SecureData

REMOTE MANAGEMENT

ADMIN GUIDE

SecureData
Remote Management
Admin Guide

SECURE DATA

TABLE OF CONTENTS

SECUREDATA REMOTE MANAGEMENT

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

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

Glossary

BT	Bluetooth
RM	Remote Management
Admin	IT Manager, administrator, or corporate manager
SMS	Short Message Service over a wireless mobile device (phone, tablet); also known as “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 BT or DUO drives
SecureDrive BT	Secure Bluetooth-capable portable drives from SecureData
SecureUSB BT	Secure Bluetooth-capable flash drives from SecureData
SecureDrive DUO	Secure portable drives from SecureData that feature onboard keypad and Bluetooth capabilities
SecureUSB DUO	Secure flash drives from SecureData that feature onboard keypad and Bluetooth capabilities
SecureData Lock Admin	Mobile Admin app (iOS/Android) that controls BT and DUO drives
SecureData Lock Managed	Mobile app used with managed BT and DUO drives, capable of being managed by RM
SecureData Lock User	Mobile app used to control BT and DUO drives that are not managed by RM

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.

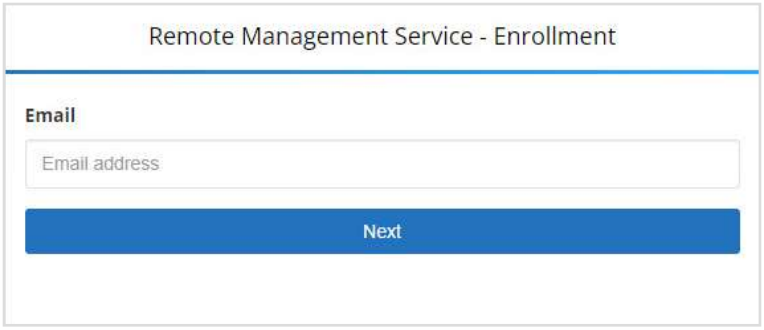
Enrolling

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**

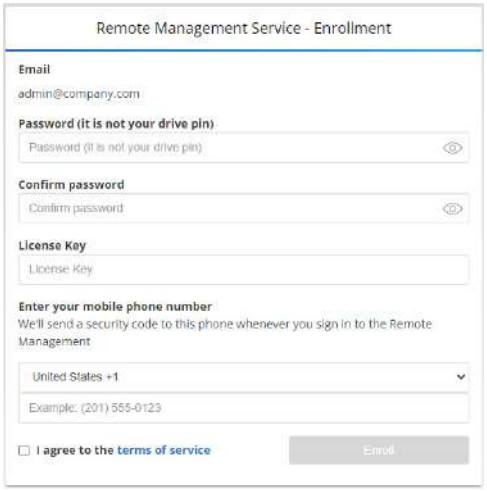
NOTE: This enrollment link and the License Key are provided to Admin via email upon the purchase of an annual subscription. If you did not receive an email, contact SecureData Customer Service.

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.

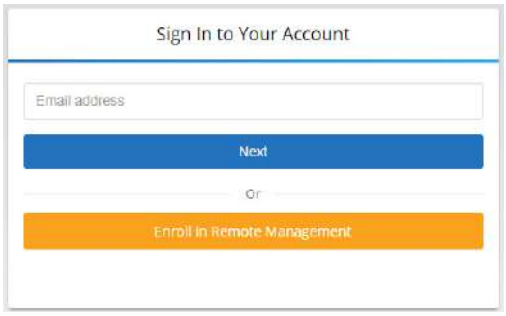
4. Check "I agree to the terms of service" and click **Enroll**.
5. On the **Enable Two-Step Verification** page, enter the 6-digit security code in the field.
6. Click **Next**.
7. On the verification page, click **Done**.

Logging In

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

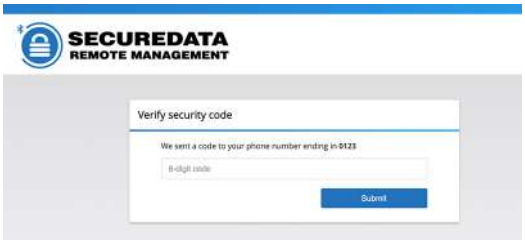
1. Go to https://rm.securedata.com/Account/Login

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**.

