CloudLock

CloudLock®

Selective Encryption™

for Google Drive

1/8/16

CloudLock's products and services and related documentation are protected by contract law, intellectual property laws and international treaties, and are authorized for use only by CloudLock customers for internal purposes in accordance with the applicable subscription agreement or terms of service. This documentation may not be distributed to third parties.

CloudLock is registered trademark of CloudLock, Inc. Security Fabric and Selective Encryption are trademarks of CloudLock, Inc. All other trademarks or other third party brand or product names included herein are the trademarks or registered trademarks of their respective companies or organizations and are used only for identification or explanation.

This documentation is provided "as is" and all express or implied conditions, representations and warranties, including implied warranty of merchantability, fitness for a particular purpose or non-infringement are hereby disclaimed, except to the extent that such disclaimers are held to be legally invalid.

The information contained in this documentation is subject to change without notice. CloudLock recommends you periodically check https://cloudlock.force.com/community to ensure you are utilizing the most current version of this documentation.

Contents

Introduction

CloudLock Selective Encryption is an app that can be embedded in Google Drive. You use it to keep confidential and sensitive documents private and password-protected. Only someone who has the password can open a protected document. Keep your document passwords safe and you're keeping your information secure.

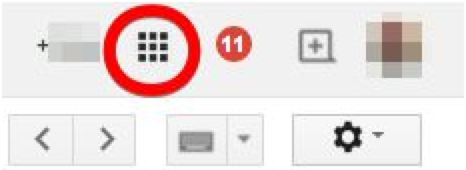
You use Selective Encryption from within Google Drive. It replaces your file with a private, encrypted version (you can also keep the original) and gives you a new "Secure Share" Secure Share button to use instead of the Google Drive Share button.

You can use Selective Encryption to share securely with anyone who has (or opens) a Google Drive account. If their organization doesn't use CloudLock, Selective Encryption Lite is available for free in the Google Marketplace.

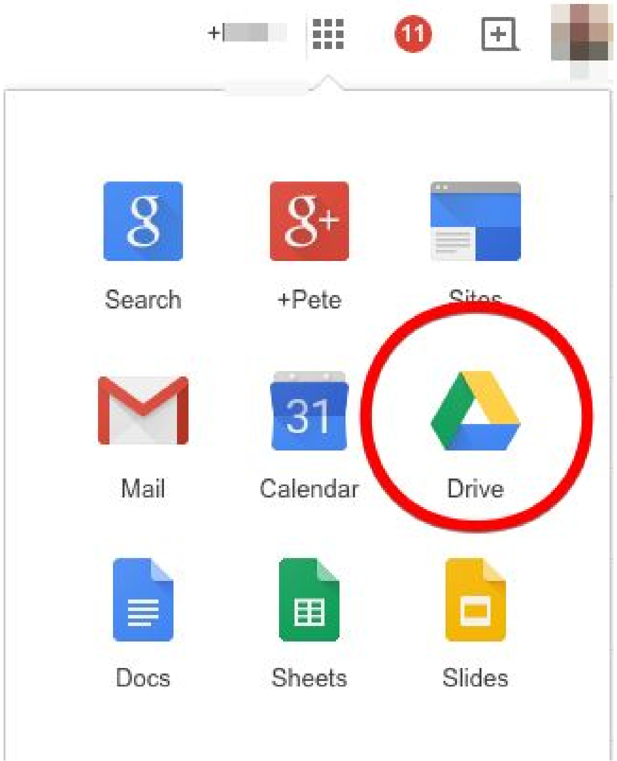
Protecting (encrypting) a file

To protect a file by encrypting it with CloudLock Selective Encryption, follow these steps:

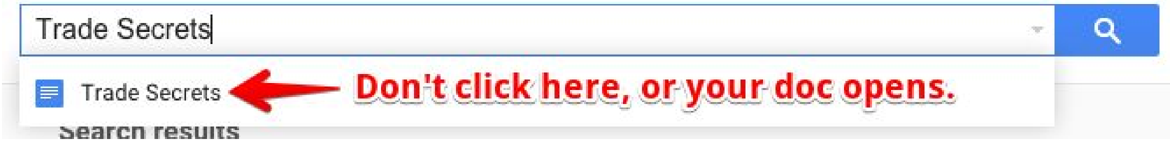
1. Open your Google Drive.
   An easy way to do this is to open Gmail, then click the Apps icon at the upper-right:



Then select the Drive icon from the Google Apps menu:

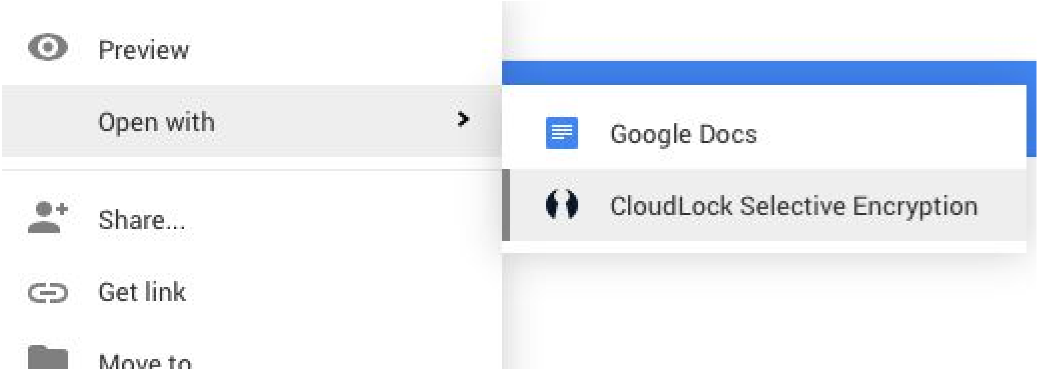


2. Next find a document you want to protect.
   To find a document in Drive, enter its name (e.g. "Trade Secrets") in the Search bar, then press Enter:



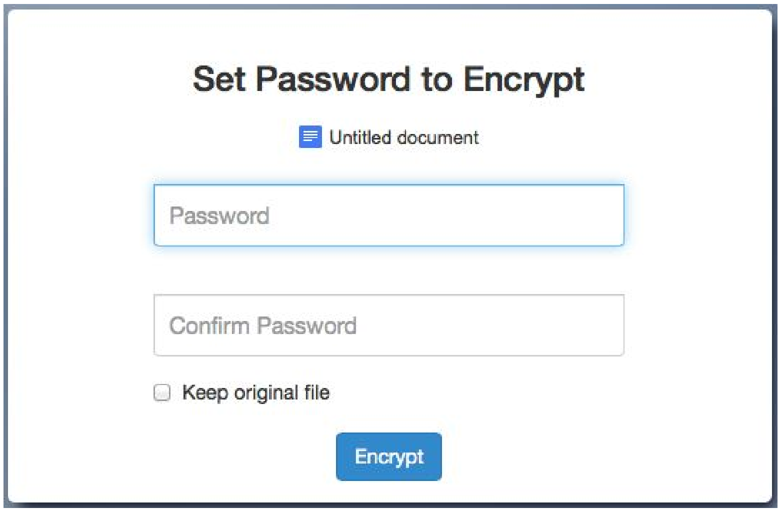
Don't click here, or your doc opens.

3. Right-click the icon for your document in the Google Drive list.
   In the menu that appears, select *Open with* > *CloudLock Selective Encryption*.

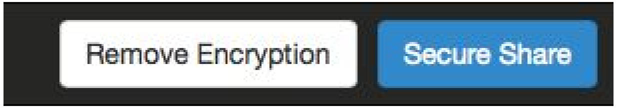


4. Enter a password to protect the document. Don't lose your password!

   Tip: Your password is stronger when it's longer and includes more different kinds of characters, such as numbers and symbols.



