SECUREGUARD USB

Through Remote Management Console

ADMIN GUIDE

SecureGuard USB
Through RM Console
Admin Guide

SECURE DATA

TABLE OF CONTENTS

SECUREGUARD USB THROUGH RM CONSOLE

SecureGuard USB through Remote Management Console (hereafter “RM”) is a Data Loss Prevention (hereafter “DLP”) service that is managed through the SecureData Remote Management Console/Services. It blocks unauthorized USB devices from accessing sensitive files by limiting computer access to whitelisted USB devices and allows individually blacklisting and whitelisting specific devices. RM provides IT Managers (hereafter “Admin”) control of computers and their allowed drives throughout an organization.

When authorized devices are inserted into a USB port, a user may have access to the computer and both upload and download data to the device. When unauthorized devices are inserted into a USB port, the SecureGuard program locks the computer and blocks the user from further access until the device is removed, preventing uploading and downloading files as well as preventing potential viruses and malware from entering the computer. It safeguards sensitive information by whitelisting and blacklisting USB devices for computers with the program installed, including: an external hard drive, flash drive, mouse, keyboard, phone, tablet, card reader, camera, and other devices.

Remote Management (RM) allows Admin to manage SecureGuard USB through the internet from a remote computer. It is a user-friendly interface that allows remote control and management of the program on all computers with SecureGuard USB installed on them. Once installed, SecureGuard client will not require the internet to function.

Glossary

Admin IT:	Manager, Admin, or corporate manager
HID:	Human Interface Devices
The License:	SecureGuard USB License
PID:	Product ID
RM:	Remote Management Console
SN:	Serial number
VID:	Vendor ID
REV:	Revision

Requirements

Windows 7 SP3 or later
MacOS 10.6 or later
Internet Access (for initial install and to apply any changes to a configuration)

SECTION 1: INSTALLATION AND CONFIGURATION

This section describes how an Admin enrolls and logs into the Remote Management application. The process outlined below is how one becomes a Super Admin.

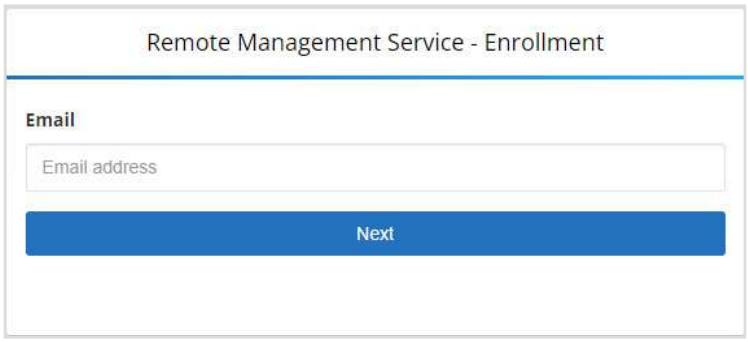
Enrolling

To enroll in Remote Management services, follow these steps:

1. Once an annual license is purchased, click on the enrollment link: **https://rm.securedata.com/Account/Register**

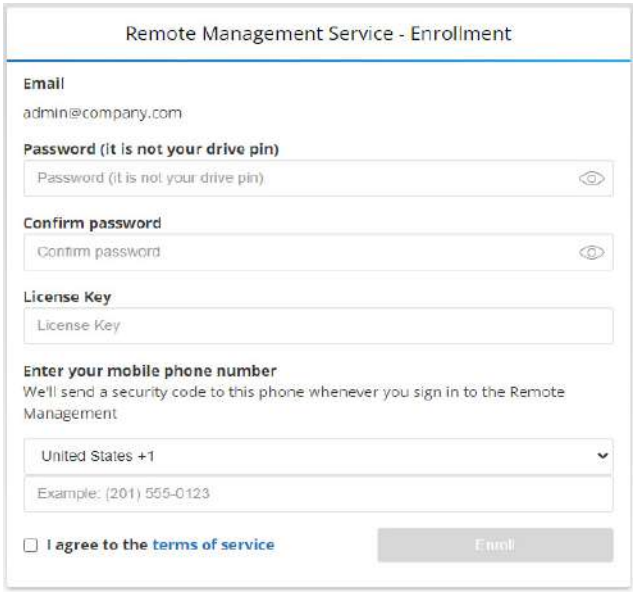
NOTE: This enrollment link and the License Key are provided to Admin via email upon the purchase of an annual subscription. If you did not receive an email, contact SecureData Customer Service.

2. Enter the email address



NOTE: If Single Sign On (SSO) is used, you will only need the license key to complete the enrollment form. You can skip steps 5 through 7.

3. Complete the enrollment form as follows:



- **Password** — Create a password.

NOTE: This password is required to be between 7 and 15 characters long and will be used throughout the process. This password is not the same as a drive PIN; users will create their own drive PIN.

