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

February 2020

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

Topics:

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*.

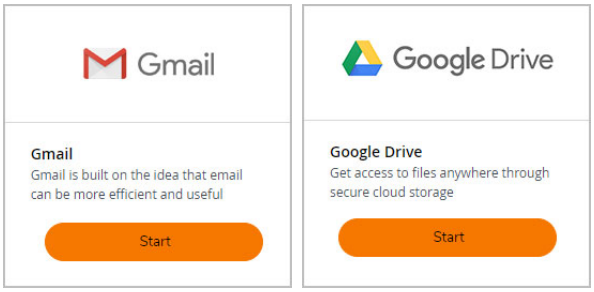
Activating G Suite for Cloud App Security

To activate G Suite for Cloud App Security:

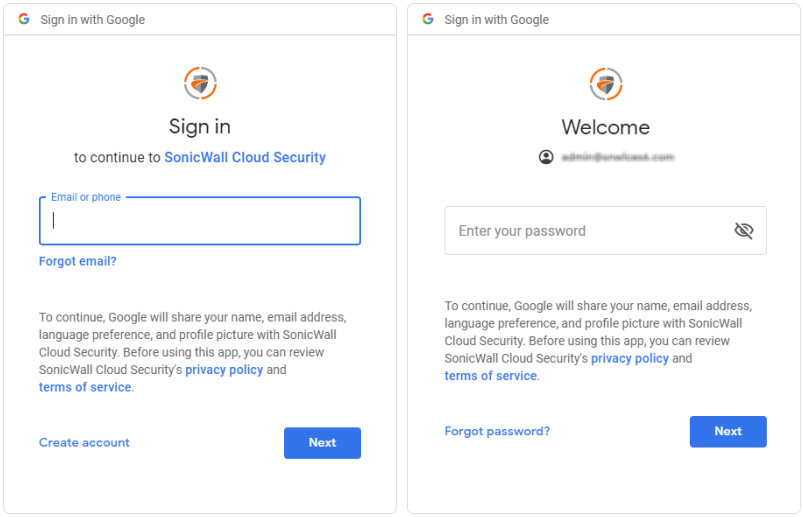
1 In Cloud App Security, navigate to either the:

- **SaaS Selection** page (during initial setup and configuration).
- **Cloud App Store** page.

2 Click **Start** on either the **Gmail** or **Google Drive** tile.



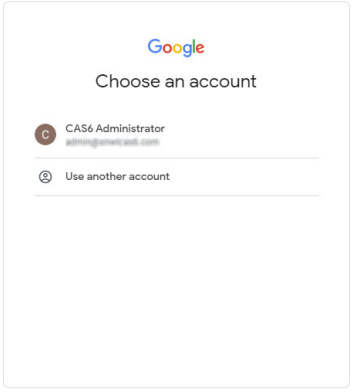
3 When prompted, log into your Google business account.



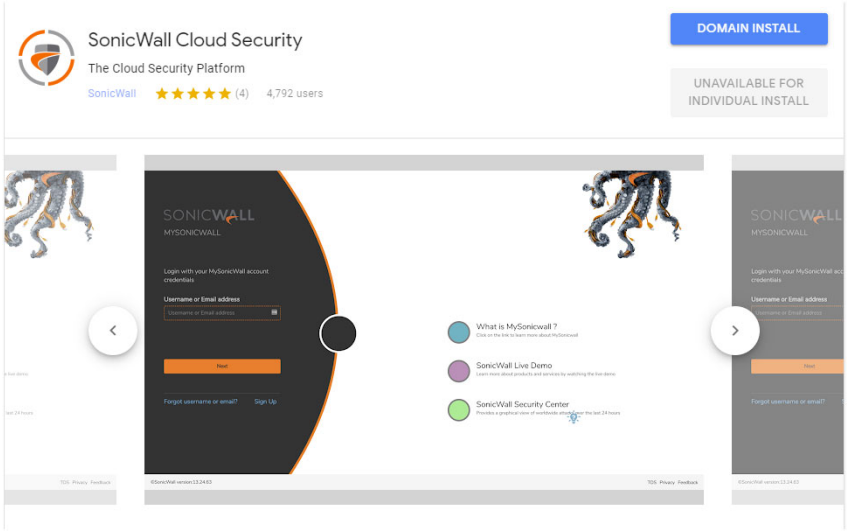
NOTE: Only G Suite Business and G Suite Enterprise accounts are supported by Cloud App Security.

