

Admin Guide

Aegis Secure R51 - Enhanced ReTransmission Device
Release 5, Nov 15, 2023



Enhanced ReTransmission Device
(ERD)

Prepared by: Cog Systems, Inc.

Classification: UNCLASSIFIED

Distribution: DISTRIBUTION LIMITED TO U.S. GOVERNMENT AGENCIES ONLY.

Overview

Welcome to the future of Ultra Secure Mobility with the Aegis R51 ERD.

This is the administrator guide for the Aegis R51 ERD – Production edition, Release 5. It explains how to manage the device including the physical connections available, device status via LED ring, power management, administration portal connectivity, and how to use the device with an EUD (end user device).

Contents

OVERVIEW.....	1
CONTENTS.....	1
FIGURES.....	2
CHANGE RECORD.....	3
DESCRIPTION.....	4
PHYSICAL CONNECTIONS.....	4
CHARGING THE ERD.....	5
CONNECTING THE POWER FOR EUD AND ERD.....	5
CONNECTING AN EUD.....	6
CONNECTING TO THE ADMIN PORT.....	6
POWER MANAGEMENT.....	7
POWERING THE ERD ON.....	7
POWERING THE ERD OFF.....	7
BOOT PROCESS TIMELINE.....	8
ADMIN PORTAL.....	9
DEFAULT ACCOUNTS.....	9
LOGGING IN.....	9
CHANGING ACCOUNT PASSWORD.....	10
CONNECTING TO WI-FI NETWORKS.....	11
CONNECTING TO HIDDEN WI-FI NETWORKS.....	12
CONNECTING TO CELLULAR NETWORKS VIA ESIM ACTIVATION.....	13
USERS TAB (ADMIN ONLY).....	14
Delete a User.....	14

<i>Add a User</i>	14
FIREWALL TAB (ADMIN ROLE ONLY)	15
<i>Toggle Whitelist On/Off</i>	15
<i>Toggle IPsec Rule On/Off</i>	15
<i>Add a new rule to the Firewall</i>	16
<i>Resetting Firewall Whitelist</i>	16
LOGS TAB (ADMIN ROLE ONLY)	17
SETTINGS TAB	17
<i>General Settings</i>	17
<i>DHCP Settings</i>	18
<i>Export Settings</i>	18
<i>Import Settings</i>	19
UPDATE TAB (ADMIN ROLE ONLY)	20
STATUS LIGHTS.....	20
REPORTING ISSUES	22

Figures

Figure 1: View of ERD case USB ports.....	4
Figure 2: Rear of Case showing magnet/Velcro	6
Figure 3: Physical Buttons.....	7
Figure 4: Dashboard Tab	9
Figure 5: Settings Tab - Change Password	10
Figure 6: WIFI Tab – Connect to Network	11
Figure 7: WIFI Tab – Connect to Hidden Network	12
Figure 8: : Cellular Tab – eSIM Profiles	13
Figure 9: Users Tab	14
Figure 10: Firewall Tab	15
Figure 11: Logs Tab	17
Figure 12: Settings Tab - General Settings	18
Figure 13: Settings Tab - Import/Export Settings	19
Figure 14: ERD in case showing status lights.....	20
Figure 15: Status Lights flow chart	22

Change Record

Date	Author	Version	Changes	Approved by
07-21-2021	Rupert Young	1.0	R51 Admin Guide Prototype Edition, Release 1	Carl Nerup
08-05-2021	Rupert Young	1.1	R51 Prototype Edition Release 2	Carl Nerup
09-15-2021	Rupert Young	1.2	R51 Prototype Edition Release 3	Carl Nerup
30-04-2022	Jason Sebranek	2.0	R51 Production Device Release 4	Carl Nerup
15-11-2023	Stephen Burke	2.1	R51 Production Device Release 5	Carl Nerup

Description

The Aegis Secure R51 takes a commercially available Retransmission Device (RD), the RelayGo Relay+, and converts it into a compliant Enhanced ReTransmission Device (ERD) when used in its case. The case attaches the ERD to a range of End User Devices (EUDs) with three USB-C ports and an integrated USB Mux to control power and data flows per requirements.

The ERD enables any EUD (mobile phone, tablet, or computer) to safely connect to any mobile or Wi-Fi network.

Physical Connections

The R51 is designed to be used when properly seated in its case. The case has three USB ports as shown in the picture below. below.



Figure 1: View of ERD case USB ports

The left port is the Charging port. The middle port is the EUD port and is the primary data connectivity port. The right port is the Administration (Admin) port.

Charging the ERD

The ERD has a relatively small battery that needs to be charged enough to ensure a successful boot (25% when plugged in). Once the device is booting, the ERD will charge from the attached EUD.

NOTE: If charging from a completely dead battery with the cable plugged into the USB-C charging port, the device will wait until the battery reaches 25% to start booting. There will be red low battery lights that illuminate as the battery charges with the last one blinking to indicate charging.

Connecting the Power for EUD and ERD

1. Plug in a USB charging cable to the Charging port.
2. Both the ERD and the EUD will charge.
3. When connected ERD will draw power from EUD.
4. The case blocks data from flowing to either device through the charging port.

NOTE: EUD will not charge when using OTG cable (known bug).

NOTE: The included ERD charger from the RD, may fail to charge larger devices depending on the power requirements of the EUD. Please instead use the charger that came with the EUD or another smart phone.

Connecting an EUD

The ERD is designed to support any EUD; however, only Mac (running Linux) and PC laptops, and Samsung S20s have been verified as EUDs at this time.

