10

WanderGuard BLUE Manager

WanderGuard BLUE Manager is a STANLEY Healthcare mobile application installed on a STANLEY Healthcare-approved Tablet. The Tablet is supplied by STANLEY Healthcare as an integral component of and specifically for use with the WanderGuard BLUE Solution. The main function of the WanderGuard BLUE Manager is to enable Controller configuration by downloading /uploading configurations from/to the Controller and displaying the status of Bracelets and Controller(s).

Starting at v1.5, the Controller also supports DC1000, GW3000, and GW3100 configuration.

Note

To modify a Controller configuration, the WanderGuard BLUE Manager first downloads the configuration from the Controller. The configuration settings can then be modified within WanderGuard BLUE Manager and uploaded to the Controller.

WanderGuard BLUE Manager runs on an off-the-shelf STANLEY Healthcare-approved Asus or Lenovo Tablet for WanderGuard BLUE.

The Tablet:

- Supports scanning for Bracelets, Controllers, and Gateways
- Displays status of Bracelets, Controllers, and Gateways
- Enables configuration of Controller and Gateway settings
- Enables configuration of user credential information stored on the Controller
- Supports up to 1,000 users including import and export options
- Displays the Keypads that are connected to the Controller (number of each Keypad)

The Tablet supplied by STANLEY Healthcare is an 8-inch Asus ZenPad Z380M Tablet with 2 GB RAM and 16 GB storage OR 8-inch Lenovo Tab 4, ZA2B0009US, Quad-Core Processor, 1.4GHz, with 16 GB storage OR Lenovo M8, ZA5G0060US, 2GHz, 32GB Storage.

Best Practice: Using any Tablet or software other than that supplied by STANLEY Healthcare automatically voids any warranty that you may have received from STANLEY Healthcare and absolves STANLEY Healthcare of any damage that may be caused to your systems resulting from its use.

Getting Started with Your Tablet

STANLEY Healthcare supplies the Tablet with the WanderGuard BLUE Manager mobile application already installed.

Note If the WanderGuard BLUE Manager installed on your Tablet needs to be upgraded as part of a system upgrade, download it from Google Play or from the STANLEY Healthcare Knowledgebase.

The default password for accessing the Tablet is "2017".

The following Tablet settings are already enabled:

- Location services
- File access
- Bluetooth®

Note If any of these services are not enabled, enable them before proceeding. Otherwise, WanderGuard BLUE Manager may not operate properly.

In addition to the WanderGuard BLUE Manager, Google Sheets is pre-installed by STANLEY Healthcare to allow you to view CSV or other text files for troubleshooting and management purposes.

TeamViewer is also installed to enable remote technical support by STANLEY Healthcare.

If remote control is supported, perform the following on site:

- To be able to use the TeamViewer, **port 5938 outgoing** must be available at your customer site. IT at the customer site must make this setting.
- Connect to the network via Wi-Fi.

For troubleshooting the tablet installation, see the tablet Troubleshooting section in this User & Deployment Guide.

Language Support

Setting a language for the WanderGuard BLUE Manager application is done through the Tablet Settings. WanderGuard BLUE Manager does not have a dedicated language setting.

The following are the WanderGuard BLUE Manager-supported languages:

- English
- Francais (French)
- Deutsch (German)
- Espanol (Spanish)
- Svenska (Swedish)

For each primary language that WanderGuard BLUE Manager supports, each variety of that language is also supported. For example, if Francais is chosen as the primary language in the Tablet, the application is displayed in the French language, no matter what specific variety of Francais it is (France, Canada, Suisse, etc.).

Note

If a language not supported by WanderGuard BLUE Manager is chosen on the Tablet, the application will be displayed in the English language.

The following Mobile Application items are in English only:

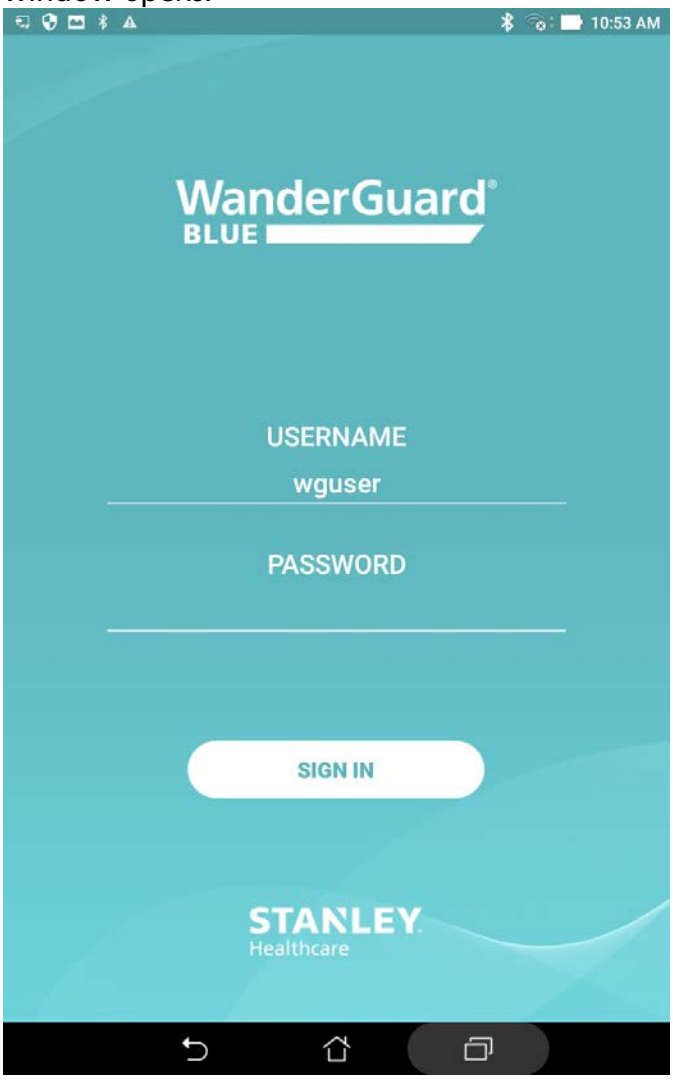
- Log files – Application and Controller
- File names
- Folder names

Application input fields (Controller name, user's first/middle/last name) are restricted to Latin letters only.

Running WanderGuard BLUE Manager

To run WanderGuard BLUE Manager:

1. Enter the password for accessing the Tablet. The default password is "2017".
2. On the Tablet's main window, locate the WanderGuard BLUE Manager icon.
3. Tap WanderGuard BLUE Manager icon to run the application .
4. The WanderGuard BLUE splash screen briefly appears. Then, the login window opens:



5. Enter the "wguser" user name. This user name is permanent and cannot be changed.

6. On the screen, tap PASSWORD.
7. Using the keyboard that opens, fill in the default password: WG2017 (use upper case letters only). You can change the password later.
8. Tap Done on the keyboard.
9. Tap SIGN IN. If you have registered a license, the Welcome window opens. If not, a license needs to be entered before using the application.

Note

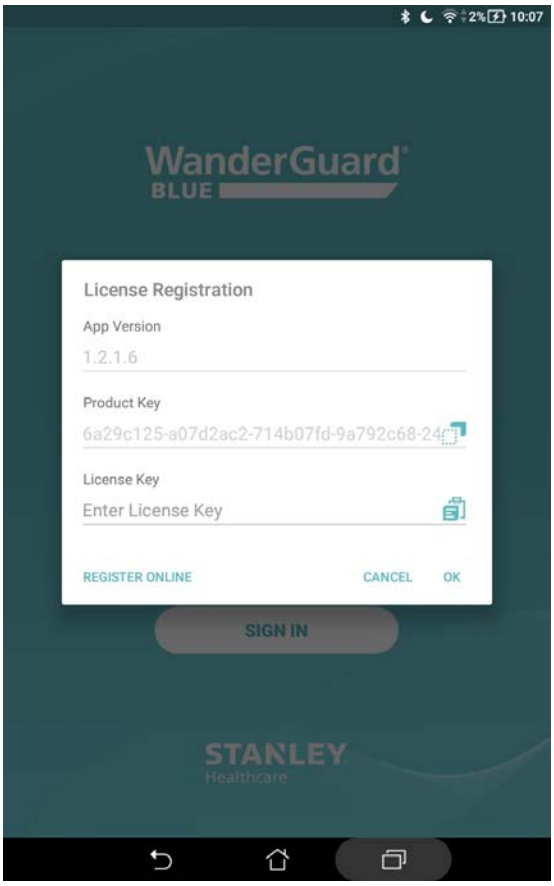
To operate WanderGuard BLUE Manager v1.2 and above, a License needs to be entered. To register a WanderGuard BLUE license, see here.

WanderGuard BLUE Manager License Registration

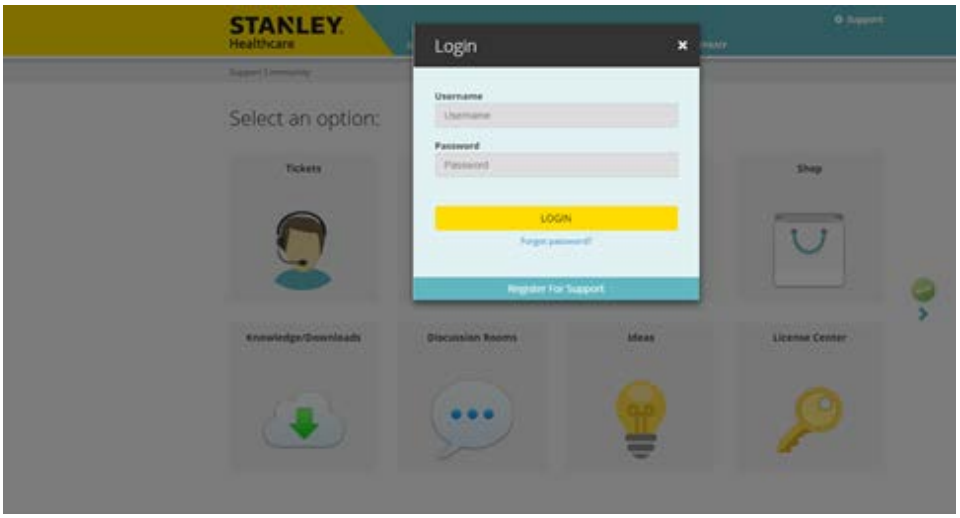
After signing in for the first time, the License Registration window opens.

To register the WanderGuard BLUE Manager License:

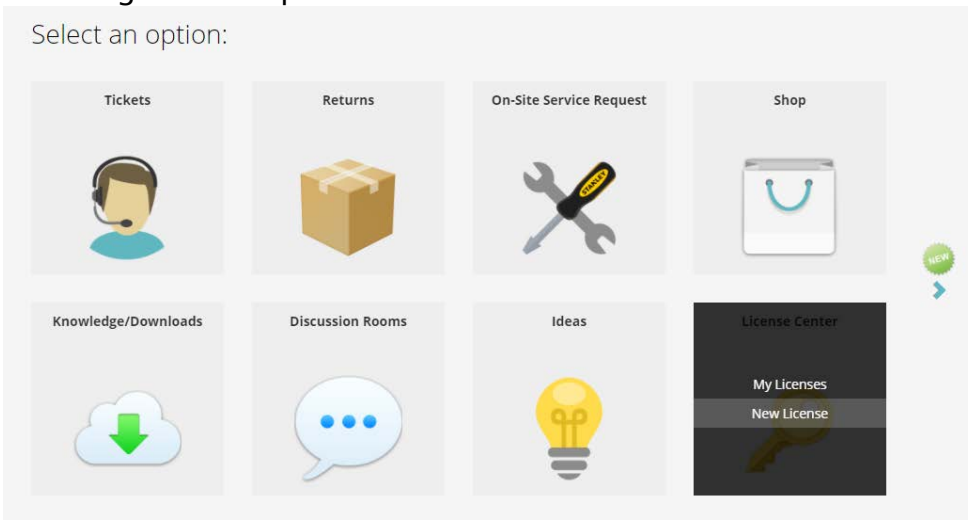
1. In the License Registration window, note that the Application Version and Product Key have already been filled in.
   In the Product Key field, tap in the right-hand **Copy** icon to copy the product key.



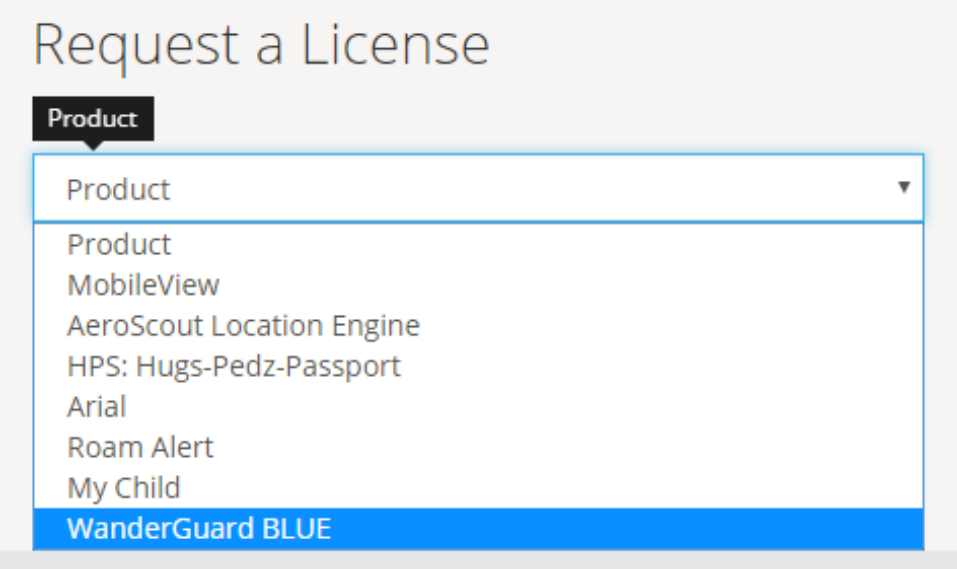
2. Tap Register Online. The STANLEY Healthcare site opens. The URL is: https://stanleyhealthcare.force.com.



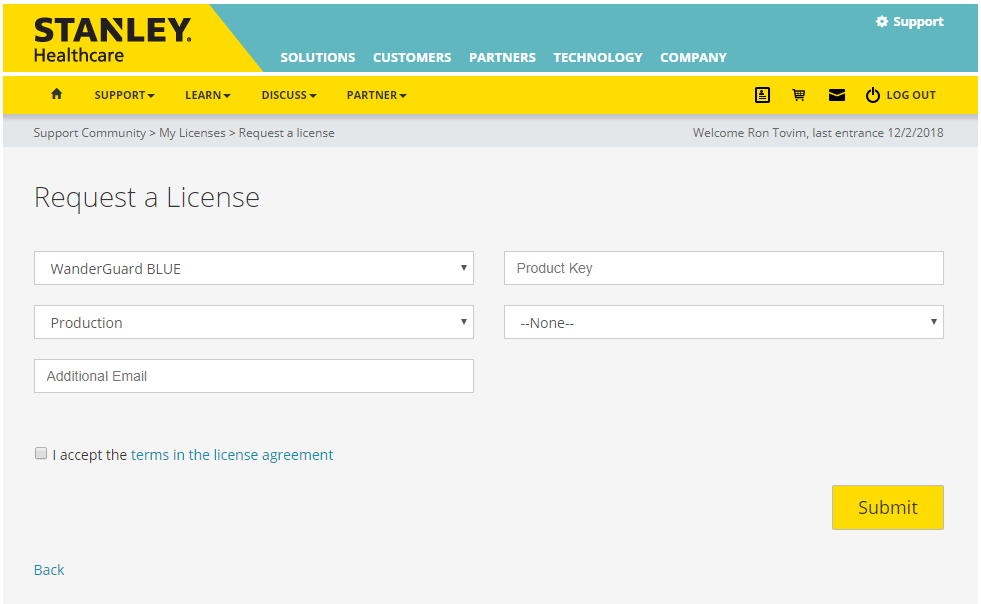
3. As a STANLEY Healthcare user, your user name and password may already be entered. If not, enter them now, and tap LOGIN. The following window opens:



4. Navigate to My Licenses and choose New License. The following window opens:



5. Choose WanderGuard BLUE.
For customers, the following window opens:

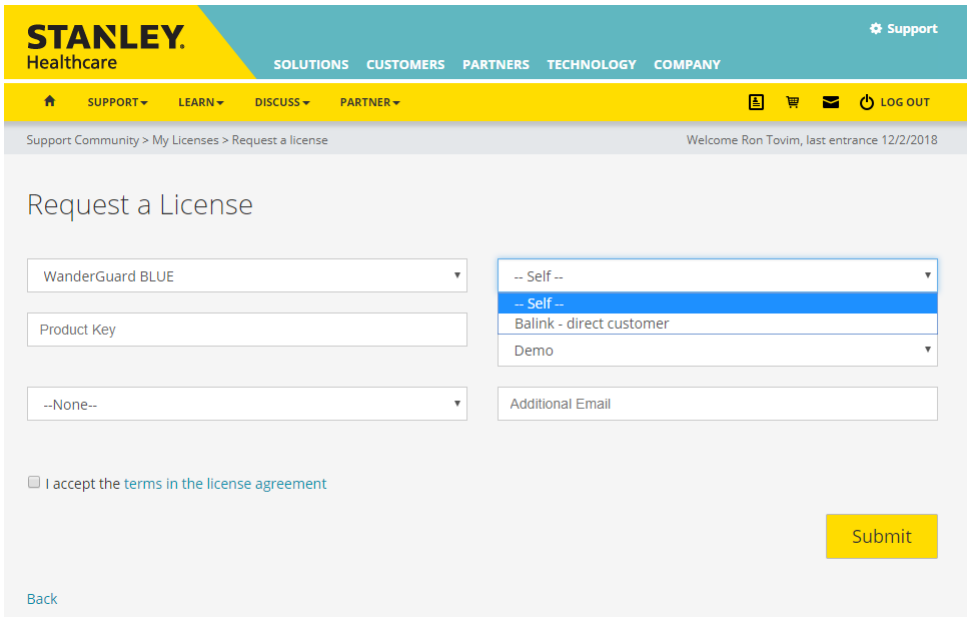


a. Paste the product key into the Product Key field copied from the WanderGuard BLUE Manager.
b. Select the Version of the WanderGuard BLUE Manager.
c. The License is sent to the email associated with the customer's account in the SalesForce system. Fill in the Additional Email field to have the License sent to an additional email address. We

recommend that you enter an email address that can be accessed from the Tablet.

d. Select the check box to accept the terms of the License agreement.
e. Tap **Submit**.