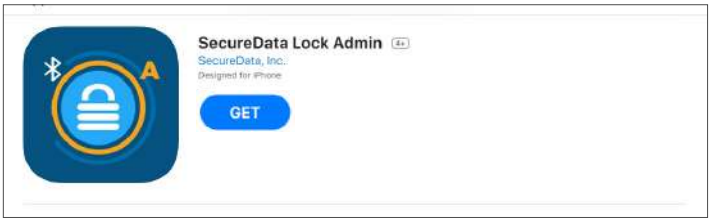
SECTION 2: SETTING UP DRIVE PROVISIONS AND ASSIGNMENTS

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

NOTE: Provisioning a drive does not create a PIN for it. The user must create a PIN when using it for the first time.

Downloading SecureData Lock Admin App

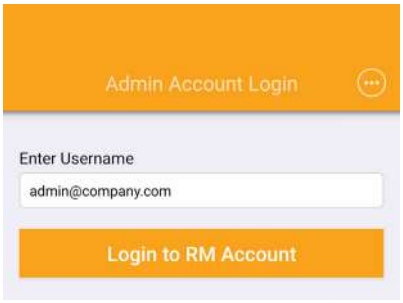
To install the SecureData Lock Admin app, visit the Apple App Store or Android Google Play store and search for the SecureData Lock Admin app. Download the app on the mobile device.



Provisioning Drives

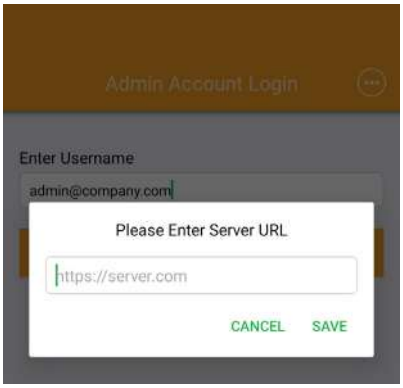
To provision a BT or DUO drive, follow these steps:

1. Open the **SD Admin** app on your mobile device.
2. Enter the Admin email and click '**Login to RM Account**'.



NOTE: If using SSO, you will be redirected to the Identity Provider and then returned to the Drive Provisioning Settings.

NOTE: The default server URL for an RM account is rm.securedata.com. If your account is on a different server, click the three dots icon in the upper right corner and enter the server URL.



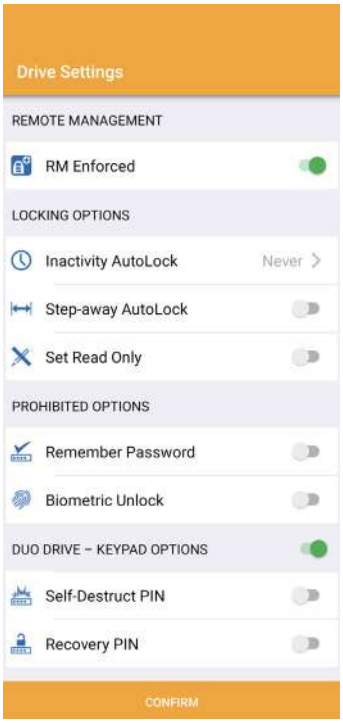
3. Enter password and click **Log In**.
4. On the **Drive Provisioning Settings** page, review and modify the following, if necessary:
   - **RM Enforced** — When turned off, this allows users to access the drives without internet connection. This also disables communication between the drive and the RM console (including Admin).
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 automatically locks after the connected mobile device is moved approximately 10 feet away.
- **Set Read Only** — To prevent users from making changes to files on the drive, tap to enable the Read Only setting.

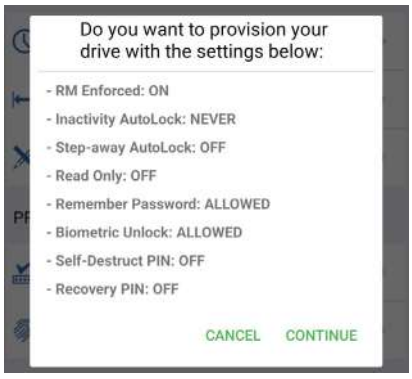
NOTE: Read Only does not prevent the user from saving a file locally and making changes.