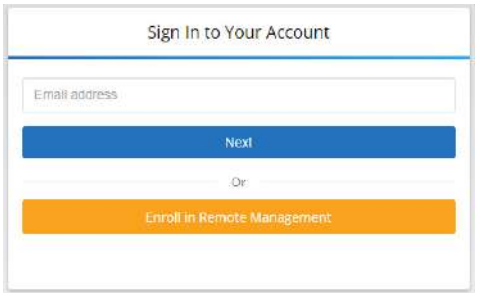
- **Confirm Password** — Re-enter the password.
- **License Key** — Enter the license key provided to you in the enrollment email.
- **Mobile Number** — Enter a mobile phone number to receive a security code for the two-step verification.

4. Check "I agree to the terms of service" and click **Enroll**.
5. On the **Enable Two-Step Verification** page, enter the 6-digit security code in the field.
6. Click **Next**.
7. On the verification page, click **Done**.

Logging In

Logging in as outlined below applies to both Super and Regular Admins. To log into Remote Management, follow these steps:

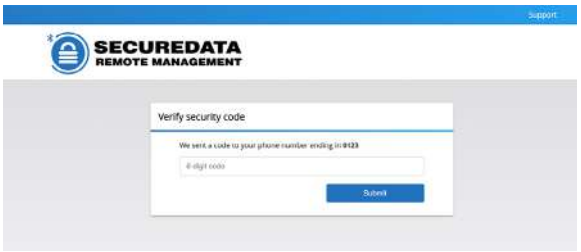
1. Go to https://rm.securedata.com/Account/Login



2. In the **Email Address** field, enter the email used previously in the enrollment process and click "**Next**".

NOTE: If Single Sign On (SSO) is used, you will be redirected to the Identity Provider.
You can skip steps 3 through 5.

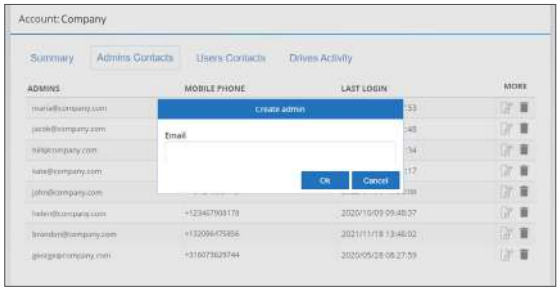
3. In the Password field, enter the password used in the enrollment process and click **Log In**
4. On the **Verify security code** page, enter the 6-digit security code in the field.



NOTE: This security code is sent to the Admin mobile phone number used in the enrollment process.

5. Click **Submit**.

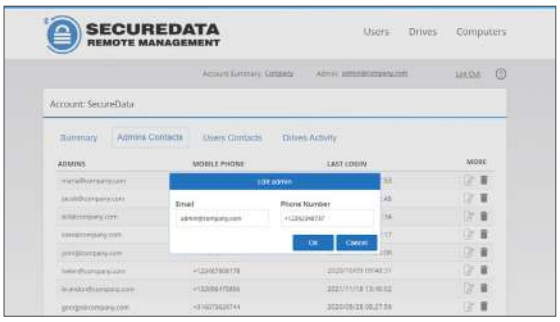
Creating New Admin



To add a new Admin, follow these steps:

1. Next to **Account Summary**, click the account name.
2. Go to the **Admins Contacts** view.
3. In the lower right corner, click **Create**.
4. Enter the new Regular Admin's email address and click **OK**.

Editing Admins



To edit Admins, follow these steps:

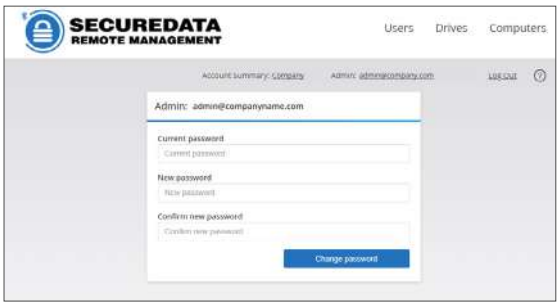
1. Next to **Account Summary**, click the account name.
2. Locate the record you want to modify under **Admins Contacts**.
3. To edit the email address or mobile number, click the paper icon.
4. To delete an Admin, click the trash can icon.

Changing the Admin Password

To change the Admin password, follow these steps:

1. Next to **Admin**, click the Admin's email address.

NOTE: Hovering the cursor over the email address displays the word "Manage."



2. In the **Current Password** field, enter the current password.
3. In the **New Password** and **Confirm New Password** fields, enter a new password.
4. Click **Change Password**.

To access the Admin guide, click the question mark icon.

To log out of the system, click **Log Out**.