4 Click **Next**.

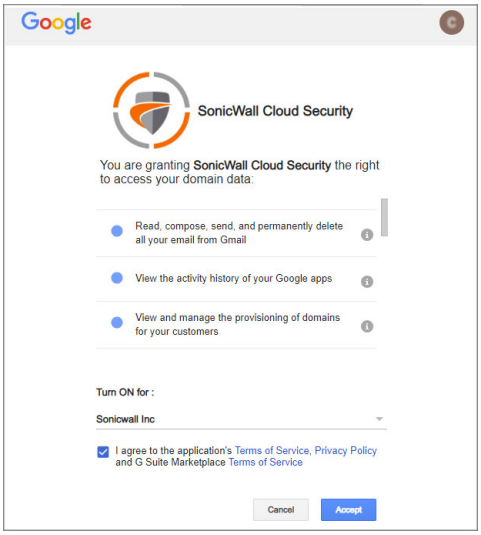
5 Select your Google account.



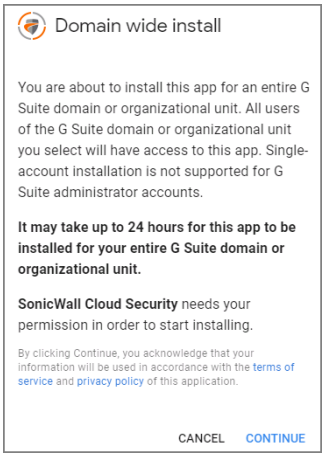
6 On the G Suite Marketplace, click the **Domain Install** button on the upper right of the page to install **SonicWall Cloud Security**.



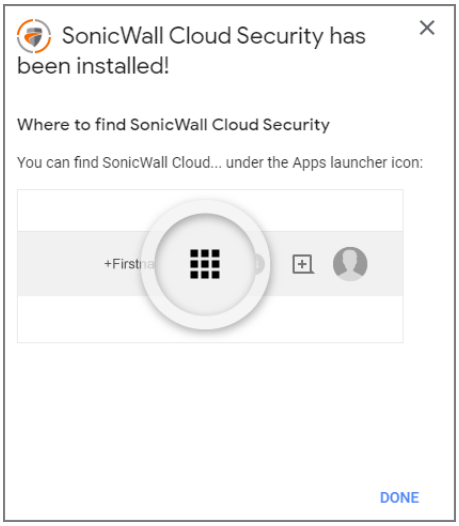
7 When prompted to grant access, click **Accept**.



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



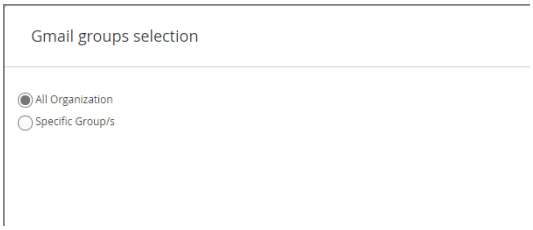
9 When the installation completes, a confirmation message displays.



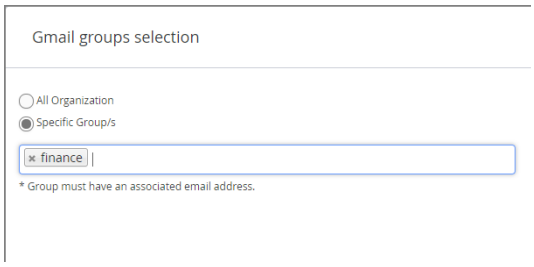
Click **Done** to continue.

10 Click **Start** on the tile for the G Suite cloud application you want to configure.

11 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 Group/s** 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 you Cloud App Security licenses for a specific subset of users within your organization.



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.

Refer to “Managing Cloud App Security (SaaS Security) Licenses” in the *Cloud App Security (SaaS Security) Administration Guide* for more information.

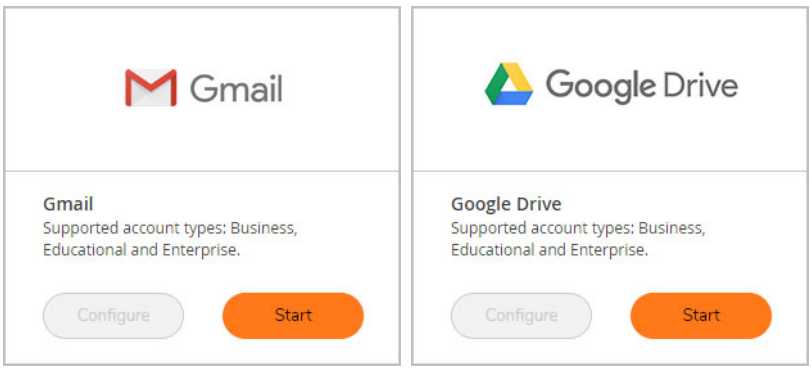
Enter the name of the G Suite group to which you want to assign the licenses.