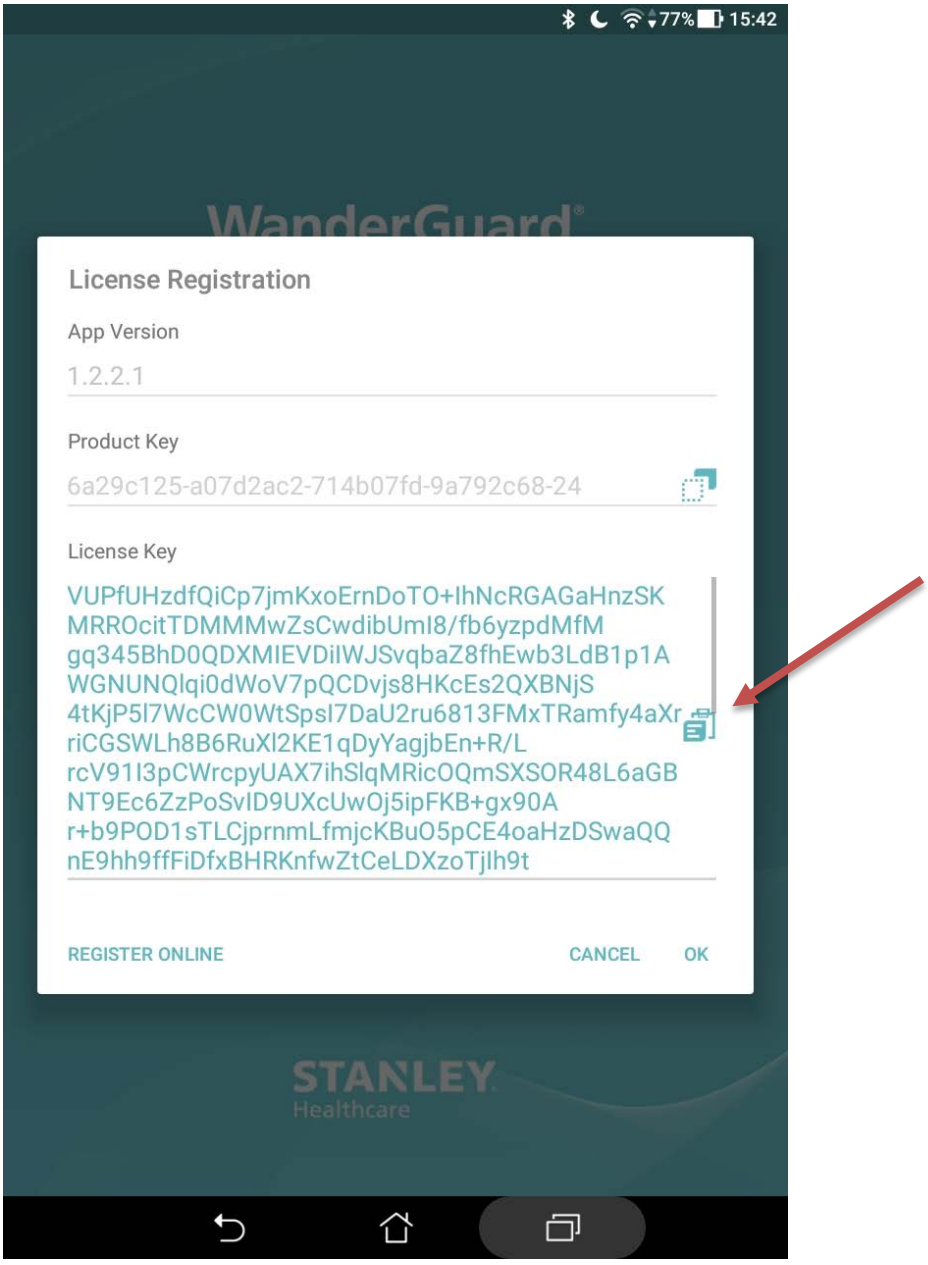
For partners, the following window opens:



a. Paste the product key into the Product Key field copied from the WanderGuard BLUE Manager.
b. Select the Version of the WanderGuard BLUE Manager.
c. The License is sent to the email associated with the Partner's account in the SalesForce system. Fill in the Additional Email field to have the License sent to an additional email address. We recommend that you enter an email address that can be accessed from the Tablet.
d. Select the customer for whom the License is intended. If the License is for self-use (demo, training), select the 'Self' option.
e. Select the environment for which the License is intended – Production, Training, or Demo. For the Production, select the customer for whom the License is being generated.
f. Select the check box to accept the terms of the License agreement.
g. Tap **Submit**.

6. When the email is received with the License key, copy the License Key.

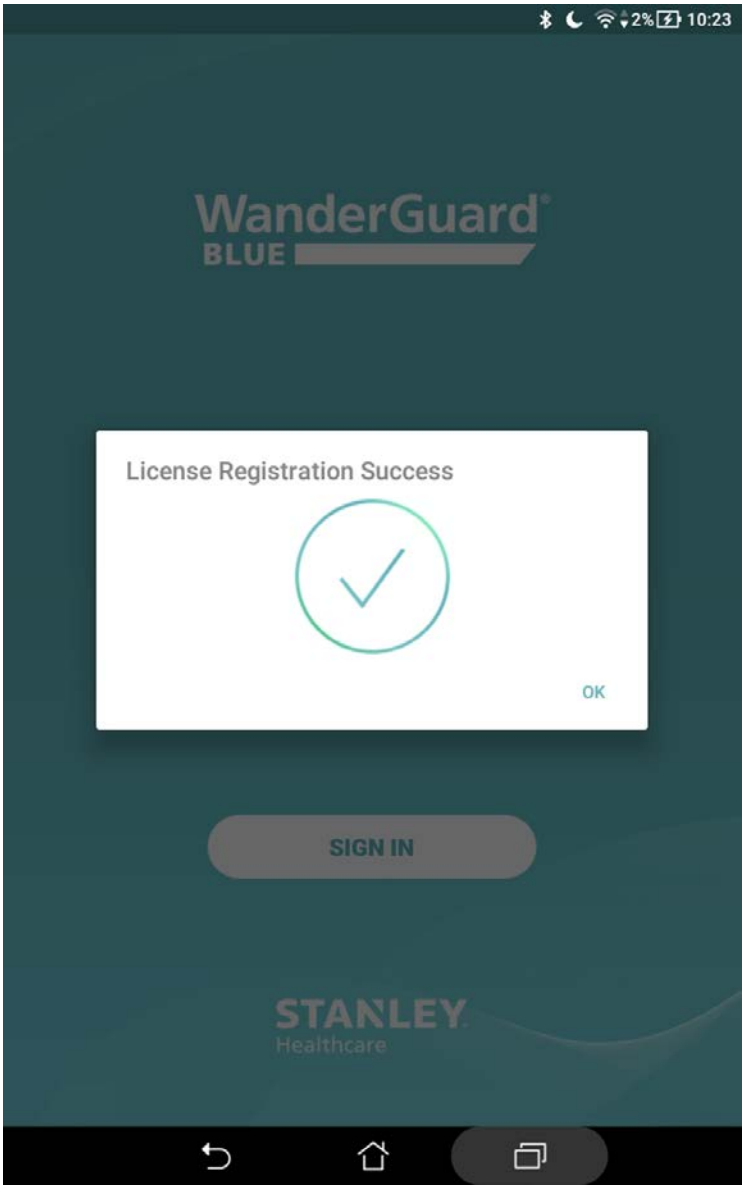
7. Open the License Registration window in the application by logging in. In the License Registration window, tap on the Paste icon on the right-hand side of the License Key field. The License Key is pasted into the License Key field.



Note

If you are registering a new License, the License Key field will be empty before pasting the License.

8. Tap OK. The License Registration Success window opens.



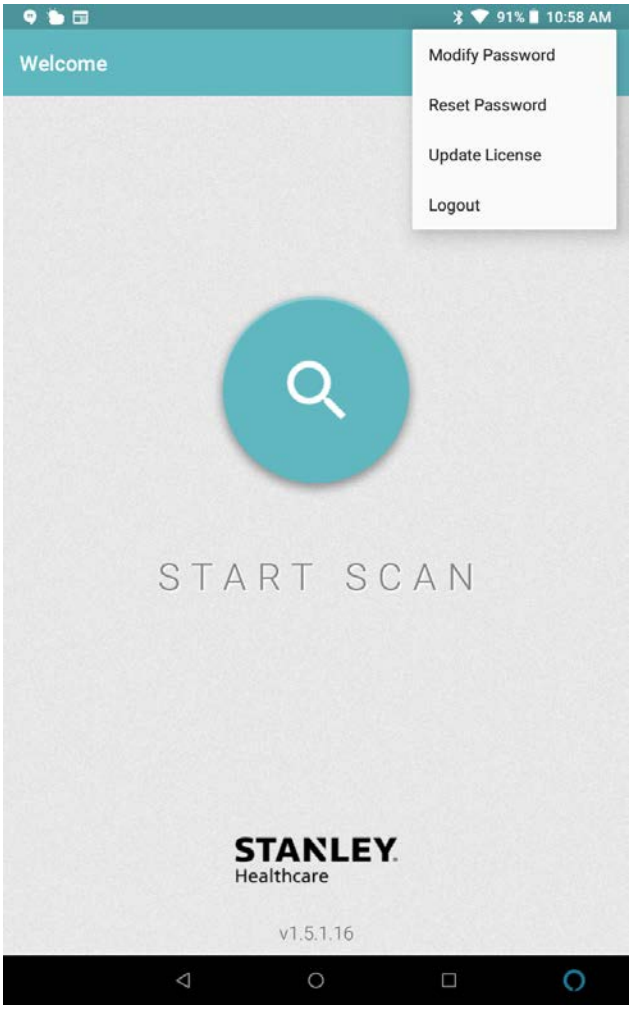
9. Tap OK to enter WanderGuard BLUE Manager. The Welcome window opens.

The Welcome Window

The Welcome window has a large **Start Scan** button in the center and a **More** button on the top-right (the "3-dots icon"). The current WanderGuard BLUE software version number is displayed on the Welcome window's bottom-middle.

In the Welcome window, the following is available:

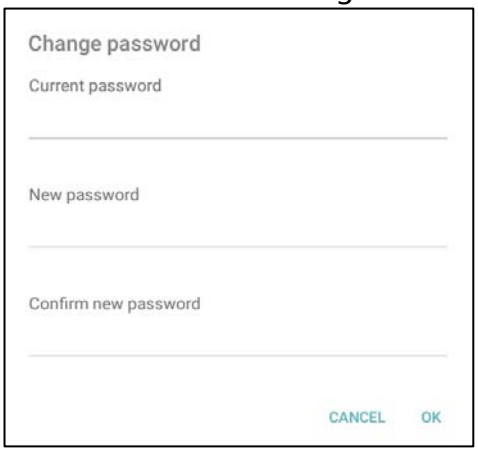
- Scan for in-field Controllers and Bracelets – tap **Scan** (see here).
- Modify the application password (see here).
- Reset the application password to its factory default – tap **More** and **Reset Password**.
- Update the WanderGuard BLUE Manager License (see here).
- Logout of the WanderGuard BLUE Manager – tap **More** > **Logout.**



Modify Password

To modify the password:

1. On the Welcome window, tap the **More** button and then **Modify Password**. The following window opens:



2. In the Current password field, enter the current password used for logging into the application.
3. Enter the new password in the New password field and Confirm new password field.

Note

Passwords must contain between 6 to 16 alphanumeric characters. The following special characters are permitted: !, @, #, $, &, *, _

4. Tap OK to save the new password in the system.

Reset Password

The password can be reset from two places in the application: the WanderGuard BLUE Manager login window and the WanderGuard BLUE Manager welcome window.

Resetting the password is important, especially in cases where the password was forgotten.

Resetting from the Login Window

From outside the application, reset the application to its default password and then log in.

To reset the password from the login window:

1. In the login window, enter "userreset" as the password.
2. A password was reset successfully message appears in the snack bar at the bottom of the WanderGuard BLUE Manager login window.

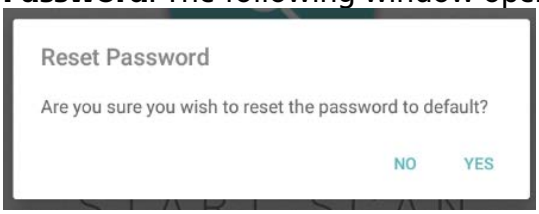
3. The application password is now reset to the default password ("WG2017").
4. You can now log in to the WanderGuard BLUE Manager application.
5. If you want to modify the default password, see here.

Resetting from the Welcome Window

Within the application, reset to the default password from the Welcome window.

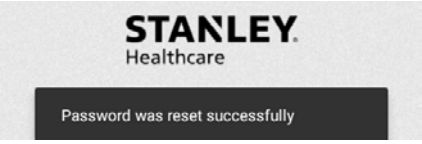
To reset the password from the Welcome window:

1. On the Welcome window, tap the **More** button and then **Reset Password**. The following window opens:



2. Tap Yes to continue resetting the application password.

3. A password was reset successfully message appears in the Snack Bar at the bottom of the WanderGuard BLUE Manager login window.

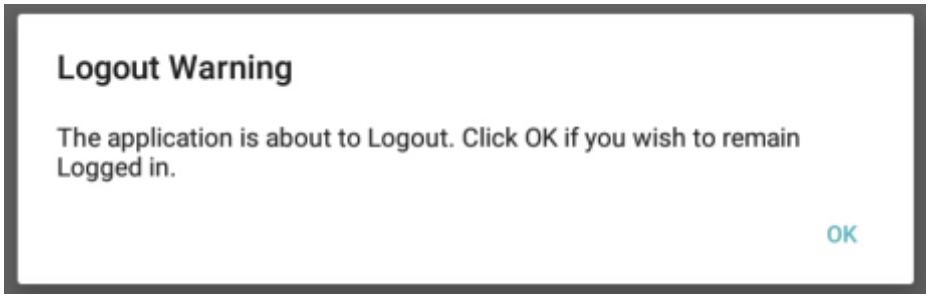


4. The application password is now reset to the default password ("WG2017").
5. You can now log in to the WanderGuard BLUE Manager application.
6. If you want to modify the default password, see here.

Automatic Logout

The WanderGuard BLUE Manager is programmed to issue a Logout Warning message after 57 minutes of no activity.

After 57 minutes, the following message appears:



If **OK** is not pressed, the app automatically logs out and returns you to the Login screen.

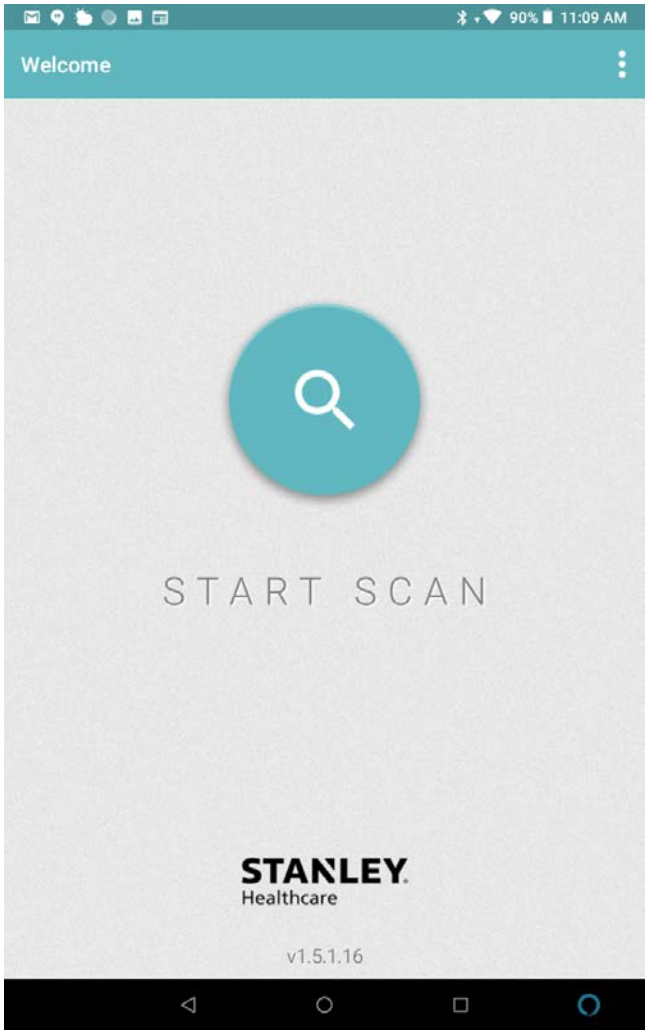
If WanderGuard BLUE Manager is connected to a Controller, it first disconnects from the Controller.

To enter the WanderGuard BLUE Manager again, log in as required.

If you press **OK** within three minutes of the Logout Warning message, the Automatic Log Out time is reset (you have another 57 minutes of no activity until the Logout Warning message reappears).

Scanning for Controllers, Gateways and Bracelets

To perform a scan, tap the Start Scan button in the Welcome window.



How It Works

Scanning with the WanderGuard BLUE Manager identifies Controllers, Gateways and Bracelets in the Tablet's range.

For Bracelets to be identified, a WanderGuard BLUE Detector needs to be active and transmitting in the Bracelets' vicinity.

The WanderGuard BLUE Detector emits an LF signal. When it is received by the Bracelet, the Bracelet sends a BLE response and continues to transmit while it is receiving LF signals from the Detector. The Bracelet BLE message is also received

by the WanderGuard BLUE Manager when it runs a scan (the WanderGuard BLUE Manager does not communicate directly with the Detector).

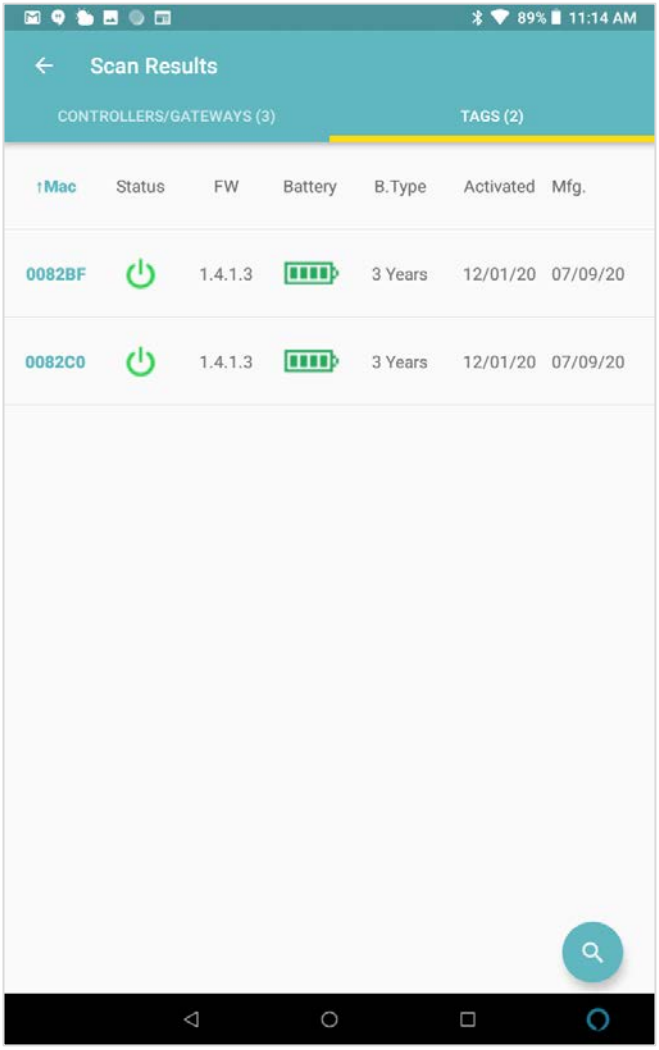
The Controller transmits its BLE messages even if there is no Detector in the vicinity. The Controller uses its BLE transceiver to send BLE messages with Controller information every three seconds. The Controller's BLE message is read by the WanderGuard BLUE Manager when it performs a scan.

WanderGuard BLUE Bracelets and Controllers are identified by WanderGuard BLUE Manager and displayed in the Scan Results window.

Performing a Scan for Controllers, Gateways and Bracelets

To scan for Controllers and Bracelets:

1. On the Home screen, tap **Scan**. A scan progress icon appears. The scan runs for about 20 seconds. You can stop/start a scan by pressing the **Start/Stop Scan** toggle button.
2. A Scan Results window opens and detected Bracelets and Controllers/Gateways are displayed.