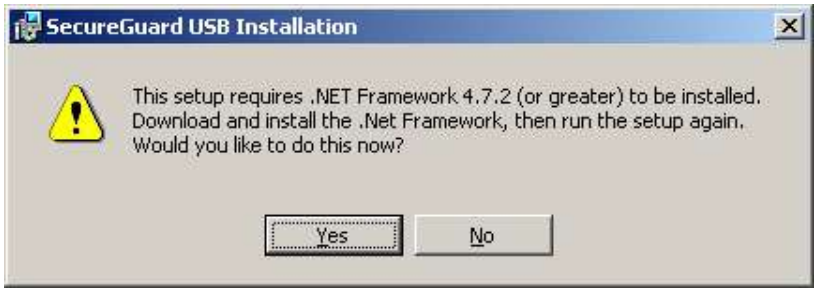
SECTION 2: WINDOWS INSTALLATION

1. After purchase, a downloadable installation pack will be sent to the email provided.
2. Open link and download file when prompted.
3. Program may be installed on a specific computer through any distribution seen fit, such as external drive or in an Active Directory environment.

NOTE: If moving the program to a USB device for installation on additional computers, copy the installation file from the device to the desktop, then remove the device and install the program directly from the desktop. During installation, the program will recognize the unauthorized device, stop the installation and prevent further action.

4. Open the launcher and click Next.

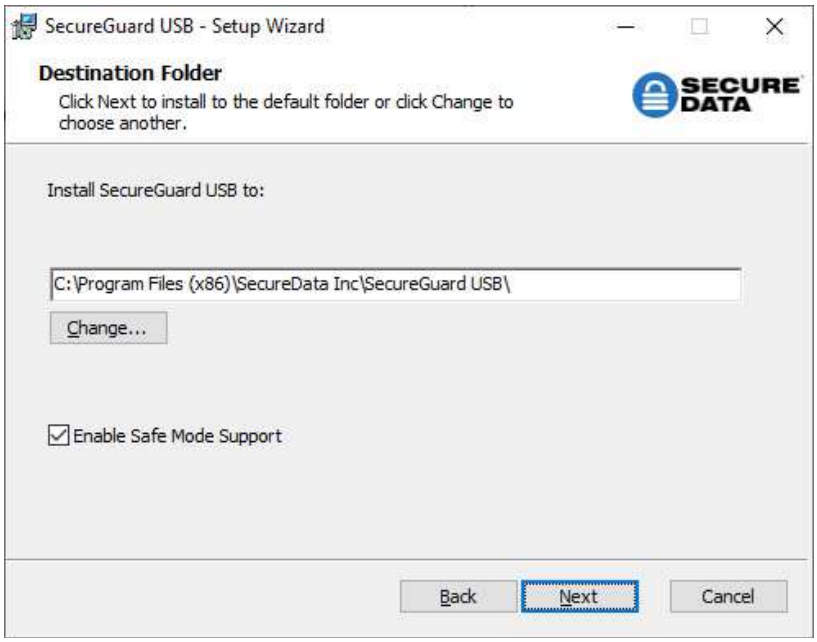
5. When the SecureGuard USB Installation prompt appears click Next to start the Setup Wizard.



NOTE: SecureGuard USB will check the .NET Framework version installed. If it is a lower version, a warning window will appear. Click **Yes** to open an internet browser to download and install .NET. This will terminate installation of SecureGuard. Once .NET Framework has been updated, begin installation again. Clicking **No** will terminate SecureGuard installation.

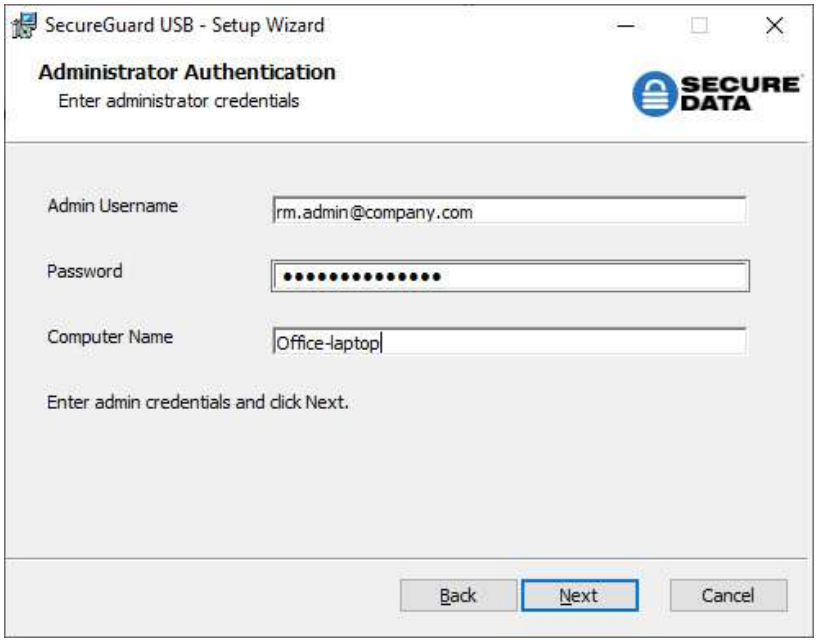
6. Read the End-User License Agreement. Check the box in the lower left to accept the terms, then click **Next**.

7. Choose the **Destination Folder** provided or manually enter a new path. Click **Next** to continue.



NOTE: We recommend leaving the Enable Safe Mode Support box checked. When a computer with SecureGuard installed on it is started in Safe Mode, the program continues to keep ports blocked.

