SafeCrypt User Guide

DataLocker Inc.

June, 2019

SafeCrypt

Contents

About SafeCrypt

SafeCrypt is a software-based encryption platform that allows management of sensitive files in a native system interface.

On Windows, The Encrypted Virtual Drive is a drive letter. On macOS, it is a Storage Volume. Files saved to this Encrypted Virtual Drive are automatically encrypted using a FIPS 140-2 approved algorithm, then stored to the System Storage Location. This System Storage Location can be any storage device accessible from the computer, including local media, network shares, or even cloud gateways.

Up to three SafeCrypt installs can connect to the same System Storage, allowing access to the SafeCrypt Drive on different machines. The underlying encryption is done at the file level, which allows efficient network utilization when changes are made in the Encrypted Virtual Drive.

Note: A SafeConsole server is required to use this product. If your company does not have a SafeConsole server, please contact us at sales@datalocker.com.

Highlights

Simply Secure:

- A Cloud Encryption Gateway software platform where users are in control of their own encryption.
- Enter your password, then drag and drop files into the virtual drive letter.
- Safe from Ransomware attacks, as these attacks scan your local drive for popularly used file types, then encrypt them. Your sensitive files are already encrypted and cannot be identified.

Military Grade Encryption:

- Encryption engine is FIPS 140-2 certified using OpenSSL certificate #2768.
- All encryption is done locally so that even if a cloud server gets hacked, your data is safe.

Central Management:

- Inventory, audit, and control all your SafeCrypt Managed endpoints from a central console.
- Keep track of your users and their whereabouts.
- Audit the file activities of all your users.
- Control access to user files by remotely performing disable, kill, and password recovery actions.

Requirements

- SafeConsole Connection Token
- Compatible operating systems:
  - Windows 7 or 10
  - macOS 10.12 to 10.14
- 1GB of RAM
- 200MB of available hard-disk space
- Connection to SafeConsole Server

License

A SafeCrypt license is required for each Encrypted Virtual Drive that is created. One license allows the Encrypted Virtual Drive to be accessed by one user on 3 systems. An active SafeConsole server is required to use SafeCrypt. If your company does not already have SafeConsole, contact sales@datalocker.com to obtain more information regarding purchasing.

Getting Started

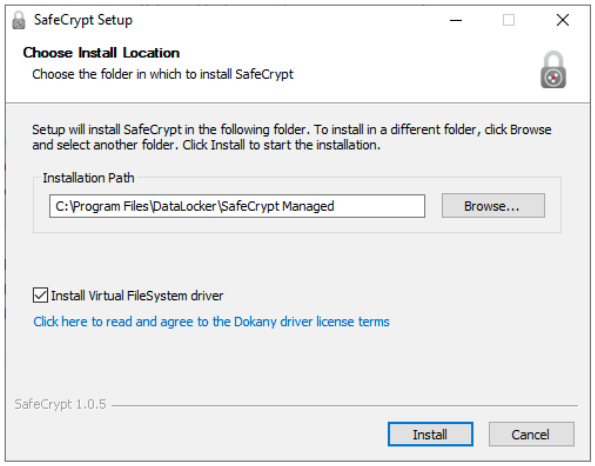
Downloading and Installing

The latest versions of SafeCrypt are always available here:

- Windows: https://media.datalocker.com/downloads/safecrypt/SafeCrypt-Setup-win64.exe
- macOS: https://media.datalocker.com/downloads/safecrypt/SafeCrypt-mac.dmg

Windows

To install SafeCrypt on a Windows computer, launch the **SafeCrypt-Setup-win64.exe**, follow the Installation Wizard, and select the Installation Path.



It is recommended that you install the Virtual FileSystem driver (checked by default) during installation. If this driver is not available, SafeCrypt Virtual Drives will not mount as native Windows filesystems, providing a slower experience and limited functionality accessing files with third-party applications.

macOS

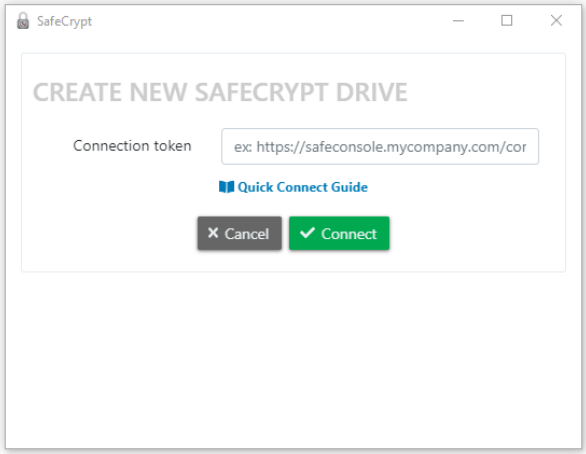
To install SafeCrypt on a macOS computer, launch the **SafeCrypt-mac.dmg** file. You can then drag the SafeCrypt icon to the Applications folder or double click the icon to run.

