

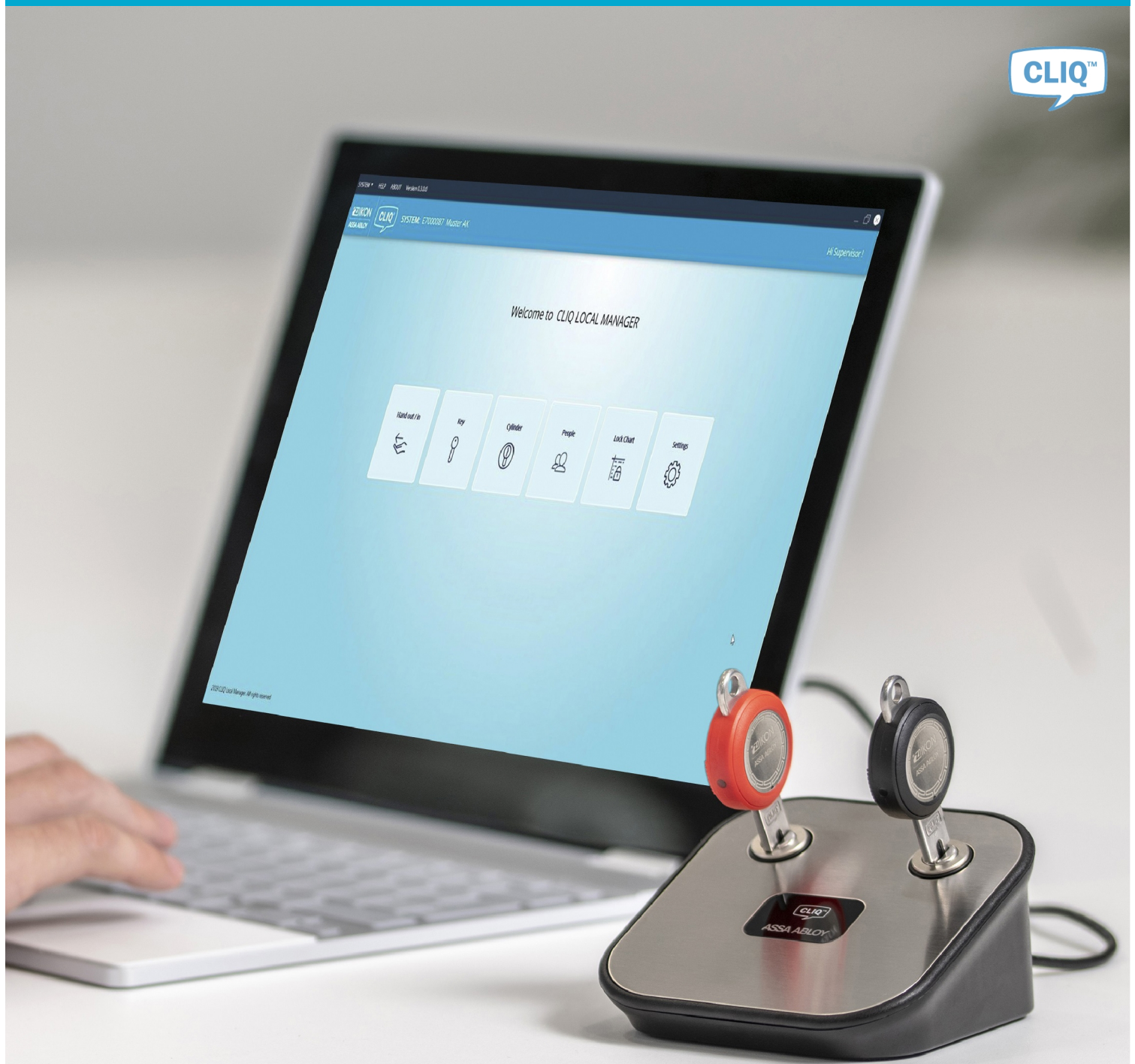
CLIQ™ Local Manager

IKON
ASSA ABLOY

User Manual

assaabloy.com

Experience a safer
and more open world



ASSA ABLOY is committed to operating in compliance with data laws globally across its various divisions. The EU General Data Protection Regulation ("GDPR") requires us to meet principles of fairness, accountability and transparency in handling personal data.

ASSA ABLOY has a focused, structural and systemic approach to data protection and privacy. Our globally applicable ASSA ABLOY Data Protection Compliance Program has been developed to protect the integrity of the personal data of our employees, customers and partners worldwide. ASSA ABLOY has dedicated resources across the Group whose continual focus is the compliance with data laws globally including the GDPR.

We keep personal data secure using equipment operating in accordance with recognized security standards. In cases where the rights of individuals are at risk, we conduct impact assessments in accordance with our standard methodology.

We recognize that data laws are continuously evolving. ASSA ABLOY has invested considerable resources in raising awareness and rolling out training in relation to its Data Protection Compliance Program. We continuously monitor data protection developments to ensure our policies, processes and procedures are relevant and adequate.

We are committed to ensuring good data governance and are invested in data trust and security for the long-term.

ASSA ABLOY
Sicherheitstechnik GmbH
Attilastrasse 61-67
12105 Berlin
GERMANY
Tel. + 49 30 8106-0
Fax: + 49 30 8106-26 00
berlin@assaabloy.com
www.assaabloy.de

Program version: V 1.9
Main document number: D001066750
Date published: 2022-07-06
Language: en-GB

1	Introduction	8
1.1	Introduction to CLM	8
2	Getting Started	9
2.1	Installing CLM	9
2.2	Setting up a Locking System	10
2.2.1	Setting up a Locking System without Remote Feature	10
2.2.1.1	Importing a Locking System	11
2.2.1.2	Restoring a Locking System	11
2.2.1.3	Migrating a Locking System	12
2.2.2	Setting up a Locking System with Remote Feature	13
2.2.3	Errors in Importing or Migrating a Locking System	14
2.3	Logging In	15
2.3.1	Logging In Using a C-key	15
2.3.2	Logging In with User Name and Password	15
2.3.3	Switching from Read-Only Mode to C-Key Authentication Mode	16
2.4	Switching to Another System	16
2.5	User Interface	16
2.5.1	Navigating in CLM	16
2.5.2	Notifications	17
2.5.3	Customising List View	17
2.5.4	Creating a View Report	18
3	Working with CLM	19
3.1	Handing out Keys	19
3.2	Handing In Keys	21
3.3	Editing Key Handouts	22
3.4	Handling Notifications	23
3.5	Setting Authorisations	24
3.5.1	Understanding the Lock Chart	24
3.5.2	Setting Electronic Access	25
3.5.2.1	Setting Electronic Access in Cylinders	26
3.5.2.2	Setting Electronic Access in Keys	28
3.5.2.3	Removing Dynamic Access from a Key	29
3.5.3	Setting Key Validity	30
3.5.4	Using the Key Revalidation Feature	30
3.5.4.1	Enabling and Disabling Key Revalidation	31
3.5.4.2	Revalidating a Key	31
3.5.5	Setting Key Schedule	31
3.5.6	Copying the Key Authorisations	32
3.5.7	Copying Cylinder Authorisations	34
3.5.8	Viewing a Key Access Report	34
3.5.9	Viewing a Cylinder Access Report	34
3.5.10	Viewing an Employee or Visitor Access Report	35
3.5.11	Viewing Key and Cylinder Event Logs	35

3.6	Managing Keys	36
3.6.1	Understanding the Key List	36
3.6.2	Managing Mechanical Keys	37
3.6.2.1	Creating a Key Line	37
3.6.2.2	Viewing and Editing Key Line Information	38
3.6.2.3	Creating a Mechanical Key	39
3.6.2.4	Creating Multiple Mechanical Keys	39
3.6.2.5	Viewing and Editing Mechanical Key Information	40
3.6.2.6	Deleting Key Lines or Mechanical Keys	41
3.6.3	Managing Electronic Keys	41
3.6.3.1	Viewing and Editing Electronic Key Information	41
3.6.3.2	Viewing and Editing Key Group Information	42
3.6.3.3	Setting DST on Quartz Keys and Dynamic Keys	43
3.6.3.4	Synchronising an Electronic Key to the System Time	43
3.6.3.5	Checking the Electronic Keys Battery Level	44
3.7	Managing Cylinders	44
3.7.1	Understanding the Cylinder List	44
3.7.2	Creating a Mechanical Cylinder	46
3.7.3	Creating Multiple Mechanical Cylinders	47
3.7.4	Viewing and Editing Cylinder Information	47
3.7.5	Creating a Cylinder Group	49
3.7.6	Viewing and Editing Cylinder Group Information	49
3.7.7	Restructuring a Cylinder Group	49
3.7.8	Deleting Cylinders or Cylinder Groups	50
3.8	Managing Employees and Visitors	50
3.8.1	Understanding the Person List	51
3.8.2	Creating an Employee or Visitor	52
3.8.3	Viewing and Editing Employee or Visitor Information	52
3.8.4	Activating and Deactivating Persons	53
3.8.5	Deleting an Employee or Visitor	53
3.8.6	Adding Persons to the Person List using a CSV File	53
3.9	Handling Audit Trails	54
3.9.1	Enabling and Disabling Key or Cylinder Audit Trails	54
3.9.2	Viewing Key Audit Trail Reports	55
3.9.3	Reading Audit Trails from Keys	55
3.9.4	Viewing Cylinder Audit Trail Reports	56
3.9.5	Reading Audit Trails from Cylinders	57
3.10	Handling Lost and Broken Keys	58
3.10.1	Reporting Lost or Broken Mechanical Keys	58
3.10.2	Reporting Lost Electronic Keys	58
3.10.3	Reporting Broken Electronic Keys	60
3.10.4	Returning Lost or Broken Keys	62
3.11	Handling Lost and Broken Cylinders	63
3.11.1	Reporting Lost or Broken Cylinders	63
3.11.2	Returning Lost or Broken Cylinders	64
3.12	Programming an Electronic Key	64
3.12.1	Programming an Electronic Key in the Local PD	64
3.12.2	Programming an Electronic Key in a Wall PD	65

3.13	Programming Cylinders	65
3.13.1	Programming Cylinders	65
3.13.2	Reprogramming Cylinders	66
3.14	Upgrading Firmware Files	67
3.14.1	Upgrading an Electronic Key's Firmware	67
3.14.2	Upgrading an Electronic Cylinder Firmware	68
3.14.3	Viewing the Status of Cylinder Firmware Upgrade	68
3.14.4	Upgrading a C-Key's Firmware	69
4	Configuring CLM	70
4.1	General System Settings	70
4.1.1	Managing Backup Reminders	70
4.1.2	Backing up Locking Systems	70
4.1.2.1	Backing up Currently Opened System	70
4.1.2.2	Backing up All Systems	71
4.1.3	Restoring Locking Systems	71
4.1.4	Extending the Locking System	71
4.1.5	Importing a Firmware File	72
4.1.6	Editing Company Information	72
4.1.7	Setting Default Periods, Date and Time	73
4.1.8	Managing Key Schedule Templates	73
4.1.9	Setting Audit Trail Retention Policy	74
4.1.10	Setting the Revalidation Period	74
4.1.11	Enabling and Disabling Approver Setting	75
4.1.12	Setting Notifications	75
4.1.13	Handling Hand Out and Hand In Text Templates	76
4.1.14	Enhancing Security	76
4.1.15	Deleting a Locking System	77
4.1.16	Updating License	77
4.1.17	Enabling and Disabling Alternative Marking Edit	77
4.1.18	Enabling and Disabling Automatic Dynamic Key Programming	78
4.1.19	Setting PD Options	78
4.2	C-Key Settings	78
4.2.1	Setting the C-Key PIN	78
4.2.2	Understanding the C-Key List	79
4.2.3	Resetting a C-Key PIN	80
4.2.4	Viewing and Editing C-Key Information	80
4.2.5	Managing C-Key Cylinder Permission	81
4.2.6	Handing Out C-Keys	81
4.2.7	Handing In C-Keys	82
4.2.8	Synchronising a C-Key to System Time	83
4.2.9	Reporting Lost and Broken C-Keys	83
4.2.10	Returning Lost or Broken C-Keys	84

4.3	C-Key User Settings	84
4.3.1	Working with the User List	84
4.3.2	Viewing and Editing User Information	84
4.3.3	Changing the System Language	85
4.3.4	Managing User Rights and Roles	86
4.3.4.1	Editing User Rights	86
4.3.4.2	Appointing or Dismissing the Approver Role	86
4.3.5	Setting a New User Password	87
4.3.6	Activating or Deactivating a User	88
4.3.7	Deleting a User	88
4.4	Managing the Controller and Remote PDs	88
4.4.1	Understanding the Remote List	89
4.4.2	Adding a New Wall PD	89
4.4.3	Viewing and Editing Controller or Remote PD Information	90
4.4.4	Activating or Deactivating a Wall PD	91
4.5	Editing System Information	92
5	CLM Concepts and Features	93
5.1	CLIQ™ Hardware	93
5.1.1	CLM Architecture	93
5.1.2	Keys	93
5.1.2.1	Key Types	93
5.1.2.2	User Keys	94
5.1.2.3	C-Keys	94
5.1.2.4	Key Groups	95
5.1.3	Cylinders	96
5.1.3.1	Cylinders	96
5.1.3.2	Cylinder Groups	96
5.1.4	Programming Devices	96
5.1.4.1	Local PDs	96
5.1.4.2	Wall PDs	97
5.2	Authorisation Principles	97
5.2.1	Authorisation Principles Overview	97
5.2.2	Mechanical Authorisation	98
5.2.3	Key Validity	98
5.2.4	Key Revalidation	98
5.2.5	Electronic Authorisation	99
5.2.6	Key Schedule	100
5.3	Remote Update	100
5.4	Audit Trails	101
5.5	User Roles and Rights	101
6	Appendix	102
6.1	Shortcut Keys	102
6.1.1	General Shortcuts	102
6.1.2	Key List Shortcuts	102
6.1.3	Cylinder List Shortcuts	102
6.1.4	C-Key List Shortcuts	103
6.1.5	Person List shortcuts	103



6.1.6	Lockchart Shortcuts	103
6.1.7	Key Schedule Card Shortcuts	104
6.1.8	System List Shortcuts	104
6.1.9	User List Shortcuts	104
6.2	Cases Cause Errors in Importing or Migrating a Locking System	104
6.3	CSV File Structure	106
6.4	Wall PD Indications	108

1 Introduction

1.1 Introduction to CLM

CLIQ™ Local Manager (CLM) is a locally installed Windows application for the day-to-day management of CLIQ™ systems. With CLM locking system administrators can perform a variety of tasks, such as configuring authorisations and handing out keys.

2 Getting Started

2.1 Installing CLM

Minimum hardware requirements:

- Windows 10 64 bits
- CPU 1.5 GHz
- 2 GB RAM
- 1 GB Hard Disk
- .NET Framework 4.7.2 installed
- Screen resolution 1024 x 768

Recommended hardware specifications:

- Windows 10 64 bits
- CPU i5 2.0 GHz
- 4 GB RAM
- 10 GB SSD Drive
- .NET Framework 4.7.2 installed
- Screen resolution 1920 x 1080

Items provided by ASSA ABLOY or a certified reseller:

- CLIQ™ Local Manager installation file
- Locking system file
- Product license file
- Programming device
- Master C-Key

To install CLM:

- 1) Connect the Local PD to the computer.
- 2) Right-click the installation file.
- 3) Click **Run as administrator**.
- 4) Click **INSTALL**.
- 5) Select the installation folder and click **OK**.

- 6) Select a language from the drop-down list and click **CONTINUE**.
- 7) Read the End User Licence Agreement.
- 8) Click the check box and **OK** to continue.



NOTE!

To install ASSA ABLOY software, the license terms must be accepted.

Wait for the program to install SQL, this might take a few minutes.

2.2 Setting up a Locking System

After installing CLM, set up a locking system by creating a new database, adding a locking system, and enrolling the controller if the locking system has the remote feature.

- For setting up a locking system **without the remote feature**, follow the instruction in Section 2.2.1 *“Setting Up a Locking System without Remote Feature”*, page 10.
- For setting up a locking system **with the remote feature**, follow the instruction in Section 2.2.2 *“Setting up a Locking System with Remote Feature”*, page 13.

2.2.1 Setting up a Locking System without Remote Feature

1. Run CLM.
2. Create a database by clicking **YES** when asked.

When executing CLM, a new database must be created.

3. Add a locking system by one of the following ways:
 - **Migrate:** If the locking system to be added is from an older ASSA ABLOY product.
See Section 2.2.1.3 *“Migrating a Locking System”*, page 12 for instructions.
 - **Import:** If the locking system to be added is newly created.
See Section 2.2.1.1 *“Importing a Locking System”*, page 11 for instructions.
 - **Restore:** If the locking system to be added is a CLM backup copy.
See Section 2.2.1.2 *“Restoring a Locking System”*, page 11 for instructions.



2.2.1.1 Importing a Locking System

- 1) Connect the Local PD to the PC.
- 2) Insert the system's Master C-Key in the left slot of the Local PD.



NOTE!

The locking system's Master C-Key must remain in the Local PD during the entire import process.

- 3) Run CLM.



NOTE!

If the system does not detect the Local PD, press **Ctrl + Alt + Shift + P** keys and select the Local PD from the working Local PD list.

- 4) Click **Import**.
- 5) Select the locking system's ELS-file.
- 6) When asked, enter the Master C-Key's **PIN**.
- 7) Read through the information shown after system creation.
- 8) When asked, import the product license file.

2.2.1.2 Restoring a Locking System

Prerequisite:

Restoring a locking system requires an SMB file generated from a previous CLM backup.

- 1) Connect the Local PD to the PC.
- 2) Insert the system's Master C-Key in the left slot of the Local PD.

**NOTE!**

The locking system's Master C-Key must remain in the Local PD during the entire import process.

- 3) Run CLM.

**NOTE!**

If the system does not detect the Local PD, press **Ctrl + Alt + Shift + P** keys and select the Local PD from the working Local PD list.

- 4) Click **Restore**.
- 5) Select the SMB file.
- 6) When asked, enter the Master C-Key's **PIN**.
- 7) Read through the information shown after system creation.
- 8) When asked, import the product license file.

2.2.1.3 Migrating a Locking System

Prerequisite:

Migrating a locking system requires an A2B file generated from a CLIQ™ Manager backup. Make sure that the backup file is generated from the latest version of the CLIQ™ Manager.

- 1) Connect the Local PD to the PC.
- 2) Insert the system's Master C-Key in the left slot of the Local PD.

**NOTE!**

The locking system's Master C-Key must remain in the Local PD during the entire import process.

- 3) Run CLM.

**NOTE!**

If the system does not detect the Local PD, press **Ctrl + Alt + Shift + P** keys and select the Local PD from the working Local PD list.

- 4) Click **Migrate**.
- 5) Select the A2B file.
- 6) When asked, enter the Master C-Key's **PIN**.



NOTE!

If the system contains a cylinder group with a single-cylinder, select whether to migrate it as a group or as a non-grouped cylinder.

- 7) When asked, import the product license file.

Check whether all the data is migrated from the CLIQ™ Manager successfully.

2.2.2 Setting up a Locking System with Remote Feature

When the system is opened with a remote license for the first time, the controller is enrolled to the system by the following process.

Prerequisites:

- A CLM Remote Controller is provided.
 - A correct CLM version with remote capabilities is downloaded.
 - A system contains at least one Wall PD.
 - A CLM Remote license is provided.
- 1) Connect the controller to a power source and connect to the same LAN that the CLM client PC connects to.
 - 2) Insert the C-Key in the left slot of the local PD.
 - 3) Run CLM **as administrator**.
If multiple communication devices are detected, the system asks to select the COM Port to which the Local PD is connected.
 - 4) Select the locking system's ELS or XLM files.
 - 5) When asked, enter the Master C-Key's **PIN**.
 - 6) Read through the information shown after system creation.
 - 7) When asked, import a license for the system that has the remote feature enabled.
The program starts the process to enrol the controller.
 - **If the controller is detected correctly:**

The system automatically starts enrolling the controller. It is not possible to operate the system until the enrolment process is completed.