6. In the **Prohibited Options** section, modify the following if necessary:
   - **Remember Password** — When set to Off, the user is allowed to use a remember password utility on their device. When On, the remember password option is prohibited and the user must enter the password each time to access the drives.
   - **Biometric Unlock** — When set to Off, the user is allowed to set a biometric unlock to access the drives. When On, the biometric unlock option is prohibited for the user.



7. **DUO Drive — Keypad Options** — When set to On, Admin can access unique DUO features:
   - **Self-Destruct PIN** — Should all data stored on the drive need to be quickly and irretrievably deleted, Admin can get a Self-Destruct PIN by selecting this option. The Self-Destruct PIN is randomly generated during provisioning and has a one-time use. Admin gets this PIN from Remote Management (described below), and provides the PIN to the user, who then enters it.
   - **Recovery PIN** — In the event a user must access the drive and cannot remember the password and there is no internet connection, Admin can select this option for a Recovery PIN. It is randomly generated and has a one-time use. The user enters the PIN via the **onboard keypad**.

8. When complete, click **Confirm**.



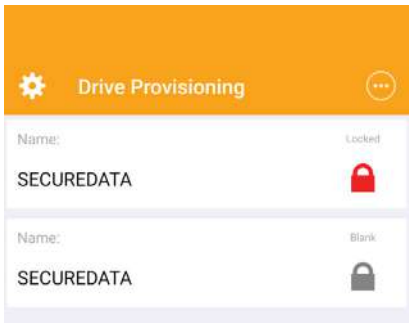
NOTE:
To get a **new PIN**, the drive must be reprovisioned.
The **Self-Destruct PIN** is entered via the app.
If the one-time **Recovery PIN** has already been used, the drive indicates an unsuccessful password attempt (see **SecureDrive DUO** or **SecureUSB DUO Manuals**; to see the user's input command, see

the **Managed App Manual**).
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.

9. On the Confirmation dialog, click **Continue**.

10. Write down the 8-digit device ID number located on the drive, for use in Step 11.
    Connect a SecureDrive to a computer via USB port.

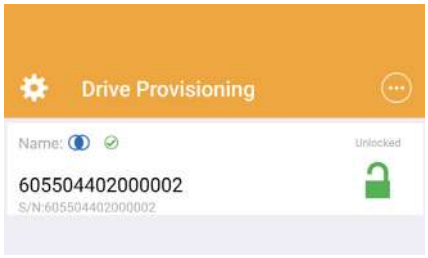
NOTE: To provision multiple drives at once, connect the drives to a multi-port USB hub and document the 8-digit Device ID numbers for each drive then insert it.



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

NOTE: The drive must be formatted every time it is provisioned.

There are two possible scenarios:



A. The drive does not have a user password. This is a new DUO or a reset BT or DUO.

1. In this instance, the drive appears with a gray lock icon and the word “blank” above it
2. Tap on the drive and wait until provisioning finishes

B. The drive has a user password. This is a BT or a used DUO.

1. The drive appears with a red lock icon and the word “locked” above it
2. Tap on the drive
3. Confirm the reset in “drive reset required”
4. Enter the Device ID and tap OK
5. Wait until provisioning finishes

NOTE: A successful provisioning is indicated by a green check mark above the drive name; in most cases, this is the serial number.

SECTION 3: MANAGING USERS AND ADMINS

Super Admin may add Regular Admins. Admins can manage users and drive assignments by disabling access, removing the drive from the user, and searching for registered drive users.

For easier navigation, most columns in the Web Console can be sorted by clicking on the column name. The sort order will be indicated by an arrow next to the name.

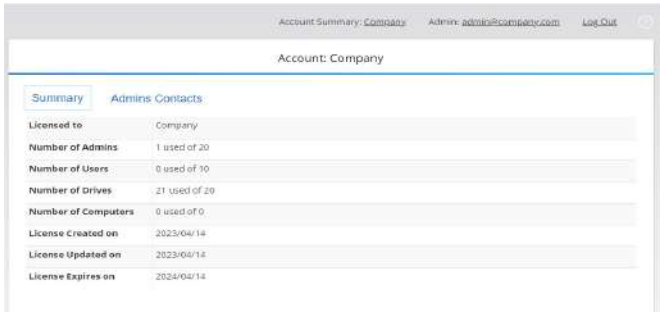
Log into **Remote Management**, as detailed above.