1. With a laptop, any USB cable can be used to connect to the EUD port.
2. **NOTE:** When using a Samsung S20 (known bug), please use an On the Go (OTG) cable to allow the S20 to act as a host device for the ERD. In future, the included short USB cable can be used. When using an OTG cable EUD will not receive power from the power port.
3. For other devices, try a regular USB and then an OTG cable. Please report any device that does not work with either.
4. To use the magnet on the back of the case, attach the included strike plate to the back of the EUD or attach the Velcro backing.



Figure 2: Rear of Case showing magnet/Velcro

Connecting to the Admin port

1. Any device or USB cable can be used when using the Admin port.
2. Plug in the device to use the Admin port.
3. When connecting a device to the Admin port, the ERD will give that device exclusive data access to the ERD even if a different EUD is also connected at that time.
4. The Admin port can be used to charge the ERD from dead (no battery charge).

Power Management

Since the ERD is a small form factor device the battery capacity is relatively small. Once the ERD is connected to an EUD the device will draw power from that device allowing it to run while charging in almost all cases and make worrying about the charge percentage a non-issue. The power switch is the + plus button on the ERD and the – minus button is the shut off button.

Powering the ERD On

1. ERD is charged
2. When plugged into power the device will try to boot given the battery is $\geq 25\%$
3. If unplugged & ERD is off: press and hold the **+ button** on the top of the ERD for ~5 sec until it vibrates. The device will turn on & start booting. The LED ring should spin white indicating booting & breathe green when the Admin Portal is available.
4. If unplugged & ERD is on: press and hold the **+ button** on the top of the ERD for ~15 sec until it vibrates. This will reboot the device. The LED ring should spin white indicating booting & breathe green when the Admin Portal is available.

NOTE: The round button (assistant button) is not active in this version of software.



Figure 3: Physical Buttons

Powering the ERD Off

1. Unplug the power cord from the ERD.
2. Hold the minus button down as red lights illuminate and after 3 seconds the device will vibrate indicating it is shut down.

Boot Process Timeline

The ERD's LED ring shows the status during the device boot. The following steps will outline the approximate timeline and indicators that the user is given.

1. 0 seconds. Power on, indicated by vibration. Happens when the + **button** is held or when a USB is plugged into a powered off ERD.
2. 15 seconds. Android boot in process, indicated by spinning white LED turning on.
3. 60 seconds. LED ring will breathe green 3 times indicating the device is done booting and Admin Portal is available.

NOTE: Once the ERD is booted the following states are observed on the EUD shortly after the 60 second mark.

1. Notification of new (unrecognized) USB device on EUD or Admin device.
2. EUD or Admin device recognizes ERD as Qualcomm Android device
3. EUD or Admin device recognizes new wired connection indicating USB tethering is enabled.
4. Internet access. End-to-end connection alive assuming Wi-Fi or LTE setup on the ERD previously.
5. ERD boot complete! Indicated by spinning white LED turning off & the LED ring breathing green 3 times. The Admin Portal is now available via the EUD. LED status button is now available to show battery, Wi-Fi, and LTE statuses.

NOTE: [Aegis Admin Portal Link](#)

To confirm successful boot, open a web browser on the EUD and navigate to the Aegis Admin Portal at <http://192.168.42.129:8081>. The user should be met with the Admin Portal Dashboard showing Battery, Wi-Fi, and LTE statuses.

Admin Portal

When first used the user and administrator profiles are defined, and password protected. Administrator profiles can create multiple admin and user profiles for a single device and change user profile passwords.

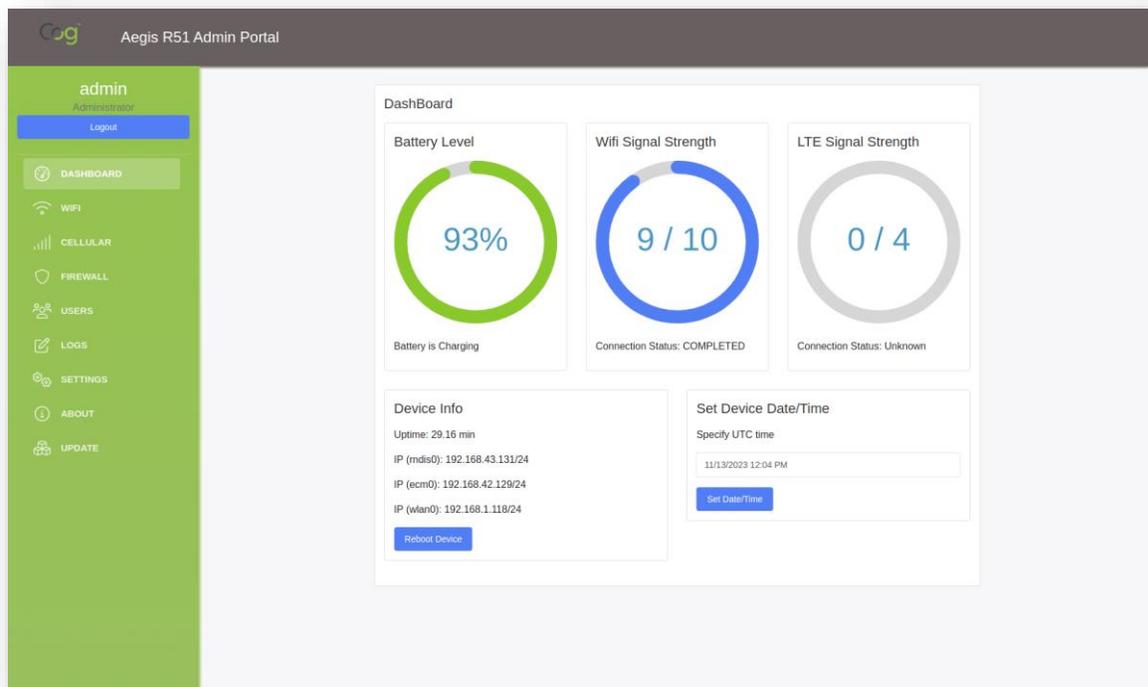


Figure 4: Dashboard Tab

Default Accounts

Username: **admin**
Password: **password**

Username: **user**
Password: **password**

An end user access is limited to accessing the Dashboard, the Network tab to configure additional Wi-Fi and Cellular networks, the Settings tab to change their password, and the About tab to find links to documentation.