When the controller is successfully enrolled to the system, click the **Remote List** button in the left menu and confirm the controller's status in the **Controller / Wall PD List**.
 - **If the connection to the controller is failed:**

The system automatically starts scanning the network.

If the information window shows the message **Could not find Controller in the network**, the controller's IP address should be manually set up by following the steps below:

a) Click the **Remote List** button in the left menu.

b) In the **Remote List**, right-click the controller.

The context window is opened.

c) Click **Info Card**.

The information card for the selected device is opened.



HINT!

Double clicking on the device in the list performs the same action.

d) Go to the **Connection Settings** tab.

e) Click the **Use Custom IP** check box and enter the IP address of the controller.

To set up a new Wall PD, see Section 4.4.2 *"Adding a New Wall PD"*, page 89.

2.2.3 Errors in Importing or Migrating a Locking System

During importing or migrating the system, wrong element values in the file cause either ceasing the process or skipping these elements.

When the process is discontinued, **There was an error importing the system file.** or **There was an error migrating the backup file.** is displayed. In some cases, a specific message regarding the error appears.

When the process is completed but the element with wrong value is skipped, the issue list is displayed at the end of the process. The list shows all the elements which are not imported due to the wrong value.

If these errors occur, check the followings:

- if the C-Key is inserted into the Local PD.
- if the Local PD is properly connected to the PC.

The user can also fix the element in the import or migrate file manually. Refer to the tables in Section 6.2 *"Cases Cause Errors in Importing or Migrating a Locking System"*, page 104 which show system's elements and their potential problem cases.

If the problems cannot be solved by the user, it is recommended to contact your local CLIQ dealer with the following information:

- the error message
- the import or migrate file
- the log files which are stored under: C: \ProgramData\CLIQ Local Manager\Logs.

2.3 Logging In

2.3.1 Logging In Using a C-key

- 1) Insert the C-Key in the left slot of the local PD.
- 2) Run CLM.
- 3) Enter the **PIN**.

After five unsuccessful login attempts the PIN will be blocked and CLM will ask for the PUK code to enter a new PIN.

Only the supervisor can see the PUK on the C-Key info card. For instructions on how to access the C-Key, see Section 4.2.4 *“Viewing and Editing C-Key Information”*, page 80.

The C-Key will be permanently blocked after 25 unsuccessful PUK login attempts.



NOTE!

To replace a permanently blocked C-Key, contact your certified CLIQ™ reseller.

- 4) Click **LOGIN**.

The system is displayed in the same language as the system language set on Windows. If it is necessary to change the interface language after logging in, see Section 4.3.3 *“Changing the System Language”*, page 85.

2.3.2 Logging In with User Name and Password

When logging in to a system without a C-Key, it will be opened in read-only mode with considerable restrictions in functionality. This login method may be used by normal users, but is intended for multi-system users, such as locksmiths and resellers in a maintenance capacity. Full access to the locking system functionality requires a C-Key.

- 1) Run CLM.
- 2) If CLM is configured as a multi system, select a system from the **System List**.
- 3) Enter **Username** and **Password**.
- 4) Click **LOGIN**.



NOTE!

It is recommended to change the provisional user password to a more secured one.

The system is displayed in the same language as the system language set on Windows. If it is necessary to change the interface language after logging in, see Section 4.3.3 *“Changing the System Language”*, page 85.

2.3.3 Switching from Read-Only Mode to C-Key Authentication Mode

If C-Key authentication is required when the system is in read-only mode, it is possible to switch to C-Key authentication mode without exiting the system.

- 1) Insert the C-Key in the left slot of the local PD.
- 2) On the menu bar, click **SYSTEM**.
- 3) Click **AUTHENTICATE C-KEY**.
- 4) Enter the C-Key PIN.

2.4 Switching to Another System

The program sometimes holds multiple systems and the user can switch to another system.

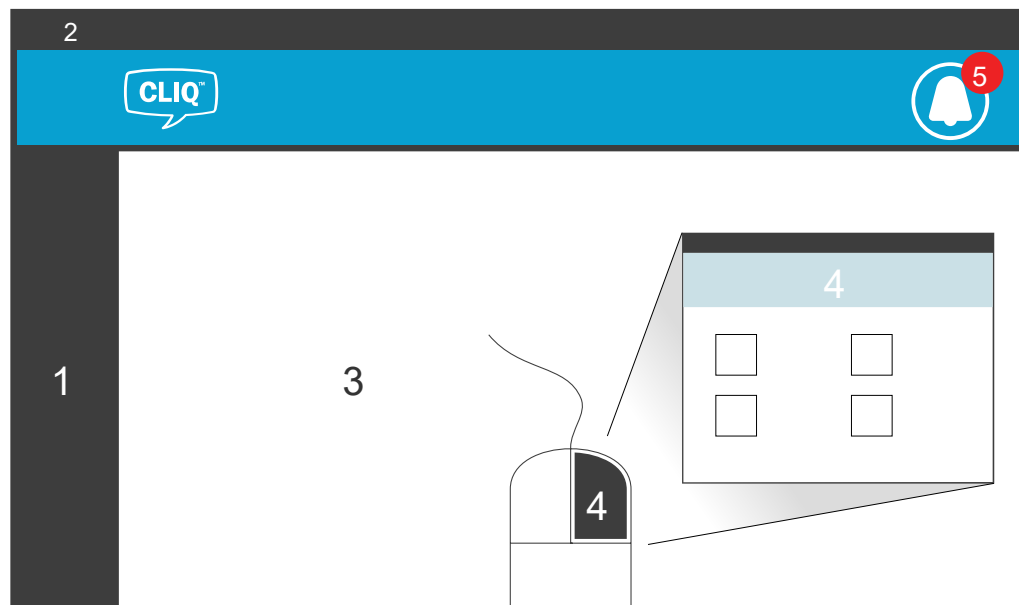
- 1) On the menu bar, click **SYSTEM**.
- 2) From the drop down list, select **CHANGE SYSTEM**.
- 3) In the pop-up screen, confirm to switch the system.
- 4) When asked, remove the C-Key from the left slot of the PD and confirm it.
- 5) From the system list, select the system to open.
- 6)
 - To open the system with read only mode:
Enter the user name and password.
 - To open the system with edit mode:
Insert the C-Key which belongs to the system and enter the PIN.

2.5 User Interface

2.5.1 Navigating in CLM

After login, the **Welcome screen** presents direct access to the most common functions. Once a function is selected, CLM displays the standard layout, with the **Left menu** listing the sections of the program, the **Top menu** listing less central functions, and the **Main screen** displaying the functionality.

One central theme in the software is the **Context window**, which can be accessed by right-clicking items in the Main window. The Context window offers easy access to the most relevant functions, depending on the situation.



1. Left menu
2. Top menu
3. Main screen
4. Context window
5. Notification area

2.5.2 Notifications

Managing scheduled events is an integral part of an electronic locking system's work flow. CLM can be configured to notify users when hand ins or backups are overdue, and when employee or visitor periods expire. The notification area displays the number of notifications by type.

To make a backup or handle the overdue employees, visitors or keys, click the notification button and select a notification type to manage. The buttons in the pop-up window navigate to the appropriate page to complete the selected task.

- To edit the backup notification setting, see Section 4.1.1 *"Managing Backup Reminders"*, page 70.
- To edit the notification settings on overdue keys, employees and visitors, see Section 4.1.12 *"Setting Notifications"*, page 75.

To handle the notifications, see Section 3.4 *"Handling Notifications"*, page 23.

2.5.3 Customising List View

All main lists in CLM can be customised in terms of column width and visibility, order and sorting. However, some core columns, for example Name or Mark, cannot be hidden.

The list setting is customised directly in the list or via the **List Settings** button.

- Set in the list:

- To change a column's width, place the cursor on the resize bar of a column heading. Hold and move the bar.

By double clicking the resize bar, the program calculates the width of the longest text and resizes the column to that width.
- To rearrange the column order, drag-and-drop the column header to move.
- Set from the **List Settings** button:
 - To hide or unhide a column, click the column's tick-box.
 - To rearrange the column order, drag-and-drop the column headers.
 - To reset the default values, click **RESET**.

2.5.4 Creating a View Report

Users work with multiple lists in CLM and the system helps to create view reports from the lists. The view report can be printed out or saved in Microsoft Excel or Adobe PDF formats.

- 1) Click the **View Report** button which is located above the list.



NOTE!

In case of viewing the **Lock Chart** report, in the pop-up window, select either of the below options:

- **Full report** to include the all keys and cylinders.
- **Custom** to show only selected range.

The pop-up window shows the current view of the list.

- 2) Optional: Adjust the view by clicking the following buttons.



Fit to window's width.



Fit one full page.



Change orientation.

- 3) Save or print out the view report by clicking the following buttons.



Save the view report in PDF format.



Export the view report as an Excel file.



Print out the view report.

- 4) Click **CLOSE** to exit.

3 Working with CLM

3.1 Handing out Keys

To hand out a C-Key, refer to Section 4.2.6 *"Handing Out C-Keys"*, page 81.

- 1) In **Hand out / in**, click **Hand out**.



HINT!

Hand Out can also be selected from the context window when right-clicking a person or a key in **Lock Chart**, **Key List** or **Person List**.

- 2) If a key is not yet selected:
 - To select the key inserted in the right slot of the Local PD, click **SCAN**.
 - To select the key from the list:
 - a) Under **Key**, click **SELECT**.
 - b) From the **Key List** pop-up window, select a key and click **OK**.
- 3) If a person is not yet selected:
 - a) Under **Person**, click **SELECT**.
 - b) Select **Employee** (default) or **Visitor** from the top right corner of the pop-up window.
 - Select the person from the list, if available.
 - If the person is not found in the list, create a new person by clicking **Create Employee** or **Create Visitor**.

For more information on creating a person, see Section 3.8.2 *"Creating an Employee or Visitor"*, page 52.
 - c) Click **OK**.
- 4) Set **Hand Out Date and Time** under **Dates**.
The default is the current date and time.
The date and time selected is for administrative purposes only.
- 5) Set **Hand In Date and Time** or select **Permanent**.



NOTE!

An expired hand in date only affects the overdue key notification, and does not automatically revoke access rights. Access rights are time-limited with the validity and key scheduling functions.

- 6) **Electronic Keys Only:** Set the key's validity under **Validity**.

- a) Select the validity type from three options:
- **Never:** The key does not open any electronic cylinder.
 - **Always:** The key opens the cylinders where it has access.
 - **From/To Date:** The key opens the cylinders where it has access between specific dates.

This option is only available for Quartz and Dynamic keys.

- b) Click the check box **Use Schedule** next to **Always** or **From/To Date** to set the details.

For instructions on how to set the schedule, see Section 3.5.5 *"Setting Key Schedule"*, page 31.

If no schedule is set here, the key will work 24/7 during the period which is set in *Step 6.a*.

7) **Dynamic Keys Only:**

- a) Click **CHANGE ACCESES** under **Key Accesses** to set key accesses.

A pop-up version of the **Lock Chart** is opened for the selected key. For more information on how to set electronic accesses in the **Lock chart**, see Section 3.5.2 *"Setting Electronic Access"*, page 25.

- b) If key accesses information should be included in the hand out report, click the check box **Include key accesses in report**.

8) Optional: Select a hand out text template:

- a) Click **SELECT TEXT TEMPLATE**.

- b) Select a **Template Name** and click **OK**.

For more information on how to add and edit hand out text templates, see Section 4.1.13 *"Handling Hand Out and Hand In Text Templates"*, page 76.

- 9) Confirm if the handing out key is in the right slot of the Local PD and click **SAVE**.



NOTE!

Electronic Keys Only: If the key is not inserted in the right slot of the Local PD, the warning message tells that the validity and the schedule are not programmed to the key.

To set the validity and the schedule after handing out process, follow the instruction in Section 3.5.3 *“Setting Key Validity”*, page 30 or Section 3.5.5 *“Setting Key Schedule”*, page 31.

- **Dynamic Keys Only:** The cylinder access, as well as the validity and the schedule, is not programmed if the key is not in the right slot of the Local PD.

To program the validity and the schedule, follow the instruction in Section 3.5.3 *“Setting Key Validity”*, page 30 or Section 3.5.5 *“Setting Key Schedule”*, page 31.

The key access list is saved in the **Job List** as a key job. The new access is automatically programmed to the key when the key is inserted into the right slot of the Local PD.

- 10) Review or print the hand out report.

The notes from the hand out text template are included at the end of the hand out report.



HINT!

The user can always review or edit the hand out report by clicking **Reprint Hand Out** or **Edit Handout** in the key's context window. The **Reprint Hand Out** button is also available in the person's context window.

- 11) **Electronic Keys Only:** Remove the key from right slot of the Local PD, if applicable.

3.2 Handing In Keys

- 1) **Electronic Keys Only:** Insert a key in the right slot of the Local PD.
- 2) In **Hand out / in**, click **Hand in**.



HINT!

Hand in can also be selected from the context window when right-clicking a person or a key in **Lock Chart**, **C-Key List**, **Key List** or **Person List**.

- 3) If a key is not yet selected:
 - To select the inserted key, click **SCAN**.
 - To select a key:

- a) Under **Key**, click **SELECT**.
 - b) From the **Key List** window, select a key and click **OK**.
- 4) Optional: Select a hand in text template:
- a) Click **SELECT TEXT TEMPLATE**.
 - b) Select a **Template Name** and click **OK**.

For more information on how to add and edit hand in text templates, see Section 4.1.13 *"Handling Hand Out and Hand In Text Templates"*, page 76.

- 5) Click **SAVE** to confirm the hand in.



NOTE!

Electronic Keys Only: To complete a hand in, the Electronic Key to be programmed must be inserted in the right slot of the Local PD.

- 6) **Electronic Keys Only:** The popped up **Question** window asks whether to reset key's validity, schedule and key access or not.

- If these key's data should be removed, click **YES**.

Cleaning process is shown in the progress bar and key's validity is set to **Never**.

- If these key's data should be kept, click **NO**.

- 7) Review or print the hand in report.

the hand in report reflects the current status of the key validity and the key schedule.



HINT!

The user can always review the hand in report by clicking **Reprint Hand In** in the context window.

- 8) **Electronic Keys Only:** Remove the key from the Local PD.

3.3 Editing Key Handouts

- 1) Insert a handed out key to the right slot of the local PD.
- 2) In the **Key List** or the **Lock Chart**, right-click the inserted key.



NOTE!

The key inserted to the right slot of the Local PD is marked by a green key symbol in the list.

- 3) Click **Edit Handout**.

The **Hand Out** page is opened.

- 4) Edit the **Hand Out** page.

For more information about the page, see Section 3.1 *“Handing out Keys”*, page 19.

- 5) Click **SAVE** to confirm the edited hand out.

- 6) Review or print the hand out report.

The notes from the hand out text template are included in the back of the hand out report.

- 7) Remove the handed out key from the Local PD.

3.4 Handling Notifications

The system displays a notification in the following cases:

- Overdue key: When a key is not handed in by the hand in date.
- Overdue employees: When the valid date of an employee is surpassed.
- Overdue visitors: When the end date of a visitor is surpassed.
- Backup reminder: When it is the time to create a backup according to the schedule.
- Remote Tasks: When a remote task is completed and automatically received by the CLM.

- 1) Click the notification button and select a notification type to manage.

A pop-up window opens.

- 2) • To handle overdue items:

- a) From the list, select the item to handle.

- b) For an overdue key: Clicking **Hand In** navigates to the **Hand In** page.

For an expired employee or visitor: Clicking the **Go to Employee** or the **Go to Visitor** button navigates to **Person List**.

- c) To process the key to be handed in, follow the instructions in Section 3.2 *“Handing In Keys”*, page 21.

To extend **End Date and Time** of the expired employees or visitors, follow the instruction in Section 3.8.3 *“Viewing and Editing Employee or Visitor Information”*, page 52.

- To create a backup:

- a) Click **Create System Backup** to create a backup of the current system or the **Do Full Database Backup** button.

- b) When asked, enter the C-Key PIN.

- To read the remote task report, click **Notification** to read a report from the Wall PDs.

The notification symbol (white bell symbol) is displayed until all tasks in the notification are completed or a remote task report is read.

3.5 Setting Authorisations





3.5.1 Understanding the Lock Chart

The **Lock Chart** is one of the central sections of CLM for daily tasks. It is used to set key accesses, while also offering an extensive overview of the system's keys and cylinders. Context windows are available for keys and cylinders, and items can also be searched for.






For Normal keys and Quartz Keys, access must be granted in the cylinder. The system creates a cylinder job which updates the affected cylinders with the Programming key. Cylinder jobs can be created in the cylinder edit mode in the **Lock Chart**.




For Dynamic Keys, access must be granted in both the key and cylinder. Cylinder jobs can be avoided by programming all cylinders to grant access for a key in the initial system order, while granting cylinder access to the selected keys. Key jobs can be created in the key edit mode in the **Lock Chart**.

Colours in the Lock Chart

Colour	Description
	The key has no access.
	The key access is stored in both key and cylinder.
	The key access is stored in the cylinder, but not in the key.
	The key access is stored in the key, but not in the cylinder.

Symbols in the Lock Chart

Symbol	Description
	Denotes double cylinder. The left field indicates the cylinder's A side, the right field indicates the B side. A grey field denotes a mechanical cylinder.
	The key is granted key access, but the affected cylinders are not yet updated.
	The key access is revoked, but the affected cylinders are not yet updated.
	There is a conflict between key access and cylinder access settings in a Dynamic Key.
	The key has a pending key job.

Symbol	Description
	The inserted key has a pending key job.
	The key is inserted to the right slot of the Local PD.
	This button enables resizing of the lock chart borders.

Buttons

- The **Show all States** toggle button
When **NO** is selected, lost, broken and planned keys/cylinders are not shown in the lock chart.
- The **Show only electronic** toggle button
When **YES** is selected, all mechanical elements in the list are removed from the lock chart.
- The **Edit Mode** buttons set the lock chart to key access edit mode or cylinder access edit mode.
- The **Job List** button
This button opens the **Job List**.
The button sometimes accompanies with the number of Dynamic Keys to be programmed at the lower left corner, and the number of cylinders to be programmed at the lower right corner.
- The **Flip** button flips the keys and cylinders view.
- The **Zoom Slider** changes the lock chart zoom value.
- The **Auto fill** button starts the process of automatically filling a series of locking authorisations to keys or cylinders.
For more information, see Section 3.5.2 "[Setting Electronic Access](#)", page 25.
- The **View Report** button
For more information, see Section 2.5.4 "[Creating a View Report](#)", page 18.
- The **List Settings** button
For more information, see Section 2.5.3 "[Customising List View](#)", page 17.

3.5.2 Setting Electronic Access

Electronic authorisation is stored in the cylinder and, for Dynamic Keys, also in the key. See Section 5.2.5 "[Electronic Authorisation](#)", page 99 for more information about the electronic authorisation.

See Section 3.5.2.1 *“Setting Electronic Access in Cylinders”*, page 26 for more information about how to set the cylinder's key access.

See Section 3.5.2.2 *“Setting Electronic Access in Keys”*, page 28 for more information about how to set the Dynamic Key's cylinder access.

3.5.2.1 Setting Electronic Access in Cylinders

The key access can be set either by double-clicking each square in the **Lock Chart** or by using **Auto fill** function.

To set the key access individually

1. In the **Lock Chart**, under **Edit Mode**, click the cylinder symbol.

The **Lock Chart** changes to the cylinder edit mode.

2. Double-click the corresponding square in the chart.



NOTE!

When changing an authorization on cylinder side, the program checks if the authorizations in the database and the cylinder match. If not, the system creates a reprogramming job for the cylinder. For more details about how to proceed the reprogramming process, see Section 3.13.2 *“Reprogramming Cylinders”*, page 66.

Cylinder jobs are created and the number appears at the lower right corner of the **Job list** icon.

To understand colours and symbols in the **Lock Chart**, see Section 3.5.1 *“Understanding the Lock Chart”*, page 24

3. Apply changes to the cylinders.

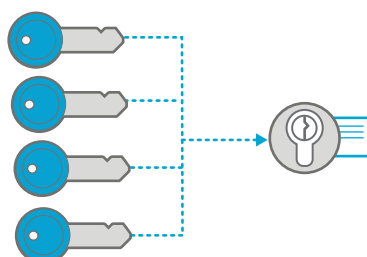
Follow the process in Section 3.13.1 *“Programming Cylinders”*, page 65.

