Integration Guide: Cloud App Security (SaaS Security) and G Suite

July 2019

This document describes how SonicWall® Cloud App Security (SaaS Security) is integrated with G Suite.

Topics:

• About Cloud App Security (SaaS Security)
• System Requirements
• Activating G Suite for Cloud App Security
• Configuring G Suite for Cloud App Security
• Testing Your Integration
• For More Information

About Cloud App Security (SaaS Security)

Cloud App Security (SaaS Security) solution delivers out-of-band scanning of traffic to sanctioned and unsanctioned SaaS applications using APIs and traffic log analysis. The solution seamlessly integrates with the sanctioned SaaS applications using native APIs delivering next-gen email security for cloud email and providing CASB-like functionalities: visibility, advanced threat protection, data loss prevention (DLP) and compliance.

When deployed with SonicWall next-generation firewall (NGFW), Cloud App Security (SaaS Security) offers shadow IT visibility and control for cloud usage on the network.

System Requirements

• SonicWall Cloud App Security (SaaS Security)
• G Suite Business or G Suite Enterprise

IMPORTANT: SonicWall Cloud App Security (SaaS Security) only supports G Suite Business and G Suite Enterprise accounts. When you attempt to activate a non-business Google account for SonicWall Cloud App Security (SaaS Security), the activation will fail with the error message, “This app isn’t verified”.

IMPORTANT: If you plan to assign Cloud App Security licenses to only a specific set of G Suite users, create the G Suite group before activating your G Suite cloud applications for Cloud App Security. After initial cloud application activation, the cloud application onboarding process may take up to 12 hours. Adding new users to the G Suite group later may result in delay in synchronizing the licensed users with both systems. For more information, refer to “Managing Cloud App Security (SaaS Security) Licenses” in the Cloud App Security (SaaS Security) Administration Guide.
Activating G Suite for Cloud App Security

To activate G Suite for Cloud App Security:

1. In Cloud App Security, navigate to either the:
   - SaaS Selection page (during initial setup and configuration).
   - Cloud App Store page.
2. Click Start on either the Gmail or Google Drive tile.
3. Select I Accept Terms of Service to accept the service terms. You can click the Terms of Service link to view its details.
4. Click Continue to authorize any supporting applications.
5. Log into your Google business account.
6. Click Next.

NOTE: Only G Suite Business and G Suite Enterprise accounts are supported by Cloud App Security.
7 Agree to the terms of service and click **Accept**.

8 On the G Suite Marketplace, click the **Domain Install** button on the upper right of the page to install SonicWall Cloud Security.

9 When prompted for a **Domain wide install**, click **Continue**.
10 When the installation completes, a confirmation message displays. Click **Done** to continue.

11 On the G Suite Marketplace, click the **Launch** button on the upper right of the page.

12 Select your Google account from the list.

**NOTE:** Make certain that you select the same Google account that you used in previous steps.
13 If prompted, log into your Google business account again.

14 When prompted for a **Domain wide install**, click **Continue**.

15 Click **Continue** to proceed.

16 On the G Suite Marketplace, click the **Domain Install** button on the upper right of the page to install **SonicWall Cloud Monitor**.
17 Agree to the terms of service and click **Accept**.

18 When the installation completes, a confirmation message displays.

Click **Done** to continue.

19 On the G Suite Marketplace, click the **Launch** button on the upper right of the page.
On the Gmail groups selection or Google Drive groups selection page:

- Select All Organization if you want to assign Cloud App Security licenses to all of the users in your organization.
- Select Specific Groups if you want to assign Cloud App Security licenses to only a specific G Suite group in your organization. Using Group Filters is the most effective way to manage your Cloud App Security licenses for a specific subset of users within your organization.

Enter the name of the G Suite group to which you want to assign the licenses.

**NOTE:** Licenses are assigned in alphabetical order.

- If the number of users exceeds the number of available licenses, all user licenses will be assigned in alphabetical order by the system automatically. You can manually unassign users in order to free up licenses.
- If the number of licenses exceeds the number of users, the remaining licenses will remain unassigned. Any new users added to the group will be assigned from the available license pool.

