

Remote Management by DATALOCK®

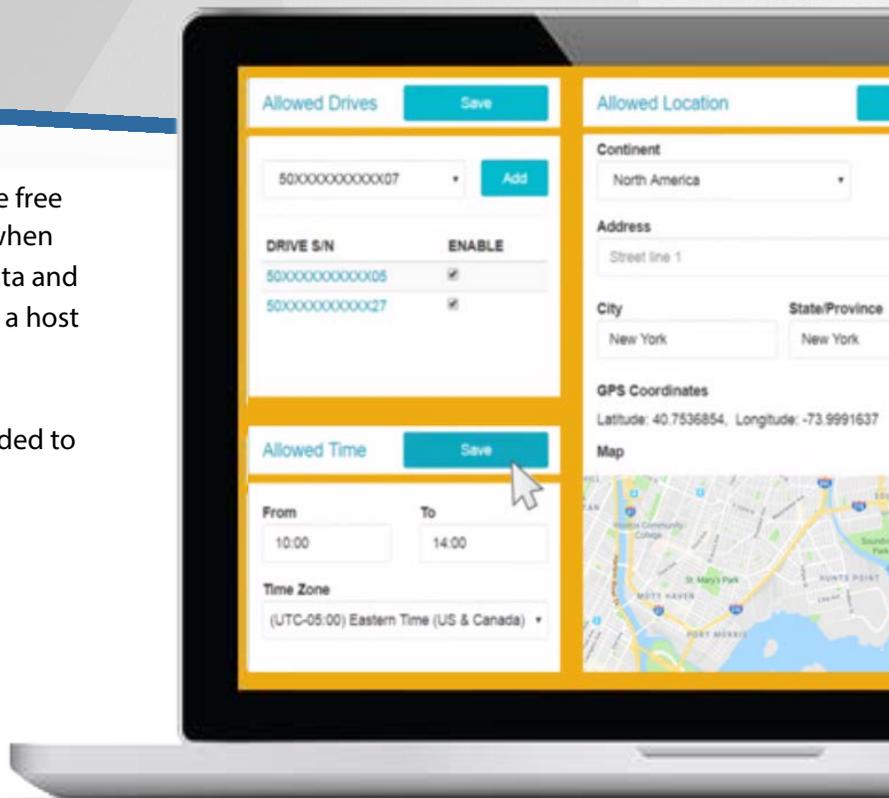
for SecureDrive® BT and SecureUSB® BT

The DataLock® Remote Management console is software free and allows the admin to take full control of where and when the drive can be unlocked, the ability to remote wipe data and disable access - even if the user has a drive pin. All from a host OS independent web console.

The DataLock® Remote Management console can be added to the SecureDrive® BT or SecureUSB® BT at any time.

Remotely enforce security policies:

- Where/When drives allowed to be used
- Wipe Drives or Disable access
- Remotely unlock/Force password reset
- Track and Manage unlimited number of drives



MAIN FEATURES



GEO-FENCING

The Admin for the account can limit access to the user by any of the following: (Continent, Country, Address, City, State or Zip Code). Once the geo-location is set, the fencing is complete by selecting the radius in KM/ MI. Geo-fencing is based on the precision of the GPS chips used in the mobile devices (vs. IP address-based geo-fencing used by competitors).



TIME FENCING

The Admin for the account can limit access for the user by setting start/end time limitations in any timezone.



DUAL FACTOR AUTHENTICATION

Unique dual factor authentication method via User Account and Drive PIN/Password combination. For managed drives, each user must have their own Username and password to access the DataLock® mobile app. Once authenticated the User must also possess the correct drive pin/password to unlock the device.



USER LOGGING

Each login is monitored and saved to show if the attempt was a success, as well as the date, time, and exact coordinates of the user.



REMOTE MANAGEMENT

ADDITIONAL ADMIN FEATURES



REMOTE WIPE

Admin Remote Wipe: remotely crypto-erases all data on the selected drive including the user's credentials.



REMOTE UNLOCK

Admin Remote Unlock: remotely unlocks the drive using the Admin's credentials.



PASSWORD CHANGES

Change User's Password: resets a user's password remotely. No data is lost.



DISABLE ACCESS

Admin can disable access to a drive even if the user has a drive PIN.

HOW IT WORKS

Step 1



Admin inputs command on Remote Management Web Console pertaining to a user/drive



Step 2



The command is sent in an encrypted signal from the server to the DataLock app



Step 3



User enters credentials into DataLock app to authenticate permission and unlock the drive



Step 4



DataLock app receives the admin command and transmits to the drive via encrypted Bluetooth signal



SECUREDATA, Inc.

3255 Cahuenga Blvd., West #111
Los Angeles, CA 90068, USA

Website: [securedrive.com](https://www.securedrive.com)

E-mail: support@securedrive.com

Toll Free: **1-800-875-3230**
International: **+1-323-944-0822**

