

**Quick Reference Guide**

**Lock Service 3G**

**ASSA ABLOY**  
Global Solutions

Experience a safer  
and more open world

# Copyrights

*The information in this document is subject to change at the sole discretion of ASSA ABLOY without notice.*

*Any use, operation or repair in contravention of this document is at your own risk. ASSA ABLOY does not assume any responsibility for incidental or consequential damages arising from the use of this manual.*

*All information and drawings in this document are the property of ASSA ABLOY. Unauthorized use and reproduction is prohibited.*

November 2022

# Table of contents

<b>1. Introduction.....</b>	<b>4</b>
1.1 Installer file verification .....	4
1.2 Security best practices .....	5
<b>2. Connections.....</b>	<b>5</b>
<b>3. Readout.....</b>	<b>6</b>
3.1 LockLog (empty) .....	6
3.2 LockLog with events .....	7
3.3 Parameters .....	8
3.4 Passage schedule .....	12
3.5 Status .....	12
<b>4. Initiation.....</b>	<b>13</b>
4.1 Initialize lock .....	13
4.2 Set time in lock .....	14
4.3 Configure lock .....	15
4.4 Upload firmware .....	18
<b>5. Setup.....</b>	<b>22</b>
5.1 Server connections .....	22
5.1.1 Add web client account in Visionline .....	22
5.1.2 Set up Web API connection in Lock Service 3G .....	23
5.1.3 Give web client in Visionline special rights .....	24
5.2 Download data from server .....	26
5.3 Download firmware .....	27
<b>6. Tools .....</b>	<b>28</b>
6.1 Export .....	28
6.2 Power open .....	29
6.3 Factory reset .....	30
6.3.1 Coldstart - 3G .....	31
<b>7. Database.....</b>	<b>32</b>
7.1 LockLog .....	32
7.2 Compress database .....	33
<b>Revision history.....</b>	<b>34</b>

# 1. Introduction

*Lock Service 3G* is a software used for reading events from a lock and initializing lock specific data. A PC running Windows 8/10/Server 2008/Server 2012/Server 2016 and with a free USB port can use *Lock Service 3G*; this PC is referred to as a service PC. To install *Lock Service 3G*, double-click on the file **LockService3G.msi** located in the *Lock Service 3G* which is located in the folder of 'Visionline bundle'. Follow the instructions on the screen.

**Note:** *Lock Service 3G* 2.2.2.7 and higher uses a WiX installer instead of the previously used InstallShield installer. It is not possible to upgrade from a *Lock Service 3G* version based on InstallShield to a *Lock Service 3G* version based on WiX; instead first uninstall the *Lock Service 3G* version based on InstallShield and then install the *Lock Service 3G* version based on WiX.

**Note:** If the Visionline option *Import user and operator data from Active Directory* is applicable, *Lock Service 3G* can from version 2.1.0.3 be run in two different modes. See *Option instruction Import user and operator data from Active Directory* for detailed information.

## 1.1 Installer file verification



In order to ensure that our customers operate authentic software free from malware, we scan our releases on a regular basis to detect existing and previously unknown threats. We also sign the installers with our certificates which are publicly recognized and trusted by Microsoft, to allow customers to trust that each release contains authentic software.

1. Follow the instructions in the document *Quick reference guide Checksum comparison* (available in the Visionline bundle) to calculate the checksum for the *Lock Service 3G* installer.
2. Compare the calculated checksum with the one provided in the PDF *Checksum for Lock Service3G vX.X.X.X installer* (located in the same folder as the *Lock Service 3G* installer).
3. See the document *Quick reference guide Checksum comparison* for information on how to proceed after the comparison.

## 1.2 Security best practices

- Always have the latest software and firmware installed to benefit from the latest functionality updates and security enhancements.
- Do not share login credentials unencrypted (e.g., via unencrypted email).
- Beware of any suspicious activity, such as signs of tampering of doors or locks.
- Service tools should only be used on restricted networks.
- Ensure all service personnel is authenticated and from an authorized partner.
- We provide security information and advisories for our products and services at [Hospitality Product Security Center](#). In case of any vulnerabilities impacting our products or services, we publish advisories in accordance with our responsible disclosure policy.

## 2. Connections

	<p>The service PC is connected to the server via LAN, and to the <i>USB interface 3G</i> via an USB port. When communicating with a lock, a service cable is connected to the <i>USB interface 3G</i>; see picture below. <b>Note:</b> For setup of the host server, see section <a href="#">Server connections</a>.</p>
	<p>At delivery, the <i>USB interface 3G</i> is configured as an FTDI device (<i>Future Technology Devices International</i>). The communication between service PC and <i>USB interface 3G</i> is handled by the FTDI driver. The first connected <i>USB interface 3G</i> will be called <i>FTDI0</i>, the second one <i>FTDI1</i> etc.</p>

**Note:** If the FTDI driver is not detected by the operating system, the driver can be downloaded from the FTDI web site; choose the applicable one among the *D2XX* drivers.



Service cable



Lock connector

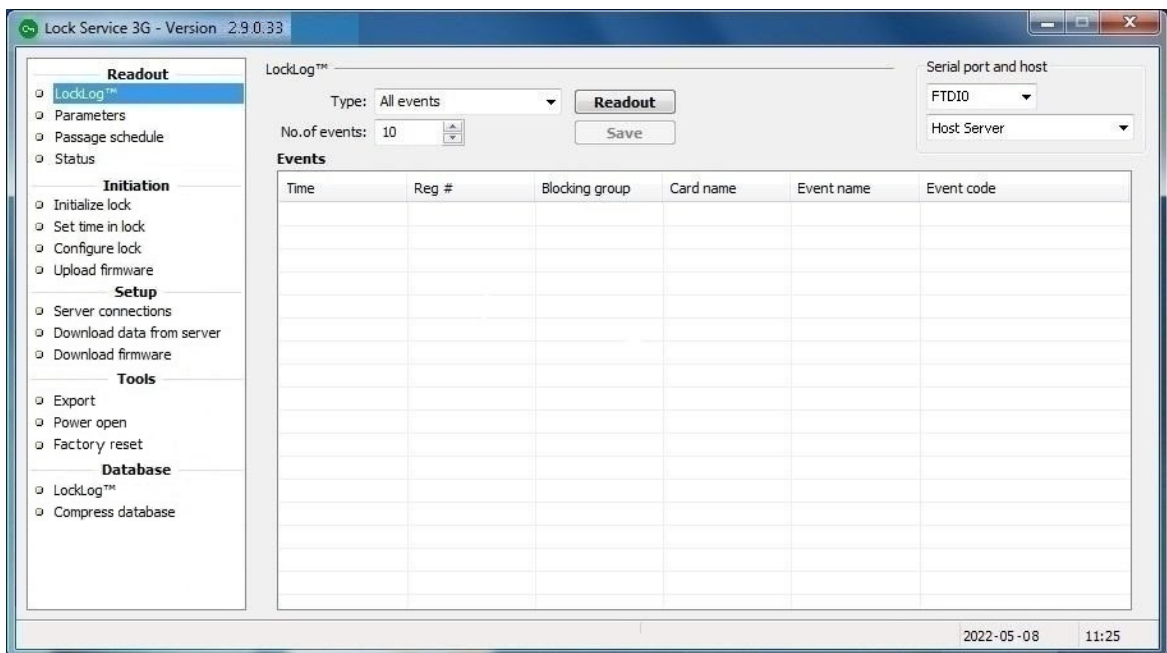
## 3. Readout

The **Readout** section includes four selections:

- LockLog
- Parameters
- Passage schedule
- Status

### 3.1 LockLog (empty)

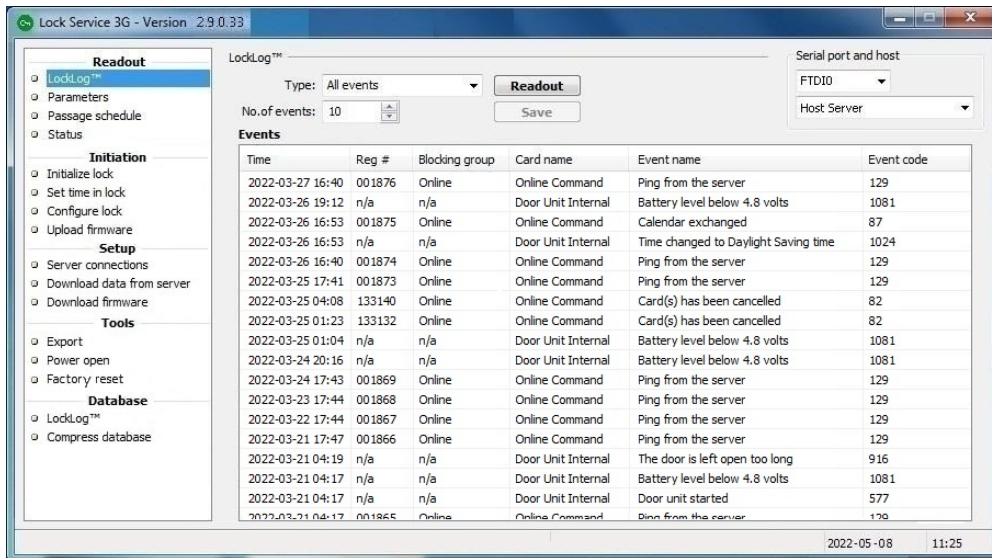
The **LockLog** shows a list of events.



1. Insert the applicable service cable in the lock.
2. Select the applicable type of event in the **Type** drop-down list.
3. Select the applicable **No. of events** and click the **Readout** button.

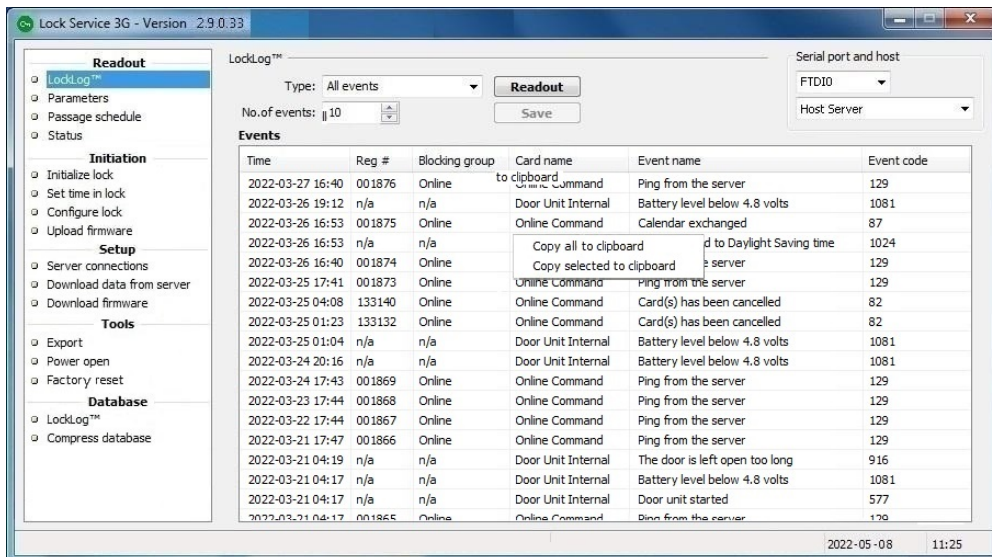
### 3.2 LockLog with events

The events are listed in the **Events** area.



1. To save, click the **Save** button. See section [LockLog](#) for information on how to look at the saved events later on.  
**Note:** 3000 events can be saved to the database.

To copy one or more events to the clipboard:



1. Right click on a parameter and choose the applicable alternative **Copy all to clipboard** or **Copy selected to clipboard**.

