

Integration Guide: Cloud App Security (SaaS Security) and Dropbox

June 2019

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

Topics:

- [About Cloud App Security \(SaaS Security\)](#)
- [System Requirements](#)
- [Activating Dropbox for Cloud App Security](#)
- [Configuring Dropbox 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)
- Dropbox Advanced or Dropbox Business account

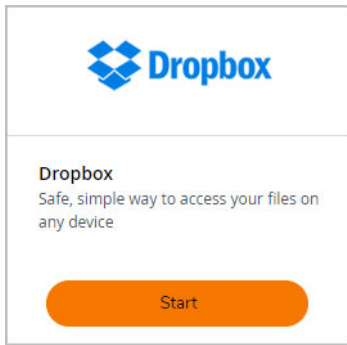
IMPORTANT: Only Dropbox Advanced and Dropbox Business accounts are supported by Cloud App Security.

Activating Dropbox for Cloud App Security

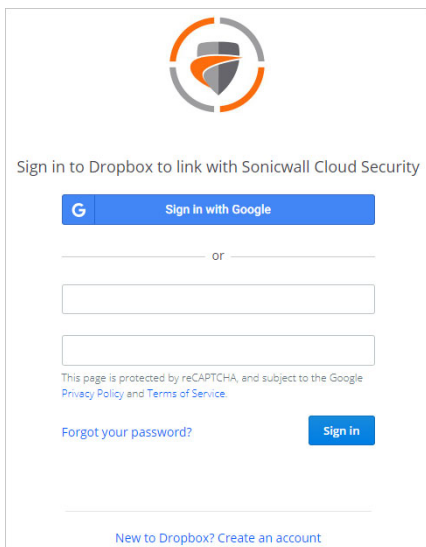
To activate Dropbox for Cloud App Security:

- 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 the **Dropbox** tile.



- 3 Sign into your Dropbox business account to authorize SonicWall Cloud App Security.

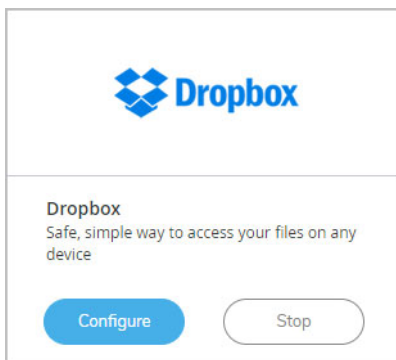


- 4 On the The **SaaS Selection** page, verify that a green checkbox appears on the tile for **Dropbox** indicating that the application has been activated for Cloud App Security.

Configuring Dropbox for Cloud App Security

To configure Dropbox for Cloud App Security:

- 1 In Cloud App Security, navigate to the **Configuration > Cloud App Store** page.
- 2 Click **Configure** on the tile for Dropbox.



- 3 Set the options you want for Dropbox.

Configure Dropbox Security

Authorize SonicWall CAS App from DropBox

Dropbox
Supported account types:
Standard, Advanced and
Enterprise.

Quarantine Options:

Create "SonicWall Quarantine" folder in the root directory

Quarantine to existing directory

Select Quarantine Path: x ▾

Select Quarantine User: x ▾

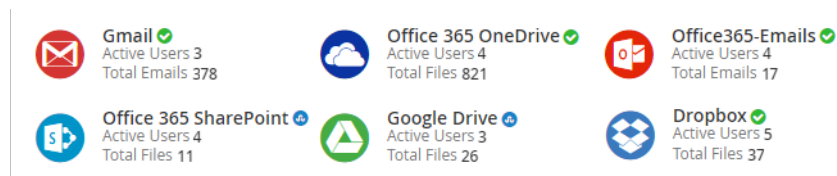
Vault folder name:

Cancel Ok

- 4 Click **Ok**.

Testing Your Integration

If Dropbox is properly activated for Cloud App Security, you will see it listed on the Cloud App Security Dashboard as a secured cloud application.



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*.

Copyright © 2019 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

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: 6/21/19