8. At the Administrator Authentication prompt, enter the email and password used when creating the administrator account, and choose a Computer Name for this individual computer. Click **Next** to continue.



NOTE: This Computer Name will appear in the Remote Management Console, discussed in Section 4: Computer Management. This makes the target computer identifiable when managed remotely.

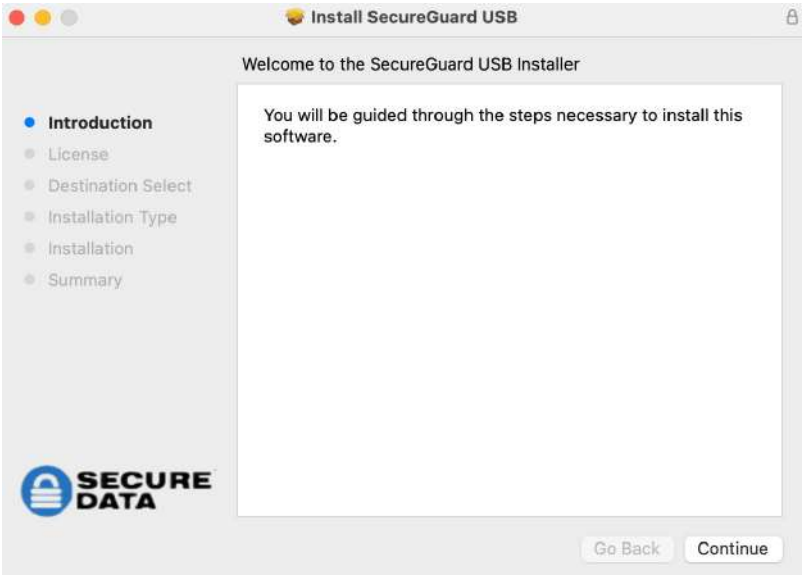
9. Click **Finish** to complete the setup.

SECTION 3: MAC INSTALLATION

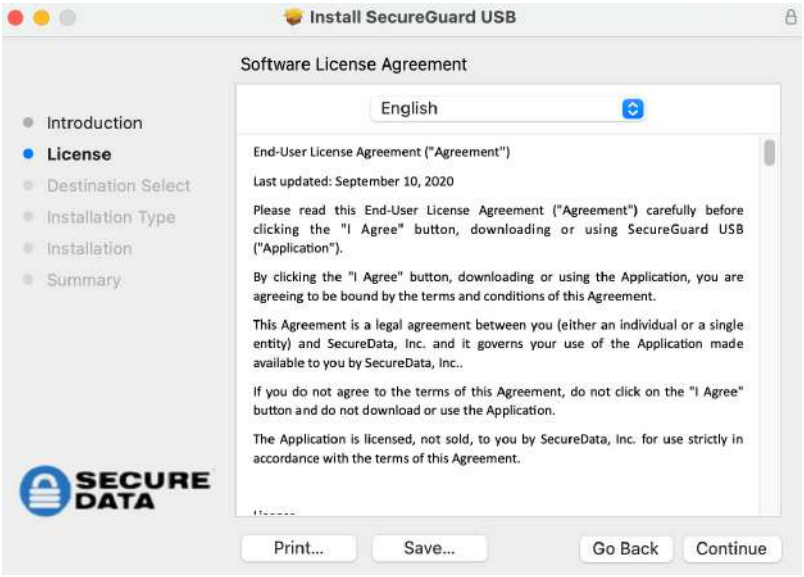
1. After purchase, a downloadable installation pack will be sent to the email provided
2. Open link and download file when prompted.
3. Program may be installed on a specific computer through any distribution seen fit, such as external drive or in an Active Directory environment.

NOTE: If moving the program to a USB device for installation on additional computers, copy the installation file from the device to the desktop, then remove the device and install the program directly from the desktop. During installation, the program will recognize the unauthorized device, stop the installation and prevent further action.

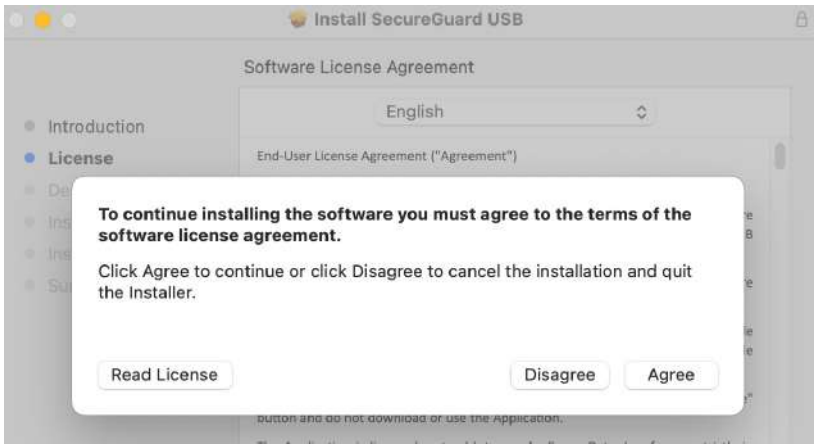
4. Open the Installer and click **Continue**.