Enter the name of the G Suite group to which you want to assign the licenses.

**NOTE:** Only one group is supported for G Suite cloud applications at this time. If you enter more than one group, an error message is displayed.

You can change this setting later, if needed, on the Configuration > Cloud App Store page. Refer to “Managing Cloud App Security (SaaS Security) Licenses” in the Cloud App Security (SaaS Security) Administration Guide for more information.

**NOTE:** If you add users to the G Suite group later, it may take up to 12 hours for the user licenses to synchronize between the systems. For more information, refer to “Managing Cloud App Security (SaaS Security) Licenses” in the Cloud App Security (SaaS Security) Administration Guide.
21 On the The SaaS Selection page, click **Start** on the tile for the G Suite application.

![Gmail and Google Drive tiles](image)

22 A confirmation message displays.

![Confirmation message](image)

Click **Close** to complete the activation process.

23 On the The SaaS Selection page, click **Next** in upper right area of the page.
24 Click **Start Now** to view the Cloud App Security Dashboard.

You're all set

Dear user,
You've started the following apps:

1. Google Drive
2. Office 365 Drive
3. Office 365 Emails
4. Office 365 SharePoint
5. Gmail

Please hold for a few minutes before the system is ready.
You'll receive an email saying onboarding finished successfully when your Office365/G Suite integration is ready.

In a few short minutes we will be setting up the service, connecting to your SAs and securing it with the security stack you have created. You can always add more cloud services and change the security stack from the app-store in the UI. For any questions, please contact support@sonicwall.com.

**NOTE:** If you have only activated one G Suite cloud application at this time, you will not need to reauthorize Cloud App Security again when you activate any additional G Suite cloud applications.

Using Cloud App Security with Google Cloud Directory Sync

If your organization uses Google Cloud Directory Sync (GCDS), you will need to perform additional configuration of your Exclusion Rules to work properly with SonicWall Cloud App Security.

**IMPORTANT:** You need to complete this configuration change *before* authorizing Cloud App Security for Gmail. Otherwise, the Google Groups will be deleted when Cloud App Security synchronizes with the Google Cloud after authorization.

Cloud App Security automatically creates and manages four Google Groups when you complete the authorization of the Gmail cloud application.

GCDS deletes the SonicWall groups when Cloud App Security synchronizes with the Google Cloud. By configuring the Exclusions Rules, the groups will not be deleted during synchronization.

**To configure the Exclusion Rules for Cloud App Security:**

1. Log into your Google Cloud management account.
2. Navigate to **Google Domain Configuration**.
3. Click on **Exclusion Rules**.
4. Click **Add Exclusion Rule**.
5. Create four new Exclusion Rules. Each new rule should contain:
   - **Type:** Group Email Address
   - **Match Type:** Exact Match

Cloud App Security (SaaS Security) and G Suite Integration Guide | 9
6 Assign one of these email addresses to each new Exclusion Rule:
   • sonicwall_inline_policy@yourdomain.com
   • sonicwall_inline_rule@yourdomain.com
   • sonicwall_monitor_policy@yourdomain.com
   • sonicwall_monitor_rule@yourdomain.com

7 Click OK.
8 Click Sync.

You can now authorize Gmail for Cloud App Security without the Google Groups getting deleted.

**Configuring G Suite for Cloud App Security**

*To configure G Suite for Cloud App Security:*

1 In Cloud App Security, navigate to the Configuration > Cloud App Store page.
2 Click Configure on the tile for Gmail or Google Drive.

3 Set the options you want for the G Suite applications.
4. Click Ok.

**Testing Your Integration**

If your G Suite applications are properly activated for Cloud App Security, you will see them listed on the Cloud App Security Dashboard as secured cloud applications.

![Cloud App Security Dashboard]

**For More Information**

For more information about configuring and using SonicWall Cloud App Security, refer to the *SonicWall Cloud App Security (SaaS Security) Administration Guide*. 