CLIQ® Web Manager

User Manual

ZIKON
ASSA ABLOY

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 2025.1
Main document number: D001583864
Date published: 2025-05-22
Language: en-GB

1 Overview

1.1 Introduction

CLIQ Web Manager (CWM) is a Web software system that enables the management and control of CLIQ, an electromechanical locking system enabling full control over access authorisations and key holder activities. The CLIQ system presents a solution that ensures the reliability of mechanical keys and cylinders as well as the security and flexibility inherent in electronic locks.

1.2 Main Features

- **Easy to Install** – CLIQ is a cost-effective offline system that does not require electrical wiring or cylinder batteries.
- **Audit Trails** – CLIQ enables easy access to precise audit trail data from every cylinder and key in a locking system.
- **Individual keys** – Protected by strong cryptographic keys, each key is designated for use by a single individual. If the key is lost it is simply rendered obsolete and a new key is generated in its place.
- **Time-based permission** – CLIQ enables the definition of a specific time slot schedule in which time slot access is permitted.
- **Key management** – CLIQ Web Manager keeps track of the issue of keys to various key holders.
- **Electronic key cancellation** – Keys can be cancelled without the presence of the physical key.
- **Revalidation of authorisations** – Adds to the security of the locking system by forcing the key holders to get permission updates from a nearby programming device. It also makes sure that the audit trail is uploaded onto the server and is available to the locking system administrators.
- **Grouping functions** for easier administration. CLIQ Web Manager makes it possible to provide access to groups of cylinders and groups of people based on for example geographical location or role in the organisation.

1.3 About This Manual

Manual Contents
This manual consists of the following parts intended for different target groups:

Section	For Administrators	For Super Administrators	Description
1 Overview	✓	✓	A brief introduction to CLIQ and this manual.
2 Setting Up CWM Clients	✓	✓	Describes how to set up a CWM client.
3 Getting Started with CWM	✓	✓	Describes how to get started when working with CWM for the first time.
4 Working with CWM	✓	✓	Describes how to execute all relevant tasks for administrators when working with a locking system.
5 Setting Up Locking Systems		✓	Describes how to set up a new locking system.
6 Configuring Locking Systems		✓	Describes how to configure various aspects of a locking system.
7 CLIQ Hardware	✓	✓	Describes the CLIQ architecture and components.
8 CLIQ Concepts and Features	✓	✓	Describes how authorisation works, and the concepts of CWM features. Some concepts are very technical and intended for Super Administrators only.
9 Appendix	✓	✓	Contains reference information.

Terminology
For a definition of terms and acronyms used in this manual, see *Section 9.1.1 "Terms", page 179* and *Section 9.1.2 "Acronyms", page 180*.

Menu options in CWM is written as **Main menu » Menu option**.

The following key names differ from the names used in CWM and in this manual:

Key Name	Name in CWM and this Manual
E1	Normal Key
E2	Quartz Key
E3	Dynamic Key

2 Setting Up CWM Clients

2.1 CWM Client Setup Overview

1) Install the Local PD.

   See *Section 2.2 "Installing Local PDs", page 12*.

2) Install CLIQ Connect PC.

   See *Section 2.3 "Installing CLIQ Connect PC", page 12*.

3) Configure CLIQ Connect PC.

   See *Section 2.4 "Configuring CLIQ Connect PC", page 13*.

2.2 Installing Local PDs

1) Ensure that the Windows user account currently logged in has Administrator access rights.
2) Connect the USB cable from the Local PD to the PC.
3) Verify that the drivers are downloaded and installed automatically.

> **NOTE!**
> Make a note of the assigned COM port that is displayed in the notification area. When logging in to CLIQ Express or the CLIQ Go app, select the assigned COM port if the COM port is not found automatically.
>
> Example: `STMicroelectronics Virtual COM Port (COM7).`

4) If the drivers are not installed automatically, contact technical support.

2.3 Installing CLIQ Connect PC

CLIQ Connect PC is a software which handles the communication between the Local PD and CLIQ Web Manager and also generate the C-Key certificates.

Prerequisites:

- The Windows user account currently logged in has Administrator access rights
- The C-Key is already handed out and the C-Key holder has received an email from CLIQ Web Manager.

1) Download and start the CLIQ Connect PC installation file.

   The link to the file can be found in the following locations:

   - The email from CLIQ Web Manager
   - The CWM login-page
   - The Enrolment Welcome page

2) When the installer has loaded, select **language** and click **OK**.

   The CLIQ Connect Setup Wizard opens.

3) Click **Next**.

4) Read the licence agreement. If you accept the agreement, check the **I accept the agreement** radio button (required to continue the setup wizard) and click **Next**.

> **NOTE!**
> Read the **Licence agreement** carefully.

5) Perform one of the following;

- To install CLIQ Connect PC for the first time: Select the destination directly and click **Next**.
- To update an existing installation: Select **Yes** to update the existing installation, or **No** to install in a different directory. Then click **Next** to continue.

6) Set the following external services:

- **Enable automatic updates** allows CLIQ Connect PC to automatically download and install the latest version of the CLIQ Connect PC software.
- Deselect **CLIQ Go** and select **CLIQ Web Manager (C-Key)**.

> **NOTE!**
> The above two settings cannot be altered after the installation or update process.

- **Directory Service Integration** allows CLIQ Connect PC to automatically obtain CLIQ Remote connection details from Central Directory Service. If CLIQ Connect PC should not connect to any external services, deselect **Directory Service Integration**. In this case, **CLIQ Remote URL** and **CLIQ Enrolment URL** have to be provided manually.

7) Click **Next** to continue.

8) To install CLIQ Connect PC for the first time:

Select or create a **Start Menu Folder** for where to place the program shortcuts and click **Next** to continue.

9) Wait while the files are extracted and installed.

10) Select whether to run the program or not when finishing the setup.

11) Click **Finish** to exit the setup.

2.4 Configuring CLIQ Connect PC

2.4.1 Configuring CLIQ Connect PC COM Selector

1) Right-click the **CLIQ Connect** icon in the system tray.

2) Click **COM selector**.

3) Select the COM-port where the Local PD is connected, or click **Auto** (default) for automatic COM-port selection.

2.4.2 Configuring CLIQ Connect PC Server Configuration

1) Right-click the **CLIQ Connect** icon in the system tray.
2) Click **Configuration** and find **Server configuration** section.
3) If Directory Service Integration is enabled:
   a) Select **Automatically**.
   b) Enter the **Directory URL**.
4) If Directory Service Integration is **not** enabled:
   a) Select **Manual**.
   b) Enter **CLIQ Remote URL** and **CLIQ Enrolment URL**.
5) Click **OK** to save and exit.

2.4.3 Configuring CLIQ Connect PC Proxy Settings

1) Right-click the **CLIQ Connect** icon in the system tray.
2) Click **Configuration**.
3) For **Proxy**, select **Enable**.
4) Enter the required information and click **OK**.

3 Getting Started with CWM

3.1 Getting Started with CWM Overview

For new administrators: Go through these steps to get started with CWM.

Prerequisites:

- CWM is set up and configured.
- A C-Key, C-Key certificate, and the C-Key PIN is available.

1) Install the C-Key certificate.

   See *Section 3.2 "Enrolling and Installing C-Key Certificates", page 15*.
2) Log in to CWM.

   See *Section 3.3 "Logging In", page 17*.
3) Set the CWM language.

   See *Section 3.4 "Setting CWM Language", page 18*.
4) Read through *Section 3.5 "Introduction to CWM User Interface", page 18*.

The most common tasks when working with CWM are listed in *Section 3.6 "Common Tasks", page 21*.

3.2 Enrolling and Installing C-Key Certificates

In order to use a C-Key with CWM, a unique certificate must be installed in the CWM client.

The procedure to install a certificate depends on whether to use **DCS Integration** or not.

Certificate Installation with DCS Integration
The C-Key is enrolled and its certificate is generated directly in the Internet browser. There is no need to obtain the certificate separately.

For more information, see *Section 3.2.1 "Enrolling C-Key Certificate via CLIQ Connect PC", page 16*.

Manual Certificate Installation
To install the C-Key certificate manually, a certificate file must be available.

For more information, see *Section 3.2.2 "Installing the C-Key Certificate Manually", page 16*.

3.2.1 Enrolling C-Key Certificate via CLIQ Connect PC

Prerequisites:

- The Local PD is installed.
- The CLIQ Connect PC software is installed on the computer.

  See *Section 2.3 "Installing CLIQ Connect PC", page 12*.
- The C-Key is handed out in CWM.
- The C-Key is allowed to be enrolled.

  Normally a C-Key can be enrolled once, but this setting can be changed by an administrator with the right permissions. For more information, see *Section 6.11.4 "Editing C-Key Information", page 126*.
- The C-Key and the C-Key PIN code are available.

1) Insert the C-Key in the left slot of the Local PD.
2) Right-click the CLIQ Connect icon in the system tray and select **Start certificate enrolment**.
3) Enter the C-Key PIN code and click **Next**.

   If the entered pin is verified, the one time password is sent to the C-Key user's email.
4) Enter the one time password and click **Next**.

   The C-Key certificate is created and added automatically to internet browsers.
5) Click **Done** to finish the C-Key enrolment.

3.2.2 Installing the C-Key Certificate Manually

Prerequisite:

- A **.p12** file for the C-Key along with a password has been obtained.

1) Double-click on the **.p12** file.

   The **Certificate Import Wizard** is displayed.
2) Select **Current User** and click **Next**.
3) Check if the proper certificate is selected and click **Next**.
4) Enter the password which was provided with the **.p12** file and click **Next**.
5) Select **Place all certificates in the following store** and click **Browse**.
6) In the pop-up window, select **Personal** and click **Next**.
7) Confirm the setting and click **Finish**.

   The C-Key certificate is installed in the supported web browsers.

> **NOTE!**
> The C-Key certificate must be re-installed if the Windows user account password is changed by an administrator. (It is not needed when users change their own passwords.)

3.2.3 Renewing C-Key Certificate

When the C-Key certificate has 60 days or less remaining before it expires, a warning message is displayed after log in.

- **With DCS Integration is enabled**:

  An email with the short description about how to renew the certificate is sent to the C-Key holder.

  The certificate is renewed in CLIQ Connect PC and the process is same as the enrolment process. For details, see *Section 3.2.1 "Enrolling C-Key Certificate via CLIQ Connect PC", page 16*.

- **Without DCS Integration**:

  The new certificate is generated in DCS and provided to the C-Key holder.

  To install the new certificate, see *Section 3.2.2 "Installing the C-Key Certificate Manually", page 16*.

HINT!
It is recommended to remove the old certificate from the browser.

3.3 Logging In

Prerequisites:

- The Local PD is installed. See *Section 2.2 "Installing Local PDs", page 12*.
- A supported Internet browser is used. See *Section 9.8 "Client PC Requirements", page 193*.
- The CLIQ Connect software is installed and running on the computer.

  See *Section 2.3 "Installing CLIQ Connect PC", page 12*.
- The CLIQ Connect software is configured and connected to CWM.

  See *Section 2.4 "Configuring CLIQ Connect PC", page 13*.
- A C-Key with a PIN code is available. The C-Key must also be handed out to an employee in CWM.

  NOTE!
  For systems with Single Sign-On (SSO), a key is not required to log in for certain operations once the C-Key certificate has been installed. For further information, see *Section 8.10 "Single Sign-On (SSO)", page 175*.
- A valid certificate for the C-Key is installed. See *Section 3.2 "Enrolling and Installing C-Key Certificates", page 15*.
- A correct URL to CWM is available.

3.3.1 Logging In With C-Key

1) Insert the C-Key in the left slot of the Local PD.
2) Navigate to the CWM start page.
3) Select the certificate for the C-Key.

CWM Login page is shown.

4) Click **Login**.

5) Enter the PIN code for the C-Key.

   The CLIQ Connect PC asks to confirm the usage of the key.

6) Click **Confirm**.

3.3.2 Logging In Without C-Key

1) Navigate to the CWM start page.

2) Select the certificate for the C-Key.

   The CWM Login page is shown.

3) Click **SSO login**.

   In most cases, automatic authentication occurs if your browser is already logged in with corporate domain credentials, allowing direct access to CWM without further action.

   If not, the identity provider sign-in window will appear.

3.4 Setting CWM Language

1) Select **Settings » Select language**.

2) Select desired language.

Language can also be selected by clicking the corresponding flag icon at the login screen.

3.5 Introduction to CWM User Interface

3.5.1 Main Menus

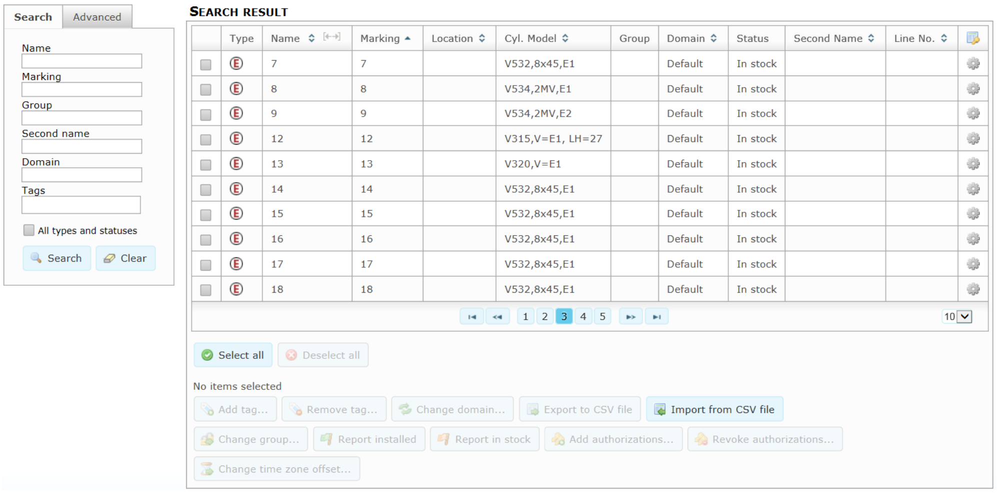
The CWM options are divided into four main menus:

Work	Contains the functions that are most commonly used in daily work.
System Info	Contains functions to administer access rights, employee and visitor information, keys, cylinders and Remote PDs.
Administration	Contains functions to set up and configure the locking system.
Settings	Contains the personal settings related to the administrator logged in.

3.5.2 Searching for Objects

First, use the default search criteria
To search for objects, like cylinders or keys, first select the corresponding menu option, for example, **System Info » Cylinders**.

Initially, a search result based on the default search criteria is displayed.



SEARCH RESULT

□	Type	Name	Marking ▲	Location	Cyl. Model	Group	Domain	Status	Second Name	Line No.	
□	Ⓔ	7	7		V532,8x45,E1		Default	In stock			
□	Ⓔ	8	8		V534,2MV,E1		Default	In stock			
□	Ⓔ	9	9		V534,2MV,E2		Default	In stock			
□	Ⓔ	12	12		V315,V=E1, LH=27		Default	In stock			
□	Ⓔ	13	13		V320,V=E1		Default	In stock			
□	Ⓔ	14	14		V532,8x45,E1		Default	In stock			
□	Ⓔ	15	15		V532,8x45,E1		Default	In stock			
□	Ⓔ	16	16		V532,8x45,E1		Default	In stock			
□	Ⓔ	17	17		V532,8x45,E1		Default	In stock			
□	Ⓔ	18	18		V532,8x45,E1		Default	In stock			

No items selected

Next, use the search functions

Search Criteria To adjust the search criteria, enter new criteria in the search box to the left and click **Search**. In the **Advanced** tab, less commonly used search options are available.

Wildcards When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

Tags When typing in the **Tags** search field, all matching tags appear as a selectable list.

Rows per page Use the arrows below search result to navigate between the pages of large search results. The number of rows displayed per page can be adjusted in the **Rows per page** drop down list.

Sorting ⇕ Click this symbol to sort the search result by the corresponding column.

▲ The search result is sorted by this column (ascending).

▼ The search result is sorted by this column (descending).

Expanding a Column [←→] Click this symbol to expand columns where some entries are too long to fit.

To view detailed information about the object and to configure that object individually, click the object's row.

3.5.3 Configuring Several Objects at the Same Time

Some operations can be performed on many objects simultaneously. The available operations vary depending on the object type.

To configure many objects simultaneously:

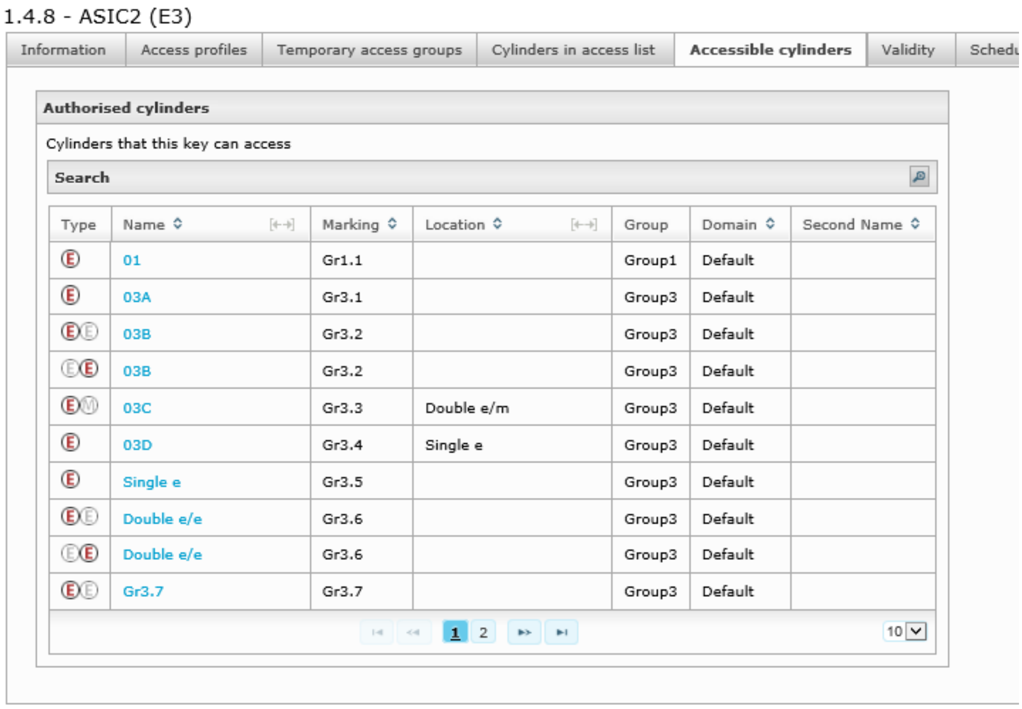
1) Select several individual objects in the leftmost column from one or more search result pages.

   Click **Select all** to select all objects from all pages of the search result.

2) Click the corresponding button at the bottom of the search result box to initiate the operation on the selected objects.

3.5.4 Filtering Long Lists

When viewing lists of, for example, cylinders or keys in access lists, a **Search** banner is visible. See the example below.



Type	Name	Marking	Location	Group	Domain	Second Name
Ⓔ	01	Gr1.1		Group1	Default	
Ⓔ	03A	Gr3.1		Group3	Default	
ⒺⒺ	03B	Gr3.2		Group3	Default	
ⒺⒺ	03B	Gr3.2		Group3	Default	
ⒺⓂ	03C	Gr3.3	Double e/m	Group3	Default	
Ⓔ	03D	Gr3.4	Single e	Group3	Default	
Ⓔ	Single e	Gr3.5		Group3	Default	
ⒺⒺ	Double e/e	Gr3.6		Group3	Default	
ⒺⒺ	Double e/e	Gr3.6		Group3	Default	
ⒺⒺ	Gr3.7	Gr3.7		Group3	Default	

Clicking the 🔍 symbol opens a box of search criteria.

3.5.5 Accessibility

3.5.5.1 Keyboard accessibility

Keyboard navigation is supported throughout CWM for users who cannot use a mouse or other pointing devices, or who prefers to use the keyboard as much as possible.

Interaction	Keystrokes	Notes
Navigate between most elements	• **Tab** • **Shift + Tab** (navigate backwards)	
Buttons	• **Enter** or **Spacebar**	
Checkboxes	• **Spacebar**	Check/uncheck a checkbox.
Comboboxes	• **Spacebar** (Optional. Open list of values). • **Up**/**Down** or **Left**/**Right**	Select a value using the arrow keys (**Up**/**Down** or **Left**/**Right**), then accept using **Enter**.
Tables	• **Up**/**Down** (Navigate table cells) • **Enter** (Enter and view the detailed information)	Navigate the table cells using the arrow keys (**Up**/**Down**).
Radio buttons	• **Up**/**Down** or **Left**/**Right**	Select an option using the arrow keys (**Up**/**Down** or **Left**/**Right**), then navigate to next element using **Tab**.

Interaction	Keystrokes	Notes
Main menu	• **Left**/**Right** (Navigate main menu options) • **Up**/**Down** (Expand/collapse sub menu option) • **Enter** (Enter sub menu option)	Navigate the main menu options, and sub menus, using the arrow keys (**Up**/**Down** or **Left**/**Right**).
Page view	• **Page Up** and **Page Down**	Scroll up and down the web page.
Workflows	• **Alt** + **Left**/**Right**	Navigate between steps.
	• **Alt** + **Q**	Cancel workflow.
	• **Alt** + **Return**	Confirm the final step.
Text editor	• **Alt** + **Q**	Exit the text editor.

3.5.5.2 Viewing Modes

High Contrast Mode
CWM supports High Contrast Mode.

200% Zoom in 1024x768 resolution
It is possible to zoom up to 200% in the browser without losing user interface functionality.

3.6 Common Tasks

This is a list of some of the most common tasks and where to find the corresponding instructions.

Logging In
Section 3.3 "Logging In", page 17

Personnel
Adding an employee or visitor: *Section 4.1.2 "Adding Employees or Visitors", page 23*

User Keys
Handing out keys: *Section 4.2.9 "Handing Out User Keys", page 37*

Receiving keys (Hand-In): *Section 4.2.10 "Receiving User Keys (Hand-In)", page 42*

When keys get lost: *Section 4.2.12.2 "Reporting and Blocking a Lost User Key", page 44*

Authorisations
Viewing keys that can access a cylinder or cylinder group: *Section 3.6 "Common Tasks", page 21*

Viewing cylinders where a key or key group has access: *Section 4.8.2 "Viewing Keys With Access to Cylinders or Cylinder Groups", page 73*

Changing authorisations on a key: *Section 4.9.1 "Configuring Authorisations in Keys", page 74*

Changing authorisations on a cylinder: *Section 4.9.2 "Configuring Authorisations in Cylinders", page 76*

Access Profiles
Associate a key or person with an access profile: *Section 4.9.5 "Selecting Employee or Visitor's Access Profiles", page 79*

Changing authorisations for an access profile: *Section 4.9.4 "Configuring Access Profile Authorisations", page 78*

Audit Trails
Checking keys that accessed a cylinder: *Section 4.11.3 "Viewing Audit Trails for Cylinder", page 87*

Programming
Programming cylinders: *Section 4.4.13 "Programming Cylinders", page 59*

4 Working with CWM

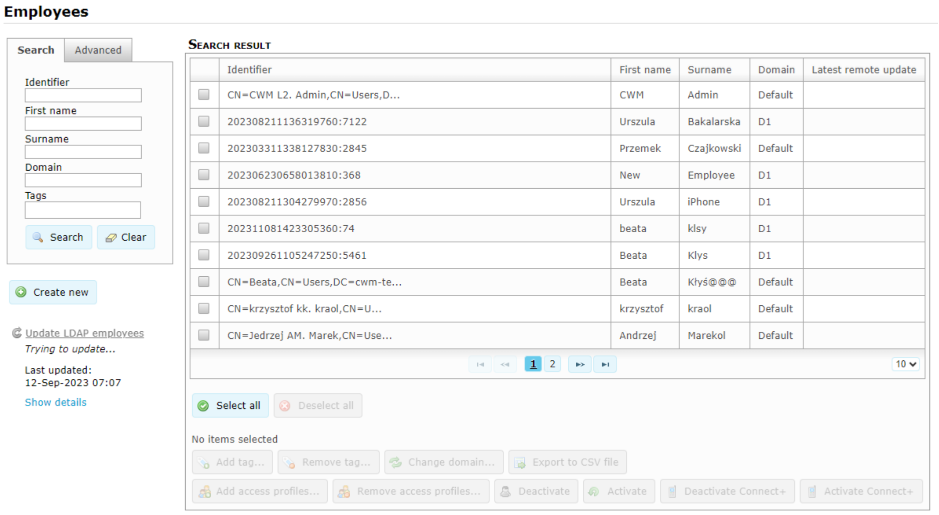
4.1 Managing Employees and Visitors

4.1.1 Searching for Employees or Visitors

1) Select **System Info » Employees** or **Visitors**.

A list of all employees or visitors is displayed.

If LDAP integration is enabled, CWM automatically fetches the latest information from LDAP every 24 hours. The updated date and time are displayed and the detailed information is available by clicking **Show details**. To update manually, click **Update LDAP employees**. For more information about LDAP integration, see *Section 8.12 "LDAP Integration", page 176*.



Employees

Search result

☐	Identifier	First name	Surname	Domain	Latest remote update
☐	CN=CWM L2. Admin,CN=Users,D...	CWM	Admin	Default	
☐	202308211136319760:7122	Urszula	Bakalarska	D1	
☐	202303311338127830:2845	Przemek	Czajkowski	Default	
☐	202306230658013810:368	New	Employee	D1	
☐	202308211304279970:2856	Urszula	iPhone	D1	
☐	202311081423305360:74	beata	klsy	D1	
☐	202309261105247250:5461	Beata	Klys	D1	
☐	CN=Beata,CN=Users,DC=cwm-te...	Beata	Kłyś@@@	Default	
☐	CN=krzysztof kk. kraol,CN=U...	krzysztof	kraol	Default	
☐	CN=Jedrzej AM. Marek,CN=Use...	Andrzej	Marekol	Default	

Update LDAP employees
Trying to update...
Last updated:
12-Sep-2023 07:07
Show details

No items selected

2) Select the **Search** or **Advanced** tab.

The **Advanced** tab includes more search fields as well as the option to search for deleted or deactivated employees or visitors, depending on how CWM is set to handle deleted persons. See *Section 8.9 "Deletion of Personal Data and GDPR Compliance", page 175* for details.

3) Enter the search criteria.

When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

When typing in the **Tags** search field, all matching tags appear as a selectable list.

4) Click **Search**.

