Alfen NG9xx series Release Notes

NG9xx firmware revision 7.1

Document version 2

7 January 2025

ALFEN
POWER TO ADAPT

Table of contents

1 Introduction

Firmware Release 7.1 includes general improvements, stability improvements, bug fixes as well as preparations for new features.

The new features supported by this firmware release are:

- Wireless Commissioning
- Wireless LAN support
- Using Eve Connect without a password (End user access)
- Support for the improved installer app: MyEve 2.0

This release note describes new features followed by an overview of improvements and bugfixes.

2 New features

2.1 Wireless commissioning feature

This firmware together with the latest hardware prepares Eve Single chargers for Wireless commissioning functionality. Wireless commissioning means configuring an Eve Single S-line or Eve Single Pro-line using a mobile device connected to the WiFi Access Point (AP) of the charging station via the MyEve version 2.0 application. The mobile device and charging station are connected without using the customer LAN. This allows commissioning without a laptop or ethernet cable.

2.1.1 Hardware requirements

The Wireless commissioning feature is available on Eve Single S-line and Eve Single Pro-line produced March 2023 or later. The production date can be found on the type label on the charging station.

2.1.2 Configuring Wireless commissioning on the charging station

By default the Wireless access point will be active after a power cycle (powering Off and On) for a 15 minute period. During this period it is possible to connect a smartphone with the MyEve app.

Wireless commissioning is not possible with the ACE Service Installer. However, it is possible to configure the access point settings via the ACE Service Installer (see the chapter below).

2.1.2.1 Configuration of access point settings using Ace Service Installer

It is required to use the ACE Service Installer Application version 3.7.0
The Ace Service Installer Setup file can be download from this link.

It is possible to permanently disable the Wireless access point via the ACE Service Installer. Alternatively, it is possible to temporarily start or stop the access point using the Ace Service Installer by selecting “Start Access Point”.

2.2 Wireless LAN feature

Wireless LAN access allows Eve Single S-line and Eve Single Pro-line charging stations to connect wirelessly to a local area network.
This connection can be used for:

- Eve Connect
- Modbus TCP energy meters for Active Load Balancing.

For optimal performance it is strongly advised to use a wired connection for Active Load Balancing.

It is not possible to connect multiple Eve Single chargers in a Smart Charging Network using wireless LAN.

2.2.1 Hardware requirements

Wireless commissioning is only available on Eve Single S-line and Eve Single Pro-line produced March 2023 or later. The production date can be found on the type label on the charging station.

2.2.2 Configuring Wireless Lan Access

Configuration of Wireless LAN Access on the charging station can be done with the ACE Service Installer. WiFi credentials cannot be set through backoffice configuration keys due to privacy related regulations.

2.2.2.1 Configuration using Ace Service Installer

It is required to use the ACE Service Installer Application version 3.7.0.
The Ace Service Installer Setup file can be download from this link.

2.2.3 Supported Wireless Network Properties

- Only 2.4 GHz networks are supported
- WPA, WPA2 and WPA3 personal security types are supported
- Open and WEP security networks are not supported due to security vulnerabilities.
- WiFi credentials need to be valid for initiating a connection.
  Valid configuration requirements:
  - SSID which is not empty
  - PSK which is not empty and at least 8 characters long
  - Security type which is one of the supported types

If all the conditions above are not met, configuration is marked as “Not Valid” and the wireless connectivity state is set to “Not configured”.

If the charging station has a valid configuration, it continuously tries to connect to the network.
The wireless interface can be configured to use “Fixed IP address” and it is possible to configure IP address and other related settings.

2.3 End user access feature

Previously the Eve Connect required the owner password of the charging station. This will be referred to as having End user access disabled.

The End user access feature allows end users to access the charging station with Eve Connect app without the owner password.

Two options are added to use Eve Connect without requiring the owner password:

- Use a PIN code to securely use Eve Connect without having to share the owner password of the charging station with the end user.
- No password or PIN code to use Eve Connect

2.3.1 Intended use of End user access

End user access is intended for privately accessible charging stations in a residential situation on a private local area network.

For security reasons it is recommended not to enable end user access on public accessible charging stations (i.e. office, commercial or public environments). For that reason End user access is disabled by default.

End user access can be enabled using Ace Service Installer or MyEve version 2.0.

2.3.1.1 Configuration using Ace Service Installer

It is required to use the ACE Service Installer Application version 3.7.0.321
The Ace Service Installer Setup file can be download from this link.