### 3.3 Parameters

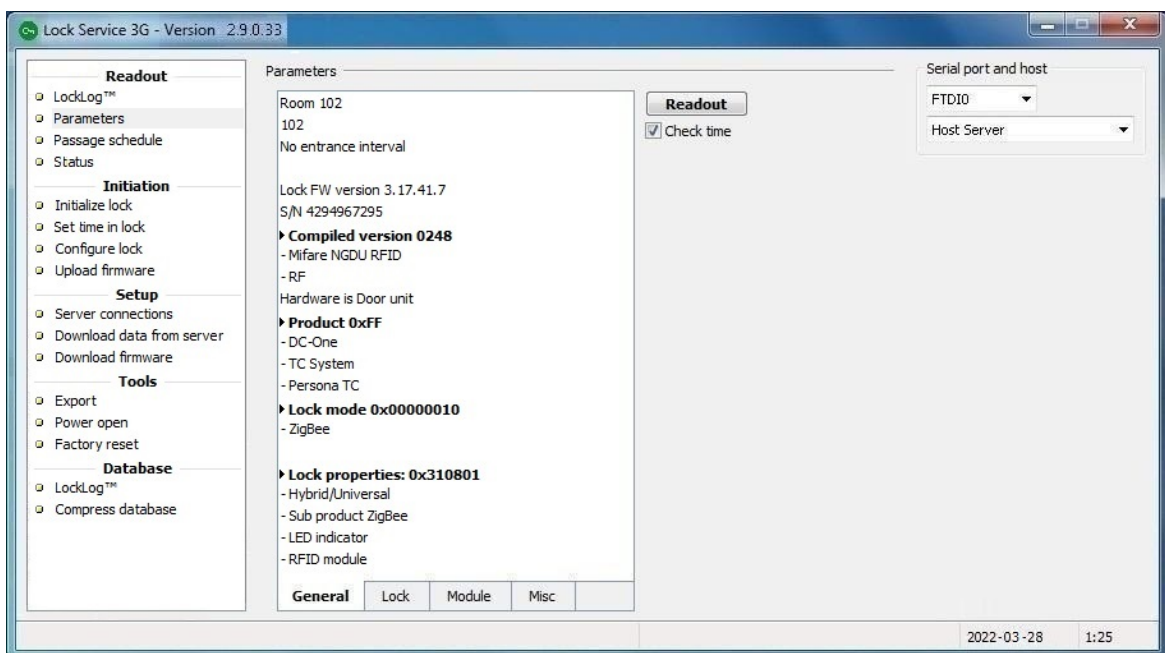
Under the **Parameters** section, there are four different tabs:

- [General](#)
- [Lock](#)
- [Module](#)
- [Misc](#)

To make a parameter read-out:

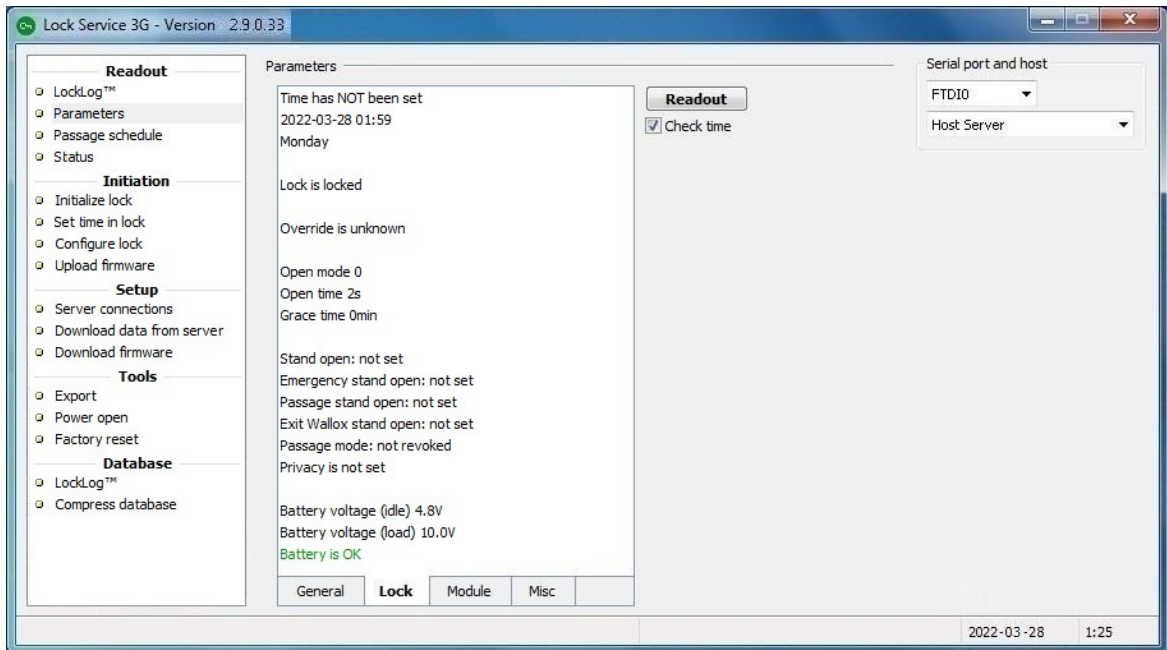
1. Connect the service cable to the lock.
2. If the checkbox 'Check time' is marked (default), the time in the lock will be compared with the time in the service PC. If the difference is more than 5 minutes, a question to set the time will be shown.
3. To read all lock specific parameters, click the **Readout** button.

**General** tab:



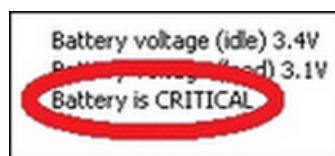
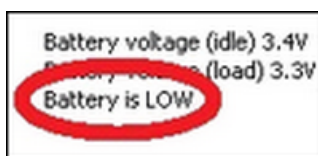


**Lock tab:**

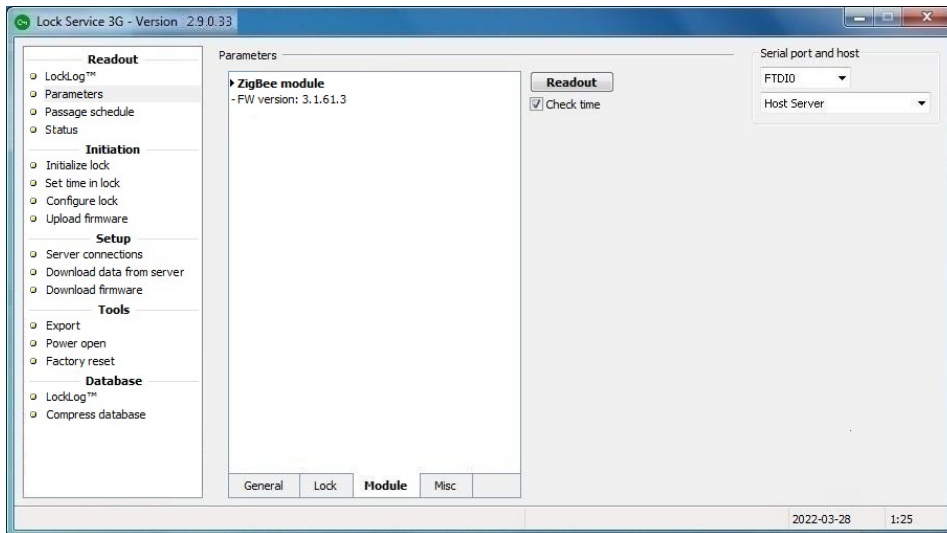


Battery voltage (idle)	Battery voltage when the lock is not used, i.e. no event is sent and no card reading is ongoing. <b>Note:</b> The <i>idle battery voltage</i> is measured once per hour.
Battery voltage (load)	Battery voltage when the lock opens

**Note:** Be aware if the battery voltage (load) is low or critical, see examples below. If a valid card is presented at the lock, 'battery is low' is signaled by four orange LED blinks and one green LED blink. 'Battery is critical' is signaled by four orange LED blinks and one red LED blink.



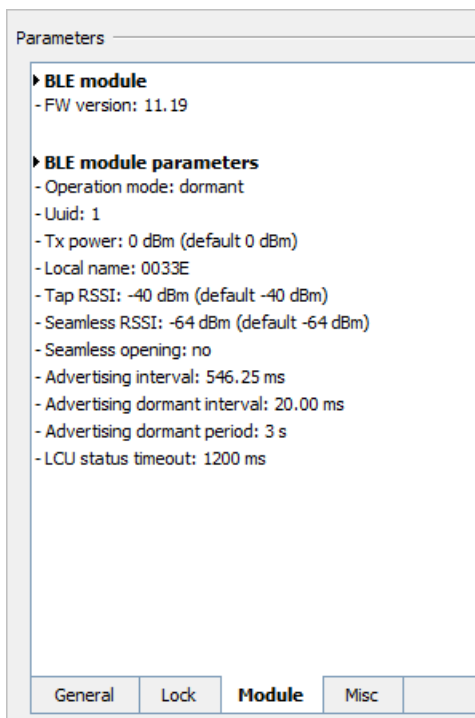
**Module tab:**



If BLE is applicable, BLE module parameters will be shown at parameter read-out as in the picture below if both of the following criteria are met:

- either a built-in BLE module in LCU 6351 / LCU5351 / LCU 5352SC1 or a separate BLE module of generation 2 (part number 4827663) is used
- the LCU firmware version is 3.xx.38.xx or higher

**Note:** If the above criteria are not fulfilled, only 'FW version' under the heading 'BLE module' will be shown.



Parameter	Description
UUID	A 'channel' identifier that the BLE module advertises, signifying the group it belongs to, for example a particular hotel chain, or in the example '9' = AAGS
Tx power	Radio transmit level of the BLE module
Local name	The local name of the BLE module, which can be seen when the module BLE advertises.
Tap RSSI	See description <a href="#">here</a> . (RSSI = <i>received signal strength indication</i> )
Seamless RSSI	See description <a href="#">here</a> .
Seamless opening	Seamless opening should only be set to 'yes' in the special cases described <a href="#">here</a> .
Advertising interval	How often the BLE module advertises when it is in advertising mode (this mode not yet implemented as of August 2020).
Advertising dormant interval	How often the BLE module advertises when it is woken from dormant mode by an LCU (pinger function).
Advertising dormant period	How long the BLE module will search for a phone after being woken up from dormant mode.

By default, all locks support *tap mode* which is the mode where a phone is tapped against the lock to unlock the door. In addition to the *tap mode*, the *seamless mode* may be used in special cases when the phone can unlock the door at a longer distance, i.e. without tapping against the lock. The currently supported seamless use cases are

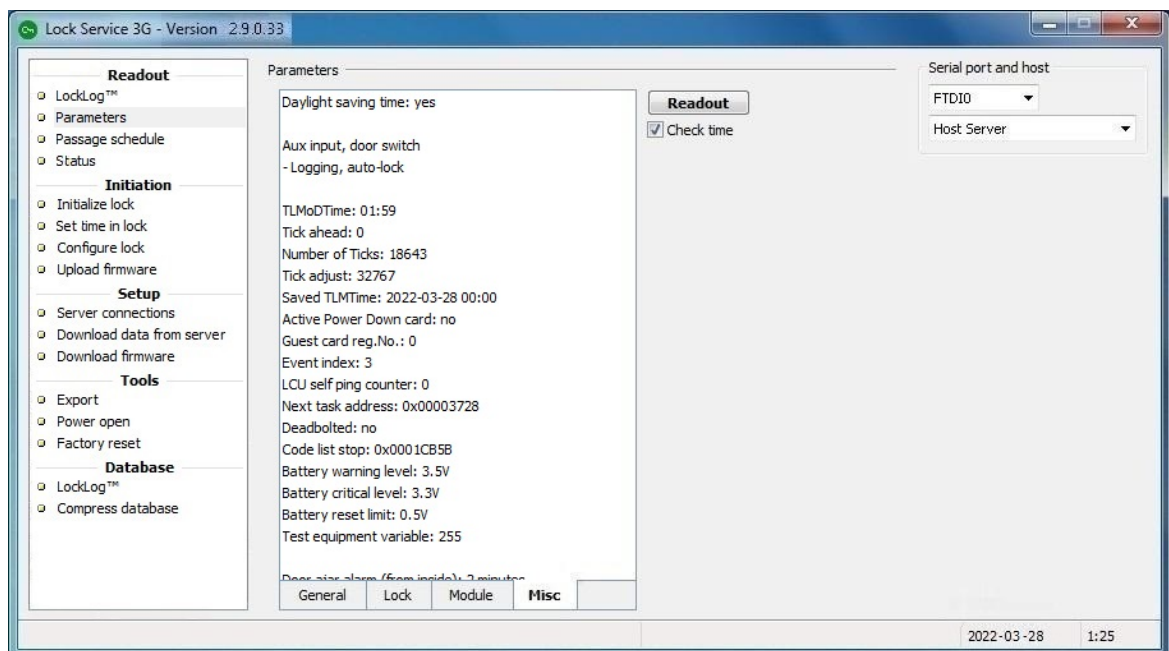
- using an Apple Watch or Android wearable device to trigger unlocking
- using beacons and positioning to trigger unlocking

**Important:** If the hotel does not support the above cases, seamless mode MUST be OFF (i.e. the checkbox 'Enable seamless opening' is unmarked).

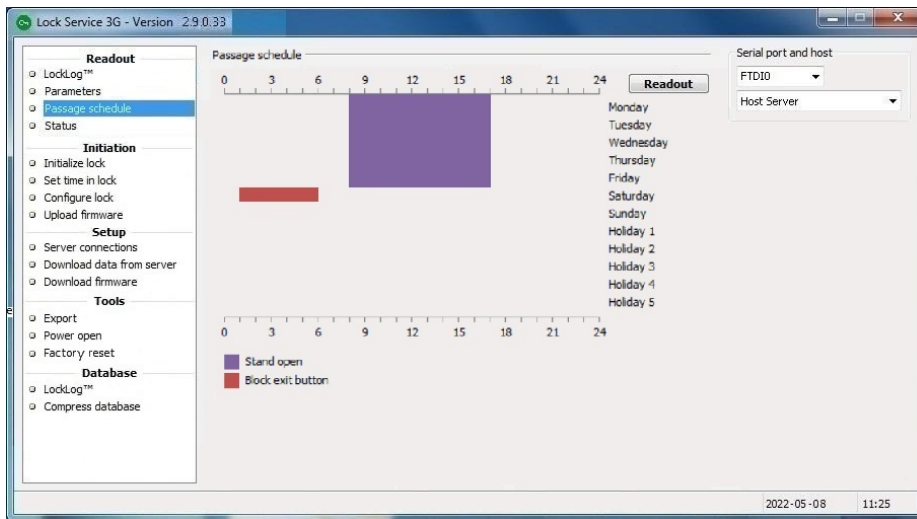
If on the other hand the seamless use cases mentioned above are supported, the checkbox 'Enable seamless opening' (see picture [here](#)) should be marked and the parameter **Seamless RSSI** be adjusted so that a suitable connection distance between phone and lock is achieved. Available values are +12 dBm, +6 dBm, 0 dBm (default) and -6 dBm.