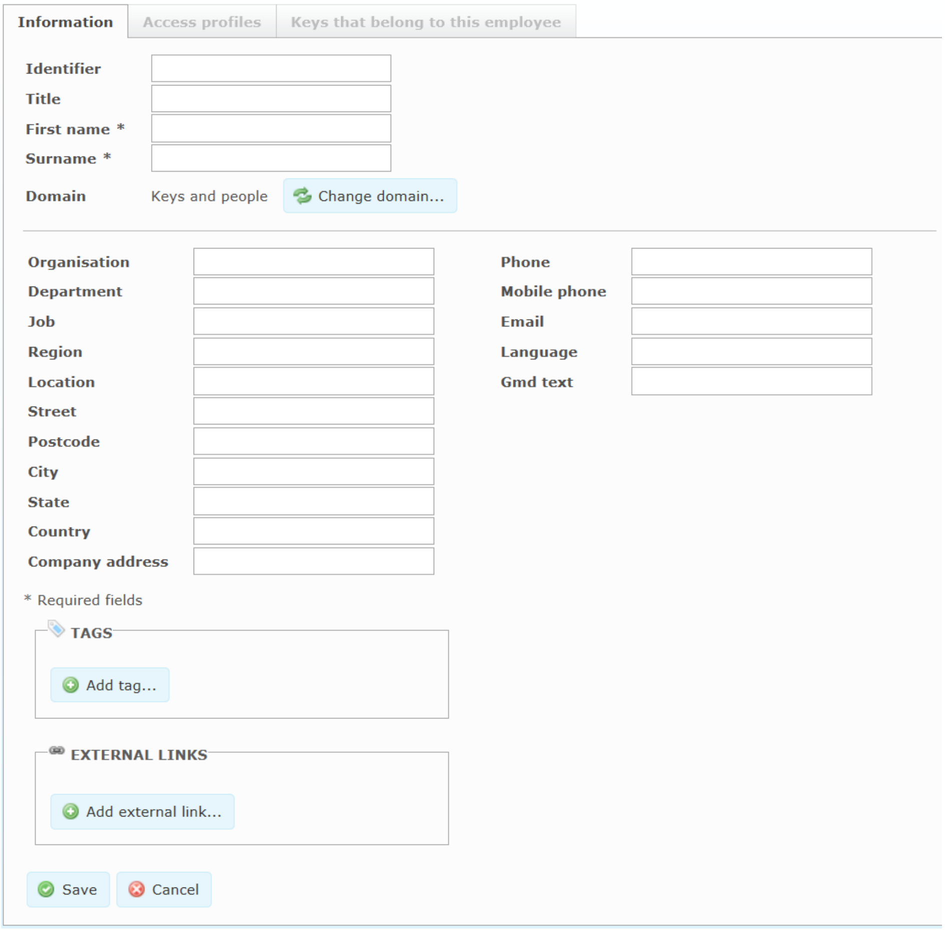
5) To display detailed information about a search result, click the specific employee or visitor.

4.1.2 Adding Employees or Visitors

> **NOTE!**
> The employee information sourced from the LDAP server is read-only.
> The newly created employees in CWM are not added to the LDAP server.

1) Select **System Info » Employees** or **Visitors**.

2) Click **Create new**.



Domain Keys and people

3) Enter the information.

First name and **Surname** are required fields.

Email address is required for sending reminders for overdue keys and the use of the DCS integration feature for new C-Key holders.

If the CLIQ Connect+ feature is enabled for the system and will be activated for the new employee or visitor, the email address must not be the same as one registered for another CLIQ Connect+ user.

For employees, the field **Identifier** is also used. The identifier must be unique. If this field is not entered, CWM will add a unique identifier in the format yyyy-mm-dd:running number.

4) To add a tag, click **Add tag...**. See also *Section 4.1.7 "Adding or Removing Employee or Visitor Tags", page 30*.

5) To add an external link, click **Add external link...**. See also *Section 4.1.8 "Managing Employee or Visitor External Links", page 31*.

6) Click **Save**.

4.1.3 Deactivating or Activating Employees or Visitors

Prerequisites:

- For deactivating, as well as searching for and reactivating deactivated employees or visitors, the administrator needs to have the permission **Key holder: Deactivate**.

  For more information about managing permissions, see *Section 6.7 "Managing Roles and Permissions", page 119*.
- In **System settings**, **Delete permanently** is selected in the **When deleting person** section.

  For more information about managing **System settings**, see *Section 6.4 "Editing System Settings", page 94*.
- The following employees or visitors cannot be deactivated:
  - Employees or visitors with handed out keys.
  - The employees integrated with LDAP.
  - Activated CLIQ Mobile Manager users.

1) Select **System Info » Employees** or **System Info » Visitors**.

   A list of all employees or visitors is displayed.

   > **HINT!**
   > Deactivated or active employees or visitors can be filtered using the **Show deactivated** filter in the **Advanced** tab.

   If necessary, enter the search criteria.

   When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

   When typing in the **Tags** search field, all matching tags appear as a selectable list.

   - To activate or deactivate individual employee or visitor, go to *Step 2*.
   - To activate or deactivate multiple employees or visitors simultaneously, go to *Step 3*.

2) **Activating or Deactivating Individual Employee or Visitor**

   1. Select the employee or visitor and go to its detailed information view.
   2. **To Deactivate an Employee or Visitor**

      a) In the information view, click **Deactivate**.

      b) In the pop-up window, click **Deactivate**.

      To Activate an Employee or Visitor

      a) In the information view, click **Activate**.

      b) In the pop-up window, click **OK**.

3) **Activating or Deactivating Multiple Employees or Visitors**

1. Select employees or visitors to deactivate or activate from the search results by checking the checkboxes.
2. **To Deactivate Employees or Visitors**

   a) Click **Deactivate** under the search results.

   b) In the pop-up window, click **Deactivate**.

   To Activate Employees or Visitors

   a) Click **Activate** under the search results.

   b) In the pop-up window, click **OK**.

4.1.4 Deleting or Restoring Employees or Visitors

In the **System settings**, the deletion of employees or visitors can be configured to either **Mark as deleted** or **Delete permanently**.

- When **Mark as deleted** is selected, the deleted employees or visitors can be restored if needed.
- When **Delete permanently** is selected, deleted employees or visitors **can not** be restored.

See also *Section 6.4 "Editing System Settings", page 94* and *Section 8.9 "Deletion of Personal Data and GDPR Compliance", page 175*.

1) Find the employee or visitor and go to its detailed information view.

   See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

   HINT!
   Deleted users can be filtered using the **Show deleted** filter in the **Advanced** tab.

2) **To Delete the Employee or Visitor:**

   NOTE!
   The following people cannot be deleted:

   - Employees or visitors with handed out keys.
   - LDAP integrated employees.
   - Activated CLIQ Connect+ users.

1. In the detailed information view, click **Delete**.
2. In the pop-up window, click **Delete**.

To Restore the Employee or Visitor:

1. In the detailed information view, click **Restore**.
2. In the pop-up window, click **Restore**.

4.1.5 Activating or Deactivating CLIQ Connect+ Access for Employees or Visitors

If CLIQ Connect+ is enabled to the system then employees and visitors can check the detailed information for their keys via CLIQ Connect. To use this feature, the administrator needs to activate the CLIQ Connect+ user status.

There are two ways to activate or deactivate the user status:

- To change the status individually, follow the instruction in *Section 4.1.5.1 "Configuring CLIQ Connect+ Access Individually", page 27*.
- To activate or deactivate more than one employee or visitor at the same time, follow the instruction in *Section 4.1.5.2 "Configuring CLIQ Connect+ Access for Multiple Employees", page 28*.

For more details about CLIQ Connect+, see *Section 8.3.4 "CLIQ Connect and CLIQ Connect+", page 168*.

Prerequisites:

- The administrator has fetched and installed the license **CLIQ Connect+**.

  To install the new license, see *Section 6.1.1 "Installing Licences", page 93*.
- The employee or visitor's email address must not belong to another CLIQ Connect+ user.

4.1.5.1 Configuring CLIQ Connect+ Access Individually

1) Find the employee or visitor and go to its detailed information view.

   See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

   HINT!
   Deactivated or deleted users can be filtered out using the filter in the **Advanced** tab.

2) Activate or deactivate the CLIQ Connect+ user status:

   To Activate the CLIQ Connect+ User Status:
   Click **Activate Connect+**.

   NOTE!
   If the email address is not entered or is already taken by another employee or visitor who has activated CLIQ Connect+, the **Activate Connect+** button is disabled.

   Click **Edit** and enter a unique email address.

   An email with information about the CLIQ Connect configuration is sent to the specified email address.

   The administrator can also manually send the email by clicking the **Resend email** button to a CLIQ Connect+ user.

   - If CLIQ Connect+ is not activated by the key holder, the email contains information about how to activate the account.
   - If CLIQ Connect+ is activated by the key holder, the email contains information about how to sign into the account.

To Deactivate the CLIQ Connect+ User Status:

1. To deactivate: Click **Deactivate Connect+**.
2. Click **Deactivate**, in the pop-up window.

4.1.5.2 Configuring CLIQ Connect+ Access for Multiple Employees

1) Find the employee or visitor and go to its detailed information view.

   See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

> **HINT!**
> Deactivated or deleted users can be filtered using the filter in the **Advanced** tab.

2) Select the employees and visitors by checking the checkboxes.

> **NOTE!**
> A maximum of 500 employees or visitors can be selected at the time to deactivate the CLIQ Connect+ user status.

3) **To Activate the CLIQ Connect+ User Status:**

> **NOTE!**
> The CLIQ Connect+ user status is not activated to the following employee or visitor:
>
> - does not have a email address registered.
> - has the same email address as another CLIQ Connect+ activated employee or visitor.
> - already has user status activated.

1. Click **Activate Connect+**.

   The information window pops up.

2. Click **Activate** in the pop-up window.

   An email with information about the CLIQ Connect configuration is sent to the specified email address.

   The administrator can also manually send the email to a CLIQ Connect+ user via the individual information view by clicking the **Resend email** button.

   – If CLIQ Connect+ is not activated by the key holder, the email contains information about how to activate the account.
   – If CLIQ Connect+ is activated by the key holder, the email contains information about how to sign into the account.

To Deactivate the CLIQ Connect+ User Status:

1. Click **Deactivate Connect+**.

   The information window pops up.

2. Click **Deactivate** in the pop-up window.

The result of the operation is displayed above the **SEARCH RESULT** table.

4.1.6 Editing Employee or Visitor Information

To edit employee or visitor information in CWM, see *Section 4.1.6.2 "Editing Employee or Visitor Information in CWM", page 30*.

Employee information can also be edited by importing an updated CSV file or via LDAP if the system is LDAP integrated. For more information about how to import employee information, see *Section 4.1.11 "Importing Employee Information", page 32*. For more information about LDAP integration, see *Section 8.12 "LDAP Integration", page 176*.

> **NOTE!**
> There are limitations in editing or deleting the email address for an employee or visitor with the CLIQ Connect+ user status activated. For more information, see *Section 4.1.6.1 "Important information about Editing or Deleting Email Address", page 29*.

4.1.6.1 Important information about Editing or Deleting Email Address

When CLIQ Connect+ is Activated
Employees or visitors with the activated CLIQ Connect+ user status log into the CLIQ Connect with the email address registered in CWM. Editing or deleting their email address, therefore, will affect login process to the CLIQ Connect.

Editing

- Editing the email address to a unique email address changes the log in credentials in CLIQ Connect.

  An email with information about the CLIQ Connect configuration is sent to the specified email address.

  - If the CLIQ Connect+ account is not activated by the key holder, the email contains the account activation code.
  - If the CLIQ Connect+ account is activated by the key holder, the email contains information about how to sign into the account.
- Editing the email address to an email address which already belongs to another CLIQ Connect+ user is not allowed in CWM.

  Such a change of email address via LDAP integration or CSV file is skipped and treated as an error.

Deleting

- Deleting the email address in CWM:

  Deletion deactivates the CLIQ Connect+ user status.
- Deleting the email address via LDAP integration or CSV file:

  Deletion is not allowed if the CLIQ Connect+ account is activated by the key holder.

When SSO Login is Enabled
Once a C-Key is assigned to an employee, their associated email address can no longer be edited or deleted.

4.1.6.2 Editing Employee or Visitor Information in CWM

This section shows how to edit the employee or visitor information in CWM.

Prerequisites:

- The employee or visitor to be edited should be active.
- The employee to be edited is not LDAP integrated.

> **NOTE!**
> In case of LDAP integrated employee, only **Domain** and **TAGS** can be changed.

1) Find the employee or visitor and go to its detailed information view.

   See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

2) Click **Edit**.

3) Update the fields.

   - To edit tags, see *Section 4.1.7 "Adding or Removing Employee or Visitor Tags", page 30*.
   - To edit external links, see *Section 4.1.8 "Managing Employee or Visitor External Links", page 31*.

4) Click **Save**.

> **NOTE!**
> Editing this information may result in email notifications being sent to the domain administrator for appropriate actions. Notifications will only be sent if activated in **System settings**.
>
> See also *Section 6.4 "Editing System Settings", page 94*.

4.1.7 Adding or Removing Employee or Visitor Tags

For information about tags, see *Section 8.2.6 "Tags", page 166*.

Prerequisite:

- The employees or visitors to be edited should be active.

1) Select **System Info » Employees** or **Visitors**.

   A list of all employees or visitors is displayed.

   - To add or remove tags for individual employee or visitor, go to *Step 2*.
   - To add or remove tags for multiple employees or visitors simultaneously, go to *Step 3*.

2) **Add or Remove Tags for an Individual Employee or Visitor:**

   1. Select the employee or visitor and go to its detailed information view.
   2. Click **Edit**.
   3. Add or remove a tag for individual employee or visitors.

To Add a Tag:

a) Click **Add tag...**.

b) Enter a name for the tag.

c) Click **OK**.

To Remove a Tag:
Click the tag to be removed.

4. Click **Save**.

3) **Add or Remove Tags for Multiple Employees or Visitors:**

1. Select employees or visitors from the search results by checking the checkboxes.

2. **To Add a Tag:**

a) Click **Add tag...**.

b) Enter a name of the tag.

c) Click **OK**.

To Remove a Tag:

a) Click **Remove tag...**.

b) Enter a name of the tag.

c) Click **OK**.

4.1.8 Managing Employee or Visitor External Links

For information about external links, see *Section 8.4 "External Links", page 169*.

Prerequisite:

- The employees or visitors to be edited should be active.

1) Find the employee or visitor and go to its detailed information view.

See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

2) Click **Edit**.

3) **To Add an External Link:**

1. Click **Add.**

2. Enter **Name** for the URL.

3. Enter **URL**. The **URL** must start with a protocol (for example http:// or ftp://).

If a root URL has been defined in **System settings** (item **External links root URL**), it is only necessary to add the last part of the URL. See also *Section 6.4 "Editing System Settings", page 94*.

4. Click **OK**.

To Edit an External Link:

1. Click **Edit** on the external link to be edited.

2. Update the fields.
3. Click **OK**.

To Remove an External Link:
Click **Remove** on the external link to be removed.

4) Click **Save**.

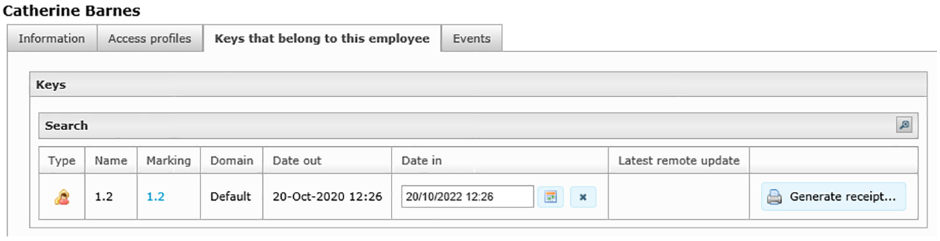
4.1.9 Viewing Employee or Visitor Keys

1) Find the employee or visitor and go to its detailed information view.

   See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

2) Select the **Keys that belong to this employee** or **Keys that belong to this visitor** tab.

   Keys currently handed out to the employee or visitor are displayed.



Type	Name	Marking	Domain	Date out	Date in	Latest remote update	
	1.2	1.2	Default	20-Oct-2020 12:26	20/10/2022 12:26		Generate receipt...

3)
- To change hand-in date for a key, edit the **Date in** field.
- To generate a receipt of the hand out and hand in of the key, click **Generate receipt...**.
- To display the detailed information view of the key, click the key marking.

4.1.10 Viewing Events for Employee or Visitor

The **Events** tab provides a record of administrative activities within CWM, including actions such as creating an employee or visitor and updating the status of CLIQ Connect+. It also logs key-related events associated with the employee or visitor.

1) Find the employee or visitor and go to its detailed information view.

   See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

2) In the detailed information view, select the **Events** tab.

   A list of employee or visitor events is displayed.

4.1.11 Importing Employee Information

Importing employees enables the mass import of new or updated employee data.

> **NOTE!**
> Employees added through LDAP integration cannot be edited through CSV import.

Prerequisite:

- Create a CSV import file following the format information in *Section 9.9 "Employee Import File Format", page 193*.

1) Select **Administration » Import employees**.

2) Click **Select...**.

3) Choose the file to upload and click **Open**.

4) Click **Upload**.

   Information on how many valid entries the file contains is displayed. If there are any invalid entries, click **Details** for more information.

5) Click **Import**.

4.1.12 Exporting Employee or Visitor Information

1) Search for the employees or visitors.

   See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

2) From the search results, select the employees or visitors whose information should be exported.

3) Click **Export to CSV file**.

   Information about deactivated employees or visitors cannot be exported.

> **NOTE!**
> To be able to open the file in Excel in the correct way, the delimiter for the file must be set according to regional settings. To change the delimiter, see *Section 6.4 "Editing System Settings", page 94*.

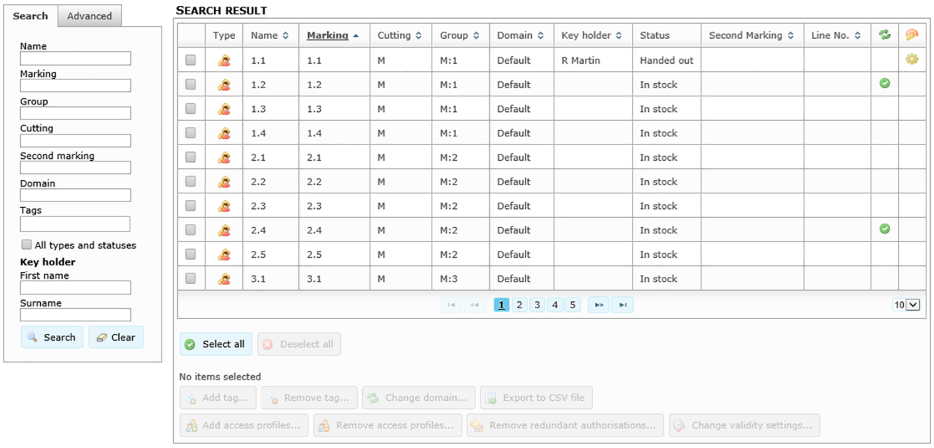
4) In the file download pop-up window, click **Open** or **Save**.

4.2 Managing Keys

4.2.1 Searching for User Keys

1) Select **System Info » Keys**.

   A list of all keys is displayed.



SEARCH RESULT

	Type	Name	Marking	Cutting	Group	Domain	Key holder	Status	Second Marking	Line No.		
□		1.1	1.1	M	M:1	Default	R Martin	Handed out				⚙
□		1.2	1.2	M	M:1	Default		In stock			✓	
□		1.3	1.3	M	M:1	Default		In stock				
□		1.4	1.4	M	M:1	Default		In stock				
□		2.1	2.1	M	M:2	Default		In stock				
□		2.2	2.2	M	M:2	Default		In stock				
□		2.3	2.3	M	M:2	Default		In stock				
□		2.4	2.4	M	M:2	Default		In stock			✓	
□		2.5	2.5	M	M:2	Default		In stock				
□		3.1	3.1	M	M:3	Default		In stock				

No items selected

Add tag...
Remove tag...
Change domain...
Export to CSV file
Add access profiles...
Remove access profiles...
Remove redundant authorisations...
Change validity settings...

The following symbols are used:

Mechanical Key

Normal Key

Quartz Key

CLIQ Connect Quartz Key

Dynamic Key

CLIQ Connect Dynamic Key

Pending remote update exists for the key

2) Select the **Search** or **Advanced** tab.

By default, mechanical keys and keys reported lost or broken are not displayed. To include also these keys in the search result, select **All types and statuses**.

The **Advanced** tab also includes the search fields type of key, CLIQ Connect key, inventory status and operational status.

3) Enter the search criteria.

When typing in the **Tags** search field, all matching tags appear as a selectable list.

When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

4) Click **Search**.

5) To display detailed information on a search result, click the row of the specific key.

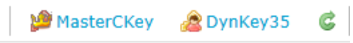
For information about the key attributes, see *Section 9.3.3 "Key Attributes", page 183*.

4.2.2 Scanning a User Key

1) Insert the key into the right slot of the Local PD.

2) Click ↻ in the upper right corner of the page.

Both keys in the Local PD are shown below the navigation bar.



3) Click the key in the right slot of the Local PD.

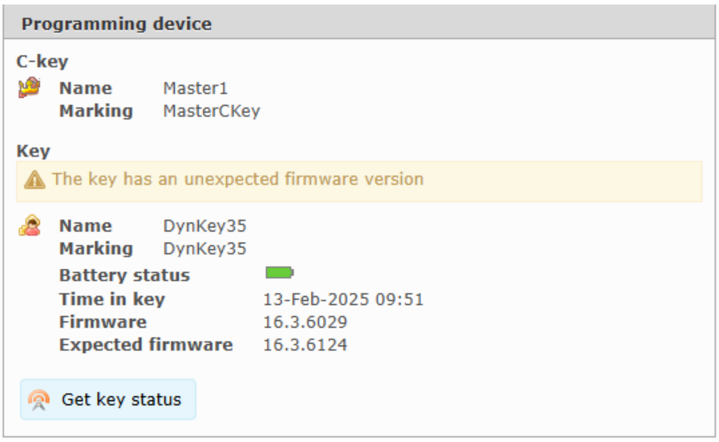
The key's detailed information view is displayed, with the key's **Name** and **Marking** shown on the right-hand side of the page.

4.2.3 Viewing Key Status

1) Scan the key. See *Section 4.2.2 "Scanning a User Key", page 34*.

2) Click **Get key status**.

Basic information about the key is displayed. For more information about the battery status indicator, see *Section 9.6 "Battery Level Indications", page 191*.



Programming device

C-key

Name Master1
Marking MasterCKey

Key

⚠ The key has an unexpected firmware version

Name DynKey35
Marking DynKey35
Battery status 🟩
Time in key 13-Feb-2025 09:51
Firmware 16.3.6029
Expected firmware 16.3.6124

4.2.4 Editing User Key Information

1) Find the key and go to its detailed information view.

   To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Click **Edit**.

3) To edit the key name, update the field **Name**.

4) To add a tag, click **Add tag**.

   See also *Section 4.2.5 "Adding or Removing User Key Tags", page 35*.

5) To add an external link, click **Add external link**.

   See also *Section 4.2.6 "Managing User Key External Links", page 36*.

6) Click **Save**.

4.2.5 Adding or Removing User Key Tags

For information about tags, see *Section 8.2.6 "Tags", page 166*.

1) Find the key to edit.

   To search for the key, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD, see *Section 4.2.2 "Scanning a User Key", page 34*

2)
   - To add or remove tags for individual key, go to *Step 3*.
   - To add or remove tags for multiple keys, go to *Step 4*.

3) **Add or Remove Tags for an Individual or Key:**

   1. Select the key and go to its detailed information view.
   2. Click **Edit**.
   3. Add or remove tag for individual key.

      To Add a Tag:

      a) Click **Add tag...**.

      b) Enter a name for the tag.

      c) Click **OK**.

To Remove a Tag:
Click the tag to be removed.

4. Click **Save**.

4) **Add or Remove Tags for Multiple Keys:**

   1. Select keys from the search results by checking the checkboxes.
   2. **To Add a Tag:**

      a) Click **Add tag...**.

      b) Enter a name of the tag.

      c) Click **OK**.

      To Remove a Tag:

      a) Click **Remove tag...**.

      b) Enter a name of the tag.

      c) Click **OK**.

4.2.6 Managing User Key External Links

For information about external links, see *Section 8.4 "External Links", page 169*.

1) Find the key and go to its detailed information view.

   To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Click **Edit**.

3) To add an external link:

   a) Click **Add**.

   b) Enter **Name** for the URL.

   c) Enter **URL**. The **URL** must start with a protocol (for example http:// or ftp://).

   If a root URL has been defined in **System settings** (item **External links root URL**), it is only necessary to add the last part of the URL. See also *Section 6.4 "Editing System Settings", page 94*.

   d) Click **OK**.

4) To edit an external link:

   a) Click **Edit** on the external link to be edited.

   b) Update the fields.

   c) Click **OK**.

5) To remove an external link: Click **Remove** on the external link to be removed.

6) Click **Save**.

4.2.7 Viewing Update History for User Key

The **Update history** tab is used for traceability of key programming.

Prerequisites:

- The user permission level should be **View** in the role **Key: Update history**.

  To change the permission level, see *Section 6.7 "Managing Roles and Permissions", page 119*.

-

1) Find the key and go to its detailed information view.

   To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Select the **Update history** tab.

   A list with all key updates is displayed.

   > **NOTE!**
   > By default, key updates, with exception of firmware updates, are deleted after 3 months.

   The following symbols are used:

   ⚙ Programming job for a local PD exists but has not been initiated

   ⚙ Pending remote update exists for the key

   ⚙ Programming Job has been finished

   ⚙ Programming Job has failed or been cancelled

   ⚙ Programming Job has been replaced with a new job

3) To display further details on a specific update, click the link in the **Reason** column.

4.2.8 Viewing Events for User Key

The Events tab is used for traceability of administrator operations in the CWM, such as handing out a key, associating access profiles, changing key authorisations, etc.

1) Find the key and go to its detailed information view.

   To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Select the **Events** tab.

   A list with all key events is displayed.

4.2.9 Handing Out User Keys

The hand out process has two phases:

1. **Hand out settings**

   In this phase, hand out settings are configured in three different pages; **General**, **Accesses** and **Time settings**.

It is mandatory to complete the settings in the **General** page, but setting in the other pages is optional.

2. **Summary of hand out**

In this phase, the hand out details are confirmed and the key is handed out. . If the handed out key is inserted in the PD it will also be programmed.