Account Actions

To view account information and activity, follow these steps:

1. Next to **Account Summary**, click the name of the account.

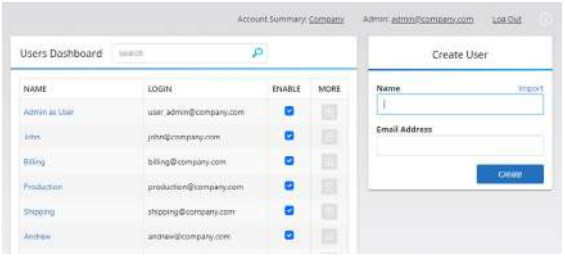
2. Navigate through the following tabs:
   - **Summary** — This tab displays the license information for the RM account, including the number of Admins, Users, and Drives used of the allotted amount, as well as expiration date of the license.
   - **Admins Contacts** — This tab displays all Admins on the account, their mobile number used, and the last time the Admin logged into RM.



Creating Users

NOTE: As an Admin, if you intend to use a SecureDrive for yourself, you must also create your own user account to lock and unlock drives. Your Admin credentials are used only by Remote Management and the SecureData Lock Admin app.

To create a user, follow these steps:



1. In the **Users Dashboard** go to **Create User** section, enter the display name and the user's email address.

2. Click **Create**. Once created, users appear on the

User dashboard.

NOTE: Follow steps above to create additional users. Each user receives an invite via email to download the **SecureData Lock Managed** app. For more information regarding the **SecureData Lock Managed** app, refer to the *SecureData Lock Managed User Guides* for either the BT or DUO. Capabilities vary between BT and DUO drives.

To import a list of users, follow these steps:

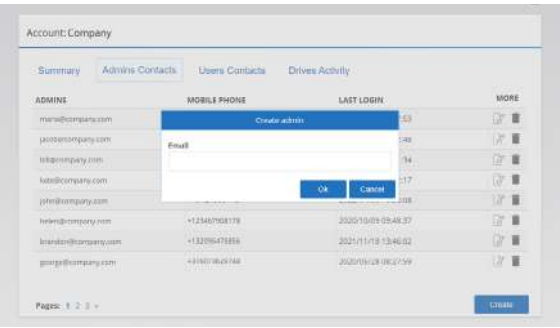
1. Create an Excel spreadsheet with the name of each user followed by a ";" and then the user's respective email address.

   Example: *User Name; username@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 select the .csv file you created.
5. Click **Import**. A message appears when the import is successful.
6. Click **Close**.

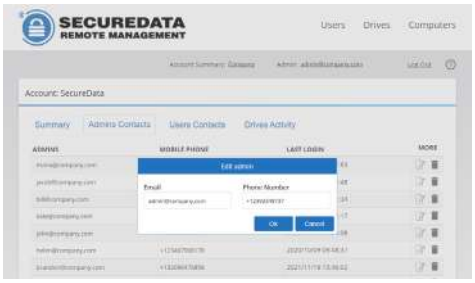
Creating New Admin

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:

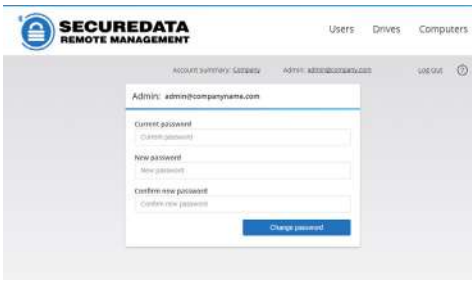
1. Next to **Account Summary**, click the account name.
2. Locate the record you want to modify under **Admins Contacts**.
3. To edit the email address or mobile number, click the paper icon.
4. To delete an Admin, click the trash can icon.

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.