To set the same key access in a range of keys or cylinders

1. In the **Lock Chart**, under **Edit Mode**, click the cylinder symbol.

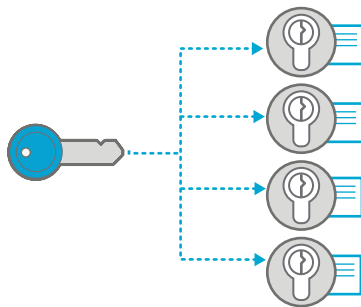
The **Lock Chart** changes to the cylinder edit mode.

2. – **To set the same access to multiple keys for a cylinder:**



In the **Lock Chart**, select the range of keys in the particular cylinder row by marking the corresponding squares.

- To set the same access to a key for multiple cylinders:



In the **Lock Chart**, select the range of cylinders in the particular key row by marking corresponding squares.



HINT!

To mark the range of access, hold and drag the mouse in the Lock Chart.

Selected squares are encircled by a red line.

3. Click the **Auto fill** button above the **Lock Chart**.

Depending on the selected cylinder types, the pop-up window shows single, double or both types of access squares.

4. Set the access state in the pop-up window.

A double-click in a square changes the access state between:

- **Fill:** grants the access, if not yet set.
- **Delete:** revokes the access, if not yet set.
- **Keep:** keeps the state of the access.

5. Click **OK**.



NOTE!

When changing an authorization on cylinder side, the program checks if the authorizations in the database and the cylinder match. If not, the system creates a reprogramming job for the cylinder. For more details about how to proceed the reprogramming process, see Section 3.13.2 *"Reprogramming Cylinders"*, page 66.

Cylinder jobs are created and the number appears at the lower right corner of the **Job list** icon.

6. Apply changes to the cylinders.

Follow the process in Section 3.13.1 *"Programming Cylinders"*, page 65.

3.5.2.2 Setting Electronic Access in Keys



NOTE!

This process is required only for Dynamic Keys.

How to set the cylinder access to the Dynamic Keys is explained in this section. To remove the cylinder access list from the Dynamic Keys, see Section 3.5.2.3 *“Removing Dynamic Access from a Key”*, page 29.

The key access can be set either by double-clicking each square in the **Lock Chart** or by using **Auto fill** function.

To set the cylinder access individually

1. In the **Lock Chart**, under **Edit Mode**, click the key symbol.

The **Lock Chart** changes to the key edit mode.

2. Double-click the corresponding square in the chart.

Key jobs are created and the number appears at the lower left corner of the **Job list** icon.

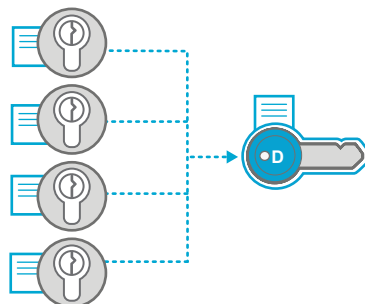
To understand colours and symbols in the **Lock Chart**, see Section 3.5.1 *“Understanding the Lock Chart”*, page 24

To set the same cylinder access in a range of keys or cylinders

1. In the **Lock Chart**, under **Edit Mode**, click the key symbol.

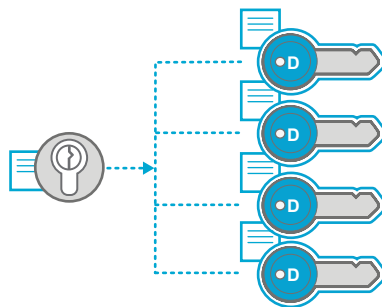
The **Lock Chart** changes to the key edit mode.

2. — **To set the same access to multiple cylinders for a Dynamic Keys :**



In the **Lock Chart**, select the range of cylinders in the particular Dynamic Key row by marking corresponding squares.

- **To set the same access to a cylinder for multiple Dynamic Keys:**



In the **Lock Chart**, select the range of Dynamic Keys in the particular cylinder row by marking corresponding squares.



HINT!

To mark the range of access, hold and drag the mouse in the Lock Chart.

Selected squares are encircled by a red line.

3. Click the **Auto fill** button on the **Lock Chart**.

Depending on the selected cylinder type, the pop-up window shows single or double cylinder access squares.

4. Set the access state in the pop-up window.

A double-click in a square changes the access state between:

- **Fill:** grants the access, if not yet set.
- **Delete:** clears the access, if not yet set.
- **Keep:** keeps the state of the access.

5. Click **OK**.

Key jobs are created and the number appears at the lower left corner of the **Job list** icon.

After key jobs are created, apply the changes to the key following the procedure in Section 3.12 *"Programming an Electronic Key"*, page 64.

3.5.2.3 Removing Dynamic Access from a Key

- 1) If the Dynamic Key to remove the dynamic access is available, insert it into the right slot of the Local PD.
- 2) In the **Key List** or the **Lock Chart**, right click the Dynamic Key.
- 3) Select **Remove Dynamic Access**.
- 4) Click **OK**.
 - If the key is in the Local PD, the key is directly programmed in the Local PD.

- If the key is not in the Local PD, an electronic key job is created and stored in the Job List to be executed either in a Wall PD or the Local PD.

For programming key jobs from the Job List, see Section 3.12 *“Programming an Electronic Key”*, page 64.

- 5) When notified that the update process is complete, remove the key from the Local PD if any.

3.5.3 Setting Key Validity

- 1) If the key to set is available, insert it into the right slot of the Local PD.
- 2) In the **Key List** or the **Lock Chart**, right click the key to set validity for.
- 3) Select **Key Validity**.
- 4) Enter the required validity settings.

See Section 5.2.3 *“Key Validity”*, page 98 for a detailed description of the settings.

- 5) Click **OK**.
 - If the key is in the Local PD, the key is directly programmed in the Local PD.
 - If the key is not in the Local PD, an electronic key job is created and stored in the Job List to be executed either in a Wall PD or the Local PD.

For programming key jobs from the Job List, see Section 3.12 *“Programming an Electronic Key”*, page 64.
- 6) When notified that the update process is complete, remove the key from the Local PD if any.

3.5.4 Using the Key Revalidation Feature

Prerequisites:

- The locking system has the remote feature.
- The user key must be either Quartz Key or Dynamic Key.

If the revalidation feature is set to a key, the key must be revalidated either in a Wall PD or in the Local PD to stay active for a certain time period.

- For more information about the feature, see Section 5.2.4 *“Key Revalidation”*, page 98.
- For setting the feature to a key, see Section 3.5.4.1 *“Enabling and Disabling Key Revalidation”*, page 31.
- For setting the revalidation period, see Section 4.1.10 *“Setting the Revalidation Period”*, page 74.

3.5.4.1 Enabling and Disabling Key Revalidation



NOTE!

To enable or disable the revalidation feature to all the user keys, see Section 4.1.10 *“Setting the Revalidation Period”*, page 74.

- 1) If the key to set is available, insert it into the right slot of the Local PD.
- 2) In the **Key List** or the **Lock Chart**, right click the key to set validity for.
- 3) Select **Revalidation Settings**.
- 4) Check or uncheck the checkbox.



NOTE!

For setting the revalidation period, refer to Section 4.1.10 *“Setting the Revalidation Period”*, page 74.

All the user keys in the system are set with the same interval length.

3.5.4.2 Revalidating a Key



HINT!

Keys are revalidated also in a Local PD when the following actions were operated locally:

- set **Schedule**
- read **Audit trail**
- change **Cylinder access list**

- 1) Insert the key in a Wall PD.
- 2) After a beep sound, remove the key from the Wall PD.

3.5.5 Setting Key Schedule

- 1) If the key to set is available, insert it into the right slot of the Local PD.
- 2) In the **Key List** or the **Lock Chart**, right-click the key line to set the schedule for.
- 3) Select **Key Schedule**.

If the schedule in the system mismatches to the one in the key, the system asks which schedule should be loaded.

- To use the schedule in the system, select **Keep schedule**.
 - To use the schedule in the key, select **Update from key**.
- 4) • If a template is to be used:
 - a) Click **Load Template**.

The **Key Schedule Templates** list pops up.

- b) Select the template from the list.
- c) Click **OK**.

See Section 4.1.8 *"Managing Key Schedule Templates"*, page 73 for more information about key schedule template.

- If no template is used, select the schedule type:

Standard: Each day is enabled separately, and the start and end time can be set.

Advanced: Time slots are added one-by-one, and the start day/time and the end day/time can be set. Click **Add Slot** to start editing.

5) Optional:

- a) Click **Save as Template** to save the current schedule settings as a new template.
- b) Give a name to the template and edit the schedule if necessary.
- c) Click **OK** to save.

6) Click **OK**.

- If the key is in the Local PD, the key is directly programmed in the Local PD.
- If the key is not in the Local PD, an electronic key job is created and stored in the Job List to be executed either in a Wall PD or the Local PD.

For programming key jobs from the Job List, see Section 3.12 *"Programming an Electronic Key"*, page 64.

7) When notified that the update process is complete, remove the key from the Local PD if any.

3.5.6 Copying the Key Authorisations

This action copies the validity, schedule, cylinder access list and the key access list of a key to the selected key. What information can be copied depends on the key type of the copy.

	To			
	Key Type	Normal Key	Quartz Key	Dynamic Key
From	Normal Key	<ul style="list-style-type: none"> • Key validity (on/off) • Cylinder access list 	<ul style="list-style-type: none"> • Key validity (on/off) • Cylinder access list 	<ul style="list-style-type: none"> • Key validity (on/off) • Cylinder access list
	Quartz Key	<ul style="list-style-type: none"> • Key validity (on/off) • Cylinder access list 	<ul style="list-style-type: none"> • Key validity with the specified time period • Revalidation setting (on/off) • Key schedule • Cylinder access list 	<ul style="list-style-type: none"> • Key validity with the specified time period • Revalidation setting (on/off) • Key schedule • Cylinder access list
	Dynamic Key	Not Applicable	Not Applicable	<ul style="list-style-type: none"> • Key validity with the specified time period • Revalidation setting (on/off) • Key schedule • Cylinder access list • Key access list



NOTE!

If the source key schedule is not correctly set, for example none of the day or time is set, it will not be copied to the new key. In this case the schedule of the new key must be set manually.

The following procedure describes how to copy the key authorisations.

- 1) In the **Lock Chart** or **Key List**, right click the original key.
The context window is opened.
- 2) Click **Copy Key**.
- 3) Read the message in the **Information** window and click **OK**.
- 4) From the list, select the key to copy and click **OK**.



NOTE!

- Only keys with the **In Stock** status are listed.
- In case of copying a Dynamic Key, only Dynamic Keys are listed in the list.

After key jobs are created, apply the changes to the key following the procedure in Section 3.12 *"Programming an Electronic Key"*, page 64.

If there is any change in the cylinder access list in the copy, it is necessary to program the affected cylinders. To program the cylinders, refer to Section 3.13.1 *“Programming Cylinders”*, page 65.

3.5.7 Copying Cylinder Authorisations

- 1) In the **Cylinder List** or the **Lock Chart**, right-click the cylinder from which the authorisations are copied.
The context window is opened.
- 2) Click **Copy authorizations**.
A new window pops up with the list of available cylinders.
- 3) From the list, select a cylinder to which the access is copied and click **OK**.
The cylinder authorisations are copied to the selected cylinder.
- 4) Read the message in the Information window and click **OK**.
A cylinder job is created and the number appears at the lower right corner of the **Job list** icon.

To complete the task, the cylinder must be programmed. For further information, see Section 3.13.1 *“Programming Cylinders”*, page 65.

Changes to the Dynamic Key accesses affecting the target cylinder have to be made manually. See Section 3.5.2.2 *“Setting Electronic Access in Keys”*, page 28 for more information how to change cylinder access to Dynamic Keys.

3.5.8 Viewing a Key Access Report

A key access report lists the cylinders that the keys can access. The report is displayed in PDF format, and can thus be printed.

- 1) In the **Key List** or the **Lock Chart**, right-click the key line.
- 2) Click **View access report**.
- 3) View or print the access report.

3.5.9 Viewing a Cylinder Access Report

A cylinder access report lists the keys which have access to the cylinder. The report is displayed in PDF format, and can easily be viewed or printed.

- 1) In the **Cylinder List** or the **Lock Chart**, right-click the cylinder line.
- 2) Click **View access report**.
- 3) If the cylinder is double sided, a pop up window asks which cylinders are included in the access report.
Select one or both cylinder sides and click **OK**.
- 4) View or print the access report.

3.5.10 Viewing an Employee or Visitor Access Report

A person's access report lists the keys handed out to the employee or visitor, and which cylinders they can access. The report is displayed in PDF format, and can easily be viewed or printed.

- 1) In the **Person List**, right-click the person.
- 2) Click **View access report**.
- 3) View or print the access report.

3.5.11 Viewing Key and Cylinder Event Logs

For keys and cylinders, events can be displayed on-screen, printed into a PDF file and exported to an Excel file.

- 1) In the context window of the key or cylinder, click **View event logs**.

The **Event Logs** window pops up.

The **Event Logs** window consists of three tabs:

- **Import / Created** shows basic information about the key or the cylinder, as well as information about when it was created or imported.
- **Status change** is a log of status changes, for example when the key was handed out, lost or returned to the system.
- **Access change** shows a log of device access changes.

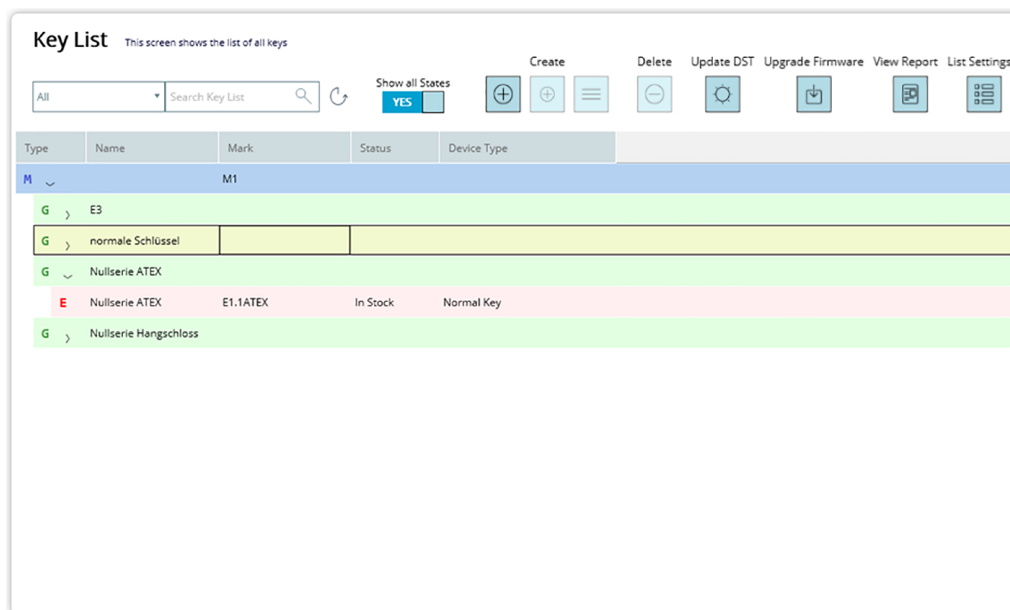
- 2) Optional: The contents in **Status change** and **Access change** can be exported or printed out.

For more information, see Section 2.5.4 *"Creating a View Report"*, page 18.

- 3) Click **CLOSE** to exit.

3.6 Managing Keys

3.6.1 Understanding the Key List



List Items

A maximum of 10,000 keys can be listed in the key list.

The list consists of three different levels:

- Key line level
- Key group level (Electronic keys only)
- Individual key level

The key line and the key group levels can be expanded or folded.

Item Colours

All rows in the list are displayed with various colours and icons.

The colour in the list indicates the types of key and level.

	Selected row
	If the key is inserted in the right slot of the Local PD, the system automatically selects the key and opens the key line or key group to which it belongs.
	Key line
	Key group
	Electronic key
	Mechanical key

Icons

The icons in the list indicate the key type.

M (in key line rows)	Mechanical cutting
G	Key Group
M	Mechanical Keys, see Section 5.1.2.1 “ <i>Key Types</i> ”, page 93 for more information.
E	Electronic Keys, see Section 5.1.2.1 “ <i>Key Types</i> ”, page 93 for more information.

Buttons

- The **Show all States** toggle button

The **Key List** displays all keys in the system, their current status, and other useful information. Broken and lost keys can be excluded from the list by setting the **Show all States** toggle button to **NO**.
- The **Create** buttons

For more information, see Section 3.6.2 “*Creating Mechanical Keys*”, page 37.
- The **Delete** button

For more information, see Section 3.7.8 “*Deleting Cylinders or Cylinder Groups*”, page 50.
- The **Update DST** button

For more information, see Section 3.6.3.3 “*Setting DST on Quartz Keys and Dynamic Keys*”, page 43.
- The **Upgrade Firmware** button

For more information, see Section 3.14.1 “*Upgrading an Electronic Key's Firmware*”, page 67.
- The **View Report** button

For more information, see Section 2.5.4 “*Creating a View Report*”, page 18.
- The **List Settings** button

For more information, see Section 2.5.3 “*Customising List View*”, page 17.

3.6.2 Managing Mechanical Keys

This section describes how to create Mechanical Keys in the system.

First, it is necessary to create a key line to which Mechanical Keys can be assigned. The process for creating single or multiple Mechanical Keys is explained in the latter part of this section.

3.6.2.1 Creating a Key Line

In order to create Mechanical Keys, it is necessary to first create a key line to which one or more Mechanical Keys can be assigned.

- 1) In the **Key List** page, click the bigger + under **Create** from the **top menu**.

The **Create Key Line** window is opened.

- 2) Enter the following information:
 - **Name** (optional): Name for the key.
 - **Mark** (optional): Marking for the key.
 - **Alt. Mark** (optional): Alternate marking for the key.
 - **Notes** (optional)
- 3) Click **OK**.
- 4) Read the message in the **Information** window and click **OK**.

The key line is added in the **Key List**.

Proceed to the steps in Section 3.6.2.3 *“Creating a Mechanical Key”*, page 39 or Section 3.6.2.4 *“Creating Multiple Mechanical Keys”*, page 39 to complete the key creation process.

3.6.2.2 Viewing and Editing Key Line Information

- 1) In the **Key List**, right-click the key line.
The context window is opened.
- 2) Click **Info Card**.
The information card for the selected key line is opened.



HINT!

Double clicking on the key line performs the same action.

- 3) View or edit the **Information Card**.

The **Information Card** consists of two tabs:

- The **General Information** tab shows the following basic information for the key line:
 - **Name:** The key line’s name.
 - **Mark:** The key line’s marking.
 - **Alt. Mark:** The key line’s alternate marking.
 - **Quantity:** Number of Mechanical Keys belonging to the key line.
 - **Notes:** General notes about the key line.
- The **Mechanical Keys** tab shows a list of the Mechanical Keys belonging to the key line.

The **List Settings** button has the same function as in the key list.

- 4) Click **OK** to save changes and close the card.

3.6.2.3 Creating a Mechanical Key


Make sure that at least one key line has been created. To create a key line, see Section 3.6.2.1 *“Creating a Key Line”*, page 37.

- 1) In the **Key List**, select the key line to which the new key will be assigned.
- 2) From the **top menu**, click the smaller + under **Create**.
The **Create Mechanical Key** window is opened.
- 3) Enter the following information:
 - **Key Line:** The key line to which the Mechanical Key will be assigned. The key line highlighted in the key list is selected by default. Use the drop down list to choose another key line if required.
 - **Name** (optional): The key's name.
 - **Mark** (optional): The key's marking.
 - **Alt. Mark** (optional): The key's alternate marking.
 - **Notes** (optional): General notes about the key.
- 4) Click **OK**.
- 5) Read the message in the **Information** window and click **OK**.

A Mechanical Key is added in the **Key List** under the selected key line.

3.6.2.4 Creating Multiple Mechanical Keys

Make sure that at least one key line has been created already. To create a key line, see Section 3.6.2.1 *“Creating a Key Line”*, page 37.