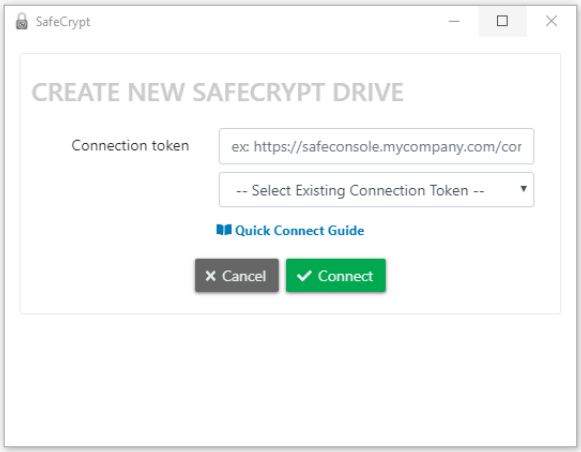
Creating An Encrypted Virtual Drive

The first time SafeCrypt is opened, it will ask for your email address and you'll have to agree to the license terms. Once entered, follow the steps outlined below to create an Encrypted Virtual Drive.

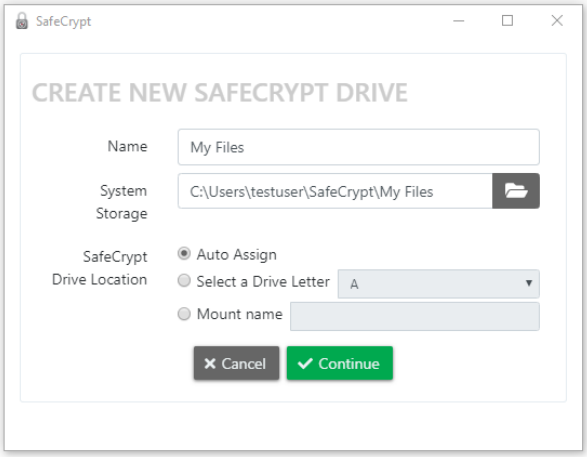
1. Click the **+** icon to begin a new drive creation.
2. Enter the **SafeConsole Connection Token** provided by your SafeConsole Administrator. Your Connection Token may have been sent to you in an email.

   Note: If a current SafeCrypt drive already exists, there will be two options: to select a previously used Connection Token or to enter a new one.





3. In the **Name** box, enter the name of your Encrypted Virtual Drive. This name will be used to identify your SafeCrypt drive. This name is also used as the volume name when the drive is unlocked.



4. In the **System Storage** section, choose where to store your Encrypted Files. Select the folder you want to use. By default, this will be a folder matching the **Name** entered above inside your users' profile folder. Example: *C:\Users\John\SafeCryptDrive*

   Warning: The folder you choose should be empty, as all files in it will be deleted upon the creation of your Encrypted Virtual Drive.

   Note: Files should never be stored directly in this folder outside of SafeCrypt. Files added to this folder outside of the SafeCrypt application will not be encrypted.

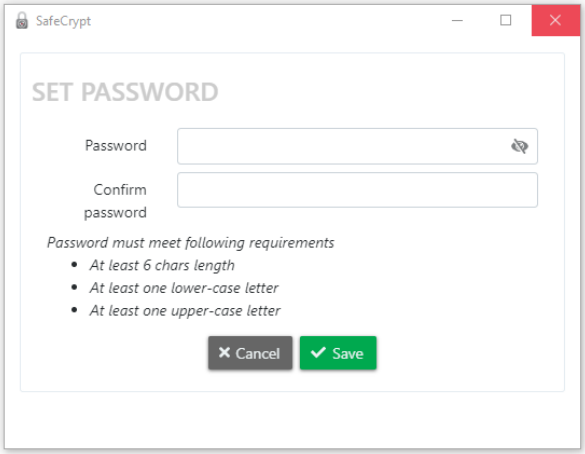
5. Choose your **SafeCrypt Drive Location** (Windows Only). There are three options for your SafeCrypt Drive Location:

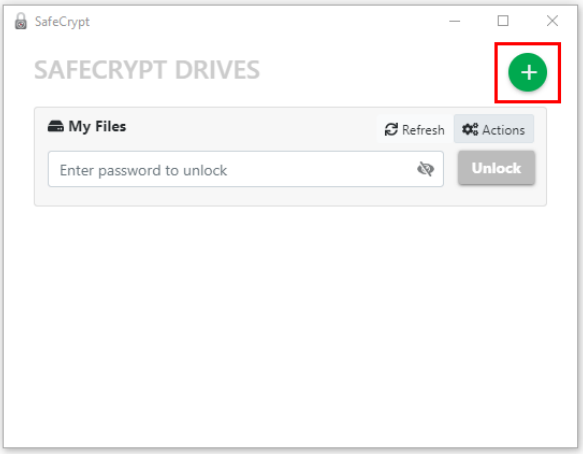
   - **Auto Assign:** the first free drive letter will be assigned to your Encrypted Virtual Drive *(Recommended)*
   - **Manually Select Drive Letter:** choose a specific drive letter for your Encrypted Virtual Drive from a list of available drive letters
   - **Mount Name:** If you are unable to mount as a drive letter, you can select *Mount Name*. The drive will behave like a network share drive. **Note:** This may cause limited compatibility with certain applications.

6. There are several settings that may have been optionally enabled by your SafeConsole Administrator. If they have been enabled, they will appear at this point the Encrypted Virtual Drive creation.

   - **User Unique Token:** Your SafeConsole Administrator may require you to enter a Unique Token to register your Encrypted Virtual Drive to SafeConsole. Your Administrator may provide this token to you in an email.
   - **Approval Pending:** Your SafeConsole Administrator may require that your Encrypted Virtual Drive be approved by them before registering to SafeConsole. Contact your Administrator to obtain approval. Once your Administrator has approved the drive, click the **activation pending** button.

7. **Create** and **Confirm** your password. The password requirements are set by the SafeConsole Administrator. Once your password meets the requirements, your drive will be created.





To create more Encrypted Virtual Drives, click the **+** in the upper right corner and follow the same steps.

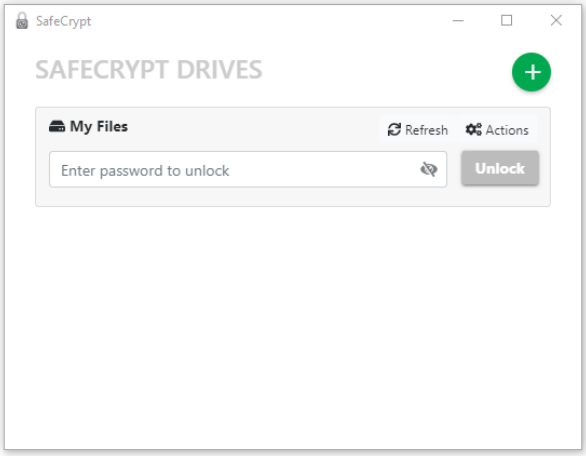
Accessing SafeCrypt Encrypted Files

A connection to SafeConsole is always required to unlock your SafeCrypt Drive.

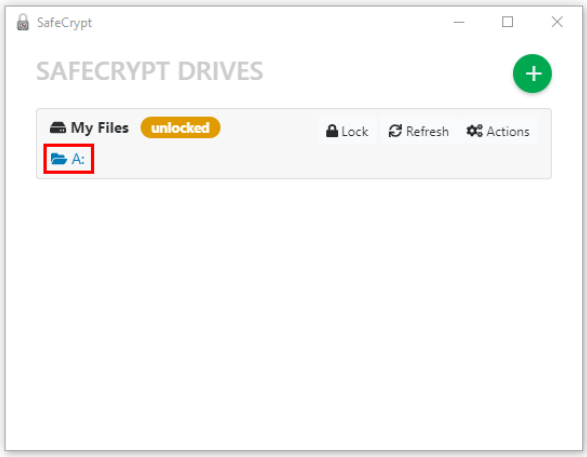
Note: If the drive is shown with **Deny Access** or **Disabled** you will not be able to unlock the drive until a SafeConsole Administrator restores the drive's status.