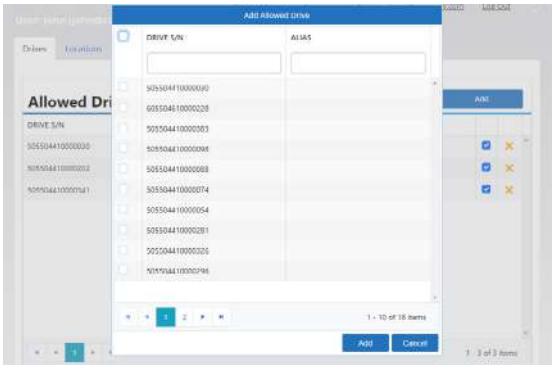
To log out of the system, click **Log Out**.

Assigning Drives to Users

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

1. Open the **Remote Management** web app and log in.
2. On the **Home** page, if not already open, click the **Users** option.
3. Click the user's name to add a drive. In the **Allowed Drives** section, click the **Add Drive** dropdown and select an available drive to assign to the user.

4. Once selected, click **Add**.



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

Disabling User Access

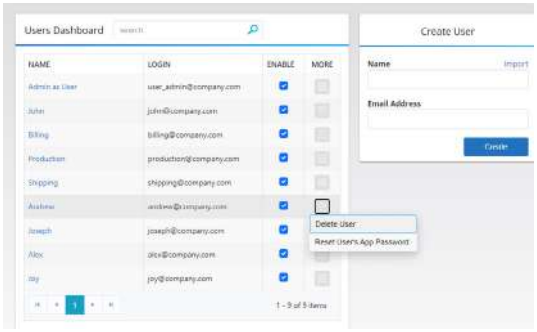
To disable a user's access to a drive, follow these steps:

1. On the **Users Dashboard**, select a user from the list.
2. In the **Allowed Drives** section, to disable a user's access to a drive, clear the checkbox
3. To remove a drive from a user, click on the 'X' icon. In the **Delete Confirmation** dialog box, click the **Delete** button.

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



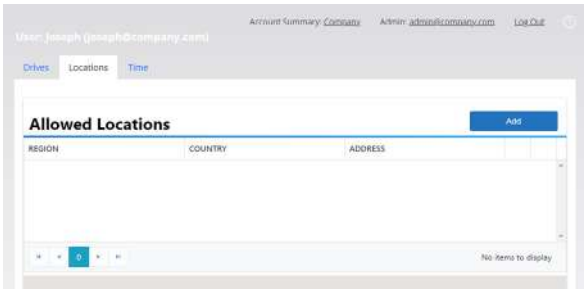
SECTION 4: SETTING UP GEO- AND TIME-FENCING

This section explains the process of setting up geo- and time-fencing for drives assigned to a user. The drives can be limited in their use by countries and/or by specific locations. Additionally, the drives can be set up to be used only during a specific time.

Log in to **Remote Management** and click **Users**.

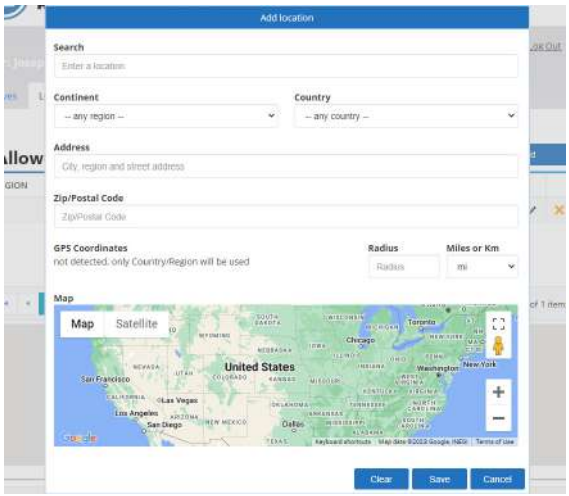
Creating Geo-Fencing Restrictions

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



1. On the **Users Dashboard**, select a user from the list.
2. Click on Locations tab.
   To edit allowed locations click on the pencil icon next to location.
   To delete allowed location click the X icon and confirm deletion in **Delete Confirmation** dialog.
   To add allowed location click **Add button**:

NOTE: Individual options in the Allowed Location section can be used to limit the location. If you want to limit a user's access to specific locations, enter the full address with city, state, and zip. Use autocomplete feature in Search for easy location entering.
Use fewer settings to create a broader geo-fence.