1) There are two ways to start the handing out process:

- Select **Work » Hand out key » To employee** or **To visitor**.
- From the employee or visitor detailed information view:

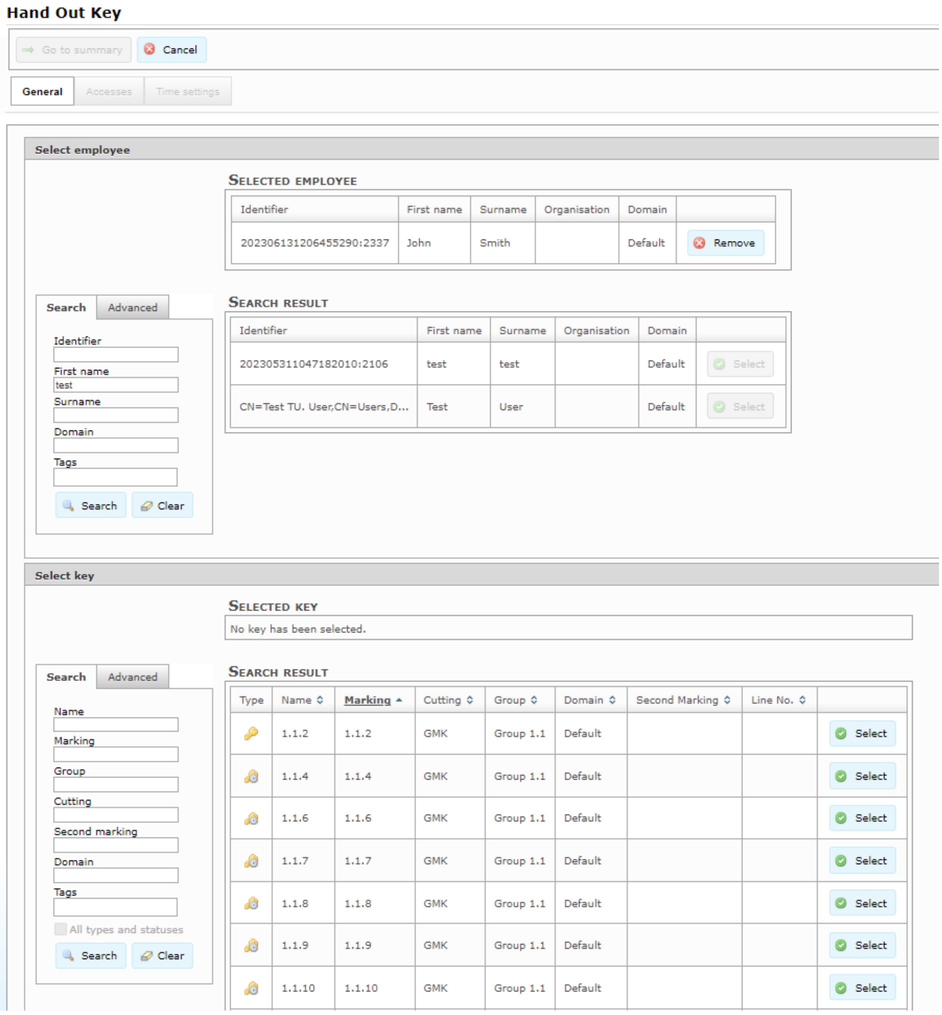
  a) Find the key and go to its detailed information view.

  To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

  To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

  b) Click **Hand out key**.

The **Hand Out Key**, **General** page is opened.



Select employee

SELECTED EMPLOYEE

Identifier	First name	Surname	Organisation	Domain	
202306131206455290:2337	John	Smith		Default	Remove

Identifier

First name: test

Surname

Domain

Tags

SEARCH RESULT

Identifier	First name	Surname	Organisation	Domain	
202305311047182010:2106	test	test		Default	Select
CN=Test TU. User,CN=Users,D...	Test	User		Default	Select

Select key

SELECTED KEY

No key has been selected.

Name

Marking

Group

Cutting

Second marking

Domain

Tags

□ All types and statuses

SEARCH RESULT

Type	Name	Marking	Cutting	Group	Domain	Second Marking	Line No.	
🔑	1.1.2	1.1.2	GMK	Group 1.1	Default			Select
🔑	1.1.4	1.1.4	GMK	Group 1.1	Default			Select
🔑	1.1.6	1.1.6	GMK	Group 1.1	Default			Select
🔑	1.1.7	1.1.7	GMK	Group 1.1	Default			Select
🔑	1.1.8	1.1.8	GMK	Group 1.1	Default			Select
🔑	1.1.9	1.1.9	GMK	Group 1.1	Default			Select
🔑	1.1.10	1.1.10	GMK	Group 1.1	Default			Select

2) If there is no selected employee or guest in the **Select employee** or **Select visitor** section, find the person and click **Select**.

To search for a specific employee or visitor, see *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

3) Select the key to hand out in one of the following ways:

- If the key to hand out is at hand:

  a) Insert the key in the right slot of the Local PD.

  b) Click ⟳ in the upper right corner of the page to scan the key.

  c) In the **User Key in PD** box, click **Select**.

  Handing out a key using the scanning function is in most cases the recommended choice since the new configuration can be programmed to the key immediately. This is especially important for non-remote systems.

- If the key to hand out is not at hand:

  a) Find the key to hand out either in the following lists and click **Select**.

  - The **PRE-ORDERED KEY** list

    If there is any pre-ordered keys to the selected person, the pre-ordered key list is displayed in the key selection view.

    > **HINT!**
    > A pre-ordered key is a key which is connected to a particular person when the key is ordered.
    >
    > By connecting the key to the particular person, it helps administrators to select the right key for the selected person during the handing out process.
    >
    > The key status stays **In stock** after the key is imported to the system regardless the physical key has arrived from the CLIQ dealer or not.
    >
    > The key can be handed out to anyone, and loses the pre-order feature once it is handed out.

  - The **SEARCH RESULT** list

    To narrow the list, enter the search criteria and click **Search**. See also *Section 4.2.1 "Searching for User Keys", page 33*.

4) If required, set the details in the **Accesses** page and **Time settings** page.

Otherwise, skip to *Step 5*.

> **NOTE!**
> All of the following settings are applicable for Dynamic Keys in cylinder group remote systems. For other key types and configurations, some of the settings are not available.

The Accesses page

- **Select access profiles**

  Select access profiles from the list.

By default, the employee or visitor access profiles are selected.

- **Select cylinder groups**

  Select the cylinder groups to which the key will have explicit access.

- **Select cylinders**

  Select the cylinders to which the key will have explicit access.

The Time Settings page

- **Set key validity**

  – SELECT HAND OUT AND HAND IN DATES

    Enter hand out date (**Date out**) and hand in date (**Date in**):

    If key hand in date is not yet determined, click **X**.

  – SET KEY VALIDITY

    Set the following settings for key validity.

    - Select activation settings among **Inactive**, **Active between selected dates** and **Always active**.

      If **Active between selected dates** is selected, set **Key active from** and **Key active to** dates.

      If the **Key active to** date is not yet determined, click **X**.

    - To use revalidation, check the box of **Use revalidation** and set the interval period.

      When it is set, the key has to be updated at the specified time interval to stay active.

    - **CLIQ Connect keys only**:

      To use **PIN validation**, check box and set the interval period.

      When it is set, the key has to be PIN validated using the CLIQ Connect at specified time intervals to stay active.

    For more information about the key validity, see *Section 8.1.4 "Key Validity", page 154*.

- **Select key schedule**

  KEY SCHEDULE

  Set the key schedule as follows:

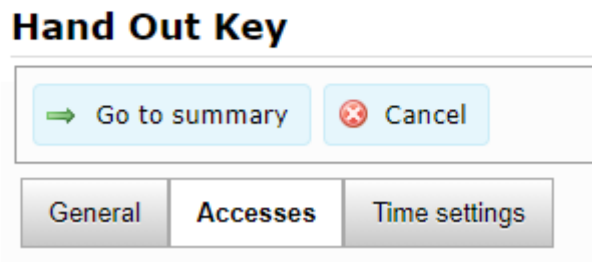
  a) If there is a schedule template to use, select from the drop-down list and click **Apply**.

  b) Click **Add period** to add a time period to the selected template or to customise the schedule.

  c) Click **Add cylinder** to set a specific time period to a cylinder.

Select a cylinder from the list displayed, and click **Add period** to set the period.

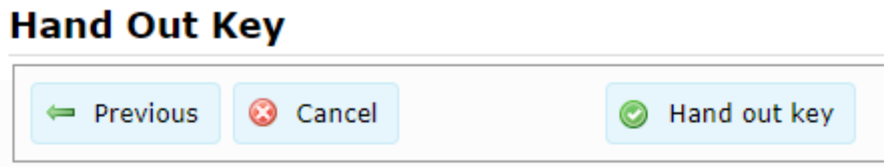
5) Click **Go to summary**.



A summary of the access rights and time settings is displayed.

6) Check the settings.

To change the settings, click **Previous** to go back to the setting pages.



7)
- If the hand out key is in the Local PD, click **Program and Save**.

  The key is directly programmed in the PD.
- If the hand out key is not in the Local PD, click **Hand out key**.

  A remote update job is created in remote systems.

8) Optional: Create a receipt.

Receipts are created as PDFs which can either be printed or saved.

To create or edit receipt templates, refer to *Section 6.9 "Managing Receipt Templates", page 122*.

a) Click **Generate receipt...**.

The **Receipt selection** window pops up.

b) Choose the appropriate language from the drop-down list.

c) Choose the appropriate template from the drop-down list.

In the drop-down list, all handout receipt templates in the selected language are shown.

d) Click **Generate receipt** or **Download**.

9) Optional: Issue a QR code for configuring the CLIQ Remote server URL and hand it out with the key.

If the key holder is going to use CLIQ Connect and the CWM system is not DCS integrated, the key holder needs to enter the CLIQ Remote server URL manually in CLIQ Connect. Generating a QR code for the CLIQ Remote server URL and giving it to the key holder simplifies the process of the app configuration.

a) Open any kind of online QR generator.

b) Enter the information in this order: `<ASSA ABLOY operating company code>, <MKS name>, <URL>`

Example:
`3,CLIQConnectTeam,https://app-team-remote.cliqapps.aa.st:443/CLIQRemote`

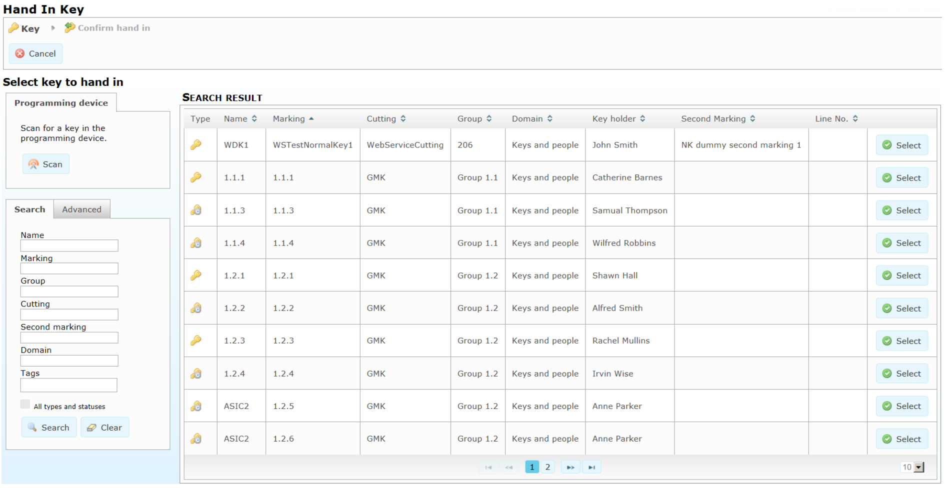
For ASSA ABLOY operating company code, refer to *Section 9.10 "ASSA ABLOY Operating Company Code", page 195*.

c) Print the QR code out.

4.2.10 Receiving User Keys (Hand-In)

1) Select **Work » Hand in key**.

A list of all keys handed out is displayed.



Type	Name	Marking	Cutting	Group	Domain	Key holder	Second Marking	Line No.	
🔑	WDK1	WSTestNormalKey1	WebServiceCutting	206	Keys and people	John Smith	NK dummy second marking 1		Select
🔑	1.1.1	1.1.1	GMK	Group 1.1	Keys and people	Catherine Barnes			Select
🔑	1.1.3	1.1.3	GMK	Group 1.1	Keys and people	Samual Thompson			Select
🔑	1.1.4	1.1.4	GMK	Group 1.1	Keys and people	Wilfred Robbins			Select
🔑	1.2.1	1.2.1	GMK	Group 1.2	Keys and people	Shawn Hall			Select
🔑	1.2.2	1.2.2	GMK	Group 1.2	Keys and people	Alfred Smith			Select
🔑	1.2.3	1.2.3	GMK	Group 1.2	Keys and people	Rachel Mullins			Select
🔑	1.2.4	1.2.4	GMK	Group 1.2	Keys and people	Irvin Wise			Select
🔑	ASIC2	1.2.5	GMK	Group 1.2	Keys and people	Anne Parker			Select
🔑	ASIC2	1.2.6	GMK	Group 1.2	Keys and people	Anne Parker			Select

2) Find and select the key to hand in by one of the following ways:

- From the list, click **Select** for the key to hand in.

  To search for the key, enter the search criteria and click **Search**. See also *Section 4.2.1 "Searching for User Keys", page 33*.

- If the key to hand in is in the right slot of the Local PD, click ⟳ in the upper right corner of the page to scan the key.

  Handing in a key using the scanning function is in most cases the recommended choice since the new configuration can be programmed to the key immediately. This is especially important for non-remote systems.

3) To hand in a key:

- If the key handed in is scanned in the Local PD, click **Reset key and hand in** or **Hand in key without resetting**.

  The resetting option is useful for keys that will have different settings with each hand out and is the recommended option in most cases.

- If the key handed in is not scanned, click **Apply**.

4) Optional: Create a receipt. Receipts are created as PDFs which can either be printed or saved.

> **NOTE!**
>
> This option is only available if **Separate hand in and hand out receipts** is selected in **System Settings**. This setting is found by selecting **Administration » System Settings » ADMINISTRATION » Key receipts**.
>
> For more information on how to edit system settings, see *Section 6.4 "Editing System Settings", page 94*.

To create or edit receipt templates, see *Section 6.9 "Managing Receipt Templates", page 122*.

a) Click **Generate receipt...**.

The **Receipt selection** window pops up.

b) Choose the appropriate language from the drop-down list.

c) Choose the appropriate template from the drop-down list.

In the drop-down list, all hand in receipt templates in the selected language are shown.

d) Click **Print receipt** or **Download**.

If **Download** is selected, the receipt is downloaded to the **Downloads** folder.

4.2.11 Printing an Empty Receipt

When a key is handed out or handed in, the receipt is generated in the PDF format with the hand-in or hand-out information. It is also possible to generate receipts which fields are left blank to be edited manually.

1) **Work » Receipt**.

2) Select either **Print empty hand out receipt...** or **Print empty hand in receipt...**.

3) In the pop-up window:

   a) Select the appropriate language from the drop-down list.

   b) Select the appropriate template to use.

   When **Custom** is selected, all templates in the same type (template for hand out or hand in) in the selected language are shown in the drop-down list.

4) Click **Generate receipt** or **Download**.

4.2.12 Handling a Lost or Broken Key

This section describes how to report user keys lost or broken. For reporting lost or broken C-Key, see *Section 6.11.9 "Reporting and Blocking a Lost C-Key", page 129* or *Section 6.11.10 "Reporting Broken or Operational C-Key", page 131*.

4.2.12.1 Reporting a Broken User Key

1) There are two ways to start reporting the broken key:

   - Select **Work » Report key broken**. Proceed to *Step 2*.

- On the detailed information view of the broken key (for searching the key, see *Section 4.2.1 "Searching for User Keys", page 33*), click the **Report broken** button. Proceed to *Step 4*.

2) Enter the search criteria to find the owner of the key and click **Search**.
3) Select the broken key.
4) Click **Apply**.

   The detailed information view for a key reported as broken will contain the option of removing the broken status.

If the broken key is replaced with a clone key, see *Section 4.2.13 "Replacing a User Key with a Clone from the Factory", page 47* for further instructions.

4.2.12.2 Reporting and Blocking a Lost User Key

Prerequisite:

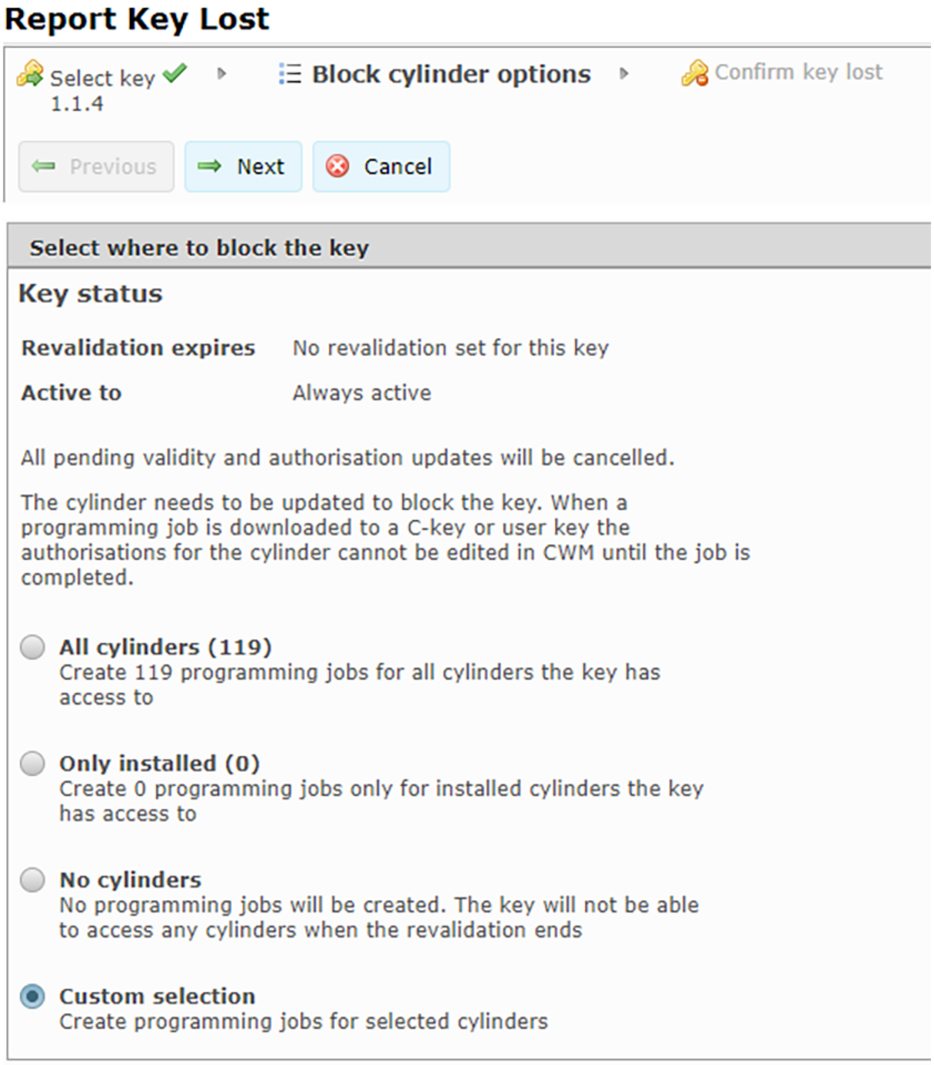
- If any cylinders need to be blocked and the cylinder programming job is assigned to a user key, ensure that "Block lost key with user keys" is enabled in the system settings. See *Section 6.4 "Editing System Settings", page 94* for instructions on changing this setting. This is only applicable to a remote system.

1) There are two ways to start reporting the lost key:
   - Select **Work » Report key lost**. Proceed to *Step 2*.
   - On the detailed information view of the lost key (for searching the key, see *Section 4.2.1 "Searching for User Keys", page 33*), click the **Report lost** button. Proceed to *Step 4*.
2) Enter the search criteria to find the owner of the key and click **Search**.
3) Select the lost key and click **Select**.
4) Select the cylinders for which the key will be blocked:
   - If it is necessary to program the cylinders to immediately block the lost key:

     HINT!
     To configure the system to block the lost key in newly added cylinders, enable **Block lost keys in new cylinders during extension import** in System settings. See *Section 6.4 "Editing System Settings", page 94*.

     – Select **All cylinders** or **Only installed** and proceed to *Step 7*.

     – Select **Custom selection** and proceed to proceed to *Step 5* to select the cylinders.
   - If the key needs to be reported as lost in CWM without blocking its access (for example, while waiting for the current revalidation interval to expire), select **No cylinders**, click **Next** and proceed to *Step 11*.



Report Key Lost

Select where to block the key

Key status

Revalidation expires No revalidation set for this key

Active to Always active

All pending validity and authorisation updates will be cancelled.

The cylinder needs to be updated to block the key. When a programming job is downloaded to a C-key or user key the authorisations for the cylinder cannot be edited in CWM until the job is completed.

○ **All cylinders (119)**
Create 119 programming jobs for all cylinders the key has access to

○ **Only installed (0)**
Create 0 programming jobs only for installed cylinders the key has access to

○ **No cylinders**
No programming jobs will be created. The key will not be able to access any cylinders when the revalidation ends

● **Custom selection**
Create programming jobs for selected cylinders

5) Click **Next**.

6) Select the cylinders for which the lost key will be blocked.

7) Click **Next**.

8) Optional: Select the blocking key from the list by clicking **Select**.

NOTE!
If this process is skipped, cylinder programming jobs are created for C-Keys.

In the **Search** tab, select **All types and statuses** to show C-Keys.

In the **Advanced** tab, under **Type**, select key types to change what is shown in the list.

NOTE!
Blocking Key Requirements:

- The blocking key must be Generation 2 with firmware version 12.2 or later.
- The blocking key must have sufficient memory.

9) In the confirmation page, select the priority level under **Priority**.

Urgent jobs should have a high priority level.

10)

WARNING!
By default, even if no cylinder programming job is created to block the lost key, the lost key is still added in CWM to the **List of Unauthorised Keys** for the affected cylinders. This information is, however, not visible in CWM. If these cylinders are later reprogrammed or replaced, the information about unauthorised keys stored in CWM is applied, in effect blocking the lost key. Therefore, even if the lost key is later reported found, it will still be blocked by any reprogrammed or replaced cylinders.

In order to reauthorise the found key in those cylinders, see *Section 4.9.2 "Configuring Authorisations in Cylinders", page 76*.

In order to change this default setting, disable the system setting **Silently block lost keys in cylinder during authorisation update**. See *Section 6.4 "Editing System Settings", page 94*.

After verifying all information, click **Report lost**.

11) Optional: Click **Print cylinder list** to generate a PDF summary view.

12)
- If a specific key was **NOT** selected to program the cylinders, continue from *Step 4* in *Section 4.4.13 "Programming Cylinders", page 59*.
- If a specific key was selected to program the cylinders, follow the instructions below.

13) Go to the detailed information view of the selected blocking key.

HINT!
Clicking **Key marking** under **Blocking key information** leads directly to the information view.

14) Go to the **Programming jobs** tab and confirm that the cylinder job is assigned to the key.

15)
- **Programming in the Local PD**

  Insert the blocking key into the right slot of the Local PD and remove the C-Key from the left slot of the Local PD.

- **Programming in a Wall PD**

  Insert the blocking key into a Wall PD.

The cylinder programming job is automatically written to the blocking key.

16) Reprogram each cylinder using the blocking key.

17) After programming the cylinders, report the completed cylinder jobs by inserting the blocking key into one of the following devices:

- The right slot of the Local PD (remove the C-Key from the left slot)
- A Wall PD

4.2.12.3 Reporting a Found User Key

1) Find the lost key in CWM and display the detailed information view.

   See *Section 4.2.2 "Scanning a User Key", page 34* or *Section 4.2.1 "Searching for User Keys", page 33*.

   NOTE!
   Lost keys are filtered using the **Lost** filter in the **Advanced** tab.

2) Click **Report found**.

   The key status changes to **In stock**.

3) Reauthorise the key by programming the affected cylinders. Follow the instructions in *Section 4.9.2 "Configuring Authorisations in Cylinders", page 76*.

   See below for information about what cylinders that are affected.

Affected cylinders
Cylinders that **must be programmed** to reauthorise the key:

- Cylinders that have already been programmed to block the lost key.
- Cylinders that have **not** been programmed to block the lost key must be programmed in the following case:
  - The cylinder has been **reprogrammed** or **replaced**.

    AND
  - The system setting **Silently block lost keys in cylinder during authorisation update** is **enabled**.

NOTE!
This applies both to cylinders for which programming jobs were not created when the key was reported lost, and to cylinders for which programming jobs were created but have not yet been executed.

All other cylinders:

The key already has access, so the cylinders do not need to be programmed. (For cylinders for which programming jobs were created but have not yet been executed, the programming jobs are automatically cancelled.)

4.2.13 Replacing a User Key with a Clone from the Factory

If a replacement clone is delivered from the factory due to a broken key, the following steps must be taken to ensure the functionality of the key.

1) When the replacement key arrives from the factory, go to **Administration » Extension import » Upload or fetch extension import file(s)** to either upload the supplied CWS-file to CWM (if DCS integration is disabled) or to fetch the file from DCS.

2) Create and program an authorization job for the replacement key. See *Section 4.9.1 "Configuring Authorisations in Keys", page 74*.

3) Create and program a validity job for the replacement key. *Section 4.10.1 "Configuring Key Validity, Revalidation, and PIN Validation", page 81*.

4) Cancel any existing scheduling jobs for the old key, recreate and program them for the replacement key. See *Section 4.10.3 "Configuring Key Schedule", page 84*.

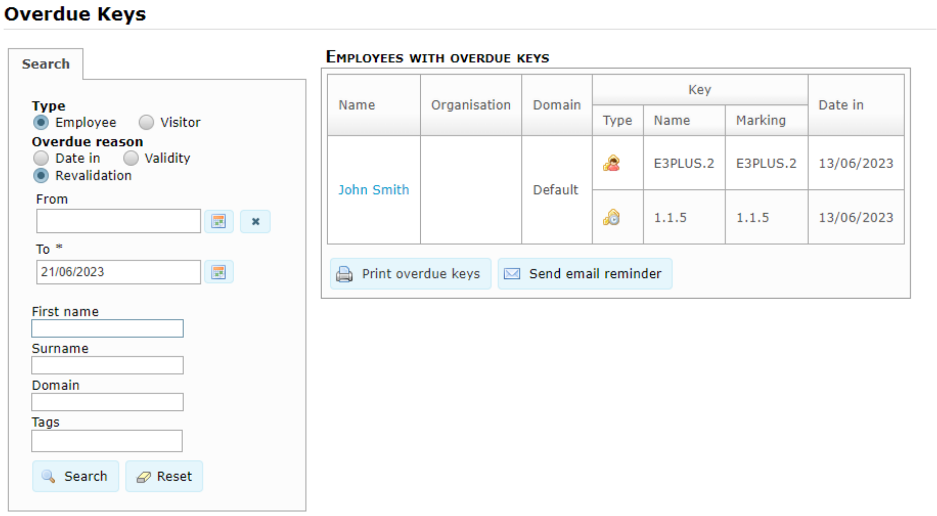
5) The replacement key is ready to use.