5. Read the Software License Agreement and click **Continue**.

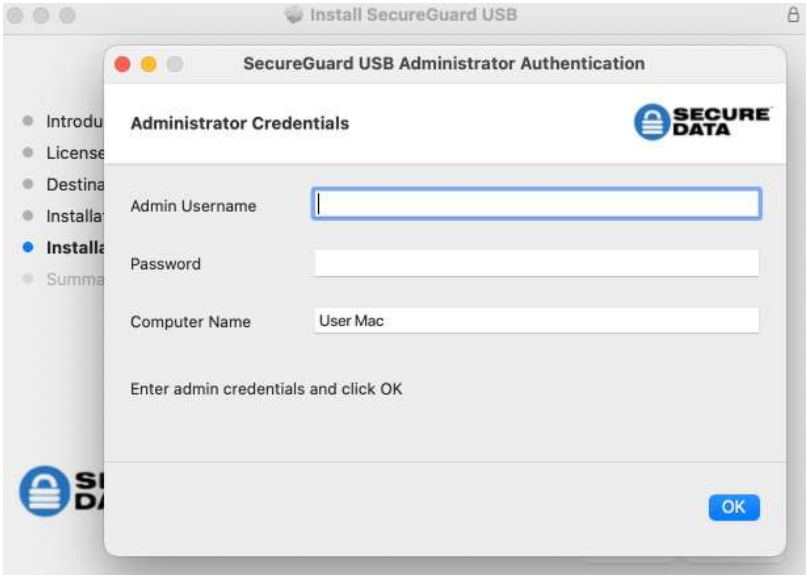


6. At the prompt, click **Agree** to proceed with installation.
7. Choose the **Install Location** provided or manually enter a new path. Click **Install** to continue.

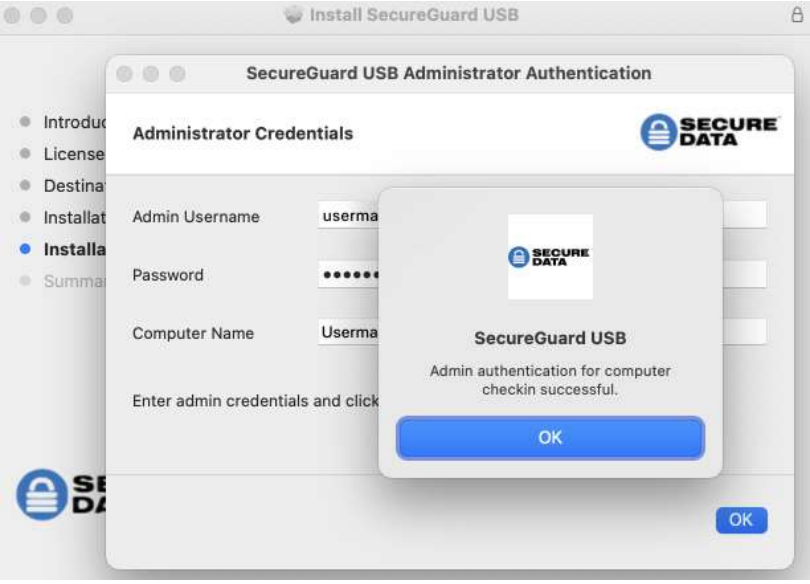


8. Enter your **User Name** and **Password**. Then click Install Software.

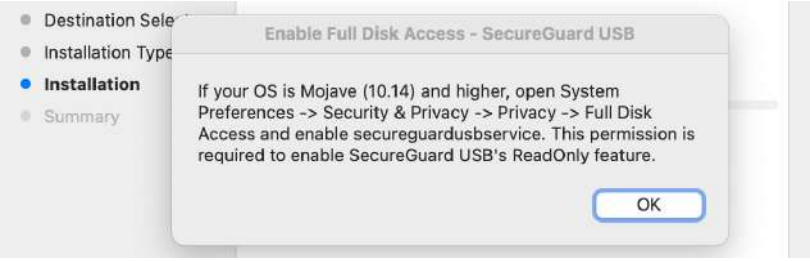
9. At the Administrator Authentication prompt, enter the email and password used when creating the administrator account, and choose a Computer Name for this individual computer. Click **OK** to continue.



