**WeGuard® Support**

# Device Security Features - What is WeGuard Admin lock functionality?
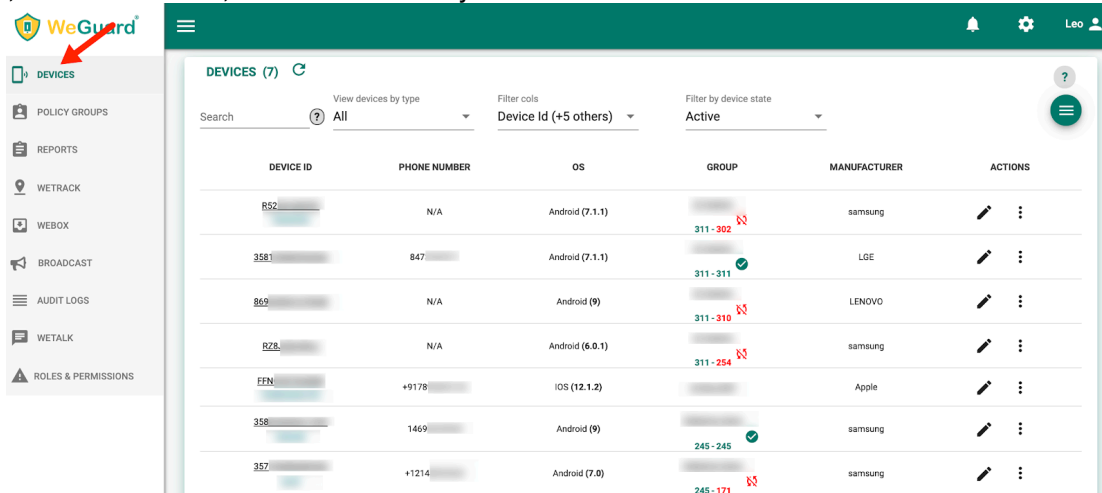
Hello and Welcome to WeGuard Enterprise Visual Knowledge-base Series.
In this KB article, We will explain about the Admin lock and how to use the functionality.

WeGuard adds one more "the most important security" feature to its wings. With "Admin Lock" functionality, devices enrolled in Kiosk or Work Managed policies can be locked down so that users may not use the device.

The assumption is, device/s enrolled with Kiosk or Work Managed policy.
- Login to WeGuard Console with valid credentials.
- Notice list of devices enrolled in the account. Refer to the picture below.
- However, for the first time, there won't be any devices. You will see tutorial videos on how to enroll a device.
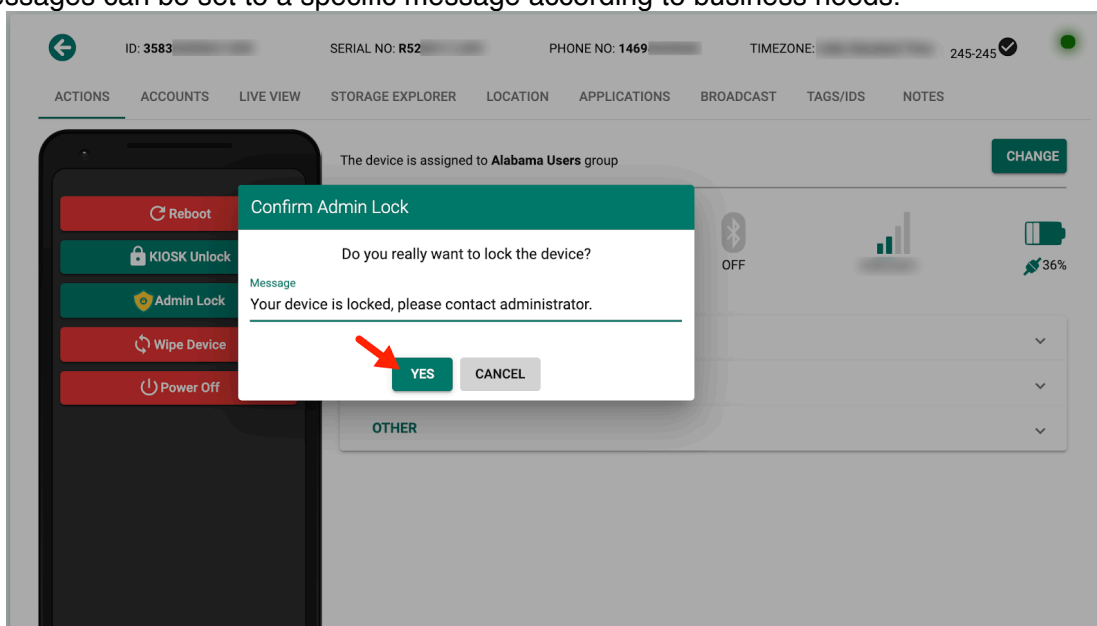