Note

- WanderGuard BLUE Manager scans for Controllers, Gateways and Bracelets in its vicinity and displays their properties in the Scan Results window.
- Bracelet activation is done ONLY by the Detector.

Viewing Scan Results

In the Scan Results window, you can view scan results for the following devices:

- Controllers and Gateways
- Bracelets

Bracelet Scan Results

Scan results are displayed in the Scan Results window. Tap **Tags** to open the Tags tab.

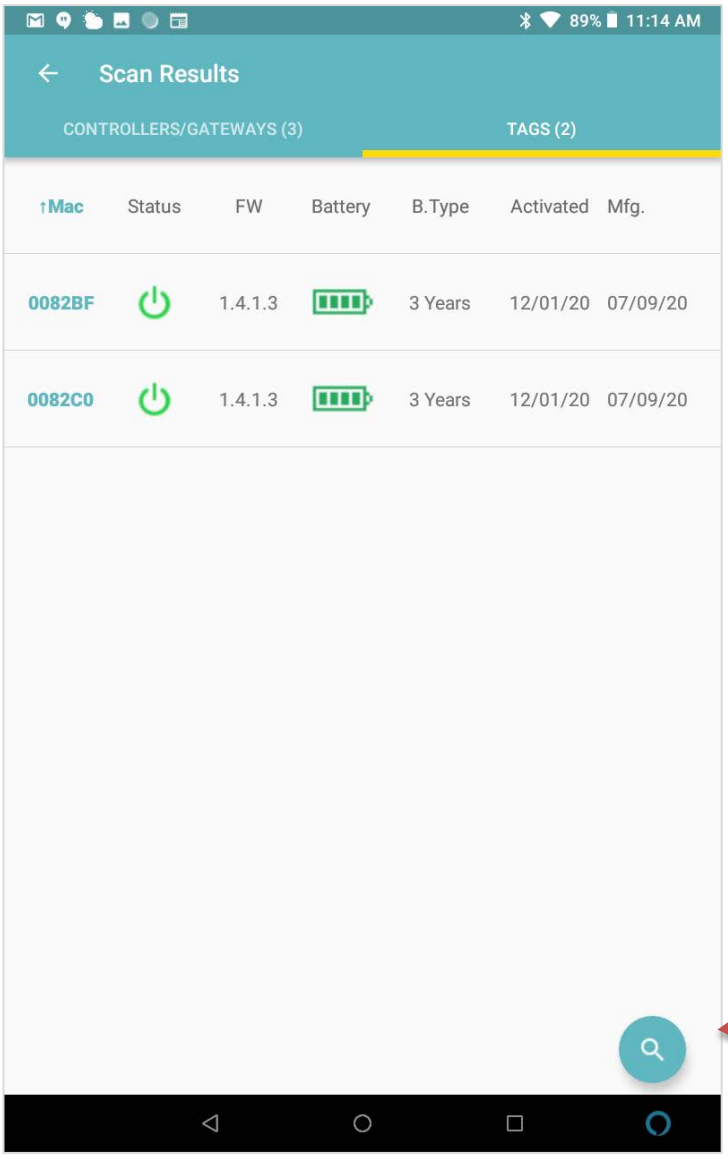
The number of identified Bracelets is displayed in parentheses adjacent to the Tags caption.

Bracelet details are displayed in a table with the following columns (see following screen):

- **Mac** – shows the last six alphanumeric characters of the Tag's MAC address. These six characters are also printed on the side of the Bracelet.
- **Status** – Dormant or Active
- **FW** - Firmware version
- **Battery** – relative charge indicator
- **B. Type** – 90 days, 1 year or 3 years
- **Activated** – date of Bracelet activation (month/day/year)
- **Mfg** – Bracelet manufacturing date (month/day/year)

Bracelete details may be sorted in ascending or descending order by tapping any column title.

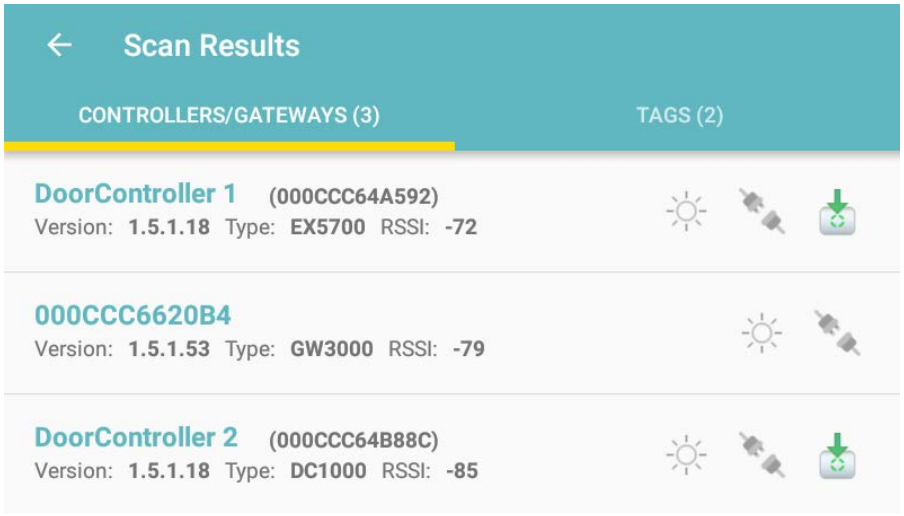
A rescan can be done by tapping the **Scan** button on the bottom right of the Scan Results screen.



Controller Scan Results

After a scan is run in the Welcome window, the Scan Results screen opens with Controllers displayed by default. The total number of identified Controllers is displayed in parentheses adjacent to the CONTROLLERS caption. If you are in the Tags tab, you can view Controller/Gateway Scan Results by tapping **CONTROLLERS/GATEWAYS** to open the tab.

Details are displayed in two-line rows: the first line shows the Controller/Gateway name and MAC address (in parentheses). The second line includes the DSP firmware version, Boot firmware version, Controller/Gateway type, and RSSI level of the received BLE signal. If more than one Controller/Gateway is identified, the list is sorted by RSSI level.



Best Practice: WanderGuard BLUE Manager can connect to only one Controller or Gateway at a time.

Tap the **Connect/Disconnect** toggle (/)to connect/disconnect from a Controller.

Tap to establish a BLE connection AND have the Controller blink for five seconds.

Controller blinking is useful to confirm that you are connected to the specific Controller to which you want to be connected (if there is more than one Controller in the vicinity).

If you try to connect WanderGuard BLUE Manager to a new Controller while the application is still connected to another Controller, WanderGuard BLUE Manager will first disconnect from the current Controller and only then connect to the new Controller.

The Update icon indicates that newer firmware is available. The icon is absent if the firmware us up-to-date. To update the Controller firmware from WanderGuard BLUE Manager, see here.

To view the Controller/Gateway configuration, tap the appropriate line in the tab. The Settings page opens after WanderGuard BLUE Manager has made a successful BLE connection to the selected device.

Note

In the event of several communication attempts in a row from the Mobile Application fail, follow these steps:

1. Disable Location and Bluetooth settings in the tablet.
2. Close the WanderGuard BLUE Manager application.
3. Enable Location and Bluetooth settings in the tablet.
4. Close the WanderGuard BLUE Manager application and try to connect again.

   If these steps do not resolve the problem, contact STANLEY Healthcare technical support.

Controller Configuration

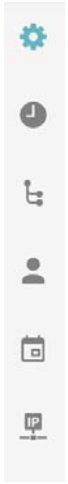
WanderGuard BLUE Manager allows you to configure the Controller after connecting to it.

To configure the Controller:

- Obtain the Controller's configuration by performing a scan and display it in the WanderGuard BLUE Manager (open the Controller/Gateway tab).
- Modify the desired parameters in WanderGuard BLUE Manager.
- Save (Apply) the modified configuration to the Controller.

Controller Pages User Interface

The User Interface (UI) has the following fixed elements:

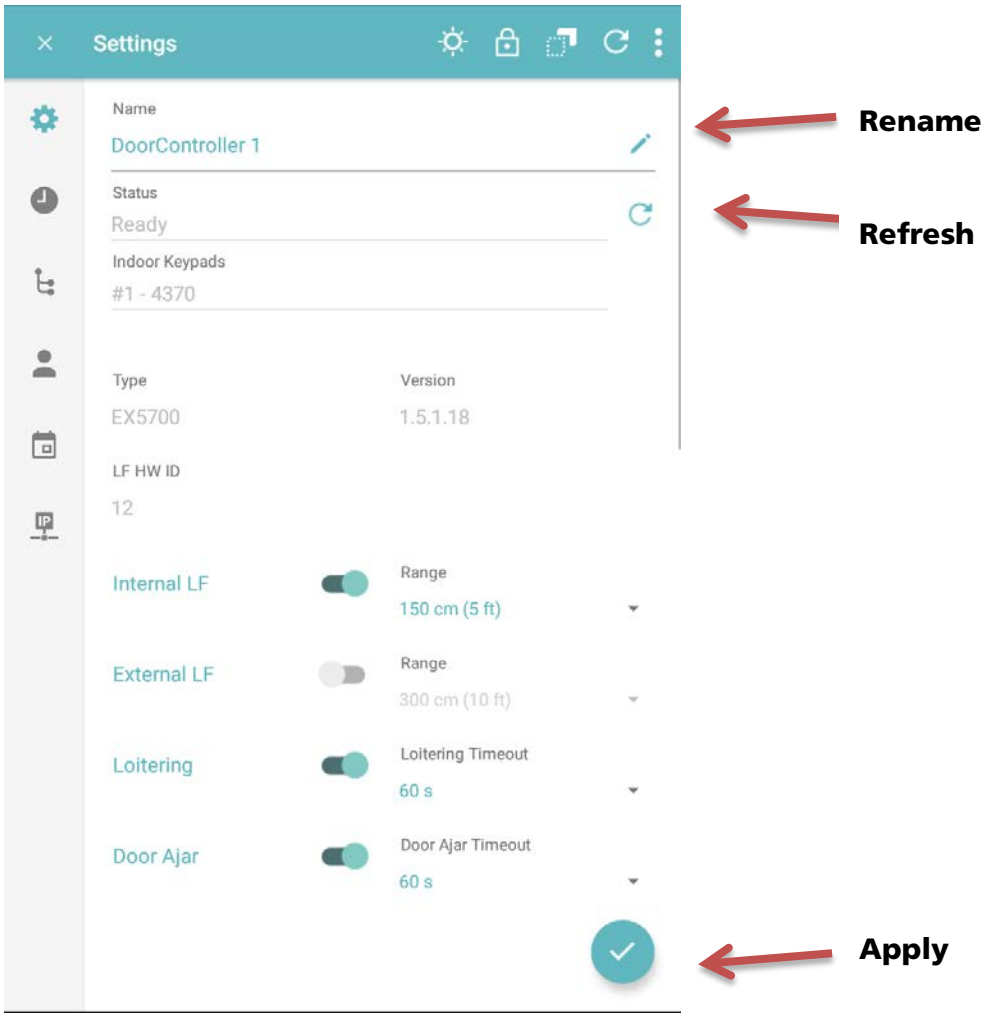
	Toolbar	Horizontal toolbar across the top of the page that provides extra functionality (see here)
	**Navigation bar**	Vertical left-hand bar to select one of the configuration pages: • **Settings** – for setting the Controller properties • **Clock** – for setting the Controller date, time, world Time Zone and Daylight Saving Time (DST) • **Outputs** – Programmable Output activation • **Users** – list of users who have an access code to the monitored door(s) • **Schedule** – Day/Night mode schedule for each day • **IP** – for setting the IP configuration
	Apply button	Validates and applies to the Controller the configuration settings of the page that the user is viewing

Settings

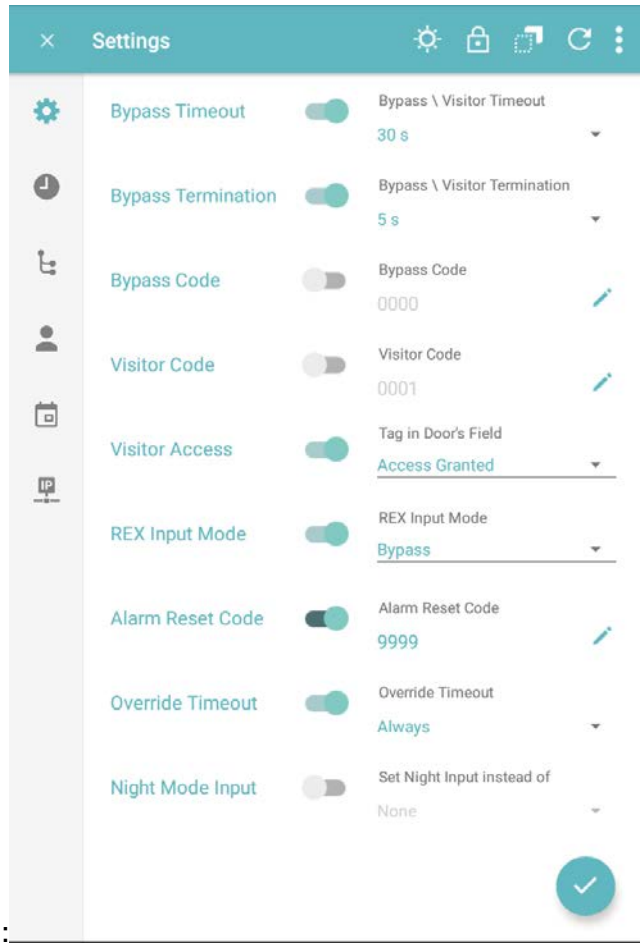
The Settings page is the default page when the Configuration page in the Controller Tab is opened.

The Controller Status, which is displayed in the Settings page, is refreshed automatically once a minute. The Status can be updated immediately by pressing the **Refresh** icon on the Status row.

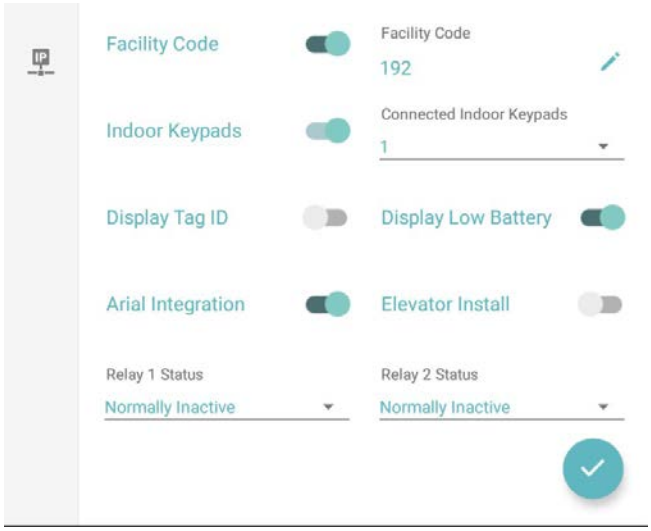
If changes are made to Controller settings, these changes can be saved to the Controller from the WanderGuard BLUE Manager by pressing the **Apply** button.

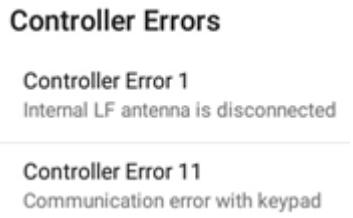


Scroll down the page to view all the Controller's settings (not all settings are visible at one time in a Tablet window).



:



PARAMETER	Definition
Name	Door Controller name. Length is limited to 16 characters.
Status	Displays Controller status. Typically, the current Controller mode is displayed (Override, Alarm, Bypass, Visitor, Night, Ready). Error messages are displayed if there are errors. Tap the message to obtain more detail: 
Indoor Keypads	The number of each Keypad that is connected to the Controller
Type	Type of Controller, e.g., EX5700, DC1000
Version	Version of the Controller firmware
LF HW ID*	Controller's LF HW ID parameter
Internal LF*	Normally ON. Can be set to up to 21 feet (650 cm). External LF can be enabled when internal LF is disabled.
External LF*	Normally OFF. Can be set to up to 10 feet (300 cm). Used only when an accessory Exciter is attached for greater coverage.
Loitering*	Timeout can be set.
Door Ajar	Timeout can be set.
Bypass Timeout	Cannot be disabled. Bypass and Visitor timeout ranges are 5-300 seconds (5 seconds resolution). The timeout range applies to both Bypass and Visitor. Default is 30 seconds.

PARAMETER	Definition
Bypass Termination	Bypass termination is the time it takes the Controller to terminate the Bypass/Visitor mode after entering the mode and the door is not opened. Cannot be disabled. Bypass and Visitor termination ranges are 5-120 seconds (5 seconds resolution). The timeout range applies to both Bypass and Visitor. Default is 5 seconds.
Bypass Code	Default can be changed by the user.
Visitor Code	Default can be changed by the user. The Visitor Code allows access but the system remains active against resident wander ("tailgating").
Visitor Access	System response when Visitor PIN code is used and there is a Tag in Field: Access Granted – Door gets unlocked Access Denied – Door remains locked
REX Input Mode	The mode the Controller can be set to either Bypass or Visitor upon triggering of the REX input.
Alarm Reset Code	General alarm reset code for the Controller
Override Limit	Limit the time the Controller is in Override mode
Night Mode input	Repurpose one of the Controller's inputs to serve as Night Mode input
Facility Code	Empty by default. Enter the Facility Code of the Badges that will be used with the Keypad/s (the Keypads are connected to the Controller). For setting up the Indoor Keypads, see here.

PARAMETER	Definition
Indoor Keypads	The number of connected Indoor Keypads can be set from 0 – 4. This number must correctly reflect the number of Indoor Keypads that are physically connected.
Display Tag ID*	Turn on to display the Tag ID that is in the Controller's field at the Indoor Keypad display.
Display Low Battery*	Turns on to show when a Bracelet that is in the Controller's field has a low battery. The indication is displayed in the Indoor Keypad display.
Arial Integration	When enabled, the WanderGuard BLUE Controller sends indications about alarm, events, errors, status, etc. via its embedded Inovonics transmitter. The messages are sent to the Arial system and presented there.
Elevator Install*	Designed to be used when the WanderGuard BLUE Controller is installed at an Elevator car. When Elevator Install is enabled, Loitering should be disabled and the Schedule should be configured to Day Mode-Always for all days.
Relay 1 Status	Can be set to Normally Inactive/Active
Relay 2 Status	Can be set to Normally Inactive/Active
*** These setting are not available in the DC1000**	

List of Possible Errors from the Controller

- Internal LF antenna is disconnected
- External LF antenna is disconnected
- Internal LF error detected
- External LF error detected
- Relay1 physical activation failed
- Relay2 physical activation failed
- UART failure with BD BLE module
- UART failure with UD BLE module
- FW upgrade failure of BD BLE module
- FW upgrade failure of UD BLE module
- Keypad(s) are not detected
- Communication error with Inovonics RF module
- Communication error with keypad #1
- Communication error with keypad #2
- Communication error with keypad #3

- Communication error with keypad #4
- More keypads connected than configured
- Keypad ID#1 version mismatch
- Keypad ID#2 version mismatch
- Keypad ID#3 version mismatch
- Keypad ID#4 version mismatch

Clock Settings

Use the Clock Settings page to update the time, date, Time Zone and Daylight Saving Time (DST). Clock settings are used by the Controller to enforce the Day/Night mode schedule.