10. At the Admin Authentication popup, click **OK**

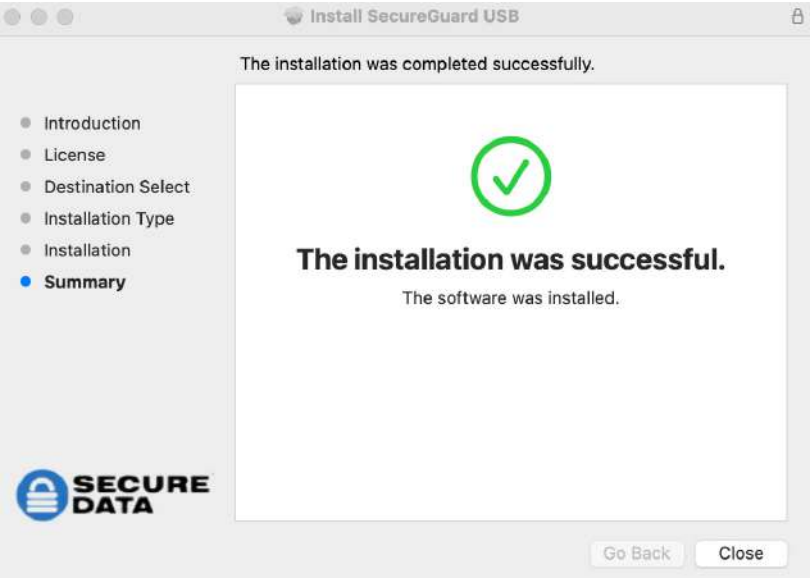


11. At the Enable Full Disk Access popup, click **OK**.



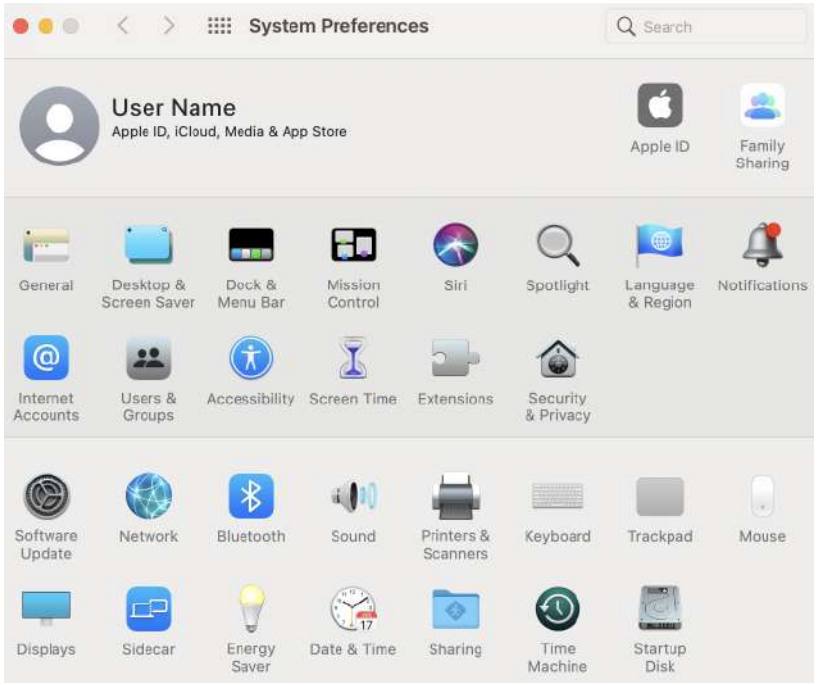
NOTE: This permission is required for the SecureGuard Read Only feature. To enable this, see the next section below.

12. Once SecureGuard completes installation, you will receive a verification. Click **Close** to continue



Full Disk Access

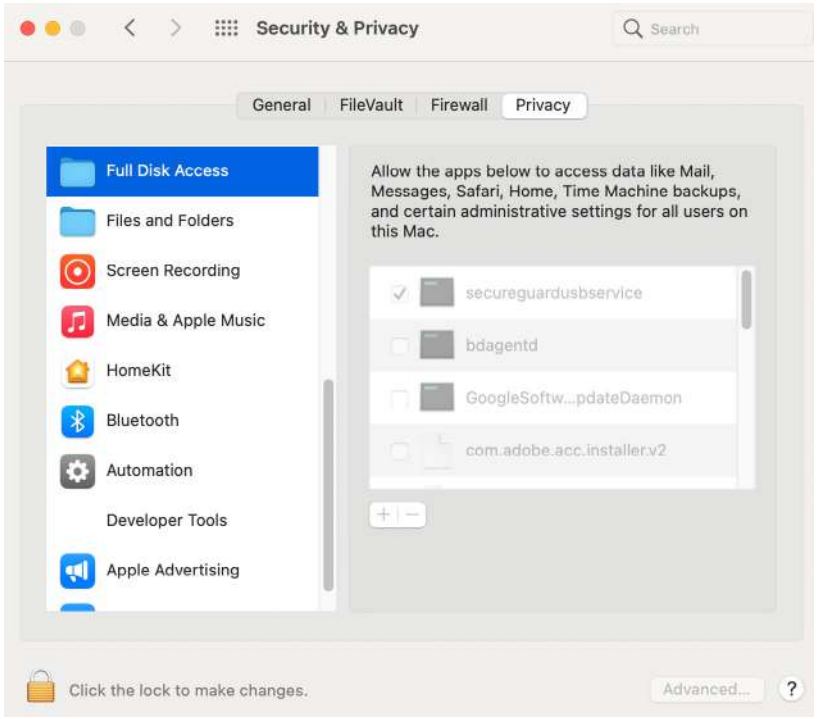
1. Open System Preferences. Select **Security & Privacy**.