- 1) In the **Key List**, select a key line by clicking.
 - 2) From the **top menu**, click .
- The **Create Multiple Mechanical Key** window is opened.

3) Enter the following information:

- **Key Line:** The key line to which the Mechanical Keys will be assigned. The key line highlighted in the key list is selected by default. Use the drop down list to choose another key line if required.
- **Quantity:** Number of Mechanical Keys to be created.
- **Start Value:** First number that will accompany the name for the new keys.
- **Increment:** Incremental jumps of the number that will accompany the name for the new keys.
- **Default Name** (optional): Name for the new keys. If this field is left blank, the start and increment values will be ignored.

4) Click **OK**.

5) Read the message in the **Information** window and click **OK**.

Mechanical Keys are added in the **Key List** under the selected key line.

3.6.2.5 Viewing and Editing Mechanical Key Information

1) In the **Key List**, right-click the Mechanical Key.

The context window is opened.

2) Click **Info Card**.

The information card for the selected Mechanical Key is opened.



HINT!

Double clicking on the Mechanical Key in the list performs the same action.

3) View or edit the **Information Card**.

The **Information Card** consists of three tabs:

- The **General Information** tab shows the following basic information for the Mechanical Key:
 - **Key Line:** The key line to which the Mechanical Key is assigned.
 - **Name:** Name of the Mechanical Key.
 - **Mark:** Marking of the Mechanical Key.
 - **Alt. Mark:** Alternate marking of the Mechanical Key.
 - **Key Holder Name:** Name of the person to whom the key is handed out. If this field is blank, the key is not handed out.
 - **Handed out date time:** Date and time of hand out. If this field is blank, the key is not handed out.

- **Handed in date time:** Date and time of hand in. If this field is blank, the key is not handed in.
- The **Additional Information** tab shows additional information about the key.
- The **Access** tab shows a list of cylinders to which the key group has access.

The **List Settings** button has the same function as in the key list.

The **View Report** button opens a PDF viewer with an access report.

- 4) Click **OK** to save changes and close the card.

3.6.2.6 Deleting Key Lines or Mechanical Keys

- 1) In the **Key List**, select a key line or a Mechanical Key to be deleted.



NOTE!

It is not possible to delete a key line that contains keys. Delete all keys in the group in order to delete the group from the system.

- 2) From the **top menu**, click the **Delete** icon.
- 3) In the **Question** window, click **YES**.
- 4) Read the message in the **Information** window and click **OK**.

3.6.3 Managing Electronic Keys

3.6.3.1 Viewing and Editing Electronic Key Information

- 1) In the **Key List**, right-click the Electronic Key.
The context window is opened.
- 2) Click **Info Card**.
The information card for the selected Electronic Key is opened.



HINT!

Double clicking on the Electronic Key in the list performs the same action.

- 3) View or edit the **Information Card**.

The **Information Card** consists of several tabs:

- The **General Information** tab shows the following basic information for the Electronic Key:
 - **Name:** Name of the Electronic Key.
 - **Mark:** Marking of the Electronic Key.

- **Alt. Mark:** Alternate marking of the Electronic Key.



NOTE!

Editing of the **Alt. Mark** field must be enabled in **Settings**. For more details, see Section 4.1.17 “*Enabling and Disabling Alternative Marking Edit*”, page 77.

- **Key Holder Name:** Name of the person to whom the key is handed out. If this field is blank, the key is not handed out.
- **Hand out date time:** Date and time of hand out. If this field is blank, the key is not handed out.
- **Hand in date time:** Date and time of hand in. If this field is blank, the key is not handed in.
- **Firmware Version:** Firmware version of the key.
- **ASIC Version:** ASIC version of the key.
- **Article Number:** Article number of the key.
- **Device Type:** Type of Electronic Key.
- The **Additional Information** tab contains information on DST time, **Dynamic Key Capacity** and **Battery Status**.
- The **Access** tab shows a list of the cylinders to which the Electronic Key has access.
 - The **List Settings** button has the same function as in the key list.
 - The **View Report** button opens a PDF viewer with an access report.
- The **Notes** tab contains additional notes for the selected key.
- The **Status history** tab shows the history of changes to the key status. This tab is only visible if there are status changes to display.

- 4) Click **OK** to save changes and close the card.

3.6.3.2 Viewing and Editing Key Group Information

- 1) In the **Key List**, right-click the key group.
The context window is opened.
- 2) Click **Info Card**.
The information card for the selected key group is opened.



HINT!

Double clicking on the key group in the list performs the same action.

3) View or edit the **Information Card**.

The **Information Card** consists of three tabs:

- The **General Information** tab shows the following basic information for the key group:
 - **Name:** The key group's name.
 - **Quantity:** Number of electronic keys assigned to the key group.
 - **Notes:** General notes about the key group.
- The **Electronic Keys** tab shows a list of the electronic keys assigned to the key group.

The **List Settings** button has the same function as in the key list.

- The **Access** tab shows a list of cylinders to which the key group has access.

The **List Settings** button has the same function as in the key list.

4) Click **OK** to save changes and close the card.

3.6.3.3 Setting DST on Quartz Keys and Dynamic Keys

CLM can update the Daylight Saving Time (DST) setting of Quartz Keys and Dynamic Keys.

1) In the **Key List** page, click **Update DST** from the **top menu**.

The **Update DST** window is displayed.

2) Set the following DST information:

- **Enable DST:** Checking or unchecking will enable or disable DST configuration.
- **Summer Time:** Set the start date for summer time.
- **Winter Time:** Set the start date for winter time.

3) Insert a user key into the right slot of the PD.

4) Remove the user key from the PD when the **Remove User Key** message is displayed.

5) Repeat [Step 3](#) and [Step 4](#) to set the remaining user keys.

6) Click **CLOSE** to exit.

3.6.3.4 Synchronising an Electronic Key to the System Time

1) Insert an Electronic Key into the right slot of the Local PD.

2) In the **Key List**, right-click the Electronic Key to synchronise it with the system time.
The context window is opened.

3) Click **Sync System Time**.

The **Sync System Time** window pops up and shows both **Current Key Time** and **Current PC Time**.

- 4) Click **SYNC**.

3.6.3.5 Checking the Electronic Keys Battery Level

- 1) Insert the Electronic Key to be checked in the right slot of the Local PD.
- 2) In the **Key List**, right-click the Electronic Key.
The context window is opened.
- 3) Click **Info Card**.

The information card for the selected Electronic Key is opened.



HINT!

Double clicking on the Electronic Key in the list performs the same action.

- 4) In the **Additional Information** tab, click the **SHOW STATUS** button under **Battery Status**.

The battery status is displayed.

3.7 Managing Cylinders

3.7.1 Understanding the Cylinder List

Cylinder List This screen shows the list of all cylinders

All Search Cylinder List

Type	Name	Mark	Status
E M	TEST SoBez seitlich	MARK163	In Stock
E		163	In Stock
E		164	In Stock
M	WZ MTL	165	In Stock
M	WZ MTL (storniert, geht n	166	In Stock
E	Nullserie NC31	167	In Stock
M	Nullserie NC31	168	In Stock
E	Nullserie N098	169	In Stock
M	Nullserie N098	170	In Stock
G	Cylinder group 1		
M	Nullserie N534, VAR=FS	171	In Stock
E	Nullserie N534, VAR=FS	172	In Stock
E	Nullserie N098	NULLSERI	In Stock
E	N1	NEW 1	In Stock
E E	N2	NEW 2	In Stock

List Items

A maximum of 10,000 cylinders can be listed in the cylinder list.

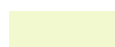
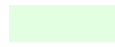
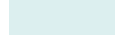
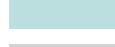

The list consists of two different levels:

- Cylinder group level. See Section 5.1.3.2 *“Cylinder Groups”*, page 96 for more information about the cylinder group.
- Individual cylinder level

Cylinder groups can be expanded to show their content.

Item Colours

In the list, items are displayed with various colours. The colour in the list indicates the type of row.

	Selected row
	Cylinder group
	Grouped cylinder
	Ungrouped cylinder
	Cylinder to which the C-Key which is currently logged in does not have access

Icons

The icons in the list indicate the cylinder type.

G	Cylinder Group
M	Mechanical cylinder, see Section 5.1.3.1 <i>“Cylinders”</i> , page 96 for more information.
E	Electronic cylinder, see Section 5.1.3.1 <i>“Cylinders”</i> , page 96 for more information.
EM	Double-sided cylinder (This example: Electronic A-side and Mechanical B-side)

Buttons

- The **Show all States** toggle button



The **Cylinder List** displays all cylinders in the system, and other useful information. Broken and lost cylinders and cylinders which are not installed can be excluded from the list by setting the **Show all States** toggle button to **NO**.
- The **Create** buttons

For more information, see Section 3.7.5 *“Creating a Cylinder Group”*, page 49, Section 3.7.2 *“Creating a Mechanical Cylinder”*, page 46 and Section 3.7.3 *“Creating Multiple Mechanical Cylinders”*, page 47.
- The **Delete** button

For more information, see Section 3.7.8 *“Deleting Cylinders or Cylinder Groups”*, page 50.
- The **View Report** button

For more information, see Section 2.5.4 *“Creating a View Report”*, page 18.
- The **List Settings** button

For more information, see Section 2.5.3 “*Customising List View*”, page 17.


- The **Upgrade Firmware** buttons
 -  creates a job to upgrade the cylinder firmware, see Section 3.14.2 “*Upgrading an Electronic Cylinder Firmware*”, page 68.
 -  shows the status of cylinder firmware upgrading jobs, see Section 3.14.3 “*Viewing the Status of Cylinder Firmware Upgrade*”, page 68.

3.7.2 Creating a Mechanical Cylinder

- 1) In the **Cylinder List**, click the smaller + under **Create** from the **top menu**.
The **Create Cylinder** window is opened.
- 2) Enter the following information:
 - **Cylinder Group**: Cylinder groups to which the new cylinder can be assigned.
Select **Not grouped** if the cylinder is not assigned to a group.
 - **Type**
 - **M**: Single-sided mechanical cylinder
 - **MM**: Double-sided mechanical cylinder
 - **Name** (optional): Name of the new cylinder.
 - **Second Name** (optional): Second name of the new cylinder.
 - **Mark** (optional): Marking of the new cylinder.
 - **Alt. Mark** (optional): Alternate marking of the new cylinder.
 - **Color** (optional): Colour of the new cylinder.
 - **Length A (mm)**: Length of the A side of the cylinder. If the cylinder is single-sided, enter the value in this field.
 - **Length B (mm)**: Length of the B side of the cylinder. This field is hidden if the cylinder type is single-sided.
 - **Article Number** (optional): The article number of the new cylinder. Enter free text.
- 3) Click **OK**.
- 4) Read the message in the **Information** window and click **OK**.

The new cylinder is added to the **Cylinder List**.

3.7.3 Creating Multiple Mechanical Cylinders

- 1) In the **Cylinder List**, click  from the **top menu**.
The **Create Multiple Cylinders** window is opened.
- 2) Enter the following information:
 - **Cylinder Group:** The cylinder groups to which the new cylinders can be assigned.

Select **Not grouped** if the cylinders are not assigned to a group.
 - **Type**
 - **M:** Single-sided mechanical cylinder
 - **MM:** Double-sided mechanical cylinder
 - **Quantity:** Number of cylinders to be created.

Max. Quantity (not editable) indicates the maximum number of cylinders that can be created.
 - **Start Value:** First number that will accompany the name for the new cylinders.
 - **Increment:** Incremental jumps of the number that will accompany the name for the new cylinders.
 - **Default Name** (optional): Name for the new cylinders. If this field is left blank, the start and increment values will be ignored.
- 3) Click **OK**.
- 4) Read the message in the **Information** window and click **OK**.

The cylinders are added to the **Cylinder List**.

3.7.4 Viewing and Editing Cylinder Information


- 1) In the **Cylinder List**, right-click the cylinder.
The context window is opened.
- 2) Click **Info Card**.
The information card for the selected cylinder is opened.



HINT!

Double clicking on the cylinder in the list performs the same action.

- 3) View or edit the **Information Card**.
The **Information Card** consists of three tabs:

- The **General Information** tab shows the following basic information for the cylinder:
 - **Cylinder Group:** Cylinder groups to which the new cylinder can be assigned.
 - **Name:** Name of the cylinder.
 - **Second Name:** Second name of the cylinder.
 - **Status**
 - **In Stock:** The cylinder is in stock.
 - **Installed:** The cylinder is installed in a lock.
 - **Length A (mm):** Length of the A side of the cylinder. If the cylinder is single-sided, enter the value in this field.
 - **Length B (mm):** Length of the B side of the cylinder. This field is hidden if the cylinder type is single-sided.
 - **Mark:** Cylinder marking.
 - **Alt. Mark:** Alternate marking of the cylinder. It is an internal code set by ASSA ABLOY in default.
-  **NOTE!**
Editing of the **Alt. Mark** field must be enabled in **Settings**. For more details, see Section 4.1.17 *“Enabling and Disabling Alternative Marking Edit”*, page 77.
- **Color** (optional): Cylinder colour.
 - **Type** (optional): Cylinder type.
 - **ASIC Version** (optional): ASIC version of the cylinder. Hidden for mechanical cylinders.
 - **Article Number** (Optional): For imported cylinders, this is an internal code set by ASSA ABLOY, and it is not editable. For mechanical cylinders, enter free text.
 - **Firmware Version A:** Firmware version of the A side of the cylinder. Hidden for mechanical cylinders.
 - **Firmware Version B:** Firmware version of the B side of the cylinder. Hidden for mechanical cylinders and single-sided electronic cylinders.
- The **Additional Information** tab shows additional information about the cylinder.
 - The **Key Access** tab shows a list of keys which have access to the cylinder.
- The **List Settings** button has the same function as in the key list.

The **View Report** button opens a PDF document with a report of the accesses.

- 4) Click **OK** to save changes and close the card.

3.7.5 Creating a Cylinder Group

- 1) In the **Cylinder List**, click the bigger + under **Create** from the **top menu**.
The **Create Cylinder Group** window is opened.
- 2) Optional: Enter a name for the cylinder group in the **Name** field.
- 3) The **Ungrouped Cylinders** list shows cylinders that do not belong to other cylinder groups.
Select cylinders for the new group from the list.
- 4) Click **OK**.
- 5) Read the message in the **Information** window and click **OK**.

The cylinder group is added to the **Cylinder List**.

3.7.6 Viewing and Editing Cylinder Group Information

- 1) In the **Cylinder List**, right-click the cylinder group.
The context window is opened.
- 2) Click **Info Card**.
The information card for the selected cylinder group is opened.



HINT!

Double clicking on the cylinder group in the list performs the same action.

- 3) View or edit the **Information Card**.
The **Information Card** consists of two tabs:
 - The **General Information** tab contains the same information as the **Create Cylinder Group** window. See Section 3.7.5 *“Creating a Cylinder Group”*, page 49 for more information of the contents in the window.
 - The **Additional Information** tab shows additional information about the cylinder group.
- 4) Click **OK** to save changes and close the card.

3.7.7 Restructuring a Cylinder Group

It is possible to change the composition of cylinders in a cylinder group.

- 1) In the **Cylinder List**, right-click the cylinder group to restructure.
The context window is opened.

- 2) Click **Info Card**.

The information card for the selected cylinder group is opened.



HINT!

Double clicking on the cylinder group in the list performs the same action.

- 3) The **General Information** tab displays all available cylinders in the system. Cylinders which already belong to the group are selected in the **Checked** column. Select or deselect the cylinders for the group.
- 4) Click **OK** to save changes and close the card.

3.7.8 Deleting Cylinders or Cylinder Groups

Cylinders or cylinder groups which have been added manually can be deleted from the system.

- 1) In the **Cylinder List**, select the cylinder or the cylinder group to be deleted.
To select multiple cylinders or cylinder groups, hold down the Shift key while selecting rows.



NOTE!

It is not possible to delete a cylinder group that contains cylinders. Delete all cylinders in the group in order to delete the group from the system.

- 2) From the top menu, click **Delete Selected Cylinder** icon.
- 3) In the **Question** window, click **YES** to confirm the action.
- 4) Read the message in the **Information** window and click **OK**.

3.8 Managing Employees and Visitors




The person list shows the **Employees** and **Visitors** currently in the system. It contains functions to add, remove, edit, and search for people. Keys can only be handed out to people in the list, but not everyone in the list is necessarily a keyholder.

To facilitate system security, there are two types of people. Employees are created for recurring and permanent keyholders, whereas visitors are created on a temporary basis.

3.8.1 Understanding the Person List

Item Colours

In the list, employees and visitors are displayed with different colours. The colour in the list indicates the type of row.

	Employee
	Visitor
	Selected line

Buttons

- The **Show all States** toggle button

The **Person List** displays all employees and visitors in the system, and other useful information. Deactivated employees and visitors can be excluded from the list by setting the **Show all States** toggle button to **NO**.
- The **Create** buttons

For more information, see Section 3.8.2 *“Creating an Employee or Visitor”*, page 52.
- The **Delete** button

For more information, see Section 3.8.5 *“Deleting an Employee or Visitor”*, page 53.
- The **View Report** button

For more information, see Section 2.5.4 *“Creating a View Report”*, page 18.
- The **List Settings** button

For more information, see Section 2.5.3 *“Customising List View”*, page 17.
- The **Import** button

For more information, see Section 3.8.6 *“Adding Persons to the Person List using a CSV File”*, page 53.
- The **Export Template** button

For more information, see Section 3.8.6 *“Adding Persons to the Person List using a CSV File”*, page 53.



HINT!

By adding the **Handed out key marking** column, the Person List shows who is possessing which keys. See Section 2.5.3 *“Customising List View”*, page 17 for more information about how to add a new column.

3.8.2 Creating an Employee or Visitor

- 1) Navigate to the **Person List**.
- 2) Create a person:
 - To create an employee, click the large + icon under **Create**.
 - To create a visitor, click the small + icon under **Create**.
- 3) The following fields under the **General Information** tab are mandatory:
 - **Number**
The employee number. If this field is left blank, the system will auto-generate a number.
 - **Title**
Enter free text or choose from the drop-down list.
 - **First Name**
 - **Last Name**
 - **Suffix**
Enter free text or choose from the drop-down list.
 - **Creation Date and Time**
Default is the current date and time. The set value does not influence the handing out process nor the key's validity.
 - **Start Date and Time** (Visitor only)
Default is the current date and time. The set value does not influence the handing out process nor the key's validity.
 - **Valid Until Date and Time** (Employee only) or **End Date and Time** (Visitor only)
The value chosen affects notification of an overdue key, but does not affect the key's validity.

The remaining fields in the **General** tab and all fields in **Address, Contact Information** and **Additional Information** are optional.

- 4) Click **OK** to save.

3.8.3 Viewing and Editing Employee or Visitor Information

The data entered when creating an employee or visitor can be displayed and edited in the **Information Card**. The **Keys In Possession** tab also lists the keys that are currently handed out to the selected person.

- 1) In the **Person List**, right-click the person.

The context window is opened.

- 2) Click **Info Card**.

The information card for the selected person is opened.



HINT!

Double clicking on the person in the list performs the same action.

- 3) View or edit the information.
- 4) Click **OK** to save any changes made.

3.8.4 Activating and Deactivating Persons

Keys cannot be handed out to inactive persons, but any keys they hold are still valid until successfully blocked or reported missing.

To activate or deactivate a person:

- 1) In the **Person List**, right-click the person.
- 2) In the context window, click **Switch Active/Inactive**.

Inactive persons appear red in the **Person List**.

3.8.5 Deleting an Employee or Visitor

- 1) From the **Person List**, select a person.
- 2) Click **Delete**.
Supervisors cannot be deleted.
- 3) Click **OK**.

3.8.6 Adding Persons to the Person List using a CSV File

To simplify administration of multiple people, CLM offers batch CSV import and export of person lists. CSV files can be edited in Microsoft Excel.

- 1) To create a CSV file template with required fields to import into the person list, click **Export Template** in the **Person List**.
- 2) Open the downloaded template and fill in the required fields.

Following fields are mandatory:

- **FirstName** (maximum 50 characters)
- **LastName** (maximum 50 characters)

For more details about how to fill the other fields in the CSV file, see Section 6.3 "[CSV File Structure](#)", page 106.