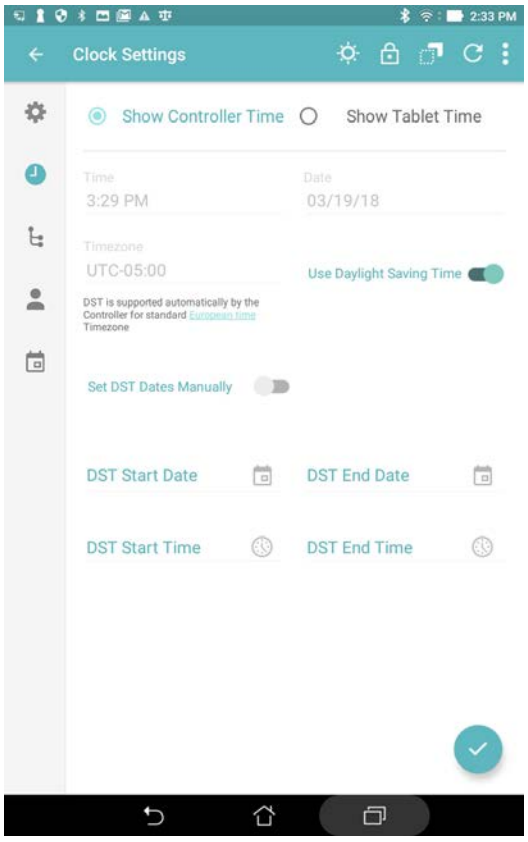
The time (shown on the Clock Settings page) is updated once per minute. Choose the device by selecting Show Controller Time or Show Tablet Time. The default view on the WanderGuard BLUE Manager is Controller Time. Time is shown by time of day, date and Time Zone.

In the Clock Settings page, you can do the following:

- View Controller Time
- View Tablet Time
- Apply the Tablet Time, Date and Time Zone to the Controller
- View and change Daylight Saving Time settings for the Controller

Best Practice: Initial setup requires setting the time of both the Controller and Tablet.

In addition to initial setup of the Controller, we recommend that you adjust (synchronize) the Controller clock once every six months.



To open the Clock settings page:

1. Tap **Scan** in WanderGuard BLUE Manager to generate a list of Controllers in your range.
2. Tap Connect to connect to the Controller of your choice.
3. The Settings page opens by default for the Controller that you chose.
4. Tap Clock Settings in the vertical navigation bar to open the Clock Settings page.
5. Verify that your device of choice is selected (Controller or Tablet).

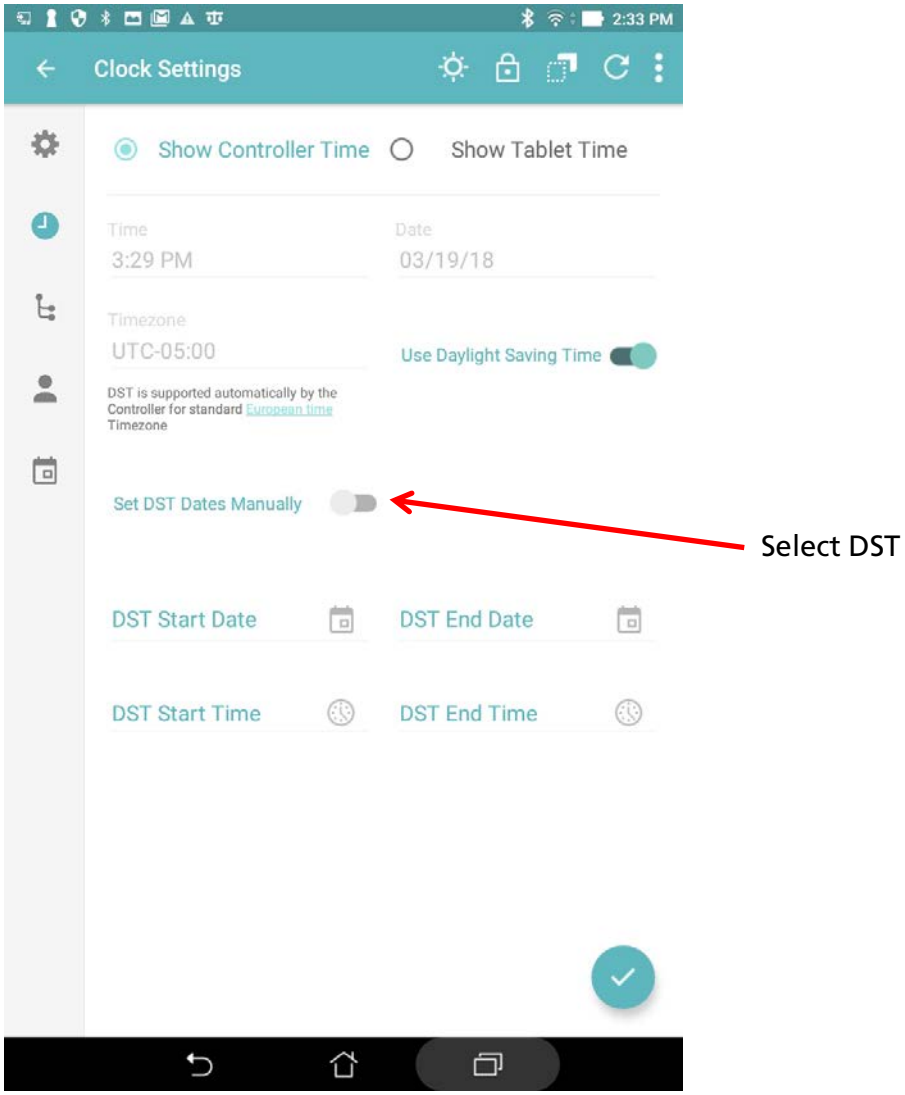
To change Controller's date and time:

1. Choose the **Show Tablet Time** radio button.
2. Verify that the Tablet Time, Date, and Time Zone are accurate.
3. Set the Daylight Saving Time parameter.
4. Tap Apply to upload Tablet time to the Controller.
5. A message appears that "Clock configuration applied successfully."
6. This date and time are subsequently displayed in the Indoor Keypad.

Best Practice: All the Clock Settings (Time, Date and Time Zone) in the Tablet are uploaded to the Controller, not just the Tablet time.

Daylight Saving Time

Daylight Saving Time (DST) is enabled by default. It can be disabled if the world Time Zone does not support DST.



There are three possible configurations of Daylight Saving Time:

- "Automatic" DST
- DST Disabled
- DST Enabled with Manual Setting of DST Times

"Automatic" DST

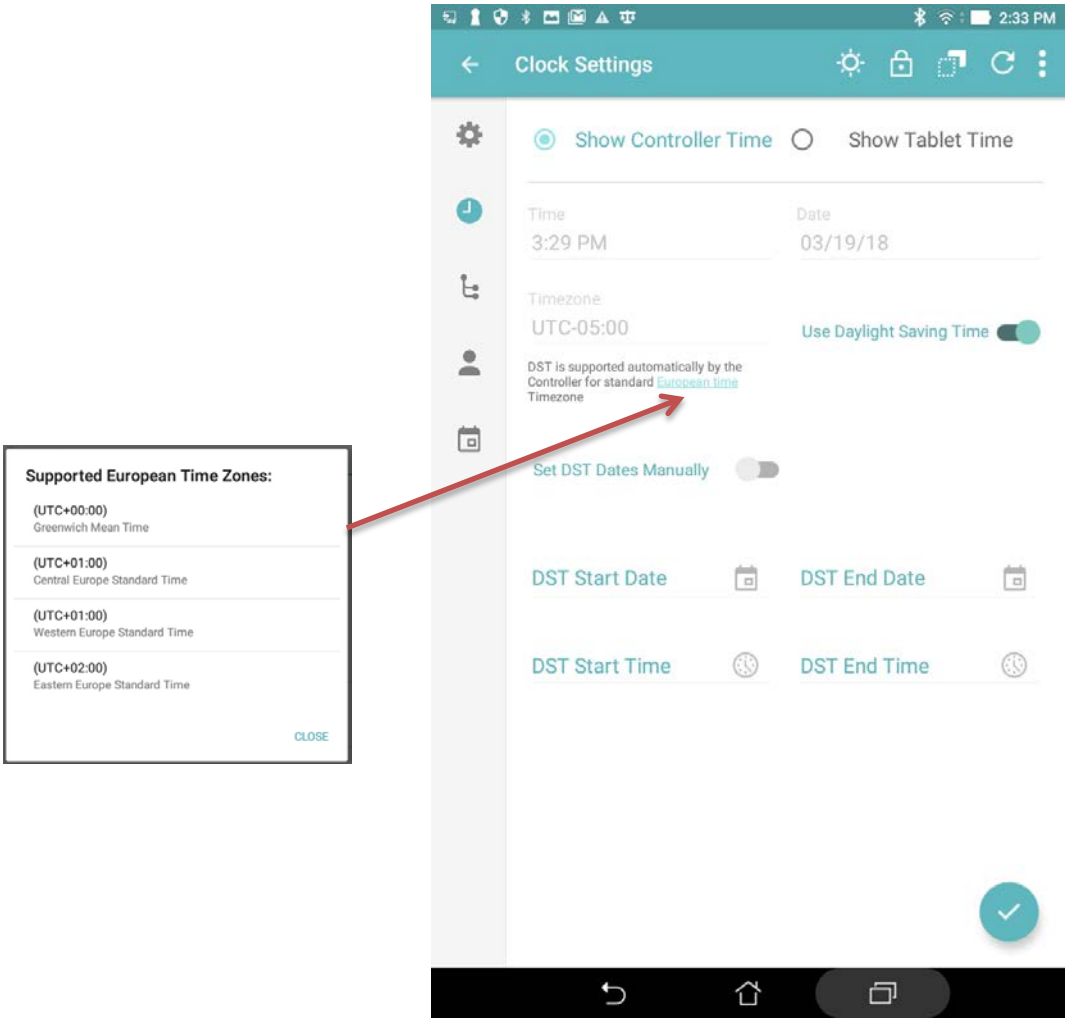
For US/Canada/Europe world Time Zones, the Controller moves to Daylight Saving Time and back automatically.

The Time Zones are:

- (UTC+00:00) Greenwich Mean Time
- (UTC+01:00) Central Europe Standard Time
- (UTC+01:00) Western Europe Standard Time
- (UTC+02:00) Eastern Europe Standard Time
- (UTC-04:00) Atlantic Time (Canada)
- (UTC-05:00) Eastern Time (US and Canada)
- (UTC-06:00) Central Time (US and Canada)
- (UTC-07:00) Mountain Time (US and Canada)
- (UTC-08:00) Pacific Time (US and Canada)
- (UTC-09:00) Alaska

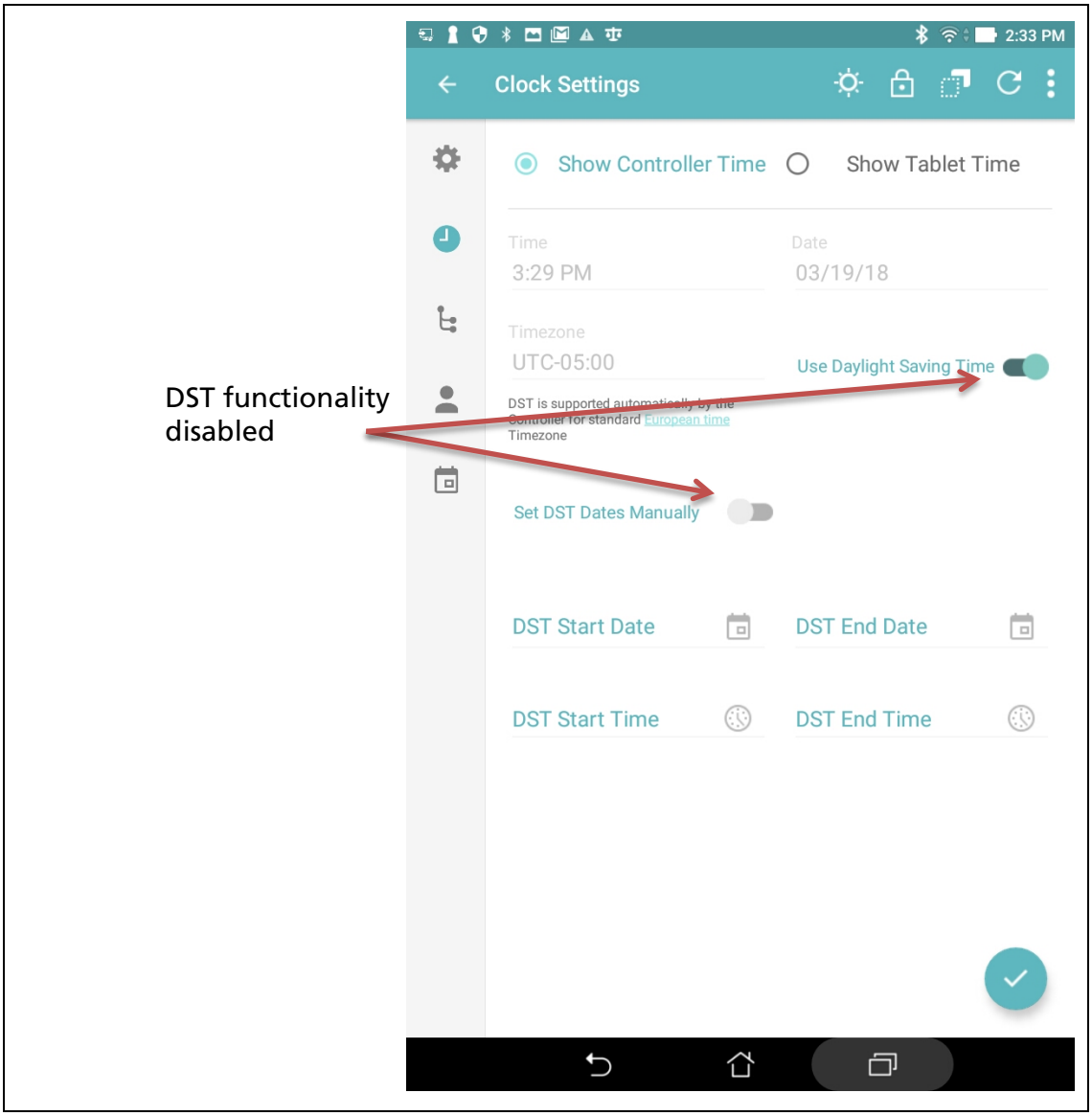
WanderGuard BLUE Manager indicates that DST is automatically supported when these Time Zones are used.

Best Practice: To use automatic DST support, your Tablet time has to be set to a US/Canada/Europe world Time Zone.


2:33 PM
Clock Settings
Show Controller Time
Show Tablet Time
Time
3:29 PM
Date
03/19/18
Timezone
UTC-05:00
Use Daylight Saving Time
DST is supported automatically by the Controller for standard European time Timezone
Set DST Dates Manually
DST Start Date
DST End Date
DST Start Time
DST End Time
Supported European Time Zones:
(UTC+00:00)
Greenwich Mean Time
(UTC+01:00)
Central Europe Standard Time
(UTC+01:00)
Western Europe Standard Time
(UTC+02:00)
Eastern Europe Standard Time
CLOSE

DST Disabled

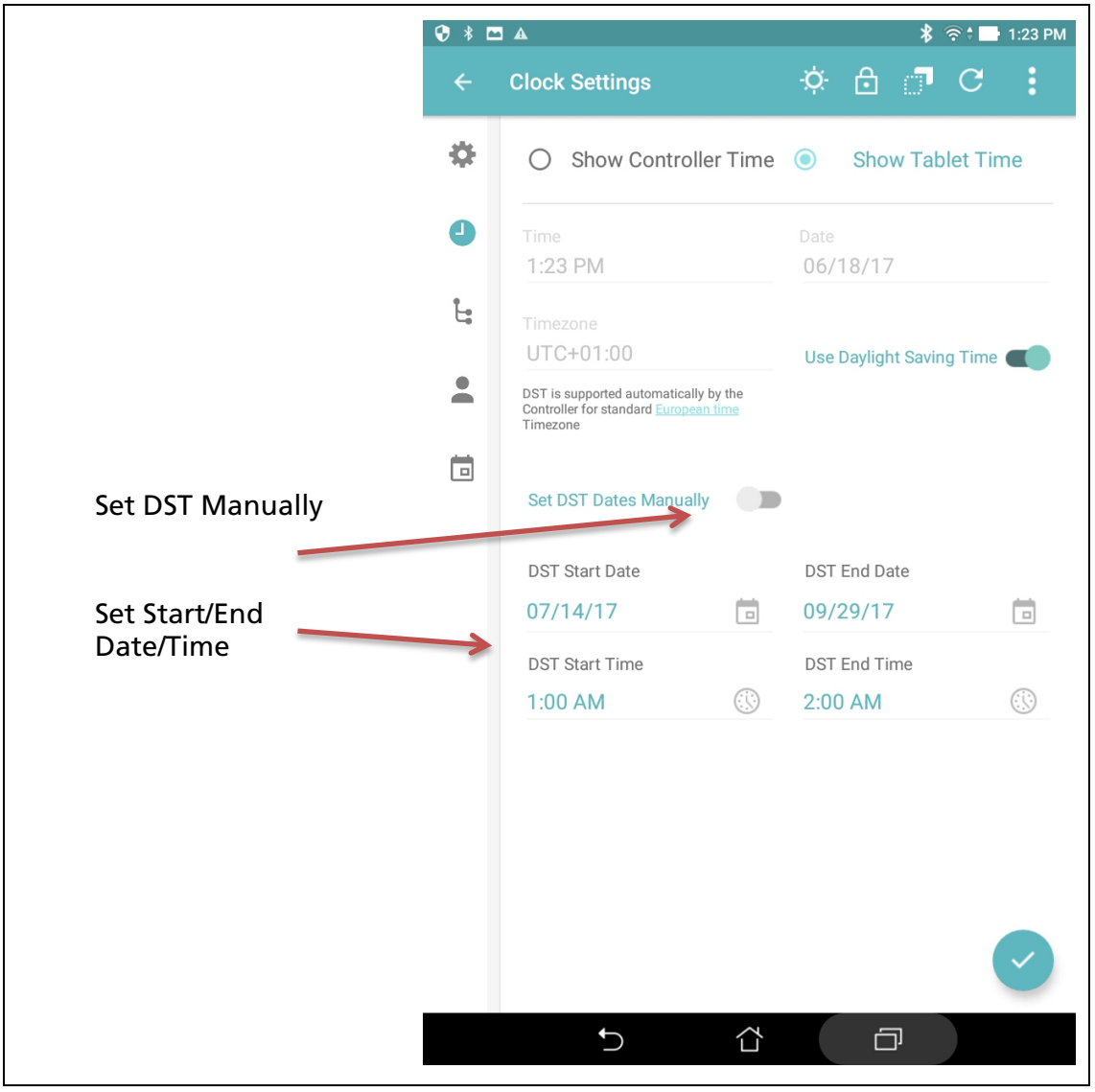
If the world Time Zone does not support Daylight Saving Time (for example, Hawaii), disable the "Use Daylight Saving Time" setting. In this case, "Set DST Dates Manually" is also disabled.



DST Enabled with Manual Setting of DST Times

In this scenario, you manually set the DST start and end dates. Manual settings override any "automatic" settings.

