Remote Management
for SecureDrive® BT and SecureUSB® BT

The SecureData Remote Management console is software free and allows the admin to take full control of where and when the drive can be unlocked. They also have the ability to remotely wipe data and disable access, even if the user has a drive pin. All of these features are accessed from a host OS independent web console.

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

Remotely enforce security policies:
- Control where and when the drives can 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 user access 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 SecureDataLock® mobile app. Once authenticated the User must also possess the correct drive pin/password to unlock the device.

USER LOGIN
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.

Learn more at securedrive.com/rm. Call us at 1-800-875-3230.
Additional Admin Features

REMOTE WIPE
This feature remotely crypto-erases all data on the selected drive including the user’s credentials.

REMOTE UNLOCK
Using the Admin’s credentials, the drive can be remotely unlocked.

PASSWORD CHANGES
A User’s Password can be reset remotely without losing data.

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

How it Works?

STEP 1
Admin inputs command on SecureData Remote Management Web Console.

STEP 2
The command is sent in an encrypted signal from the Remote Management Web Console to the SecureData Lock Managed app.

STEP 3
User enters credentials into SecureData Lock Managed app to authenticate and unlock the Drive.

STEP 4
SecureData Lock Managed app receives the admin command and transmits it to the Drive via encrypted Bluetooth signal.

SecureDrive® Management via SecureData Remote Management Web Console