MRS MCharger

Release Notes

Version 2.1.0-Connected

Prepared for MRS Electronic

Contents

Abbreviations 3
Introduction to MRS MCharger Release Notes 4
Notices 4
Pre-Requisites 4
Browser Compatibility 4
Software Access 4
1. New Features 5
1.1. Signature Verification for S32K Module 5
2. Enhancements 7
2.1. RFID Authentication for Scheduled Charging 7
2.2. User Rights for Cloud Users 7
2.3. Status Upload to Cloud 7
2.4. RFID Scanning in EOL 7
2.5. Local Web Portal Login 7
2.6. CAN Communication Status 8
3. Bug Fixes 9
3.1. UI Distortion in Local Web Portal 9
3.2. RFID Label 9
3.3. Activity Chart Date 9
3.4. Password Validation for Wi-Fi 9
3.5. RFID Cards Addition/Deletion 9
3.6. Firmware URL Display 9
3.7. Multiple User Deletion 9

Abbreviations

The following table displays abbreviations used in the document along with their full forms.

Abbreviation	Full Form
CAN	Controller Area Network
OTA	Over the Air
EOL	End of Line
CRC	Cyclic Redundancy Check

Introduction to MRS MCharger Release Notes

Notices

This section lists important notices related to the Mcharger Connected wallbox.

The release date of this version is **September 30th, 2022**.

Pre-Requisites

An internet connection is required for downloading the charging history from the **Local Web Portal**.

Browser Compatibility

The **Local Web Portal** works accurately with the following browsers:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Opera
- Safari

Software Access

Please click the following link for access to the latest version of the Mcharger Connected Software:

https://cloud.mrs-electronic.com/s/3mdCNHBzkEX5jj9

1. New Features

This section discusses the new features included in this release.

1.1. Signature Verification for S32K Module

During OTA installation, **Signature Verification** process is performed for firmware on the S32K module. This ensures that only the trusted firmware is being flashed and running on Wallbox. Bootloader and BL Protocol version **v31** has been provided to support this feature.

Both the bootloader and application have the capability to verify firmware signature.

> **Important**
>
> If the signature verification process fails, the firmware update process will also fail. This prevents receiving firmware updates from invalid sources.

Application Behavior

Application is mainly involved in signature verification during the OTA update. The below-mentioned steps describe the application's behavior for the Signature Verification feature:

- During OTA update, the application writes new firmware to external SPI flash in small chunks.
- Once the write process is complete, firmware is read, and its signature and CRC are verified.
- In case of success, availability of new firmware is communicated to the bootloader and the OTA process continues normally.
- In case of failure, the new firmware gets discarded and the device reboots with the firmware that is already running.

Bootloader Behavior

Bootloader performs the signature verification process at two occasions:

- During the OTA process, when a new firmware is being copied from external SPI flash to internal flash.
- While flashing the application via MRS Developers Studio.

The below-mentioned steps describe the bootloader's behavior for the Signature Verification feature:

- During the OTA process, if the verification fails, bootloader will try to load backup firmware from another partition (if available). Otherwise, the application will not be allowed to run and Wallbox will have to be programmed using MRS Developers Studio.
- While using MRS Developers Studio for flashing, if the verification process fails, the bootloader will enter a **No Program** state. This will halt the bootloader from jumping to application. User is then required to manually send signal to bootloader to bring it out

of this state. This can be done by pressing the **Start MRS** button under **Factory Data** menu in MRS Developers Studio. Bootloader will then get the latest valid firmware from external SPI flash and run the application normally.

> **Important**
>
> Currently, bootloader does not perform signature verification on every bootup. The functionality may be added as an improvement in the later versions, if required.

Backward Compatibility

Following are some of the behavioral expectations with the previous release (v2.0.0-Connected), which does not support signature verification:

> **Important**
>
> Following are the expectations related to OTA updates where the bootloader remains the same and only application gets updated.