Logging In

The Dashboard tab is available without logging in. Other tabs require login to a user or admin profile. Once logged in, access to other tabs is based on the profile type. The directions below assume the user is logged in. Once logged in, status will be stored until web browser is refreshed or the cache for the site is cleared. Additional user accounts can be added by an admin user.

Changing Account Password

The following steps will walk the user through changing their account's password. The following figure shows the Settings tab when a user with administrator access is logged in.

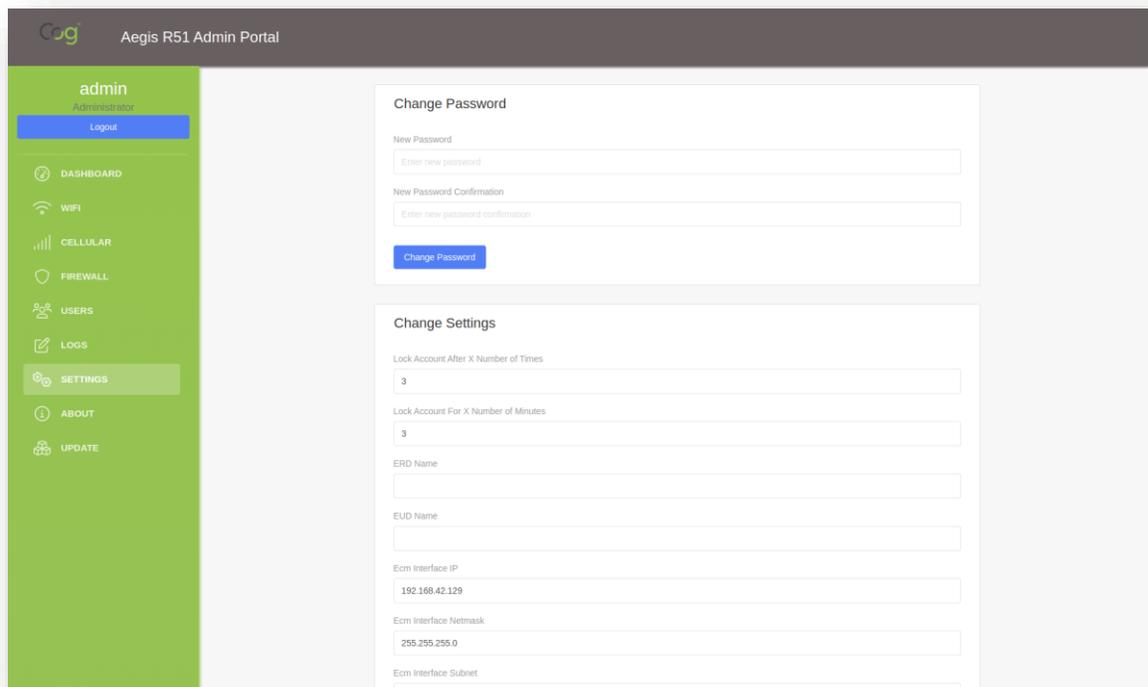


Figure 5: Settings Tab - Change Password

1. Click on **Settings** tab
2. Notice the **Change Password** section
3. Type in new password (must be ≥ 14 characters long and include at least one of each of the following characters: lowercase, uppercase, symbol, and a number). Will provide error message if it does not match password requirements.
4. Type in **New Password Confirmation** again to confirm
5. Click **Change Password**

Connecting to Wi-Fi Networks

The following steps will walk the user through connecting to a Wi-Fi access point. The following figure shows the Wi-Fi tab where a user can select an existing Wi-Fi access point or connect manually to a broadcasting or hidden access point. After the Wi-Fi network is added, various properties will become available for review. The Wi-Fi network will be saved in the system after being added and will automatically connect in the future.