**Note:** The **Tap RSSI adjustment** should normally not be touched, but be left at the default. If necessary, the default can however be modified by -3 or -6dBm (to make mobile keys work further away from the lock) or by +3 or +6dBm (to make mobile keys work nearer to the lock).

#### Misc tab:



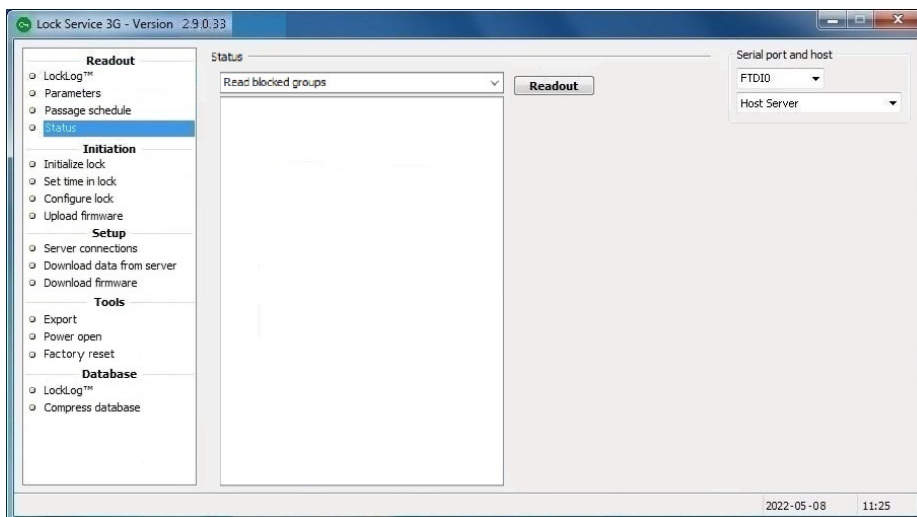
### 3.4 Passage schedule



1. Connect the service cable to the lock.
2. To read all the lock passage schedules, click the **Readout** button.

### 3.5 Status

A status read-out will show blocked groups.



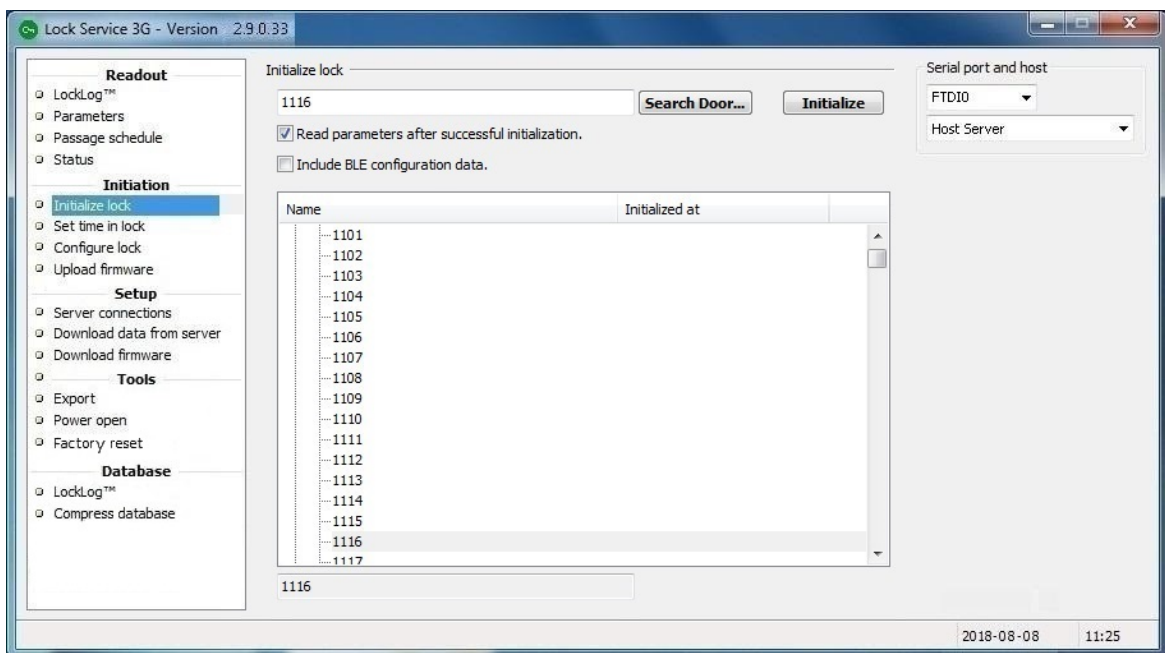
1. Connect the service cable to the lock.
2. Click the **Readout** button.

## 4. Initiation

The **Initiation** section includes four selections:

- Initialize lock
- Set time in lock
- Configure lock
- Upload firmware

### 4.1 Initialize lock



1. Connect the service cable to the lock.
2. Enter the desired room number in the field on top of the window and click **Search Door**. If the door exists in the database, it will be marked in the list and the room number will also appear in the grey field underneath the list. If the door does not exist in the database, a message about this will be shown.
3. If the lock parameters should be read out directly after the initialization, mark the checkbox 'Read parameters after successful initialization'. *Lock Service 3G* will then switch to the dialog **Parameters** (see section [Parameters](#)) when the initialization has succeeded, and automatically perform a parameter read-out.
4. If the Visionline software option *Mobile access* is applicable, mark the checkbox 'Include BLE configuration data'. The signal strength is by default 0 dBm and seamless is by default OFF; if any of this should be changed, go to [Configure lock](#) and change it there.

5. Select a room and click the **Initialize** button.

**Note:** From Lock Service 3G v2.9.0 (included in Visionline bundle v1.28.0), the following applies:

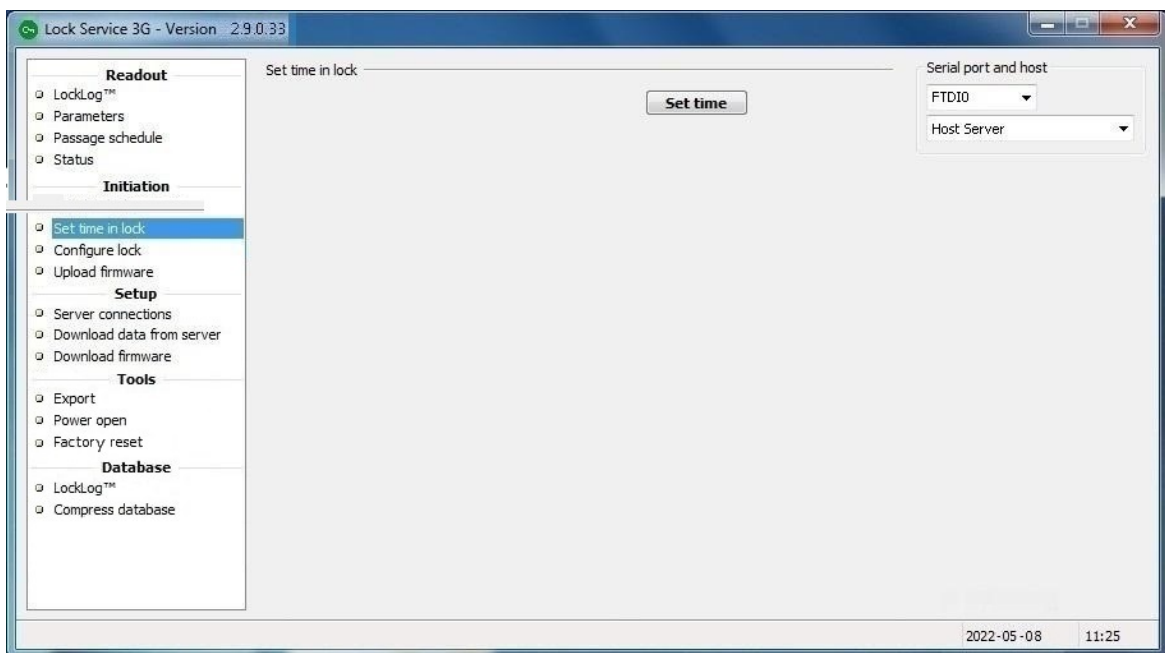
- **Set system ID in lock** is no longer available as a separate alternative in Lock Service 3G. System ID is now set during the lock initialization.
- Valid guest cards will not be cancelled when a lock is initialized.

When a room is initialized, the initialization time will be saved in the database. The initialization time will be shown to the right of the door in the **Initialize lock** dialog; see screenshot above. If new door data is read from the server, the initialization time will disappear from the dialog. When the room is initialized with the new door data according to steps 1-2 above, the new initialization time will be shown in the **Initialize lock** dialog.

**Note:** At initialization, the time will be set in the lock.

## 4.2 Set time in lock

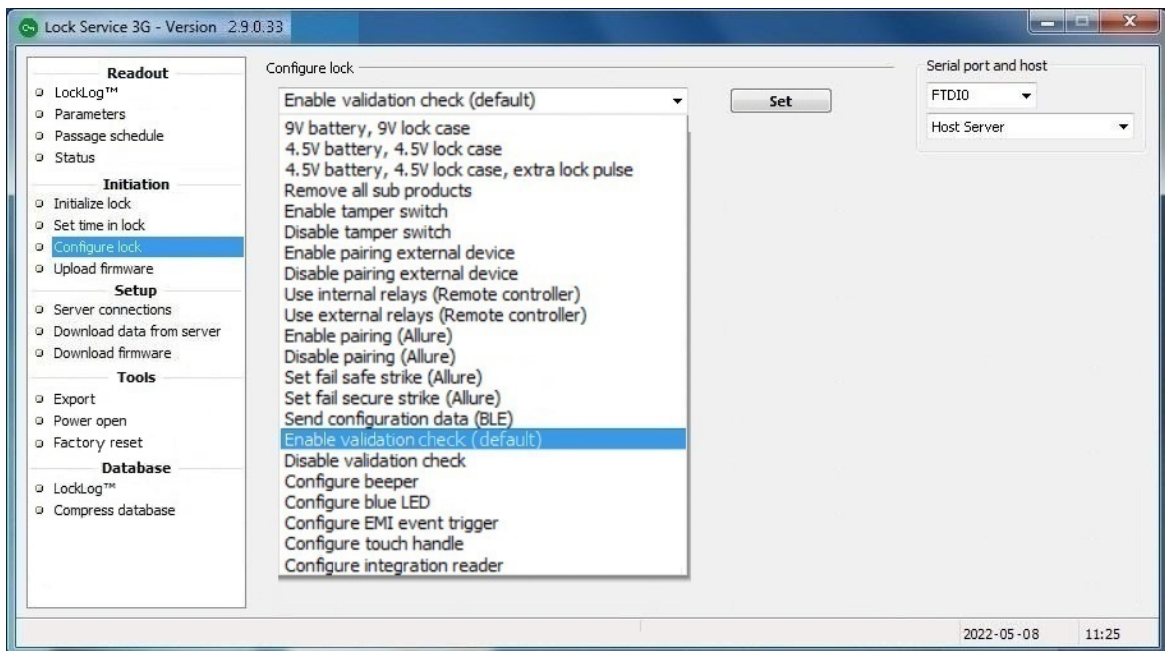
The time in the lock is set at initiation, so normally the choice **Set time in lock** is not necessary to use. However, if the time is for some reason lost this choice must be used.



1. Connect the service cable to the lock.
2. Click the **Set time** button.

**Note:** Make sure that the time in the service PC is correct.

### 4.3 Configure lock



With **Configure lock**, some parameters can be set in the locks. Table 1 describes some of the alternatives under **Configure lock**. **Note:** Discuss with Technical support before using any of the lock case alternatives under **Configure lock**.

1. Connect the service cable to the lock.
2. Select the desired configuration.  
**Note:** If [Send configuration data \(BLE\)](#) or [Configure EMI event trigger](#) is chosen, further actions should be taken before going to step 3; see details following the applicable link.
3. Click the **Set** button.

