Remote Management by DATALOCK® for SecureDrive® BT and SecureUSB® BT

The DataLock® Remote Management console allows the admin to take full control of where and when the drive can be unlocked, the ability to remotely wipe data, and disable access - even if the user has a drive’s PIN. All from a web console.

For your convenience, add the DataLock® Remote Management console to the SecureDrive® BT or SecureUSB® BT at any time.

Remotely enforce security policies:
• Where/When drives allowed to be used
• Wipe Drives
• 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 an admin sets geo-location by selecting the radius (KM/MI) the fencing is complete. 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 time zone.

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

USER LOGGING
Admins can easily monitor all logins and unlock attempts. Admins also see the date, time, and exact coordinates of any login or unlock attempts.

Learn more at securedrive.com/rm
REMOTE MANAGEMENT

ADDITIONAL ADMIN FEATURES

REMOTE WIPE
Admin Remote Wipe: remotely crypto-erase 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