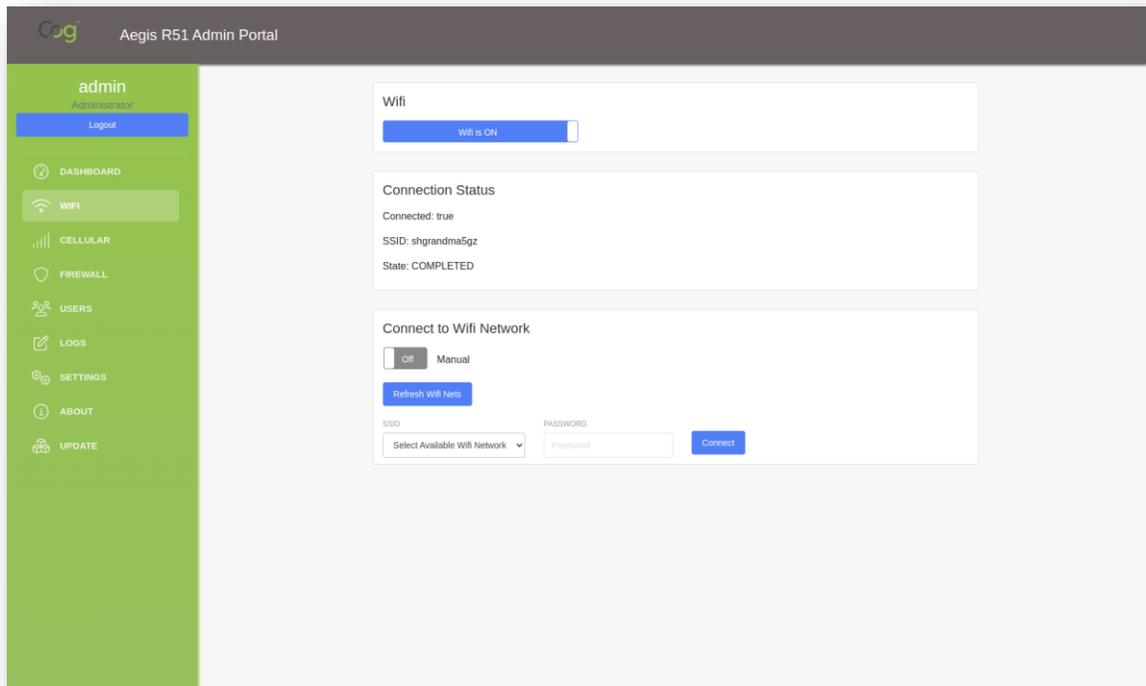


Figure 6: WIFI Tab – Connect to Network

1. Select **WIFI** tab in the side menu
2. Turn on **WIFI** with **Wifi is ON** switch
3. Click **Refresh Wifi Nets** so the device will scan for Wi-Fi networks
4. In the **Connect to Wifi Network** section choose the Wi-Fi network SSID from the drop down menu and enter the **Password**. Depending on your Wi-Fi router you may have to click multiple times on **Refresh Wifi Nets** to show all networks.
5. Click **Connect**

Connecting to Hidden Wi-Fi Networks

To connect to a hidden Wi-Fi network, the hidden check box needs to be checked.

1. Turn on **WIFI** with **Wifi is ON** switch
2. In the **Connect to Wifi Network** section click the check box for **Hidden SSID** if the network is not broadcasting its SSID.
3. Choose the **Security Mode** (WPA2 and None are supported) from the dropdown menu.
4. Type in the **SSID**
5. Type in the **Password**
6. Click **Connect**