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.

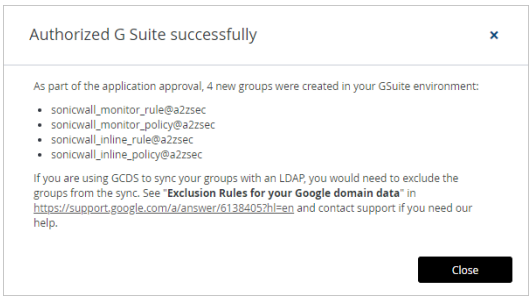
You can change this setting later, if you needed, on the **Configuration > Cloud App Store** page. Refer to "Managing Cloud App Security (SaaS Security) Licenses" in the *Cloud App Security (SaaS Security) Administration Guide* for more information.

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*.

12 On the The **SaaS Selection** page, click **Start** on the tile for the G Suite application.

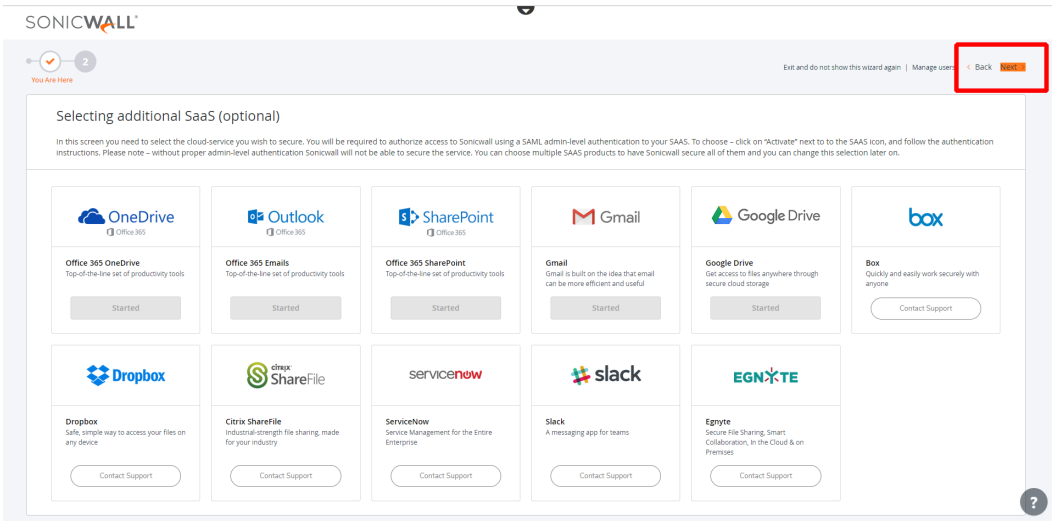


13 A confirmation message displays.

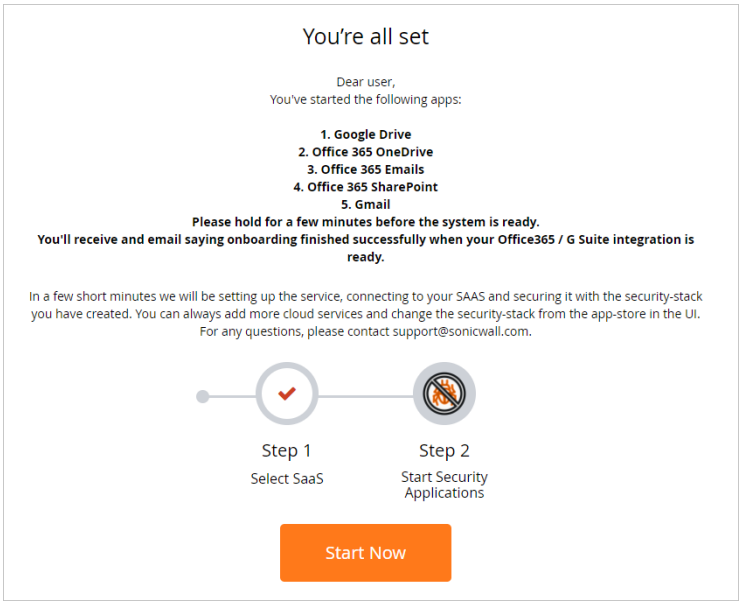


Click **Close** to complete the activation process.