Choice	Description
Enable pairing external device <b>Note:</b> This configuration is only applicable for remote controllers.	For older remote controllers (serial number earlier than <i>12370450001</i> ), this configuration must be used at first setup; discuss with Technical support for details. From serial number <i>12370450001</i> and later (remote controllers produced from 2012-09-15 and afterwards), pairing is not recommended. The serial number is found on a label on the noteback of the interface board (located inside the remote controller).
Disable pairing external device <b>Note:</b> This configuration is only applicable for remote controllers.	If an interface board needs to be exchanged and it has been paired according to above, the pairing must first be disabled. As above, it is not recommended to enable pairing again if the new interface board has a serial number which is <i>12370450001</i> or later.
Use internal relays (Remote controller)	This configuration is applicable if 'relay 1' on the remote controller should be used; see <i>Installation manual Remote controller Visionline 3G RFID</i> .
Use external relays (Remote controller)	This configuration is applicable in remote controller configurations where the external relays on the RS-485 gateway should be used; see <i>Installation manual Remote controller Visionline 3G RFID</i> .



Enable pairing (Allure)	It is possible to pair an <i>Allure main control unit</i> with its corresponding LCU. Before choosing this configuration, the concerned <i>Allure main control unit</i> and LCU should however be run in demo mode (i.e. without the <b>Enable pairing</b> configuration set) for a while, to verify that everything works as it should.
Set fail safe strike (Allure)	If the doors should be unlocked at a power failure, choose this alternative.
Set fail secure strike (Allure)	If the doors should be locked at a power failure, choose this alternative.
Send configuration data (BLE)	This configuration is applicable for the Visionline software option Mobile access, if the signal strength should be adjusted and/or if seamless mode is applicable; see details <a href="#">here</a> .
Start orphan join in ZigBee (shown if the Online option has been set in Visionline)	As it can take up to three hours for the endnodes to get online after recovery from a power cut, this configuration alternative can be used for initiating an orphan join. <b>Note:</b> If the orphan join is successful, a green LED signal will be shown. If the endnode in the lock is busy at the moment, a <b>very short</b> green LED signal will be shown. In this case, make a new try by clicking <b>Set</b> again.
Start discovery in ZigBee (shown if the Online option has been set in Visionline)	Discovery is the process when a node shall join a PAN ( <i>personal area network</i> ). It starts by the node broadcasting a discovery message. Any plausible parent will answer and the node will join the one on which "permit joining" has been made, provided that it is within range. An endnode makes discovery when 'Start discovery in ZigBee' is chosen and <b>Set</b> is clicked. <b>Note:</b> If the discovery is successful, a green LED signal will be shown. If the endnode in the lock is busy at the moment, a <b>very short</b> green LED signal will be shown. In this case, make a new try by clicking <b>Set</b> again. The configuration alternative 'Start discovery in ZigBee' also sets the sub product ZigBee in the lock.
Check ZigBee status (shown if the Online option has been set in Visionline)	To check the online status directly at the lock, this configuration alternative can be used. With this configuration, a check is made whether the endnode in the lock has still got contact with its parent or not. <b>Note:</b> If a green LED signal is shown, the lock is online. If three red LED signals are shown, the lock is offline. If the endnode in the lock either is busy at the moment or is connected to the LCA ( <i>lock case adapter</i> ), a very short green LED signal is shown instead. In this case, make a new try by clicking <b>Set</b> again.
Enable auto-DND	This configuration is applicable for Orion installations. If <b>Enable auto-DND</b> is enabled, the lock will enter privacy mode when a guest is in the room.
Enable EMI events	This configuration is needed if the <i>Orion EMS</i> option or <i>Online Inncom via ZigBee</i> option is applicable.
Enable validation check (default)	If validation check has been disabled in a remote controller/elevator controller/lock (see below) and should later be enabled again, this configuration is applicable.
Disable validation check	By default, there is a validation check in all remote controllers/elevator controllers/locks. By choosing 'Disable validation in lock', it is however possible to exclude certain remote controllers/elevator controllers/locks from the validation check. This is useful e.g. if a remote controller is located outside a staff entrance door and an auto-update encoder is located on the inside of the door. This requires the following minimum firmware versions (included in <i>Lock Service 3G 2.2.2.8</i> ): <ul style="list-style-type: none"> <li>• 3.17.35.0</li> <li>• 3.18.34.2</li> <li>• 3.20.34.2</li> <li>• 3.40.34.2</li> </ul>
Configure beeper	This configuration can be used for future hardware (LCU 5351 and LCU 6351) to enable the beeper. <b>Note:</b> If this configuration is set and the hardware does not support it, the user will be notified.
Configure blue LED	This configuration can be used for future hardware (LCU 6351) to enable the blue LED, if it has been mounted in production. Blue LED is only applicable if the lock/remote controller/elevator controller has been initialized with BLE. If 'Configure blue LED' is set, there will be a blue flickering during communicating with the phone. If the credentials are valid, there will then be the normal green LED access indication and/or a chirp (if available and enabled) when the lock/remote controller/elevator controller is unlocked. <b>Note:</b> If this configuration is set and the hardware does not support it, the user will be notified.
Configure EMI event trigger	If this configuration is set to 'Credential' (see details <a href="#">here</a> ), the EMI output is triggered when a valid credential is presented at the lock.

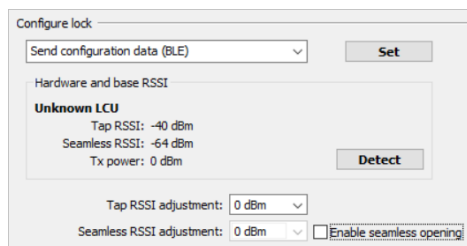


<b>Note:</b> This configuration is only applicable for <i>VingCard Allure</i> .	
Configure touch handle	This configuration is only needed for certain Marine applications.
Configure integration reader	See details in <i>Installation manual ASSA ABLOY Reader 3139 incl. daisy chain module</i> .
<i>Table 1</i>	

**Send configuration data (BLE):**

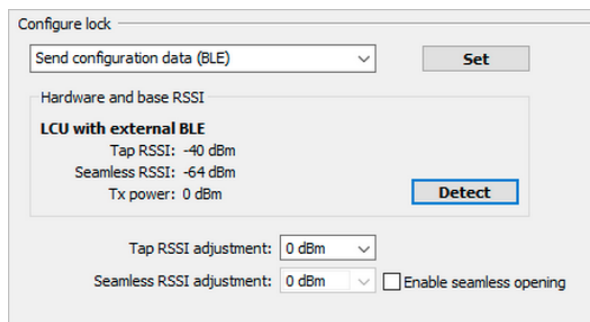
Visionline contains the predefined BLE profiles 'Guest lock', 'Allure lock' and 'Remote controller/Elevator controller', and it is in Visionline also possible to create new profiles or update existing ones. Each profile is a collection of lock BLE settings which can be used for several locks, thus facilitating the setup of lock BLE details.

**Important:** Before assigning a BLE profile to one or more locks in Visionline, first use *Lock Service 3G* for trying out the BLE parameters on one or a few locks. Follow the procedure below:



1. When **Send configuration data (BLE)** is chosen, a screen as to the left is shown.

2. While the service cable is still connected to the lock as described [here](#), click **Detect** to check which LCU (*lock controller unit*) the lock has.
3. After clicking **Detect**, Lock Service 3G will show the LCU type; see example in the left picture below. Default values of *tap RSSI*, *seamless RSSI* and *Tx power* for the concerned LCU type are shown. **Note:** Default for all LCU types is that 'Enable seamless opening' is unmarked, and **Seamless RSSI adjustment** is greyed out.

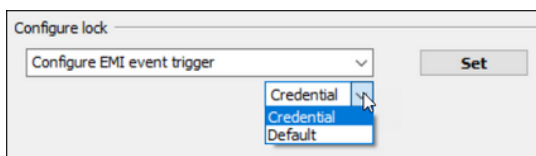


4. If needed, make adjustments to the default values for the LCU type at **Tap RSSI adjustment** and/or **Seamless RSSI adjustment**; see details [here](#). If the 'Enable seamless opening' checkbox is marked, the drop-down-menu for **Seamless RSSI adjustment** will be available as shown in the picture to the right.
5. Apply the configuration on the lock by clicking the **Set** button.
6. If any value needs to be adjusted, make the desired finetuning. After this, repeat step 5.

7. After a successful test with *Lock Service 3G*, go to Visionline and
  - choose one of the predefined BLE profiles (can if needed be adjusted in Visionline if the outcome of the Lock Service 3G tests is that adjustment is required) **OR**
  - create a new BLE profile.
8. Download data from the Visionline server to *Lock Service 3G*; first make sure to include 'Doors and Door areas' (see details [here](#)).
9. Initialize the locks via *Lock Service 3G*; first make sure to mark the checkbox 'Include BLE configuration data' (see details [here](#)).

If any BLE parameter should later be changed: connect the service cable to the lock and repeat steps 1-9 above.

#### **Configure EMI event trigger:**



If 'Credential' is chosen in the drop-down-menu at **Configure EMI event trigger**, the EMI output is triggered when a valid credential is presented at the lock.

## **4.4 Upload firmware**

[Recommended procedure](#)

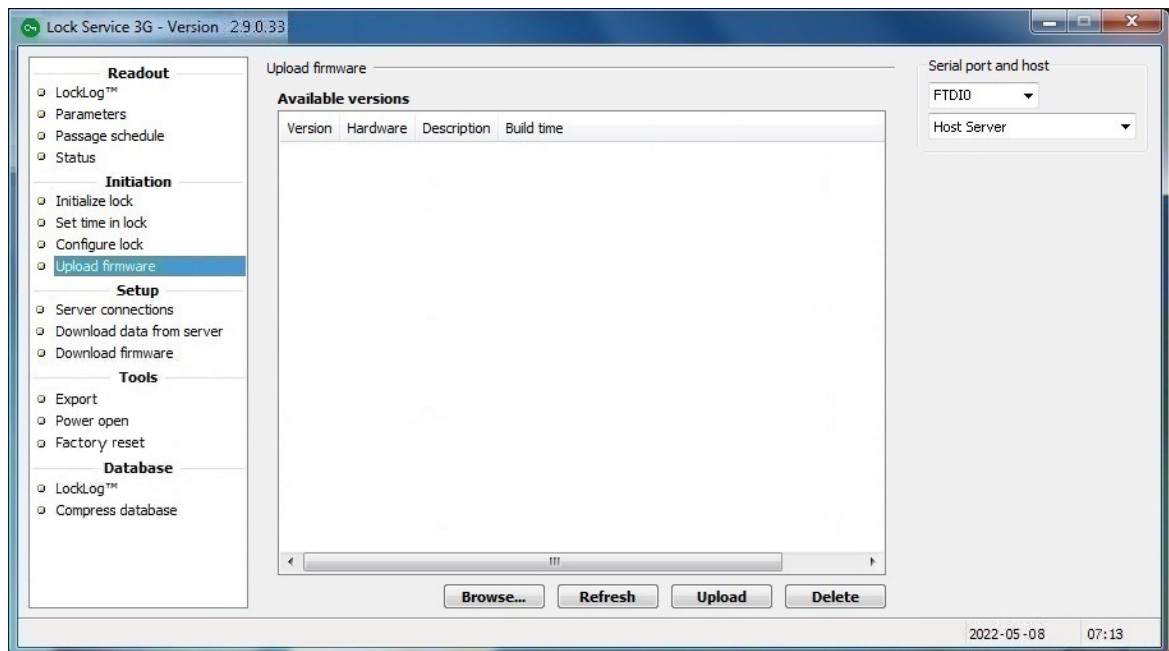
[Add/edit firmware description](#)

[Delete firmware from the Lock Service 3G database](#)

[Procedure for special firmware](#)

[Save firmware to the Lock Service 3G database](#)

## Recommended procedure



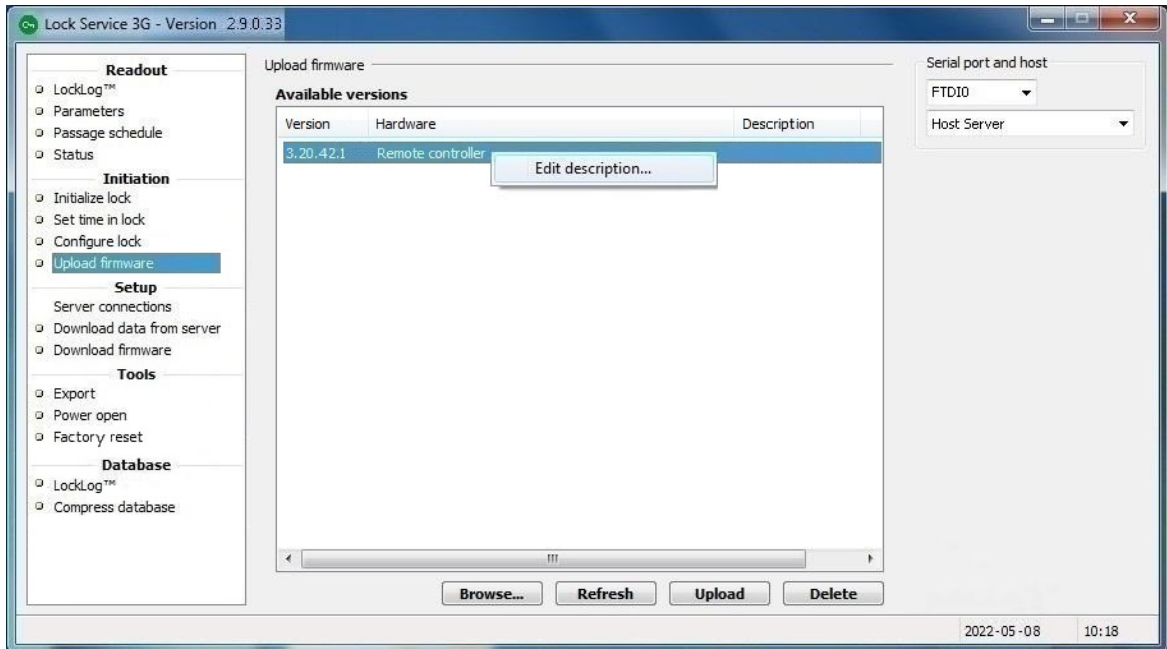
1. Once a firmware has been downloaded to the *Lock Service 3G* database according to the section [Download firmware](#), the firmware will appear under **Available versions** in the **Upload firmware** window. To upload the firmware to a lock (or remote controller, elevator controller etc), mark it in the **Available versions** list and click the **Upload** button.
2. On the bottom of the **Upload firmware** window, a progress bar will show how far the uploading process has reached. To the left, it is also stated as a percentage how far the uploading process has reached.