4.2.14 Viewing Overdue User Keys

1) Select **Work » Overdue keys**.

2) In the **Search** tab, select **Employee** or **Visitor** to choose the keyholder type.

A list of all keys handed out to employees or visitors with a hand-in date within a specified number of days is displayed.



Overdue Keys

Search

Type

● Employee ○ Visitor

Overdue reason

○ Date in ○ Validity

● Revalidation

From

To *

21/06/2023

First name

Surname

Domain

Tags

Search Reset

EMPLOYEES WITH OVERDUE KEYS

Name	Organisation	Domain	Key			Date in
			Type	Name	Marking	
John Smith		Default	🔑	E3PLUS.2	E3PLUS.2	13/06/2023
			🔑	1.1.5	1.1.5	13/06/2023

Print overdue keys Send email reminder

The default number of days can be edited in the System Settings. See *Section 6.4 "Editing System Settings", page 94*.

3) Select an **Overdue reason** and enter other search criteria and click **Search**.

Overdue reason:

- If **Date in** is selected, keys with a hand-in date within the specified number of days are listed.
- If **Validity** is selected, keys with a validity period ending within the specified number of days are listed.
- If **Revalidation** is selected, keys with a revalidation period ending between the specified dates are listed.

4) To print a list of the overdue keys or keys needing revalidation, click **Print overdue keys**.

5) To send an email reminder to employees or visitors with overdue keys, click **Send email reminder**.

For this option to be available, **User messaging** in **System settings** must be selected. See *Section 6.4 "Editing System Settings", page 94*.

4.2.15 Updating and Revalidating a User Key

Via Local PDs
If a key is inserted in the right slot of the Local PD, the key is directly updated during the operation in CWM.

When the following actions were operated locally, the key is revalidated in the Local PD at the same time:

- set **Schedule**
- read **Audit trail**
- change **Cylinders in access list**

If the following conditions are fulfilled, a key is updated and/or revalidated in the right slot of the Local PD **without** C-Key:

- Generation 2 key with firmware version 12.3 or later
- CLIQ Connect PC is activated

> **NOTE!**
> The C-Key must be removed from the left slot of the Local PD before update and revalidation.

Via Remote PDs
Key holders can update and/or revalidate their keys by inserting them in a Wall PD or CLIQ Mobile PD.

The key can also be updated and/or revalidated when it is connected to CLIQ Connect via a CLIQ Connect Mobile PD.

For more information about key revalidation, see *Section 8.1.5 "Key Revalidation", page 154* and *Section 8.1.6 "Flexible Revalidation", page 156*.

4.2.16 Copying User Key Configuration

The configuration on one key can be copied to another key scanned in the Local PD. The following settings are copied when applicable:

- Validity
- Schedule
- Revalidation settings
- Key Access List
- Access profiles

For keys included in cylinder access lists:

- Cylinder programming jobs are created to update the cylinder access lists.

1) Find the key from which configuration should be copied and go to its detailed information view.

   See *Section 4.2.1 "Searching for User Keys", page 33*.

2) Insert the target key in the Local PD.

3) Click **Copy key configuration**.

   The key is being scanned.

4) Click **Select**.

5) Select a **Priority** for the required cylinder programming jobs.

   Urgent jobs should have a high priority level.

6) Click **Apply**.

   Existing configuration on the target key is replaced and, if required, cylinder programming jobs are created.

   An event specifying date and time for the change and marking from source key and C-Key are created.

4.2.17 Printing User Key Report

1) Find the key and go to its detailed information view.

   To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Click **Print key report**.

3) Select whether to include mechanical cylinders or not in the list and click **OK**.

4) In the pop-up window, a preview is presented.

   - To save, click the save icon and specify a folder to save.
   - To print out, click **...** and select **Print**.

4.2.18 Exporting User Key Information

1) Select **System Info » Keys**.

   A list of all keys is displayed.

2) Search for the keys.

   See *Section 4.2.1 "Searching for User Keys", page 33*.

3) From the key search results, select the keys whose data to export.

4) Click **Export to CSV file**.

5) In the file download pop-up window, click **Save**.

   A CSV file is downloaded in the **Downloads** folder.

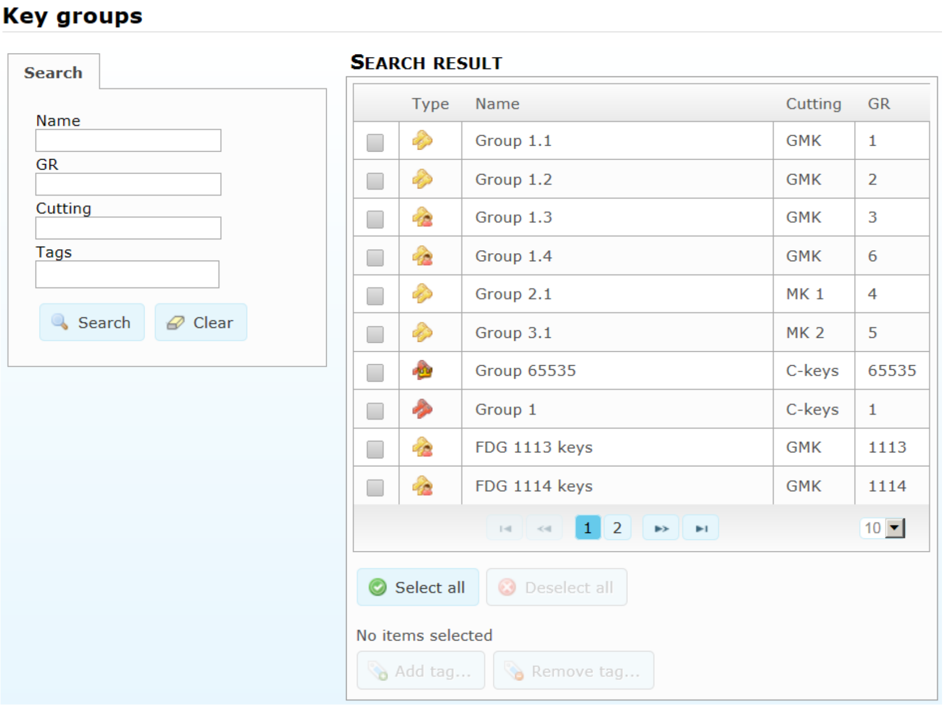
NOTE!
To be able to open the file in Excel in the correct way, the delimiter for the file must be set according to regional settings. To change the delimiter, see *Section 6.4 "Editing System Settings", page 94*.

4.3 Managing Key Groups

4.3.1 Searching for Key Groups

1) Select **System Info » Key groups**.

A list of all key groups is displayed.



Key groups

Search

Name

GR

Cutting

Tags

Search | Clear

SEARCH RESULT

	Type	Name	Cutting	GR
□		Group 1.1	GMK	1
□		Group 1.2	GMK	2
□		Group 1.3	GMK	3
□		Group 1.4	GMK	6
□		Group 2.1	MK 1	4
□		Group 3.1	MK 2	5
□		Group 65535	C-keys	65535
□		Group 1	C-keys	1
□		FDG 1113 keys	GMK	1113
□		FDG 1114 keys	GMK	1114

Select all | Deselect all

No items selected

Add tag... | Remove tag...

The following symbols are used:

- Normal Key Group
- Dynamic Key Group

2) Enter the search criteria.

When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

When typing in the **Tags** search field, all matching tags appear as a selectable list.

3) Click **Search**.

4) To display detailed information about a search result, click the row of the specific key group.

4.3.2 Editing Key Group Information

1) Find the key group and go to its detailed information view.

See *Section 4.3.1 "Searching for Key Groups", page 51*.

2) Click **Edit**.

3) To edit the key group name, type the name.

4) To add a tag, click **Add tag**. See also *Section 4.3.3 "Adding or Removing Key Group Tags", page 52*.

5) Click **Save**.

4.3.3 Adding or Removing Key Group Tags

1) Find the key group.

   To search for the key group, *Section 4.2.1 "Searching for User Keys", page 33*.

2) - To add or remove tags for individual key group, go to *Step 3*.
   - To add or remove tags for multiple key groups, go to *Step 4*.

3) **Add or Remove Tags for an Individual Key Group:**

   1. Select the key group and go to its detailed information view.
   2. Click **Edit**.
   3. Add or remove tag for individual key group.

      To Add a Tag:

      a) Click **Add tag...**.

      b) Enter a name for the tag.

      c) Click **OK**.

      To Remove a Tag:
      Click the tag to be removed.

   4. Click **Save**.

4) **Add or Remove Tags for Multiple Key Groups:**

   1. Select key groups from the search results by checking the checkboxes.
   2. **To Add a Tag:**

      a) Click **Add tag...**.

      b) Enter a name of the tag.

      c) Click **OK**.

      To Remove a Tag:

      a) Click **Remove tag...**.

      b) Enter a name of the tag.

      c) Click **OK**.

See also *Section 8.2.6 "Tags", page 166*.

4.3.4 Viewing Key Group Members

1) Find the key group and go to its detailed information view.

   See *Section 4.3.1 "Searching for Key Groups", page 51*.

2) Select the **Members** tab.

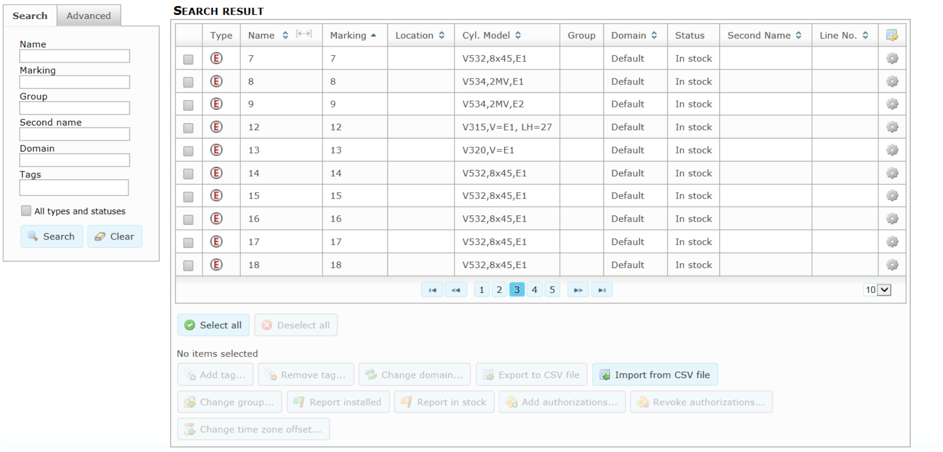
   A list with all keys in that key group is displayed.

4.4 Managing Cylinders

4.4.1 Searching for Cylinders

1) Select **System Info » Cylinders**.

A list of all cylinders, excluding mechanical and broken cylinders, is displayed.



	Type	Name	Marking	Location	Cyl. Model	Group	Domain	Status	Second Name	Line No.	
□	E	7	7		V532,8x45,E1		Default	In stock			
□	E	8	8		V534,2MV,E1		Default	In stock			
□	E	9	9		V534,2MV,E2		Default	In stock			
□	E	12	12		V315,V=E1, LH=27		Default	In stock			
□	E	13	13		V320,V=E1		Default	In stock			
□	E	14	14		V532,8x45,E1		Default	In stock			
□	E	15	15		V532,8x45,E1		Default	In stock			
□	E	16	16		V532,8x45,E1		Default	In stock			
□	E	17	17		V532,8x45,E1		Default	In stock			
□	E	18	18		V532,8x45,E1		Default	In stock			

No items selected

The following symbols are used:

E	Electronic Cylinder
M	Mechanical Cylinder
EM	Double Cylinder (This example: Electronic A-side and Mechanical B-side)

2) Select the **Search** or **Advanced** tab.

By default, mechanical and broken cylinders are not displayed. To include also these cylinders in the search result, select **All types and statuses**.

The **Advanced** tab also includes the search fields type of cylinder, inventory status, operational status, second marking and, via a drop-down list, custom fields (if defined in **System settings**. This setting is found by selecting **Administration » System Settings » ADMINISTRATION » Cylinder custom fields**.).

3) Enter the search criteria.

When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

When typing in the **Tags** search field, all matching tags appear as a selectable list.

4) Click **Search**.

5) To display detailed information on a search result, click the row of the specific cylinder.

For information about the cylinder attributes, see *Section 9.3.5 "Cylinder Attributes", page 184*.

4.4.2 Editing Cylinder Information

1) Find the cylinder and go to its detailed information view.

See *Section 4.4.1 "Searching for Cylinders", page 52*.

If **Second name** or **Custom fields** needs to be edited, proceed to *Step 6*.

2) Click **Edit**.

3) Edit the fields.

For more information about the cylinder attributes, see *Section 9.3.5 "Cylinder Attributes", page 184*.

4) - To add a tag, click **Add tag**. See also *Section 4.4.3 "Adding or Removing Cylinder Tags", page 54*
   - To add an external link, click **Add external link**. See also *Section 4.4.4 "Managing Cylinder External Links", page 55*

5) Click **Save**.

6) **Second name** and **Custom fields** are edited in the **Additional information** tab.

> **NOTE!**
> Custom fields are defined in **System settings**. See *Section 6.4 "Editing System Settings", page 94*.

   a) Select the **Additional information** tab.
   b) Click **Edit**.
   c) Update the field.
   d) Click **Save**.

4.4.3 Adding or Removing Cylinder Tags

For information about tags, see *Section 8.2.6 "Tags", page 166*.

1) Select **System Info » Cylinders**.

   A list of all cylinders is displayed.

   - To add or remove tags for individual cylinder, go to *Step 2*.
   - To add or remove tags for multiple cylinders simultaneously, go to *Step 3*.

2) **To Add or Remove Tags for an Individual Cylinder:**

   1. Select the cylinder and go to its detailed information view.
   2. Click **Edit**.
   3. Add or remove a tag for individual cylinder.

      To Add a Tag:

      a) Click **Add tag...**.
      b) Enter a name for the tag.
      c) Click **OK**.

      To Remove a Tag:
      Click the tag to be removed.
   4. Click **Save**.

3) **To Add or Remove Tags for Multiple Cylinder:**

   1. Select cylinders from the search results by checking the check boxes.
   2. **Adding a Tag:**

      a) Click **Add tag...**.
      b) Enter a name of the tag.
      c) Click **OK**.

Removing a Tag:

a) Click **Remove tag...**.

b) Enter a name of the tag.

c) Click **OK**.

4.4.4 Managing Cylinder External Links

For information about external links, see *Section 8.4 "External Links", page 169*.

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Click **Edit**.

3) **To Add an External Link:**

   1. Click **Add.**
   2. Enter **Name** for the URL.
   3. Enter **URL**. The **URL** must start with a protocol (for example http:// or ftp://).

      If a root URL has been defined in **System settings** (item **External links root URL**), it is only necessary to add the last part of the URL. See also *Section 6.4 "Editing System Settings", page 94*.
   4. Click **OK**.

   To Edit an External Link:

   1. Click **Edit** on the external link to be edited.
   2. Update the fields.
   3. Click **OK**.

   To Remove an External Link:
   Click **Remove** on the external link to be removed.

4) Click **Save**.

4.4.5 Viewing Key Groups and Exceptions in a Cylinder Access List

The **Keys in access list** tab is used to show key groups and exceptions in the cylinders access list..

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Select the **Keys in access list** tab.

   A list with all key groups and exceptions in this cylinder's access list is displayed. To edit it, see *Section 4.9.2 "Configuring Authorisations in Cylinders", page 76*.

4.4.6 Viewing Update History for Cylinder

The Update history tab is used for traceability of key programming.

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Select the **Update history** tab.

   A list with all cylinder updates is displayed.

   The following symbols are used:

   ⚙ Programming Job exists but has not been initiated

   ⚙ Programming Job has been programmed to C-Key

   ⚙ Programming Job has been finished

   ⚙ Programming Job has failed or been cancelled

   ⚙ Programming Job has been replaced with a new job

3) To display further details on a specific update, click the link in the **Type** column.

4.4.7 Viewing Events for Cylinder

The **Events** tab is used for traceability of administrator operations in the CWM, such as reporting a broken cylinder.

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Select the **Events** tab.

   A list with all cylinder events is displayed.

4.4.8 Editing Cylinder Time Zone Offset

The time zone can be offset for cylinders in a domain if they are located in different time zones. This setting is only available for generation 2 cylinders.

For more information about key generations, see *Section 7.2.5 "Key Generations", page 146*.

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Click **Change time zone offset...**.

3) Set **Time zone offset** to the desired number of minutes.

4) Set job priority.

5) Click **OK**.

   A cylinder programming job is created. To program the cylinder, see *Section 4.4.13 "Programming Cylinders", page 59*.

> **NOTE!**
> While the programming job is awaiting execution, the button **Cancel change time zone offset** is shown in the detailed information for the cylinder.
>
> Click the button, while editing, to cancel the change of time zone offset.

The time zone offset can be edited for several cylinders simultaneously. Select the cylinders in the search result list and click **Time zone offset**.

4.4.9 Changing Cylinder Status

Cylinders have an inventory status of either **in stock** or **installed**, and an operational status of either **operational** or **broken**.

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) **To Change to Installed Status**

   1. Click **Report installed**.
   2. Click **OK**.

      Multiple cylinders can be reported as installed simultaneously. Select the cylinders in the search result list and click **Report installed**.

   To Change to In-Stock Status

   1. Click **Report in stock**.
   2. Click **OK**.

      Multiple cylinders can be reported as in stock simultaneously. Select the cylinders in the search result list and click **Report in stock**.

   To Report as Broken

   1. Click **Report broken**.
   2. Select **Report broken only**.

      If a replacement process is required, see *Section 4.4.10 "Replacing Broken Cylinder", page 57*.

   3. Click **Next**.
   4. Click **Apply**.

   To Report the Cylinder is Back in Operation

   1. Click **Report operational**.

      This option is only available foo cylinders previously reported as broken.

   2. Click **OK**.
   3. A programming job is created.

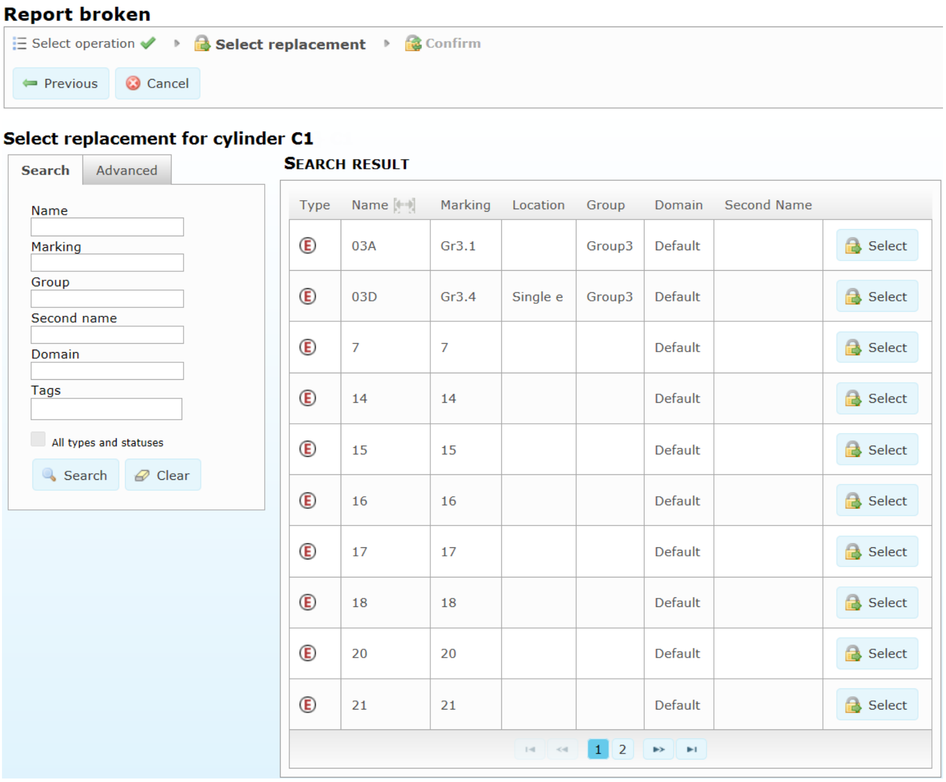
4.4.10 Replacing Broken Cylinder

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Click **Report Broken**.
3) Select **Report broken and replace with another cylinder**.
4) Click **Next**.

   A list showing all cylinders of the same type as the reported cylinder, as found in stock, will be displayed.



Select replacement for cylinder C1

SEARCH RESULT

Type	Name	Marking	Location	Group	Domain	Second Name	
Ⓔ	03A	Gr3.1		Group3	Default		Select
Ⓔ	03D	Gr3.4	Single e	Group3	Default		Select
Ⓔ	7	7			Default		Select
Ⓔ	14	14			Default		Select
Ⓔ	15	15			Default		Select
Ⓔ	16	16			Default		Select
Ⓔ	17	17			Default		Select
Ⓔ	18	18			Default		Select
Ⓔ	20	20			Default		Select
Ⓔ	21	21			Default		Select

5) To search for specific cylinders, enter the search criteria and click **Search**.

6) Select a replacement cylinder by clicking **Select**.

7) Select a **Priority** level.

   Urgent jobs should have a high priority level.

8) Click **Apply**.

   The current configuration, including pending updates, for the replacement cylinder will be discarded and replaced by the configuration of the broken cylinder.

   Remote update jobs will be created for associated keys and access profiles that give access to the broken cylinder will be updated.

4.4.11 Replacing a Cylinder with a Clone from the Factory

If a replacement clone is delivered from the factory due to a broken cylinder, the following steps must be taken to ensure the functionality of the cylinder.

1) When the cloned cylinder arrives from the factory, go to **Administration » Extension import » Upload or fetch extension import file(s)** to either upload the supplied CWS-file to CWM (if DCS integration is disabled) or to fetch the file from the DCS.

2) Create a reprograming job for the replacement cylinder. See *Section 4.4.12 "Requesting Cylinder Reprogramming", page 58*.

3) Program the replacement cylinder. See *Section 4.4.13 "Programming Cylinders", page 59*.

4) The replacement cylinder is ready to use.

4.4.12 Requesting Cylinder Reprogramming

When a cylinder is reprogrammed, its memory content is deleted, including the audit trails. The access list of the cylinder is restored as part of the reprogramming. A Master

C-Key or a Normal C-Key with Cylinder Reprogramming rights is needed to perform the actual reprogramming job.

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Click **Reprogram**.

   For double-sided cylinders, click **Reprogram side A**, **Reprogram side B** or both.

3) Select **Priority**.

   Urgent jobs should have a high priority.

4) Click **OK**.

See also *Section 4.4.13 "Programming Cylinders", page 59*.

4.4.13 Programming Cylinders with a C-Key

Prerequisites:

- A C-Key with the **Cylinder programming** permission
- For jobs involving the change of a cylinder's cylinder group: a C-Key with the **Cylinder group programming** capability
- For reprogramming jobs: A Master C-Key or a Normal C-Key with the **Cylinder Reprogramming** permission

If the C-Key to be used for the programming is immediately available, follow the procedure in *Section 4.4.13.1 "Programming Cylinders using C-Key with Local PD", page 59*.

If the C-Key to be used for the programming is not immediately available, follow the procedure in *Section 4.4.13.2 "Programming Cylinders using Connect C-Key or C-Key with Remote PD", page 61*. This procedure requires a Remote PD or a CLIQ Connect C-key.

For more information about cylinder programming, see *Section 8.5 "Cylinder Programming", page 169*.

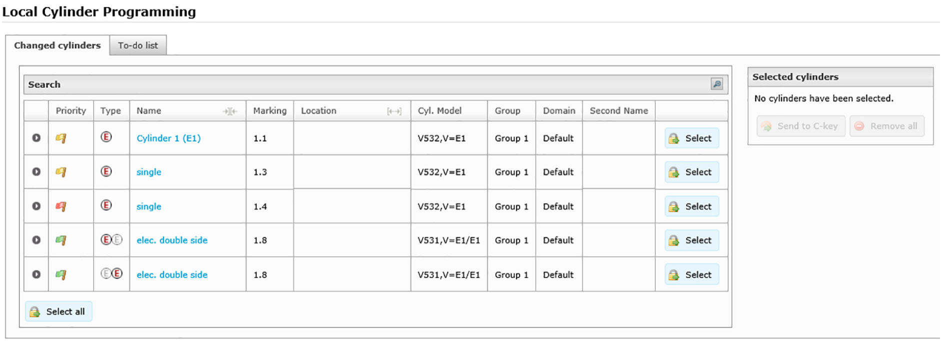
4.4.13.1 Programming Cylinders using C-Key with Local PD

To send programming jobs to an immediately avalable C-Key and program cylinders:

1) Select **Work » Cylinder programming**.

   A list of the cylinders requiring programming is displayed. The priority levels for the jobs are listed in the left most column.

2) To select the jobs to be executed, click **Select** in the list or **Select all** which is located under the list.