1. Enable DST ("Use Daylight Saving Time").
2. Enable "Set DST Manually."
3. Set the Start and End date/time of the DST.



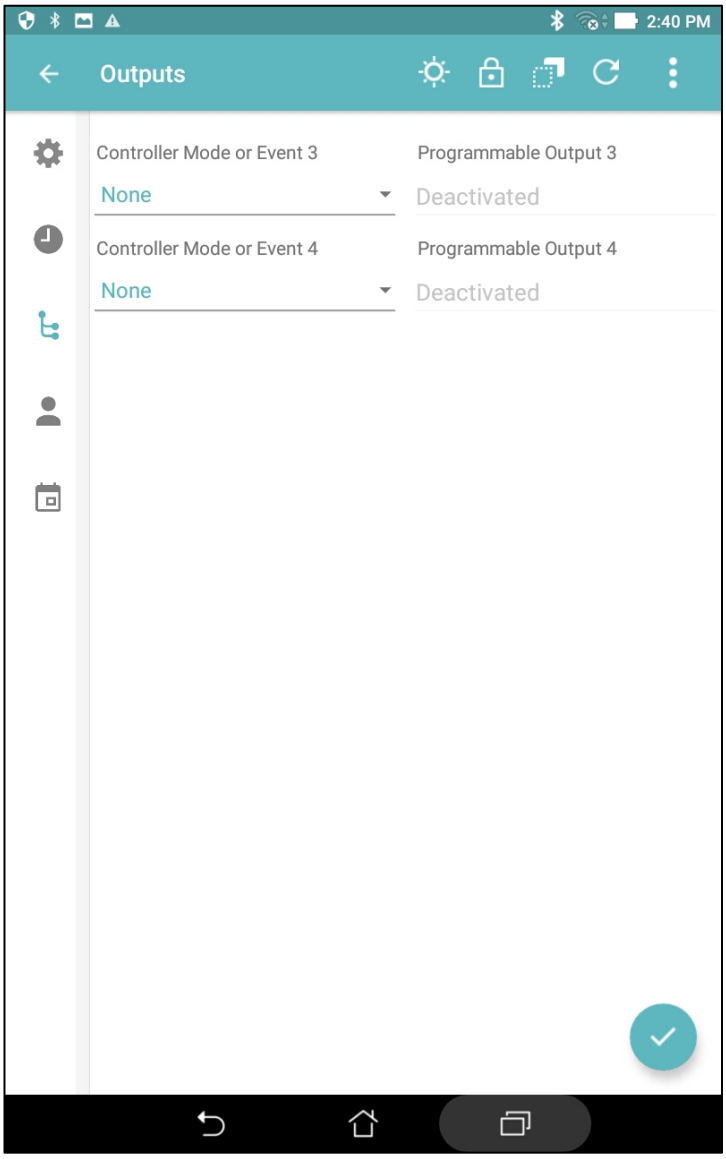
Outputs

The Controller has two programmable outputs – Outputs 3 and 4. These outputs can be programmed to be activated when a Controller mode changes or event occurs. When the event is cancelled or the Controller mode changes back to its previous mode, the output is deactivated.

Outputs can be an alarm or bell, flashing light, etc., depending on the mode and desired result.

The Controller's terminal block has the following outputs (see the Controller chapter in this Guide for more details):

- Controller's OUT3 – WanderGuard BLUE Manager's programmable Output 3
- Controller's OUT4 – WanderGuard BLUE Manager's programmable Output 4



The following output activation options can be set:

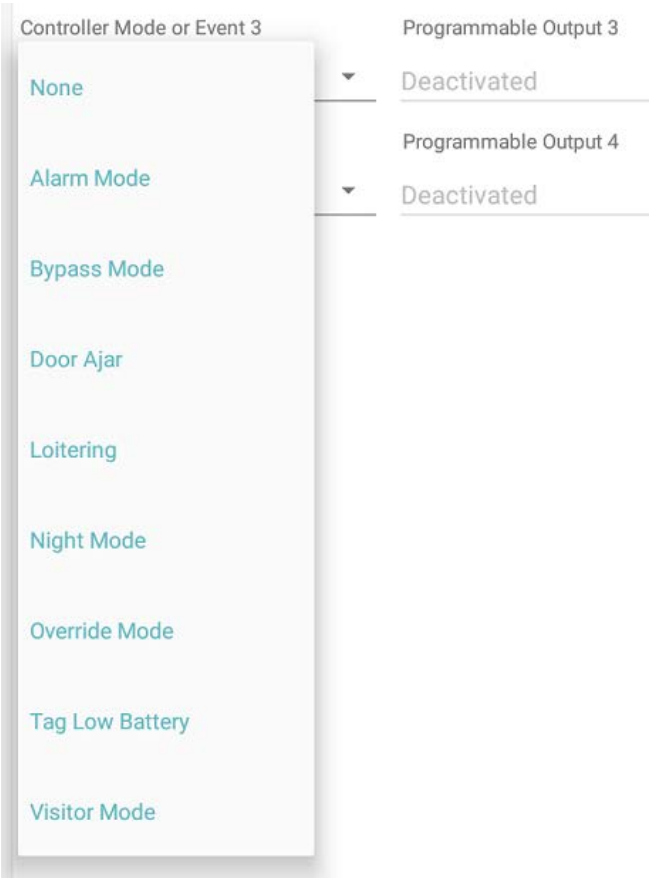
- None (disabled)
- Bypass mode
- Alarm mode
- Override mode
- Night mode
- * Loitering (if LF and Loitering are enabled)
- Door Ajar (if Door Ajar is enabled)
- Visitor mode (if Visitor mode is enabled)
- * Tag Low Battery

* Loitering and Tag Low Battery do not apply to DC1000

To activate a Programmable Output option:

1. Tap the Scan button in WanderGuard BLUE Manager to generate a list of Controllers in your range.
2. Tap Connect to connect to the Controller of your choice.
3. The Settings page opens by default for the Controller that you chose.
4. Tap Outputs in the vertical navigation bar to open the Outputs page.
5. On the Outputs page, select your desired mode in the Controller Mode or Event pull-down menu.
6. In Programmable Output 3, tap the Activated/Deactivated toggle.
7. Repeat step 5 and 6 for Controller Mode or Event and Programmable Output 4, as necessary.
8. Tap Apply to save any changes to the current Controller.

(ii)


Controller Mode or Event 3
None
Alarm Mode
Bypass Mode
Door Ajar
Loitering
Night Mode
Override Mode
Tag Low Battery
Visitor Mode
Programmable Output 3
Deactivated
Programmable Output 4
Deactivated

Users

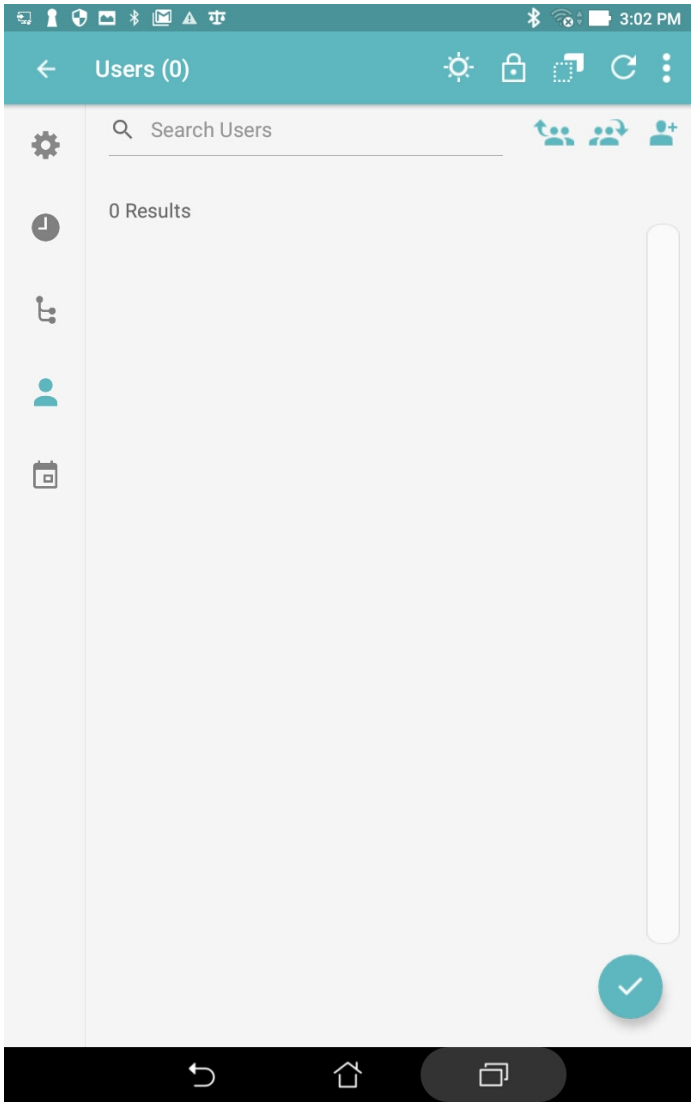
Users are displayed in WanderGuard BLUE Manager User Page ("users" can be either staff or residents).

An individual Controller supports up to 1000 users. User data is stored in the Controller and downloaded to the WanderGuard BLUE Manager when a Controller is scanned and identified. Users of the selected controller are displayed in the Users List.

If you wish to add or update users for multiple controllers at the same time, use Arial.

Getting Started with the Users Page

Out of the box, a Controller has no configured users.



The parameters of a user record are as follows:

- User Type – can be 'Employee' or 'Visitor'
- First Name (required; up to 16 alpha-numeric characters including '-' (dash), ' ' (space) and '.' (period)
- Middle Name (required; up to 16 char)
- Last Name (required; up to 16 char)
- PIN code (4 digits; must be unique)
- Badge ID (up to 5 digits (0-65535); must be unique)
- Permission to Start/End Override/Night Mode using a PIN Code

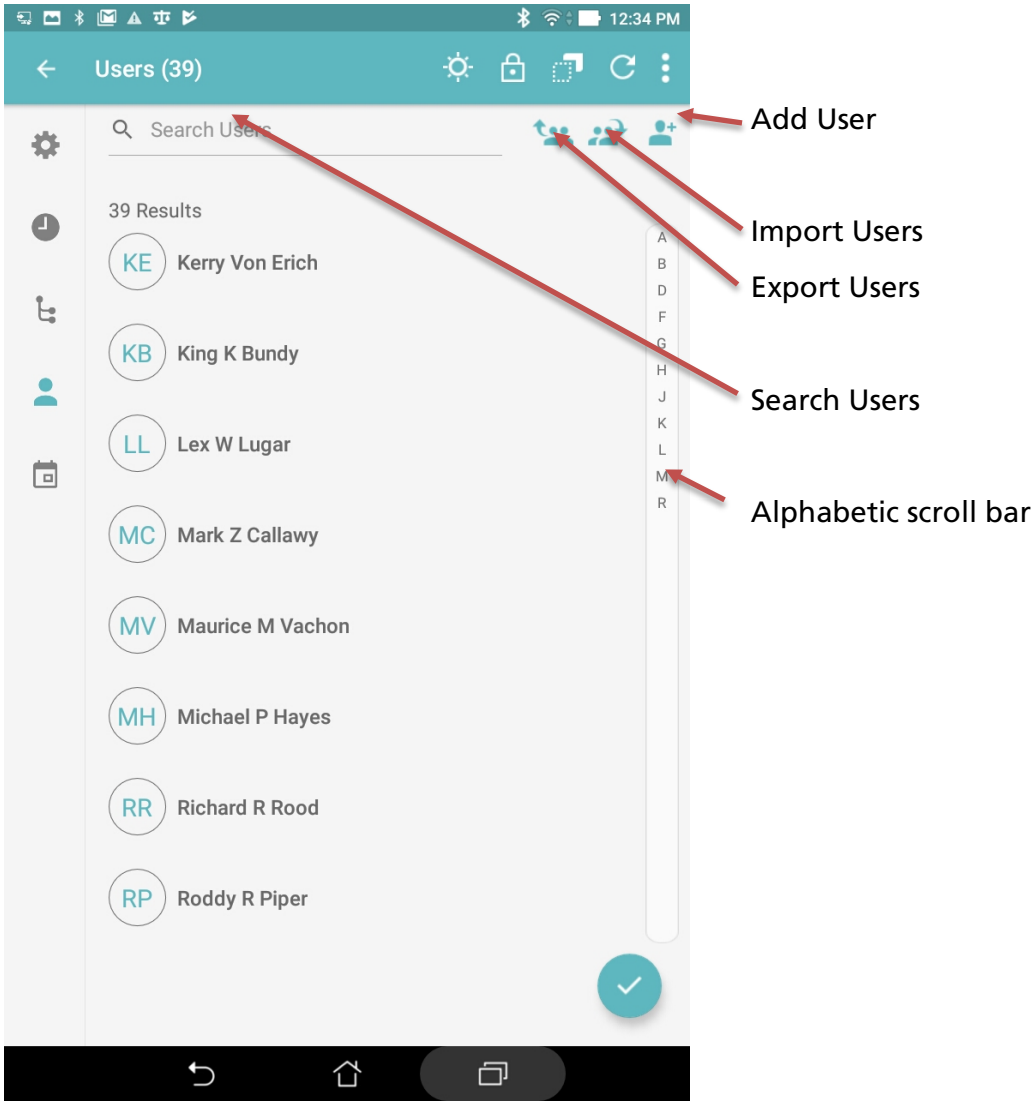
Note

The combination of names (First, Middle, Last) must be unique.
A PIN code and/or a Badge ID are required.

The Users Page has the following functionality:

	Export Users	Exports users to a csv file with the default file name and format.
	Import Users	Imports users from a csv file
	Add User	Opens the Add User window

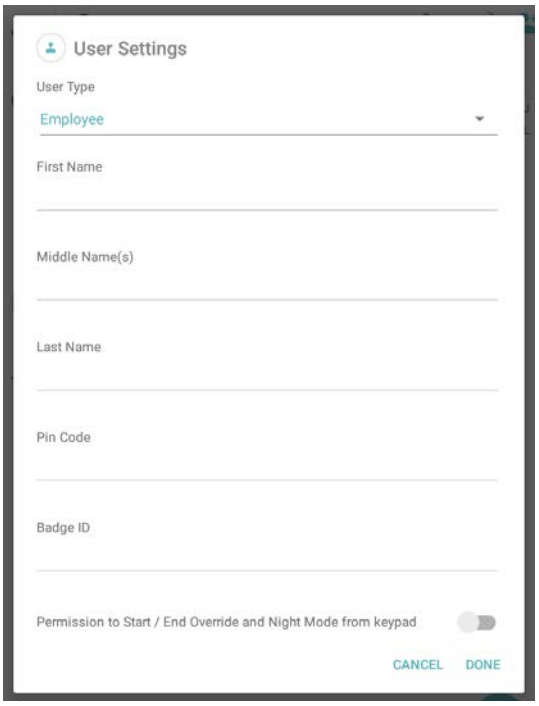
The Search Users supports searching for first, last, and middle name. In addition, the Badge ID can be searched. A typical, populated Users list may look like this:



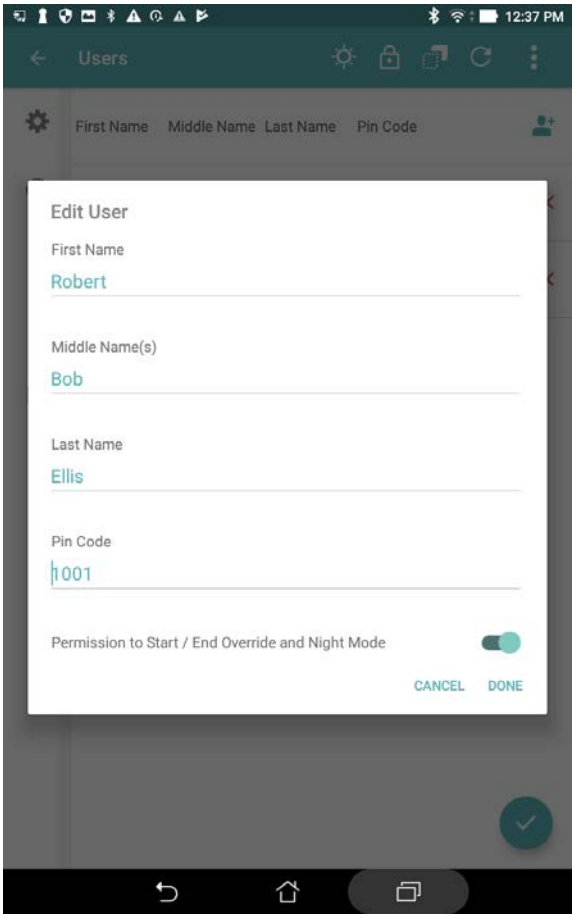
Add a New User

1. Tap Scan in WanderGuard BLUE Manager to generate a list of Controllers in your range.
2. Tap Connect to connect to the Controller of your choice.
3. The Settings page opens by default for the Controller that you chose.
4. Tap Users in the vertical navigation bar to open the Users page.

5. On the Users page, tap the New User icon. The User Settings page opens.



6. Select “Employee” or “Visitor” from the User Type field.
7. Fill in the name fields. Middle Name is also required.
8. Tap Next to move from one name field to the next one.
9. Fill in the PIN code and/or Badge ID (either a PIN code or Badge ID are required).
10. If this user has permission to Start / End Override and Night Mode from the Keypad, enable the setting.



11. Tap Done to finish or Cancel to disregard your work. Tapping Done validates the new user or reports errors if the entered data is not compliant. You are returned to the Users page.

12. Tap Apply to save any changes to the current Controller.

Note

If you do not tap Apply, your changes will be lost when you leave WanderGuard BLUE Manager.

Edit User

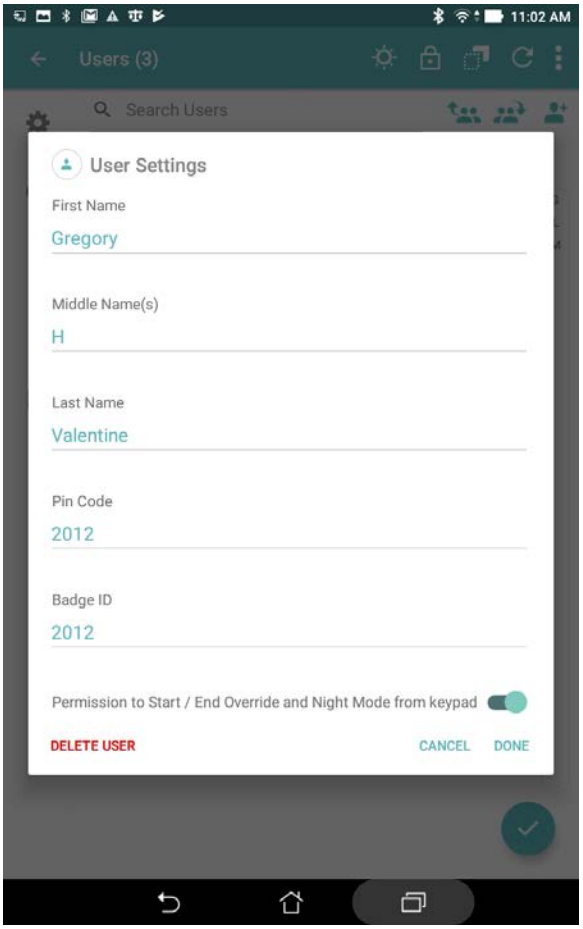
1. Tap Scan in WanderGuard BLUE Manager to generate a list of Controllers in your range.