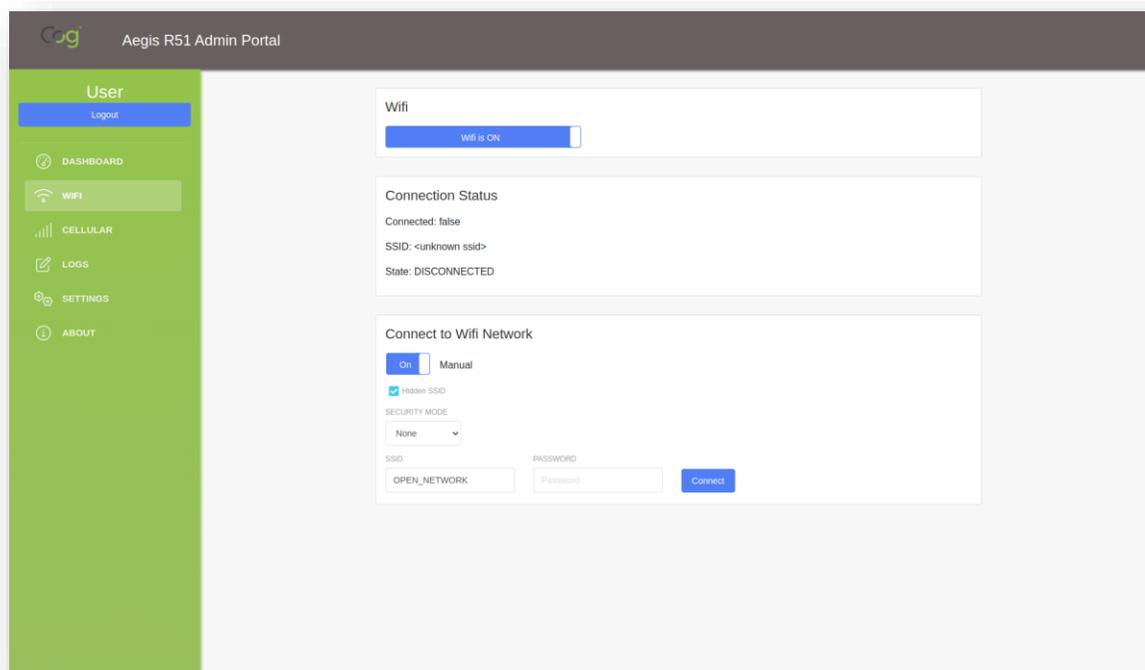


Figure 7: WIFI Tab – Connect to Hidden Network

Connecting to Cellular Networks via eSIM Activation

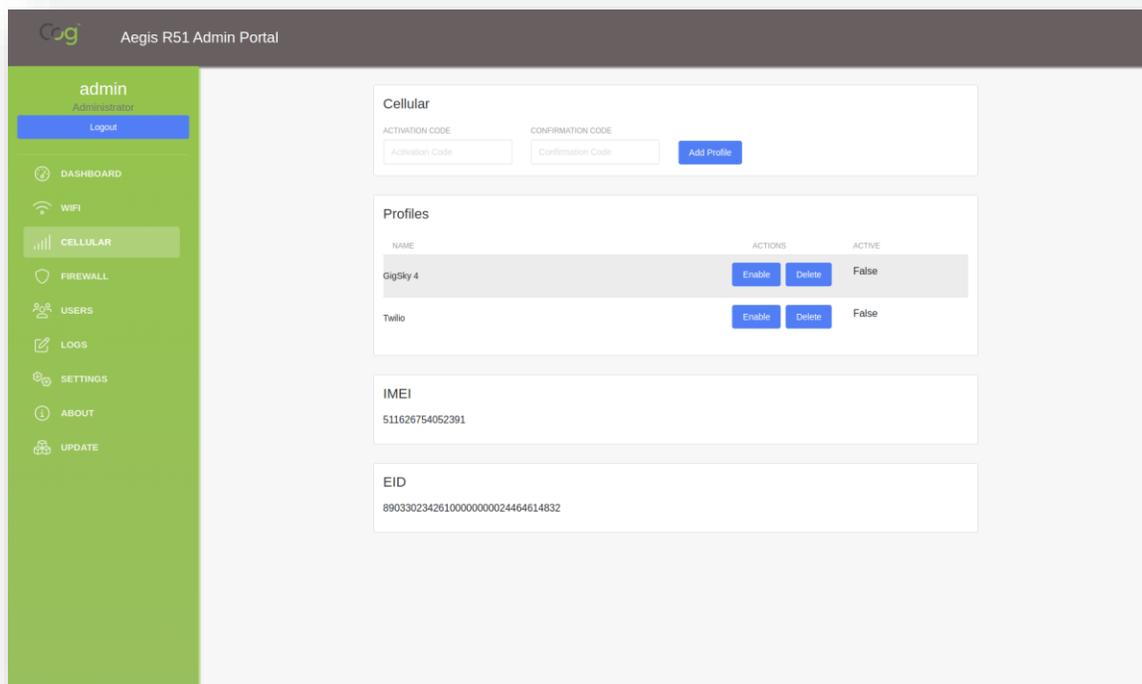


Figure 8: : Cellular Tab – eSIM Profiles

NOTE: Requires support from the carrier. This support is typically configured by the eSIM vendor or specified in their web portal when an account and eSIM are purchased. The ERD has been tested with AT&T, Twilio, and IDSecure. In the case of aggregators such as Twilio & IDSecure their back end will determine what cell network is available and connect accordingly based on the location and other factors.

1. User looks up and records the ERD IMEI. It can be viewed from the **CELLULAR** tab in the Admin portal. Alternatively, the ERD IMEI is printed on the back of the ERD (visible when out of case).
2. Carrier representative provides the eSIM (likely as an eSIM QR code card.)
3. Carrier representative will connect the eSIM to the ERD IMEI in their systems.
4. Assumes Admin device is plugged-in via usb into the Admin port
5. Select **CELLULAR** tab in the side menu
6. Enter the **Activation Code** of the eSIM. If the eSIM has a QR Code use this site to extract the activation code from an image of the QR Code. It should look something like this:
LPA:1\$cust-001-v4-prod-atl2.gdsb.net\$A4412879E6202C6EA71CC8D79D083D86
7. **Confirmation Code** is optional and can be left empty.
8. Click **Add Profile**
9. A spinner will appear until the eSIM profile appears in the list. Multiple eSIM profiles can be kept for use in the device.

10. Enable the eSIM profile by clicking the **Enable** button. The active profile shows **True** in the **Active** column when activated and will be highlighted green. After LTE is connected, the data connection's properties can be viewed in the profiles table entry.

NOTE: If Wi-Fi and LTE are active at the same time, the ERD will default to Wi-Fi.

Users Tab (Admin only)

To review user and admin accounts, navigate to the Users tab. This will present a list of users on the device, whether they are an admin or regular user profile and allow any profile to be deleted except the current profile being used. Shown below is an example Users page.

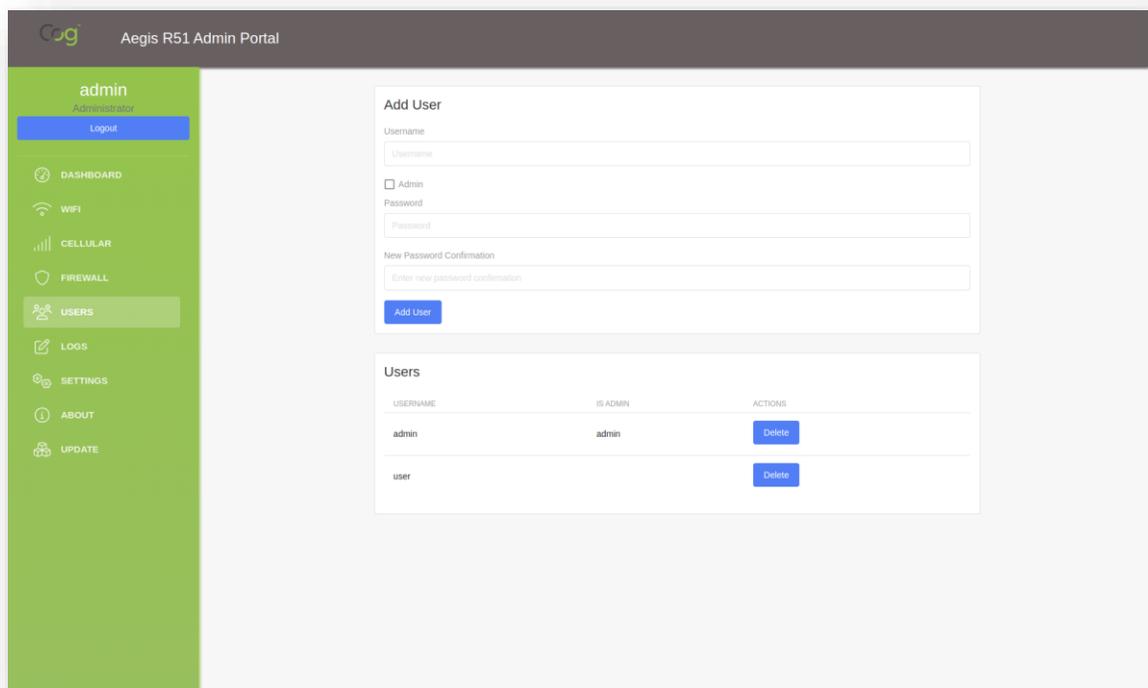


Figure 9: Users Tab

Delete a User

1. Click the **Delete** button under the **Actions** column

Add a User

1. Click on **USERS** tab on sidebar
2. Enter the new **Username** and **Password**. Type in a new password (must be ≥ 14 characters long and include at least one of each of the following characters: lowercase, uppercase, symbol, and a number). Will provide error message if it does not match password requirements.
3. Select **Admin** checkbox to control whether profile is a regular user or admin user

4. Click the **Add User** button
5. User will be added to the list below

Firewall Tab (Admin role only)

The Firewall tab allows for rules to be added to the firewall for traffic to be matched against. The firewall used by the ERD is *iptables* hence the usage of the filter table chains. Most rules will need to be added to the FORWARD_WL chain which is created by the ERD and used for forwarded traffic through the ERD. The INPUT and OUTPUT chains can be added to but will likely not be needed since ERD traffic is typically forwarded traffic from an EUD to an endpoint and back.