Other fields can be filled in the person's **Info Card** after adding to the list.

- 3) Save the file as CSV format.



NOTE!

The Excel program changes the file format when saving, and makes the file unusable.

To avoid this, click the **Save** button to save the file, then select **No** or **Cancel** in the following pop-up dialogues:

- whether to keep the same format
- whether to save the file in a folder
- whether to save changes in closing the program

- 4) Click **Import Persons** in the **Person List** page to import the CSV file into the **Person List**.
- 5) Select the CSV file to import from the file explorer and click **Open**.
The **Question** window pops up.
- 6) Click **OK** to proceed.
- 7) If the **Number** value conflicts with an existing number, the pop-up window asks what to do with the duplicated number. Select the appropriate choice and click **OK**.
The **Import Persons Result** window pops up.
- 8) Click **CLOSE** to complete the process.



HINT!

In case of failure to import due to special characters or other formatting, try to import and save the file using a file editor and UTF-8 coding.

3.9 Handling Audit Trails

3.9.1 Enabling and Disabling Key or Cylinder Audit Trails

The actions performed with a Quartz Key, Dynamic Key or electronic cylinder are recorded in the key or cylinder as audit trails. This function can be enabled or disabled as follows.

- 1) • To enable or disable the key audit trails,
In the **Key List**, right-click the key.
- To enable or disable the cylinder audit trails,
In the **Cylinder List**, right-click the cylinder.

The context window is opened.

- 2) Click **Switch ON/OFF Audit Trail**.
The **Switch ON/OFF Audit Trail** window pops up.
- 3) Check or uncheck the box next to the text **Enable Audit Trail**.
If the cylinder is double-sided, check or uncheck the each cylinder.
- 4) Click **OK**.
- 5) Read the message in the **Information** window and click **OK**.
In case of enabling or disabling the cylinder audit trails, a cylinder job is created in the job list.
- 6) **Enabling or Disabling Cylinder Audit Trails only:**
Program the cylinder using a C-Key. For more information, see Section 3.13.1 *"Programming Cylinders"*, page 65.

3.9.2 Viewing Key Audit Trail Reports

The key audit trail report shows the list of actions performed with a Quarts or Dynamic Key.

Prerequisite:

The Quarts or Dynamic Key has been read via the Local PD. See Section 3.9.3 *"Reading Audit Trails from Keys"*, page 55 for more information about how to read audit trails from the Quarts or Dynamic Key.

- 1) In the **Key List**, right-click the the Quarts or Dynamic Key.
The context window is opened.
- 2) Click **View Audit Trail**.
The key audit trail report from the last audit trail reading is displayed.
- 3) To export the list, click **View Report** and follow the instructions in Section 2.5.4 *"Creating a View Report"*, page 18.

3.9.3 Reading Audit Trails from Keys

Actions performed with Quartz Keys and Dynamic Keys can be read via the Local PD and stored in the system.

- 1) In the **Key List**, right-click the key to read the audit trails.

The context window is opened.

- 2) Click **Read Audit Trail**.
- 3) Enter the system PIN in the pop up window and click **OK**.
- 4) If the system requires the approver, follow the steps below. Otherwise, proceed to [Step 6](#).
 - a) Insert the approver C-Key in the right slot of the Local PD, and click **OK**.
 - b) Enter the approver PIN and click **OK**.
 - c) Replace the approver C-Key with the key to read in the right slot of the Local PD, and click **OK**.
- 5) If the key is not in the Local PD, the information window pops up and informs that an electronic key job is created and stored in the Job List to be executed either in a Wall PD or the Local PD.

Click **OK** to continue.

- 6) Select events to include in the audit trail report from the **Select an option** window.
 - **Complete Audit Trail:** Full audit trail for the key.
 - **Last # Audit Events:** The last specified number of events performed with the key.
 - **Between Dates:** Events performed within the specified time frame.
- 7) Click **OK**.
 - If the key is in the Local PD the system starts reading the specified events for the key.

After the audit trail is successfully read, the audit trail report is automatically opened.
 - If the key is not in the Local PD, an electronic key job is created and stored in the Job List to be executed either in a Wall PD or the Local PD.

For executing key jobs from the Job List, see Section 3.12 [“Programming an Electronic Key”](#), page 64.

3.9.4 Viewing Cylinder Audit Trail Reports

The cylinder audit trail report shows the list of actions performed at the cylinder.

Prerequisite:

The cylinder has been read into the C-Key, and data was transferred to the system. See Section 3.9.5 [“Reading Audit Trails from Cylinders”](#), page 57 for more information about how to read audit trails from the cylinder.

- 1) In the **Cylinder List**, right-click the cylinder.

The context window is opened.

- 2) Click **View audit trail**.
The cylinder audit trail report from the last audit trail reading is displayed.
- 3) To export the list, click **Export to Excel** or **Export to PDF**.

3.9.5 Reading Audit Trails from Cylinders

Actions performed by the cylinder are collected with a C-Key and stored in the system.

- 1) Insert the C-Key in the Local PD.
- 2) In the **Cylinder List**, right-click the cylinder.
The context window is opened.
- 3) Click **Read Audit Trail**.
- 4) Enter the system PIN in the pop up window and click **OK**.
- 5) If the system requires the approver, follow the steps below. Otherwise, proceed to [Step 6](#).
 - a) Insert the approver C-Key into the right slot of the Local PD, and click **OK**.
 - b) Enter the approver PIN and click **OK**.
- 6) If both sides of the cylinder are electronic, select which side of audit trails should be read.
The **Select an option** window is displayed.
- 7) Select events to include in the audit trail report.
 - **Complete Audit Trail:** Full audit trail for the cylinder.
 - **Last # Audit Events:** The last specified number of events performed with the cylinder.
 - **Between Dates:** Events performed within a specified time frame.
- 8) Click **OK**.
- 9) Read the message in the **Information** window and click **OK**.
The system creates a job to read the audit trails of the cylinder and sends it to the job list.
- 10) Collect the audit trails from the cylinder with the C-Key following the steps below. See Section 3.13.1 ["Programming Cylinders"](#), page 65 for more detailed instruction.
 - a) Send the audit trail job to the C-Key via the Local PD.
 - b) Insert the C-Key into the cylinder and collect audit trails.
 - c) Insert the C-Key into the PD and transfer audit trails to the system.

3.10 Handling Lost and Broken Keys

This section describes how to report lost or broken keys. The procedure is different for different key types.

3.10.1 Reporting Lost or Broken Mechanical Keys

- 1) Specify the lost or broken key in the system.
 - If the lost or broken key can be identified:
 - a) In the **Key List** or **Lock Chart**, right-click the key to be reported as lost or broken.
The context window is opened.
 - b) In the context window, click **Mark as Lost** or **Mark as Broken**.
 - If the person who possesses the lost key can be identified:
 - a) In the **Person List**, right-click the person who possesses the key reported as lost.
The context window is opened.
 - b) In the context window, click **Mark as Lost**.
 - c) If the person possesses more than two keys, the **Select key** window pops up.
Select the lost broken key from the list and click **OK**.

The confirmation window pops up.

- 2) Click **YES** to continue the reporting process.
- 3) If necessary, enter the reason in the next window and click **CONTINUE**.
- 4) Read the message in the **Information** window and click **OK**.

In the **Key List**, the key appears in red and its status is changed to **Lost** or **Broken**.

3.10.2 Reporting Lost Electronic Keys

This section describes how to report lost Electronic Keys. After completing this process:

- The key is registered as lost in the system.
 - Optional: A replacement key is created.
 - A new cylinder job is created to block the lost key.
- 1) Specify the lost key in the system.
 - If the lost key can be identified:

- a) In the **Key List** or **Lock Chart**, right-click the key to be reported as lost.
The context window is opened.
- b) In the context window, click **Mark as Lost**.
- If the person who possesses the lost key can be identified:
 - a) In the **Person List**, right-click the person who possesses the key reported as lost.
The context window is opened.
 - b) In the context window, click **Mark as Lost**.
 - c) If the person possesses more than two keys, the **Select key** window pops up.
Select the lost key from the list and click **OK**.

The confirmation window pops up.

- 2) Click **YES** to continue the reporting process.
The next pop-up window asks whether to create a replacement key.
- 3) • If it is not necessary to create a replacement key, click **NO** and proceed to *Step 4*.
- If it is necessary to create a replacement key:
 - a) Click **YES**.
The list of available keys is opened.
 - b) Select a replacement key from the **Key List**.
 - c) If the replacement key is physically available, insert it into the right slot of the Local PD.
 - d) Select the following information to be copied to the replacement key, and click **OK**.
 - Accesses (preselected)
 - Validity
 - Schedule

The selected information is copied to the replacement key in the Local PD.
 - e) If the replacement key is not inserted, a message pops up about how to continue.
 - If the replacement key is available, insert it into the right slot of the Local PD and click **YES**.

The selected information is programmed to the key.

- To continue the reporting process without inserting the replacement key, click **NO**.



NOTE!

If the key is not inserted, the following limitations apply.

It is not possible to copy validity and schedule to the replacement key. In such a case, set the validity and the schedule later following the instruction in Section 3.5.3 *"Setting Key Validity"*, page 30 or Section 3.5.5 *"Setting Key Schedule"*, page 31.

In case of Dynamic Keys, the key access list is separately saved in the **Job List** as a key job. The accesses are automatically copied to the key when the key is inserted into the right slot of the PD.

- To abort the reporting process, click **CANCEL**.

- 4) In the text fields, enter the reason if necessary and click **CONTINUE**.

The list of cylinders to which the lost key has access is opened.

- 5) From the list, select cylinders which need to be programmed to block the lost key and click **OK**.



NOTE!

The choice of affected cylinders can be changed after this reporting process. The cylinders which are not selected in this step do not block the lost key. It is only possible to block the lost key manually in the lock chart.

- 6) Read the message in the **Information** window and click **OK**.

In the **Key List**, the key appears in red and its status is changed to **Lost**.

The cylinders to which the lost key has access need to be updated. To update the cylinders, see Section 3.13.2 *"Reprogramming Cylinders"*, page 66.

3.10.3 Reporting Broken Electronic Keys

This section describes how to report broken Electronic Keys. After completing this process:

- The key is registered as broken in the system.
- Optional: A replacement key is created.

- 1) In the **Key List** or **Lock Chart**, right-click the key to be reported as broken.

The context window is opened.

- 2) In the context window, click **Mark as Broken**.

The confirmation window pops up.

- 3) Click **YES** to continue the reporting process.

The next pop-up window asks whether to create a replacement key.

- 4) • If it is not necessary to create a replacement key, click **NO** and proceed to *Step 4*.

- If it is necessary to create a replacement key:

- a) Click **YES**.

The list of available keys is opened.

- b) Select a replacement key from the **Key List**.

- c) If the replacement key is physically available, insert it into the right slot of the Local PD.

- d) Select the following information to be copied to the replacement key, and click **OK**.

- Accesses (preselected)
- Validity
- Schedule

The selected information is copied to the replacement key in the Local PD.

- e) If the replacement key is not inserted, a message pops up about how to continue.

- If the replacement key is available, insert it into the right slot of the Local PD and click **YES**.

The selected information is programmed to the key.

- To continue the reporting process without inserting the replacement key, click **NO**.



NOTE!

If the key is not inserted, the following limitations apply.

It is not possible to copy validity and schedule to the replacement key. In such a case, set the validity and the schedule later following the instruction in Section 3.5.3 “*Setting Key Validity*”, page 30 or Section 3.5.5 “*Setting Key Schedule*”, page 31.

In case of Dynamic Keys, the key access list is separately saved in the **Job List** as a key job. The accesses are automatically copied to the key when the key is inserted into the right slot of the PD.

- To abort the reporting process, click **CANCEL**.

5) In the text field, enter a reason if necessary and click **CONTINUE**.

6) **Handed Out Electronic Keys Only:**

If the broken key had been handed out before it was broken, **Hand In Report** is automatically created.

Check the report, print or save it if necessary, then click **CLOSE** to exit.

7) Read the message in the **Information** window and click **OK**.

In the **Key List**, the key appears in red and its status is changed to **Broken**.

3.10.4 Returning Lost or Broken Keys

When lost keys are found or broken keys are fixed, they must be returned to the system in order to manage them in CLM.

Prerequisite:

The key has been reported as lost or broken to the system. Lost or broken keys are displayed in red in the **Key List**.

1) **Electronic Keys Only**

If available, insert the key to return into the right slot of the Local PD.

2) In the **Key List**, right-click the key to return.

The context window is opened.

3) Click **Return to System**.

The confirmation window pops up.

4) Click **YES** to continue the returning process.

5) **Electronic Keys Only**

- If the key to return is not inserted in the Local PD, proceed to [Step 5.a](#),
 - If the key in the Local PD had been handed out before lost or broken, proceed to [Step 5.b](#).
 - If the key in the Local PD had not been handed out before lost or broken, proceed to [Step 6](#).
- a) If the key to return is not inserted in the Local PD, a message pops up about how to continue.
- To set the key validity **Never**, insert the key to return into the right slot of the Local PD and click **YES**.
 - To keep the key validity, click **NO**.

b) **Handed Out Electronic Keys Only:**

If the key had been handed out before it was lost or broken, the **Select the new status** window opens and asks which status the key should have.

Select the preferable choice and click **OK**.



NOTE!

Even though choosing to set the validity **Never** in the previous step, the validity and the schedule settings are used after choosing to keep **Handed out** status.

- 6) In the text field, enter a reason if necessary and click **CONTINUE**.
- 7) **Handed Out Electronic Keys Only:**
- If the key had been handed out before it was lost or broken, in the following cases, the **Hand In report** or **Hand Out report** is automatically generated.
- **Hand In report:** when **Set key as In Stock** is selected in returning the lost key in [Step 5.b](#).
 - **Hand Out report:** when **Keep handed out to the previous person** is selected in returning the broken key in [Step 5.b](#).

Check the report, print or save it if necessary, then click **CLOSE** to exit.

- 8) Read the message in the **Information** window and click **OK**.

3.11 Handling Lost and Broken Cylinders

3.11.1 Reporting Lost or Broken Cylinders

This section describes how to report lost or broken cylinders.

- 1) In the **Cylinder List**, right-click the cylinder to be reported as lost or broken. The context window is opened.

- 2) Click **Mark as Lost** or **Mark as Broken**.
- 3) In the **Question** window, click **YES** to confirm the action.
 - If the cylinder type is electronic and there are planned jobs for this cylinder, a second **Question** window asks whether to delete these jobs or not.
Select **YES** or **NO** as appropriate. Selecting **CANCEL** exits the reporting process.
- 4) If necessary, enter the reason in the next window and click **OK**.
- 5) Read the message in the **Information** window and click **OK**.

In the **Cylinder List**, the cylinder appears in red and its status is changed to **Lost** or **Broken**.

3.11.2 Returning Lost or Broken Cylinders

When lost cylinders are found or broken cylinders are repaired, the cylinders must be returned to the system in order to manage them in CLM.

Prerequisite:

The cylinder has been reported as lost or broken to the system. Lost or broken cylinders are displayed in red in the **Cylinder List**.

- 1) In the **Cylinder List**, right-click the cylinder to be returned to the system.
The context window is opened.
- 2) Click **Return to System**.
- 3) In the **Question** window, click **YES** to confirm the action.
- 4) If necessary, enter the reason in the next window and click **OK**.
- 5) Read the message in the **Information** window and click **OK**.

In the **Cylinder List**, the cylinder status is changed to **In Stock**.

3.12 Programming an Electronic Key

3.12.1 Programming an Electronic Key in the Local PD

- 1) In the **Lock Chart**, click **Job List**.
- 2) Insert the electronic key to be programmed in the the right slot of the Local PD.
If automatic programming is enabled, the system starts programming the key automatically.
- 3) If automatic programming is disabled, click the **Apply Changes** button on the **Lock Chart**.



NOTE!

Automatic programming can be set in the system settings. See Section 4.1.18 *“Enabling and Disabling Automatic Dynamic Key Programming”*, page 78.

3.12.2 Programming an Electronic Key in a Wall PD

The key jobs to be executed in a Wall PD are sent to the controller but it is still possible to execute them in the Local PD.

The controller holds the key jobs and automatically removes them after they are executed either in the Local PD or a Wall PD.

Prerequisite:

- The locking system has a remote license.

- 1) In the **Lock Chart**, click **Job List**.
- 2) Make sure that the **Key Jobs** tab is selected.
- 3) Click **Select All**, or manually select the jobs to be sent.
- 4) Click the **Send To Controller** button.

The selected key jobs are sent to the controller to be executed in a Wall PD.

An Information window notifies the user when the jobs are sent to the controller successfully.

- 5) Insert the key into a Wall PD to program.

When the jobs in the controller is executed in the Wall PD, the key jobs are automatically removed from the controller.

- 6) Confirm if the jobs are executed in a Wall PD in the remote task report:

- a) Check if a new notification is available.

For finding the notification, refer to Section 2.5.1 *“Navigating in CLM”*, page 16.

- b) Click **Controller Tasks Completed**.

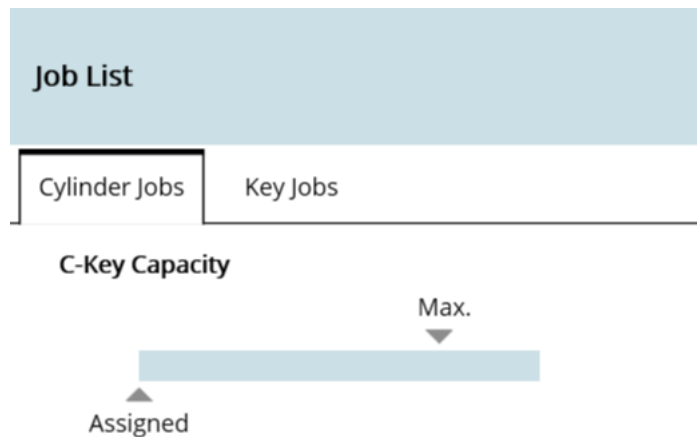
The system shows a report with the result of the jobs, showing the jobs that were executed in a Wall PD.

- c) If required, print the PDF report for reference.

3.13 Programming Cylinders

3.13.1 Programming Cylinders

- 1) In the **Lock Chart**, click **Job List**.
- 2) Make sure that the **Cylinder Jobs** tab is selected.



- 3) Click **Select All**, or manually select which cylinders to program.
A graph at the top of the Cylinder Jobs tab now displays the cylinder job size in relation to the current C-Key's memory capacity.
 - If the graph shows that the C-Key's memory capacity is exceeded, deselect cylinders until the selected jobs are below the maximum.
- 4) Click **Send Jobs**.
When the cylinder jobs are successfully sent to the C-Key, a report of the sent jobs is opened in a PDF viewer.
- 5) If required, print the PDF report for reference.
- 6) Close the PDF viewer with the Esc key.
- 7) Remove the C-Key from the Local PD.
- 8) Insert the C-Key at every cylinder listed in the PDF report.
After cylinders are programmed, go back to the system.
- 9) In the **Cylinder Jobs** tab, click **Receive Jobs**.
This will empty the C-Key and update CLM. A report detailing the success status of the cylinder jobs is displayed.
- 10) Insert the C-Key in the left slot of the Local PD, and enter the PIN.
- 11) To make sure the system is up to date, review the receive jobs report.
- 12) Repeat steps [Step 1](#) to [Step 11](#) for remaining cylinder jobs, if any.



NOTE!

Cylinder jobs can also be divided between several C-Keys by logging in with a different C-Key.

3.13.2 Reprogramming Cylinders

When changing an authorisation on cylinder, the system always compares the authorizations both in the database and the cylinder. If these authorisations do not match,

the cylinder needs to be reprogrammed. In such a case, the system creates a reprogramming job for the cylinder automatically. The reprogramming job can also be created manually.

The cylinder job reprograms the cylinder as it is configured in the lock chart.



NOTE!

This reprogramming process erases the audit trail.

- 1) In the **Lock Chart** or **Cylinder List**, right-click the cylinder.
- 2) In the context window, click **Reprogram**.

A cylinder task in the job list is created in the background.



NOTE!

If there is a reprogramming task for the same cylinder, the **Reprogram** button is greyed out.