5. Select *Encrypt*.
   In a moment your document opens within a CloudLock frame, showing that it is now protected. Look for these new buttons in the upper-right:



Remove Encryption makes your document unprotected again.
Secure Share works just like the *Share* button (the *Share* button itself is disabled).

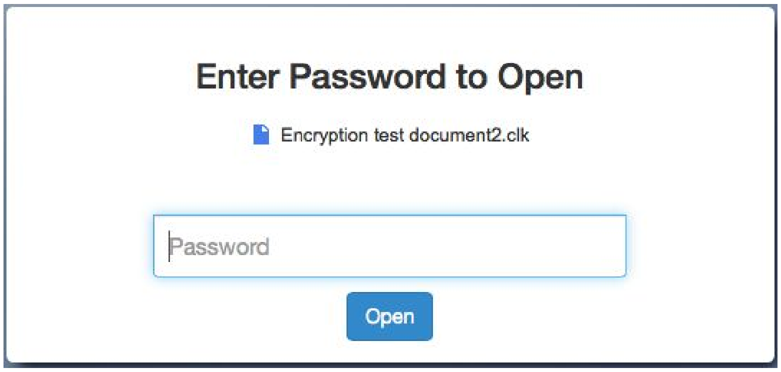
By the way: When you look at your Google Drive list, you will see the protected document. It will be in CloudLock's encrypted file format (.clk).

Opening a protected file

To open a file protected by CloudLock Selective Encryption, follow these steps:

1. Open the document from your Google Drive.

2. In the dialog box that appears, enter the password, then select *Open*.



Enter Password to Open

Encryption test document2.clk

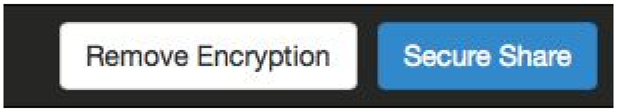
You can work with your document just as you normally do. When you close it, the document is automatically re-encrypted, including any changes you made.

Sharing a document securely

You can share and collaborate on documents while keeping them secure from anyone who doesn't have the password. You can also collaborate with users who don't yet use CloudLock Selective Encryption; Selective Encryption Lite is available without charge in the Google Marketplace.

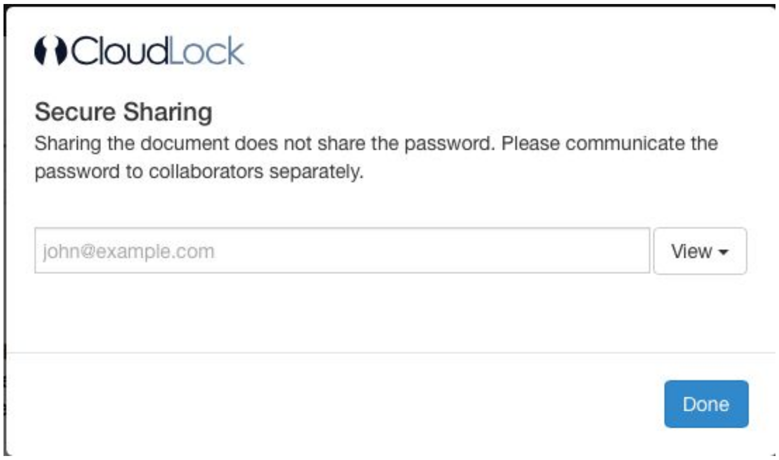
To share a document securely, open it from your Google Drive page, then follow these steps:

1. Click Secure Share in the upper-right corner of the page:



Tip: The black bar is the CloudLock frame. It serves as a reminder that this document is protected.

