

SecureData BT

REMOTE MANAGEMENT



ADMIN GUIDE

TABLE OF CONTENTS

SECUREDATA BT REMOTE MANAGEMENT	2
SECTION 1: INITIAL SETUP AND CONFIGURATION	3
Enrolling	3
Logging In	4
Creating Users	5
Account Actions	7
SECTION 2: SETTING UP DRIVE PROVISIONS AND ASSIGNMENTS	8
Downloading SecureData Lock Admin	8
Provisioning Drives	8
Assigning Drives to Users	10
SECTION 3: SETTING UP GEO- AND TIME- FENCING	12
Creating Geo-Fencing Restrictions	12
Creating Time-Fencing Restrictions	14
SECTION 4: MANAGING USERS	15
Disabling User Access	15
Removing User-Assigned Drives	15
Searching for Users	15
Resetting Users Passwords	16
Deleting Users	16
SECTION 5: MANAGING DRIVES	17
Remotely Wiping Drives	17
Disabling Drive Access	17
Remotely Unlocking Drives	18
Deleting Drives	18
Changing User's Drive Passwords	19
Viewing Drive's Assigned Users and Settings	19
Viewing Access Log	19
CONTACT AND COPYRIGHT INFORMATION	20

SECUREDATA BT REMOTE MANAGEMENT

SecureData Remote Management (hereafter “SecureData RM” or “RM”) is a web based software service application that provides IT Managers (hereafter “Admin”) control of company-wide, centralized policy using managed SecureDrive or SecureUSB BT, portable drives (hereafter “managed drives” or “drives”) throughout an organization.

RM enables IT Managers to enforce relevant security policies and remotely help users of the managed drives or to disable their access. The managed functions include control of drive access, drive reset (remote erase), password management, geo-fencing, and time-fencing.



Glossary

BT	Bluetooth
RM	Remote Management
Admin	IT Manger, Admin, or corporate manager
SMS	Short Message Service over a wireless mobile device (phone, tablet), commonly known as a “text message.”
Remote Licenses	An Admin requires an RM License Key annual subscription from SecureData or its licensees, authorized distributors, or resellers.
SecureData RM	Web software service to remotely control managed SecureData BT drives.
SecureDrive BT	Secure Bluetooth-capable drives from SecureData, Inc.
SecureData Lock Admin	Mobile Admin app (iOS/Android) that controls SecureDrive BT portable drives (Flash, HDD/SSD, etc.)
SecureData Lock Managed	Mobile app similar to SecureData Lock but to be used with the managed SecureDrive BT drives and capable of being managed by SecureData RM.
SecureData Lock	Mobile app (iOS/Android) that controls the security features (including unlocking/locking, password set up and change, and reset) of the BT drives. Note: This app is utilized by users and is not part of RM.

SECTION 1: INITIAL SETUP AND CONFIGURATION

This section describes how an Admin enrolls and logs into the Remote Management application. It also includes the process for creating new users.

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 is provided to the Admin via email upon the purchase of an annual subscription. If you did not receive an email, contact SecureData Customer Service.

2. Complete the enrollment form as follows:

- **License Key**—Enter the license key provided to you in the enrollment email.
- **Admin username**—Enter the email address used for the Admin setup.
- **Password**—Create a password.

Note: This password is required to be between 7 and 15 characters long and will be utilized throughout the process. This password is not the same as the drive PIN.

- **Confirm Password**—Re-enter the password.
- **Mobile Number**—Enter a mobile phone number to receive a security code for the two-step verification.

The screenshot shows a registration form with the following sections:

- License Key:** A text input field labeled "License Key".
- Admin username:** A text input field labeled "Email address".
- Password (it is not your drive pin):** A text input field labeled "Password (it is not your drive pin)".
- Confirm password:** A text input field labeled "Confirm password".
- Enter your mobile phone number:** A section with the text "We'll send a security code to this phone whenever you sign in to the SecureDataLock Remote Management". It includes a dropdown menu for the country code (currently showing "United States +1") and a text input field for the phone number (with an example "(201) 555-0123").

At the bottom right of the form is a blue button labeled "Enroll".

Figure 1.1: Login Page

3. Click **Enroll**.
4. On the **Enable Two-Step Verification** page, enter the 6-digit security code in the field.
5. Click **Next**.
6. On the verification page, click **Done**.