- 3) Read the warning message in the information window and click **OK** to continue.
- 4) To physically reprogram the cylinder, follow the instructions in Section 3.13.1 *"Programming Cylinders"*, page 65, ensuring that the cylinder is selected in the job list.

3.14 Upgrading Firmware Files

3.14.1 Upgrading an Electronic Key's Firmware

When the system detects the newer key firmware for the electronic key which is in the PD, the **Upgrade Firmware** button is displayed above the key list.



NOTE!

The buttons are not visible unless an extension file with enriched firmware (ELS+FW) is imported to the system.

- 1) Insert the key to upgrade the firmware into the right slot of the Local PD.
- 2) In the **Key List** page, click the **Upgrade Firmware** button from the **top menu**.
Upgrading process starts automatically.
- 3) When the pop-up window indicates, remove the user key from the Local PD



NOTE!

Do not remove the user key from the Local PD during the upgrading process.

- 4) Insert next user key to the right slot of the Local PD or click **CLOSE** to exit.

3.14.2 Upgrading an Electronic Cylinder Firmware


After the newer firmware for the cylinders is imported, the **Upgrade Firmware** buttons are displayed above the cylinder list.



NOTE!

The buttons are not visible unless an extension file with enriched firmware (ELS+FW) is imported to the system.

- 1) Confirm that C-Key which fulfil the following requirements is in the left slot of the Local PD:
 - the C-Key's firmware is the latest one. To upgrade the C-Key firmware, see Section 3.14.4 *"Upgrading a C-Key's Firmware"*, page 69.
 - the C-Key is not expected to carry other cylinder jobs until the cylinder firmware upgrade task is completed.


- 2) In the **Cylinder List** page, click  from the **top menu**.

The new cylinder job to upgrade cylinders is created and transferred to the C-Key in the left slot of the Local PD.



NOTE!

Once the C-Key is programmed the cylinder firmware, the C-Key becomes the firmware upgrade mode. In this mode, the C-Key is not able to carry or be assigned other tasks until the firmware upgrading task is completed up to [Step 9](#).

- 3) When it is indicated in the pop-up screen, remove the C-Key from the left slot of the Local PD.
- 4) Insert the C-Key into the cylinder to be upgraded its firmware.
- 5) Remove the C-Key from the cylinder when cylinder firmware is upgraded.
- 6) If necessary, repeat [Step 4](#) and [Step 5](#) for other cylinders.
- 7) Insert the C-Key into the left slot of the Local PD.
- 8) In the **Cylinder List** page, click  from the **top menu**.
- 9) Click **Read result**.

The cylinder upgrading status is updated and stored in the system.

The firmware upgrade status can be checked in the status list. To access to the list, see Section 3.14.3 *"Viewing the Status of Cylinder Firmware Upgrade"*, page 68.


3.14.3 Viewing the Status of Cylinder Firmware Upgrade

Once a cylinder firmware upgrading job is created, the upgrading status is shown in the list.



NOTE!

The buttons for cylinder firmware upgrade are not displayed unless the new firmware file is imported to the system which version is 2.0 or later.

- 1) In the **Cylinder List** page, click  from the **top menu**.
The firmware upgrade jobs are listed.
- 2) Double click the row or click **View details** to show more details of a particular job.

3.14.4 Upgrading a C-Key's Firmware

When the system detects the newer firmware for C-Key which is in the left slot of the Local PD, the **Upgrade Firmware** button is displayed above the key list.



NOTE!

The buttons are not visible unless an extension file with enriched firmware (ELS+FW) is imported to the system.

- 1) Confirm that C-Key in the left slot of the Local PD is the one to be upgraded.
- 2) In the **C-Key List** page, click the **Upgrade Firmware** button from the **top menu**.
- 3) Enter the C-Key PIN.
Upgrading process starts automatically.



HINT!

If the button is grayed out, it means that the C-Key does not have to upgrade the firmware.

- 4) When the pop-up window indicates, remove the C-Key from the left slot of the Local PD



NOTE!

Do not remove the C-Key from the Local PD during the process.

- 5) Insert next C-Key to the left slot of the Local PD or click **CLOSE** to exit.

4 Configuring CLM

4.1 General System Settings

The **General** system settings handles reminders, notifications, backups, templates, and other settings for CLM.

4.1.1 Managing Backup Reminders

Backup reminders are used to remind the supervisor to backup the system. Reminders are shown as a bell icon in the upper right corner of the CLM window.

- 1) In **Settings**, click **General**.
- 2) Expand the **Backup Settings** panel.
- 3)
 - To turn on the reminder function:
 - a) Select the check box **Notify backup reminders**.
 - b) Set the day and time to receive the reminder.
 - To turn off the reminder function, deselect the check box **Notify backup reminders**.

If the reminder is set, the notification appears as the bell icon in the upper right corner of the CLM window.

4.1.2 Backing up Locking Systems

A locking system should be backed up at regular intervals. Backup files are not usable outside CLM, but should be treated as confidential assets. It is recommended to store them on another computer or storage media for added safety.

4.1.2.1 Backing up Currently Opened System

- 1) There are two ways to start backup process:
 - From the menu bar, click **SYSTEM**.
 - or
 - From the **Settings**,
 - a) Click **General**.
 - b) Expand **Backup Settings** panel.
- 2) Click **CREATE SYSTEM BACKUP**.
- 3) Select where to store the backup file in the pop-up file explorer.
- 4) Click **Save**.

The backup is stored as an SMB file.

4.1.2.2 Backing up All Systems

If the program holds multiple systems, all system data can be backed up at once.

- 1) From the **Settings**, click **General**.
- 2) Expand **Backup Settings** panel.
- 3) Click **DO FULL DATABASE BACKUP**.
- 4) In the pop-up window, enter the C-Key PIN.
- 5) Select where to store the backup file in the pop-up file explorer.
- 6) Click **Save**.

The backup is stored as an SMB file.

4.1.3 Restoring Locking Systems

- 1) In **Settings**, click **General**.
- 2) Expand **Backup Settings** panel.
- 3)
 - To restore the currently opened system:
Click **RESTORE SYSTEM**.
 - To restore all systems in the program:
 - a) Click **RESTORE FULL DATABASE BACKUP**.
 - b) In the pop-up window, enter the C-Key PIN.
- 4) Select the file to import in the pop-up file explorer.
- 5) Click **Open**.

When the system is successfully restored, **Information** windows pop up and inform the user when the process is completed and when CLM is about to be shut down.

- 6) Click **OK**.

The program is shut down. If required, restart CLM.

4.1.4 Extending the Locking System

When more keys or cylinders are added to a locking system, it must be extended. An extension file (*.els or *.xml) contains all factory-made elements of the locking system, that is existing and re-ordered cylinders, keys and their relationship to one another.

To import an extension file:

- 1) There are two ways to start the extension process:
 - From the menu bar,

- a) Click **SYSTEM**.
 - b) Click **IMPORT EXTENSION FILE**.
- From the **Settings**,
 - a) Click **General**.
 - b) Expand **Backup Settings** panel.
 - c) Click **IMPORT EXTENSION FILE**.
- 2) Enter the C-Key PIN.
- 3) Select the file to import and click **OPEN**.
Question window pops up.
- 4) Confirm the details of the file and click **YES** to start importing.
- 5) Enter the C-Key PIN again.

4.1.5 Importing a Firmware File

When a firmware file is upgraded, the user receives .els file from the dealer via an e-mail.

The .els file is imported by the same process as importing an extension file. For more information, see Section 4.1.4 *"Extending the Locking System"*, page 71.

For upgrading an electronic key firmware, see Section 3.14.1 *"Upgrading an Electronic Key's Firmware"*, page 67.

For upgrading an electronic cylinder firmware, see Section 3.14.2 *"Upgrading an Electronic Cylinder Firmware"*, page 68.

For upgrading a C-Key firmware, see Section 3.14.4 *"Upgrading a C-Key's Firmware"*, page 69.

4.1.6 Editing Company Information

To edit the company information:

- 1) In **Settings**, click **General**.
- 2) Expand the **Company Information** panel.
- 3) Enter the company information.
 - To insert a company logo:
 - a) Click **OPEN**.
 - b) Select the file.
Valid file formats are JPG, BMP and PNG.
 - To clear the company logo, click **CLEAR**.

4.1.7 Setting Default Periods, Date and Time

System management can be simplified by setting a default period of key possession, employee and key validity. Hour format, date format and DST settings can also be set here.

- 1) In **Settings**, click **General**.
- 2) Expand the **Date and Time settings** panel.
 - To set the default hand in period:
Under **Hand in period**, set **Years**, **Months** and **Days** or select **Permanent**.
 - To set the default employee validity period:
Under **Employee validity period**, set **Years**, **Months** and **Days**, or select **Always** to set a new employee's default validity to always valid.
 - To set the default for key validity which is used when handing out an Electronic Key:
Under **Validity**, select **Never** or **Always**. It is also possible to select **Use Schedule** for Dynamic Keys.
 - To enable daylight saving time, select **Use DST Settings**.
 - To set the **Hour format** and **Date format** which are used by the program, select the corresponding options.

4.1.8 Managing Key Schedule Templates

This function enables the creation, editing and removal of key schedule templates, simplifying the key schedule process.

See Section 3.5.5 "*Setting Key Schedule*", page 31 for information on using the key schedule templates.

- 1) In **Settings**, select **General**.
- 2) Expand the **Key Schedule Templates** panel.
- 3) • To add a template:
 - a) Click **ADD**.
The **Create Key Schedule Template** window opens.
 - b) Enter the template name.
 - c) Select the **Schedule Type**.
 - **Standard**: Enable each day separately and set the start and end time.
 - **Advanced**: Click **Add Slot** to start editing. Time slots are added one-by-one and the start day/time and the end day/time can be set.

It is possible to add up to 32 slots.

- d) Optional: Enter the **Additional Information**.
- e) Click **OK** to exit.
- To edit a template:
 - a) Select a template from the list.
 - b) Click **ADD**.

The **Information Card** window opens.

- c) Edit the schedule.
- d) Click **OK** to exit.
- To delete a template:
 - a) Select a template from the list.
 - b) Click **DELETE**.

The **Question** window opens.

- c) Click **YES** to delete the selected template.

4.1.9 Setting Audit Trail Retention Policy

- 1) In **Settings**, click **GENERAL**.
- 2) Expand the **Archival / Retention Policy** panel.
- 3) Select each required information type, and set the number of days to retain.
 - **Audit Trails:** When enabled, audit trail entries are removed from the database after the set number of days.
 - **Log Files:** When enabled, log files stored in the application folder are removed after the set number of days. By default, it is set to 90 days.

The **OPEN LOGS FILE FOLDER** button opens a Window's folder for browsing the log files.

- **Events:** When enabled, events stored in the database are removed after the set number of days.

4.1.10 Setting the Revalidation Period



NOTE!

The revalidation period set here is applied to all keys which are enabled the revalidation feature.

- 1) In **Settings**, click **General**.

- 2) Expand the **Remote Settings** panel.
- 3) To enable the revalidation on all keys, check the checkbox.



NOTE!

To set the revalidation on the specific keys, refer to the procedure in Section 3.5.4.1 *"Enabling and Disabling Key Revalidation"*, page 31.

- 4) Enter a number of days and hours for the revalidation period.
This is the time the key stays active after revalidation in a Remote PD.
- 5) Click **APPLY CHANGES** to exit.

4.1.11 Enabling and Disabling Approver Setting

The Approver function adds extra security to the system by requiring permission for certain actions regarding audit trail data. Any user can be set as the Approver.



NOTE!

- The C-Key handed out to the Approver cannot be used to log in to the program.
- Only one Approver can be appointed per system.

To set a user as the Approver, see Section 4.3.4.2 *"Appointing or Dismissing the Approver Role"*, page 86.

Prerequisite:

- To disable the Approver functionality, the C-Key handed out to the Approver must be inserted in the right slot of the Local PD.

- 1) In **Settings**, click **General**.
- 2) Expand the **Approver Settings** panel.
- 3) Select or deselect **Enable Approver Functionality**.
- 4) To disable, insert the approver's C-Key in the right slot of the Local PD.



NOTE!

The approver is automatically set as a User after disabling the approver functionality.

4.1.12 Setting Notifications

- 1) In **Settings**, click **General**.
- 2) Expand the **Notification Settings** panel.

- To receive notifications when keys exceed their expiry date, select **Notify overdue keys**.
- To receive notifications when employees exceed their expiry date, select **Notify overdue employees**.
- To receive notifications when visitors exceed their expiry date, select **Notify overdue visitors**.

4.1.13 Handling Hand Out and Hand In Text Templates

Hand out and hand in text templates are used to create printable messages. For example, these messages could contain a set of company rules and responsibilities, general information for key-holders, or confirmation that a key has been handed in.

To create or edit hand out and hand in templates:

- 1) In **Settings**, click **General**.
- 2) Expand the **Hand Out Text Templates** panel or the **Hand In text Templates** panel.
The process for managing hand out text templates and hand in text templates is the same.
 - To add or edit a text template:
 - a) • To add, click **ADD**
 - To edit, select the template from the list and click **EDIT**
 - b) Enter or edit the template name in **Name**.
 - c) In the RTF editor, edit the message text.
The RTF editor allows for the insertion of images, and copy-and-pasting of formatted data from other text editors.
 - d) Click **OK** to save.
 - To delete a text template:
 - a) From the list, select the template.
 - b) Click **DELETE**.

4.1.14 Enhancing Security

In order to increase security, it is possible to require users to enter the C-Key PIN after a period of inactivity.

- 1) In **Settings**, select **General**.
- 2) Expand the **Security Setting** panel.
- 3) Click the check box next to the text **Force type in C-Key PIN code for C-key operations after being idle for a specific time**.
- 4) Enter the idle time.

The system requires entering the C-Key PIN code if the idle time is longer than set time.

4.1.15 Deleting a Locking System

CLM is designed for importing, expanding, restoring, or migrating locking systems, but systems can also be deleted. For example, this is useful in multi-system CLM installations.

To delete a locking system:

- 1) In **Settings**, select **General**.
- 2) Expand the **Other Settings** panel.
- 3) Click **DELETE SYSTEM**.
- 4) To confirm the deletion, enter the word that the pop-up window asks for.
- 5) Click **OK**.
- 6) When asked, enter the C-Key PIN

4.1.16 Updating License

The valid period of a license varies. When the expiry date is approaching, a new license is provided by an ASSA ABLOY competence partner.

- 1) In **Settings**, click **General**.
 - 2) Expand the **Other Settings** panel.
 - 3) Click **UPDATE LICENSE**.
- The **Question** window pops up.
- 4) Click **OK** to proceed.
 - 5) Select the new license from the pop-up file explorer and click **Open**.

An **Information** window notifies the user when the license is update successfully.

- 6) Click **OK**.

4.1.17 Enabling and Disabling Alternative Marking Edit

By enabling editing of alternative markings, custom markings can be tailored to fit the locking system implementation.

- 1) In **Settings**, click **General**.
- 2) Expand the **Other Settings** panel.
- 3) Select or deselect **Allow to edit alternative markings**.

4.1.18 Enabling and Disabling Automatic Dynamic Key Programming

By default, a Dynamic Key is automatically detected and programmed in the **Lock Chart** and **Job List** window when it is inserted into the Local PD. This automatic function can be disabled.

- 1) In **Settings**, click **General**.
- 2) Expand the **Other Settings** panel.
- 3) Select or deselect **Do not use automatic programming for dynamic keys**.
The **Question** window pops up and asks to confirm the action.
- 4) Click **OK**.

4.1.19 Setting PD Options



By enabling this option, the user can select the Local PD at the next login.

- 1) In **Settings**, click **General**.
- 2) Expand the **PD Options** panel.
- 3) Click **Setup PD Communication**.

4.2 C-Key Settings

C-Keys are special keys associated with users. They are used for system functions, and cannot open doors.

Go to **Settings**, and select **C-Key Settings**. C-Key settings are divided into the following three categories.

- **** **PIN Management**
-  **C-Key List**
-  **User List/User Information**



NOTE!

Only a supervisor can view the **User List**, other users can view their **User Information** instead.

4.2.1 Setting the C-Key PIN

This topic describes how to change the PIN of the C-Key which is currently logged in, that means the C-Key in the left slot of the Local PD.

To reset the PIN of a C-Key which is not in the left slot of the Local PD, see Section 4.2.3 *“Resetting a C-Key PIN”*, page 80.

- 1) In **Settings**, click **C-Key Settings**.
- 2) Click **PIN Management**.
- 3) Enter the current PIN once.
- 4) Enter the new PIN twice.
- 5) Click **OK** to confirm.

4.2.2 Understanding the C-Key List

The **C-Key List** displays all C-Keys in the current locking system.

C-Key List

This screen shows the list of all keys

All

Search C-Key List

Reset PIN

Cylinder Domains

Upgrade Firmware

Upgrade Cylinder Firmware

View Report

List Settings

Name	Mark	C-Key Type	User Assigned	Status
PR01		Master	Supervisor	Handed Out
PSM01		Sub-Master		In Stock
PN01		Normal		In Stock

Item Colours

The following colours are used in the C-Key List.

	C-Key
	Selected line

Buttons

- The **Reset PIN** button
For more information, see Section 4.2.3 *“Resetting a C-Key PIN”*, page 80.
- The **View Report** button
For more information, see Section 2.5.4 *“Creating a View Report”*, page 18.
- The **Lock Chart** button
For more information, see Section 4.2.5 *“Managing C-Key Cylinder Permission”*, page 81.

- The **Upgrade Firmware** button
For more information, see Section 3.14.4 “*Upgrading a C-Key's Firmware*”, page 69.
- The **List Settings** button
For more information, see Section 2.5.3 “*Customising List View*”, page 17.

4.2.3 Resetting a C-Key PIN

Sometimes the user needs to reset the PIN of a C-Key which is not currently logged in. The new C-Key PIN is programmed in the right slot of the Local PD.

In order to set the new PIN of the C-Key which is in the left slot of the Local PD, refer to Section 4.2.1 “*Setting the C-Key PIN*”, page 78.

- 1) In **Settings**, click **C-Key Settings**.
- 2) Click **C-Key List**.
- 3) Select the C-Key for which the PIN is to be reset.
- 4) Click the **Reset PIN** button above the **C-Key List**.
Information window pops up and asks to insert the C-Key which needs to reset the PIN.
- 5) Click **OK**.
- 6) Type in PIN of the C-Key which is currently logged in, and click **OK**.
The window with the new C-Key PIN pops up.
- 7) Optional: To copy the new C-Key PIN to the clipboard, click **COPY**
- 8) Click **CLOSE** to exit.

4.2.4 Viewing and Editing C-Key Information

- 1) In the **C-Key List**, right-click the C-Key.
The context window is opened.
- 2) Click **Info Card**.
The information card for the selected C-Key is opened.



HINT!

The PUK code is only visible to the supervisor.

- 3) View or edit the information.
- 4) Click **OK** to save.

4.2.5 Managing C-Key Cylinder Permission

Each C-Key can be set cylinder permission individually by the CLM Administrators. If a C-Key has permission to a cylinder, the cylinder jobs can be sent to the C-Key which has permission and the C-Key can perform jobs generated for that cylinder.





C-Key cylinder permission is managed in the **Cylinder Domains Chart**.

- 1) Click the **Cylinder Domains** button above **C-Key List**.

The **Cylinder Domains Chart** window pops up.

- 2) Double click the square where the cylinder and the C-Key cross to grant or remove the cylinder permission.

The colours shows different types of permission.

Colour	Description
	The C-Key has no permission to program the cylinder.
	The Master C-Key has permission to program the cylinder.
	The Submaster C-Key has permission to program the cylinder.
	The Normal C-Key has permission to program the cylinder.



NOTE!

The Master C-Key always has permission to all cylinders and it is not changeable.

4.2.6 Handing Out C-Keys

To hand out a Normal Key, refer to Section 3.1 *"Handing out Keys"*, page 19.



HINT!

Before handing out the C-Key, it is recommended to check or edit the **User Rights** of the person to whom the C-Key is assigned. For more information about user rights, see Section 4.3.4.1 *"Editing User Rights"*, page 86.

- 1) In **Hand out / in**, click **Hand out**.