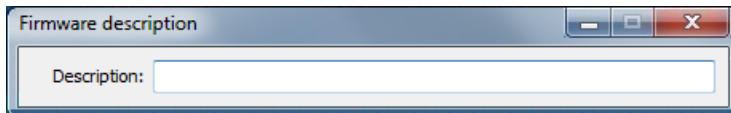
3. After the upload, the question 'Do you want to set the time?' is shown; click the applicable answer 'Yes' or 'No'.

## Add/edit firmware description

1. To add/edit the description for a firmware, right click on the firmware when it has been saved to the database and choose **Edit description**.



2. Write the applicable description and click **Enter**.



## Delete firmware from the Lock Service 3G database

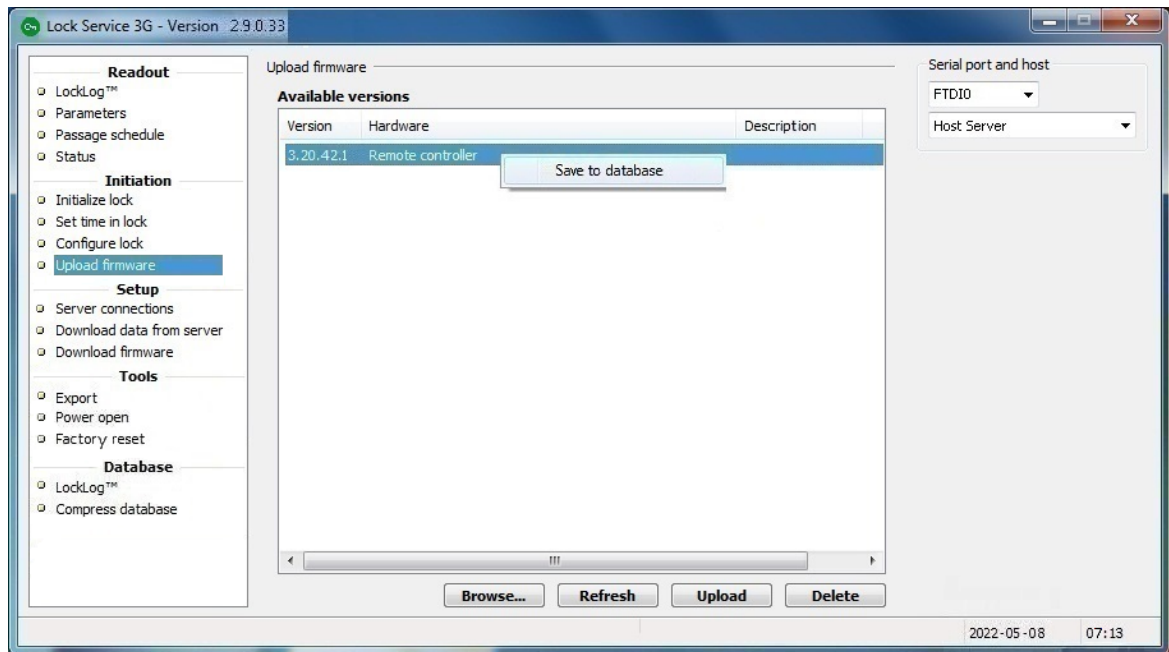
1. To delete a firmware from the *Lock Service 3G* database, select it under **Available versions** in the **Upload firmware** window and click the **Delete** button.

## Procedure for special firmware

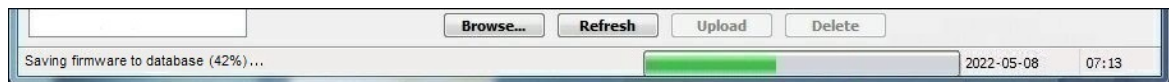
1. Click **Browse** in the **Upload firmware** window and select the desired firmware file on e.g. a USB memory.
2. If the firmware should be saved to the *Lock Service 3G* database, follow [these steps](#).

## Save firmware to the Lock Service 3G database

1. To save the firmware file to the database, right click on it and choose **Save to database**.



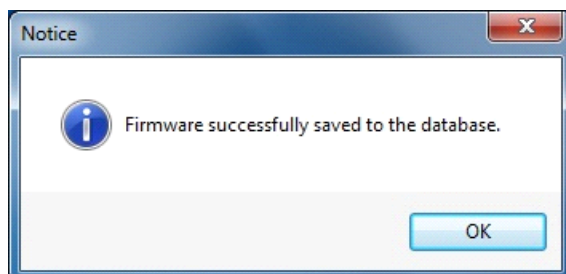
2. On the bottom of the **Upload firmware** window, a progress bar will show how far the saving process has reached. To the left, it is also stated as a percentage how far the saving process has reached.



**Note:** If the firmware 'Single-chip ZigBee endnode w/ext. antenna switch (EN3) I2C' is uploaded, the status bar in *Lock Service 3G* will during the waiting state (i.e. when the endnode is updating and restarting) change to orange color to raise attention; a descriptive text about the state will also be shown.



3. When the firmware has been successfully saved, there will be an alert.



## 5. Setup

The **Setup** section includes three selections:

- Server connections
- Download data from server
- Download firmware

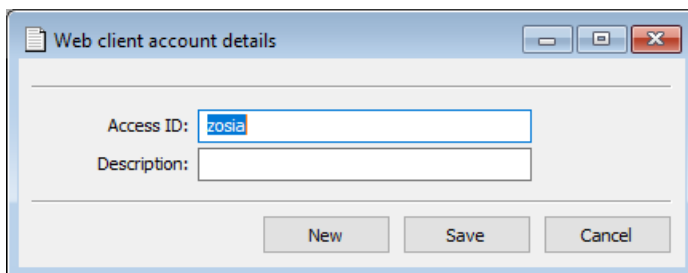
### 5.1 Server connections

To connect a service PC to the server, the following steps must be performed:

1. A web client account must be configured in Visionline; see [5.1.1](#).
2. A Web API connection must be set up in *Lock Service 3G*, specifying the *access ID* for the web client account created in step 1 above; see [5.1.2](#).
3. The web client in Visionline must be given special rights; see [5.1.3](#).

#### 5.1.1 Add web client account in Visionline

1. Double-click on **Web client accounts** under **Lists** in the navigation window, or choose **Web client accounts** in the **View** menu.
2. Click **Add** to add a new account.
3. In the **Web client account details** dialog, enter **Access ID** and (if desired) **Description**.
4. Click **Save** and **Close**; the account will appear in the **Web client accounts** list.

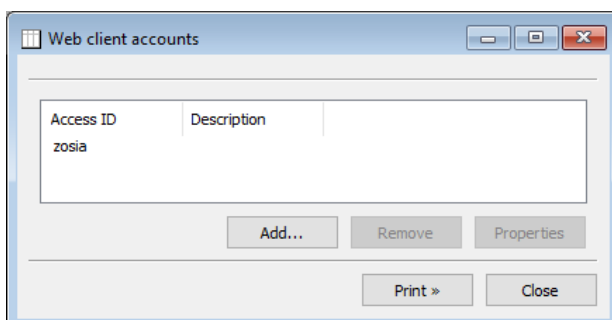


Web client account details

Access ID: zosia

Description:

New Save Cancel



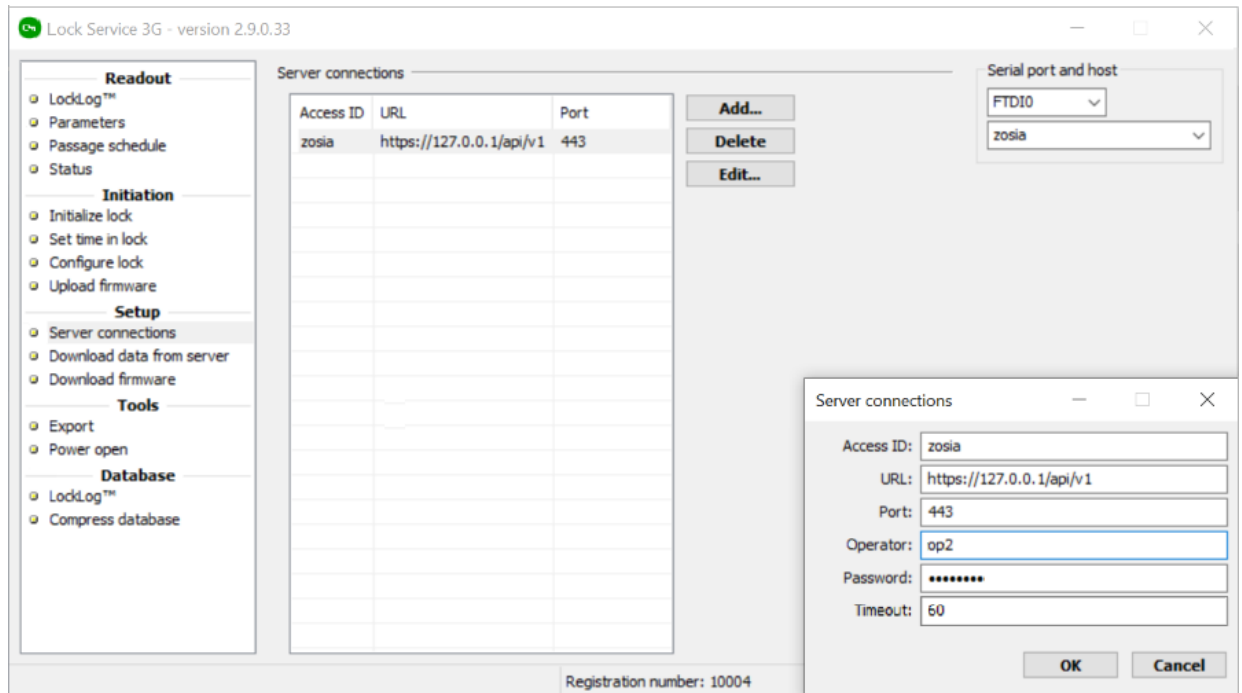
Web client accounts

Access ID	Description
zosia	

Add... Remove Properties

Print > Close

## 5.1.2 Set up Web API connection in Lock Service 3G

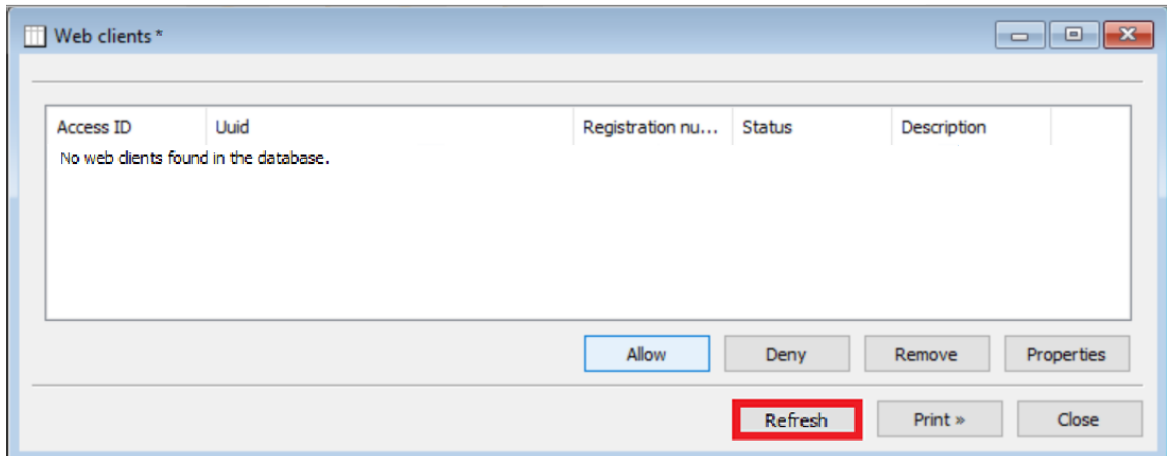


1. To add a connection, click the **Add** button on the **Server connections** page. The smaller **Server connections** dialog will be shown. Some fields are prefilled:
  - **URL** is prefilled to show the format, but should be changed to the applicable URL.
  - **Port** is prefilled to 443 (standard port for HTTPS).
  - **Timeout** (for Web API requests) is prefilled to 60 seconds, but can if desired be modified in the range 1-720 seconds.Fill in the remaining fields. Use the **Access ID** from [section 5.1.1](#).
2. To delete a connection, select the connection and click the **Delete** button.
3. To edit a connection, select the connection and click the **Edit** button; make the desired changes in the **Server connections** dialog.