2. At the Security & Privacy popup, select **Full Disk Access**.

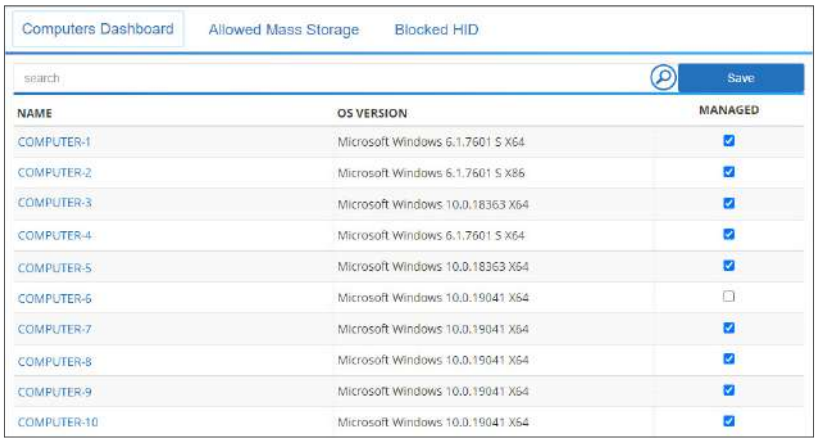
3. At the prompt, enter your computer's **User Name** and **Password**.

4. Select **secureguardusbservice** to enable Read Only mode.

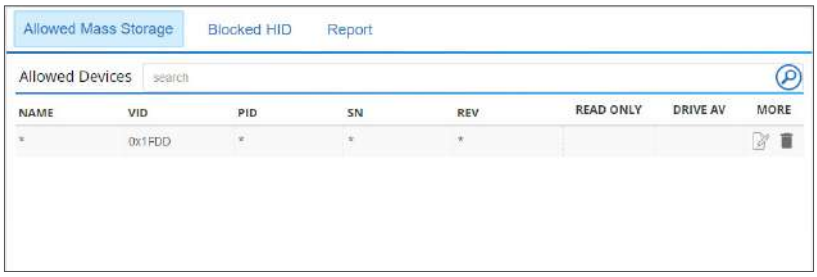


SECTION 4: COMPUTER MANAGEMENT

1. To begin managing computers, log into RM. For a **global configuration**, on the main **Computers Dashboard** you may click **Allowed Mass Storage** and enter a new record. This record applies to all computers with SecureGuard installed on them.



2. To customize a computer, **select** one of the names or use the **Search Field**.
3. By default all mass storage devices are blacklisted. To create a list of authorized devices, select the **Allowed Mass Storage** tab.



4. To customize whitelisted devices, click **Create**. In the popup, enter the relevant information as detailed below.

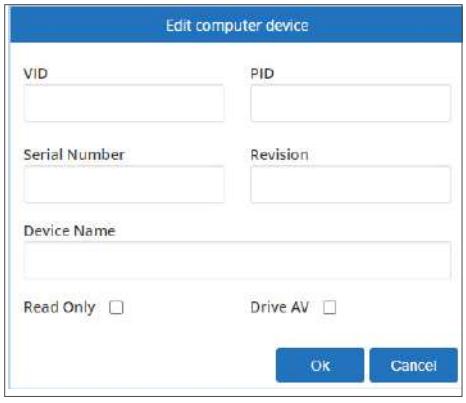
NOTE: Adding or editing a record requires entering at least one VID, PID, Revision, or Serial Number. There is an optional "Device Name" field you may enter for convenience.

VID: To allow a series of USB devices by vendor ID, enter the vendor ID

PID: To allow a series of USB devices by product ID, enterthe product ID

Serial Number: To allow individual USB devices only, enter each device's serial number. You will need to create a separate record for each SN

Revision: To allow USB devices by revision number, enter the revision number

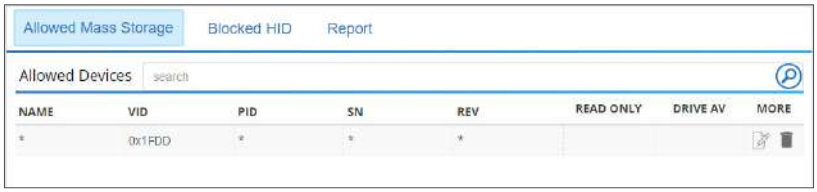


For help locating identification numbers for mass storage devices, see **Step 9** below. After filling out information, click **OK** to authorize a device to this computer.

NOTE: SecureGuard will not need internet access to function. However, a computer will need internet access for any changes made via RM to go into effect.

CAUTION: When entering authorized devices, entries apply to selected computer only. Select another computer and enter the same or alternate devices for use. Not authorizing devices on a computer with SecureGuard installed will block all USB mass storage devices , smartphones, flash card readers etc.