Unlocking Your SafeCrypt Drive

1. Open SafeCrypt. SafeCrypt should always be running in order to access your files.
2. Enter the password for the drive you would like to unlock. Once the password has been entered correctly, the drive will show *unlocked*.



3. Click the **Folder Icon** to open your files in your operating system file browser.

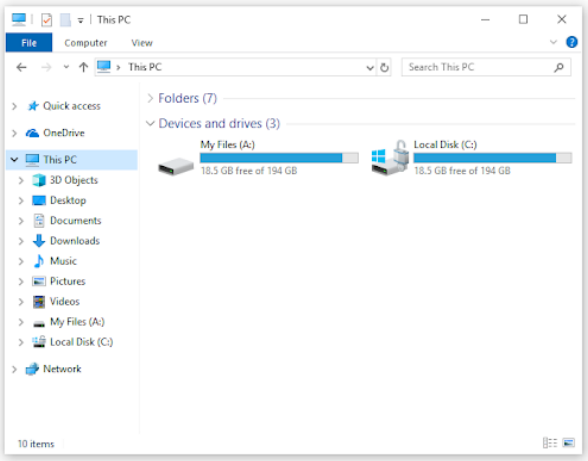


Applications will be able to interact with the Encrypted Virtual Drive much like a standard storage drive.

The SafeCrypt Drive can be locked at any time by clicking the **Lock** icon or by quitting SafeCrypt

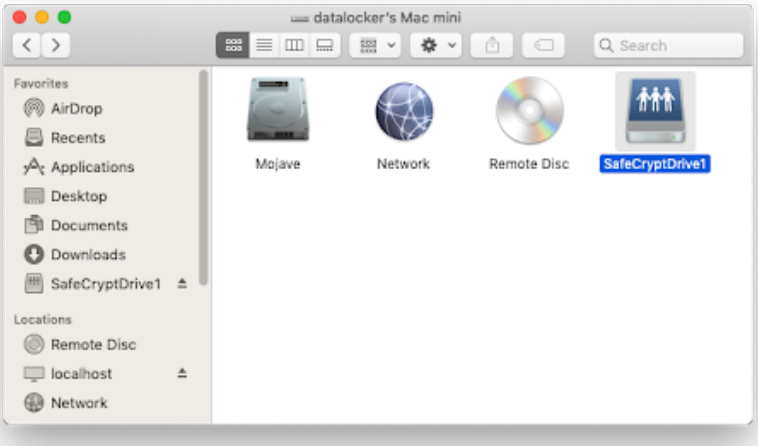
File Access on Windows

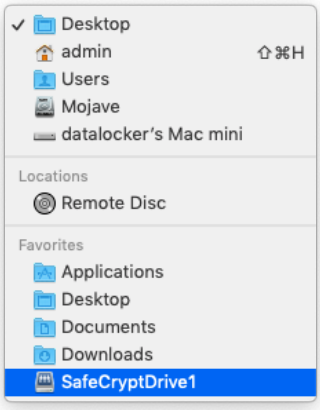
On Windows machines, the drive will show up as a Network Location and be assigned the first available drive letter or the specific drive letter as defined when the drive was created. To locate the drive letter assigned to SafeCrypt, open **Windows Explorer** and navigate to **Computer** on Windows 7 or **This PC** on Windows 10. Files can be transferred to this drive letter or saved directly with a program's **Save As** dialog box.



File Access on macOS

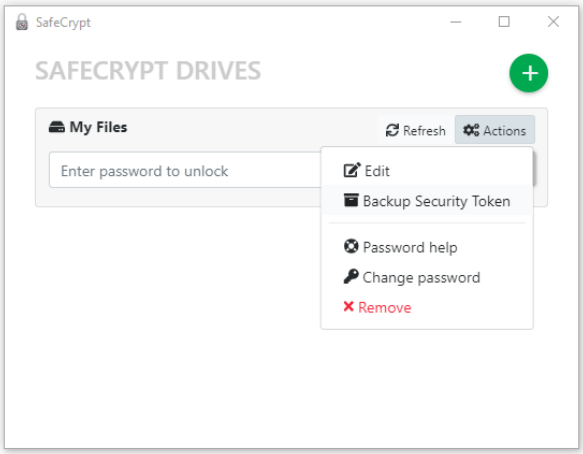
On macOS machines, the drive will show up as a volume connected to the localhost location. On the first drive unlock you will be prompted to allow SafeCrypt access to Finder. This will allow creating a *favorite* shortcut inside Finder for quick access to unlocked SafeCrypt Drives. This shortcut will only be available while the drive is unlocked. Look for your SafeCrypt Drive name in the favorite section inside Finder or an application's save dialog box to copy and save files to your SafeCrypt Drive.