Local Cylinder Programming

	Priority	Type	Name	Marking	Location	Cyl. Model	Group	Domain	Second Name	
●	⚑	Ⓔ	Cylinder 1 (E1)	1.1		V532,V=E1	Group 1	Default		Select
●	⚑	Ⓔ	single	1.3		V532,V=E1	Group 1	Default		Select
●	⚑	Ⓔ	single	1.4		V532,V=E1	Group 1	Default		Select
●	⚑	ⒺⒺ	elec. double side	1.8		V531,V=E1/E1	Group 1	Default		Select
●	⚑	ⒺⒺ	elec. double side	1.8		V531,V=E1/E1	Group 1	Default		Select

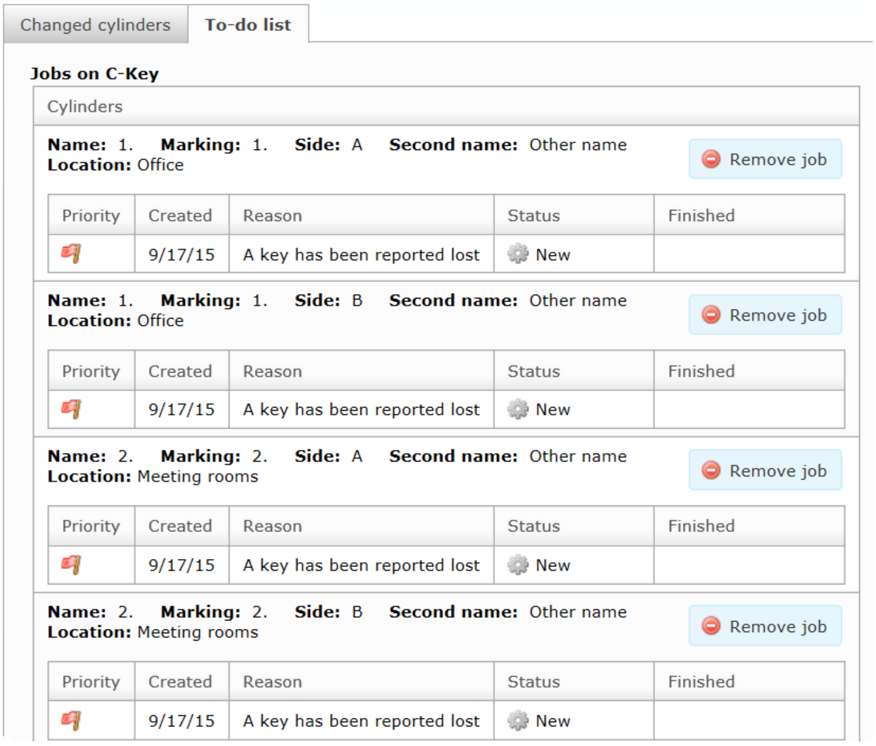
Selected cylinders

No cylinders have been selected.

3) Click **Send to C-key**.

NOTE!
While a cylinder programming job is loaded to a C-Key, the authorisation settings for that cylinder are locked from editing in CWM.

- To see a list of jobs currently on the C-Key, select the **To-do list** tab.



Jobs on C-Key

Cylinders

Name: 1. **Marking:** 1. **Side:** A **Second name:** Other name
Location: Office

Priority	Created	Reason	Status	Finished
⚑	9/17/15	A key has been reported lost	New	

Name: 1. **Marking:** 1. **Side:** B **Second name:** Other name
Location: Office

Priority	Created	Reason	Status	Finished
⚑	9/17/15	A key has been reported lost	New	

Name: 2. **Marking:** 2. **Side:** A **Second name:** Other name
Location: Meeting rooms

Priority	Created	Reason	Status	Finished
⚑	9/17/15	A key has been reported lost	New	

Name: 2. **Marking:** 2. **Side:** B **Second name:** Other name
Location: Meeting rooms

Priority	Created	Reason	Status	Finished
⚑	9/17/15	A key has been reported lost	New	

- To print the list, click **Print to-do list**.

4) Insert the C-Key into the cylinders to be programmed, one by one.

CAUTION!
Keep the C-Key inserted until the programming job is completed.

If the job fails, insert the C-Key into a Remote PD connected to CWM to reload the programming job to the C-Key again. See also *"Reprogramming"*.

5) Log in to CWM again.
6) Select **Work » Cylinder programming**.
7) Select the **To-do list** tab.
8) Click **Update**.

   The status of the programming jobs are loaded from the C-Key.
9) Optional: Click **Remove finished jobs**.

4.4.13.2 Programming Cylinders using Connect C-Key or C-Key with Remote PD

Throughout the procedure of programming cylinder jobs, the status of the Remote PD interaction is indicated by LEDs. For more information about the LED indicator, see *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190* or *Section 9.5.2 "Wall PD (Generation 2) Indications", page 191*.

1) Assign cylinder programming jobs to a C-Key:

   a) Find the C-Key.

      To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

   b) Select the **Cylinder programming** tab.

   c) Click **Assign cylinders for programming**.

   d) Click **Select** for each cylinder programming job to be executed.

      > ⚠ **WARNING!**
      > For jobs including cylinder group changes, a maximum of 100 jobs can be assigned to a C-Key. Assigning more jobs could result in programming errors.

   e) Click **Apply**.

      After assigning the cylinder programming job to the C-Key, an email is generated to the C-Key holder with information that there are programming jobs to pick up.

2) Insert the C-Key into a Remote PD or connect the Connect C-Key to CLIQ Connect to load the cylinder programming jobs.

   Once the cylinder programming job is transferred, an email is generated to the C-Key holder with information about what cylinders to program.

3) Insert the C-Key in the cylinders to be programmed.

   > ◆ **CAUTION!**
   > Keep the key inserted until the programming job is completed.
   >
   > If the job fails, insert the key into a Remote PD connected to CWM to reload the programming job to the key again. See also *"Reprogramming"*.

4) Insert the C-Key in a Remote PD or connect the Connect C-Key to CLIQ Connect to update the status of the programming jobs.

4.4.14 Importing Cylinder Information

Importing Cylinder Information enables mass import of updated cylinder data. The function is only applicable for updating existing cylinder data.

A CSV file is used for the import. To write a new CSV file, the easiest way is to export a CSV file with existing cylinder data and then edit the exported file in Excel or a text editor. See *Section 4.4.15 "Exporting Cylinder Information", page 62*.

> **NOTE!**
> Cylinder information can be imported from both CSV files and **Extension import files** but the content does not overlap. CSV files update cylinder information that users can change in the GUI whereas extension import files update non-editable factory data. As a result, CSV files cannot overwrite extensions or the other way round. For more information about extensions, see *Section 6.16 "Importing Extensions", page 142*.

1) Click **System info » Cylinders**.

2) Click **Import from CSV file**.

3) Click **Select** to find the locally saved file on the computer.

4) Click **Open**.

5) Click **Import** to import and validate the file.

   Information on how many valid entries the file contains is displayed. If the file does not follow the specifications, import is not possible.

> **NOTE!**
> When importing cylinder information, only the following columns in the CSV file are updated.
>
> - Name
> - Second name
> - Location
> - Inventory status
> - Custom fields (if defined in **System settings**)
>
> Existing cylinder data is overwritten.

> **NOTE!**
> To import cylinder information from a CSV file, the values in **Marking** or the combined values from **Marking** and **Second Marking** must be unique.

4.4.15 Exporting Cylinder Information

1) Search for the cylinders.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) From the cylinder search results, select the cylinders whose data to export.

3) Click **Export to CSV file**.

NOTE!
To be able to open the file in Excel in the correct way, the delimiter for the file must be set according to regional settings. To change the delimiter, see *Section 6.4 "Editing System Settings", page 94*.

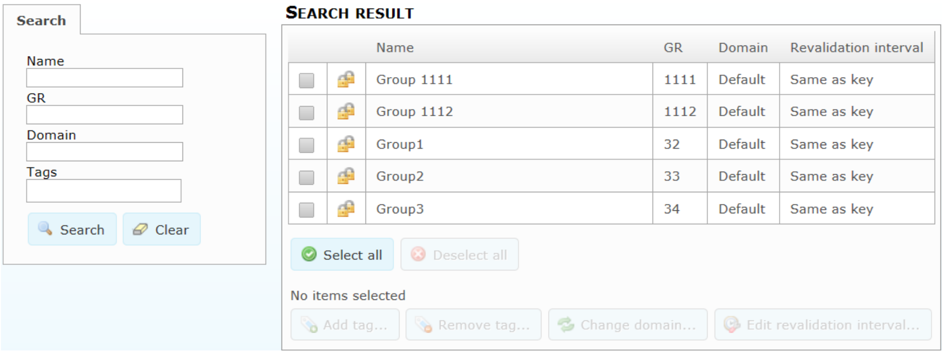
4) In the file download pop-up window, click **Open** or **Save**.

4.5 Managing Cylinder Groups

4.5.1 Searching for Cylinder Groups

1) Select **System Info » Cylinder groups**.

A list of all cylinder groups is displayed.



Search

Name

GR

Domain

Tags

Search Clear

SEARCH RESULT

		Name	GR	Domain	Revalidation interval
☐		Group 1111	1111	Default	Same as key
☐		Group 1112	1112	Default	Same as key
☐		Group1	32	Default	Same as key
☐		Group2	33	Default	Same as key
☐		Group3	34	Default	Same as key

Select all Deselect all

No items selected

Add tag... Remove tag... Change domain... Edit revalidation interval...

2) Enter the search criteria.

When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

When typing in the **Tags** search field, all matching tags appear as a selectable list.

3) Click **Search**.

4) To display detailed information on a search result, click the specific cylinder group.

4.5.2 Editing Cylinder Group Information

1) Find the cylinder group and go to its detailed information view.

See *Section 4.5.1 "Searching for Cylinder Groups", page 63*.

2) Click **Edit**.

3) To edit the cylinder group name, update the field **Name**.

4) To add a tag, click **Add tag...**. See also *Section 4.5.3 "Adding or Deleting Cylinder Group Tags", page 64*

5) To change domain, click **Change domain...**. See also *Section 6.6.8 "Changing Domain For Cylinder Groups", page 118*.

6) Click **Save**.

4.5.3 Adding or Deleting Cylinder Group Tags

1) Find the cylinder group.

   To search for the cylinder group, *Section 4.2.1 "Searching for User Keys", page 33*.

2) - To add or remove tags for individual cylinder group, go to *Step 3*.
   - To add or remove tags for multiple cylinder groups, go to *Step 4*.

3) **Add or Remove Tags for an Individual Cylinder Group:**

   1. Select the cylinder group and go to its detailed information view.
   2. Click **Edit**.
   3. Add or remove tag for individual cylinder group.

      To Add a Tag:

      a) Click **Add tag...**.

      b) Enter a name for the tag.

      c) Click **OK**.

      To Remove a Tag:
      Click the tag to be removed.

   4. Click **Save**.

4) **Add or Remove Tags for Multiple Cylinder Groups:**

   1. Select cylinder groups from the search results by checking the checkboxes.
   2. **To Add a Tag:**

      a) Click **Add tag...**.

      b) Enter a name of the tag.

      c) Click **OK**.

      To Remove a Tag:

      a) Click **Remove tag...**.

      b) Enter a name of the tag.

      c) Click **OK**.

See also *Section 8.2.6 "Tags", page 166*.

4.5.4 Viewing Cylinder Group Members

1) Find the cylinder group and go to its detailed information view.

   See *Section 4.5.1 "Searching for Cylinder Groups", page 63*.

2) Select the **Members** tab.

   A list with all cylinders in that group is displayed.

4.5.5 Viewing Events for Cylinder Group

The Events tab is used for traceability of administrator operations in CWM, such as changing domain for a cylinder group.

1) Find the cylinder group and go to its detailed information view.

See *Section 4.5.1 "Searching for Cylinder Groups", page 63*.

2) Select the **Events** tab.

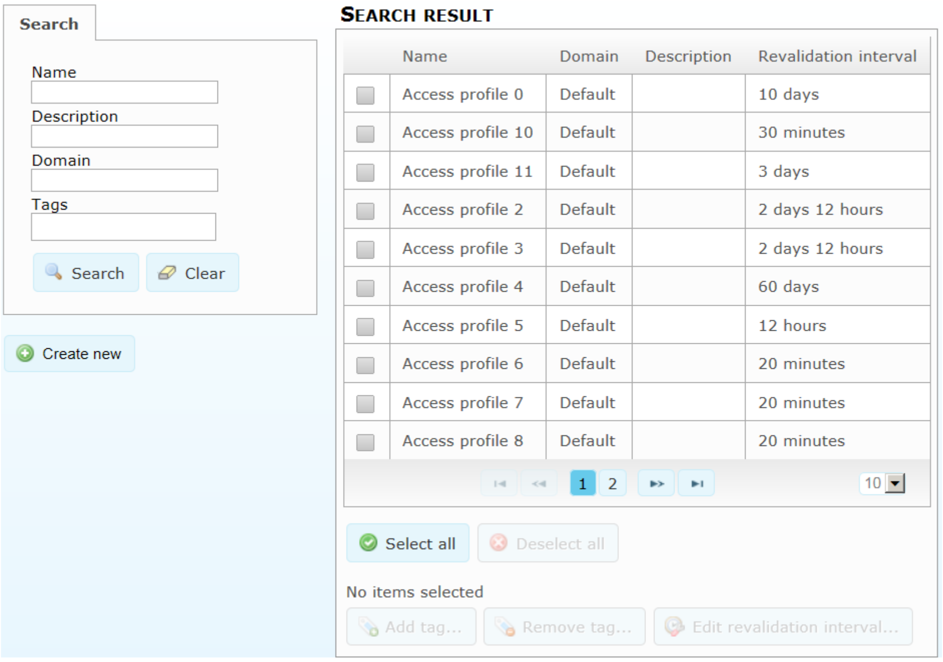
A list with all cylinder group events is displayed.

4.6 Managing Access Profiles

4.6.1 Searching for Access Profiles

1) Select **System Info » Access profiles**.

A list of all access profiles is displayed.



SEARCH RESULT

	Name	Domain	Description	Revalidation interval
☐	Access profile 0	Default		10 days
☐	Access profile 10	Default		30 minutes
☐	Access profile 11	Default		3 days
☐	Access profile 2	Default		2 days 12 hours
☐	Access profile 3	Default		2 days 12 hours
☐	Access profile 4	Default		60 days
☐	Access profile 5	Default		12 hours
☐	Access profile 6	Default		20 minutes
☐	Access profile 7	Default		20 minutes
☐	Access profile 8	Default		20 minutes

No items selected

2) Enter the search criteria.

When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

3) Click **Search**.

4) To display detailed information on a search result, click the specific access profile.

4.6.2 Creating and Deleting Access Profiles

Access profiles are only applicable for dynamic keys that support remote updates. They can be applied on a key or a person.

1) Select **System Info » Access profiles**.

2) To create an access profile:

a) Click **Create New**.

b) Enter **Name** and an optional **Description**.

> **NOTE!**
> The name field must be unique.

c) To change domain from default:

- Click **Change domain**
- Click **Select** for the specific domain.

d) To add a tag, click **Add tag**. See also *Section 4.6.4 "Adding or Deleting Access Profile Tags", page 66*

e) To add an external link, click **Add external link**. See also *Section 4.6.5 "Editing Access Profile External Links", page 67*

f) Click **Save**.

3) To delete an access profile:

a) Find the access profile and view the detailed information.

See *Section 4.6.1 "Searching for Access Profiles", page 65*.

b) Click **Delete**.

c)
- If there are no keys or persons which are associated to the profile:

  Click **Delete profile**.
- If there are keys or persons which are associated to the profile:

  a) Confirm that access profiles is permanently deleted, then click on the checkbox.

  b) Click **Delete profile**.

See also *Section 8.2.4 "Access Profiles", page 162*.

4.6.3 Editing Access Profile Information

1) Find the access profile and go to its detailed information view.

See *Section 4.6.1 "Searching for Access Profiles", page 65*.

2) Click **Edit**.

3) Update the fields.

4) To add tags, click **Add Tag...**. See also *Section 4.1.7 "Adding or Removing Employee or Visitor Tags", page 30*.

5) To add edit external links, click **Add external link...**. See also *Section 4.1.8 "Managing Employee or Visitor External Links", page 31*.

6) Click **Save**.

4.6.4 Adding or Deleting Access Profile Tags

1) Find the access profile.

To search for the access profile, see *Section 4.6.1 "Searching for Access Profiles", page 65*.

2)
- To add or remove tags for individual access profile, go to *Step 3*.
- To add or remove tags for multiple access profiles, go to *Step 4*.

3) **Add or Remove Tags for an Individual Access Profile:**

1. Select the access profile and go to its detailed information view.
2. Click **Edit**.
3. Add or remove tag for individual access profile.

To Add a Tag:

a) Click **Add tag...**.

b) Enter a name for the tag.

c) Click **OK**.

To Remove a Tag:
Click the tag to be removed.

4. Click **Save**.

4) **Add or Remove Tags for Multiple Access Profiles:**

1. Select access profiles from the search results by checking the checkboxes.
2. **To Add a Tag:**

a) Click **Add tag...**.

b) Enter a name of the tag.

c) Click **OK**.

To Remove a Tag:

a) Click **Remove tag...**.

b) Enter a name of the tag.

c) Click **OK**.

For more information about tags, see *Section 8.2.6 "Tags", page 166*.

4.6.5 Editing Access Profile External Links

1) Find the access profile and go to its detailed information view.

See *Section 4.6.1 "Searching for Access Profiles", page 65*.

2) Click **Edit**.

3) To add an external link:

a) Click **Add.**

b) Enter **Name** for the URL.

c) Enter **URL**. The **URL** must start with a protocol (for example http:// or ftp://).

If a root URL has been defined in **System settings**, it is enough to add the last part of the URL. See also *Section 6.4 "Editing System Settings", page 94*.

d) Click **OK**.

4) To remove an external link, click **Remove** for the external link to be removed.

5) To edit an external link:

a) Click **Edit** on the external link to be edited.

b) Update the fields.

c) Click **OK**.

6) Click **Save**.

See also *Section 8.4 "External Links", page 169*.

4.6.6 Viewing Keys Associated with an Access Profile

The **Keys** tab displays all keys associated with the selected access profile. It also displays keys in expired Temporary Access Groups that are associated with the selected Access Profile.

1) Find the access profile and go to its detailed information view.

   See *Section 4.6.1 "Searching for Access Profiles", page 65*.

2) Select the **Keys** tab.

   A list with all keys that have the access profile is displayed.

4.6.7 Viewing Events for Access Profile

The Events tab is used for traceability of administrator operations in CWM, such as adding and removing cylinders in an access profile.

1) Find the access profile and go to its detailed information view.

   See *Section 4.6.1 "Searching for Access Profiles", page 65*.

2) Select the **Events** tab.

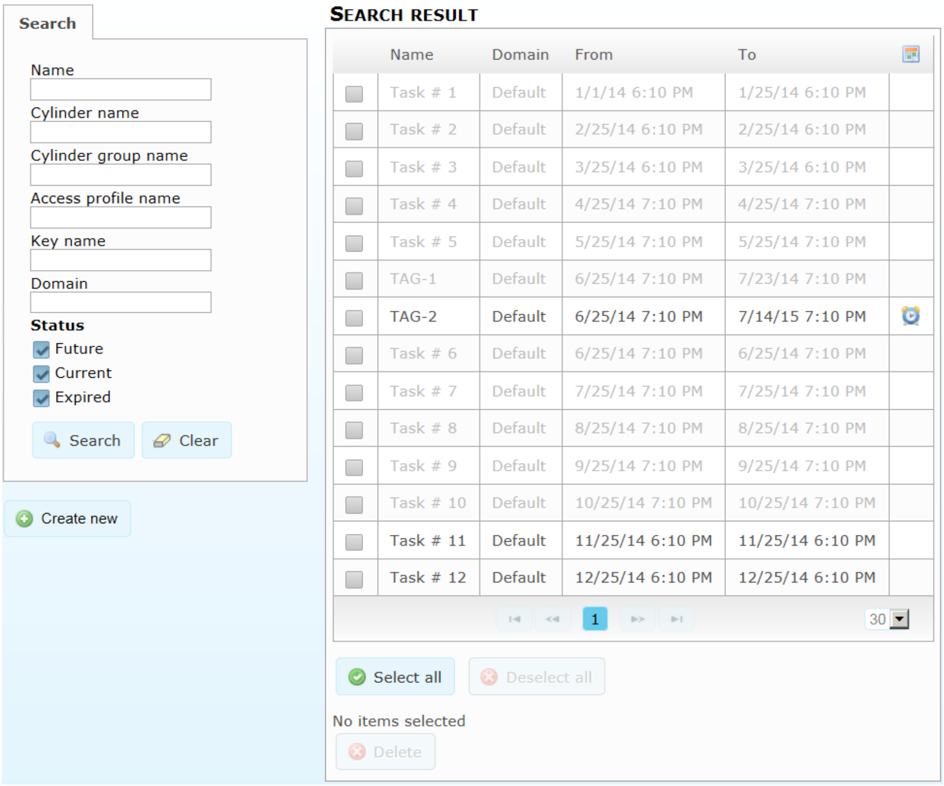
   A list with all access profile events is displayed.

4.7 Managing Temporary Access Groups

4.7.1 Searching for Temporary Access Groups

1) Select **System Info » Temporary access groups**.

   A list of all temporary access groups is displayed.



Search

Name

Cylinder name

Cylinder group name

Access profile name

Key name

Domain

Status

☑ Future

☑ Current

☑ Expired

SEARCH RESULT

	Name	Domain	From	To
☐	Task # 1	Default	1/1/14 6:10 PM	1/25/14 6:10 PM
☐	Task # 2	Default	2/25/14 6:10 PM	2/25/14 6:10 PM
☐	Task # 3	Default	3/25/14 6:10 PM	3/25/14 6:10 PM
☐	Task # 4	Default	4/25/14 7:10 PM	4/25/14 7:10 PM
☐	Task # 5	Default	5/25/14 7:10 PM	5/25/14 7:10 PM
☐	TAG-1	Default	6/25/14 7:10 PM	7/23/14 7:10 PM
☐	TAG-2	Default	6/25/14 7:10 PM	7/14/15 7:10 PM
☐	Task # 6	Default	6/25/14 7:10 PM	6/25/14 7:10 PM
☐	Task # 7	Default	7/25/14 7:10 PM	7/25/14 7:10 PM
☐	Task # 8	Default	8/25/14 7:10 PM	8/25/14 7:10 PM
☐	Task # 9	Default	9/25/14 7:10 PM	9/25/14 7:10 PM
☐	Task # 10	Default	10/25/14 7:10 PM	10/25/14 7:10 PM
☐	Task # 11	Default	11/25/14 6:10 PM	11/25/14 6:10 PM
☐	Task # 12	Default	12/25/14 6:10 PM	12/25/14 6:10 PM

No items selected

2) Enter the search criteria.

When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

3) To filter the search:

   a) Check the box **Expired** to show temporary access groups that are not valid anymore.

      In the result list, temporary access groups that have expired are formatted with grey text.

   b) Check the box **Current** to show temporary access groups that are currently valid.

      In the result list, temporary access groups that are currently valid are formatted with black text and indicated by an icon:

      ⏰

   c) Check the box **Future** to show temporary access groups that are valid in the future.

      In the result list, temporary access groups that are valid in the future are formatted with black text.

4) Click **Search**.

5) To display detailed information on a search result, click the specific temporary access group.

4.7.2 Creating and Deleting Temporary Access Groups

Temporary access groups are only applicable for dynamic keys that support remote updates. They are applied on a key.

1) Select **System Info » Temporary access groups**.

2) To create a temporary access group:

   a) Click **Create New**.

   b) Enter **Name**.

   c) Enter the period values **From** and **To** date.

> **NOTE!**
> When the temporary access group is no longer valid for a key, a remote job will automatically be created to remove the access of the temporary access group from the key. However, cancellation of the key's access will not take effect until the key is updated in a Remote PD.

   d) To change domain from default:

   - Click **Change domain**
   - Click **Select** for the specific domain.

   e) Click **Save**.

3) To delete a temporary access group:

a) Find the temporary access group and view the detailed information.

   See *Section 4.7.1 "Searching for Temporary Access Groups", page 68*.

b) Click **Delete**.

c) Click **OK**.

It is also possible to create a temporary access group from the key view. In the detailed information view, select the **Temporary access groups** tab, click **Create new** and follow the instructions above, starting from *Step 2 b*.

See also *Section 8.2.5 "Temporary Access Groups", page 164*.

4.7.3 Editing Temporary Access Groups

1) Find the temporary access group and go to its detailed information view.

   See *Section 4.7.1 "Searching for Temporary Access Groups", page 68*.

2) In the detailed information view, click **Edit**.

3) Update the fields.

4) Click **Save**.

4.7.4 Adding or Removing Keys from Temporary Access Groups

NOTE!
When a temporary access group is no longer valid for a key, a remote job will automatically be created to remove the access of the temporary access group from the key. However, cancellation of the key's access will not take effect until the key is updated in a Remote PD. To cancel the key holder's possibility to use the key after the temporary access group has expired, do one of the following prior to adding keys:

- Set **Active between selected dates** in the activation settings, see *Section 8.1.4 "Key Validity", page 154*.
- Activate key **Revalidation**, see *Section 8.1.5 "Key Revalidation", page 154*.

It is strongly recommended to combine temporary access groups with key revalidation.

1) Find the temporary access group and go to its detailed information view.

   See *Section 4.7.1 "Searching for Temporary Access Groups", page 68*.

2) Select the **Keys** tab.

3) Click **Edit**.

4) To add keys to a temporary access group:

   a) Click **Add keys...**.

   b) Click **Select** for individual keys to add. Click **Select all** to add all keys.

   c) Click **Done**.

   d) Click **Save**.

      A remote job is automatically created.

5) To remove keys from a temporary access group:

a) Click **Remove** for individual keys to remove. Click **Remove all** to remove all keys.

b) Click **Save**.

4.7.5 Editing Explicit Access for Temporary Access Groups

1) Find the temporary access group and go to its detailed information view.

   See *Section 4.7.1 "Searching for Temporary Access Groups", page 68*.

2) Select the **Explicit access** tab.

3) Click **Edit**.

4) To add or remove cylinder groups:

   a) Under **SELECTED CYLINDER GROUPS**, click **Add cylinder groups...** .

      All available cylinder groups are displayed.

   b) To filter the available cylinder groups, enter search criteria and click **Search**.

   c) To add cylinder groups, click **Select** for the cylinders to add or click **Select all**.

   d) Click **OK**.

   e) To remove cylinder groups, click **Remove** for the cylinders to remove or click **Remove all**.

5) To add or remove cylinders:

   a) Under **SELECTED CYLINDERS**, click **Add cylinders...** .

      The search result list displays available cylinders.

      NOTE!
      Only cylinders where the cylinder access list includes the selected key are available.

   b) To filter the available cylinders, enter search criteria and click **Search**.

   c) To add cylinders, click **Select** for the cylinders to add or click **Select all**.

   d) Click **OK**.

   e) To remove cylinders, click **Remove** for the cylinders to remove or click **Remove all**.

6) Click **Save**.

4.7.6 Viewing Events for Temporary Access Group

The Events tab is used for traceability of administrator operations in CWM, such as adding and removing keys in a temporary access group.

1) Find the temporary access group and go to its detailed information view.

   See *Section 4.7.1 "Searching for Temporary Access Groups", page 68*.

2) Select the **Events** tab.

   A list with all temporary access group events is displayed.

4.7.7 Removing Redundant Key Authorisations

Removing redundant authorisations is useful when introducing access profiles in a locking system where the keys are already configured with explicit authorisations. Explicit authorisations are considered redundant if the key is also associated with an access profile that gives access to the same cylinder or cylinder group.

> **HINT!**
> It is recommended to remove redundant authorisations to give a better overview of authorisations.

1) Search for the keys.

   See *Section 4.2.1 "Searching for User Keys", page 33*.

2) In the search result list, select the keys.