5. By default HID are allowed, including a mouse, keyboard and headset. To make exceptions to authorized devices, select the **Blocked HID** tab.
6. Under the Blocked HID tab, enter a VID, PID, Serial Number or Revision for the device, then click **Create**. For help locating identification numbers for HID, see **Step 9** below.
7. To view device details, click the **Allowed Mass Storage** or **Blocked HID** tabs.



8. Under either tab, you may revise details for applicable devices within this field by clicking the **Edit** icon. At the prompt, select a box to enable the feature:

   Read Only: this prevents saving files from the desktop to the drive and will prevent from editing files on device; check this box to put the disk in Read Only mode or uncheck to allow it to function in normal mode, then click OK

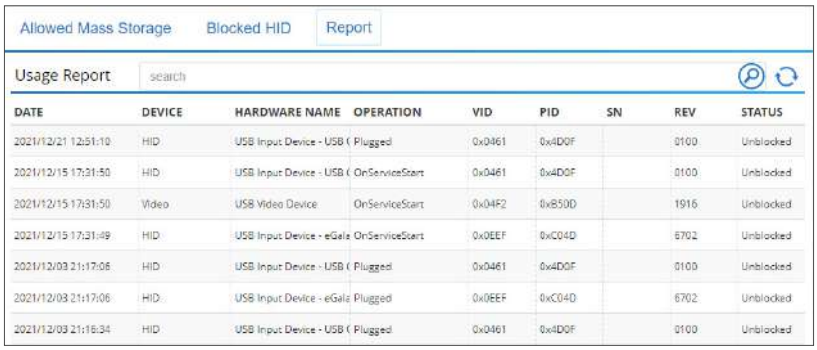
   Drive AV: this forces a drive to have DriveSecurity antivirus installed on it in order to use on the computer.

NOTE: Drive AV requires DriveSecurity, but no other antivirus software.

Edit: click the paper and pencil icon to edit a line

Delete: click the trashcan icon to remove this line

9. To see a detailed log of user actions on a USB port, click **Report**.



RM provides an access log for Admin to review:

Date: provides date and time action was taken (Note: this is adjusted to Admin's local time)

Device: this shows the type of device detected

Hardware Name: this displays the hardware name of the device

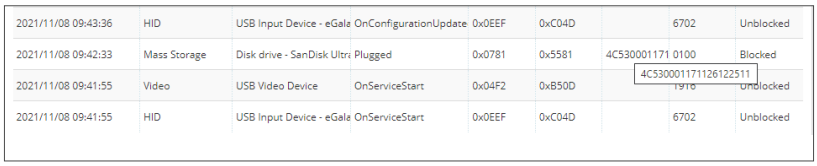
Operation: this is the action taken on a USB port on this computer

PID, VID, SN, REV: these identify the specific device used, whether it has been entered into RM or not

Status: this shows SecureGuard USB's action on the device

10. The access log updates within seconds. To get an updated view click the **Refresh** icon next to the search bar.

NOTE: Hovering the cursor over text will display the full text. This is useful for Serial Numbers.



11. To search for a specific record in the **Report**, enter a date, time, device type, operation type, PID, VID, Serial Number, Revision, or Status in the search field.

NOTE: The search is case sensitive.

12. To disable SecureGuard USB on selected computer, clear **Managed** check mark in **Computers Dashboard** and click **Save**.

SECTION 5: SECUREGUARD USB IN USE

1. Insert unauthorized drive into USB port.
2. If installed properly, the following message will appear.

The computer should completely lock now, including the mouse cursor's location on the screen and display information about the unauthorized device, which is stored on the access log in RM.

3. Remove unauthorized device to regain access to the computer.
4. While a whitelisted device is inserted, plugging in an unauthorized device will override the authorization and lock computer until unauthorized device is removed.
5. If a whitelisted device is inserted and becomes remotely blacklisted through RM, within seconds the target computer will lock. If an unauthorized device is inserted and locks the computer, then becomes remotely whitelisted through RM, the computer will unlock.
6. When charging an unauthorized phone or tablet via the computer's USB port, the computer will lock until the device is removed. The device also will not charge when the computer is locked.

CONTACT AND COPYRIGHT INFORMATION

Contact Information

SecureData, Inc.
625 Fair Oaks Ave Suite 325,
South Pasadena, CA 91030

www.securedrive.com
US: 1-800-875-3230
International: 1-424-363-8535

Copyright Information

SecureDrive and SecureUSB products are developed and manufactured by SecureData and are based on DataLock technology licensed from ClevX, LLC. U.S. Patent. www.clevx.com/patents

All other trademarks and copyrights referred to are the property of their respective owners.

Registered Trademark	Owner
Android	Google, Inc.
Bluetooth	Bluetooth SIG, Inc.
DataLock, ClevX	ClevX, LLC
Mac, iOS	Apple, Inc.
SecureUSB, SecureDrive, SecureData	SecureData, Inc.
Windows	Microsoft