- **Continent** — Click the dropdown to select a continent.
- **Country** — Click the dropdown to select a country within the selected continent.
- **Address** — Enter the exact address.
- **State/Province** — ZIP/Postal Code - Enter zip or postal code.Please note that using zip or postal code requires country and does not require exact address.
- **Radius** — Enter the distance and unit of measurement in this field to set a radius.

3. When complete, click **Save**.

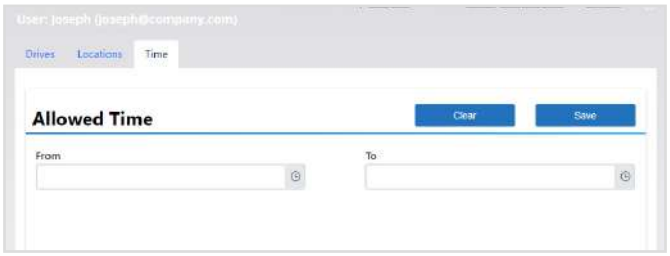
Creating Time-Fencing Restrictions

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

1. On the **Users Dashboard**, select a user from the list.

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

2. Click on Time tab and in the Allowed Time section, complete the following steps if applicable:



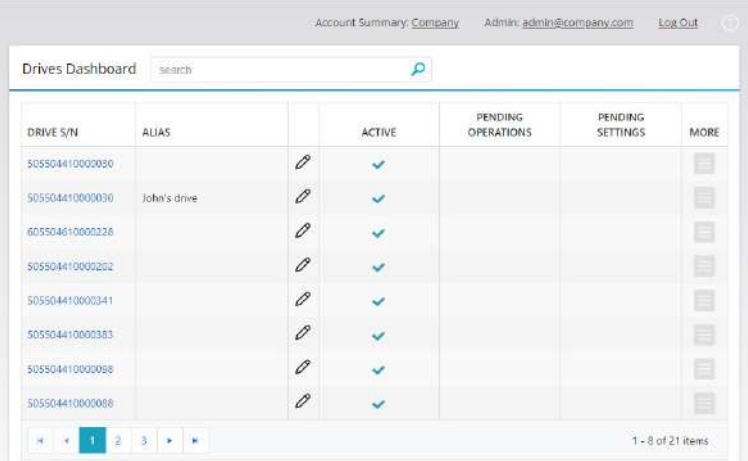
- **From** — Click the clock icon to set a start time for the beginning of the range. Select the start hour from the dropdown.
- **To** — Click the clock icon to set an end time for the end of the time range. Select the ending hour from the dropdown.

3. Click **Save**.
4. To remove the selected time restriction, click the **Clear** button.

SECTION 5: MANAGING DRIVES

Super and Regular Admins can remotely wipe, unlock, change the password, and disable access to drives. DUO drives also allow offline mode. Additionally, Admins can view users and settings on specific drives and the log, which displays the activity for that drive.

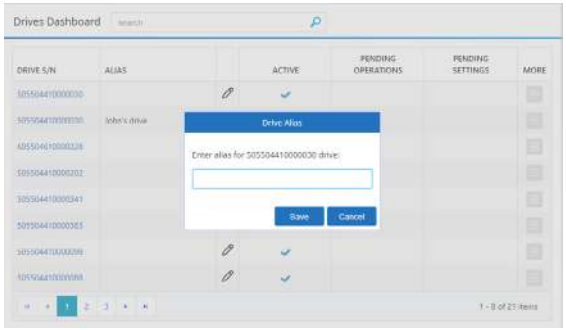
NOTE: All operations under this section are one-time and pending until a user opens the Managed app. In the Drives Dashboard, you can see their status in the Pending Operations column by hovering the cursor over the check mark.



NOTE: Drives from the list of available drives can be searched by Drive S/N and/or Alias.Drive S/N and Alias columns are sortable

Log in to **Remote Management** and click **Drives**.