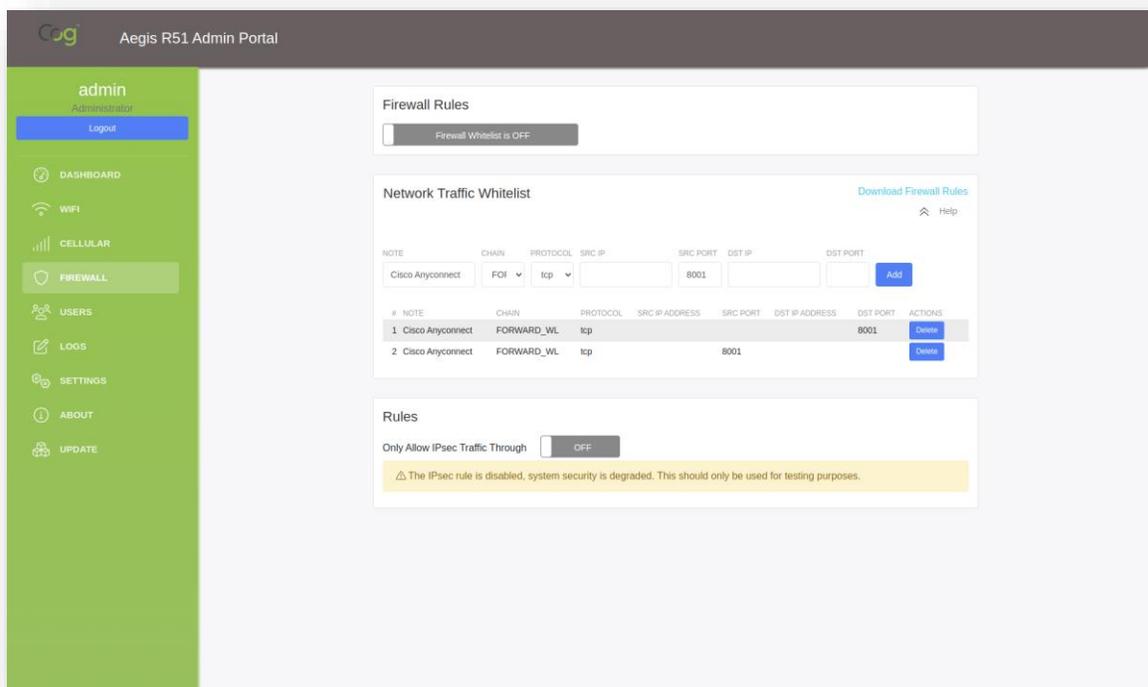


Figure 10: Firewall Tab

Toggle Whitelist On/Off

1. Click **Firewall Whitelist** switch to turn it on/off
2. This enables the FORWARD_WL chain so traffic is matched against rules in that chain. If the Whitelist is enabled, the default policy of the FORWARD_WL chain is DROP and rules need to be added to punch through the firewall, so the traffic is ACCEPTED.

Toggle IPsec Rule On/Off

1. Click **Only Allow IPsec Traffic Through** Switch to turn it on/off

2. This matches and allows only IPsec traffic through the firewall. Admin portal access is also allowed through the firewall.

Add a new rule to the Firewall

1. Clicking on the **Help** link in the top right corner of the **Network Traffic Whitelist** shows common rules to add for forwarded traffic such as connecting to a VPN endpoint needing a particular port open for example.
2. Fill in the following entries for a Firewall rule:
 - Note (descriptive text for administrative purposes)
 - Chain
 - FORWARD_WL (src & dest IP are not the ERD)
 - INPUT/OUTPUT (src or dest is the ERD)
 - Protocol (TCP or UDP)
 - Source IP Address
 - Source Port
 - Destination IP Address
 - Destination Port
3. Click **Add** button

NOTE: Not all the firewall fields need to be filled out for the rule to be added. Use the [Download Firewall Rules](#) link to inspect any rules that are added.

Resetting Firewall Whitelist

Resetting the Whitelist will remove all entries from the FORWARD_WL chain and reset it to default, which is off. The entries are shown on the Firewall page.