Logging In

To log into Remote Management, follow these steps:

1. Go to <https://rm.securedata.com/Account/Login>.
2. In the **Email Address** and **Password** fields, enter the Admin credentials used in the enrollment process.



Figure 1.2: Login Page

3. Click **Log In**.
4. On the **Enable Two-Step Verification** page, enter the 6-digit security code in the field.

Note: This security code will be sent to the Admin mobile phone number utilized in the enrollment process.

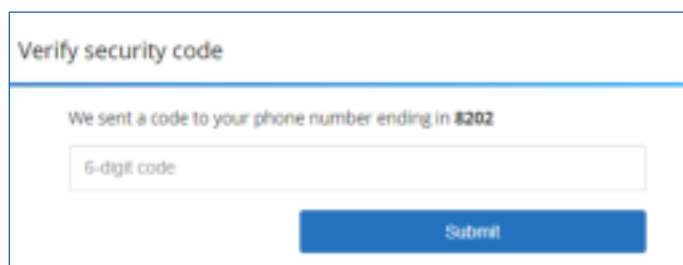


Figure 1.3: Login Security Code Verification Page

5. Click **Submit**.

Creating Users

As an Admin, if you intend to use a SecureDrive, you must also create a user account for yourself to lock and unlock drives. Your Admin credentials are **only** utilized by Remote Management and SecureData Lock Admin apps.

To create a user, follow these steps:

1. Log in to Remote Management. Go to **Logging In** on page **4** for instructions.
2. In the **Create User** section, enter the display name and an email address of the user.

Figure 1.4 Create User Dialog

3. Click **Create**. Once created, users display on the User dashboard.

Note: Steps 1 through 3 is used to create additional users. Each user will receive an invite email to download the **SecureData Lock Managed** app. For more information regarding the **SecureData Lock Managed** app, refer to the *SecureData Lock Managed User Guide*.

NAME	LOGIN	ENABLE	MORE
Test User	test@securedata.com		

Figure 1.5: Users Dashboard Example

To import a list of users, follow these steps:

1. Create an excel spreadsheet with the name of each user followed by a “;” before the email address.

Example: Import User; import@test.com

2. Save as a “.csv” file.
3. In the **Create User** section on RM, click the **Import** button.
4. Click **Choose a file...** and then select the .csv file.
5. Click **Import**. A message will appear when the import is successful.
6. Click **Close**.

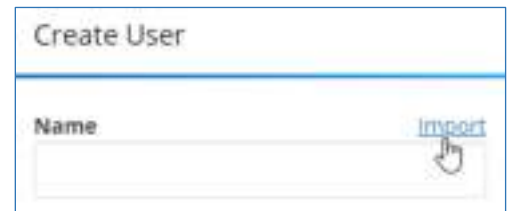
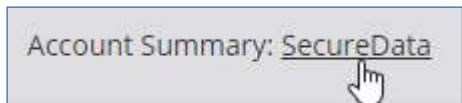


Figure 1.6: Import Option Location

Account Actions

To view account information and activity, follow these steps:

1. Next to **Account Summary**, click the name of the account.
2. Navigate through the following tabs:
 - **Summary**—This tab displays the license information for the Remote Management account including the number of Admins, Users, and Drives used out of the allotted amount, and expiration date of the license.
 - **Admins Contacts**—This tab displays all admins on the account, the mobile number utilized, and the last time the admin logged into Remote Management.
 - **Users Contacts**—This tab displays all user names, emails, and the last login attempt date and time for each.
 - **Drives Activity**—This page displays the drive and provisioning information as well as the last attempted login with date and time.



To change the Admin password, follow these steps:

1. Next to **Admin**, click the admin email address.
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 logout of the system, click **Log Out**.

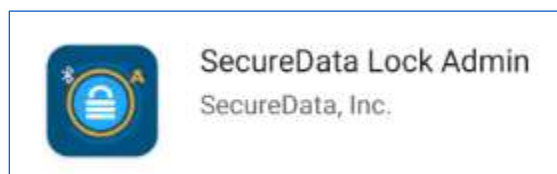


SECTION 2: SETTING UP DRIVE PROVISIONS AND ASSIGNMENTS

This section explains how an Admin can set up, provision, and manage assignments to SecureDrives using the SecureData Lock Admin app. This app is required and works with the Remote Management web application allowing Admins to provision drives and enforce security policies.