HINT!

Hand Out can also be selected from the context window when right-clicking a person or a key in **C-Key Key List**.

- 2) If a C-Key is not selected:

- To select the C-Key which is in the right slot of the Local PD, click **SCAN**.
- To select a C-Key from the list:

- a) Under **Key**, click **SELECT C-KEY**.
 - b) From the **C-Key List** pop-up window, select a C-Key and click **OK**.
- 3) If a person is not yet selected:
 - a) Under **Person**, click **SELECT**.
 - b) Select **Employee** (default) or **User** from the top right corner of the pop-up window.
 - c)
 - Select the required person from the list, if available.
 - If the person is not in the list, create a new person by clicking **Create Employee**.

For more information on creating a person, see Section 3.8.2 *"Creating an Employee or Visitor"*, page 52.
 - d) Click **OK**.
- 4) Set **Hand In Date and Time** or select **Permanent**.



NOTE!

An expired hand in date does not automatically revoke access rights.

- 5) Optional: Select a hand out text template:
 - a) Click **SELECT TEXT TEMPLATE**.
 - b) Select a **Template Name** and click **OK**.

For more information on how to add and edit hand out text templates, see Section 4.1.13 *"Handling Hand Out and Hand In Text Templates"*, page 76.
 - 6) Click **SAVE** to confirm the hand out.
 - 7) Review or print the hand out report.
- The notes from the hand out text template are included at the end of the hand out report.



HINT!

The user can always review or edit the hand out report by clicking **Reprint Hand Out** or **Edit Handout** in the context window.

4.2.7 Handing In C-Keys

The process for handing in C-Keys is the same as for Normal Keys.

- 1) In the **C-Key List**, right-click the C-Key.
The context window is opened.
- 2) In the context window click **Hand In**.

This option is disabled if the C-Key is not handed out.



HINT!

Hand In page can also be reached by clicking **Hand out / in » Hand in**.

- 3) Complete the hand in process.

For more information on the process, see Section 3.2 *"Handing In Keys"*, page 21.

4.2.8 Synchronising a C-Key to System Time

- 1)
 - To synchronise the C-Key which is in the left slot of the Local PD, proceed to *Step 2*.
 - To synchronise a C-Key which is not currently logged in, insert the C-Key in the right slot of the Local PD.



NOTE!

The logged in C-Key should not be removed from the left slot of the Local PD.

- 2) In the **C-Key List**, right-click the C-Key to be programmed.
The context window is opened.
- 3) In the context window, click **Sync System Time**.
- 4) Enter the PIN of the programmed C-Key.

4.2.9 Reporting Lost and Broken C-Keys



NOTE!

The Master C-Key can be declared as neither Lost nor Broken. If the Master C-Key is lost or broken, it needs to be replaced with a new Master C-Key.

- 1) In the **C-Key List**, right-click the C-Key to be reported as lost or broken.
The context window is opened.
- 2) Click **Mark as Lost** or **Mark as Broken**.
- 3) In the **Question** window, click **YES** to confirm the action.
- 4) Optional: Enter the reason in the next window and click **OK**.
- 5) Read the message in the **Information** window and click **OK**.

4.2.10 Returning Lost or Broken C-Keys



NOTE!

Do not insert the C-Key to be returned into the right slot of the Local PD until *Step 3*.

If the returning C-Key is inserted before *Step 3*, the tasks on the C-Key are automatically deleted.

- 1) In the **C-Key List**, right-click the C-Key to be returned to the system.
The context window is opened.
- 2) Click **Return to System**.
Information window opens and asks whether to keep the tasks on the returning C-Key or not.
- 3)
 - To keep the tasks:
 - a) Click **NO**.
 - b) If necessary, enter the reason in the next window if necessary and click **OK**.
 - To delete the tasks:
 - a) Insert the returning C-Key into the right slot of the Local PD.
 - b) Click **YES**.
 - c) If necessary, enter the reason in the next window if necessary and click **OK**.
 - d) Type in PIN of the returning C-Key.
- 4) Read the message in the **Information** window and click **OK**.

4.3 C-Key User Settings

4.3.1 Working with the User List

The **USER LIST** can only be accessed by supervisors, and offers the same search functionality and **List Settings** as other lists in CLM.

A user is created and added to the list when a C-Key is handed out to a person.

To view the user list:

- 1) In **Settings**, click **C-KEY SETTINGS**.
- 2) Click **USER LIST**.

4.3.2 Viewing and Editing User Information

- 1) In **Settings**, click **C-Key Settings**.

- If logged in as a normal user:
 - a) Click **User Information**.
 - b) View or edit the user information card.
- If logged in as a supervisor:
 - a) Click **User List**.
 - b) In the **User List**, right-click the person.
The context window is opened.
 - c) Click **Info Card**.
The information card for the selected key group is opened.



HINT!

Double clicking on the key line performs the same action.

- d) View or edit the information card.
- e) Click **OK** to save.

4.3.3 Changing the System Language

CLM is a multi-language system and allows each C-Key user to set their own language preference.

By default, the system uses English.

- 1) In **Settings**, click **C-KEY SETTINGS**.

- If logged in as a normal user:
 - a) Click **USER INFORMATION**.
The user's **Information Card** pops up.
 - b) Select the preferred language from the drop-down list under **Language**.
- If logged in as a supervisor:
 - a) Click **USER LIST**.
 - b) In the **Person List**, right-click the person.
The context window is opened.
 - c) Click **Info Card**.
The information card for the selected key group is opened.



HINT!

Double clicking on the key line performs the same action.

- d) Select the preferred language from the drop-down list under **Language**.

- 2) Read the **Information** window and click **OK**.

- 3) Click **OK** to exit.

The new language will be applied next time the user logs into the program.

4.3.4 Managing User Rights and Roles

4.3.4.1 Editing User Rights

Giving user rights enables the user to access or manage the sections in the system. The supervisor can set individual user the user rights.

Prerequisite:

The user must log in as the supervisor.

- 1) In the **User List**, right-click the user to change or edit the user rights.

The context window is opened.

- 2) In the context window click **User Rights**.

The **User Rights** window pops up.

- 3) Set the rights for the selected user. Each task has three different levels of accessibility.

- **None:**

The user is denied access to the section of the program.

- **View:**

The user can access the section but is not able to make changes.

- **Full:**

When selected, the list expands and shows individual functions. The user can access and edit the section of the program.

4.3.4.2 Appointing or Dismissing the Approver Role

The following steps describe how to appoint or dismiss a user as the Approver.

For more information about Approver roles, see Section 5.5 *"User Roles and Rights"*, page 101.

To enable the Approver setting, see Section 4.1.11 *"Enabling and Disabling Approver Setting"*, page 75.

Prerequisite:

- Log in as the supervisor to appoint or dismiss the Approver.



NOTE!

- The C-Key handed out to the Approver cannot be used to log in to the program.
- Only one Approver can be appointed per system.

Select an appropriate person as the Approver.

If someone has already been appointed as the Approver, change her/his role to **User**.

- To dismiss the Approver role, the C-Key handed out to the Approver must be inserted in the right slot of the Local PD.

- 1) In the **User List**, right-click the user to appoint or dismiss.
The context window is opened.

- 2) Click **Info Card**.
The information card for the selected user is opened.



HINT!

Double clicking on the user in the list performs the same action.

- 3)
 - To appoint the Approver role:
In the **General Information** tab, under **Role**, select **Approver**.
 - To dismiss the Approver role:
 - a) Insert the C-Key which was handed out to the Approver in the right slot of the Local PD.
 - b) In the **General Information** tab, under **Role**, select **User**.
 - c) Enter the C-Key PIN.
- 4) Click **OK**.

4.3.5 Setting a New User Password

User passwords are used to log in to CLM without a C-Key. To change the PIN of a C-Key, see Section 4.2.1 “*Setting the C-Key PIN*”, page 78.

To change a user's password:

- 1) In **Settings**, click **C-KEY SETTINGS**.
- 2) Click **USER LIST**

- 3) Right-click the user.
- 4) Click **Set Password**
- 5) Enter a **New Password** and **Confirm Password**.
- 6) Click **OK** to confirm.

4.3.6 Activating or Deactivating a User

The activation and deactivation of a user works the same as for persons. New C-Keys cannot be handed out to inactive users, but any C-Keys they already hold retain their validity.

To switch a user between active and inactive:

- 1) In **Settings**, click **C-KEY SETTINGS**.
- 2) Click **USER LIST**.
- 3) Right-click the user.
- 4) Click **Switch Active/Inactive**.

Inactive users appear red in the **User List**

4.3.7 Deleting a User

Before a user can be deleted, all C-Keys handed out to the user must be handed in. A supervisor cannot be deleted.

To delete a user:

- 1) In **Settings**, click **C-KEY SETTINGS**.
- 2) Click **USER LIST**.

The user list is only available when logged in as a supervisor.

- 3) Select a user.
- 4) To delete and remove the user from the list, click **Delete**.

4.4 Managing the Controller and Remote PDs

To manage the controller and Remote PDs, click the **Remote List** button in the left menu.

4.4.1 Understanding the Remote List

Controller / Wall PD List This screen shows the list of Wall PDs and the controller

All

Name	Mark	Status	Last Status Update
Controller		Connected	09/11/2021 at 12:29
Wall-PD mit SUR	WPD01	Connected	09/11/2021 at 12:29
Wall-PD	WPD02	Not Connected	
Wall-PD mit SUR	NULLSUR1	Disabled	

Item Colours

In the list, controllers and Remote PDs are displayed with different colours. The colour in the list indicates the type of row.

	Wall PD
	Controller
	Selected line

Buttons

- The **Show Only Active** toggle button
The **Controller / Wall PD List** displays all controllers and Remote PDs in the system, and other useful information. Deactivated controllers and Remote PDs can be excluded from the list by setting the **Show Only Active** toggle button to **YES**.
- The **Sync Controller** button
Click this button to start the process to sync the controller information with the CLM information.
- The **View Report** button
For more information, see Section 2.5.4 “*Creating a View Report*”, page 18.
- The **List Settings** button
For more information, see Section 2.5.3 “*Customising List View*”, page 17.

4.4.2 Adding a New Wall PD

Up to three Wall PDs can be enabled in a Remote CLM system.

When a new Wall PD is added to the system, the configuration file has to be generated and imported to the Wall PD.

- 1) In the **Controller / Wall PD List**, right-click the Wall PD to be added.
The context window is opened.
- 2) Click **Generate Config File**.
CLM connected to the controller to receive the certificate assigned to the selected Wall PD.
- 3) Select the destination folder and click **OK**.
Two files are created and stored in the folder.



NOTE!

Do not change the name of the files. The Wall PD can recognise only files with the original name.

- 4) Copy the configuration file to an USB memory storage device.



NOTE!

Use an empty USB memory storage device.

- 5) Connect the USB memory storage device to the Wall PD via a mini-USB adapter cable.
- 6) Remove the USB memory storage device after a beep sound from the Wall PD.
When the Wall PD establishes the connection to the controller, the LED indicator in the Wall PD turns from white blinking light to white solid light.
- 7) Back to the CLM system and verify the Wall PD's status is **Connected** in the **Controller / Wall PD List**.

4.4.3 Viewing and Editing Controller or Remote PD Information

The data entered when creating a controller or Remote PD can be displayed and edited in the **Information Card**.

- 1) In the **Remote List**, right-click the device.
The context window is opened.
- 2) Click **Info Card**.
The information card for the selected device is opened.



HINT!

Double clicking on the device in the list performs the same action.

- 3) View or edit the information.

General Information tab

- **Name**
The devices name.
- **Status**
Connection status of the device.
- **Last Online**
Last time the Wall PD was successfully reached by the controller.
- **Marking**
The device's marking.
- **MAC Address** (Remote PD only)
The MAC address of the device.
- **Type** (Remote PD only)
The type of the device.
- **Firmware Version** (Remote PD only)
Firmware version installed in the device.
- **Hostname** (Remote PD only)
The hostname assigned to the device.

Connection Settings tab (Controller only)

- **IP Address**
 - If **Use Custom IP** is selected:
The system connects to the controller using the specified IP address.
 - If **Use Custom IP** is not selected:
The system connects to the controller using the device's hostname CLMremoteController.

4) Click **OK** to save any changes made.

4.4.4 Activating or Deactivating a Wall PD

Up to three Wall PDs can be enabled in a Remote CLM system.

When a Wall PD is deactivated, the controller ignores all communication with the Wall PD.

- 1) In the **Remote List**, right-click the Wall PD.
The context window is opened.

- 2) Click **Switch Active/Inactive**.
The selected Wall PD status is changed.

4.5 Editing System Information

The **System Information** contains general information on the locking system as well as customer details.

To edit the system and customer information:

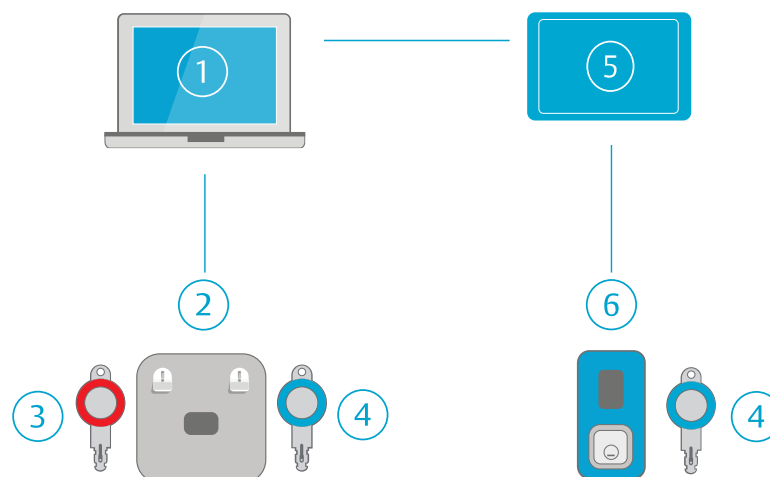
- 1) In **Settings**, click **SYSTEM INFORMATION**.
- 2) In the **Information Card**, select the **General Information** or **Customer Information** tab.
- 3) View or edit the information.
- 4) Click **OK** to save.

5 CLM Concepts and Features

5.1 CLIQ™ Hardware

5.1.1 CLM Architecture

The basic architecture of a CLM system is shown in the image below.



1. **CLM Client** is a computer used by an administrator to administer a locking system. Several clients can be connected to the server.
2. **Local PDs** are connected to the CLM client, and are used by the administrator to log in to CLM (using a C-Key) and to program keys locally. See Section 5.1.4.1 “*Local PDs*”, page 96 for more details.
3. **C-Keys**. See Section 5.1.2.3 “*C-Keys*”, page 94.
4. **User Keys**. See Section 5.1.2.2 “*User Keys*”, page 94.
5. **Controller** handles remote update of keys. Key update jobs are sent from the CLM client to the controller. The update jobs are stored until they are executed from either a Wall PD or the Local PD.
6. **Wall PDs**. A type of Remote PD. By inserting a key in a Wall PD the key update jobs stored in the controller are executed. See Section 5.1.4.2 “*Wall PDs*”, page 97 for more details.

5.1.2 Keys

5.1.2.1 Key Types

There are two types of key handled in CLM:

- **C-Keys**, also called system keys, are Electronic Keys used by administrators to administrate the locking system.
- **User Keys** are used by employees and visitors to access the facilities. There are two types of user keys:
 - **Mechanical Keys**

Mechanical Keys are added or deleted manually in the system. CLM keeps track of the keys that have access to certain mechanical cylinders.

— **Electronic Keys**

The CLIQ™ keys are electromechanical keys that contain electronics and a battery and may also have a mechanical cutting. Each CLIQ™ key is programmed and can be controlled and managed using CLM. CLM keeps track of the CLIQ™ keys that have mechanical access to a certain cylinder, and takes this into consideration when determining the possibility to grant electronic access.

For more information about these key types, see Section 5.1.2.3 “C-Keys”, page 94 and Section 5.1.2.2 “User Keys”, page 94.

5.1.2.2 User Keys

User Keys are used by employees and visitors to access the facilities. There are several types of User Keys.

Mechanical Key	A traditional key with no electronic components. Can be managed in CLM but cannot be used with CLIQ™ cylinders.
Normal Key	An electromechanical key that can open mechanical cylinders when the cutting is compatible, and that can be authorised to open CLIQ™ cylinders based on the cylinder access list.
Quartz Key	This key type has the same functionality as a Normal Key. In addition, it has a quartz clock function and can be programmed to be active between certain dates (see Section 5.2.3 “Key Validity”, page 98). It can also be programmed to have access to cylinders based on a schedule (see Section 5.2.6 “Key Schedule”, page 100). Keys of this type can also store audit trails (see Section 5.4 “Audit Trails”, page 101).
Dynamic Key	This key type has the same functionality as a Quartz Key. In addition, it can store an access list of cylinders that the key is authorised to open (see Section 5.2.5 “Electronic Authorisation”, page 99).

5.1.2.3 C-Keys

System keys, also called **C-Keys**, are keys that are used by locking system administrators. C-Keys do not open cylinders, but are used to access CLM and to program cylinders.

There are three types of C-Keys: **Master C-Keys**, **Sub-Master C-Keys**, and **Normal C-Keys**.

Master C-Key	<p>The Master C-Key is used by the Super Administrator to manage the locking system.</p> <p>There is only one Master C-Key per locking system and it must be kept in a secure place. If a new Master C-Key is imported to the system, the existing one is automatically replaced by the new one.</p> <p>The Master C-Key always has full access to all functions in CLM and cannot be limited by assigning user roles or rights.</p>
Sub-Master C-Key	<p>Sub-Master C-Keys are used by administrators. There can be multiple Sub-Master C-Keys in a locking system. A Sub-Master C-Key can be given the same full access rights as the Master C-Key, but the rights can also be limited by assigning user roles and rights. See Section 5.5 “User Roles and Rights”, page 101.</p>
Normal C-Key	<p>Like Sub-Master C-Keys, Normal C-Keys are used by administrators and there can be multiple Normal C-Keys in a locking system. The rights for Normal C-Keys can also be configured using user roles and rights (see Section 5.5 “User Roles and Rights”, page 101), but Normal C-Keys can never be given the right to:</p> <ul style="list-style-type: none"> • Change the PIN code of other C-Keys. • Execute Cylinder Programming Jobs that include updated access for C-Keys. • Report a lost C-Key found.



NOTE!

The term **C-Key** is used when describing functionality that applies to all types of C-Keys.

5.1.2.4 Key Groups

Key Groups are used to set access rights and other attributes to a group of keys rather than to each key individually.

Key group benefits:

- Key groups simplify the cylinder access settings.
- Adding a new key to a key group automatically gives the new key access to all cylinders where the key group is allowed. No programming of cylinders is required.

When a key group is given access to a cylinder, all keys in the key group are automatically given access.



NOTE!

When a key group is added to the **Key List** in a cylinder, any individual entries of keys of that key group (now redundant) are automatically removed. This means that if a key group is added and then later removed, all keys in the group will lose their access, including keys that previously had individual access.

Mechanical keys cannot belong to a key group.

5.1.3 Cylinders

5.1.3.1 Cylinders

There are two different cylinder types, mechanical and electronic. Electronic cylinders can store access rights for keys and key groups, as well as audit trail information.

Cylinders can be single-sided or double-sided. For double-sided cylinders, the sides can be either of the same type or different types.

A cylinder can be installed in many types of locks, doors, padlocks, cabinet locks etc. An identifying number is marked on each cylinder body.

An electronic cylinder stores information for:

- Authorised key groups and key individuals
- Blocked keys
- Normal Audit trails: Audit trails for key insertions by keys of the same locking system
- Foreign Audit trails: Audit trails for key insertions by keys of other locking systems

Different cylinder configurations have different memory capacities. For more information refer to the product information.

5.1.3.2 Cylinder Groups

A **Cylinder Group** is a set of cylinders in a locking system. In CLM, cylinder groups **are not** used to give keys access to multiple cylinders at a time. They are intended to provide an overview of cylinders in the cylinder list and lock chart.

Cylinders can only belong to one cylinder group.

5.1.4 Programming Devices

5.1.4.1 Local PDs

The Local PD is used to connect C-Keys and User Keys to CLM.