14 On the The **SaaS Selection** page, click **Next** in upper right area of the page.



15 Click **Start Now** to view the Cloud App Security Dashboard.



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

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**.

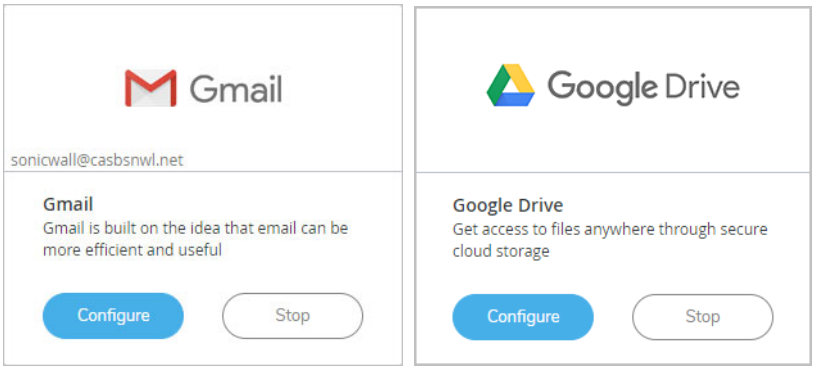
You can now authorize Gmail for Cloud App Security without the Google Groups getting deleted.

Configuring G Suite for Cloud App Security

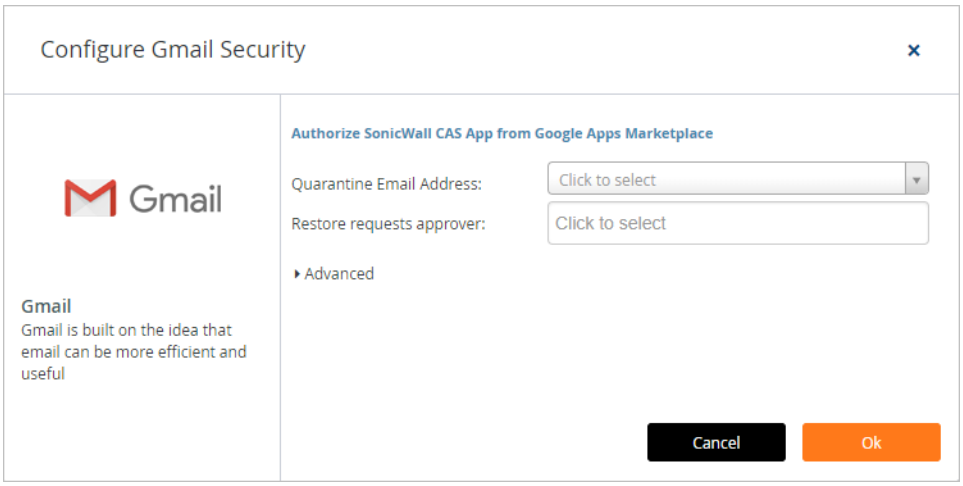
To configure G Suite for Cloud App Security:

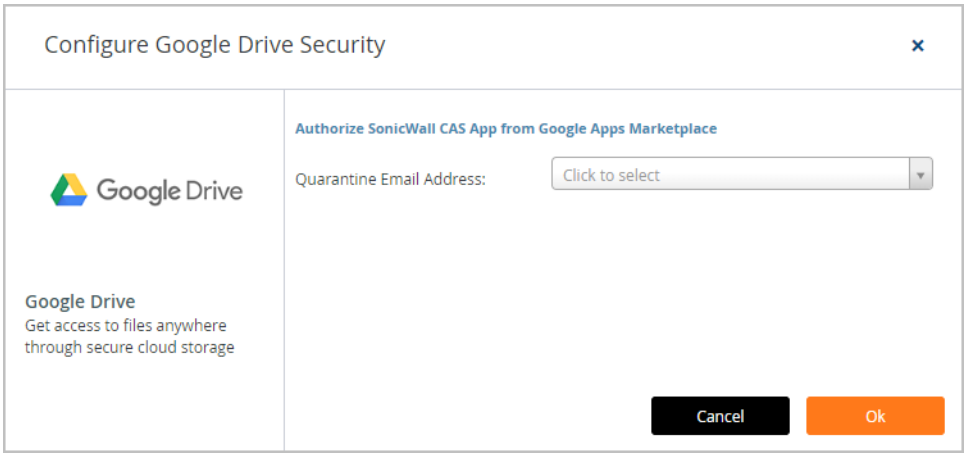
1 In Cloud App Security, navigate to the **Configuration > Cloud App Store** page.

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 Dasboard as secured cloud applications.

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*.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 1/31/20