3) Click **Remove redundant authorisations...**.

4) Click **OK**.

4.8 Viewing Authorisations

4.8.1 Viewing Accessible Cylinders for Keys or Key Groups

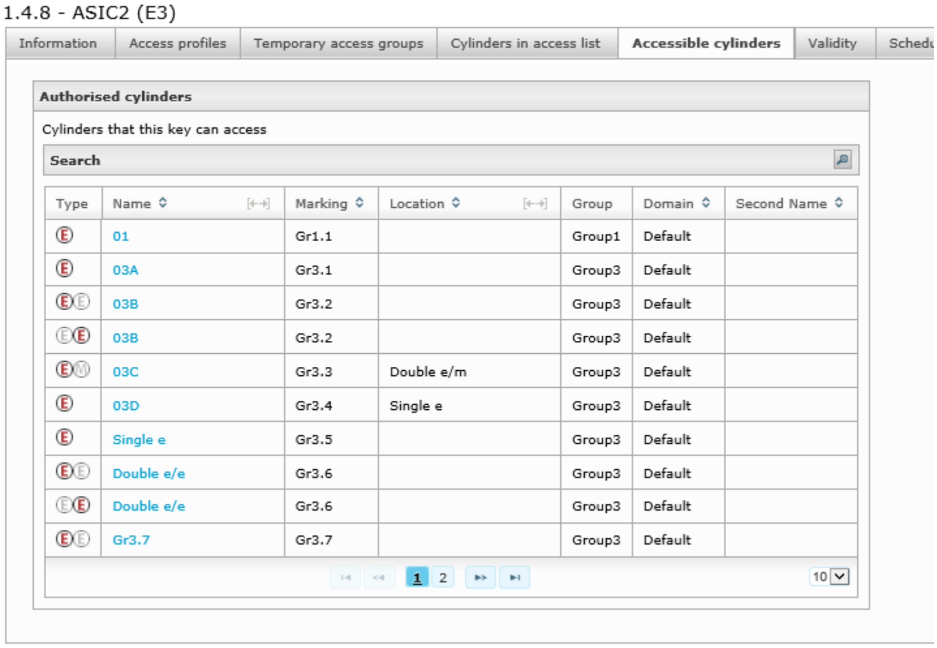
The actual authorisations show the cylinders a certain key has access to, considering both the key access list and the cylinder access lists. These are the cylinders that the key can actually open.

1) Find the key or key group and go to its detailed information view.

   See *Section 4.3.1 "Searching for Key Groups", page 51*.

2) Select the **Accessible cylinders** tab.

   A list with all cylinders where the key group is authorised is displayed.



1.4.8 - ASIC2 (E3)

Authorised cylinders

Cylinders that this key can access

Type	Name	Marking	Location	Group	Domain	Second Name
Ⓔ	01	Gr1.1		Group1	Default	
Ⓔ	03A	Gr3.1		Group3	Default	
ⒺⒺ	03B	Gr3.2		Group3	Default	
ⒺⒺ	03B	Gr3.2		Group3	Default	
ⒺⓂ	03C	Gr3.3	Double e/m	Group3	Default	
Ⓔ	03D	Gr3.4	Single e	Group3	Default	
Ⓔ	Single e	Gr3.5		Group3	Default	
ⒺⒺ	Double e/e	Gr3.6		Group3	Default	
ⒺⒺ	Double e/e	Gr3.6		Group3	Default	
ⒺⒺ	Gr3.7	Gr3.7		Group3	Default	

For double cylinders, the A-side and the B-side are listed separately. The symbol indicates which side that is concerned (the other side is greyed out).

ⒺⒺ Information concerns the A-side

ⒺⒺ Information concerns the B-side

NOTE!
Individual keys might be excluded from access. See *Section 8.1.2 "Electronic Authorisation", page 152*.

4.8.2 Viewing Keys With Access to Cylinders or Cylinder Groups

Keys with access means keys that can access the cylinder considering both the key access lists and the cylinder access lists. These are the keys that can actually open the cylinder.

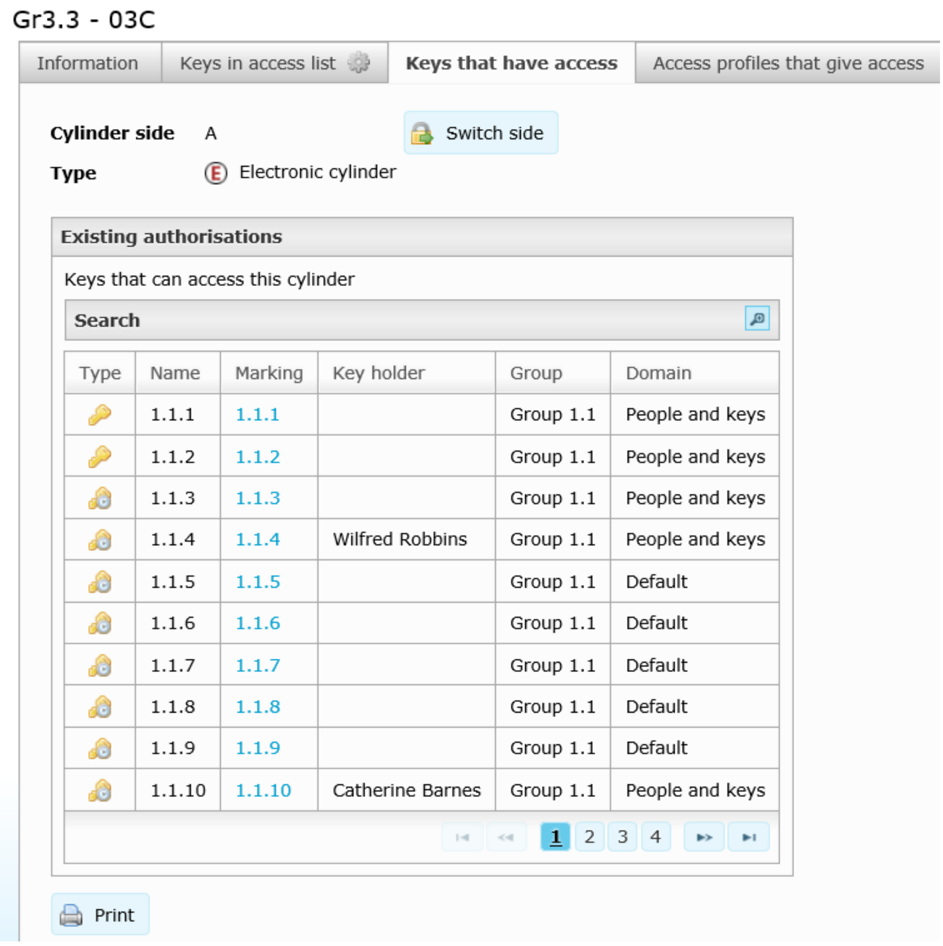
1) Find the cylinder or cylinder group and go to its detailed information view.

- To search for a cylinder, see *Section 4.4.1 "Searching for Cylinders", page 52*.
- To search for a cylinder group, see *Section 4.5.1 "Searching for Cylinder Groups", page 63*.

2) Select the **Keys that have access** tab.

A list of keys with actual access to the cylinder or cylinder group is displayed.

Keys belonging to authorised key groups are displayed individually.



Gr3.3 - 03C

Cylinder side A

Type Ⓔ Electronic cylinder

Existing authorisations

Keys that can access this cylinder

Type	Name	Marking	Key holder	Group	Domain
🔑	1.1.1	1.1.1		Group 1.1	People and keys
🔑	1.1.2	1.1.2		Group 1.1	People and keys
🔑	1.1.3	1.1.3		Group 1.1	People and keys
🔑	1.1.4	1.1.4	Wilfred Robbins	Group 1.1	People and keys
🔑	1.1.5	1.1.5		Group 1.1	Default
🔑	1.1.6	1.1.6		Group 1.1	Default
🔑	1.1.7	1.1.7		Group 1.1	Default
🔑	1.1.8	1.1.8		Group 1.1	Default
🔑	1.1.9	1.1.9		Group 1.1	Default
🔑	1.1.10	1.1.10	Catherine Barnes	Group 1.1	People and keys

4.8.3 Viewing Access Profiles That Give Access to Cylinder or Cylinder Group

Keys associated with an access profile automatically have access to the cylinders and cylinder groups specified by that access profile. Note that this does not necessarily mean that the key can open the cylinder, since actual access depends also on the access list in the cylinder.

1) Find the cylinder or cylinder group and go to its detailed information view.

   - To search for a cylinder, see *Section 4.4.1 "Searching for Cylinders", page 52*.
   - To search for a cylinder group, see *Section 4.5.1 "Searching for Cylinder Groups", page 63*.

2) Select the **Access profiles that give access** tab.

See also *Section 4.9.4 "Configuring Access Profile Authorisations", page 78*.

4.9 Configuring Authorisations

4.9.1 Configuring Authorisations in Keys

Dynamic Keys have an access list that includes the cylinder and cylinder groups that the key is authorised to open. Configuring authorisations in keys means editing the explicit authorisations in this access list. The access list can also contain implicit authorisations that originate from access profiles. To configure access profile authorisations, see *Section 4.9.4 "Configuring Access Profile Authorisations", page 78*.

Note that a cylinder included in the key access list does not necessarily mean that the key has actual access, as actual access depends also on the access list in the cylinder. To view the cylinders that the key can actually open, see *Section 4.8.1 "Viewing Accessible Cylinders for Keys or Key Groups", page 72*.

To remove all access for a cylinder, see *Section 4.9.3 "Removing All Access for a Cylinder", page 78*.

For more information about authorisation principles, see *Section 8.1 "Authorisation Principles", page 152*.

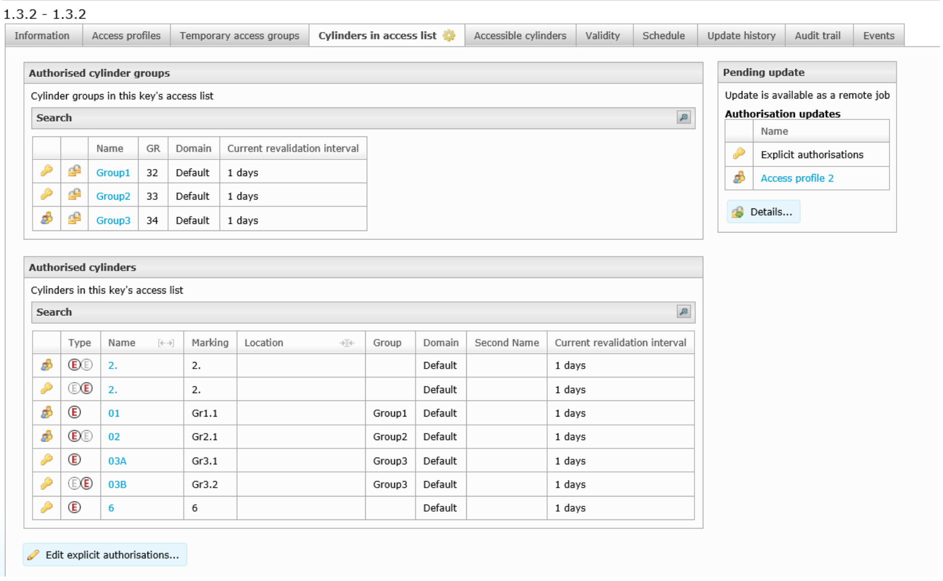
1) Find the key and go to its detailed information view.

   To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Select the **Cylinders in access list** tab.

   Currently authorised cylinder groups and cylinders are displayed.



1.3.2 - 1.3.2

Authorised cylinder groups

Cylinder groups in this key's access list

		Name	GR	Domain	Current revalidation interval
🔑	🔒	Group1	32	Default	1 days
🔑	🔒	Group2	33	Default	1 days
👥	🔒	Group3	34	Default	1 days

Pending update

Update is available as a remote job

Authorisation updates

	Name
🔑	Explicit authorisations
👥	Access profile 2

Authorised cylinders

Cylinders in this key's access list

	Type	Name	Marking	Location	Group	Domain	Second Name	Current revalidation interval
👥	ⒺⒺ	2.	2.			Default		1 days
🔑	ⒺⒺ	2.	2.			Default		1 days
👥	Ⓔ	01	Gr1.1		Group1	Default		1 days
👥	ⒺⒺ	02	Gr2.1		Group2	Default		1 days
🔑	Ⓔ	03A	Gr3.1		Group3	Default		1 days
🔑	ⒺⒺ	03B	Gr3.2		Group3	Default		1 days
🔑	Ⓔ	6	6			Default		1 days

The access list contains explicit authorisations.

🔑 Explicit authorisation

👥 Authorisation from access profile

For double cylinders, the A-side and the B-side are listed separately. The symbol indicates which side that is concerned (the other side is greyed out).

ⒺⒺ Information concerns the A-side

ⒺⒺ Information concerns the B-side

Pending remote updates are listed under **Pending update**.

3) Click **Edit explicit authorisations...**.

The defined explicit authorisations for the key are displayed.

HINT!
Removing cylinder groups and cylinders can be done directly in this view by clicking **Remove** for the cylinder group or cylinder to remove.

When removing from keys with long access lists, it might be convenient to filter the cylinder groups and cylinders first.

4) To add or remove cylinder groups:

a) Under **Explicit cylinder group authorisations**, click **Change cylinder groups...** .

All available cylinder groups are displayed.

b) To filter the available cylinder groups, enter search criteria and click **Search**.

c) Click **Select** for the cylinder groups to add, or click **Select all**.

d) Click **Remove** for the cylinder groups to remove, or click **Remove all**.

e) Click **OK**.

5) To add or remove individual cylinders:

a) Under **Explicit cylinder authorisations**, click **Change cylinders...** .

The search result list displays available cylinders.

> **NOTE!**
> Only cylinders where the cylinder access list includes the selected key are available.

b) To filter the available cylinders, enter search criteria and click **Search**.

c) Click **Select** for the cylinders to add, or click **Select all**.

d) Click **Remove** for the cylinders to remove, or click **Remove all**.

e) Click **OK**.

6) Click **Save**.

Progress is shown in a pop-up window with the estimated duration of the operation.

7) If the key is scanned, click **Write access list to key locally** to update the key.

> **NOTE!**
> If revalidation is enabled on the key, the key is revalidated in the Local PD during the programming process.

Otherwise, a key update job is created.

4.9.2 Configuring Authorisations in Cylinders

A cylinder access list is stored in cylinders and includes the keys and key groups that are authorised to open the cylinder. Configuring authorisations in cylinders means editing this access list.

For user keys, the fact that a key is included in the cylinder access list does not necessarily mean that the key has actual access, as actual access also depends on the access list in the key. To view the keys that can actually open the cylinder, see *Section 4.8.2 "Viewing Keys With Access to Cylinders or Cylinder Groups", page 73*.

For more information about authorisation principles, see *Section 8.1 "Authorisation Principles", page 152*.

1) Find the cylinder and go to its detailed information view.

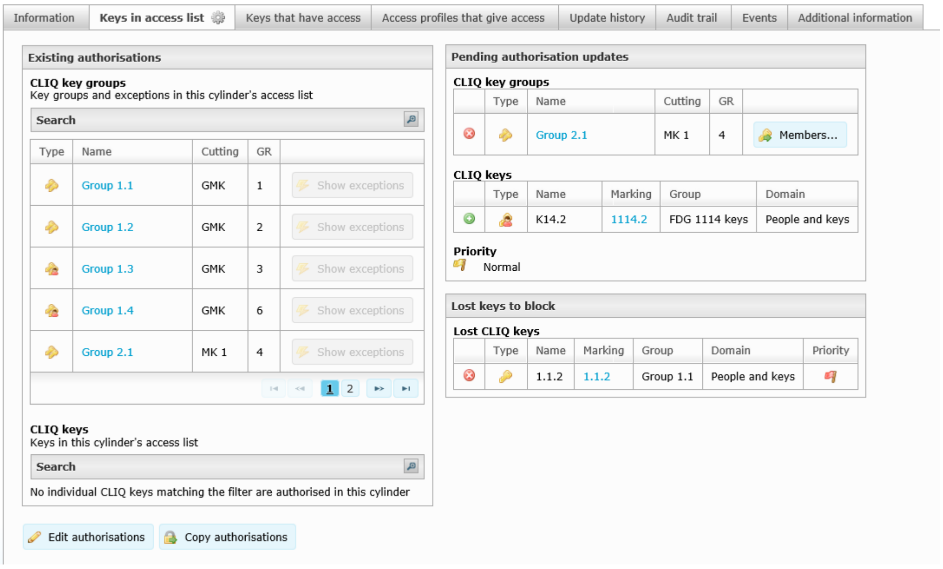
See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Select the **Keys in access list** tab.

Currently authorised key groups and keys are displayed.

Any Cylinder Programming Jobs with authorisation updates are listed under **Pending authorisation updates**.

Any Cylinder Programming Jobs due to lost keys are listed under **Lost keys to block**.



Existing authorisations

CLIQ key groups
Key groups and exceptions in this cylinder's access list

Search

Type	Name	Cutting	GR	
	Group 1.1	GMK	1	Show exceptions
	Group 1.2	GMK	2	Show exceptions
	Group 1.3	GMK	3	Show exceptions
	Group 1.4	GMK	6	Show exceptions
	Group 2.1	MK 1	4	Show exceptions

CLIQ keys
Keys in this cylinder's access list

Search

No individual CLIQ keys matching the filter are authorised in this cylinder

Pending authorisation updates

CLIQ key groups

	Type	Name	Cutting	GR	
⊗		Group 2.1	MK 1	4	Members...

CLIQ keys

	Type	Name	Marking	Group	Domain
⊕		K14.2	1114.2	FDG 1114 keys	People and keys

Priority
Normal

Lost keys to block

Lost CLIQ keys

	Type	Name	Marking	Group	Domain	Priority
⊗		1.1.2	1.1.2	Group 1.1	People and keys	

3) To view keys that belong to an authorised key group but are excluded from access, click **Show exceptions**.

4) Click **Edit authorisations**.

5) **To Add Key Groups or Individual Keys**

1. Click **Add CLIQ key group**.

   The search result list displays all available key groups.

2. To filter the available key groups, enter search criteria and click **Search**.

3. Click **Select** for the key groups to add.

> **NOTE!**
> When a key group is added to an access list, 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.

4. Click **Done**.

To Exclude Keys from a Key Group Authorisation

1. Click **Edit** for the key group.

2. Click **Unauthorise** for the keys to exclude from access.

To Reauthorise Keys from a Key Group Authorisation

> **NOTE!**
> To reauthorise the key, the key needs to be reported as found.
>
> Click **Report found** on the key's detailed information view.

1. Click **Edit...** for the key group.

2. Click **Authorise** for the keys to authorise the access to the cylinder.

To Remove Key Groups or Individual Keys
Click Remove for the key group to remove.

6) When editing is complete, click **To view**.

   A cylinder programming job is created.

   To program cylinders, see *Section 4.4.13 "Programming Cylinders", page 59*.

Authorisations for several cylinders can be edited at the same time. Select the cylinders in the search result list (see *Section 4.4.1 "Searching for Cylinders", page 52*) and click **Add authorisations** or **Revoke authorisations**.

4.9.3 Removing All Access for a Cylinder

Individual cylinders can be removed from all keys, access profiles and temporary access groups.

The possibility to remove all access for a cylinder requires a locking system with Dynamic Keys.

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Select **Remove key side authorisations**.

> ℹ **NOTE!**
> To remove the access, all keys that used to have access to the cylinder must be updated.

> ℹ **NOTE!**
> **Remove key side authorisations** only removes the cylinder from the access list on keys that support remote updates.
>
> To see if there are any non-remote keys with access to the cylinder, select the **Keys that have access** tab. For each of these keys, put the key in the Local PD, scan the key, select the **Cylinders in access list** tab, click **Edit explicit authorisations** and remove the cylinder.
>
> For information about remote features, see *Section 8.3.1 "Remote Feature Overview", page 166*.

3) In the pop-up window, click **OK**.

4.9.4 Configuring Access Profile Authorisations

Configuring access profile authorisations means editing the implicit authorisations for keys and people associated with the access profile.

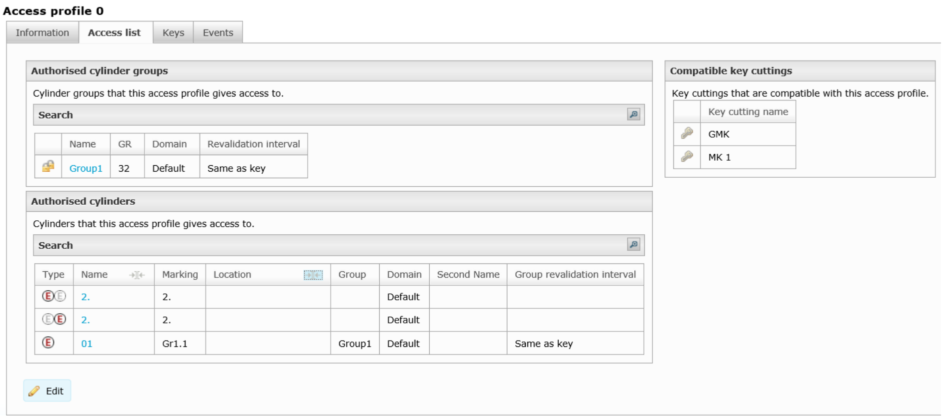
1) Find the access profile and go to its detailed information view.

   See *Section 4.6.1 "Searching for Access Profiles", page 65*.

2) Select the **Access list** tab.

   Currently authorised cylinders and cylinder groups are displayed.

3) Click **Edit**.



Access profile 0

Authorised cylinder groups

Cylinder groups that this access profile gives access to.

Search

	Name	GR	Domain	Revalidation interval
	Group1	32	Default	Same as key

Compatible key cuttings

Key cuttings that are compatible with this access profile.

	Key cutting name
	GMK
	MK 1

Authorised cylinders

Cylinders that this access profile gives access to.

Search

Type	Name	Marking	Location	Group	Domain	Second Name	Group revalidation interval
EE	2.	2.			Default		
EE	2.	2.			Default		
E	01	Gr1.1		Group1	Default		Same as key

For double cylinders, the A-side and the B-side are listed separately. The symbol indicates which side that is concerned (the other side is greyed out).

EE Information concerns the A-side

EE Information concerns the B-side

4) **To add cylinders or cylinder groups**

1. Click **Add cylinders...** or **Add cylinder groups...**.

   The pop-up window shows the list of availabe cylinders or cylinder groups.

2. To filter the result, enter search criteria and click **Search**.

3. Click **Select** for the items to add or click **Select all**.

4. Click **OK**.

To remove cylinders or cylinder groups

1. Click the search icon and enter the search criteria.

2. Click **Search**.

   The table shows the search result.

3. – To remove individual items:

     Click **Remove**.

   – To remove all items in the search result:

     Click **Remove all listed**.

5) Flexible revalidation can also be edited in this view. See *Section 4.10.2 "Configuring Flexible Revalidation", page 83*.

6) Click **Save** to exit the edit more.

See also *Section 8.2.4 "Access Profiles", page 162*.

4.9.5 Selecting Employee or Visitor's Access Profiles

Access profiles are only applicable to dynamic keys, other types of keys will not be included.

1) Find the employee or visitor and go to its detailed information view.

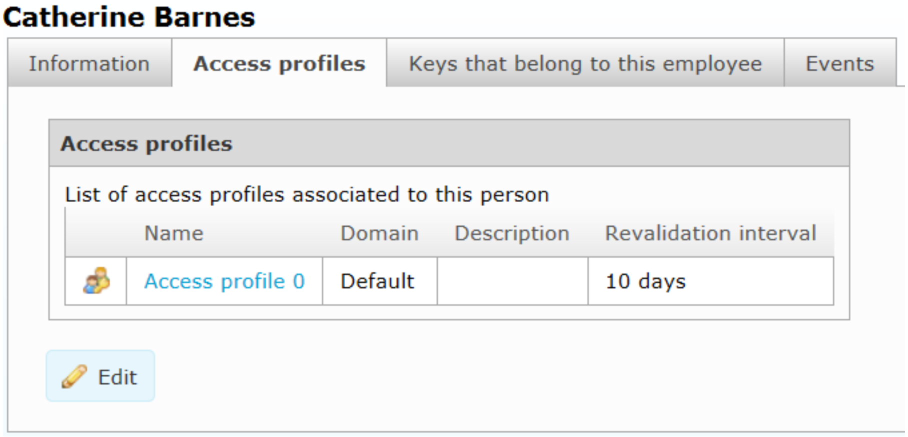
   See *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

2) Select the **Access profiles** tab.

   The search result list displays the access profiles currently associated with the employee or visitor.

3) Click **Edit**.

   A list of associated access profiles is displayed.



Catherine Barnes

Access profiles

List of access profiles associated to this person

	Name	Domain	Description	Revalidation interval
	Access profile 0	Default		10 days

4) To add access profiles:

   a) Click **Add access profiles**.

      The search result list displays all available access profiles.

   b) To filter the available access profiles, enter **Name**, **Description**, **Domain** and/or **Tags** in the Search field.

   c) Click **Select** to select one access profile or click **Select all**.

   d) Click **Done**.

5) To remove access profiles, click **Remove** to remove one access profile or click **Remove all**.

6) Click **Save**.

Access profiles for several employees or visitors can be simultaneously added or removed. Select the employees or visitors in the search result list and click **Add access profiles** or **Remove access profiles**.

See also *Section 8.2.4 "Access Profiles", page 162*.

4.9.6 Selecting Key's Access Profiles

Access profiles are only applicable to dynamic keys.

1) Find the key and go to its detailed information view.

   To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Select the **Access profiles** tab.

   The search result list displays the access profiles currently associated with the key.

3) Click **Edit**.

4) To add access profiles:

a) Click **Add access profiles**.

The search result list displays all available access profiles.

b) To filter the available access profiles, enter search criteria and click **Search**.

c) Click **Select** to select one access profile or click **Select all**.

d) Click **Done**.

5) To remove access profiles, click **Remove** to remove one access profile or click **Remove all**.

6) Click **Save**.

Access profiles for several keys can be edited at the same time. Select the keys in the search result list and click **Add access profiles** or **Remove access profiles**.

See also *Section 8.2.4 "Access Profiles", page 162*.

4.9.7 Selecting Temporary Access Groups' Access Profiles

1) Find the temporary access group and go to its detailed information view.

See *Section 4.7.1 "Searching for Temporary Access Groups", page 68*.

2) Select the **Access profiles** tab.

3) Click **Edit**.

4) To add access profiles to a temporary access group:

a) Click **Add access profiles...**.

b) Click **Select** for individual access profiles to add. Click **Select all** to add all access profiles.

c) Click **Done**.

d) Click **Save**.