Figure 1. Local Programming Device

The Local PD is used by the administrators of a locking system. It has two key slots, the left slot is for C-Keys and the right slot is for user keys. To be able to login to CLM, a Local PD connected to a CLM Client together with a C-Key is required. The PD can be connected using the USB port.

The Local PD has two ports:

- A USB port
- A port for connecting cylinders (not used with CLM)

5.1.4.2 Wall PDs

Wall PDs are used in remote systems for transferring data between the controller and the key.

They are typically mounted on the wall and connected to the controller via an Local Area Network and supports mini-USB On-The-Go (OTG) cable.

When the key is inserted into a Wall PD, the following is executed:

- The key jobs sent to the controller.
- The time on the key is updated.
- The audit trail is read from the key, if so configured.



Figure 2. Wall Programming Device

5.2 Authorisation Principles

5.2.1 Authorisation Principles Overview

For a key to be able to open a cylinder, the following requirements need to be fulfilled:

- The mechanical code is correct. See Section 5.2.2 “*Mechanical Authorisation*”, page 98.
- The key is **valid**. See Section 5.2.3 “*Key Validity*”, page 98.
- The cylinder is electronically programmed to give the key access. See Section 5.2.5 “*Electronic Authorisation*”, page 99.
- For Dynamic Keys: The key has been programmed to have access to the cylinder. See Section 5.2.5 “*Electronic Authorisation*”, page 99.

- For Quartz Keys and Dynamic Keys: The key schedule allows access at the current time. See Section 5.2.6 “*Key Schedule*”, page 100.

5.2.2 Mechanical Authorisation

As with a traditional Master Key System, each key in a CLIQ™ locking system has a mechanical cutting and each cylinder is compatible with one or more key cuttings. CLM keeps track of the keys that have mechanical access to a certain cylinder, and takes this into consideration when determining the possibility to grant electronic access.

5.2.3 Key Validity

In order for a key to open a cylinder, it must be **valid** at the specific time.

The validity settings for a key can be found via the context menu in the **Key List** and the **Lock Chart**, or in the key **Hand Out** view.

Never	The key is never valid.
Always	The key is always valid.
From/To Date	The key is valid between specific dates. From Date is the first day the key is valid. To Date is the last day the key is valid. From/To Date is only available for Quartz Keys and Dynamic Keys.

Changing the validity of a key requires programming in the right slot of the Local PD.

5.2.4 Key Revalidation

Key Revalidation is a feature that ensures that keys are updated at a certain period.

With key revalidation, keys must be updated (“revalidated”) at specified time period to stay active. Once revalidated, the key stays active for the number of days, hours, and minutes specified as the revalidation period, counting from the time it was revalidated. If a key is not revalidated within the specified period, it becomes inactive until it is revalidated again.

Figure 3 “*Key revalidation*”, page 99 shows the principle of key revalidation. When a key is revalidated in a Remote PD a timer starts (1). The key has access as long as it is used within the revalidation period (2). When the revalidation period has expired (3) the key needs to be revalidated in a Remote PD (1). When the key is revalidated the timer is reset.

Keys are revalidated also in a Local PD when the following actions were operated locally:

- set **Schedule**
- read **Audit trail**
- change **Cylinder access list**

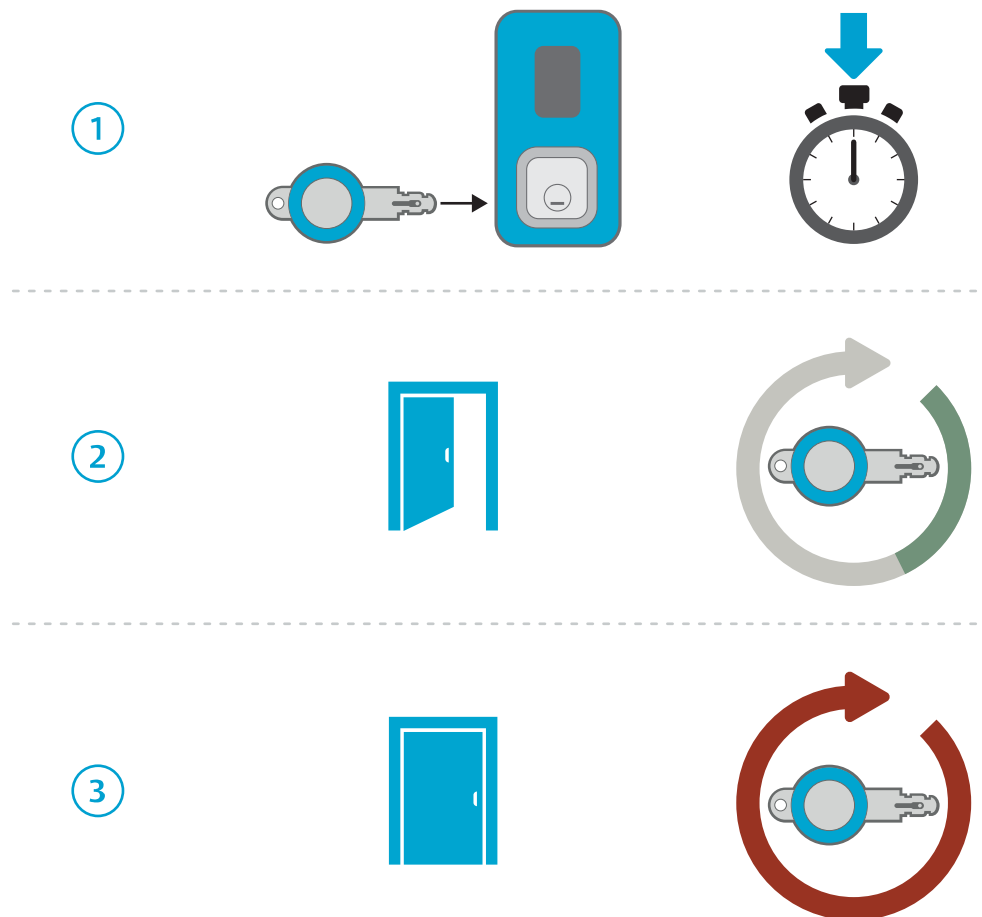


Figure 3. Key revalidation

Revalidation has the following advantages:

- Ensures that pending key updates are programmed to keys on a regular basis.
- Ensures frequent retrieval of key audit trails.
- Limits exposure of lost keys. A lost key loses all access when the specified time is up and if it is reported as lost in CLM it cannot be revalidated.

Setting the revalidation period is a trade-off between convenience for the key holder and the locking system security. A short revalidation period, such as 24 hours, ensures frequent updates and limited exposure of lost keys but requires the key holder to update the key every day. A long revalidation period is more convenient for the key holder, but increases the exposure of lost keys and results in less frequent updates of accesses and audit trails.

5.2.5 Electronic Authorisation

Electronic authorisation is based on information stored in the cylinder and, for Dynamic Keys, also in the key.

The following information can be stored in cylinders:

- A **Cylinder Access List** that contains the keys and key groups that have access to the cylinder.

When a key group is added to a Cylinder Access List, any individual entries of keys belonging to that key group (now redundant) are automatically removed. This means that if a key group is added and then later removed, all keys in the group will lose their access, including keys that previously had individual access.

For Quartz Keys and Normal Keys the information in cylinders alone determines if a key has access to a cylinder.

In Dynamic Keys, the following information can be stored:

- A **Key Access List** that contains the cylinders and cylinder groups to which the key has access.

In order for a Dynamic Key to be able to open a cylinder, the accesses in the cylinder and the key must match. In a system with Dynamic Keys, the cylinders are typically programmed to provide access to all keys. The actual access is controlled by the key access list. In the **Lock Chart**, it is shown in yellow when the access is given to the cylinder access list but not to the key access list.

The capacity of a Key Access List is limited. The maximum and currently available capacity can be viewed from the **Information Card** of a Dynamic Key.

5.2.6 Key Schedule

In order for a key to be able to open a cylinder, it must have a schedule that grants access at the specific time.

The schedule settings for a key are found in the context window in the **Key List** and the **Lock Chart**, or in the key **Hand Out** view. The schedule can be set on Quartz Keys and Dynamic Keys.

Schedules can be of two **Schedule Types**:

- In the **Standard** schedule type, one time period per day in a week can be specified.
- In the **Advanced** schedule type, a number of separate time periods per week can be specified and each period can be extended over several days.

Changing schedule requires the key to be inserted to the right slot of the Local PD.

5.3 Remote Update

The remote feature enables administrators to update key configurations, such as authorisations, validity or schedule without the key being present. That means the key update jobs can be executed in Wall PDs.

Key update jobs are sent to the Controller from the system, and the Controller passes the correct key job to a Wall PD in which the key to be updated is inserted. Unless the key is scanned and updated in the Local PD, they remain in the database of the Controller until being executed in a Wall PD.

Systems are either delivered as remote or non-remote systems. A non-remote system that is later converted to a remote system, may contain both keys that support and keys that do not support remote updates. In a system initially delivered as a remote system, all keys support remote updates at delivery.

Contact your certified CLIQ™ reseller to add the remote feature to the current system.

5.4 Audit Trails

Both Quartz and Dynamic keys and cylinders have an audit trail feature. An Audit Trail event is logged when a key requests access from a cylinder. Events are also logged when keys and cylinders are programmed. There are two types of audit trails:

- **Normal audit trails** contain events from devices within the same locking system.
- **Foreign audit trails** contain events from devices which belong to different locking systems.

When the audit trail is full, the oldest event is replaced every time a new event is created. The audit trail capacity varies according to the type of key or cylinder. For more information, refer to the local CLIQ™ dealer.

Key Audit Trails

The key audit trail records which cylinders the key has attempted to access, the key holder at the time (if not permanently deleted or deactivated) and programming jobs that have been performed on the key. It also records the time and the outcome of these events.

Cylinder Audit Trails

The cylinder audit trail records which keys have attempted access, the key holder at the time (if not permanently deleted) and programming jobs that have been performed. It also records the time and the outcome of these events.

Approvals

In locking systems where the **Approver Functionality** is enabled, all audit trail access from keys and cylinders must be approved by an administrator with the **Approver** role. Once the audit trail is read from a key or a cylinder, it can also be viewed by administrators with the **User** role. See also Section 5.5 “*User Roles and Rights*”, page 101.

5.5 User Roles and Rights

User roles in CLM:

Supervisor	The system owner and highest role.
Approver	Can approve audit trails.
User	Default C-Key holder role, if audit trail is enabled.

User rights in CLM:

None	No access to the program section.
View	Read-only access to the program section.
Full	Read and write access to the program section.

Only supervisors can change roles and user rights. When a user is created and assigned to a role, default user rights are set accordingly. The user rights for a specific user in a particular role may also be edited individually.

6 Appendix

6.1 Shortcut Keys

The following sections show the list of shortcut keys for each section of the program.

6.1.1 General Shortcuts

Key	Description
F1	Open the Help window.
ESC	Close windows. If the window is a question message, CANCEL or NO will be selected.
Shift + *	Navigate the next section.
Shift + /	Navigate the previous section.

6.1.2 Key List Shortcuts

Key	Description
F3	Open the Create Key Line window.
F4	Open the Create Mechanical Key window.
Shift + F4	Open the Create Multiple Mechanical Key window.
F5	Open the Update DST window
F7	Upgrade user key firmware
Shift + F8	Expand all nodes in the key list.
Ctrl + F8	Collapse all nodes in the key list.
F10	Open List Settings .
Shift + F10	Show a report of the key list.
F11	Delete the currently selected element, when possible.

6.1.3 Cylinder List Shortcuts

Key	Description
F3	Open the Create Cylinder Group window.
F4	Open the Create Cylinder window.
Shift + F4	Open the Create Multiple Cylinders window.
F5	Move one row up.
F6	Move one row down.
F7	Upgrade cylinder firmware.
F8	Show upgrade firmware sessions.
Shift + F8	Expand all cylinder groups.
Ctrl + F8	Collapse all cylinder groups.
F10	Open List Settings .

Key	Description
Shift + F10	Show a report of the cylinder list.
F11	Delete the currently selected element, when possible.

6.1.4 C-Key List Shortcuts

Key	Description
F5	Upgrade cylinder firmware.
F7	Upgrade system key firmware.
F8	Reset the PIN of the C-Key in the second port.
F9	Show the C-Key lock chart.
F10	Open List Settings .
Shift + F10	Show a report of the C-Key list.

6.1.5 Person List shortcuts

Key	Description
F3	Open the Create Employee window.
F4	Open the Create Visitor window.
F7	Export template.
F8	Import persons.
F10	Open List Settings .
Shift + F10	Show a report of the person list.
F11	Delete the currently selected element, when possible.

6.1.6 Lockchart Shortcuts

Key	Description
Shift + F2	Open the information card of the currently selected cylinder.
Ctrl + F2	Open the information card of the currently selected key.
F3	Auto fill accesses.
F5	Apply changes to the dynamic key, when the key is inserted in the PD.
Shift + F6	Switch to the cylinder edit mode.
Ctrl + F6	Switch to the key edit mode.
F7	Open the Job List window.
F8	Scan key.
Shift + F8	Expand all key nodes.
Ctrl + F8	Collapse all key nodes.
F9	Flip lockchart.
Shift + F9	Expand all cylinder groups.
Ctrl + F9	Collapse all cylinder groups.
F10	Open List Settings .
Shift + F10	Show the lockchart report.

6.1.7 Key Schedule Card Shortcuts

Key	Description
F3	Add Advanced Slot.
F6	Delete Selected Slot.

6.1.8 System List Shortcuts

Key	Description
F2	Migrate system.
F3	Import system.
F4	Restore system.
F10	Open list settings.

6.1.9 User List Shortcuts

Key	Description
F10	Open List Settings .
Shift + F10	Show a report of the user list.
F11	Delete a user, when possible.

6.2 Cases Cause Errors in Importing or Migrating a Locking System

When an element has any wrong value, the system stops migrating or importing process or skips migrating or importing the element. In this section, all conditions which cause such error are listed by element.

C-Key

Condition	Result
Master Key or replacement is not defined.	The migration or import process is stopped.
C-Key ID is 0 or less.	The migration or import process is stopped.
C-Key Type is master or replacement, and defined CLIQGroup is not 65535 (Master group)	The migration or import process is stopped.
C-Key Type is master or replacement, but CLIQUID is 0 or less.	The migration or import process is stopped.
C-Key Type is none (by error or not defined).	The element is skipped and added in the issue list.
C-Key Type is submaster, but defined CLIQGroup is not 65535 (Master group)	The element is skipped and added in the issue list.
C-Key Type is any other type (Not defined, OldMaster or normal), but CLIQGroup in less than 0	The element is skipped and added in the issue list.
C-Key Type is any other type (Not defined, OldMaster, Submaster or normal), but CLIQUID is 0 or less.	The element is skipped and added in the issue list.

Condition	Result
Programmed mode is not unprogrammed or functional.	The element is skipped and added in the issue list.
Electronic product is not found in file	The element is skipped and added in the issue list.

Cylinder

Condition	Result
Cylinder PID is 0 or less.	The migration or import process is stopped.
Cylinder group is not found in the file.	The migration or import process is stopped.
If mechanical type and CLIQCode is not NormalLock.	The element is skipped and added in the issue list.
Programmed mode is not unprogrammed or functional.	The element is skipped and added in the issue list.
Programmed mode is functional, and any of CLIQGroup or CLIQUID is 0 or less.	The element is skipped and added in the issue list.
Cylinder electronic product is not found in the file.	The element is skipped and added in the issue list.
Element reached maximum number.	The migration or import process is stopped.

Key Line

Condition	Result
Key line PID is 0 or less.	The migration or import process is stopped.

Key Group

Condition	Result
Key group PID is 0 or less.	The migration or import process is stopped.
Key group key line is not found.	The migration or import process is stopped.
Key group is not dynamic or normal.	The element is skipped and added in the issue list.

Electronic Key

Condition	Result
Electronic Key PID is 0 or less.	The migration or import process is stopped.
Electronic Key keyline is not found in file.	The migration or import process is stopped.
Electronic Key type is not defined.	The element is skipped and added in the issue list.
Electronic Key type is normal and validity is from to .	The element is skipped and added in the issue list.
If mechanical and CLIQCode is not defined or industrial.	The element is skipped and added in the issue list.
If functional and any of CLIQGroup or CLIQUID is 0 or less.	The element is skipped and added in the issue list.
Programmed mode is not unprogrammed or functional.	The element is skipped and added in the issue list.

Condition	Result
Electronic Key electronic product not found in file.	The element is skipped and added in the issue list.
Element reached maximum number.	The migration or import process is stopped.

Mechanical Key

Condition	Result
Mechanical Key PID is 0 or less.	The migration or import process is stopped.
Mechanical key keyline is not found.	The migration or import process is stopped.
Element reached maximum number.	The migration or import process is stopped.

Remote PD

Condition	Result
Remote PD PID is 0 or less.	The migration or import process is stopped.
Remote PD firmware version is not found in file.	The element is skipped and added in the issue list.

Accesses

Condition	Result
Access key keyline is not found.	The element is skipped and added in the issue list.

Person

Condition	Result
Person status is undefined.	The element is skipped and added in the issue list.

Handout

Condition	Result
Handout person is not found.	The migration or import process is stopped.
Handout element type is not defined.	The migration or import process is stopped.
Handout element (electronic or mechanical key) is not found.	The migration or import process is stopped.

Cylinder jobs

Condition	Result
Job is sent to C-Key and not received	The migration or import process is stopped.
Job is planned, not sent	The jobs are deleted or, migration or import process is stopped.

Encrypted firmware

Condition	Result
Encrypted firmware type is not defined	The element is skipped and added in the issue list.

6.3 CSV File Structure

To be able to import employee data, a file in the correct format and with the correct contents is needed.

File Format

The file format is CSV (Comma Separated Values), with character encoding **Unicode UTF-8**.

File Size

The maximum file size allowed to be imported is 4.9MB.











File Content

Table 1. CSV File Structure

Name	Description	Mandatory	No of Characters
Type	Type of the person. Valid values: <ul style="list-style-type: none"> Employee: Employee or 1 Visitor : Visitor or 2 		
Title	Title to address the person		Max. 25
FirstName	The person's first name	✓	Max. 50
MiddleName	The person's middle name		Max. 50
LastName	The person's last name	✓	Max. 50
Suffix	The person's suffix		Max. 25
Number	Person's number		Max. 25
Status	Status of the person. Valid values: <ul style="list-style-type: none"> Active: Active or 1 Inactive : Inactive or 2 		
Phone	Person's phone number		Max. 25
WorkFax	Person's fax number		Max. 25
Email	Person's emails address		Max. 100
Organization	Organization to which the person belongs to		Max. 100
WorkPlace	Place of work of the person		Max. 100
Profession	Person's profession		Max. 100
Department	Person's department		Max. 100
Office	Person's office		Max. 100
CreationDateTime	Date and time when the person is created		Max. 7
EmployeeValidDateTime	Time and date of the end of validity for the employee person		Max. 7
VisitorInDateTime	Date and time when the visitor person gets in		Max. 7
VisitorOutDateTime	Date and time when the visitor person leaves		Max. 7
Street	Street address of the person		Max. 50
City	City of residence of the person		Max. 50

Name	Description	Mandatory	No of Characters
ZipCode	Zip Code of the person		Max. 50
State	State or province of the person's residence		Max. 50
Country	Person's residence country		Max. 50

6.4 Wall PD Indications

LED Indications	Buzzer	Interpretation
 Solid white		Power On and Online
 Fast white blinking		Acquiring IP Address
 Slow white blinking		Connecting to Controller during Startup Sequence
 Solid		Key Battery Low
 Blinking		Connecting during Remote Update
 Solid		Connected during Remote Update
 Solid	1 beep	Firmware Upgrade Finished Operation Finished OK Wall PD Settings Updated
 Blinking		Downloading and Processing
 Solid		Not in use
 Solid	3 beeps	Operation finished with error

For operations involving a key, beeps are repeated every three seconds until the key is removed.



ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.



ASSA ABLOY Sicherheitstechnik GmbH

Attilastrasse 61-67
12105 Berlin
GERMANY
Tel. + 49 30 8106-0
Fax: + 49 30 8106-26 00
berlin@assaabloy.com

www.assaabloy.de