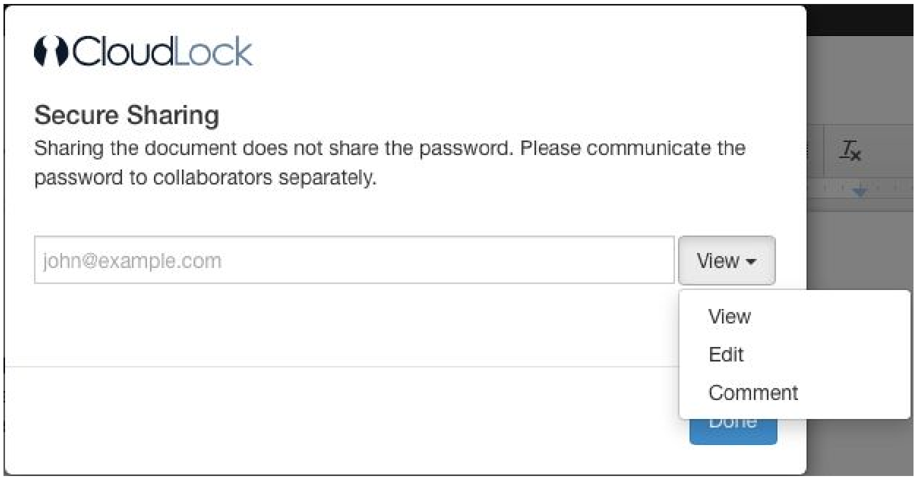
2. In the dialog box that appears, enter the email address(es) you want to share the document with:



Secure Sharing

Sharing the document does not share the password. Please communicate the password to collaborators separately.

3. Use the drop-down menu to select the level of permission you want to grant to the document. These are the same as in Google Drive sharing:



Secure Sharing

Sharing the document does not share the password. Please communicate the password to collaborators separately.

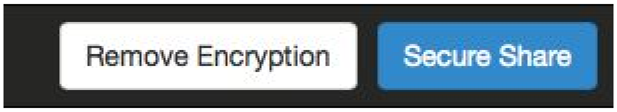
View means a user can read, download, and sync the document.
Comment means a user can *View* the document and suggest changes.
Edit means a user can *View* and *Comment*, and can also make changes.

4. Select *Done* to notify your collaborators.
Note: you must give them the password separately. Without the password they will not be able to access the document.

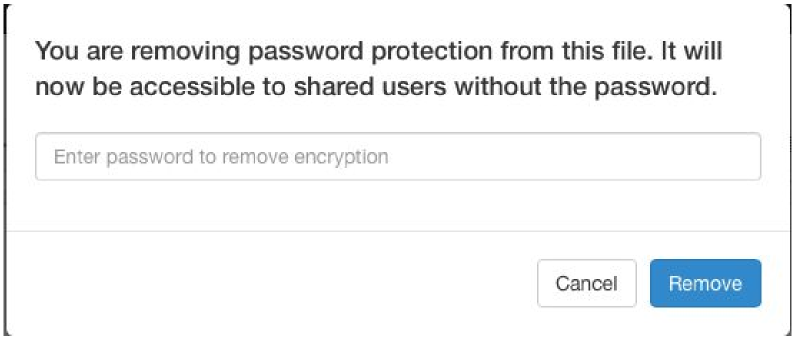
Removing encryption from a document

Only the owner of a document can remove its encryption. Before you do this, make sure the document does not contain confidential information or that you can protect it by other means.

1. To remove encryption from a document, open it and select Remove Encryption in the upper-right corner:



2. In the dialog box that appears, enter the document password, then select *Remove*:

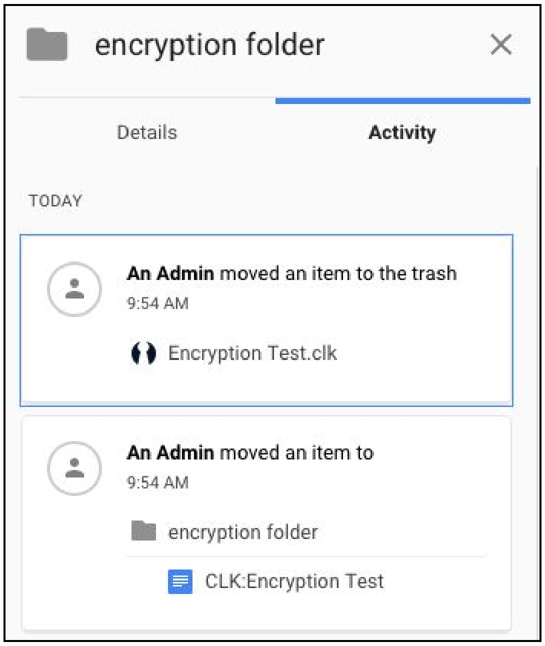


You are removing password protection from this file. It will now be accessible to shared users without the password.