5) To remove access profiles from a temporary access group:

a) Click **Remove** for individual access profiles to remove. Click **Remove all** to remove all access profiles.

b) Click **Save**.

4.10 Configuring Key Validity and Schedule

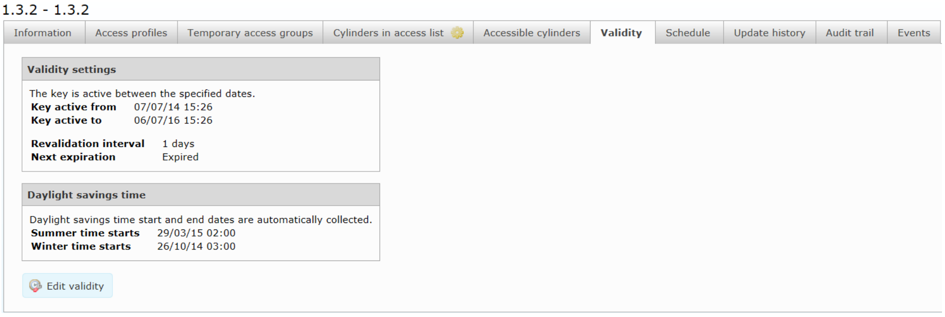
4.10.1 Configuring Key Validity, Revalidation, and PIN Validation

1) Find the key and go to its detailed information view.

To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Select the **Validity** tab.



Validity settings

The key is active between the specified dates.

Key active from	07/07/14 15:26
Key active to	06/07/16 15:26
Revalidation interval	1 days
Next expiration	Expired

Daylight savings time

Daylight savings time start and end dates are automatically collected.

Summer time starts	29/03/15 02:00
Winter time starts	26/10/14 03:00

The Validity tab displays:

- Validity settings: If the key is always active, if it is always inactive or the dates between which the key is active.
- If revalidation is used:
  - **Revalidation interval**: The time the key stays active after a revalidation, before it needs to be revalidated again.
  - **Next expiration**: Date and time when the key becomes inactive if not revalidated.

    When enabling revalidation remotely on a key that is **Always active**, **The key can always be revalidated** is displayed, the next expiration will be **Never** until the key is revalidated for the first time.

    When enabling revalidation remotely on a key that is **Active between dates**, this will be equal to **Key active to** until the key is revalidated for the first time.
- If PIN validation is used:
  - **PIN validation interval**: The time the key stays active after a PIN validation, before the PIN code needs to be entered again.
- Daylight savings time settings

3) Click **Edit validity**.

4) Select if the key will be **Inactive**, **Active between selected dates** or **Always active**.

5) If **Active between selected dates** is chosen, enter **Key active from** and **Key active to**.

6) To configure Revalidation:

    a) Select **Use key revalidation**.

    b) Enter a number of days, hours, and minutes for **Revalidation interval**.

    This is the time the key stays active after revalidation in a Remote PD.

    c) To allow revalidation only once, select **One-time update**.

7) To configure PIN validation:

    a) Select **Use PIN validation**.

b) Enter a number of days, hours, and minutes for **PIN validation interval**.

This is the time the key stays active after validation with PIN.

The specified interval needs to be somewhere between one minute and 45 days.

c) A random PIN code is automatically generated for **New initial PIN**. It is also possible to overwrite the generated PIN and enter a New initial PIN manually.

Select **Show value** to make the PIN code visible.

If the key holder has a registered email address, an email with the initial PIN code is sent. This PIN code needs to be changed by the user at the first use.

8) To confirm the updates:

a) If the key is scanned, click **Write to key**.

The key is updated with the new settings.

b) If the key is not scanned, click **Send remote update**.

A remote update job is created.

Validity, Revalidation, and PIN validation can be edited for several keys simultaneously. Select the keys in the search result list and click **Change validity settings...** and follow the instructions.

See also *Section 8.1.4 "Key Validity", page 154*, *Section 8.1.5 "Key Revalidation", page 154*, and *Section 8.1.7 "PIN Validation", page 157*.

4.10.2 Configuring Flexible Revalidation

CAUTION!
Since Flexible Revalidation is an advanced and complex feature, it is recommended to read *Section 8.1.6 "Flexible Revalidation", page 156* carefully before configuring it.

Prerequisites:

- At least one user key has firmware with Flexible Revalidation support (see *Section 9.7 "Firmware Dependent Functionality", page 192*).
- The feature is enabled in **System settings** (see *Section 6.4 "Editing System Settings", page 94*).

NOTE!
When using Flexible Revalidation, all keys that are affected by the revalidation settings on access profiles or cylinder groups must have revalidation enabled.

1) To set the revalidation interval on an access profile:

a) Find the access profile and go to its detailed information view.

See *Section 4.6.1 "Searching for Access Profiles", page 65*.

b) Click **Edit**.

c) Select option for **Revalidation**.

- To specify a revalidation interval, select **Use specific interval**.
- To leave the revalidation interval unspecified, select **Use revalidation interval from cylinder groups**.

  The revalidation interval set on cylinder groups is used for the cylinder groups where an interval has been specified. Otherwise, the revalidation interval set on keys is used.

d) If **Use specific interval** was selected, enter the interval as a number of days, hours, and minutes.

e) Click **Save**.

f) The revalidation interval for several access profiles can be edited simultaneously. Select the access profiles in the search result list and click **Edit revalidation interval**.

2) To set the revalidation interval on a cylinder group:

a) Find the cylinder group and go to its detailed information view.

See *Section 4.5.1 "Searching for Cylinder Groups", page 63*.

b) Click **Edit**.

c) Select option for **Revalidation**.

- To specify a revalidation interval, select **Use specific interval**.
- To leave the revalidation interval unspecified, select **Use revalidation interval from keys**.

  The revalidation interval set on keys is used.

d) If **Use specific interval** was selected, enter the interval as a number of days, hours, and minutes.

e) Click **Save**.

f) The revalidation interval for several cylinder groups can be edited simultaneously. Select the cylinder groups in the search result list and click **Edit revalidation interval**.

3) To check whether the revalidation intervals for a key are configured as intended, view the **Current revalidation interval** column for each cylinder in the Key Access List. See *Section 4.9.1 "Configuring Authorisations in Keys", page 74*.

See also *Section 8.1.6 "Flexible Revalidation", page 156*.

4.10.3 Configuring Key Schedule

There are two types of schedules, Basic Schedule and Multiple Time Window Schedule (see *Section 8.1.8 "Key Schedules", page 158*). The key firmware determines which type that is used. For information about which key firmware versions support which schedule type, see *Section 9.7 "Firmware Dependent Functionality", page 192*

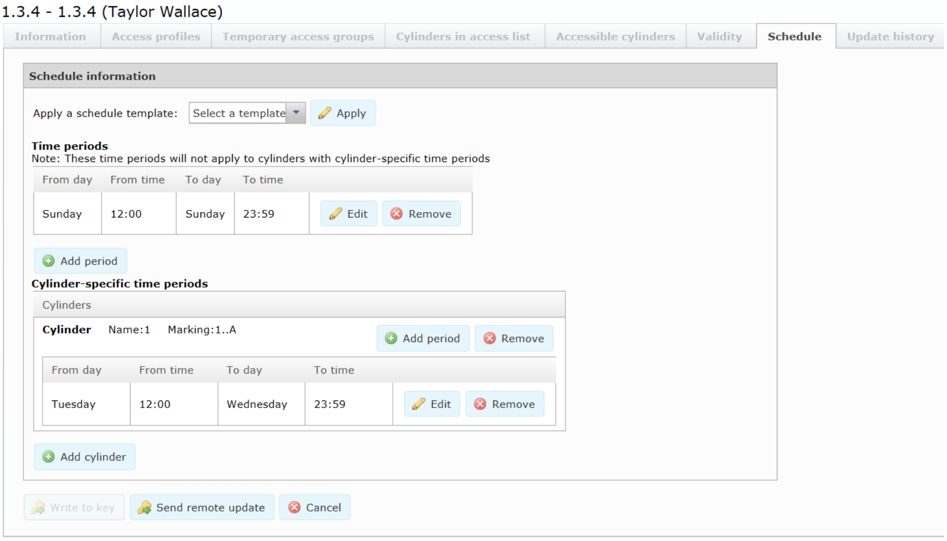
1) Find the key and go to its detailed information view.

To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Select the **Schedule** tab.

3) Click **Edit Schedule**.



1.3.4 - 1.3.4 (Taylor Wallace)

Schedule information

Apply a schedule template: Select a template

Time periods

Note: These time periods will not apply to cylinders with cylinder-specific time periods

From day	From time	To day	To time
Sunday	12:00	Sunday	23:59

Cylinder-specific time periods

Cylinders

Cylinder Name:1 Marking:1..A

From day	From time	To day	To time
Tuesday	12:00	Wednesday	23:59

4) To apply a schedule template, select a template in the drop-down menu and click **Apply**.

The template is applied, but the schedule can still be edited.

5) Determine if the key has a Basic Schedule or a Multiple Time Window Schedule.

If the key has a Multiple Time Window schedule, in addition to **Time periods**, **Cylinder-specific time periods** is also displayed.

6) To edit a Basic Schedule:

a) Click **Edit** on the row of day to edit.

b) Select **All day**, **Never** or **Custom**.

c) If the custom option is selected, enter the period values **From time** and **To time**.

d) Click **Save**.

7) To edit a Multiple Time Window Schedule:

a) To add a period:

- Click **Add period**.
- Enter the period values **From date** and **To date**.
- Click **Save**.

b) To edit period, click **Edit period**.

c) To remove a period, click **Remove period**.

d) To add a period for a specific cylinder:

- Click **Add cylinder**.

  The search result list displays all available cylinders.
- To filter the available cylinders, enter search criteria and click **Search**.
- Click **Select** for the cylinder to add.
- Add, edit, and remove periods for the cylinder.

> **NOTE!**
>
> **For generation 1 keys**:
>
> - For cylinders included in the key access list individually (not as a part of a cylinder group), specifying one or more time periods for a cylinder means that the general schedule is ignored for that cylinder.
> - For cylinders included in the key access list as a part of a cylinder group, the cylinder specific time periods are ignored.
>
> **For generation 2 keys**:
>
> - Specifying one or more time periods for a cylinder means that the general schedule is ignored for that cylinder.

8) To confirm the updates:

   a) If the key is scanned, click **Write to key**.

      The key is updated with the new settings. If revalidation is enabled on the key then the key will be revalidated at the same time.

   b) If the key is not scanned, click **Send remote update**.

      A key update job is created.

4.10.4 Configuring Key Group Schedule

A schedule can be configured for all keys in a key group.

1) Find the key group and go to its detailed information view.

   See *Section 4.3.1 "Searching for Key Groups", page 51*.

2) Click **Bulk key configuration**.

3) Select **Set schedule**.

4) Click **Next**.

5) Enter the schedule settings. For reference, see *Section 4.10.3 "Configuring Key Schedule", page 84*.

6) Click **Next**.

   The selected settings are displayed.

7) To confirm the updates, click **Apply**.

   Key update jobs are created.

4.11 Managing Audit Trails

Quartz and Dynamic Keys and cylinders have an audit trail feature.

An audit trail is a list of events and shows access attempts, the key holder at the time, and the programming records of the device. For more information, see *Section 8.6 "Audit Trails", page 171*.

4.11.1 Viewing Audit Trails for User Key

1) Find the key and go to its detailed information view.

   To search for the key and display the detailed information view, see *Section 4.2.1 "Searching for User Keys", page 33*

   To scan the key in the Local PD and display the detailed information view, see *Section 4.2.2 "Scanning a User Key", page 34*

2) Select the **Audit trail** tab.

   If any audit trail has been requested and read by a Remote PD, a list of the audit trail events is displayed.

3) If the **Approvals** feature is enabled (see *Section 6.4 "Editing System Settings", page 94*):

   a) To request a new audit trail, click **Request remote audit trail**.

   b) Enter a comment to the approver and click **Send request**.

4) If the **Approvals** feature is disabled (see *Section 6.4 "Editing System Settings", page 94*):

   - If the key is in the Local PD, click **Read audit trail**. This may take some time.
   - If the key is not in the Local PD, click **Request remote audit trail**.

     The audit trail is read the next time the key is inserted in a Remote PD and saved in CWM. It will then be displayed in the audit trail tab.

     > **NOTE!**
     > **Request remote audit trail** is automatically turned on at key hand-out and turned off at key hand-in.

5) Optional: Export the table as a PDF. See *Section 4.11.5 "Exporting Audit Trail Information", page 88*.

See also *Section 8.6 "Audit Trails", page 171*.

4.11.2 Viewing Audit Trails for Cylinder

> **NOTE!**
> The cylinder audit trails which record the access attempted by Normal Keys do not display time in the **Time in key** column.

1) Find the cylinder and go to its detailed information view.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Select the **Audit trail** tab.

   If audit trails have already been collected they are displayed as a list.

3) To request a new audit trail, click **Request audit trail**.

   If **Approvals** is enabled (see *Section 6.4 "Editing System Settings", page 94*), enter a comment to the approver.

4) Select **Priority**.

   Urgent jobs should have a higher priority.

5) Click **OK**.

A programming job for collecting an audit trail from the cylinder is created.

To get the audit trail from the cylinder, see *Section 4.4.13 "Programming Cylinders", page 59*.

6) Optional: Export the table as a PDF. See *Section 4.11.5 "Exporting Audit Trail Information", page 88*.

See also *Section 8.6 "Audit Trails", page 171*.

4.11.3 Viewing Audit Trail Archive

The audit trail archive contains all audit trails collected from keys and cylinders in the locking system. By selecting a key or a cylinder, it is possible to view all collected audit trails for that key or cylinder.

There are no restrictions on how many audit trails will fit in the audit trail archive. The archive can be configured to automatically remove audit trails older than a defined number of days, see *Section 6.4 "Editing System Settings", page 94*.

1) Select **System Info » Audit trail archive**.

   A list of the audit trail events shows interactions between keys, cylinders, C-Keys, Remote PDs and/or the software.

   > ℹ **NOTE!**
   > Due to the large scale of the audit trail data, some extended information such as historical key holders or historical domains is available with delay. While this information is processed in the background, **Processing data** is displayed in the list.

2) Specify the search criteria and click **Search**.

   For example, to view all key interactions with a specific cylinder:

   Select **Key** under **Collected from**, then select **Cylinder** specifying **Name** or **Marking** of the specific cylinder under **Event by**.

3) Optional: Export the table as a PDF. See *Section 4.11.5 "Exporting Audit Trail Information", page 88*.

4.11.4 Exporting Audit Trail Information

1) Display a list of audit trails:

   - To view the audit trail for a specific key, see *Section 4.11.2 "Viewing Audit Trails for User Key", page 86*.
   - To view the audit trail for a specific cylinder, see *Section 4.11.3 "Viewing Audit Trails for Cylinder", page 87*.
   - To view all the audit trail archive, see *Section 4.11.4 "Viewing Audit Trail Archive", page 88*.

2) Click **Print full audit trail** to print or save the table in PDF format.

   The table appears in a pop-up window.

3) - To save, click the save icon and specify a folder to save.
   - To print out, click **...** and select **Print**.

4.11.5 Approving Audit Trail Requests

If the **Approvals** feature is enabled, audit trail requests must be approved before they can be executed. A C-Key with the approver role must be used to log into the system to approve pending audit trail requests.

To change the **Approvals** setting, see *Section 6.4 "Editing System Settings", page 94*.

1) Insert the approver C-Key in the left slot of the local PD.
2) Log in to the system.

   Only the **Work** menu and **Settings** menu are available.
3) Select **Work » Jobs for approval**.

   A list of jobs pending approval is displayed.
4) Click **Respond**.
5) To approve: Enter an optional comment, click **Approve**.

   To reject: Enter an optional comment, click **Reject**.

To view already approved or rejected jobs, select the **Approval history** tab.

5 Setting Up Locking Systems

5.1 Locking System Setup Overview

This overview describes the work flow when setting up the locking system for the first time.

Prerequisites:

- The database is prepared and the server software is installed on the CWM server.
- If it is a remote system, the database is prepared and the server software is installed also on the Remote Server.
- Firewalls and proxys are configured to allow SSL traffic.
  - From the client PCs to the CWM Server (Port 443 and 8443).
  - From the Remote PDs to the Remote Server (Port 443).
  - From the CWM Server to the SMTP server (Port 25).

1) Set up a CWM Client.

   See *Section 2.1 "CWM Client Setup Overview", page 12*.

2) Install the Master C-Key Certificate.

   See *Section 5.2 "Installing Master C-Key Certificate", page 90*.

3) Log in to CWM.

   See *Section 5.3 "Logging in to a new locking system", page 91*.

4) Set the CWM language.

   See *Section 3.4 "Setting CWM Language", page 18*.

5) Install a licence.

   See *Section 6.1.1 "Installing Licences", page 93*.

6) Perform Initial Configuration.

   See *Section 5.4 "Performing Initial Configuration", page 92*.

5.2 Installing Master C-Key Certificate

If DCS integration is enabled:

An email address for the Master C-Key holder is specified in DCS. Within an hour of the locking system database preparation, an email is sent to that email address.

The number of times a Master C-Key certificate can be generated is determined by a setting in DCS.

How to install the Master C-Key certificate is same as the way to install the C-Key certificate. For more information, see *Section 3.2.1 "Enrolling C-Key Certificate via CLIQ Connect PC", page 16*.

If DCS integration is not enabled:

The Master C-Key certificate is already provided. For more information on how to install the certificate, see *Section 3.2.2 "Installing the C-Key Certificate Manually", page 16*.

5.3 Logging in to a new locking system

Prerequisites:

- The Local PD is installed. See *Section 2.2 "Installing Local PDs", page 12*.
- A supported Internet browser is used. See *Section 9.8 "Client PC Requirements", page 193*.
- CLIQ Connect PC is installed and running on the computer.

  See *Section 2.3 "Installing CLIQ Connect PC", page 12*.
- CLIQ Connect PC is configured and connected to CWM.

  See *Section 2.4 "Configuring CLIQ Connect PC", page 13*.
- The Master C-key with a PIN code is available.
- A valid certificate for the Master C-key is installed. See *Section 5.2 "Installing Master C-Key Certificate", page 90*.
- The URL to CWM is available.

1) Insert the C-Key in the left slot of the Local PD.
2) Navigate to the CWM start page.
3) Select the certificate for the C-Key.

   CWM Login page is shown.
4) Click **Login**.
5) Enter the PIN code for the C-Key.

   The CLIQ Connect PC asks to confirm the usage of the key.
6) Click **Confirm**.
7) Select **Base time zone** from the drop-down list.

   NOTE!
   This setting cannot be changed after clicking **Confirm**.
8) Select the choices for **Approval of audit trail requests** from the followings:

   - **Disabled**

     If this is selected, all administrators can request audit trail information without approval by another administrator.
   - **Enabled**

     If this is selected, all administrators require approval from another administrator to request audit trail information.

   For more details about the approver role for audit trails, see *Section 4.11.6 "Approving Audit Trail Requests", page 89*.
9) Click **Activate extension import**.

   The **Confirmation** window is opened.
10) Check the settings carefully.

⚠ **WARNING!**
The settings cannot be changed later.

11) Click **Confirm**.

5.4 Performing Initial Configuration

1) Unlock the locking system. See *Section 6.3 "Unlocking the System", page 93*.
2) Edit the system settings. See *Section 6.4 "Editing System Settings", page 94*.
3) Set up the Remote PDs. See *Section 6.5.1 "Setting Up Remote PDs", page 98*.
4) Create the domains. See *Section 6.6.4 "Creating And Deleting Domains", page 117*.
5) Specify domain for the cylinders and cylinder groups. See *Section 6.6.7 "Changing Domain For Cylinders", page 118* and *Section 6.6.8 "Changing Domain For Cylinder Groups", page 118*.
6) Set up access profiles. See *Section 4.6.2 "Creating and Deleting Access Profiles", page 65*.
7) Create receipt templates for hand-out and hand-in receipts. *Section 6.9 "Managing Receipt Templates", page 122*.
8) Create schedule templates. See *Section 6.10 "Managing Schedule Templates", page 124*.
9) Add and delete administrator roles and adjust the role permissions as desired. See *Section 6.7 "Managing Roles and Permissions", page 119*.
10) Issue C-Keys to the locking system administrators. See *Section 6.11.7 "Handing Out C-Keys", page 128*.
11) Import Employee information to CWM. See *Section 6.8 "Importing Employee Information", page 121*.

6 Configuring Locking Systems

6.1 Managing Licences

6.1.1 Installing Licences

Prerequisites:

- A new licence file is available.
  - For manual installation: Stored on a USB flash drive or the computer's hard disk.
  - For automatic retrieval in systems with DSC Integration: Stored in DCS.
- The licence number of the new licence file is higher than that of the installed licence. It is not possible to install an older licence.

1) Select **Administration » License**.

   Information about the currently installed licence, and the features it contains, is displayed.

2) For systems with DCS Integration, and where the licence file is stored in DCS:

   Click **Fetch license**.

   The licence is downloaded and installed.

3) For systems without DCS Integration, or where the licence file is not available in DCS:

   a) Click **Select...**.

   b) Select the licence file.

   c) Click **Upload**.

      The licence is uploaded and installed.

6.1.2 Viewing Licence Status

1) Select **Administration » License**.

   Information about the currently installed licence, and the features it contains, is displayed.

To install a new licence, see *Section 6.1.1 "Installing Licences", page 93*.

6.2 Locking the System for Maintenance

A locking system can be locked to perform maintenance.

1) Select **Administration » Maintenance**.

2) Select a date and time to lock the specific system for maintenance.

   The chosen time must be at least 10 minutes into the future.

3) Click **Lock locking system**.

6.3 Unlocking the System

1) Select **Administration » Maintenance**.

2) Click **Unlock locking system**.

6.4 Editing System Settings

Some of the system settings described are only applicable for a remote system.

1) Select **Administration » System settings**.

   The system settings are displayed.

2) To edit the system settings, click **Edit**.

3) Update the required settings:

SYSTEM

- **Approvals**. If selected, audit trail requests for cylinders and keys must be approved before audit trails can be collected.

> **NOTE!**
>
> **Restrictions**:
>
> - Logged in with the Master C-Key.
> - To disable the approval feature, first ensure that all pending audit trail jobs are cancelled or completed.
> - To enable the approval feature, first ensure to deactivate **AUTOMATIC AUDIT TRAIL RETRIEVAL** in all C-Keys. See *Section 6.11.13 "Activate or Deactivate Automatic Audit Trail Retrieval for C-Key", page 133*.
>
>   Even after enabling the approval feature, existing pending jobs remain unaffected and do not require approval. Only new audit trails jobs require approvals.

- **CLIQ Remote System** shows whether the Remote functionality is enabled.

  Can only be selected when first setting up the locking system.

- **Supports Cylinder Groups** shows whether the use of cylinder groups is enabled.

  Can only be selected when first setting up the locking system.

- **Base time zone**. Time zone used for different printouts in the application.

  Can only be selected when first setting up the locking system.

- **Web Services Integration** enables communication with other systems, for example HR systems.

- **User messaging** enables CWM to send emails to employees and visitors, for example reminders of overdue keys.

  - **Emails after remote update** controls whether an email listing new access information is sent to key holders after a Remote Update.

    Check the box and click **Configure** to select whether to include mechanical cylinders or not in this email.

    - **Emails after employees data change** controls whether an email listing changes to employee information is sent to the administrator of the domains where the employee's key has actual or pending access to at least one cylinder.

      Check the box and click **Configure** to select which type of changes will result in a notification.

    - **Emails after visitors data change** controls whether an email listing changes to visitor information is sent to the administrator of the domains where the visitor's key has actual or pending access to at least one cylinder.

      Check the box and click **Configure** to select which type of changes will result in a notification.

    - **Emails after Wall PD goes offline** controls whether an email is sent to the specified person when a Wall PD goes offline.

      Check the box and click **Configure** to enter the mail recipient and set the number of consecutive missing heart beats after which notification is sent.

- **Flexible revalidation** makes it possible to set the revalidation interval per access profile and per cylinder group.
- **Silently block lost keys in cylinder during authorisation update**

  Check the checkbox to allow the system to silently add lost keys to the list of unauthorised keys in order to block them in cylinders.

- **Block lost key with user keys** allows a cylinder block job to be programmed onto any user key (Dynamic Key) to block a lost key in the cylinders.

  This is only applicable to a remote system.

- **Block lost keys in new cylinders during extension import** When adding cylinders to a system, any previously reported lost keys may need to be blocked in the new cylinders. If this setting is enabled, CWM automatically generates cylinder programming jobs to block the lost keys when the import file is activated.
- **Hierarchical administrators** (editable only by Super Administrators)

  Check the checkbox to enable the administrator hierarchy functionality, so that the user can choose a flat or hierarchical structure for permissions.

CLIQ REMOTE

- **Service URL**. Remote server used by CWM and Remote PDs. Note that a warning is displayed if the URL does not match the host name defined in the remote server certificate.
- **Alternative service URL**. Option to specify an alternative service URL to the remote server used by CWM and Remote PDs. The URL is visible in the **Settings** tab of the Remote PDs view only if the firmware version of the Wall PD or CLIQ Mobile PD is 4.0 or higher. Note that the **Alternative service URL** targets the same remote server as the **Service URL**.

- **Server CA certificate**. The Certificate Authority (CA) certificate issuing the server certificate on the CLIQ Remote server. It requires super administrator rights to import the certificate.

DEFAULT KEY SETTINGS

- **Enable revalidation in hand out**. If selected, the option of revalidation is available in the key hand out flow.
- **Revalidation interval**. The default setting for the key revalidation interval.
- **Enable PIN validation in hand-out**. If selected, the option of PIN validation is available in the key hand out flow.
- **PIN validation interval**. The default setting for the PIN validation interval.
- **Time until hand in**. The default setting for time until key should be handed in starting from the hand out date. Enter `0` if end time should not be specified.
- **Validity setting**. The default setting for validity of keys.
- **Validity time**. Default setting for how long the key validity time should be if the validity option **Active between selected dates** has been selected.

ADMINISTRATION

- **Default days in overdue key search**. Default search option for overdue keys.
- **User messaging language**. The language used when emails are sent by CWM, for example of overdue keys.
- **Key receipts** defines if key hand-out and hand-in receipts should be printed separately or combined.
- **External links root URL**. A root URL which is used to form external links for keys, employees, and so on.
- **CSV delimiter**, semicolon or comma is selected to delimit entities when exporting CSV files.
- **Audit trails and events**. Audit trails and events that are older than a defined number of days are automatically removed from the audit trail and event archive. The days are counted from the date when the audit trails and events were collected.