Downloading SecureData Lock Admin

To install the SecureData Lock Admin app, go to the Apple App Store or Android Google Play store and search for the “**SecureData Lock Admin**” app. Download the app on the mobile device.



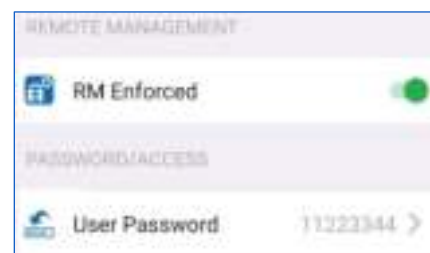
Provisioning Drives

To provision a SecureDrive BT, follow these steps:

1. Open the **SecureData Lock Admin** app on your mobile device.
2. Enter the Admin credentials created in the **Enrolling** section on page 3.
3. Click **Login to RM Account**.
4. On the **Drive Provisioning Settings** page, review and modify the following if necessary:



- **RM Enforced**—When turned off, this will allow users to access the drives without internet connection. This also disables communication between the drive and the RM console (including Admin).
- **User Password**— This is the password that will be used by the User to unlock the drive. The User will be able to change this password in the drive settings. We recommend using a default password for all drives during set up.

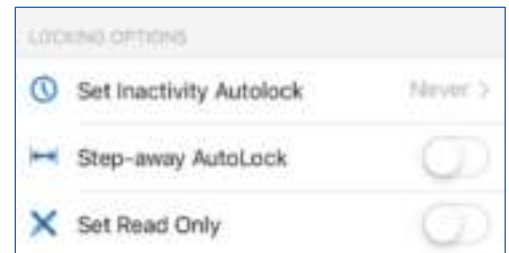


5. In the **Locking Options** section, modify the following if necessary:

Note: These are universal settings that, once set, cannot be modified by the user.

- **Set Inactivity Autolock**—When enabled, the drive can be set to automatically lock after a pre-set amount of time of inactivity between 1 and 60 minutes.

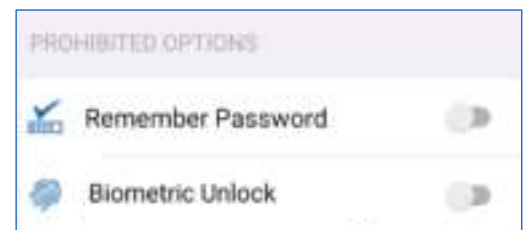
- **Step-away Autolock**—When enabled, the drive will automatically lock after the connected mobile device is moved approximately 10 ft. away.
- **Set Read Only**—To prevent users from making changes to files on the drive, tap to enable the Read Only setting.



Note: This setting does not prevent the user from saving a file locally and making changes.

6. In the **Prohibited Options** section, modify the following if necessary:

- **Remember Password**—When set to Off, the user will be allowed to use a remember password utility on their device. When On, the remember password option will be prohibited and the user must enter the password each time to access the drives.
- **Biometric Unlock**—When set to Off, the user will be allowed to set a biometric unlock to access the drives. When On, the biometric unlock option will be prohibited for the user.



7. When complete, click **Confirm**.

Note: The **Confirmation** dialog displays all the settings for the drives. To set your selected options, continue with Step 8. To modify these options, click **Cancel** and return back to Step 4.

8. On the **Confirmation** dialog, click **CONTINUE**.
9. Connect a SecureDrive to a computer via USB port.

Write down the 8-digit Drive ID number located on the drive for use in Step 11.