1. Click **SETTINGS** Tab
2. Scroll down to **Reset Firewall Whitelist** Section
3. Click **Are you sure?** Switch
4. Click **Reset Whitelist**

Logs Tab (Admin role only)

The device captures logs of all admin changes, user logins as well as firewall events. To see a list of available logs:

1. Click **LOGS** Tab on the Sidebar

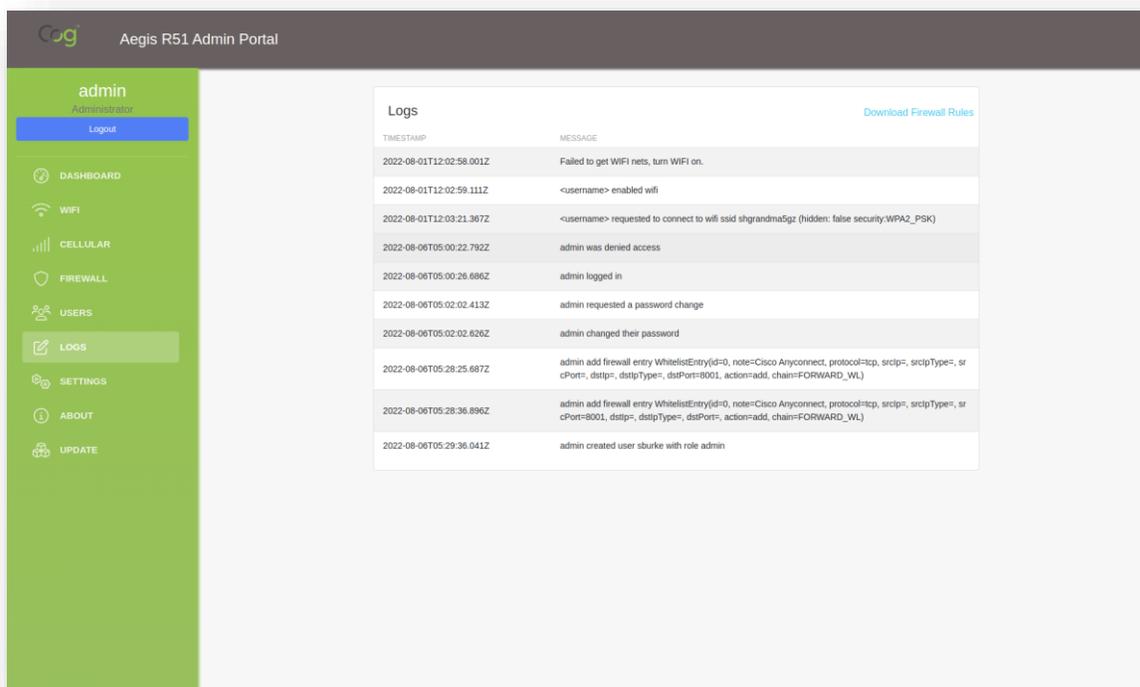


Figure 11: Logs Tab

Settings Tab

The following settings are available to change. Once changed via the edit boxes, click the Save Settings button to persist the changes on the ERD.

General Settings

These settings apply to the Admin Portal Account Locking feature as well as how the network interfaces will be setup on the ERD. This allows for changing the IP and subnets so that it can integrate into other network setups that require the use of specific subnets.

- Lock Account After X Number of Times
- Lock Account For X Number of Minutes
- ERD Name (administrative purposes)
- EUD Name (administrative purposes)
- Ecm Interface IP

- Ecm Interface Netmask
- Ecm Interface Subnet
- Rndis Interface IP
- Rndis Interface Netmask
- Rndis Interface Subnet

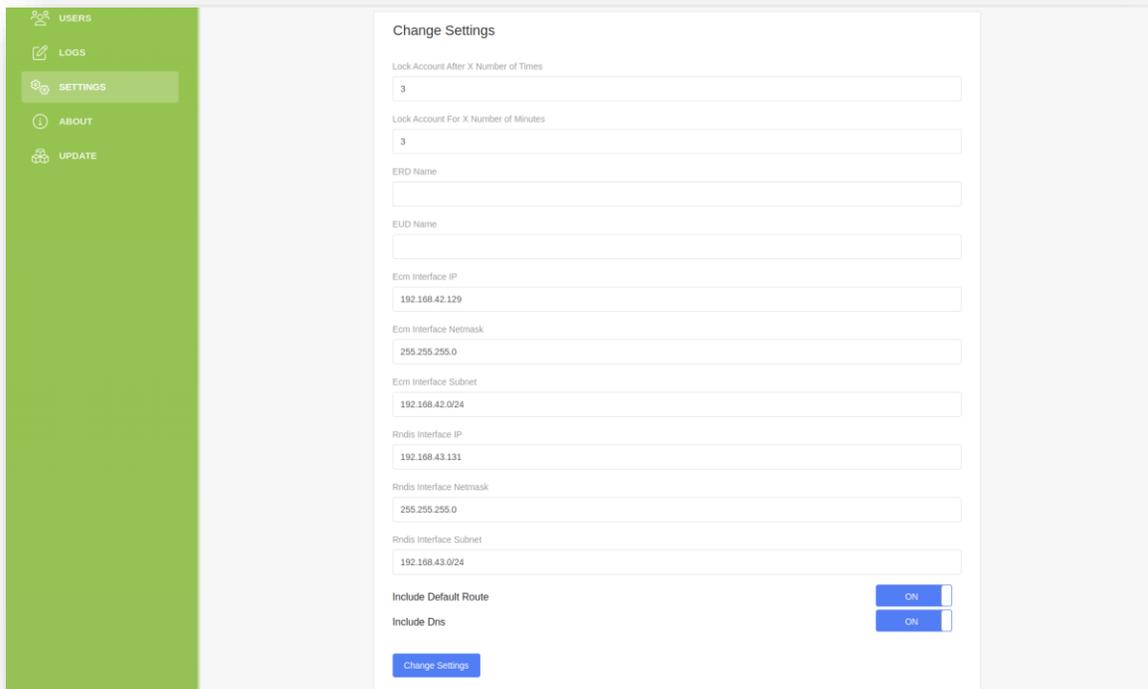


Figure 12: Settings Tab - General Settings

DHCP Settings

These settings refer to fields in the DHCP response that is sent to the EUD when it is connecting to the ERD. Typically, a user should keep these defaulted to ON unless there is a local DNS server. In the case of a local DNS server, a user may want to ignore the ERD DNS settings to integrate with their local network setup.

- Include Default Route
- Include Dns

Export Settings

The ERD can be backed up by exporting the settings from the device via the Export R51 Settings Section as follows.

