Integration Guide: Cloud App Security (SaaS Security) and Citrix ShareFile

November 2020

This document describes how SonicWall Cloud App Security (SaaS Security) is integrated with Citrix ShareFile.

Topics:

- About Cloud App Security (SaaS Security)
- System Requirements
- Activating Citrix ShareFile for Cloud App Security
- Configuring Citrix ShareFile for Cloud App Security
- Testing Your Integration
- For More Information

About Cloud App Security

SonicWall 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 data protection capabilities—visibility, advanced threat protection, data loss prevention (DLP) and compliance. When deployed with SonicWall next-generation firewall, Cloud App Security (SaaS Security) offers shadow IT visibility and control for cloud usage on the network.

System Requirements

Cloud App Security (SaaS Security) can secure Citrix ShareFile with these subscription types:

- Citrix ShareFile Standard and above

Activating Citrix ShareFile for Cloud App Security

Citrix ShareFile offers file sharing and file collaboration tools that allow employees and outside collaborators to share files. SonicWallCloud App Security (SaaS Security) adds layers of security, privacy, and compliance not offered for Citrix ShareFile.

ⓘ **IMPORTANT:** Only Citrix ShareFile Standard subscriptions and above are supported by SonicWallCloud App Security (SaaS Security).

To activate Citrix ShareFile for Cloud App Security (SaaS Security):

ⓘ **IMPORTANT:** We highly recommend that you deactivate all folder and file download email notifications for all of your participating Citrix ShareFile users. This will prevent all of your users from receiving automatic email-notifications for every file that is scanned. You can find instructions for doing this here: https://support.citrix.com/article/CTX208286.

1. Navigate to either the:
    - **SaaS Selection** page (during initial setup and configuration).
    - **Cloud App Store** page.
2. Click **Start** on the **Citrix ShareFile** tile.

3. Sign into your Citrix ShareFile business account to authorize SonicWallCloud App Security (SaaS Security).
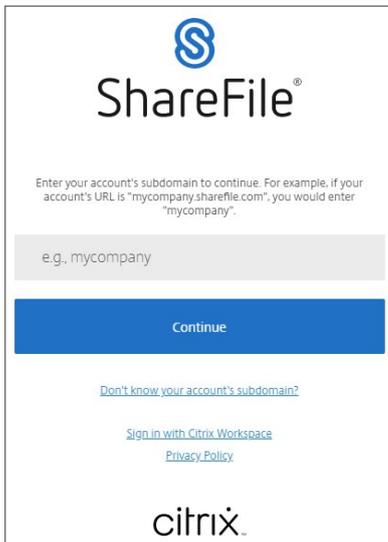
4. An informational warning displays, recommending that you deactivate all folder and file download email notifications for all of your participating Citrix ShareFile users.

    Click **OK** to complete the activation process.
5. On the **SaaS Selection** page, verify that a green checkbox appears on the tile for **Citrix ShareFile** indicating that the application has been activated for Cloud App Security (SaaS Security).

Configuring Citrix ShareFile for Cloud App Security

To configure Citrix ShareFile for Cloud App Security:

1. Navigate to the **Configuration > Cloud App Store** page.
2. Click **Configure** on the **Citrix ShareFile** tile.
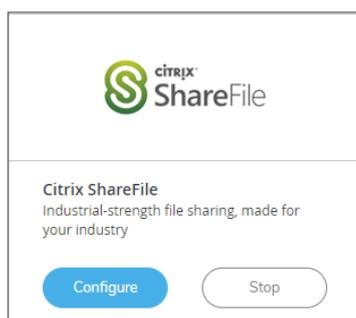
3. Set the options you want for the cloud application.
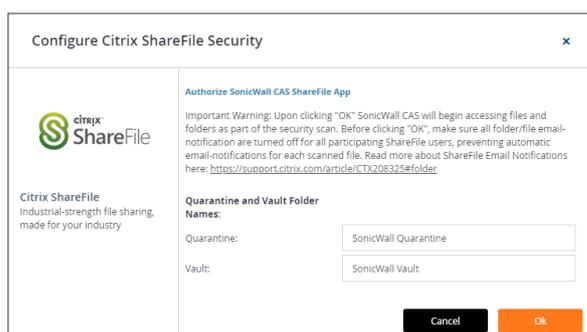
Most of the settings are related to specifying a quarantine email address and authorized administrators. See Managing Quarantine for Citrix ShareFile for more information on configuring these options.

You can also:

- Re-authorize Cloud App Security for the cloud application. (See Re-Authorizing Cloud Applications for more information.)
- Configure the Group filter for licensing Cloud App Security. (See Managing Cloud App Security (SaaS Security) Licenses for more information.)

4. Click **Ok**.

Testing Your Integration

If Citrix ShareFile is properly activated for Cloud App Security (SaaS Security), you will see it listed on the Cloud App Security Dasboard as a secured cloud application.

For More Information

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

About This Document

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

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

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

Cloud App Security (SaaS Security) Integration Guide for Citrix ShareFile
Updated - November 2020