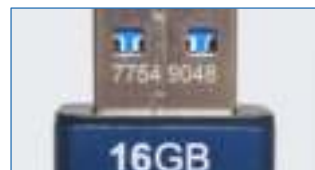
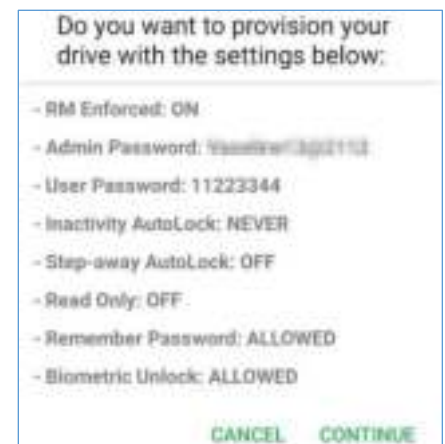
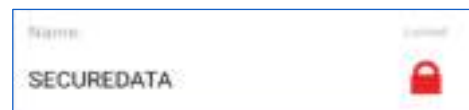


Figure 2.1: Device ID Location Examples

Note: To provision multiple drives at once, connect the drives to a multi-port USB hub and document the 8-digit Drive ID numbers for each drive.

10. On the **Drive Provisioning** page, select the drive you want to provision.



Note: These steps are for drives that are new and have never been provisioned. If the drive has been provisioned before and you want to reset it, follow the steps in **PART A**. If the provisioned drive needs provisioned without a reset, follow the steps in **PART B**.

11. In the **Device ID** field, enter the 8 digit drive ID number. Once entered, you will be returned to the drive page where the gray lock displays and says 'Blank.'
12. Select the drive again.
13. Once the drive is successfully provisioned, the Lock icon will display as 'Unlocked' and green. To provision additional drives, repeat Steps 9 through 13.



Note: Once the drive is provisioned for the first time, it will need to be formatted. Refer to the drive's user guide for steps on reformatting the drive.

PART A: PROVISION WITH RESET – Follow Steps 1-10 above.

- In the **Device ID** field, enter the 8 digit drive ID number.
- On the dialog, select the **Provision with Reset** option. This will wipe the drive of all contents.
- The drive number will appear with a gray lock and say 'Blank.' Select the drive again.
- Once the drive is wiped, the drive will need to be reformatted. Refer to the drive's user guide for steps on reformatting the drive.

PART B: PROVISION WITHOUT RESET – Follow Steps 1-10 above.

- In the **Device ID** field, enter the 8 digit drive ID number.
- On the dialog, select the **Provision without Reset** option.
- Click the drive to provision. The drive will display as the serial number and the lock icon will be green and 'Unlocked'.

Assigning Drives to Users

To assign a drive to a user, follow these steps:

1. Open the **Remote Management** web app and login. Refer to the **Logging In** section on page 4.
2. On the **Home** page, if not already open, click the **Users** option.
3. Click the user's name to add a drive.

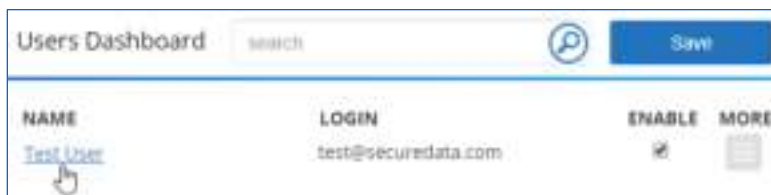


Figure 2.2: User Select Example

4. In the **Allowed Drives** section, click the **Add Drive** dropdown and select an available drive to provision to the user.
5. Once selected, click **Add**.

Note: Once added, the Drive will display in the **Drive S/N** section.

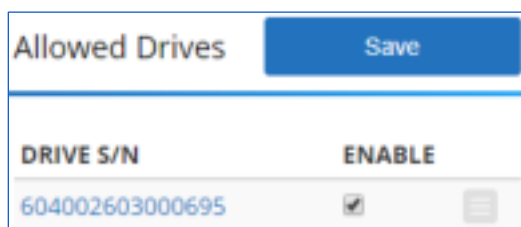


Figure 2.3: Add Selected Drive to User Example

6. In the **Allowed Drive** section, click **Save**.

Note: To provision additional drives, repeat Steps 3 through 6.

SECTION 3: SETTING UP GEO- AND TIME- FENCING

This section goes through the process of setting up geo- and time- fencing for drives. The drives can be limited in their use by country or by a specific location. Additionally, the drives can be set up to be used only during a specific time.