NOTE: The zip file contains plaintext passwords so secure the zip file as if it was key material.

1. Specify a Wi-Fi net to save (SSID, Password, Hidden, Security Mode)

2. Specify an **Admin Password** to save
3. Click **Export**
4. The exported zip file will be saved where your browser typically saves files

Import Settings

All the General Settings, Users, Firewall, Logs, Wifi Net, and Admin password are imported on the device.

1. Click **Choose File** button to upload the exported zip file.
2. Click **Import**
3. Reboot the device

The screenshot shows a web interface with three main sections:

- Reset Firewall Whitelist:** A blue button labeled "Reset Whitelist" is next to a grey button labeled "Are you sure?".
- Import R51 Settings:** A text input field labeled "EXPORTED ZIP FILE" contains the text "Choose File" and "No file chosen". Below it is a blue button labeled "Import".
- Export R51 Settings:** This section contains several input fields: "WIFI SSID", "WIFI PASSWORD", a checkbox for "Hidden SSID", a dropdown menu for "SECURITY MODE" (currently showing "WPA2_PSK"), and "ADMIN PASSWORD". A blue button labeled "Export" is at the bottom.

Figure 13: Settings Tab - Import/Export Settings

Update Tab (Admin role only)

The update tab allows for updating the device with an OTA (over the air) package that contains a new device flash.

NOTE: This wipes the device of all user data and updates to the build specified via the zip file.

1. Click **Choose File** to upload an OTA zip
2. Click **Upload OTA Package**
3. The zip file is transferred to the device
4. The OTA package digital signature is verified
5. The device reboots & the ring light spins white
6. The device is updated & reboots when it is done
7. Finally, the ring light will breathe green 3 times to indicate the boot is finished and the admin portal is available.

Status Lights

To check the status of the ERD, press the button in the middle of the case. It is surrounded by a ring of lights that changes color to show the status.



Figure 14: ERD in case showing status lights

The following list details the status reporting cycle:

1. First press displays Battery charge level and charging indication (red or green LEDs).
2. Second press displays Wi-Fi status and signal strength (blue LEDs).
3. Third press displays LTE status and signal strength (orange LEDs).
4. Additional presses repeat the cycle.
5. The LEDs will timeout after 15 seconds if the button is not pressed again.

Battery status:

- The number of LEDs indicates the current charge percentage level from 0 to 100%.
- If the device is charging the next LED to 'fill' in the battery charge level will blink.
- Red LEDs indicate low battery (less than or equal to 25%).

Wi-Fi status:

- The number of LEDs indicates the current signal strength percentage level from 0 to 100%.
- A single LED indicates the Wi-Fi is disabled.

LTE status:

- The number of LEDs correlates to signal coverage bars. Four bars, or 12 LEDs, is the maximum signal strength.
- A single LED indicates it is searching for coverage.

The following figure shows the status reporting cycle:

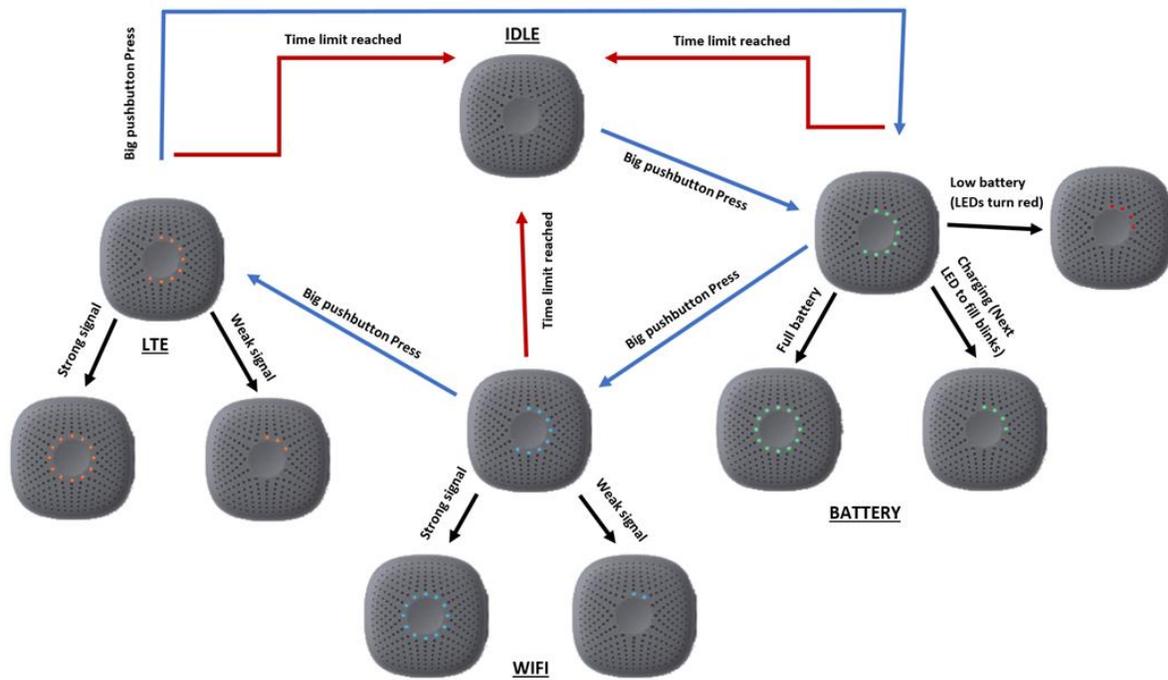


Figure 15: Status Lights flow chart

NOTE: The button may have a slight lag to display the status because pressing it will poll the API for updated values.

Reporting Issues

Please report any issues discovered while using the ERD or this guide to Aegis so it can be corrected in a future release.