **Policy Key**: The unique identifier for the policy within Google Workspace
- **Description**: A brief explanation of what the setting controls
- **Recommendation**: Our recommended best practice for this setting, including the rationale behind the recommendation
- **Recommended Value**: The ideal value for the setting to be compliant.
- **More Info**: A link to Google's official support documentation for more in-depth information about the setting
- **Target Configuration Details**: This table provides details on how the setting is configured across different Organisational Units (OUs) within your Google Workspace
    - **Target**: The specific Organisational Unit to which the setting applies
    - **Source**: Indicates whether the setting is SYSTEM defined or ADMIN defined
    - **Current Value**: The actual value currently configured for the setting in your Google Workspace
    - **Compliant**: Indicates if the current value for that specific OU is compliant with the recommended value
    - **Actions**: This column may be empty in your report, but at certain purchase levels contains a button allowing you to capture a rationale for why a setting has that certain value, notably exception handling eg: for a valid business reason you allow a setting that is benchmarked as not meeting best practice.

Other Tabs

Depending on the SAT version purchased you will have a range of other Tabs that either give even more insight to the configuration of your GWS instance or provide additional logs and management features.

Additional Metrics

The Additional Metrics tab provides a range of insights into User and Device related security and metrics.

Where relevant these metrics can be sorted using the arrow icon in the table header for the various fields to reveal the insight for which you are looking. Metrics include:

- Password Strength
- External Document Sharing
- My Drive Storage
- Groups - Owners
- Groups - Join status
- Groups - External members
- GWS Admin Roles
- Authorised Third Party Apps
- ChromeOS version.

Changelogs

This log shows the most recent changes to your security settings. Up to 200 of the latest changes are shown. Allowing you to track changes in your workspace and monitor actions from the Admin team.

Regenerate report

This button will only work for appropriately permissioned users, and further is tier dependent, as ‘once off’ settings capture levels will not allow for later updating. Talk to our team or visit the Google Workspace Marketplace to change tiers, for extra features.

User management

This button will access a control panel that will allow you to authorise access to view the report by others in your Workspace.

Interpreting Compliance Status

- **Yes (Green)**: The setting's current value matches the recommended best practice
- **No (Red)**: The setting's current value does not match the recommended best practice, indicating a potential security vulnerability
- **Varies (Amber)**: The setting has different configurations across your Organisational Units, leading to mixed compliance status. You will need to examine the "Target Configuration Details" to see which OUs are compliant and which are not. This setting regularly occurs when you have.

Understanding Priority Levels

- **High Priority**: These are critical settings that, if misconfigured, could lead to significant security breaches, data loss, or unauthorised access. Addressing these issues should be your immediate focus
- **Medium Priority**: These settings, while important, may not pose an immediate risk but could contribute to a weakened security posture or lead to compliance issues

- **Low Priority**: These settings generally have a minor impact on overall security but are still recommended for a more robust security environment.

Next Steps

After reviewing your security assessment report, we recommend the following:

1. **Prioritise High-Priority Issues**: Focus on addressing all "High Priority" non-compliant settings first
2. **Review Medium and Low Priority Issues**: Once high-priority items are addressed, systematically work through medium and low-priority issues
3. **Consult More Info Links**: For a deeper understanding of each setting and its implications, refer to the "More Info" links provided in the policy details
4. **Implement Recommendations**: Based on the recommendations, adjust your Google Workspace settings accordingly
5. **Regular Assessments**: Security is an ongoing process. We recommend regular security assessments to ensure continuous compliance and protection against evolving threats.

If you have any questions or require assistance in interpreting your report or implementing the recommendations, please do not hesitate to contact our support team. We conduct remediation of GWS settings regularly and can action your items promptly to return your Workspace to a secure and healthy posture.