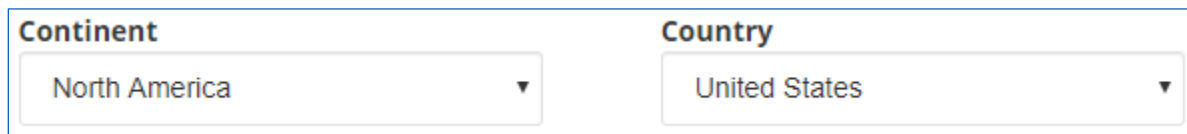
Creating Geo-Fencing Restrictions

To create a geo-fence for a drive, follow these steps:

1. Login to **Remote Management** and click **Users**.
2. On the **Users Dashboard**, select a user from the list.
3. In the **Allowed Location** section, complete the following when applicable:

Note: Individual options in the **Allowed Location** section can be used to limit the location. If you want to limit a user access to a specific location, enter the full address with city, state, and zip. Use less settings to create a broader geo-fence.

- **Continent**—Click the dropdown to select a continent.
- **Country**—Click the dropdown to select a country in the selected continent.



The image shows a screenshot of a web interface with two dropdown menus. The first dropdown is labeled 'Continent' and has 'North America' selected. The second dropdown is labeled 'Country' and has 'United States' selected. Both dropdowns have a downward-pointing arrow on the right side.

Figure 3.1: Continent and Country Selection Example

- **Address**—Enter an address in the available fields, if desired.
- **City**—Enter a city name in the field, if desired.
- **State/Province**—Enter a state or province in the field, if desired.
- **Zip/Postal Code**—Enter a zip or postal code in the field, if desired.
- **Radius**—To widen the geo-fence from a pinpointed location, enter the distance in the field and select the unit of measurement in the dropdown.

Address

Street line 1

Street line 2

City	State/Province	Zip/Postal Code
Cleveland	Ohio	Zip/Postal Code

GPS Coordinates

Latitude: 41.49932, Longitude: -81.6943605

Radius	Miles or Km
Radius	mi ▼

Map




Figure 3.2: Specific Location Selection Example

4. When complete, click **Save**.

Note: To view geo-fencing settings for all users on a drive, go to Drives, select the drive and then click Used by. This will display the geo-fencing settings when applicable.

5. To clear the settings and to remove the saved geo-fence, click the **Clear** button.

Creating Time-Fencing Restrictions

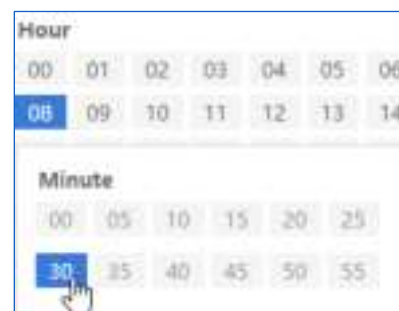
To create a time-fence for a drive, follow these steps:

1. Login to **Remote Management** and click **Users**.
2. On the **Users Dashboard**, select a user from the list.
3. In the **Allowed Drives** section, if not already enabled, select the checkbox to enable the device.

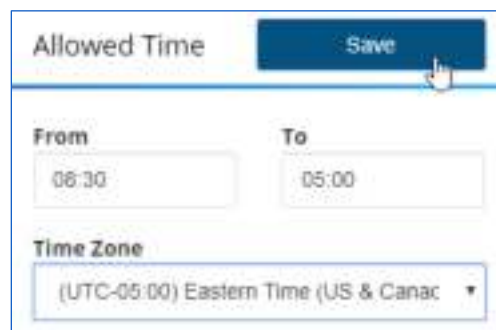
Note: If there are multiple drives provisioned for the selected user, any time restrictions created will apply to all drives.

4. In the **Allowed Time** section, complete the following steps if applicable:

- **From**—Click the field to set a start time for the beginning of the range. Select the start hour from the grid and then set the minute, if applicable.
- **To**—Click the field to set an end time for the end of the time range. Select the ending hour from the grid and then set the minute, if applicable.
- **Time Zone**—Click the dropdown field and select the appropriate time zone.



5. Click **Save**.
6. To remove the selected time restriction, click the **From** and the **To** fields, remove the content and then click **Save**.



SECTION 4: MANAGING USERS

In this section, Admins can manage users and drives assignments by disabling access, removing the drive from the user, and searching for registered drive users.