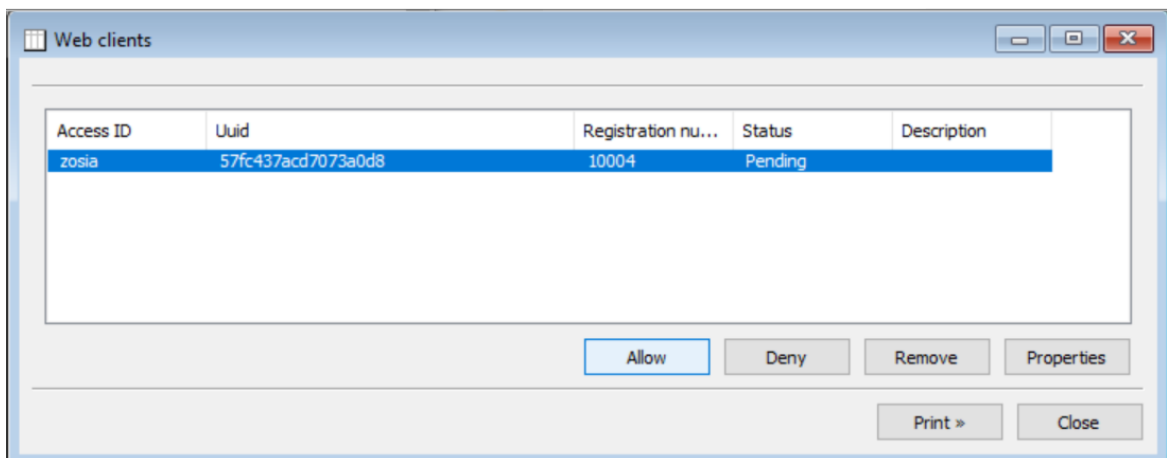
### 5.1.3 Give web client in Visionline special rights

For the data download operation in [section 5.2](#) to be successful, a web client in Visionline must be given special rights.

1. Double-click on **Web clients** under **Lists** in the navigation window.
2. The web client tries to log in; the asterisk in the dialog caption indicates this. Click the **Refresh** button.



3. When **Refresh** is clicked, the web client will appear in the **Web clients** list.

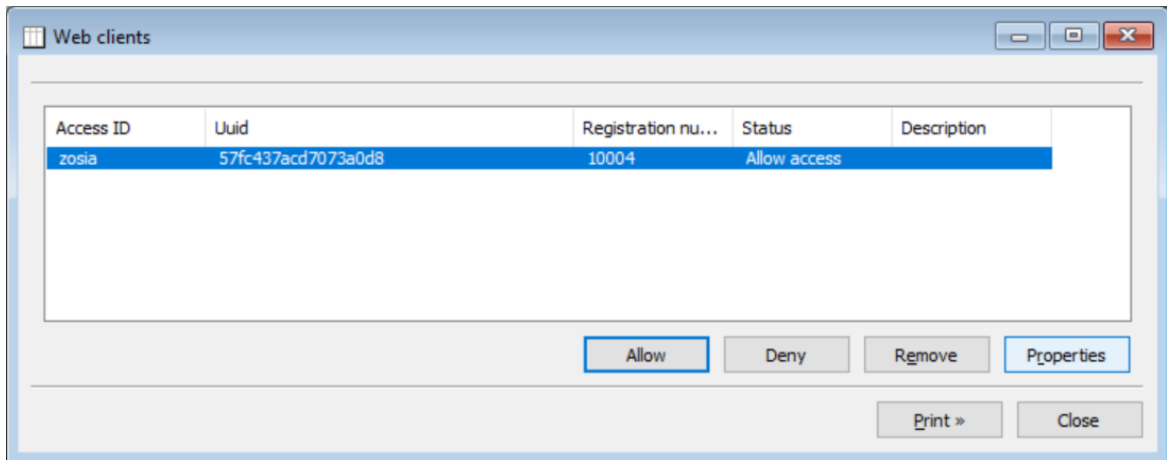


4. The status of a web client will from the start be *Pending*.
  - The **Uuid** comes from the web client and is unique for that client.
  - The **Registration number** is created by Visionline and is also a unique number which is applicable for certain types of web clients.  
**Note:** Make sure that the registration number shown in the **Web client** list in Visionline is the same as the registration number shown at the bottom of the *Lock Service 3G* window (see e.g. picture in [section 5.1.2](#)).
5. Mark the web client in the list, and click the applicable button **Allow** or **Deny**.  
**Note:** The alternative **Deny** is e.g. applicable if you wish to block a client,



e.g. if a service PC has been lost. The blocking is however not permanent; previously blocked clients can later be allowed again.

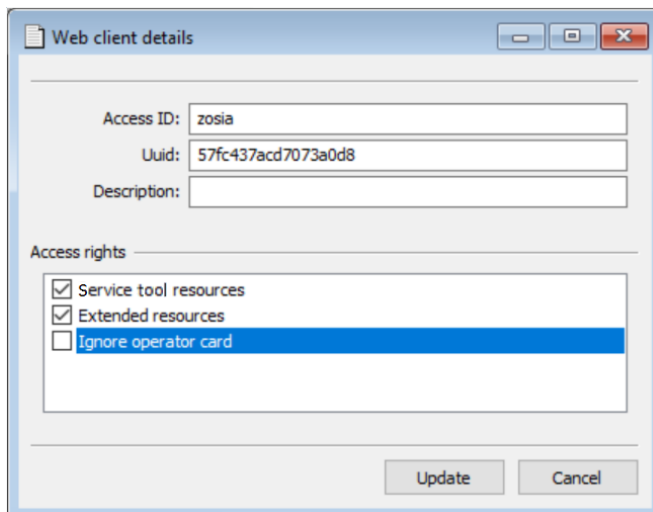
6. If **Allow** was chosen, the **Status** column will now state 'Allow access'.



7. If marking a web client in the list and clicking **Properties**, a dialog with access right alternatives will be shown (see picture below).

**Note:** If information is entered in the **Description** field in Visionline, the description sent from the web client will be discarded.

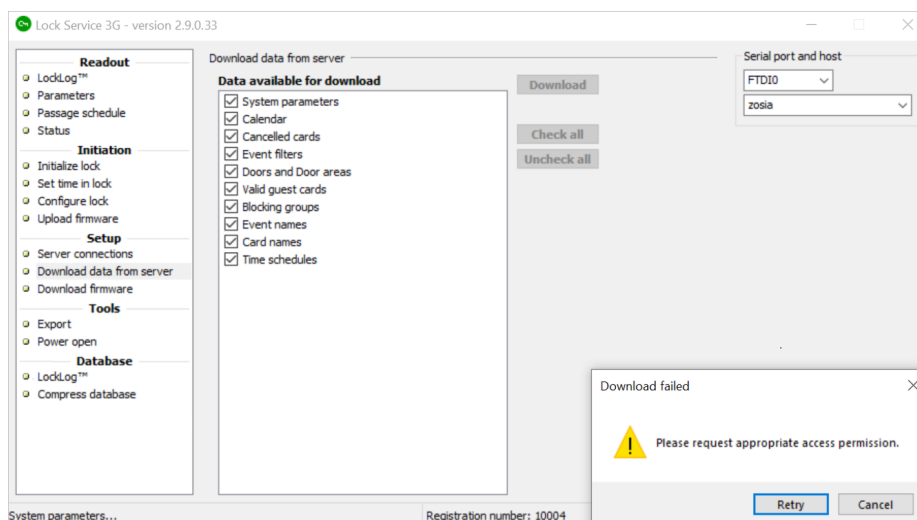
8. Once the applicable access rights have been marked and **Update** has been clicked, the web client should be able to log in/use the Web API.



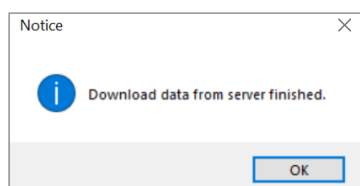
## 5.2 Download data from server

**Note:** Remember to download data from server also at later occasions than at setup, if needed. This is applicable if information about doors, cancelled cards, system ID etc is changed.

1. Select data by checking the applicable boxes in the **Data available for download** list. If necessary, use the **Check all/Uncheck all** buttons.
2. Click the **Download** button.
3. If the steps for giving the web client special rights have not been performed for the web client in question:
  - A message 'Please request...' as below will be shown.
  - Perform the steps for [giving special rights](#).
  - Click the **Download** button again.



3. When the download is ready, a message as below will be shown.



**Note:** During the downloading operation, status texts and a progress bar at the bottom of the *Lock Service 3G* window will show the progress.

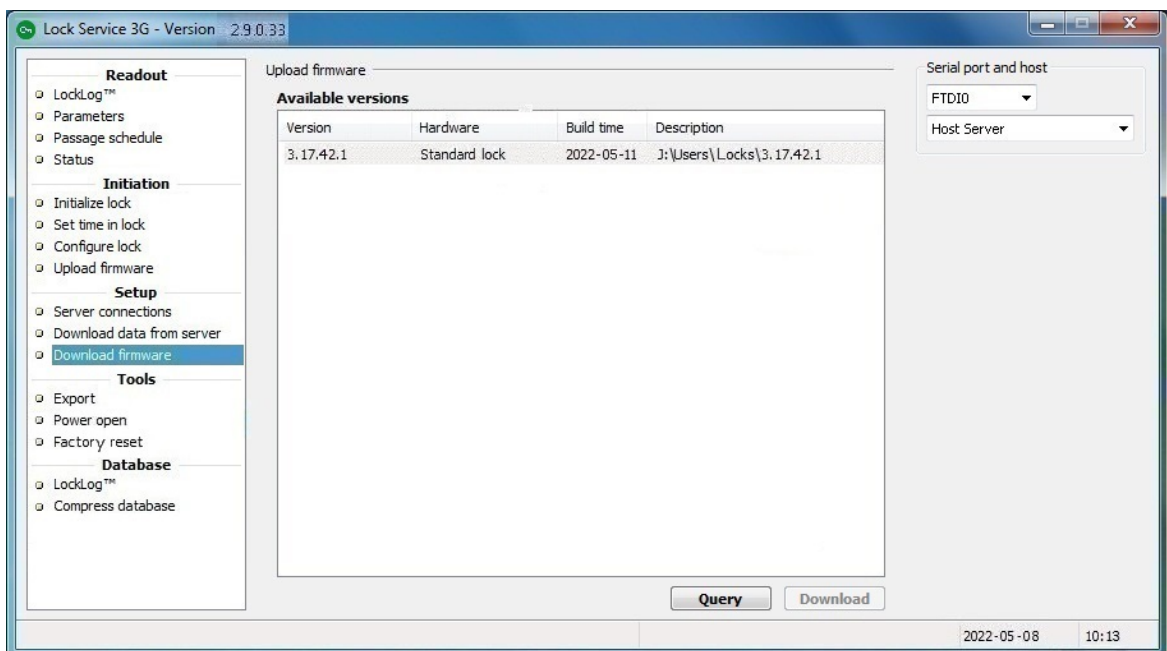
**Note:** The *power open token*, *factory reset token* and (for legacy key mode) *coldstart token* are only available when system ID has been set. The tokens are valid for a short time and should only be downloaded when needed, i.e. normally not at the first server connection.

**Note:** At each download of a *power open token*, *factory reset token* or (for legacy key mode) *coldstart token*, the operator must enter his password.

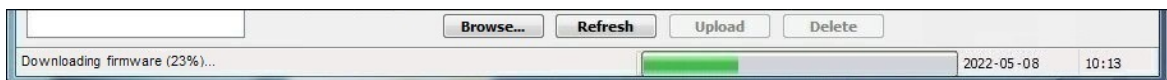
## 5.3 Download firmware

Each Visionline bundle includes a lock firmware pack with the latest available firmware at that point in time. If needed, lock firmware packs can also be released between two Visionline bundle versions. When installing a lock firmware pack, the firmware will by default be available in a folder **Firmwares** in the Visionline installation folder (the pack can if desired be installed in any other location).