SafeCrypt Actions

The options listed below are available while the SafeCrypt Drive is locked.



Edit Drive

The Name, System Storage, and SafeCrypt Drive Location can be modified from when the drive was originally created.

When changing the System Storage the files should be manually moved to the new location. SafeCrypt will not attempt to move the files for you.

Backup Security Token

A Backup of the Security Token allows the SafeCrypt drive to be imported, giving access to the encrypted files. This import can either be done on a new machine allowing concurrent access to the SafeCrypt Drive or on the same machine if needed in the future.

When selected, you will be prompted to pick a location to save the Security Token as an SCM file. This file should not be saved inside the SafeCrypt Volume, as it is needed to import the SafeCrypt drive and access its contents. This file should be kept safe.

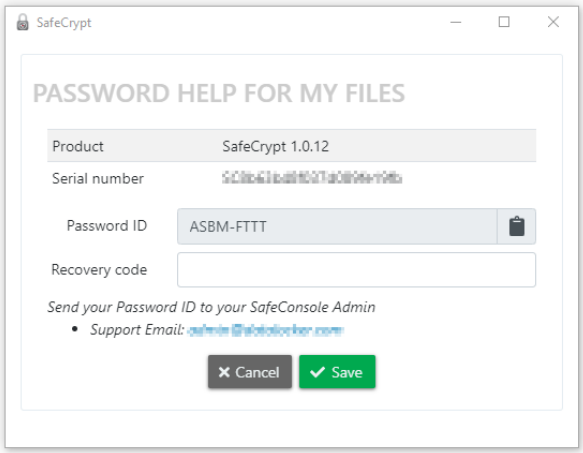
Note: The Security token does not need to backed up again after adding new files.

Along with the Security Token, a backup of the system storage should be made as well. This contains the encrypted contents of your files stored in your SafeCrypt Drive. The System Storage should be backed up after changes or additions to files in you SafeCrypt Drive.

Password Help

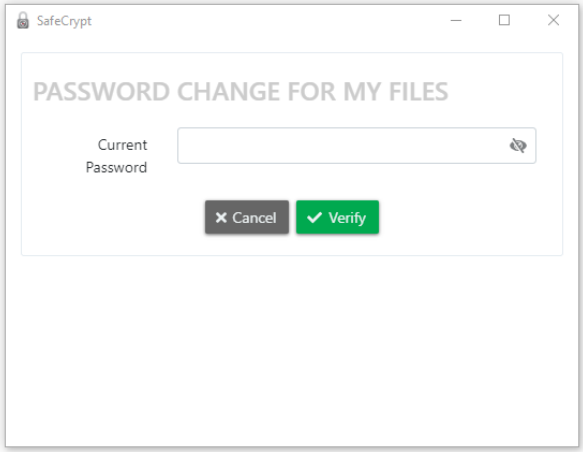
In the event that you are unable to remember a password to a SafeCrypt Drive, your SafeConsole Administrator can help you set a new password using **Password Help.** When selected, this will show the drive's serial number and the Password ID. This information should be given to your SafeConsole Administrator to perform a password reset. Clicking the support email link will prefill an email in your system's email client to your SafeConsole Administrator.

Enter the recovery code once received from your SafeConsole Administrator. If correct, you will be prompted to create a new password that fits the current password policy.



Change Password

If you know the current SafeCrypt Drive password you are able to change the password at any time. The new password will need to meet the current requirements in the password policy set by your SafeConsole Administrator.



Remove

Optional: This setting may be disabled by your SafeConsole Administrator. If this option is not available, please contact your SafeConsole Administrator to have the drive removed remotely.

Warning: This will remove all data stored in the SafeCrypt Drive and cannot be undone!

This action will remove the drive and its contents from your computer. It will also remove the drive from SafeConsole, freeing up a license seat. Once confirmed, the drive is gone and cannot be reimported even with a backup of the Security Token.

