



How is a key firmware update made, even for different key generations?

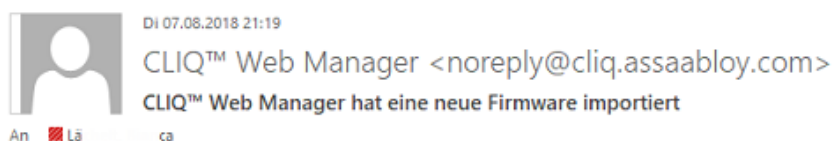
A basic explanation on the subject of "firmware" (abbreviated to FW) can be found in this FAQ: [What is the meaning of firmware?](#)

If we have released key firmware (FW) for you, there are two things to note regarding the keys. There are two different key generations that also have to be updated differently - generation 1 and generation 2. The information card of the key shows which firmware is present in the key and which ASIC chip (generation 1 or 2) is installed there.

For Generation-1 (ASIC 1) keys, there is only single-digit firmware up to 6.x. Generation-2 (ASIC2) keys, on the other hand, have two-digit FW from version 10.x upwards.

Name	Reinigung 1
Org.-Nr.	1.2
Org.-Nr. 2	
Domäne	Default
Schließung	Mechanik
Gruppe	GHS Grup
Typ	E2-Schlüssel
Firmware	6.3.1
Generation	Generation 1
Status	Ausgegeben
Zeile Nummer	

The new firmware can be ordered via the trade partner. It is provided by ASSA ABLOY Sicherheitstechnik GmbH via the CLIQ Data Center (DCS) and the owners of the programming keys with the corresponding role receive an e-mail from the system. For hosting systems and purchase systems with DCS connection, this FW is then automatically imported by the Web Manager.



Firmware für System E7 wurde heruntergeladen.

Bitte folgen Sie dem Link unten, um die neue Firmware zu verwenden.

<https://cliqwebserver03.assaabloy.com/CLIQWebManager>

Diese Tabelle enthält weitere Informationen zu den importierten Firmware-Dateien

Dateiname	Version
16.1.5	16.1.5

MKS: E7 3

- Diese E-Mail wurde automatisch von CLIQ™ Web Manager gesendet

Update Generation-1 Key

For Generation 1 keys, there is the special feature that only one wall programming device can be switched to Updater mode. To do this, a wall-mounted device is selected and changed over via "System info/Remote devices". Updater mode is only active if firmware has been

imported!

WorkSystem InfoAdministrationSettingsAbout

Remote PD

Office

InfoRemote logsSettingsForwardEvents

SYSTEM SETTINGS

Service URLhttps://remoteserver01.assaabloy.com:443/CLIQRemote

Alternative service URL

Server CA certificateO=ASSA ABLOY AB, OU=ASSA ABLOY Sicherheitstechnik GmbH, CN=CLIQ IKON CA

GENERAL

Heartbeat rate (in minutes) *5

Programming device mode☒ Normal☐ Diagnostic

Plug and play☐ Disabled☒ Enabled

Client certificateCN=IKON, OU=60000470, SERIALNUMBER=38-1-1, CN=ED000470-WPD01

Certificate expire date08/10/2023

Select file

Select a .p12 file

IP

Hostname *WALLPD_1_1

IP configuration☐ Static IP☒ Dynamic IP

SaveCancel

* Required fields

PROXY

Proxy☒ Disabled☐ Enabled

OFFLINE UPDATE

Offline update☐ Disabled☒ Enabled

Maximum number of offline updates following an online update per key20 offline updates

Maximum time period between an online and an offline update7 days0 hours0 minutes

Key revocation list validity2 days0 hours0 minutes

Offline revalidation time3 days0 hours0 minutes

KEY FIRMWARE UPGRADE MODE

Key firmware upgrade☐ Disabled☒ Enabled

The firmware is then activated/imported in the CLIQ Web Manager under Administration-Firmware.
Note: A manual import is only necessary if the CLIQ Web Manager is not connected to the CLIQ Data Center (DCS).
To use the current firmware, please press "Apply".

Firmware

Firmware import

Please select a firmware file, and then press the upload button.