Once the lock firmware pack has been installed, it is recommended to store the firmware in the Visionline database by following the steps in the appendix *Firmware upgrade* (section *Prepare for lock firmware upgrade*) of *Setup manual Visionline*. Once stored in the Visionline database, the firmware can be downloaded to *Lock Service 3G* according to the steps below. The firmware can then be uploaded to locks (or remote controllers, elevator controllers etc) according to the section [Upload firmware](#).



1. To list the available firmware versions on the server, click the **Query** button.
2. To locally store the version in the service PC, select version and click **Download**.
3. On the bottom of the *Lock Service 3G* window, a progress bar will show how far the downloading process has reached. To the left, it is also stated as a percentage how far the downloading process has reached.



4. When the firmware has been successfully downloaded, there will be an alert.

## 6. Tools

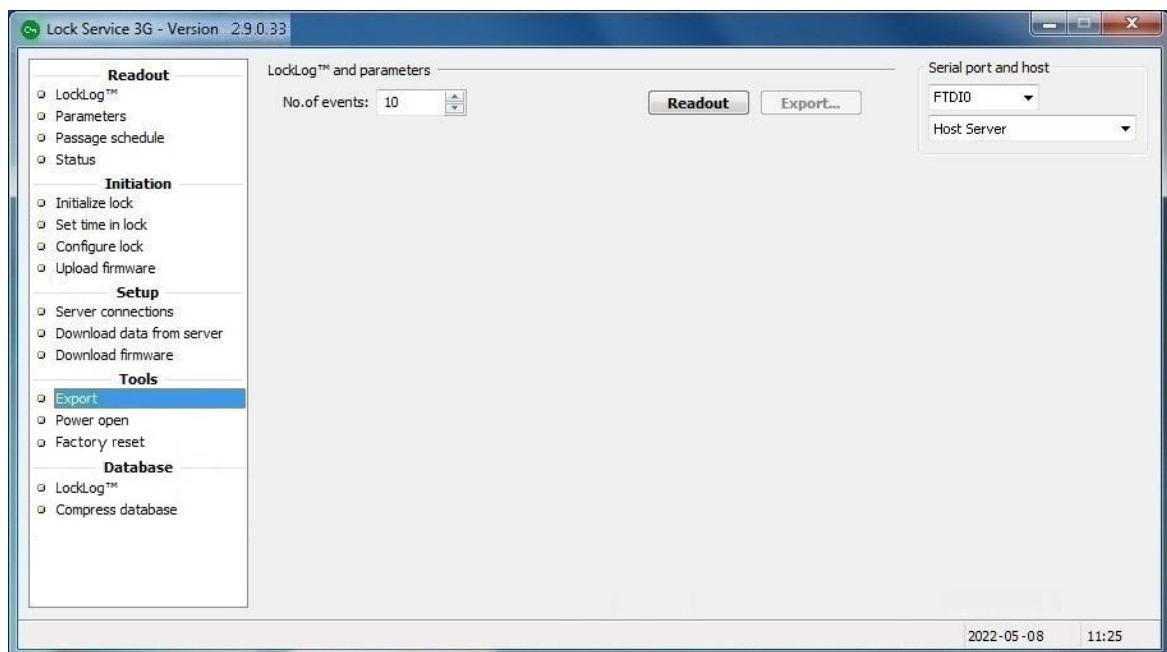
The **Tools** section includes three selections:

- Export
- Power open
- Coldstart

**Note:** The **Coldstart** selection is only available if system ID has been set.

### 6.1 Export

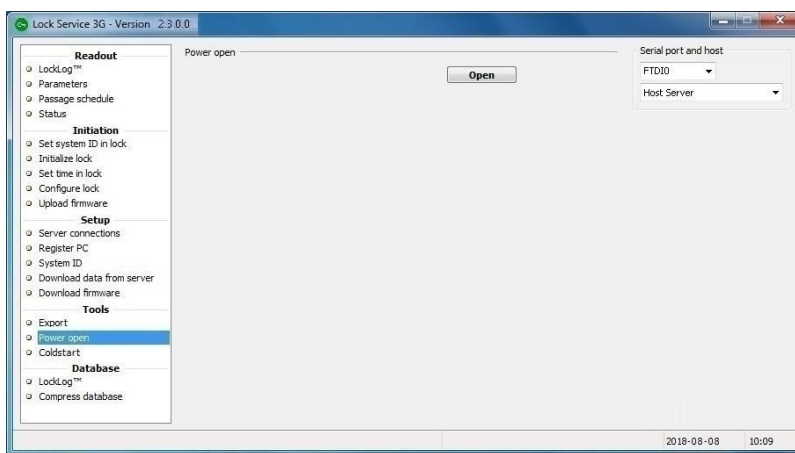
It is possible to make a readout of LockLog and parameters and export this information to a text file, which can later be sent to Tech support.



1. Connect the service cable to the lock.
2. Choose the applicable **No of events**; default is 10.
3. Click the **Readout** button.
4. When the readout is ready, the **Export** button will be enabled. Click it and choose a suitable location for the text file.

## 6.2 Power open

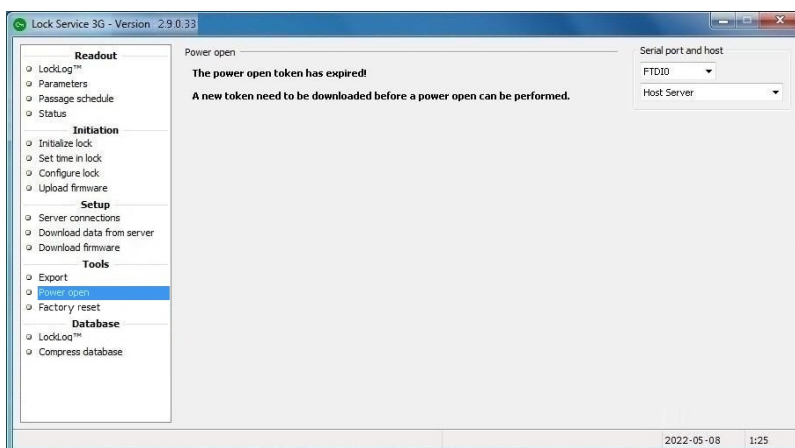
If the battery in the lock has been drained, the service PC can be used to power open the lock. To use this function, the power open token (only available if system ID has been set) must be downloaded from the server; see section [Download data from server](#) for details. The power open token is by default valid for 30 minutes. This can if desired be changed at **Tools/Options/System/Power open token** in Visionline if you are logged on as distributor; enter the applicable value in the range 1-1440 minutes and click **OK**. If this setting is changed, do not forget to go to [Download data from server](#) and download system parameters before following the steps below.



1. Connect the service cable to the lock.
2. Click the **Open** button to power open the lock.


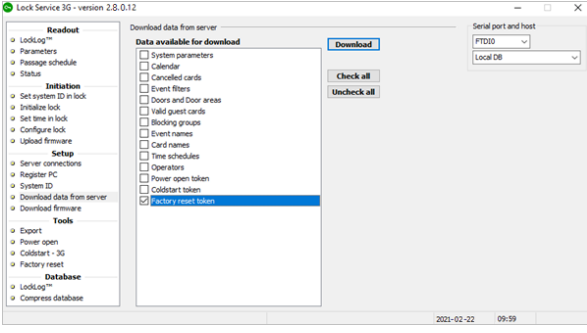
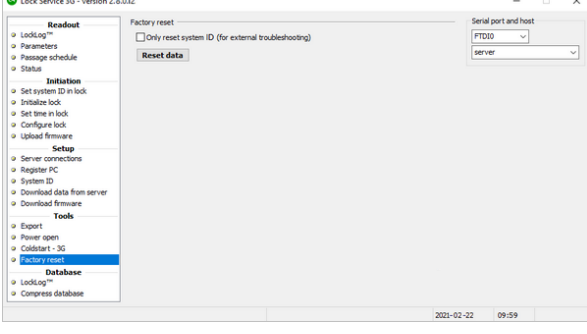
**Note:** If power open is performed in demo mode, an event is sent to the lock.

If the *power open token* is not used within 30 minutes after it has been downloaded from the server, the following message will be shown when the **Open** button is clicked:



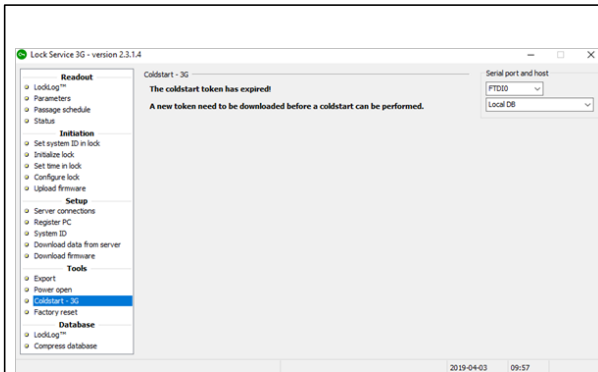
## 6.3 Factory reset

**Note:** For firmware 3.XX.41.6 and onwards (i.e. from Visionline bundle v1.27.0 and onwards), the alternative **Coldstart - 3G** (see [section 6.3.1](#)) is phased out and use of that functionality will result in an error. Instead use the alternative **Factory reset** (performed on site) which is described below. Firmware older than 3.XX.41.6 will still work with **Coldstart - 3G**.

	<p>If system ID has been set, it is possible to perform a factory reset of a lock which needs to be set back to factory status.</p> <ol style="list-style-type: none"> <li>1. Before a factory reset token has been downloaded, the <b>Factory reset</b> screen looks as in the picture to the left.</li> </ol>
	<ol style="list-style-type: none"> <li>2. Choose <b>Download data from server</b> in the left part of <i>Lock Service 3G</i>.</li> <li>3. Mark the checkbox 'Factory reset token' (requires that 'Operators' have previously been downloaded).</li> <li>4. Click <b>Download</b>. <b>Note:</b> The factory reset token is valid for 30 minutes.</li> </ol>
	<ol style="list-style-type: none"> <li>5. Enter your login credentials; the page to the left is shown.</li> <li>6. If only system ID should be reset, mark the checkbox.</li> <li>7. Connect the service cable to the lock.</li> <li>8. Click <b>Reset data</b>. If the factory reset token is not used within 30 minutes after it has been downloaded from the server, the message about expired token (see step 1) will be shown.</li> </ol>

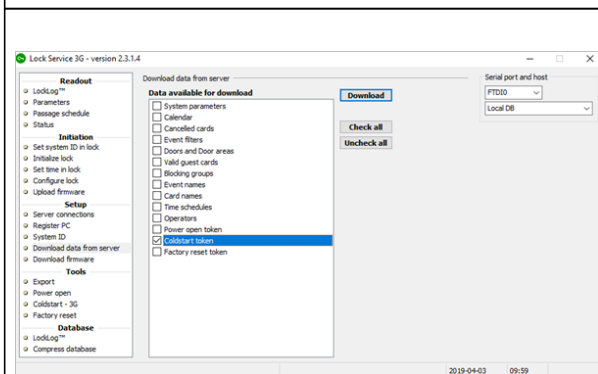
### 6.3.1 Coldstart - 3G

**Note:** Coldstart - 3G will not be shown at all if AES key mode has been set.

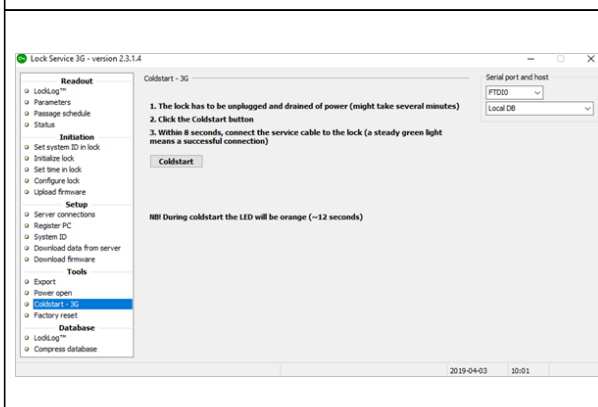


If system ID has been set, it is possible to perform a coldstart of a lock which needs to be set back to factory status.

1. Before a coldstart token has been downloaded, the **Coldstart - 3G** screen looks as in the picture to the left.



2. Choose **Download data from server** in the left part of *Lock Service 3G*.  
 3. Mark the checkbox 'Coldstart token' (requires that 'Operators' have previously been downloaded).  
 4. Click **Download**.  
**Note:** The coldstart token is valid for 30 minutes.



5. Enter your login credentials; the page to the left is shown.  
 6. Follow the instructions on the screen. If the coldstart token is not used within 30 minutes after it has been downloaded from the server, the message about expired token (see step 1) will be shown.