- To lock a desired device, click on DeviceID or edit button (pencil like) in actions column

- Notice the "Admin Lock" button along with other buttons in the device details page.
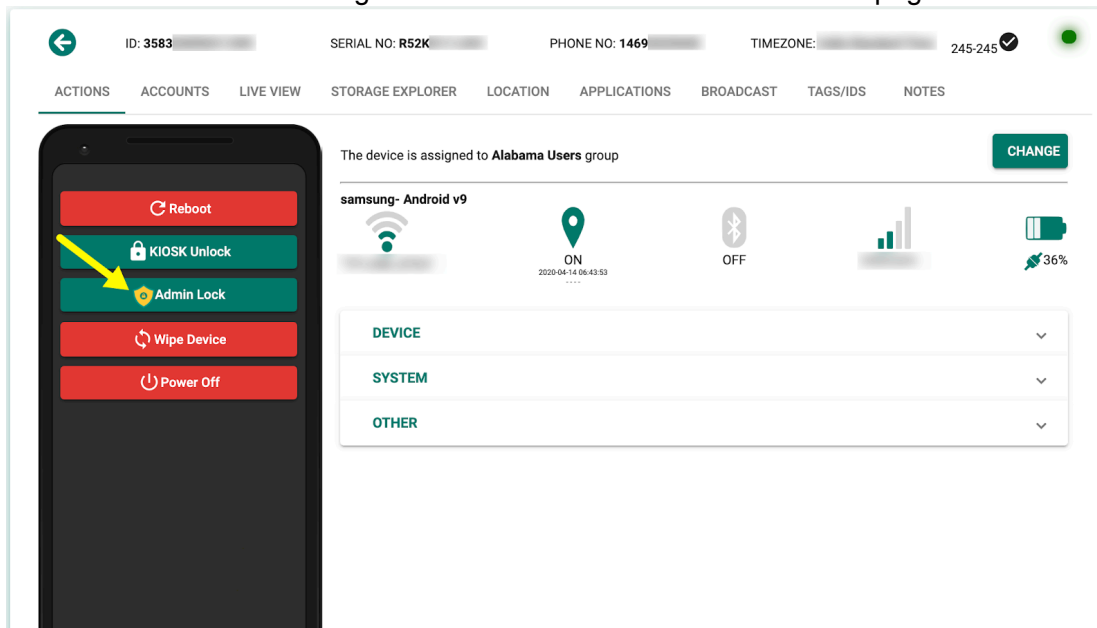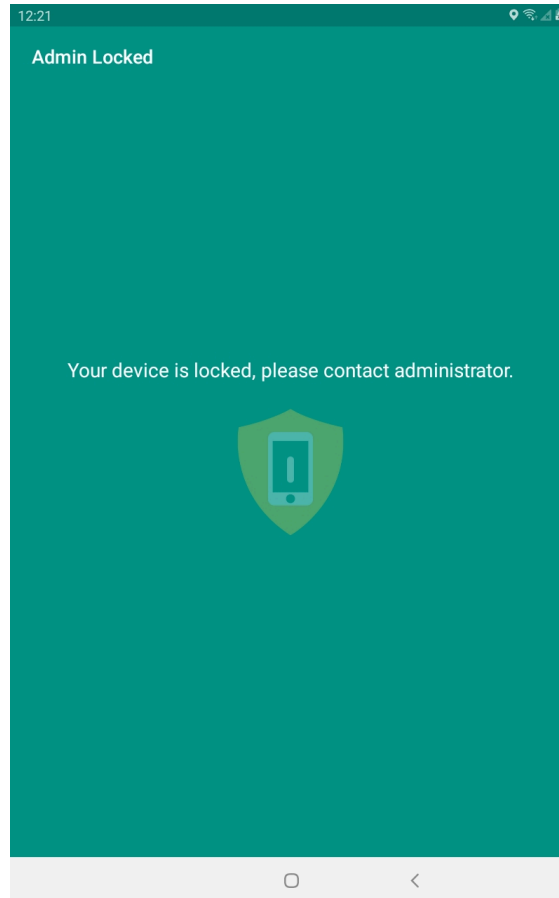