Select...Upload Firmware

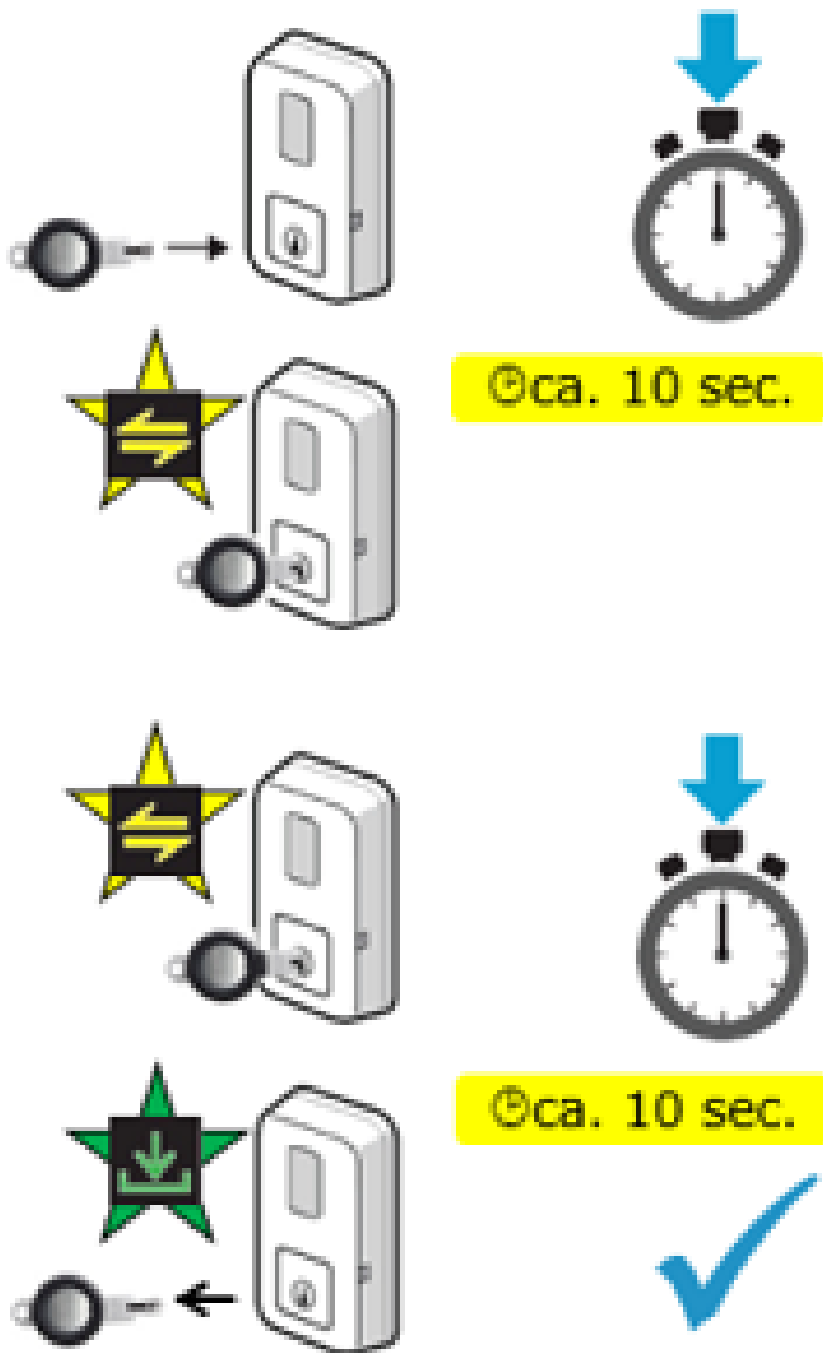
Imported user key firmwareImported C-Key firmwareImported remote PD firmware

Type	Name	Version	Generation	Multi time period schedules	Remote support	Cylinder group support	Flexible revalidation support	Status
🔑	18.1.0	18.1.0	Generation 2	✔	✔	✔	✔	DeleteApplyCancel
🔑	XC_key_16_3_6_fw2	16.3.6	Generation 2	✔	✔	✔	✔	DeleteApplyCancel
🔑	16.3.3	16.3.3	Generation 2	✔	✔	✔	✔	DeleteApplyCancel
🔑	XC_key_16_3_0_fw2	16.3.0	Generation 2	✔	✔	✔	✔	DeleteApplyCancel
🔑	XC_key_16_2_1_fw2	16.2.1	Generation 2	✔	✔	✔	✔	DeleteApplyCancel
🔑	XC_key_16_1_5_fw2	16.1.5	Generation 2	✔	✔	✔	✔	DeleteApplyCancel

This triggers a remote job on all affected Generation 1 keys (with lower firmware).
Tip: The administrator should inform the users accordingly to go to this one updater wall programming device.

Both the new firmware and the restoration of the time and locking authorisation are loaded onto the keys with a single insertion. This takes some time. We recommend a notice on the corresponding wall-mounted devices.

Please be sure to wait until it beeps and the process is complete! If the key is removed too early, it is defective and must be replaced!



Once all Generation-1 keys have received the new firmware, please reset the wall programming device to normal mode.

Update Generation-2 Key

Then the administrator can start the update for Generation 2 key firmware. There are two differences here..

1. All wall programming devices can be activated simultaneously into updater mode as soon as the firmware is applied. The activation can remain permanently in the system and only becomes active when a new firmware is imported.
2. If users remove an ASIC2 key too early during the upgrade process, the key may have lost its permissions. To regain them, the key must be reinserted into the wall programming device. It is not defective.

If a key does not respond for an update on the 2nd attempt at the wall programming device, please remove the battery from the key and insert it into a cylinder. This removes the residual power in the key and resets the key. Then reinsert the battery and insert the key into the wall programming device again.

To activate the updater for ASIC2, only the checkbox in the WPD must be activated. This enables the WPD to perform FW updates for ASIC2 keys if the corresponding FW for ASIC2 keys has been activated.

TIP: For large systems, it would make sense to activate only one unit at a time as an updater.

[Link zum FAQ-Eintrag](#) | Status as of: 15.04.2020 | RedTeam