Disabling User Access

To disable a user’s access to a drive, follow these steps:

1. Login to **Remote Management** and click **Users**.
2. On the **Users Dashboard**, select a user from the list.
3. In the **Allowed Drives** section, to disable a user’s access to a drive, clear the checkbox in the **Enable** column.
4. Click **Save**.



Figure 4.1: Disable Drive Access Example

Removing User-Assigned Drives

To remove a drive from a user, follow these steps:

1. On the **Users Dashboard**, select a user from the list.
2. In the **Allowed Drives** section, to remove a drive from a user, click the menu and select **Delete**.
3. In the **Delete Confirmation** dialog, click **Delete**.

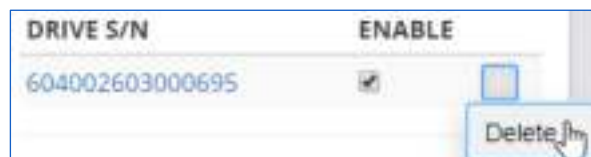


Figure 4.2: Remove Drive Example

Searching for Users

To search for a user, follow these steps:

1. On the **Users Dashboard**, click the **Search** field and enter a user name.
2. Click **Enter**.

Note: The users associated with your search will display in the grid.

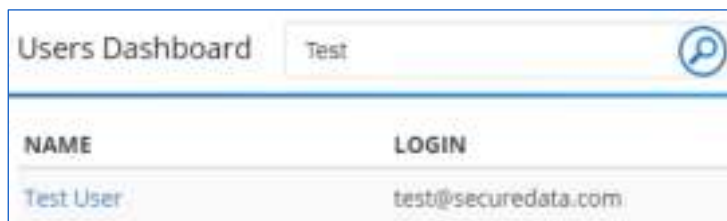


Figure 4.3: User Search Result Example

Resetting Users Passwords

Note: This process is resetting the user credentials password and not the drive password.

To reset a user’s password for the app, follow these steps:

1. On the **Users Dashboard**, in the row of the user, click the menu in the **More** column.
2. Click **Reset User’s App Password**.

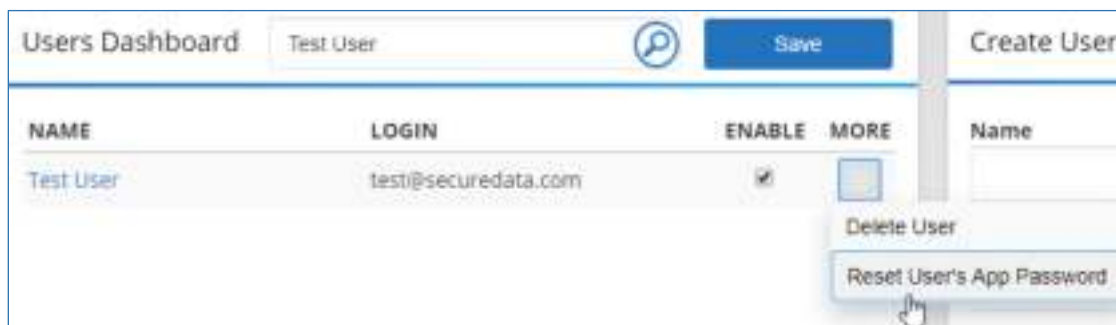


Figure 4.4: Reset User Password Example

3. On the **Reset Confirmation** dialog, click **Reset**.

Deleting Users

To delete a user, follow these steps:

1. On the **Users Dashboard**, in the row of the user to be deleted, click the menu in the **More** column.
2. Click **Delete User**.