The document is no longer protected.

Folder Activity Details

Selective Encryption places notifications in the Drive Folder Activity Details indicating that an administrator has moved and/or deleted items:



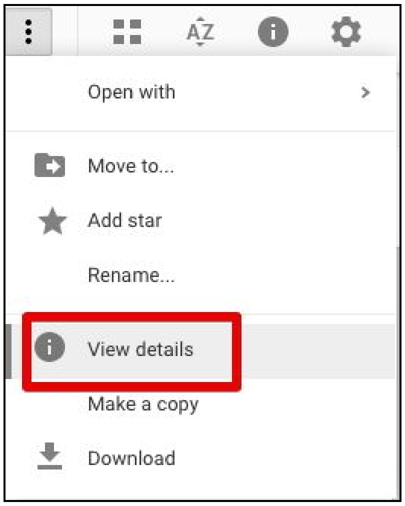
An Admin moved an item to the trash
9:54 AM
Encryption Test.clk

An Admin moved an item to
9:54 AM
encryption folder
CLK:Encryption Test

This is normal, and indicates standard actions taken by the CloudLock Selective Encryption application as files are encrypted, unencrypted, and have encryption removed.

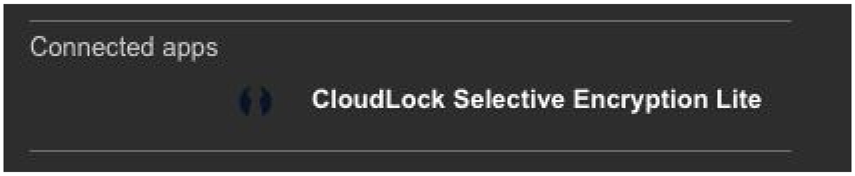
CloudLock has no control over the Google Activity Details view and so cannot provide more informative messages in this context.

Note: see the following illustration to access Details view in Drive:



Making CloudLock Selective Encryption a default app

The first time you open a protected document, you may see a message like this:

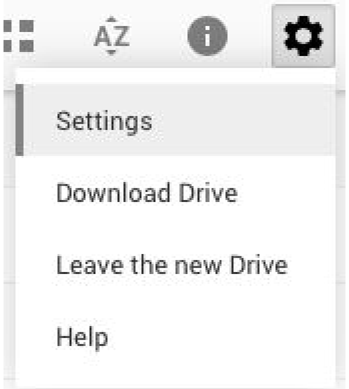


Connected apps

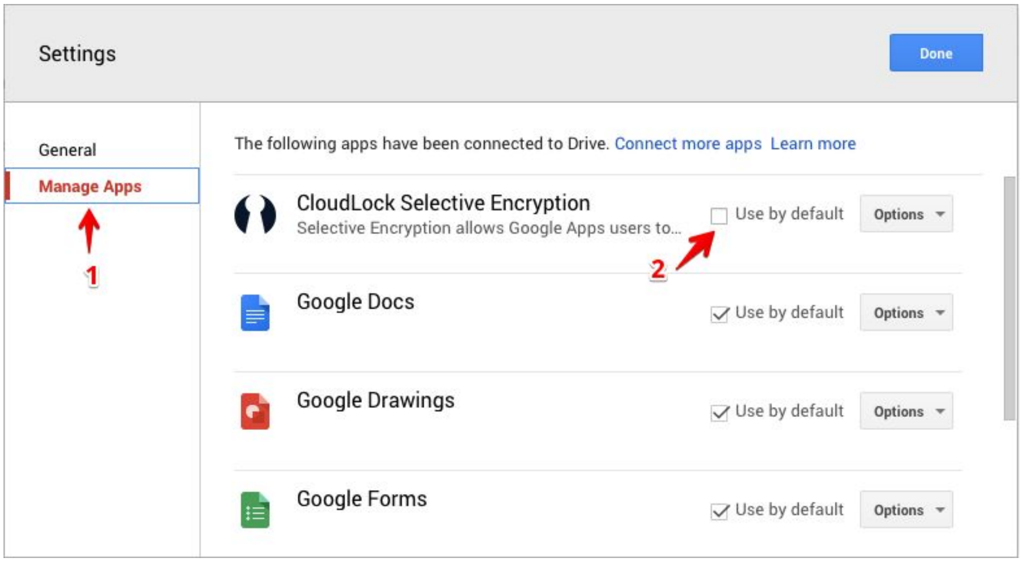
CloudLock Selective Encryption Lite

This means CloudLock Selective Encryption is not a default application in your Google Drive settings. To update your settings, follow these steps:

1. On your Google Drive page, select the gear icon, then choose Settings:



2. Choose *Manage Apps*, then select the checkbox next to CloudLock Selective Encryption:


Settings

The following apps have been connected to Drive. Connect more apps Learn more

CloudLock Selective Encryption
Selective Encryption allows Google Apps users to... □ Use by default

Google Docs ☑ Use by default

Google Drawings ☑ Use by default

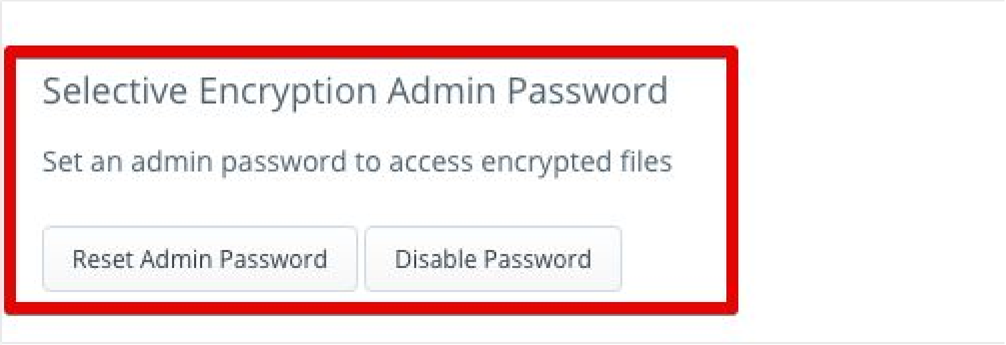
Google Forms ☑ Use by default

3. Select *Done.*
   Protected documents will now open directly from your Google Drive page.

Administering Selective Encryption

A CloudLock administrator can remove encryption from files encrypted in an organization’s domain. This ensures that the content of documents is not lost if a user loses the password to a file or leaves the organization.

In order to remove encryption as an administrator, set an administrative password in the Settings panel of the CloudLock Security Fabric.


Selective Encryption Admin Password

Set an admin password to access encrypted files

When the admin password is set, select any Selective Encryption file and click to enable the “Admin Access” checkbox. Enter the admin password to gain access to the file.

Limiting SE Use to a Group

Google Administrators can make SE (or any app) available for use by groups and OUs in a Google domain. However, while *use* can be restricted, *visibility* cannot. Thus users in the Google domain outside the group granted access will still see the SE app, but will not be able to use it. This is a characteristic common across all Google domains and apps.

When a user is removed from a group granted access, there may be a brief period (less than 1 hour) during which the removed user may still be able to access Selective Encryption. This is due to caching and is temporary.

CloudLock

CloudLock, Inc. 203 Crescent Street, Suite 105 Waltham, MA 02453

🌐 www.cloudlock.com ✉ support@cloudlock.com ☎ (781) 996-4332