2.3.1.2 Configuration using MyEve

MyEve 2.0 availability is planned shortly after the official FW 7.1 release.
For the latest information check out the Alfen Knowledge Base.

3 Back-end communication changes

No changes

4 Minor changes

4.1 Progressive webserver lockout

When logging in to the charging station webserver via a local connection, progressive logout of 1, 2, 5 and max 15 minutes enforced when the wrong password is entered more than 5 times for all users. The counter is reset upon a successful login.

4.2 OCPP2.0.1 Improvements

- TC_B_22_CS: Reset Charging Station - With Ongoing Transaction - Immediate:
  Resolved issue with the reset
- TC_E_50_CS: Retry sending transaction message when failed - Max retry count reached - CallError:
  Now complies with TC_E_50_CS. If a transaction event message transmission fails, reschedule the next attempt by multiplying the waiting interval by the number of times the message has been send already
- TC_A_20_CS: Upgrade Charging Station Security Profile - No valid CSMSRootCertificate installed:
  Moved the check on allowed networkprofiles, when using security profile 2 or 3, if there are certificates present inside the charging station, from setNetworkProfile to setNetworkPrio
- TC_M_02_CS: Install CA certificate - ManufacturerRootCertificate:
  Fixed an issue where the charging station was not able to handle the update of a manufacturer root cert via OCPP
- TC_N_28_CS: Get Customer Information - Accepted + no data:
  Add some task switch possibilies and throw the watchdog bone after intensive database queries
- TC_M_07_CS: Install CA certificate - Rejected - Certificate invalid:
  Decline installation of certificate if the certificate has expired
- TC_M_01_CS: Install CA certificate - CSMSRootCertificate:
  Fixed an issue with the OCPP 2.0.1 getInstalledCertificates command that didn't pass the parameters correctly. It didn't pass that it was sending certificateType and certificateHashData
- TC_L_01_CSMS: Secure Firmware Update - Installation successful:
  After a successful firmware installation, send a Security Event Notification Request of type "FirmwareUpdated" as per OCPP 201 specs
- OCPP 1.6 feature profiles are not set correctly:
  Now return
  “Core,FirmwareManagement,Reservation,LocalAuthListManagement,RemoteTrigger,SmartCharging" (including SmartCharging) if we are OCPP 1.6 and 2.0.1 for configuration key "SupportedFeatureProfiles"
- Fixed an issue where a negative value for a charging profile ID causes the charging station to indefinitely keep sending ReportChargingProfiles if the charging profile was requested via OCPP 2.0.1 with a GetChargingProfile request. This has now been fixed and it only sends it once.

4.3 Other changes:

- No longer retry to send OCPP messages that are not supported or implemented by CSMS
- Change modbus function codes to be the same as documentation to decimal
- End user access: Added a way to know the end user password type via the info and mDNS
- Added improvement for Eve Connect to display “Green share” per transaction when Solar Charging
- Fixed the Issue tripped on a DE charging station where at the start of a transaction the activated RCD is no longer reported as 102 but the expected 106.
- Display languages have been updated
- Changing supported TLS cipher:
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 is no longer supported
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 is now supported
- Access Point SSID should always be upper case :
  The AP SSID will automatically convert to upper case upon configuration save, ensuring consistency across all access points.
- Made the interval shorter between OCPP messages that are stored in the transaction database. These are start/stop transaction messages, metervalues, security events, reservations and statusnotifications. This is especially beneficial on charging stations that have a short metervalue interval configured
- Add support for Croatian and Catalan languages to NG9xx translations
- Added support for displaying some Czech character symbols
- We now chunk the getConfiguration message, this allows us to not have to give a message length beforehand. Therefore, we can now buffer per item and keep sending until we are done. The complete message will be buffered by the server side.

5 Firmware update instructions

With the release of NG9xx Firmware 7.0, there is no longer the option between "A and B firmware versions", as first introduced with version 4.14.0

To update to NG9xx Firmware 7.1, please follow the steps according to below schedule:

Current firmware version	Step 1	Step 2
4.12 or lower	Update to intermediate firmware version 6.6.2 version 'A'	Update to the latest firmware version (currently 7.1)
Between 4.14.0 and 6.x	Update to intermediate firmware version 6.6.2 version 'B'	Update to the latest firmware version (currently 7.1)
6.6.2 and higher	Update to the latest firmware version (currently 7.1)	Not applicable

6 Document Revision control

Document revision control			
Date	Version	Description/status	Author
18 November 2024	1	External release (RC)	
7 January 2025	2	External release (official release)	