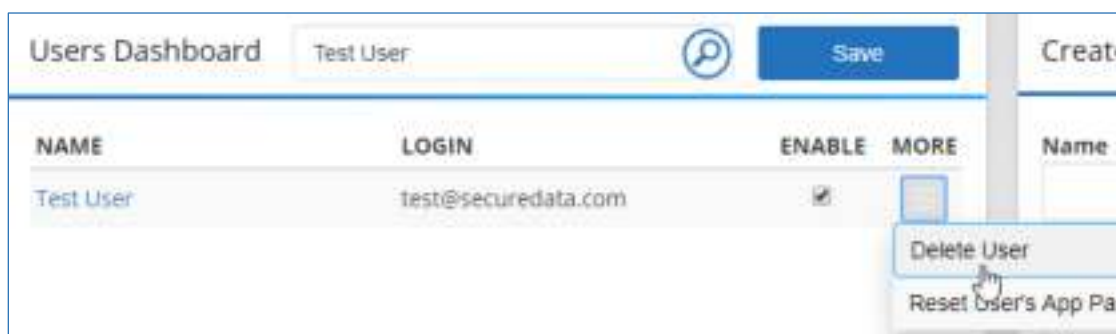


Figure 4.5: Delete User Example

3. On the **Delete Confirmation** dialog, click **Delete**.

SECTION 5: MANAGING DRIVES

From the Drives section of Remote Management, admins can remotely wipe, unlock, and disable access to drives. Additionally, admins can view users and settings on specific drives and the log, which displays the activity for that user on the drive.

Remotely Wiping Drives

To remote wipe a drive, follow these steps:

1. Login to **Remote Management** and click **Drives**.
2. On the **Drives Dashboard**, select a drive from the list.
3. In the **Drive Operation** row, click the dropdown and select the **Admin Remote Wipe** option.
4. Click **Save**.

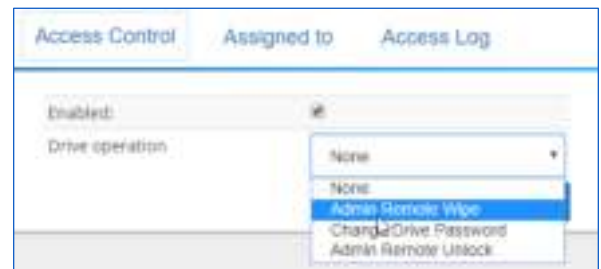


Figure 5.1: Remote Wipe Example

Note: Once the drive is connected and usage is attempted, the contents of the drive will be deleted. Until that point, the drive displays as “Admin Remote Wipe” on the dashboard.

DRIVE S/N	ACTIVE	ADMIN REMOTE WIPE	ADMIN REMOTE UNLOCK	CHANGE DRIVE PASSWORD	MORE
604002603000695	✓	✓			

Disabling Drive Access

To lock a drive for all users, follow these steps:

1. On the **Drives Dashboard**, select a drive from the list.
2. On the **Access Control** tab, deselect the checkbox in the **Enabled** row.
3. Click **Save**.

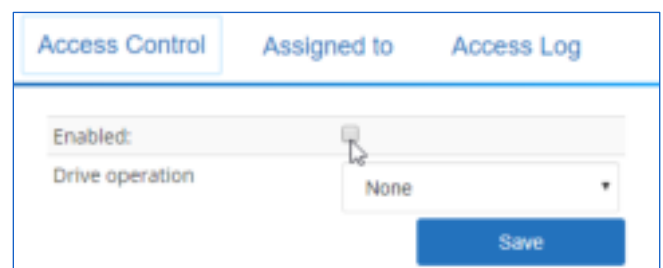


Figure 5.2: Disabling Drive Access Example

Note: On the Drive Dashboard, the drive will display as inactive.

DRIVE S/N	ACTIVE
604002603000695	

Remotely Unlocking Drives

Note: This process is a one-time unlock for admins to use.

To remotely unlock a drive, follow these steps:

1. On the **Drives Dashboard**, select a drive from the list.
2. In the **Drive Operation** row, click the dropdown and select the **Admin Remote Unlock** option.
3. Click **Save**.

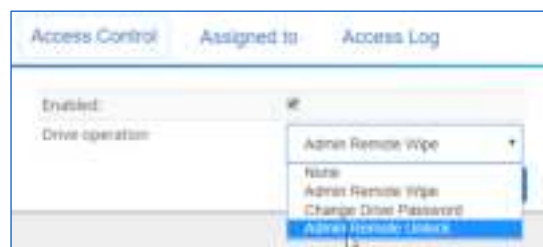


Figure 5.3: Remote Unlock Example

Note: The drive displays on the dashboard as “Admin Remote Unlock.”

DRIVE S/N	ACTIVE	ADMIN REMOTE WIPE	ADMIN REMOTE UNLOCK	CHANGE DRIVE PASSWORD	MORE
604002603000695	✓		✓		☰

Deleting Drives

To delete a drive, follow these steps:

Note: It is recommended to backup all necessary data before deleting the drive.