2. Tap Connect to connect to the Controller of your choice.

3. The Settings page opens by default for the Controller that you chose.

4. Tap Users in the vertical navigation bar to open the Users page.

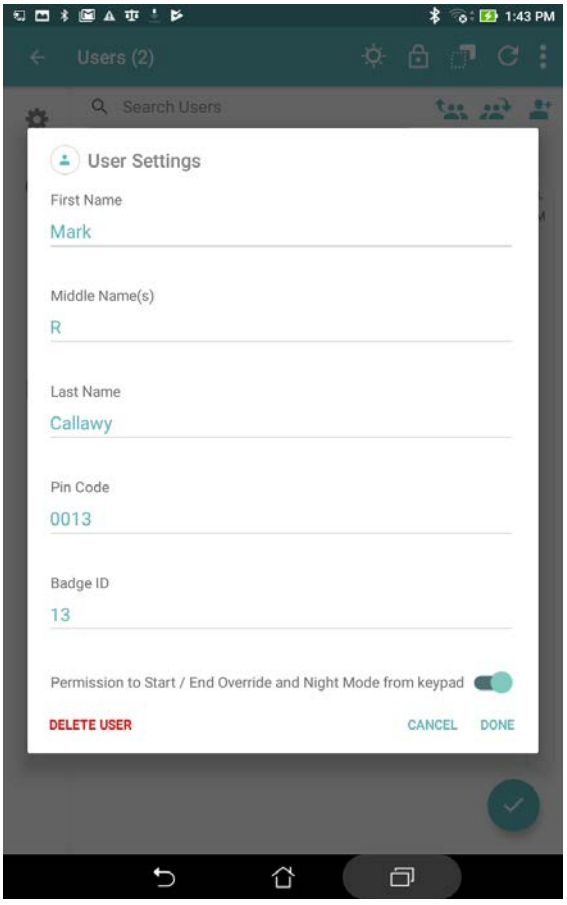
5. On the Users page, tap to select your desired user from the displayed list. Edit the name fields, Badge ID and PIN code, as necessary.
6. If this user will have permission to Start / End Override and Night Mode, activate this setting now and tap Done.
7. Tap Done to finish or Cancel to disregard your work. Pressing Done validates the modified user entry or reports errors if the entered data is not compliant. You are returned to the Users page.
8. Tap Apply to save any changes to the current Controller.



Delete User

1. Tap Scan in WanderGuard BLUE Manager to generate a list of Controllers in your range.
2. Tap Connect to connect to the Controller of your choice.
3. The Settings page opens by default for the Controller that you chose.
4. Tap Users in the vertical navigation bar to open the Users page.

5. On the Users page, tap to select your desired user from the list.
6. Tap Delete User.



7. The Confirm User Deletion window opens.

8. Tap Delete to remove the user from the list.
9. Tap Apply to save changes to the current Controller.

Import Users

This function saves the tedious activity of manually importing a large number of users and adding them one by one and can also update an existing list of users (for example, updating a list of user PIN codes).

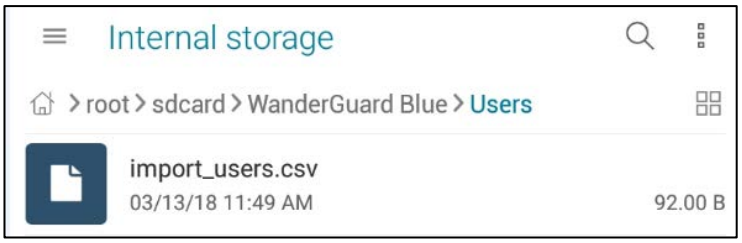
When a nearby Controller is scanned in the application, the users listed in the Controller are automatically downloaded to the application. When users are

imported from an external file into the application, the application performs a comparison between the two lists.

Note The system has a limit of 1,000 users (a Controller can store only 1,000 users). In addition, the system can process only the first 1,000 rows of very large import files (.csv) even if the files have over 1,000 rows.

Importing an External File of Users

The file containing users for import must be first uploaded to the WanderGuard Blue > Users folder in the Tablet. This can be done by standard file transfer. By default, the Users folder already includes a sample file called import_users.csv.



The file to be imported can have any name insofar as it is a compliant CSV file, and user records are properly populated in the file.

The following constraints apply to the import file:

- Must have the format of the sample file
- Must be in CSV format
- Headers must be exactly as in the header file.
- Permission field options must be only TRUE or FALSE.
- Type field may only contain “Employee” or “Visitor”

The following is a typical user record:

First Name	Middle Name	Last Name	PIN Code	Badge ID	Permission	Type
Michael	John	Winter	1234	33111	FALSE	Employee

System Messages and Handling Anomalies

After import, the system displays data on the status of the imported records:

Successful – number of records added to the list of users in the application. To save new records in the Controller, use the Apply button.

Identical – records ignored and not added to the list of users because they are identical to existing records. These records do not require user action in the application and are displayed for information purposes.

Failed – records that have invalid information and were not added. These records cannot be imported into the application and are displayed for information purposes only.

Conflict – the imported user record – first, middle, and last names – already exists, but the user has a PIN code or Badge ID or permission setting that is different from the setting of the existing record in the Controller. The import result allows you to either discard the imported user or overwrite the existing one.

Consider the following typical user record:

First Name	Middle Name	Last Name	PIN Code	Badge ID	Permission	Type
Michael	John	Winter	1234	33111	FALSE	Employee

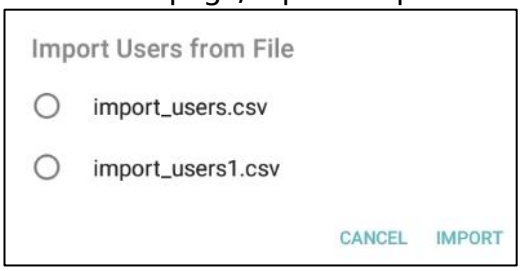
- The new user record has the same first, middle, and last name, but the PIN code and permission are different from the record that already exists:

First Name	Middle Name	Last Name	PIN Code	Badge ID	Permission	Type
Michael	John	Winter	1235	33111	TRUE	Employee

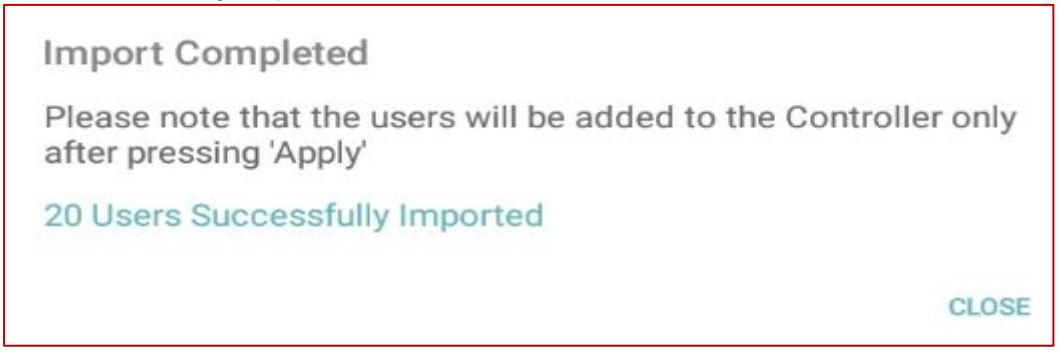
Conflict records require user action in the application.

To import users:

1. In the Users page, tap the Import Users icon. .



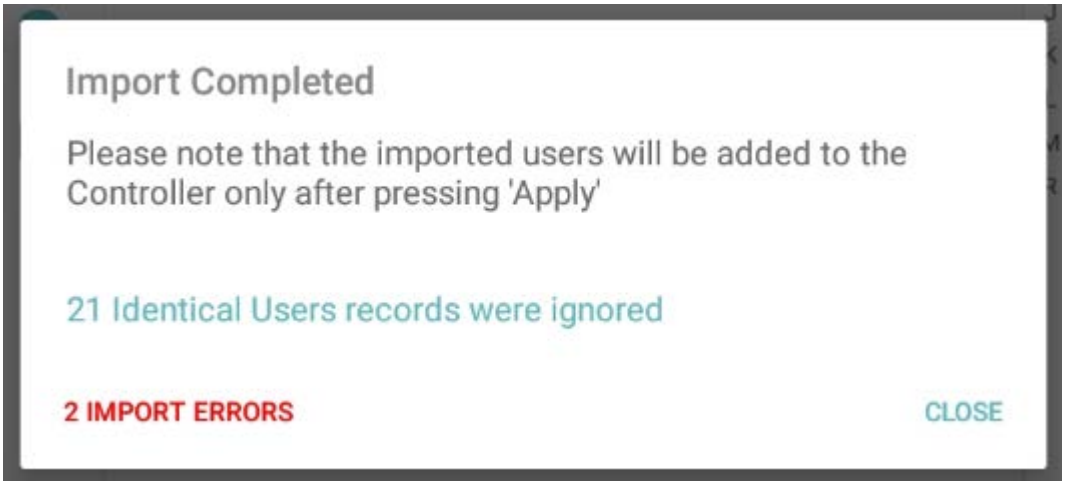
2. Select the file to import from the list. All the files shown in the list are the CSV files currently located in the Users folder (non-CSV files, if any, are not displayed by the application).
3. Tap IMPORT.
4. Records are processed by the application. After importing has finished, the Import Completed message appears with information on the status of imported User records. The following is an example where all the records were successfully imported:



Note

Remember to tap Apply to upload the configuration to the Controller, otherwise your work will be lost.

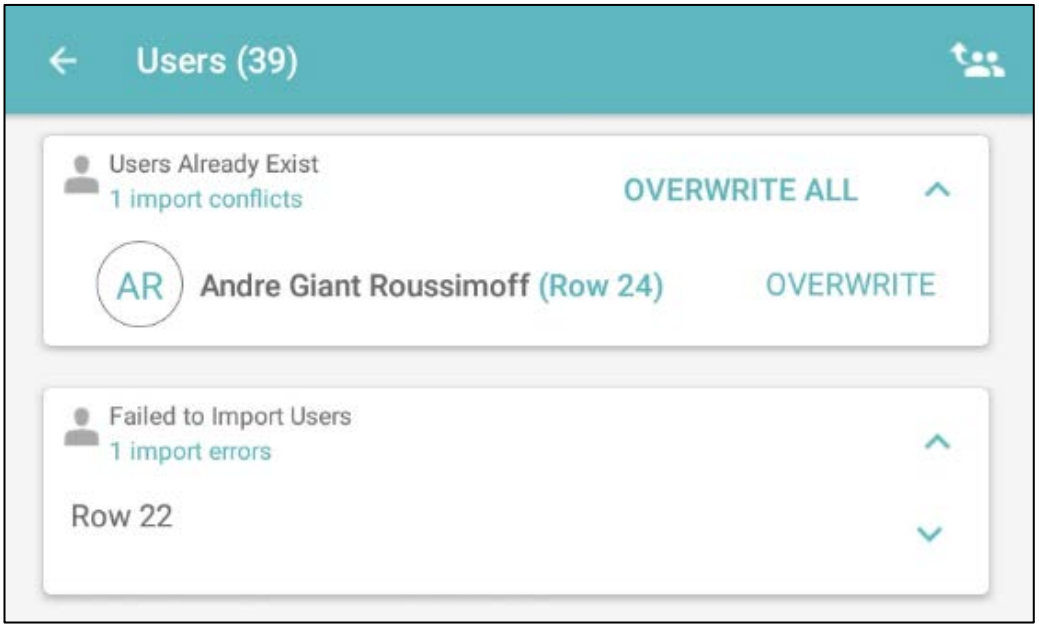
5. If some users were not successfully imported, tap IMPORT ERRORS to open a more detailed page.



6. The page that opens provides more information about user records that were not successfully imported, i.e., user records that already exist in the system but have conflicting data or user records that completely failed to be imported (the system determined the records to be invalid). The row number at the import file is indicated near each record.

   Tap OVERWRITE ALL to overwrite all conflicting user records (if there are more than one) with the imported records or individually examine each conflicting record and tap OVERWRITE next to each specific record, as appropriate.

   Failed to Import User records cannot be imported at this stage. These records can be examined after exporting the Import Results to file (see next section). Touching the record displays the error/s generated when the record was imported. For example, a PIN code is not unique.



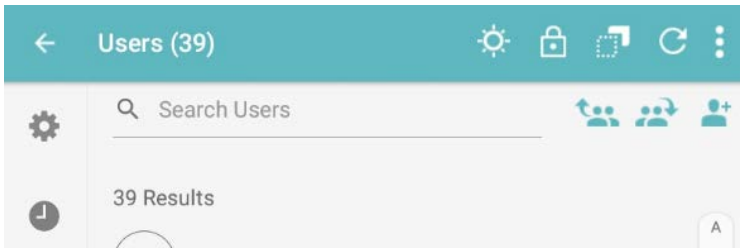
Note

Remember to tap Apply to upload the configuration to the Controller, otherwise your work will be lost.

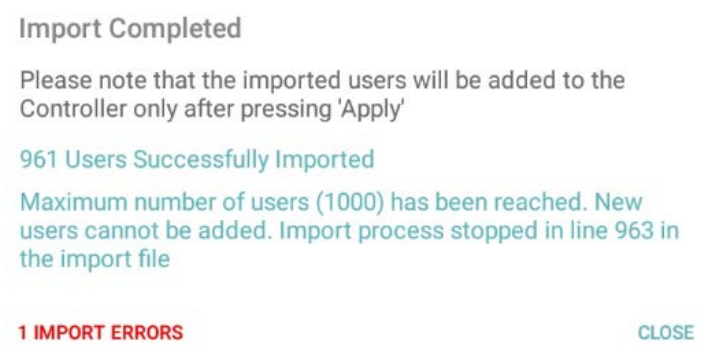
Maximum Number of Users

The Controller supports up to 1,000 users, which are stored in its memory. In addition, the WanderGuard BLUE Manager application processes only the first 1,000 rows of an import file (even if the file contains more than 1,000 rows/users. This section describes how the system handles these boundary situations.

When the Users page is opened in the application, the number of existing uses is displayed.

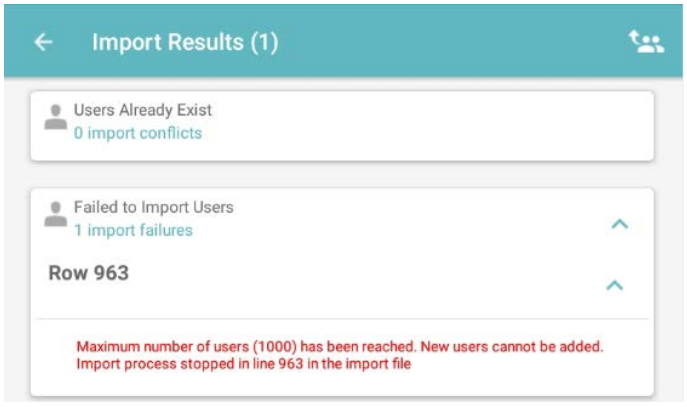


When trying to import users from a file that contains more than 1000 users, a message such as the following is displayed:



Since there are already 39 users in the application, the system imported 961 users successfully (39 + 961 = 1,000). However, an error message is displayed. The reason for the error is that other user entries in the import file were not imported.

After tapping "1 import errors":

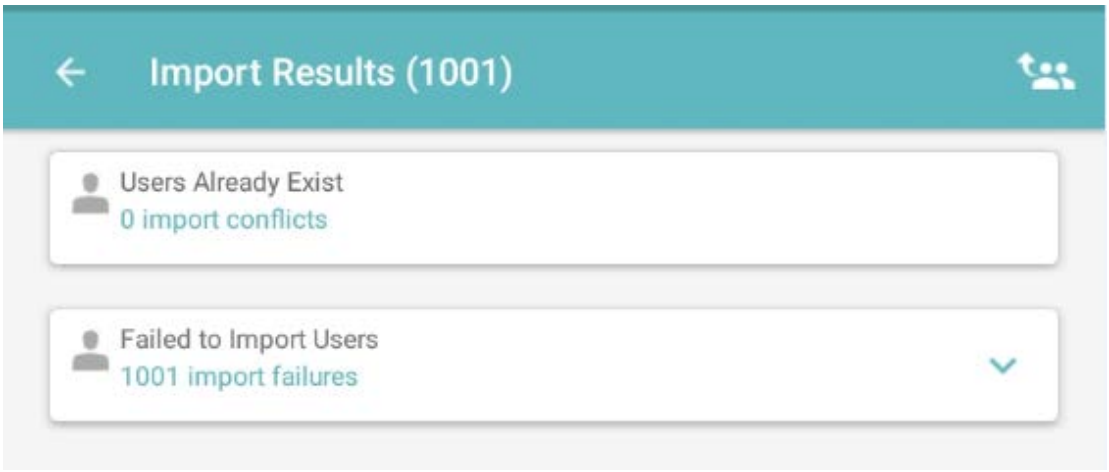


Adding Users from a File with Empty Rows

If an import file includes empty row(s), the system identifies the row(s) as empty, skips them and moves to the next row – up to a total of 1,000 users. If a file has 1,000 rows or more, up to 1,000 rows will be processed, but only those rows with valid data are imported.

Taking an extreme case, if the import file contains 1,000 empty rows (or invalid rows) and valid rows occur only after row 1,000, the import process will stop at row 1,000 and the later (valid) rows will not be reached (or imported).

At the end of the import process, a message appears. This message states that in the import file, 1,001 rows were processed and no new users were found. Tapping the down arrow shows the user rows and that the fields are empty.



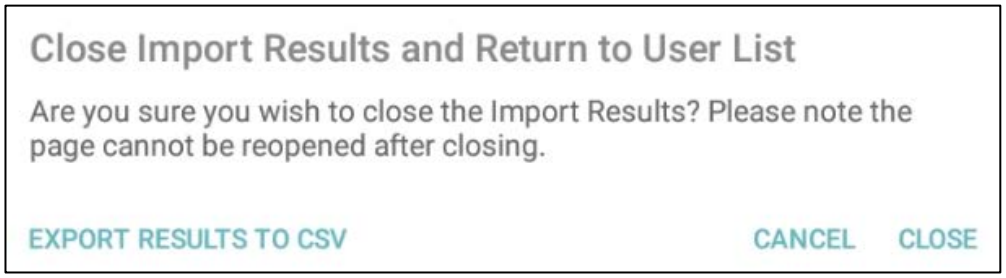
Exporting Results to a CSV File

The imported results can be exported to a CSV file for further examination by tapping the EXPORT icon .

After tapping EXPORT, the exported file is placed in the WanderGuard BLUE folder.

To navigate back to the Users page, tap the back arrow.

Note that you are given a chance to EXPORT RESULTS TO CSV before leaving the page.

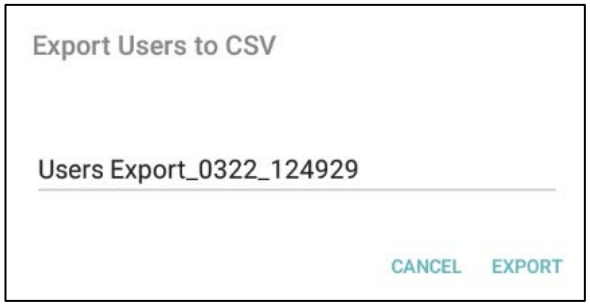


Export Users to a File

User information that was downloaded from the Controller can be exported to a CSV file. The file can later be used for import to another Controller or copied to a computer for maintenance. Alternatively, the file contents can be examined for anomalies, if necessary.