Assigning or Editing Alias to Drives



To assign or edit alias of a drive, follow these steps:

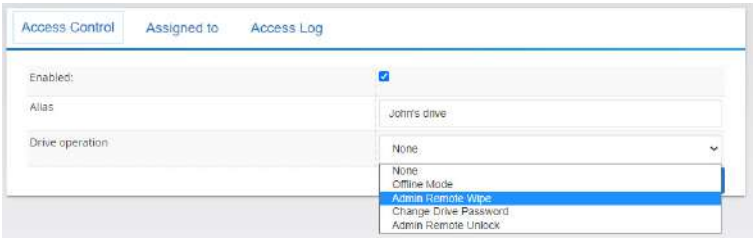
1. On the **Drives Dashboard**, find a drive
2. Click on the **pencil icon**
3. In Drive Alias dialog type the desired alias
4. Click **Save**

Remotely Wiping Drives

To remotely wipe a drive, follow these steps:

1. On the **Drives Dashboard**, select a drive from the **Drive S/N** column.

2. On the **Access Control** tab, in the **Drive Operation** row, click the dropdown and select the **Admin Remote Wipe** option.
3. Click **Save**.

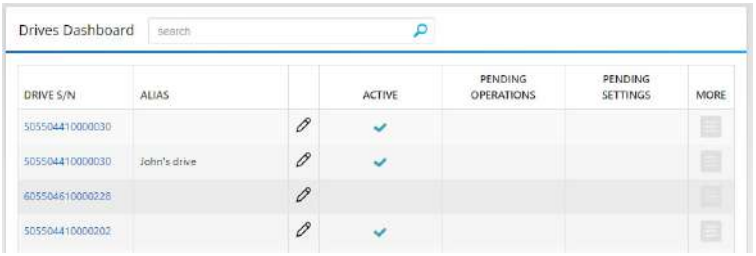


NOTE: Once the drive is connected and someone attempts to use it, its contents **will be deleted**.

Disabling Drive Access

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

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



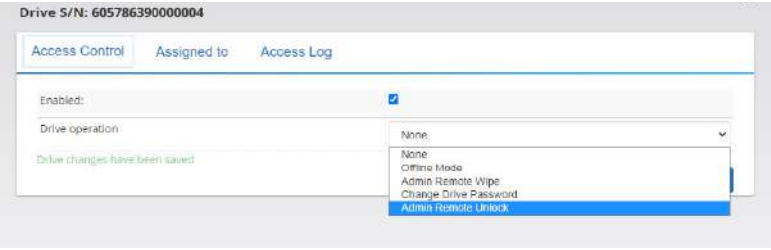
NOTE: On the Drives Dashboard, the drive will not display a checkmark in Active column.

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 **Drive S/N** column.
2. On the **Access Control** tab, in the **Drive Operation** row, click the dropdown and select the **Admin Remote Unlock** option.
3. Click **Save**.

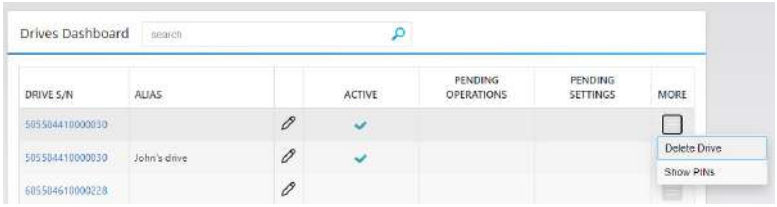


Deleting Drives

To delete a drive, follow these steps:

NOTE: It is recommended to back up all necessary data before deleting the drive.

1. On the **Drives Dashboard**, in the **More** column, click the menu.
2. Click **Delete Drive**.
3. On the **Delete Confirmation** dialog, click the **Delete** button.
4. If the drive is in use, an additional confirmation dialog appears. Click **Delete**.