1. On the **Drives Dashboard**, in the **More** column, right-click the menu.
2. Click **Delete Drive**.

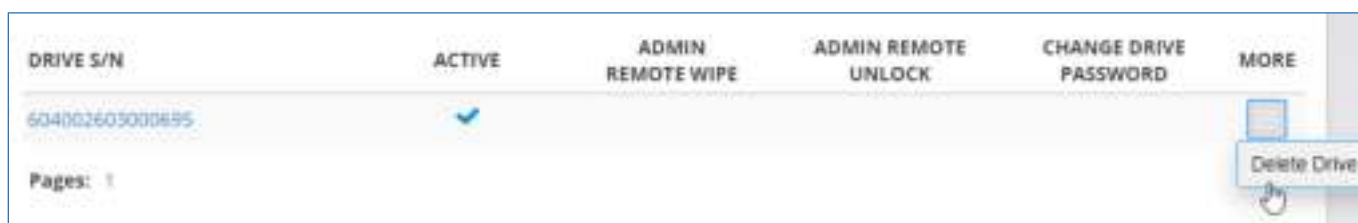


Figure 5.4: Deleting Drive Example

3. On the **Delete Confirmation** dialog, click the **Delete** button.
4. If the drive is in use, an additional confirmation dialog appears. Click **Delete**.

Note: Once complete, the drive is removed from the dashboard. To continue using the drive, it must be re-provisioned. This process will remove all data from the drive. To use the drive without RM, disable the **RM Enabled** option during re-provisioning.

Changing User's Drive Passwords

To change a user's drive password, follow these steps:

1. On the **Drives Dashboard**, select a drive from the list.
2. In the **Drive Operation** row, click the dropdown and select the **Change Drive Password** option.
3. In the available field, enter the drive's user password.
4. Click **Save**.

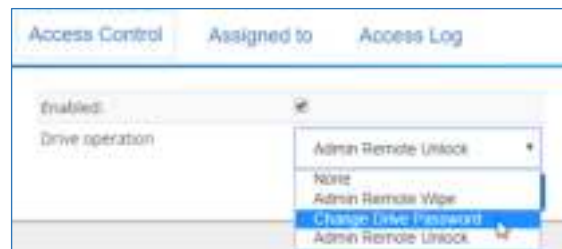


Figure 5.4: Change Password Example

DRIVE S/N	ACTIVE	ADMIN REMOTE WIPE	ADMIN REMOTE UNLOCK	CHANGE DRIVE PASSWORD	MORE
604002603000695	✓			✓	☰

Viewing Drive's Assigned Users and Settings

To view a drive's assigned users and fencing settings (when applicable), follow these steps:

1. On the **Drives Dashboard**, select a drive from the **Drive S/N** column.
2. Click the **Assigned To** tab.

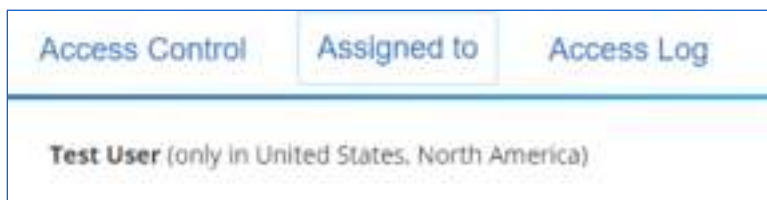


Figure 5.6: Drive Assigned To Example

Viewing Access Log

To view the access log for a drive, follow these steps:

1. On the **Drives Dashboard**, select a drive from the **Drive S/N** column.
2. Click the **Access Log** tab.

Note: The log will display any operation with the date, time, user, type of operation and the details.

3. Click the icon in the **Map** column to view the location the drive was accessed at the time of logged operation.

CONTACT AND COPYRIGHT INFORMATION

Contact Information



SecureData, Inc.
 3255 Cahuenga Blvd. West #301
 Los Angeles, CA 90068-1178

www.securedrive.com
 US: 1-800-875-3230
 International: 1-323-944-0822

Copyright Information

Copyright © 2019 SecureData, Inc. All rights reserved.

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

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is **prohibited** unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