To export the users to a file:

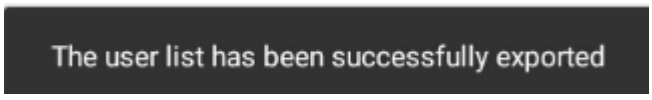
1. In the Users page tap the Export Users icon.
2. The Export Users to CSV message appears:



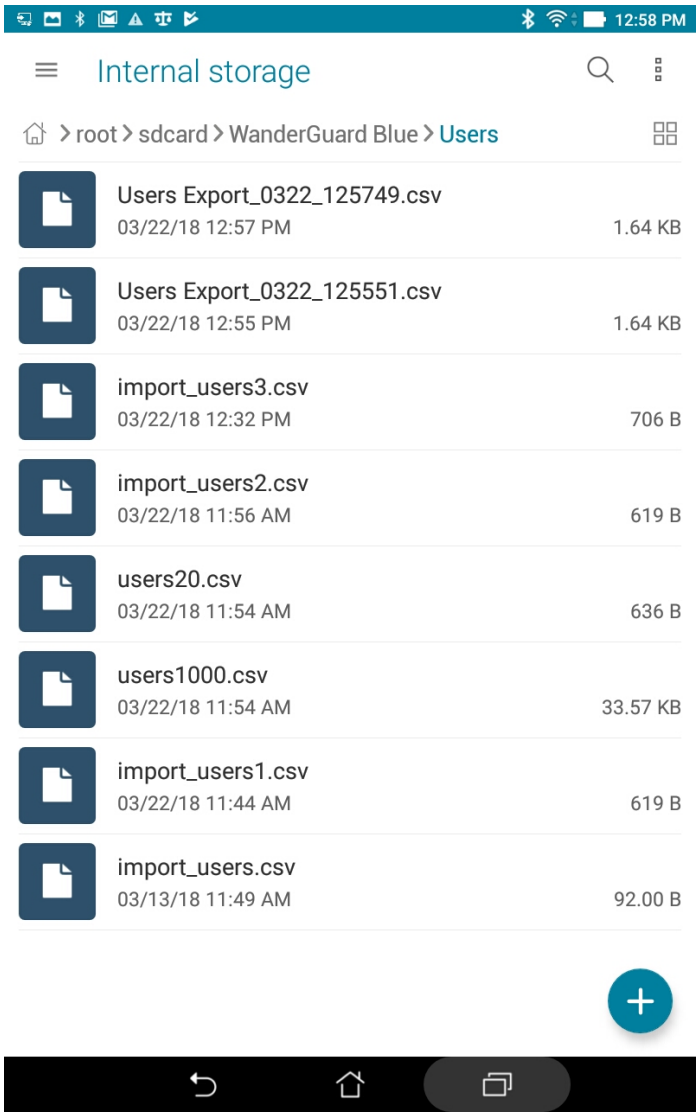
3. Tap EXPORT.

Note the default name given to the file. It can be modified by tapping on the name field and entering your preferred file name.

After finishing the export process, the Export Completed message briefly appears on the snack bar at the bottom of the User page:



The list of imported and exported files can be viewed in WanderGuard BLUE > Users folder in the tablet's Internal Storage folder.

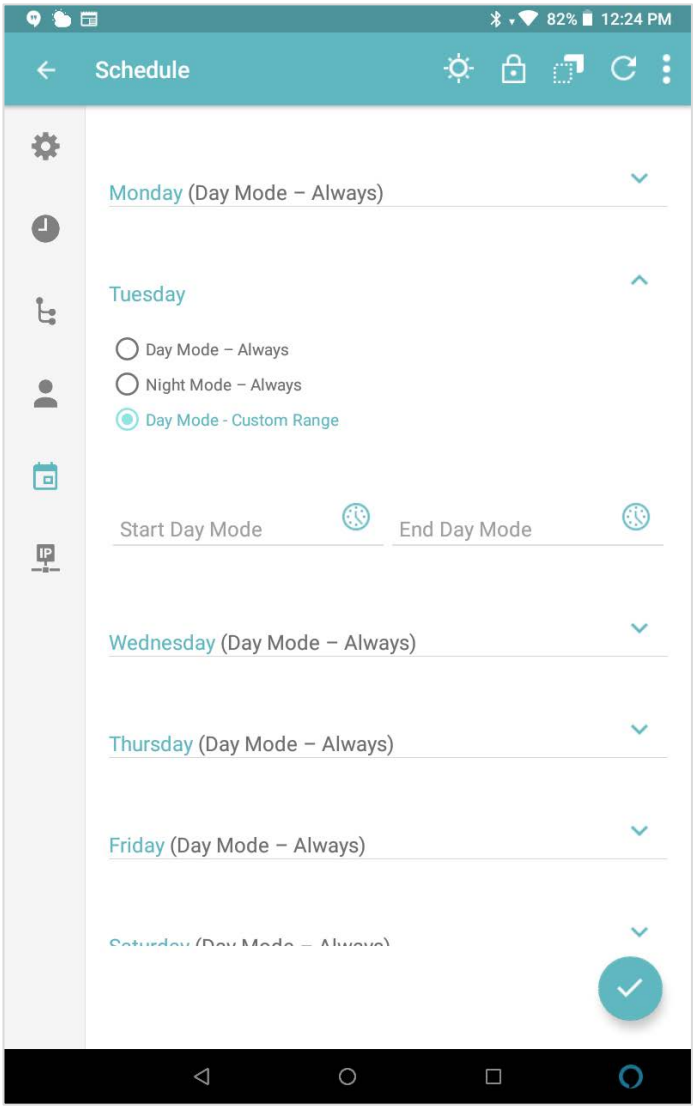


Schedule

The Day/Night Schedule page allows you to schedule day and night shifts for each individual day of the week.

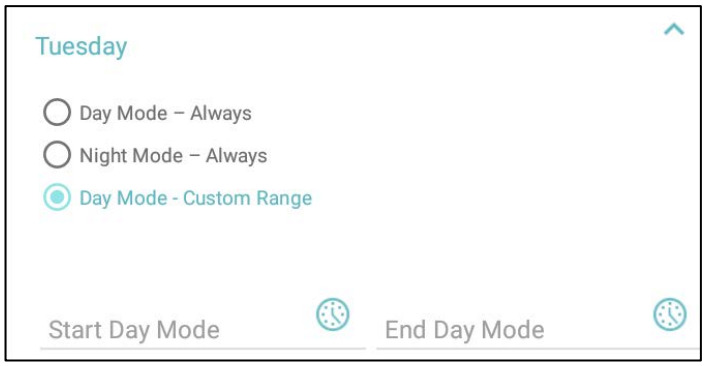
The following options are available:

- **Day Mode - Always** – the Controller is in Day mode all day
- **Night Mode - Always** – the Controller is in Night mode all day
- **Custom Range** – the Controller is in Day mode during specified hours



To Edit the Day/Night mode schedule through the Tablet Mobile App:

1. Tap **Scan** in WanderGuard BLUE Manager to generate a list of Controllers in your range.
2. Tap the Controller of your choice.
3. The Settings page opens for the Controller that you chose.
4. Tap Schedule in the vertical navigation bar to open the Schedule page.
5. For each day in the Schedule page, the configuration options can be expanded:
   ⌄ to expand the daily options
   ⌃ to compress the daily options
6. The following options window opens:



7. If Custom Range is chosen, the Start Day Mode time and End Day Mode are enabled and a specific time can be selected for starting/ending Day mode:

8. Tap Apply to save any changes to the current Controller.

IP Settings

IP Settings of the Controller can be configured in this page. The following parameters are available for configuration

- DHCP
- Static IP Address:
    - IP Address
    - Subnet
    - Default Gateway
- Listening Port (1511)
- Destination Port (12091)

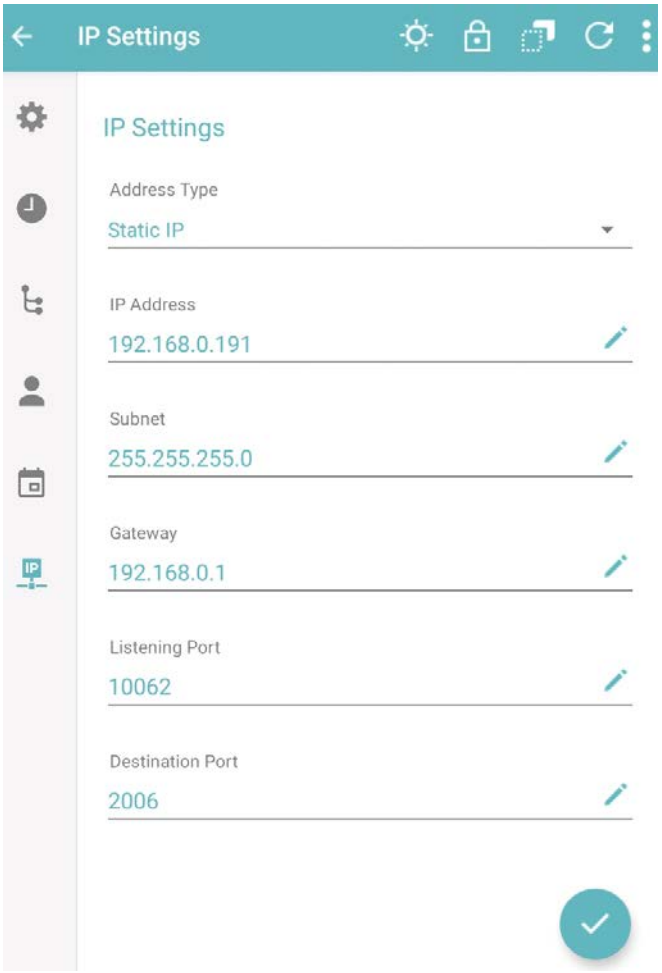
Status

When connecting to the Controller that is set to DHCP, the IP fields will present the IP settings of the Controller. The get status will get the status of the Controller and the IP settings (IP Address, Subnet, Gateway)

When setting the Controller to DHCP, the IP fields are disabled and display the last value until a get status is performed by the application (every 1 min) or by the user (manually).

In a Copy operation:

- Not copied– Type (DHCP, Static), Subnet Mask, Default Gateway, and the IP Address
- Copied - Listening and Destination ports


IP Settings
IP Settings
Address Type
Static IP
IP Address
192.168.0.191
Subnet
255.255.255.0
Gateway
192.168.0.1
Listening Port
10062
Destination Port
2006

Toolbar Actions

The following actions are available from the WanderGuard BLUE Manager toolbar:

- Start/Stop Day/Night Mode
- Start/Stop Override Mode
- Copy/Paste Controller Configuration
- Refresh (Get Controller Properties)
- More – additional options

Start/Stop Day/Night Mode

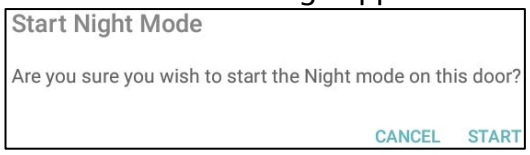
This toggle switches between Day Mode and Night Mode.

Note

Day Mode is the default mode of the Controller.

To toggle from Day to Night Mode:

1. Tap the Day Mode icon .
2. A confirmation message appears:



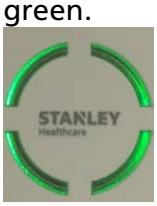
3. Tap Start to begin Night Mode.
4. The Day Mode icon switches to the Night Mode icon .
5. The color of the Controller LED switches to red.

6. The color of the Indoor and Outdoor LEDs switches to red, and the Indoor Keypad screen displays "Ready, Night Mode."

To toggle from Night to Day Mode:

1. Tap the Night Mode icon .
2. A confirmation message appears:

3. Tap Stop to stop Night Mode.
4. The Night Mode icon switches to the Day Mode icon .
5. The color of the Indoor Keypad LED and Controller LED switches to green.



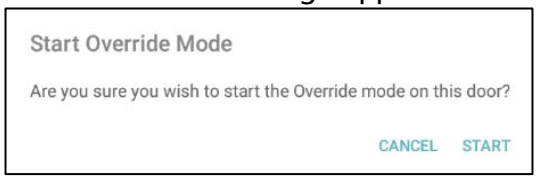
6. The color of the Indoor and Outdoor LEDs switches to green, and the Indoor Keypad screen displays "Ready."

Start/Stop Override Mode

This toggle switches between Starting/Stopping Override Mode on the door supervised by the Controller.

To toggle from non-Override Mode to Override Mode:

1. Tap the icon . This icon is shows that you are in non-Override Mode.
2. A confirmation message appears:



3. Tap Start to begin Override Mode.
4. The icon toggles to the Override Mode icon , and the Controller LED starts flashing Green continuously.
5. The Indoor Keypad LED flashes green and the screen displays "Override."

To toggle from Override Mode to non-Override Mode:

1. Tap the Override Mode icon .
2. A confirmation message appears:

3. Tap Stop to stop Override Mode.
4. The icon toggles to , and the Indoor Keypad and Controller LEDs return to their previous mode (solid Green if it was in Day Mode; solid Red if it was in Night Mode).

Copy / Paste Configuration

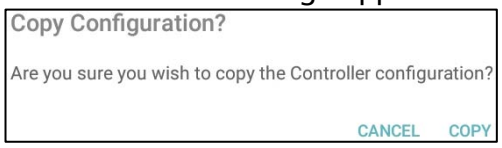
The Copy / Paste function on the Toolbar is used to copy the Controller configuration from one Controller to another. For example, if there are 1000 users defined in one Controller, the user definitions can be copied to another Controller(s) with the entire Controller configuration.

Note

Only one Controller configuration can be current on the tablet at a time. The current configuration on the tablet cannot be "saved" to the tablet for future use. The configuration that was copied in WanderGuard BLUE Manager is available to be pasted until another configuration is copied (over it), or the WanderGuard BLUE Manager application is closed or logged out.

To copy a configuration from a source Controller to a target Controller:

1. Connect to the source Controller.
2. Tap the Copy Configuration icon in the Navigation Bar.
3. A confirmation message appears:



4. Tap Copy to continue.
5. The configuration is copied to WanderGuard BLUE Manager. A message momentarily appears at the bottom of the Tablet screen informing that the configuration was copied, and a Paste icon is added to the Navigation Bar.

In addition, a Copy icon appears in the bottom-left of the window .

6. At this point, the configuration data is stored in the application and is displayed in the WanderGuard BLUE Manager window.
The configuration remains on screen until either a new configuration is copied or you log out of the application.
7. Disconnect from the source Controller.

Best Practice: Typically, a disconnect occurs when physically moving to the target Controller since this usually involves moving out of the BLE coverage of the source Controller. The Paste icon, however, still remains in the Navigation Panel so the configuration is ready to paste into the target Controller.

If the application is still within the BLE range of the target Controller, disconnecting from the Controller can be done by leaving the configuration pages: tap "**X**" next to **Settings** at the top of your WanderGuard BLUE Manager screen.

To paste a configuration from the source Controller to the target Controller:

1. Connect to the target Controller.
2. Tap the **Paste Configuration** icon in the Navigation Bar.
3. A confirmation message appears:

4. There are two options:
   - Tap **Paste**. The copied source configuration is now pasted into the active Configuration pages. The Configuration, however, has not yet been applied to the Controller. The user has the option to change the configuration before uploading to the target Controller.
   - Tap **Paste and Apply.** The configuration is pasted into the WanderGuard BLUE Manager and all copied configuration pages are applied to the target Controller.
5. The **Paste** option allows you to review the configuration and make changes, if necessary, before applying it to the Controller.
   - There is an option to copy only specific pages to the target Controller by navigating to those pages (for example, the Clock Settings page or the Users page) and then tapping **Apply**.
   - There is an option to copy the whole configuration (all the pages) to the target Controller by tapping **More** and then **Apply All**.

Note

A copied configuration that was pasted and applied does not include the Controller Name, Time, Date or Time Zone. This information is taken from the Target Controller.

Refresh Configuration

Refresh updates the WanderGuard BLUE Manager configuration pages (Settings, Clock, Outputs and Schedule) with those of the current Controller configuration.

All changes that were made in the WanderGuard BLUE Manager and not applied are refreshed.

Best Practice: Refresh is a quick way to verify configuration changes that you made in WanderGuard BLUE Manager are applied to the Controller.

To refresh a configuration in WanderGuard BLUE Manager:

1. Tap the Refresh icon in the Navigation bar .
2. A confirmation message appears:

3. Tap Refresh to continue.
4. A "completed successfully" message appears at the bottom of the WanderGuard BLUE Manager screen, and the pages are refreshed with current data from the Controller.

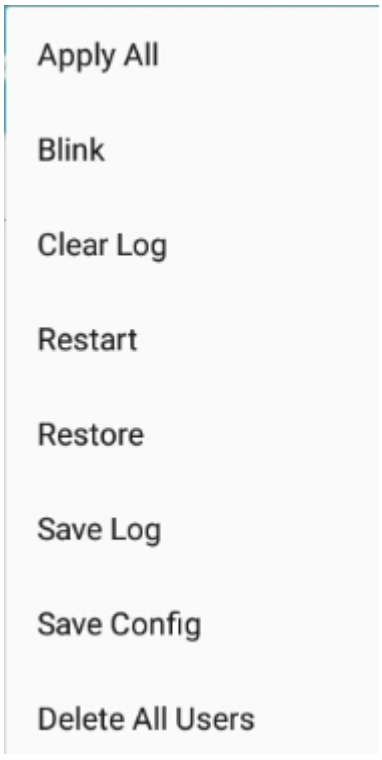
More

The More button contains additional options for working efficiently with WanderGuard BLUE Manager. The same More button options are available from all the Controller Configuration pages.

These include:

- **Apply All** – applies all configuration parameters to the Controller
- **Blink** – Makes the Controller "blink"
- **Clear Log** – Clears the Controller's Log
- **Restart** – Restarts the Controller
- **Restore** – Restores the Controller configuration to the default configuration
- **Save Log** – Saves the Controller Log to a file
- **Save Config** – Saves the Controller Configuration to a file
- **Delete All Users** – Deletes all users on the Users page and Controller

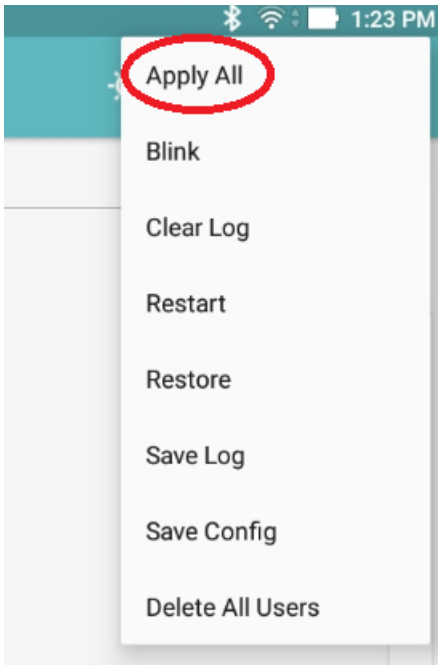
Tap **More** to open a selection window:

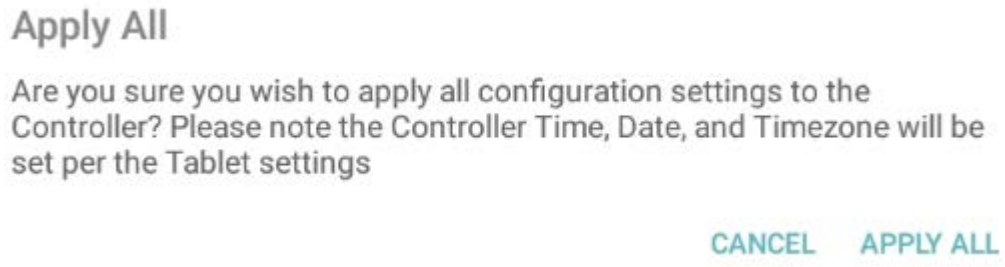


Apply All

This option does the following:

- Applies the entire current configuration in the WanderGuard BLUE Manager to the Controller
- Validates the entire configuration prior to applying the configuration
- Controller's Time (time/date/world Time Zone) is updated with the Tablet's time





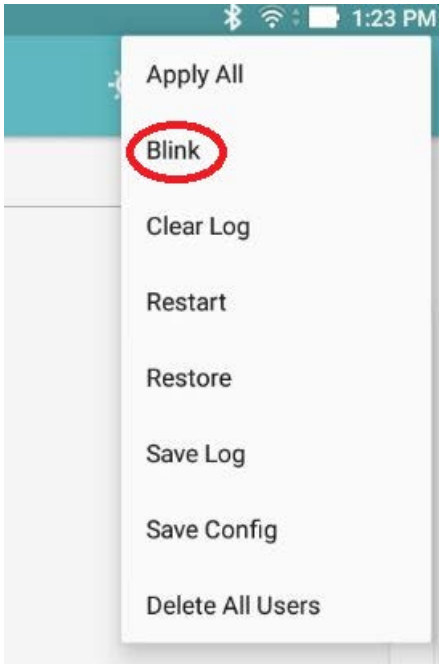
If a validation error is found, the following error message appears:

Blink

Sends a command to the Controller to flash for 5 seconds.