- A device running with v2.0.0 can be successfully updated to v2.1.0, but there will be no signature verification performed during the process at any step.
- A device after completing the update from v2.0.0 to v2.1.0 will have the capability to perform signature verification, but only at application level.
- A device updated to v2.1.0 cannot be reverted to v2.0.0. This is because v2.1.0 application will now expect a valid signature in the new firmware that will be missing in the v2.0.0 application header. This will cause the firmware to get discarded and the OTA update will eventually fail.
- A device updated to v2.1.0 will only have the OTA update successful if signature is valid. If the signature is invalid, the OTA process will fail.
- As the bootloader is not updated during the OTA process, no verification will be performed by the bootloader during the OTA or while flashing application via MRS Developers Studio.

2. Enhancements

This section lists all the enhancements made to this release.

2.1. RFID Authentication for Scheduled Charging

RFID authentication, if enabled, is mandatory for the Scheduled Charging feature. The authorization can be performed while the vehicle is plugged-in for charging. Once the vehicle is disconnected from charger, the user will be logged out from the session. This allows Wallbox to retain the information for the users using the Scheduled Charging feature.

2.2. User Rights for Cloud Users

For Wallbox Cloud, access rights for the *Operator* user role have been restricted to call the following functions only:

- **Create/Register:** Allows registering new Wallbox devices.
- **Get:** Retrieves a list of all of the available Wallbox devices.
- **Delete:** Deletes a registered Wallbox device from the database.

2.3. Status Upload to Cloud

The Wallbox status shared with the Cloud is now stored in time series database, instead of keeping it temporarily in cache. This information can then be viewed on dashboard as well.

2.4. RFID Scanning in EOL

RFID scanning can now be verified during End of Line (EOL) Testing through the newly added RFID Test Mode. A CAN message with an expected RFID tag is sent to the Wallbox to enable the scanning process. When in testing mode, Wallbox ignores the RFID authentication flag state.

After scanning a card, the status message showing success or failure of card detection is sent through the CAN bus. The status message contains the following information:

- Whether the scanned RFID tag is the same as the one passed initially to Wallbox.
- State of the RFID module.

If RFID module is not connected or initialized, the status message is sent immediately, indicating a failure.

2.5. Local Web Portal Login

For the Local Web Portal users, you can now log into the portal using either the **User Name** or **Email** field. To support the change, it is mandatory to fill the **User Name** field at the time of signup while providing the email ID is optional.

2.6. CAN Communication Status

In Load Balancing scenario, a new state has been added to the Local Web Portal that indicates a CAN communication error between multiple Wallbox devices. This helps users identify any anomaly in the CAN connection between the devices such as loss of CAN connection.

3. Bug Fixes

This section lists all the bug fixes made to this release.

3.1. UI Distortion in Local Web Portal

The User Interface for Google Chrome users has now been fixed for a sleek display. Previously, if an Admin other than the default one used to login through Google Chrome, the UI would distort. The problem could only be fixed by navigating between other tabs on the dashboard.

3.2. RFID Label

Upon changing the label of an RFID card, only corresponding data is updated. Previously, updating label on one card was affecting data of other cards as well.

3.3. Activity Chart Date

Date/Time displayed in **Activity** section of the dashboard now stays the same as set on the device by the user. Previously, the date and time were being retrieved from internet which was conflicting with that set by the user.

3.4. Password Validation for Wi-Fi

The password field for **Access Point** section now allows you to input alpha-numeric characters. Previously, the field allowed having only integers as input.

3.5. RFID Cards Addition/Deletion

RFID authentication can be applied and removed simultaneously if two cards are added at one time. Previously, if the second card was removed, its re-addition was not allowed. This would also generate an error that the maximum limit for cards has reached.

3.6. Firmware URL Display

Complete firmware URL can now be seen during the OTA installation by hovering over the URL string. Previously, it was overlapping with the other text present on the page.

3.7. Multiple User Deletion

Subsequent deletion of users is now working correctly. Previously, upon deleting a user, deletion of the next user was causing an error.