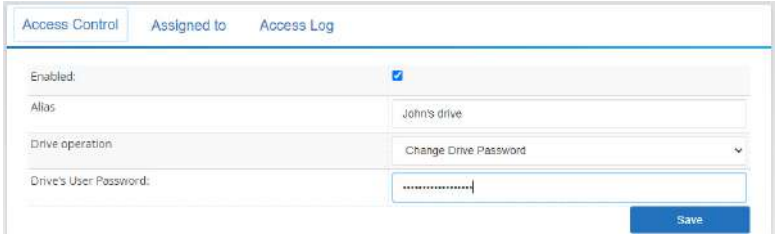


NOTE: Once complete, the drive is removed from the dashboard. To continue using the drive, it must be reprovisioned. This process removes all data from the drive. To use the drive without RM, disable the **RM Enabled** option during reprovisioning.

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 **Drive S/N** column.
2. On the **Access Control** tab, 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 (alphanumeric for BT and numeric for DUO).
4. Click **Save**.



Viewing Drive's Assigned Users

To view a drive's assigned users, follow these steps:

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

Viewing Access Log

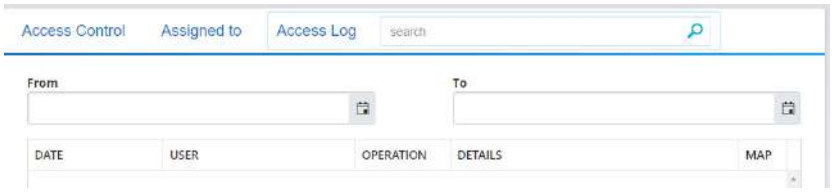
To view the access log for a drive, follow these steps:

1. On the **Drives Dashboard**, select a drive from the Drive S/N column.

NOTE: If a drive was not successfully unlocked, it appears highlighted in red with an exclamation point icon next to its serial number. Clicking on the drive takes you to the Access Log.

2. Click the **Access Log** tab.

NOTE: The log will display any operation with the date, time, user, type of operation, and the details. For ease of use, the Access Log can be searched by content and date range. The Date, User, and Operation columns are sortable for added convenience.



3. Click the icon in the Map column to view the location the drive was accessed at the time of logged operation.
   Details: The Access Log column indicates the status history of a drive.
   Successful – A user successfully unlocked the drive.
   Failed to unlock. x of 10 attempts remaining. – See how many attempts to unlock the drive remain. After 10 consecutive, unsuccessful attempts the user password will be removed and the drive becomes inaccessible to the user, however Admin can remotely unlock the drive and the User will be forced to create a new password. Alternatively, Admin can create a password through "Change Drive Password" in the Access Control tab.
   Drive is disabled – The drive cannot be unlocked if it was made inactive.

4. Show PINs

To see if a Self-Destruct and/or Recovery PIN is available for a drive, follow these steps:

NOTE: This is available only for SecureDrive DUO and SecureUSB DUO; SecureDrive BT and SecureUSB BT do not have this capability.

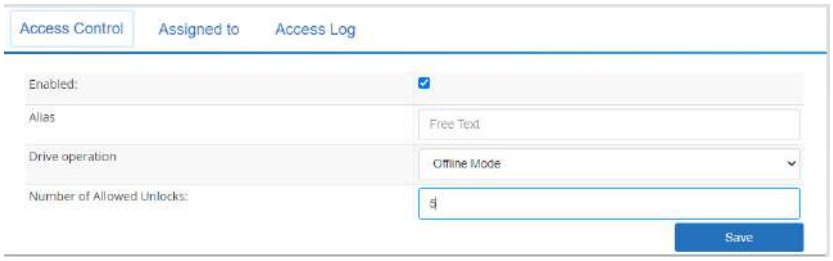
1. On the **Drives Dashboard**, find a drive in the **Drive S/N** column.
2. Click the gray box in the drive's row in the **More** column.
3. When the dialog pops up, click **Show PINs**.
4. You will see a box appear with the Self-Destruct PIN and/or Recovery PIN. If these have not been created yet, their respective fields read "**n/a**"

Offline Mode

Admin may set a number of drive unlocks via the onboard keypad.

NOTE: Offline Mode is available only for DUO drives. The user must connect to a drive using the Managed app in order to store offline counters in the DUO drive.

1. On the **Drives Dashboard**, select the drive in the **Drive S/N** column.
2. Under **Access Control**, select **Offline Mode** from the dropdown.
3. In the **Number of Allowed Unlocks** field, specify the number of times a user can unlock the drive via the onboard keypad.
4. Click **Save**.



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