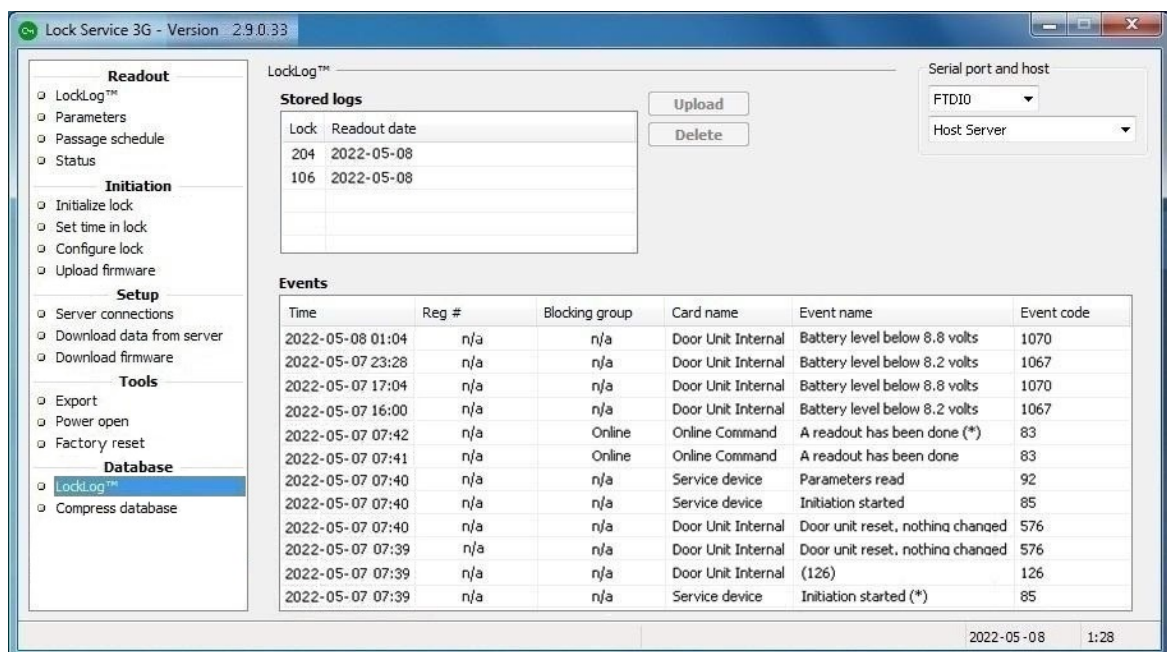
## 7. Database

The **Database** section includes two selections:

- LockLog
- Compress database

### 7.1 LockLog

Saved events are shown here; see section [LockLog with events](#) for information about saving the events.



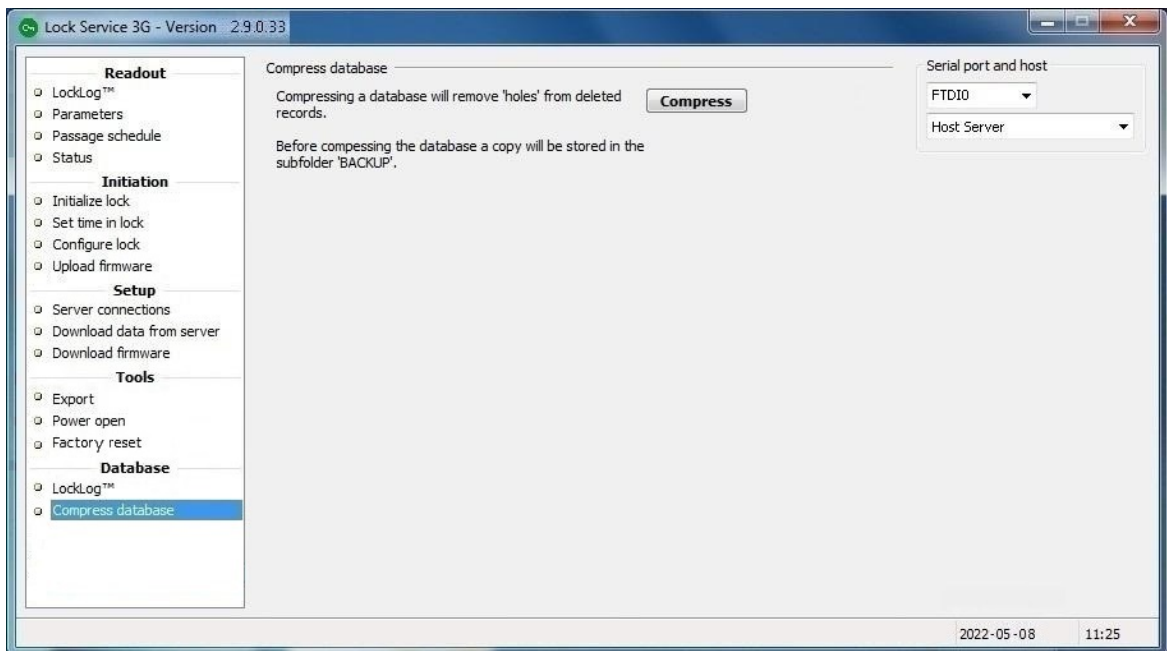
The screenshot shows the 'Lock Service 3G - Version 2.9.0.33' application window. The 'Database' section is selected in the sidebar, and 'LockLog™' is highlighted. The main window displays the 'LockLog™' section with a 'Stored logs' table and an 'Events' table. The 'Stored logs' table has two columns: 'Lock' and 'Readout date'. The 'Events' table has seven columns: 'Time', 'Reg #', 'Blocking group', 'Card name', 'Event name', and 'Event code'. The 'Events' table contains 14 rows of data.

Time	Reg #	Blocking group	Card name	Event name	Event code
2022-05-08 01:04	n/a	n/a	Door Unit Internal	Battery level below 8.8 volts	1070
2022-05-07 23:28	n/a	n/a	Door Unit Internal	Battery level below 8.2 volts	1067
2022-05-07 17:04	n/a	n/a	Door Unit Internal	Battery level below 8.8 volts	1070
2022-05-07 16:00	n/a	n/a	Door Unit Internal	Battery level below 8.2 volts	1067
2022-05-07 07:42	n/a	Online	Online Command	A readout has been done (*)	83
2022-05-07 07:41	n/a	Online	Online Command	A readout has been done	83
2022-05-07 07:40	n/a	n/a	Service device	Parameters read	92
2022-05-07 07:40	n/a	n/a	Service device	Initiation started	85
2022-05-07 07:40	n/a	n/a	Door Unit Internal	Door unit reset, nothing changed	576
2022-05-07 07:39	n/a	n/a	Door Unit Internal	Door unit reset, nothing changed	576
2022-05-07 07:39	n/a	n/a	Door Unit Internal	(126)	126
2022-05-07 07:39	n/a	n/a	Service device	Initiation started (*)	85

1. To send the log to the server, mark the log at 'Stored logs' and click the **Upload** button.
2. To delete the log, mark the log at 'Stored logs' and click the **Delete** button.



## 7.2 Compress database



1. To compress the database, click the **Compress** button.

## Revision history

Date	Change	By
June 21, 2012	<ul style="list-style-type: none"> <li>• First release</li> </ul>	KG
October 16, 2012	<ul style="list-style-type: none"> <li>• Added information about <i>battery voltage (idle)</i> and <i>battery voltage (load)</i></li> <li>• Added information about new message about LED after setting system ID</li> <li>• <b>Configure lock:</b> added alternatives for tamper switch and external devices; the latter applicable for <i>remote controllers</i> of certain batches</li> <li>• <b>Upload firmware</b> and <b>Download firmware:</b> lock firmware and module firmware are now shown in the same dialog</li> <li>• <b>Upload firmware:</b> added that firmwares are already available in the <b>Available versions</b> list</li> <li>• <b>Upload firmware:</b> added information about the right-click choices <b>Save to database</b> and <b>Edit description</b></li> <li>• Added information about progress bars during firmware uploading/downloading/saving processes</li> <li>• Added that if the database is moved to another PC, the system ID will be reset to demo</li> <li>• Added that <i>power open token</i> and <i>coldstart token</i> are only available if system ID has been set</li> <li>• Added that at each download of a <i>power open token</i> and/or a <i>coldstart token</i>, the operator must enter his password</li> <li>• <b>Download firmware:</b> added that this is normally never used</li> <li>• Added that up to 100 firmwares can be saved to the database</li> <li>• Added that if power open is performed in demo mode, an event is sent to the lock</li> <li>• Added information about coldstart</li> </ul>	KG
April 8, 2013	<ul style="list-style-type: none"> <li>• Updated to match version 1.0.2</li> </ul>	KG
February 28, 2014	<ul style="list-style-type: none"> <li>• New page <b>Status</b> added</li> <li>• <b>Configure lock:</b> added the possibility to select internal/external relays for remote controller; added the configurations 'set fail safe strike' and 'set fail secure strike' for Allure</li> <li>• <b>Export:</b> the parameters in the log will now include both 'idle' and 'load' value of the battery voltage</li> </ul>	KG
November 4, 2014	<ul style="list-style-type: none"> <li>• Updated to match version 1.1.0 (BLE added)</li> </ul>	KG
January 27, 2015	<ul style="list-style-type: none"> <li>• Updated to match version 1.1.1 (updated firmwares)</li> </ul>	KG

February 27, 2015	<ul style="list-style-type: none"> <li>Updated to match version 1.2.0 (updated firmwares; new alternatives for pairing of Allure under <b>Configure lock</b>)</li> </ul>	KG
June 23, 2015	<ul style="list-style-type: none"> <li>Updated to match version 1.2.1 (updated firmwares; enabled search in the door list at <b>Initialize lock</b>; new alternatives for ZigBee under <b>Configure lock</b>)</li> </ul>	KG
March 16, 2016	<ul style="list-style-type: none"> <li>Updated layout</li> </ul>	KG
May 9, 2016	<ul style="list-style-type: none"> <li>Updated screenshots to match combo firmware</li> </ul>	KG
June 1, 2016	<ul style="list-style-type: none"> <li>Added Allure firmware</li> </ul>	KG
December 7, 2016	<ul style="list-style-type: none"> <li>Updated with information about <i>Active Directory</i></li> <li>Updated screenshots to match version 2.1.1.0</li> </ul>	KG
August 23, 2017	<ul style="list-style-type: none"> <li>Added new <b>Configure lock</b> alternatives: enabling/disabling validation, configuring beeper and configuring blue LED</li> <li>Updated with information about msi file</li> </ul>	KG
March 1, 2018	<ul style="list-style-type: none"> <li>If the firmware 'Single-chip ZigBee endnode w/ext. antenna switch (EN3) I2C' is uploaded, the status bar in <i>Lock Service 3G</i> will during the waiting state (i.e. when the endnode is updating and restarting) change to orange color to raise attention; a descriptive text about the state will also be shown</li> </ul>	KG
April 23, 2018	<ul style="list-style-type: none"> <li>Added <i>VingCard E100</i> to <b>Upload firmware</b> screenshot</li> <li>Updated all other screenshots as well to match version 2.2.5.0</li> </ul>	KG
November 28, 2018	<ul style="list-style-type: none"> <li>Updated to match version 2.3.0.5</li> </ul>	KG
April 10, 2019	<ul style="list-style-type: none"> <li>Added information about configuration of EMI event trigger</li> <li>Added factory reset</li> <li>Firmware updated to match version 2.3.1.4</li> <li>Rebranded the document</li> </ul>	KG
November 7, 2019	<ul style="list-style-type: none"> <li>Removed firmware from 'Upload firmware'</li> </ul>	KG
November 2, 2020	<ul style="list-style-type: none"> <li>Updated BLE configuration</li> <li>Added 'Configure touch handle'</li> </ul>	KG
June 15, 2021	<ul style="list-style-type: none"> <li>Added 'Configure integration reader'</li> <li>Under 'Factory reset', added option to reset system ID only</li> </ul>	KG
November 18, 2022	<ul style="list-style-type: none"> <li>Sections 'Register PC' and 'System ID' are removed</li> <li>Server connection is now done as below: <ul style="list-style-type: none"> <li>- A web client account is configured in Visionline</li> <li>- A Web API connection is set up in <i>Lock Service 3G</i></li> <li>- The web client in Visionline is given special rights</li> </ul> </li> <li>'Coldstart - 3G' is not shown if AES key mode has been set</li> </ul>	KG

The ASSA ABLOY Group is the global leader in access solutions. Every day we help people feel safe, secure and experience a more open world.

**ASSA ABLOY**  
Global Solutions

ASSA ABLOY Global Solutions APAC  
[apac.globalsolutions@assaabloy.com](mailto:apac.globalsolutions@assaabloy.com)  
Phone: +852 23162200

ASSA ABLOY Global Solutions EMEA  
[emea.globalsolutions@assaabloy.com](mailto:emea.globalsolutions@assaabloy.com)  
Phone: +47 69 24 50 00

ASSA ABLOY Global Solutions North America  
[nam.globalsolutions@assaabloy.com](mailto:nam.globalsolutions@assaabloy.com)  
Phone: +1 972 907 2273

ASSA ABLOY Global Solutions Latin America  
[lac.globalsolutions@assaabloy.com](mailto:lac.globalsolutions@assaabloy.com)  
Phone: +52 55 36 40 12 00

[assaabloyglobalsolutions.com](http://assaabloyglobalsolutions.com)