- Clicking on the "Admin Lock" button will prompt for confirmation along with a lock message.
- Lock messages can be set to a specific message according to business needs.



- Click on "Yes" to lock the device. Refer to below picture of the device after issuing "Admin Lock"

- Once the device is locked, mobile users will not be able to use the device any more.



- Further, notice the label of the button changes to "Admin Unlock".
- To unlock the device, click on "Admin Unlock".

📄 Note : For Kiosked devices, you will notice the Kiosk lock/unlock button. Once admin lock is issued, kiosk lock/unlock will be disabled as it won't be of any use.
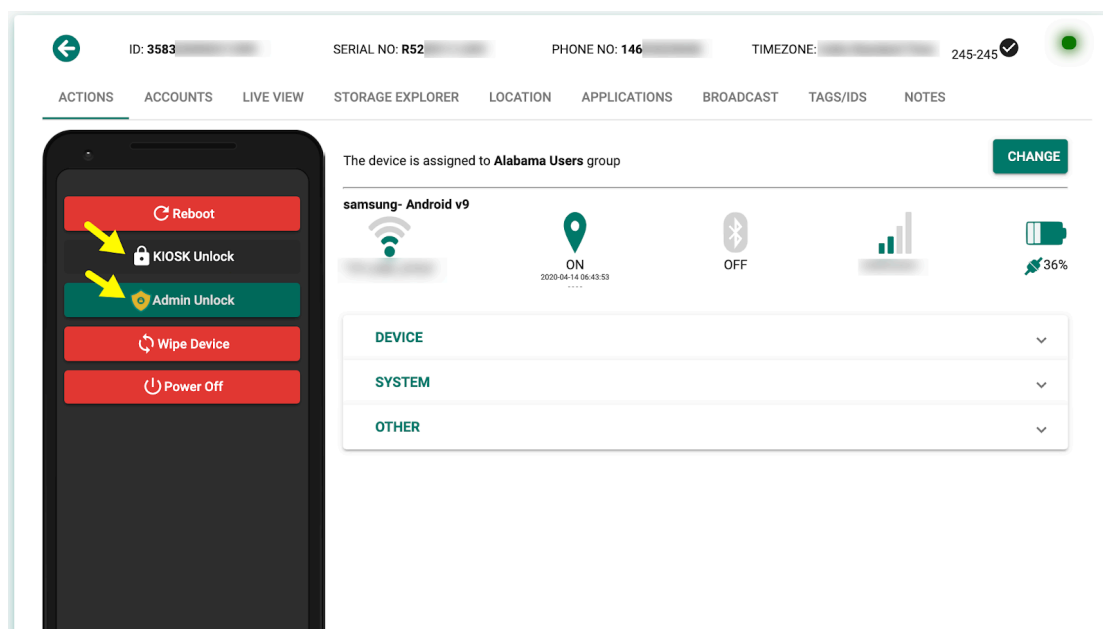


We hope this article was useful. Thank you for reading.

For more WeGuard insights, please explore the Visual Knowledge-base Series
For more details, please do visit https://www.weguard.com
If you need any help on this, do call up WeGuard Support +1 833-936-2253 or contact WeGuard Support Email

https://support.weguard.com/portal/en/kb/articles/device-security-features-weguard-admin-lock-functionality