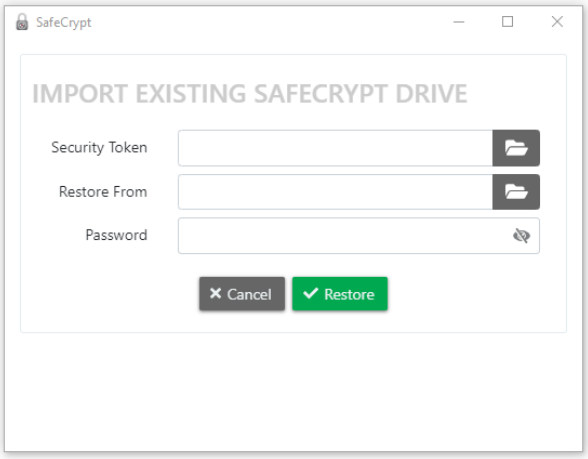
Importing A SafeCrypt Drive

SafeCrypt Drives can be imported from a backup if both the Security Token and the System Storage are available and the password is known. The SafeCrypt Drive also needs to be available on SafeConsole. If the SafeCrypt Drive is removed either from an action or during uninstall, the drive will not be able to be imported.

This process is the same for both importing the drive on a new computer or a second computer. A second computer will allow concurrent usage to the same SafeCrypt Drive.

To import a SafeCrypt Drive:

1. Install SafeCrypt on your machine. See Downloading And Installing for more information.
2. Import the System Storage to your computer. If the System Storage is linked with a cloud sync application, this can be as simple as reinstalling the cloud agent to the new computer.
3. Find the SafeCrypt icon in the System Tray and click **Import Drive**.



   Click the folder icon for the Security Token to navigate to the SCM backup file created by following the steps in the Backup Security Token section.

   SafeCrypt will automatically fill in the System Storage Location based on the previous computer settings. If this differs on the new computer, point the **Import From** to the new location.

4. Enter the password for the drive, then click **Import**. The Drive will now be added to your SafeCrypt list.

Note: SafeCrypt limits usage to 3 drives. Files should be closed from any open applications before attempting to access them on a different computer.

Settings

The user settings can be accessed by right-clicking on the system tray and clicking **Settings**.

Proxy

To use the proxy settings, enter the settings provided by your network administrator.

Enable Debug

Debug mode only needs to be enabled if DataLocker Technical Support requests you do so. You will need to restart SafeCrypt to fully enable this setting.

The debug log can be found by right clicking on the **SafeCrypt** icon in the System Tray, clicking **About**, then clicking **Show Log File**. The logs created can be emailed to support@datalocker.com in the event of issues with your SafeCrypt installation.

Updates

SafeCrypt updates automatically on both Windows and macOS systems. Every time SafeCrypt is started, the application will check for any new updates. If there is a new version available, you will be prompted to update SafeCrypt. You will be able to view the new Release Notes in your web browser before installing.

To manually check for updates, right click on the SafeCrypt icon in the System Tray, click **About**, then clicking **Check for Updates**.

Uninstalling

To uninstall SafeCrypt from your computer use the uninstall method for your operating system:

- **Windows:** Navigate to **Add/Remove Programs** and find SafeCrypt.
- **macOS:** Drag SafeCrypt from the Applications list to **Trash**.

Uninstall Options

These options are only available on Windows.

Clear All SafeCrypt Settings

This option removes all local SafeCrypt settings. It does not remove the actual data files in the System Storage Location. Your drive can be imported again if the Security Token was backed up prior to clearing the settings.

Unregister SafeCrypt Drives

Unregistering the SafeCrypt application attempts to remove the drives on the remote SafeConsole Server and free up a license seat. If successful, the drive will not be able to be imported even if a backup of the Security Token is available.

Where Can I Get Help?

If you have any unresolved issues with our software after referring to this manual, email us or refer to the following places for more information:

- support.datalocker.com: Information, knowledgebase articles, and video tutorials
- support@datalocker.com: Feedback and feature requests
- datalocker.com: General information
- datalocker.com/warranty: Warranty information

You can also right click on the SafeCrypt icon in the System Tray and then click **Help**.

By turning on *Debug Mode* before contacting support and following the steps in the Debug Mode section, you can reduce the time needed for our Technical Support team to assist you.

NOTE: DataLocker is not liable for technical or editorial errors and/or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing or use of this material. The information provided herein is subject to change without notice. The information contained in this document represents the current view of DataLocker on the issue discussed as of the date of publication. DataLocker cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. DataLocker makes no warranties, expressed or implied, in this document. DataLocker, and the DataLocker logo are trademarks of DataLocker Inc. and its subsidiaries. All other trademarks are the property of their respective owners. All rights reserved.