Best Practice: This option is useful if you are working with more than one Controller in a specific area.

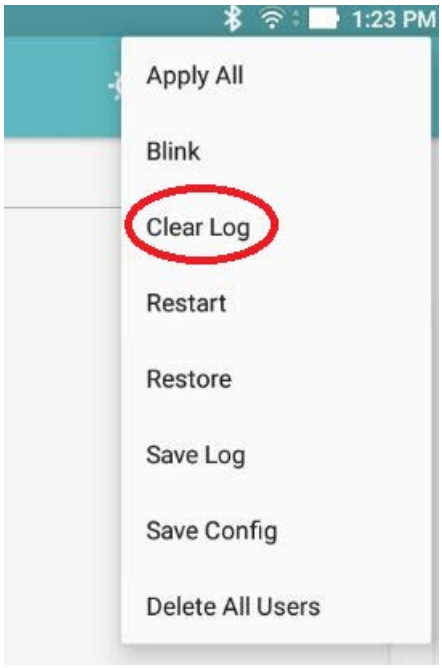
For example, if you wanted to verify that you are connected to a specific Controller, you could "blink" it.



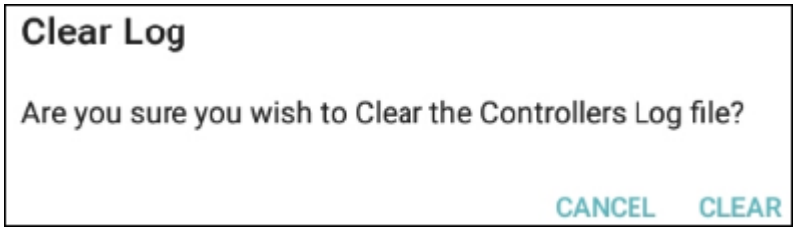
Clear Log and Save Log

Clears all log entries currently in the Controller.

Best Practice: This function is useful during maintenance to eliminate errors and alerts that are no longer relevant.



When you tap **Clear Log**, a confirmation message appears:



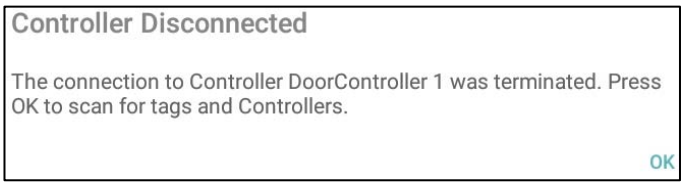
Tap **Clear** to clear the log or **Cancel** to exit without clearing the log.

Restart

Tapping **Restart** power cycles the Controller. The WanderGuard BLUE Manager application automatically jumps to the Scan page and starts the scan process.

When you select **Restart**, a confirmation message appears.

Tap **Restart**. The following message appears:

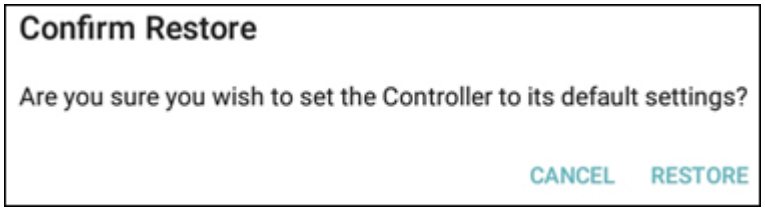


Tap **OK** to continue.

Restore

Restore returns the Controller to its default factory configuration. The default configuration is permanently stored on the Controller.

Tapping **Restore** opens a confirmation message.

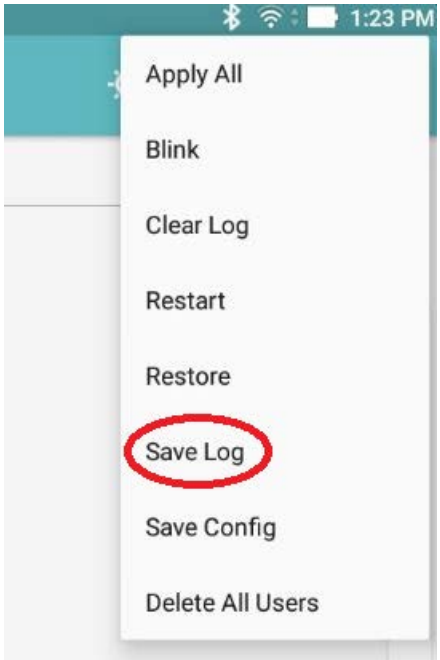


Tap **Restore** to continue. When the command is successfully received at the Controller, the Controller is returned to its default settings.

See the Default settings in Appendix B.

Save Log

Saves the Controller log to a CSV file. The file itself is saved to the Tablet. The Controller log can save up to 1000 entries.



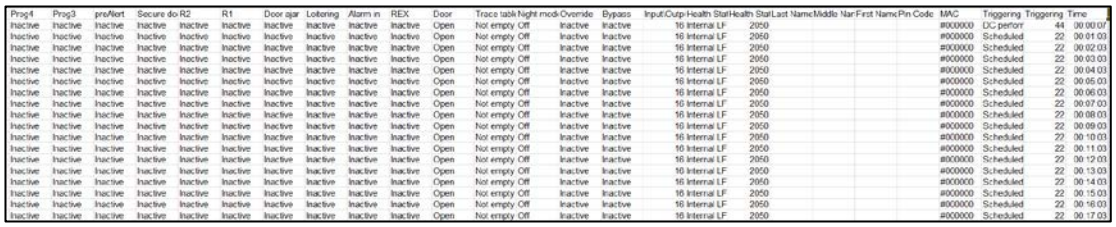
The saved log file can be viewed in Google Sheets, which is installed on the Tablet. The file location is:

- My Files\Internal storage\WanderGuard BLUE

The file name can be changed. The following are the criteria for a valid log file name:

- 1-32 chars: a-z, A-Z, 0-9, ' ', '-', '.', '(', ')'.

The following is a typical Door Controller log file:

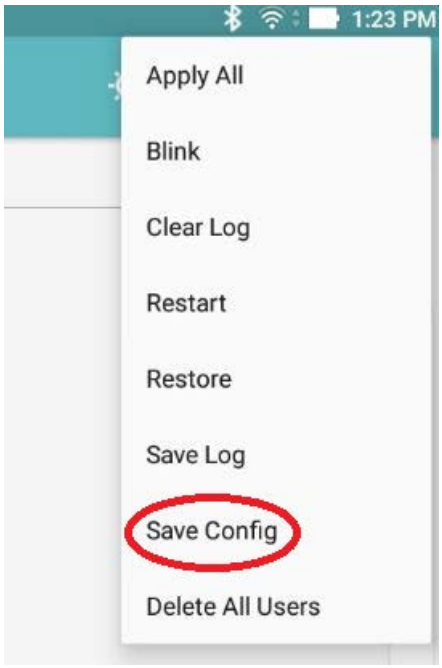


Prog4	Prog3	preAlert	Secure do	R2	R1	Door ajar	Loitering	Alarm in	REX	Door	Trace tabl	Night mod	Override	Bypass	Input/Outp	Health Stat	Health Stat	Last Name	Middle Nar	First Name	Pin Code	MAC	Triggering	Triggering	Time
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	DC perforr	44	00:00:07
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:01:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:02:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:03:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:04:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:05:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:06:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:07:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:08:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:09:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:10:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:11:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:12:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:13:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:14:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:15:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:16:03
Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive	Open	Not empty	Off	Inactive	Inactive	16 Internal I/F	2050						#000000	Scheduled	22	00:17:03

Save Configuration

Saves the entire Controller configuration to a text file.

Best Practice: This function is useful to STANLEY Healthcare's support team for offline troubleshooting.



Tap **Save Config**. A confirmation message opens:

Note

The message informs you that you are saving the Controller's configuration and not the Application Log. The WanderGuard BLUE Application Log is described here.

Tap **Save** to save the configuration. The file is saved in the following location:

- My Files\Internal storage\WanderGuard Blue

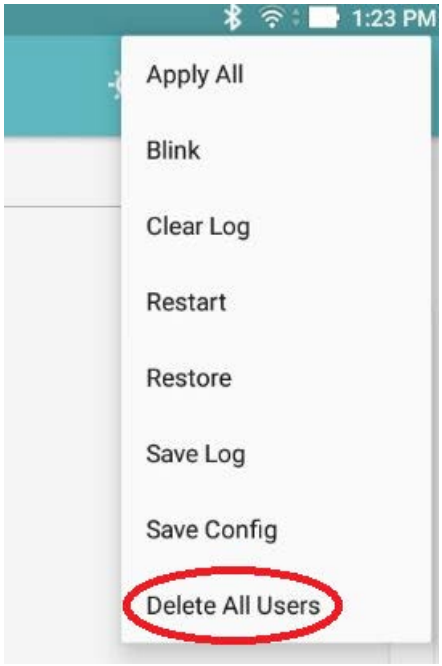
Criteria for a valid file name: 1-32 chars: a-z, A-Z, 0-9, ' ', '-', '.', '(', ')'.

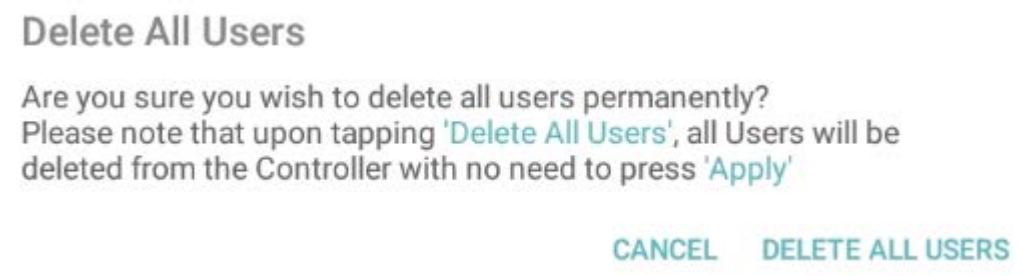
A typical configuration file looks like this:


```
{"clock":{"date":"Jan 23, 2017 12:00:00 AM","hour":
{"hours":7,"minutes":3,"seconds":37},"isDstEnabled":true,"isManualDstEnabled":false,"utcTime":"UTC_MINUS_06_00"},"controllerO
utputs":{"output1":"DEACTIVATED","output2":"DEACTIVATED"},"isConnected":false,"rssi":"-83","schedulerDetails":
{"dayModeConfigurations":{"SUNDAY":{"configurationMode":"INCLUDE_ALL_DAY","day":"SUNDAY"},"MONDAY":
{"configurationMode":"INCLUDE_ALL_DAY","day":"MONDAY"},"TUESDAY":
{"configurationMode":"INCLUDE_ALL_DAY","day":"TUESDAY"},"WEDNESDAY":
{"configurationMode":"INCLUDE_ALL_DAY","day":"WEDNESDAY"},"THURSDAY":
{"configurationMode":"INCLUDE_ALL_DAY","day":"THURSDAY"},"FRIDAY":
{"configurationMode":"INCLUDE_ALL_DAY","day":"FRIDAY"},"SATURDAY":
{"configurationMode":"INCLUDE_ALL_DAY","day":"SATURDAY"}},"settings":{"alarmResetCode":
{"code":"9999","defaultCode":"9999","pattern":{"flags":0,"pattern":"[0-9]{4,4}"}},"bootVersion":"612.18","bypassCode":
{"code":"0000","defaultCode":"0000","pattern":{"flags":0,"pattern":"[0-9]
{4,4}"}},"bypassCodeEnabled":false,"bypassTimeoutDuration":
{"defaultValue":30,"maxRange":300,"minRange":5,"step":5,"unit":"s","value":30,"valueName":"Bypass Timeout
Duration"},"doorAjarDuration":
{"defaultValue":60,"maxRange":300,"minRange":60,"step":10,"unit":"s","value":60,"valueName":"Door Ajar
Duration"},"doorControllerType":"EX5700","dspVersion":"404.20","isDoorAjarEnabled":false,"isLedEnabled":true,"isVisitorCodeEn
abled":false,"lfConfiguration":{"enableExternalLf":false,"externalLfRange":
{"defaultValue":300,"maxRange":300,"minRange":25,"step":25,"unit":"cm","value":250,"valueName":"External LF
Range"},"internalLfRange":
{"defaultValue":600,"maxRange":650,"minRange":150,"step":50,"unit":"cm","value":600,"valueName":"Internal LF
Range"},"isInternalLfEnabled":true,"isLoiteringEnabled":false,"loiteringDuration":
{"defaultValue":60,"maxRange":300,"minRange":60,"step":10,"unit":"s","value":200,"valueName":"Loitering
Duration"},"txInterval":{"defaultValue":300,"maxRange":1000,"minRange":300,"step":10,"unit":"ms","value":300,"valueName":"LF
Tx Interval"}},"mac":{"_mac":[-92,8,-22,-50,105,-18],"_value":180358206089710},"name":"DoorController
1","relayState1":"Inactive","relayState2":"Inactive","visitorCode":{"code":"0001","defaultCode":"0001","pattern":
{"flags":0,"pattern":"[0-9]{4,4}"}}},"status":
{"healthBitMap":2050,"isAlarmModeOn":true,"isBypassModeOn":false,"isNightModeOn":false,"isOverrideModeOn":false,"isVisitorMod
eOn":false},"users":{"usersList":[{"firstName":"tg","lastName":"bb","middleName":"hb","personalPinCode":
{"code":"1254","pattern":{"flags":0,"pattern":"[0-9]{4,4}"}},"userType":"STAFF_MEMBER"}]}}
```


Delete All Users

Allows you to delete all users listed on the Users page and in the Controller. When Delete All Users is tapped, a dialog appears to confirm the deletion of all users. After confirming, the users are deleted from the Controller.





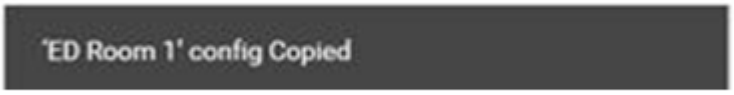
After completion, a "Delete All Users" snack bar message appears.

Note

There is no "undo" to this activity. Use it with care.

Snack Bar

The Snack Bar is located at the bottom of the WanderGuard BLUE Manager page, and a Snack Bar message appears for less than three seconds. It provides immediate feedback regarding whether the action taken by the user (Apply, Start/End, Restore, Save, etc.) was completed successfully.



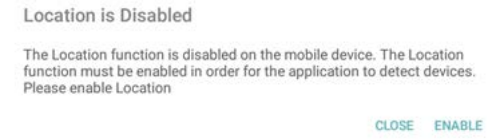
Some messages that appear in the Snack Bar are:

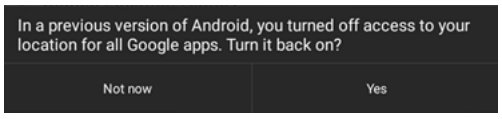
- Successful operation
- Timeout
- Failure in sending the command

Troubleshooting the Tablet Installation

Location services

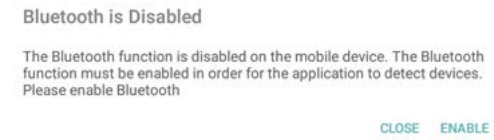
Tap **Enable** when you receive the following message, or if Location is disabled, enable it:





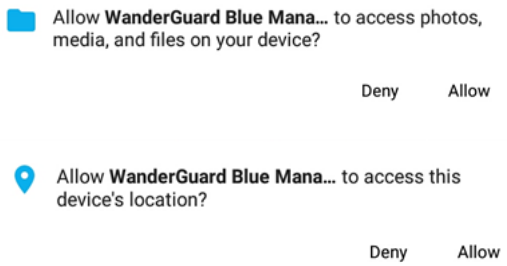
Bluetooth®

Tap **Enable** when you receive the following message, or if Bluetooth is disabled, enable it:



WanderGuard BLUE Manager Access

If you receive requests to allow WanderGuard BLUE Manager to access a device, allow it.

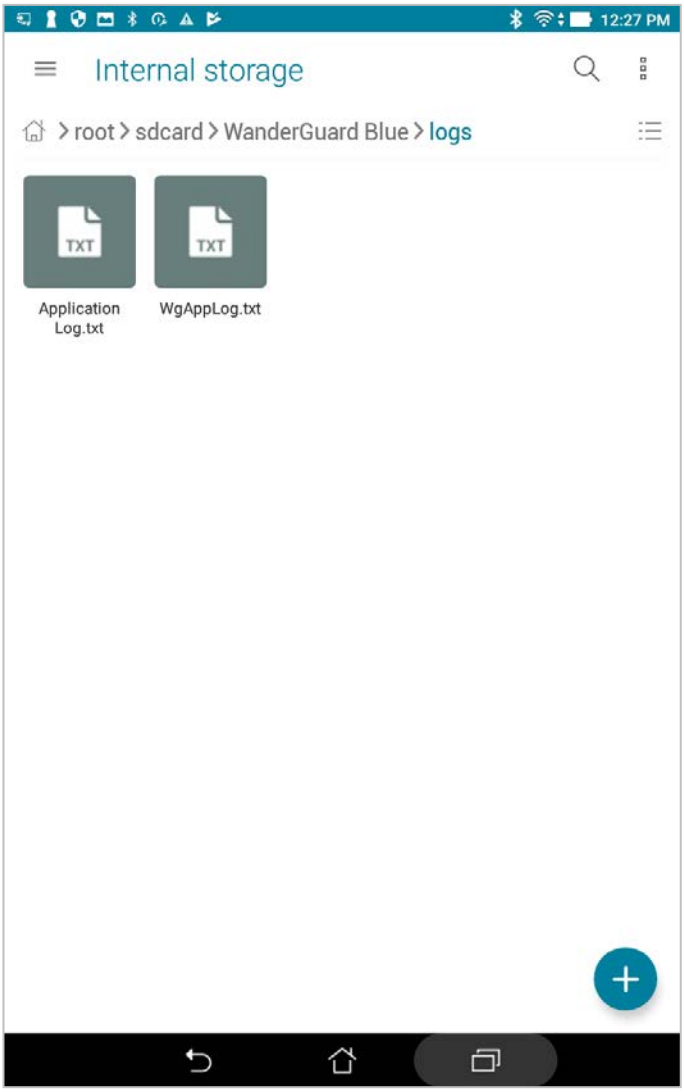


TeamViewer

The TeamViewer application is installed on the Tablet to enable remote access by STANLEY Healthcare service personnel.

Application Log

WanderGuard BLUE Manager logs all system events and records them in the "Application Log.txt" file. Customers or support personnel may be asked to send the Application Log to STANLEY Healthcare service personnel if service is required.

Access the Application Log from the File Manager in the following path:

>root > sdcard > WanderGuard BLUE > logs.