  The audit trail and event retention period can be set from one to 366 days by default, or up to 3660 days with an additional licence.

  Starting from CWM 11.6, deletion follows the creation date, which is when the entry was generated on the physical element. This replaces the previous method of using the parse date, which is when the entry was stored in the CWM database.
- **When deleting persons**. When set to **Mark as deleted**, deleting a person changes the status of the person to "deleted" but all information is kept in the database. When set to **Delete permanently** (default setting for new locking systems), deleting a person removes the person and corresponding information from the database altogether. The setting **Delete permanently** supports GDPR and enables functionality to deactivate a person. See *Section 8.9 "Deletion of Personal Data and GDPR Compliance", page 175* for more information.

When changing the setting from **Mark as deleted** to **Delete permanently** all persons that have been marked as deleted are removed permanently.

To change the setting from **Delete permanently** to **Mark as deleted** all deactivated persons must first be activated.

- **Collect last login date** specifies if the last login date for a C-Key certificate is collected. When enabled, the **Last used date** is displayed in the **Certificates** tab in the C-Key detailed view. See *Section 6.11.14 "Listing C-Key Certificates", page 133*.
- **Cylinder custom fields** define and add, or edit custom fields to store additional cylinder information in CWM. The custom field values can be edited in the detailed cylinder view for each cylinder. They can also be used to find cylinders using advanced cylinder search.
- **Initial cylinder domain** defines the assigned domain for new or imported cylinders.
- **Initial person domain** defines the assigned domain for new or imported employees or visitors.
- **Initial key domain** defines the assigned domain for new or imported keys.

NETWORK AUTHENTICATION FOR WALL PD GENERATION 2

- **802.1x authentication**

  If network authentication for any Wall PDs in the system is enabled, it is not possible to select **Disabled** in the system setting level. Click **How to disable authentication?** and fetch the list of the Wall PDs whose network authentication is enabled. To disable the network authentication at the device level, see *Section 6.5.7.1 "Editing Wall PD Settings", page 103*.
- **802.1x authentication server hostname**

  Enter the server hostname.
- **802.1x server CA certificate**

  All certificates are listed here. If any certificate is invalid, an error message is displayed below the certificate.

  Up to 3 certificates in the .pem format can be uploaded.

  To upload a CA certificate:

  a) Click **Select new...** and select a CA certificate (`.pem`).

  b) Click **Upload certificate**.

     The CA certificate is now displayed.

LDAP INTEGRATION

- **Enabled**. If selected, the option of LDAP integration is available.
- **LDAP server type**. Select the LDAP server type from the drop-down list.
- **Connection Type**. Select from **START TLS** or **LDAPS**
- **LDAP host**. Enter the address to the LDAP server in the network.

- **LDAP port**. Enter the specific port needed to access the LDAP server.
- **DN user** is the LDAP administrator who has access to the Base DN.
- **Password** is the administrator's password.
- **Base DN** specifies the root for searches in the Active Directory.
- **Search filter** defines search criteria which enables more efficient and effective searches.

SINGLE SIGN ON (SSO)

- **Enabled SAML**. If selected, the SSO login option becomes available. For more information about SSO, see *Section 8.10 "Single Sign-On (SSO)", page 175*.
- **Reload SAML configuration on Save**: If an already existing SAML configuration is changed in the database and this option is selected, configuration is reloaded when the **Save** button on this page is clicked. After saving, the **Download verification certificate** button will appear.
- **Recreate verification certificate**: If a SAML configuration already exists on the system and this option is selected, the certificate is created when the **Save** button on this page is clicked. This may be necessary if the certificate has changed or expired. After saving, the **Download verification certificate** button will appear. Download the certificate and upload it to the Identity Provider service.

CLIQ CONNECT+

- **Show accessible cylinders**. If selected, CLIQ Connect+ users can see which cylinders are accessible from their key in CLIQ Connect+.
- **Include mechanical cylinders**. If selected, the mechanical cylinders assigned to the key holder are also visible in the accessible cylinder list in CLIQ Connect+.
- **Show access profiles**. If selected, the list of access profiles assigned to the key is visible in CLIQ Connect+

  To enable this feature, the user permission level should be **View** or higher in the role **Key: Authorisation**. To change the permission level, refer to *Section 6.7 "Managing Roles and Permissions", page 119*.

6.5 Managing Remote PDs

6.5.1 Setting Up Remote PDs

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Edit the Remote PD information, tags and external links as desired.

   See *Section 6.5.3 "Editing Remote PD Information", page 99*, *Section 6.5.5 "Adding or Removing Remote PD Tags", page 101*, and *Section 6.5.6 "Managing Remote PD External Links", page 102*.

3) Edit the Remote PD Settings and load the configuration to the Remote PD. This includes installing the certificate.

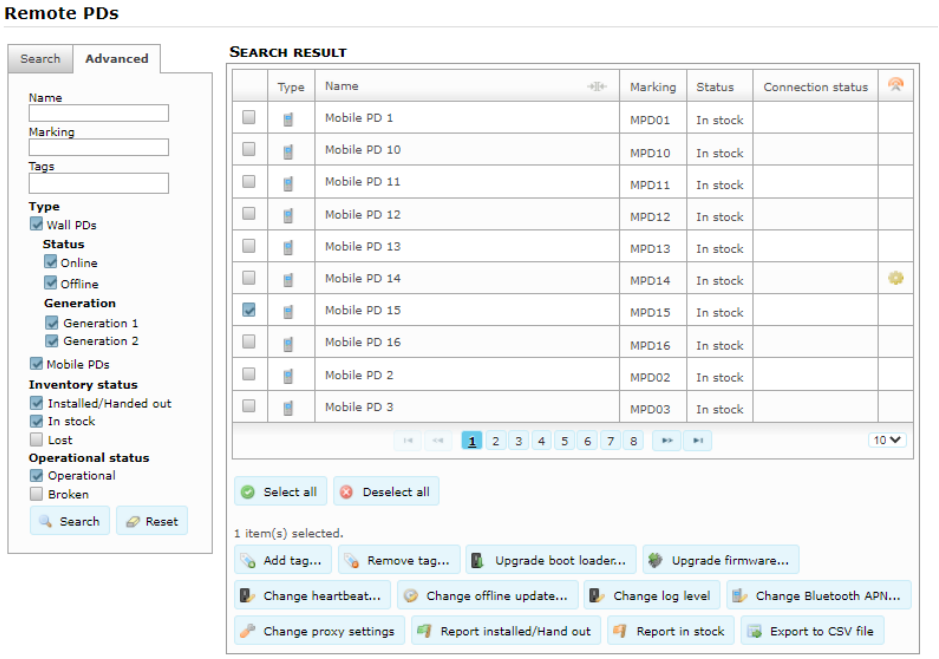
   For Wall PDs, see *Section 6.5.7 "Configuring Wall PDs", page 102*.

For CLIQ Mobile PDs, see *Section 6.5.8.1 "Editing CLIQ Mobile PD Settings", page 109*.

6.5.2 Searching for Remote PDs

1) Select **System Info » Remote PDs**.

Search result displays a list of Remote PDs.



Remote PDs

Search | Advanced

Name

Marking

Tags

Type

☑ Wall PDs

Status

☑ Online

☑ Offline

Generation

☑ Generation 1

☑ Generation 2

☑ Mobile PDs

Inventory status

☑ Installed/Handed out

☑ In stock

□ Lost

Operational status

☑ Operational

□ Broken

Search | Reset

Search result

	Type	Name	Marking	Status	Connection status	
□	📱	Mobile PD 1	MPD01	In stock		
□	📱	Mobile PD 10	MPD10	In stock		
□	📱	Mobile PD 11	MPD11	In stock		
□	📱	Mobile PD 12	MPD12	In stock		
□	📱	Mobile PD 13	MPD13	In stock		
□	📱	Mobile PD 14	MPD14	In stock		⚙
☑	📱	Mobile PD 15	MPD15	In stock		
□	📱	Mobile PD 16	MPD16	In stock		
□	📱	Mobile PD 2	MPD02	In stock		
□	📱	Mobile PD 3	MPD03	In stock		

1 2 3 4 5 6 7 8 | 10

Select all | Deselect all

1 item(s) selected.

Add tag... | Remove tag... | Upgrade boot loader... | Upgrade firmware... | Change heartbeat... | Change offline update... | Change log level | Change Bluetooth APN... | Change proxy settings | Report installed/Hand out | Report in stock | Export to CSV file

The following symbols are used:

▮ Wall PD

📱 CLIQ Mobile PD

> **NOTE!**
> CLIQ Connect Mobile PDs are not included in the list.

2) Enter the search criteria.

When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

To filter the search result list by Remote PD type, check the box for either **Wall PDs** or **Mobile PDs** in the **Advanced** search tab.

Wall PDs can be filtered by status, **Online** or **Offline**.

3) Click **Search**.

4) To display detailed information, click the specific Remote PD.

Several Remote PDs can be configured simultaneously. Select the Remote PDs in the search result list and click one of the buttons to change the corresponding settings.

6.5.3 Editing Remote PD Information

1) Find the Remote PD and go to its detailed information view.

See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Click **Edit**.

3) To edit the Remote PD name, update the field **Name**.

4) To add tags, click **Add Tag...**. See also *Section 6.5.5 "Adding or Removing Remote PD Tags", page 101*.

5) To add edit external links, click **Add external link...**. See also *Section 6.5.6 "Managing Remote PD External Links", page 102*.

6) Click **Save**.

6.5.4 Editing Remote PD Status

Remote PDs have an inventory status of either in stock, handed out or lost, and an operational status of either operational or broken.

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) **To Change the Wall PD Status**

   - Reporting **Installed**
     - Go to the detailed information view and click **Report Installed** and click **OK**.
     - If there are multiple devices to report, select Wall PDs in the search result, click **Report installed/Hand out** and click **OK**.
   - Reporting **In stock**
     - Go to the detailed information view and click **Report in stock** and click **OK**.
     - If there are multiple devices to report, select Wall PDs in the search result, click **Report in stock** and click **OK**.
   - Reporting **Lost**
     - Go to the detailed information view and click **Report lost** and click **OK**.
   - Reporting **Found**
     - Go to the detailed information view and click **Report found** and click **OK**.
   - Reporting **Broken**
     - Go to the detailed information view and click **Report broken** and click **OK**.
   - Reporting **Operational**
     - Go to the detailed information view and click **Report operational** and click **OK**.

3) **To Change the CLIQ Mobile PD Status**

   - Reporting **Handed out**

- Go to the detailed information view and click **Hand out** and click **OK**.
- If there are multiple devices to report, select Wall PDs in the search result, click **Report installed/Hand out** and click **OK**.

- Reporting **In stock**
  - Go to the detailed information view and click **Hand in** and click **OK**.
  - If there are multiple devices to report, select Wall PDs in the search result, click **Report in stock** and click **OK**.
- Reporting **Lost**
  - Go to the detailed information view and click **Report lost** and click **OK**.
- Reporting **Found**
  - Go to the detailed information view and click **Report found** and click **OK**.
- Reporting **Broken**
  - Go to the detailed information view and click **Report broken** and click **OK**.
- Reporting **Operational**
  - Go to the detailed information view and click **Report operational** and click **OK**.

6.5.5 Adding or Removing Remote PD Tags

1) Select **System Info » Remote PDs**.

   A list of all Remote PDs is displayed.

   - To add or remove tags for individual Remote PD, go to *Step 2*.
   - To add or remove tags for multiple Remote PDs simultaneously, go to *Step 3*.

2) **To Add or Remove Tags for an Individual Remote PD:**

   1. Select the Remote PD and go to its detailed information view.
   2. Click **Edit**.
   3. Add or remove a tag for individual Remote PD.

      To Add a Tag:

      a) Click **Add tag...**.
      b) Enter a name for the tag.
      c) Click **OK**.

      To Delete a Tag:
      Click the tag to be removed.
   4. Click **Save**.

3) **To Add or Remove Tags for Multiple Remote PD:**

   1. Select Remote PDs from the search results by checking the checkboxes.

2. **To Add a Tag:**

   a) Click **Add tag...**.

   b) Enter a name of the tag.

   c) Click **OK**.

   To Delete a Tag:

   a) Click **Remove tag...**.

   b) Enter a name of the tag.

   c) Click **OK**.

See also *Section 8.2.6 "Tags", page 166*.

6.5.6 Managing Remote PD External Links

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Click **Edit**.

3) **To Add an External Link:**

   1. Click **Add.**

   2. Enter **Name** for the URL.

   3. Enter **URL**. The **URL** must start with a protocol (for example http:// or ftp://).

      If a root URL has been defined in **System settings** (item **External links root URL**), it is only necessary to add the last part of the URL. See also *Section 6.4 "Editing System Settings", page 94*.

   4. Click **OK**.

   To Edit an External Link:

   1. Click **Edit** on the external link to be edited.

   2. Update the fields.

   3. Click **OK**.

   To Remove an External Link:
   Click **Remove** on the external link to be removed.

4) Click **Save**.

See also *Section 8.4 "External Links", page 169*.

6.5.7 Managing Wall PD Settings and Certificate

Prerequisites:

- For a Wall PD that is configured for the first time with **Plug and play** disabled, or cannot connect with the existing settings:

  – A USB cable:

        - **Generation 1 Wall PD:** USB On-The-Go (OTG) Cable with USB Mini Male (both type A and B supported) to USB Standard Female (type A).

        - **Generation 2 Wall PD:** USB-C Male to USB Standard Female (type A).
    - A USB flash drive:
        - **Generation 1 Wall PD:** Formatted with the FAT32 file system. Recommended memory size is 8-16 GB.
        - **Generation 2 Wall PD:** Formatted with the FAT32 file system. There is no restriction in USB flash drive size. Use a standard USB-C flash drive or connect a USB-A flash drive with a standard adapter or cable.
- To use Offline Update:
    - A generation 1 Wall PD with firmware 2.11 or higher or generation 2 Wall PD.
- To install or renew certificates **without** DCS Integration:
    - A .p12 certificate file. This is obtained from the local CLIQ dealer.

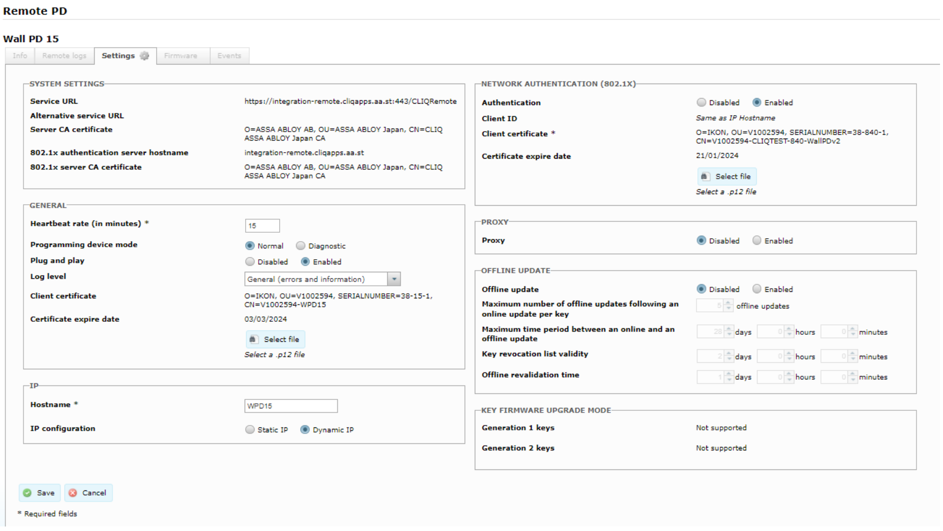
6.5.7.1 Editing Wall PD Settings

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Select the **Settings** tab.

3) Click **Edit**.



Remote PD

Wall PD 15

SYSTEM SETTINGS

Service URL	https://integration-remote.cliqapps.aa.st:443/CLIQRemote
Alternative service URL	
Server CA certificate	O=ASSA ABLOY AB, OU=ASSA ABLOY Japan, CN=CLIQ ASSA ABLOY Japan CA
802.1x authentication server hostname	integration-remote.cliqapps.aa.st
802.1x server CA certificate	O=ASSA ABLOY AB, OU=ASSA ABLOY Japan, CN=CLIQ ASSA ABLOY Japan CA

GENERAL

Heartbeat rate (in minutes) *	15
Programming device mode	● Normal ○ Diagnostic
Plug and play	○ Disabled ● Enabled
Log level	General (errors and information)
Client certificate	O=IKON, OU=V1002594, SERIALNUMBER=38-15-1, CN=V1002594-WPD15
Certificate expire date	03/03/2024 Select file *Select a .p12 file*

IP

Hostname *	WPD15
IP configuration	○ Static IP ● Dynamic IP

NETWORK AUTHENTICATION (802.1X)

Authentication	○ Disabled ● Enabled
Client ID	*Same as IP Hostname*
Client certificate *	O=IKON, OU=V1002594, SERIALNUMBER=38-840-1, CN=V1002594-CLIQTEST-840-WallPDv2
Certificate expire date	21/01/2024 Select file *Select a .p12 file*

PROXY

Proxy	● Disabled ○ Enabled

OFFLINE UPDATE

Offline update	● Disabled ○ Enabled
Maximum number of offline updates following an online update per key	5 offline updates
Maximum time period between an online and an offline update	28 days 0 hours 0 minutes
Key revocation list validity	2 days 0 hours 0 minutes
Offline revalidation time	1 days 0 hours 0 minutes

KEY FIRMWARE UPGRADE MODE

Generation 1 keys	Not supported
Generation 2 keys	Not supported

* Required fields

4) Update the required settings:

   GENERAL

   - **Heartbeat rate (in minutes)**

Recommended value: 15.

Heartbeat frequency is the number of minutes between heartbeats sent from the Wall PD to the CLIQ Remote Server to notify CWM that it is online. The Wall PD also checks for Wall PD updates (firmware or configuration updates) when sending the heartbeat.

- **Programming device mode**

  Select **Normal**. Do not select **Diagnostic** unless advised by technical support.

- **Plug and play**

  > **NOTE!**
  > **Plug and play** requires DCS Integration to be enabled and **Proxy settings** to be disabled in order to function.

  Plug and play enables the Remote PD to automatically receive a certificate from a server, if it does not have one yet. The certificate is downloaded from DCS through the enrolment application.

  Select **Enabled** (recommended default setting) if using the Remote PD in a network connected to the internet without restrictions. Select **Disabled** if loading a certificate to the Remote PD using a USB flash drive.

- **Log level** (Generation 2 Wall PD Only)

  The Wall PDs send error logs to the Remote Server and the logs are kept in one place for 10 days. The log level is configurable for generation 2 Wall PD from the following levels:

  – **Critical (only errors)**

  – **General (errors and information)**

  – **Detailed (errors, information and debug)**

  – **No log**

> **HINT!**
> It is also possible to apply the same log level to multiple Generation 2 Wall PDs from the Remote PD list.

IP

- **Hostname**

  The hostname is the name of the Wall PD in the network. It is recommended to use descriptive host names to help identifying the Remote PD when troubleshooting.

- **IP configuration**

  Select **Static IP** or **Dynamic IP**.

  If **Static IP** is selected, enter **IP address**, **Subnet mask**, **Gateway**, and **DNS**.

NETWORK AUTHENTICATION (802.1X) (Generation 2 Wall PD Only)

- **Authentication**

  Select **Disabled** or **Enabled**.

  > **NOTE!**
  > After enabling NETWORK AUTHENTICATION (802.1X) for the first time, the Wall PD needs to be configured using a USB flash drive.
  >
  > For more details, see *Section 6.5.7.3 "Configuring a Wall PD with NETWORK AUTHENTICATION (802.1X)", page 108*.

- **Client ID** is same as IP Hostname
- **Client Certificate**

  A client certificate is listed here.

  To upload the client certificate:

  a) Click **Select file...**.

  b) In a pop-up window, enter the certificate file password and click **Select...**.

  c) In the pop-up file explorer, select a certificate (`.12`) file.

  d) Click **Upload**.

  Client certificate and **Certificate expire date** are displayed.

For editing the system wide settings for 802.1x, see *Section 6.4 "Editing System Settings", page 94*.

PROXY

- **Proxy**

  If **Enabled** is selected, enter **Host**, **Port**, **User name**, and **Password**.

  Host is the address to the proxy server in the network.

  Port is the specific port needed to access the proxy server. Normally these ports are 8080.

OFFLINE UPDATE

See also *Section 8.3.3 "Offline Update", page 168*.

> **NOTE!**
> To update a key in offline mode the key must have firmware version 6 or higher.

- **Maximum number of offline updates following an online update per key**

  Specifies the number of updates that can be made in offline mode for each key before an online update is required.

- **Maximum time period between an online and an offline update**

  Specifies the period after the last online update during which offline updates are allowed.

  The value defines the time period when the key must have been revalidated in online mode.

- **Key revocation list validity**

  Specifies how long the Key Revocation List is stored in the Wall PD and offline updates are allowed. See also *Section 8.3.3 "Offline Update", page 168*.

  The value defines the period that a Remote PD allows offline revalidation. After this time, offline updates cannot be performed. For example, if a 48 hours service break is expected, at least 48 hours should be set.

- **Offline revalidation time**

  Specifies the period for which key validity is extended. The revalidation interval set on keys is ignored at offline updates.

KEY FIRMWARE UPGRADE MODE

> **NOTE!**
> Generation 2 Remote PDs do not support upgrading the firmware for generation 1 keys.

To enable and disable key upgrades, see *Section 6.5.11 "Enabling and Disabling Key Upgrades in Remote PDs", page 114*.

5) Click **Save**.

6) Transfer the updated configuration to the PD.

   - If the Wall PD is online or can connect with its current settings:

     The updated settings are sent to the Wall PD after the next heartbeat. The Wall PD is configured automatically and connects to the Remote Server.

     To see whether a Wall PD is online, view the detailed information.

   - If the PD is configured for the first time with **Plug and play** disabled, or cannot connect with the current settings:

     a) Insert a USB flash drive into the client computer.

     b) Click **Save to file** and save the file to the root folder of the USB flash drive.

     > **NOTE!**
     > Make sure there are no other files than configuration files in root folder of the USB flash drive.
     >
     > There can be several configuration files on the same USB flash drive.

     c) Connect the USB flash drive to the Wall PD using the appropriate USB cable (see *Section 6.5.7 "Configuring Wall PDs", page 102*).

The PD is configured automatically and connects to the Remote Server. This should take less than a minute.

7) Check that CLIQ LED lights indicates the PD is online and correctly configured.

   See *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190* or *Section 9.5.2 "Wall PD (Generation 2) Indications", page 191*.

6.5.7.2 Installing or Renewing a Wall PD Certificate

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Select the **Settings** tab.

3)
   - If DCS Integration is enabled, click **Generate client certificate**.

     The certificate is generated.
   - If DCS Integration is not enabled:

     a) Click **Edit** to enter the edit more.

     b) In the **GENERAL** section, click **Select file**.

     c) Click **Select...** and select the certificate file (.p12)

     d) Enter the **Certificate file password**.

     e) Click **Upload**.

     f) Click **Save** to exit the edit mode.

4) Transfer the updated configuration to the PD.
   - If the Wall PD is online or can connect with its current settings:

     The updated settings are sent to the Wall PD after the next heartbeat. The Wall PD is configured automatically and connects to the Remote Server.

     To see whether a Wall PD is online, view the detailed information.
   - If the PD is configured for the first time with **Plug and play** disabled, or cannot connect with the current settings:

     a) Insert a USB flash drive into the client computer.

     b) Click **Save to file** and save the file to the root folder of the USB flash drive.

     > **NOTE!**
     > Make sure there are no other files than configuration files in root folder of the USB flash drive.
     >
     > There can be several configuration files on the same USB flash drive.

     c) Connect the USB flash drive to the Wall PD using the appropriate USB cable (see *Section 6.5.7 "Configuring Wall PDs", page 102*).

     The PD is configured automatically and connects to the Remote Server. This should take less than a minute.

5) Check that CLIQ LED lights indicates the PD is online and correctly configured.

See *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190* and *Section 9.5.2 "Wall PD (Generation 2) Indications", page 191*.

6.5.7.3 Configuring a Wall PD with NETWORK AUTHENTICATION (802.1X)

After enabling NETWORK AUTHENTICATION (802.1X) for the first time, the Wall PD needs to be configured using a USB flash drive.

> **NOTE!**
> This is only applicable for Wall PDs of generation 2.

Prerequisite:

- **802.1x authentication** is enabled in **System settings**. See *Section 6.4 "Editing System Settings", page 94*.

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Select the **Settings** tab.
3) Click **Edit** to enter the edit more.
4) Upload the NETWORK AUTHENTICATION (802.1X) client certificate:
   a) In the **NETWORK AUTHENTICATION (802.1X)** section, click **Select file...**.
   b) In a pop-up window, enter the certificate file password and click **Select...**.
   c) In the pop-up file explorer, select a certificate (`.12`) file.
   d) Click **Upload**.

      Client certificate and **Certificate expire date** are displayed.

   e) Click **Save** to exit the edit mode.
5) Transfer the updated configuration to the Wall PD:
   a) Insert a USB flash drive into the client computer.
   b) Click **Save to file** and save the file to the root folder of the USB flash drive.

      > **NOTE!**
      > Make sure there are no other files than configuration files in root folder of the USB flash drive.
      >
      > There can be several configuration files on the same USB flash drive.

   c) Connect the USB flash drive to the Wall PD using the cable (USB-C Male to USB Standard Female (type A)).

      The PD is configured automatically and connects to the Remote Server.

   d) Check that the middle LED in the progress bar on the Wall PD is on continuously when process is finished.

      If the LED indicators behave differently, see *Section 9.5.2 "Wall PD (Generation 2) Indications", page 191* to check the status.

6.5.8 Managing CLIQ Mobile PD Settings and Certificate

Prerequisites:

- For use with an iPhone or Android mobile phone:
  - A CLIQ Mobile PD with firmware version 2.10 or higher.
  - A Mini USB cable is required to connect the CLIQ Mobile PD to the phone without using Bluetooth. For the appropriate cable, see *Section 7.4.2 "Remote PDs", page 148*.
- For a CLIQ Mobile PD that is configured for the first time with **Plug and play** disabled, or cannot connect with the existing settings,
  - A USB On-The-Go (OTG) cable: USB Mini Male (both type A and B supported) to USB Standard Female (type A).

  - A USB flash drive formatted with the FAT32 file system. The recommended memory size is 8-16 GB.
- To use Offline Update:
  - A CLIQ Mobile PD with firmware 2.10 or higher.
- To install or renew certificates **without** DCS Integration:
  - A .p12 certificate file. This is obtained from the local CLIQ dealer.
- The documentation supplied with the CLIQ Mobile PD is available.

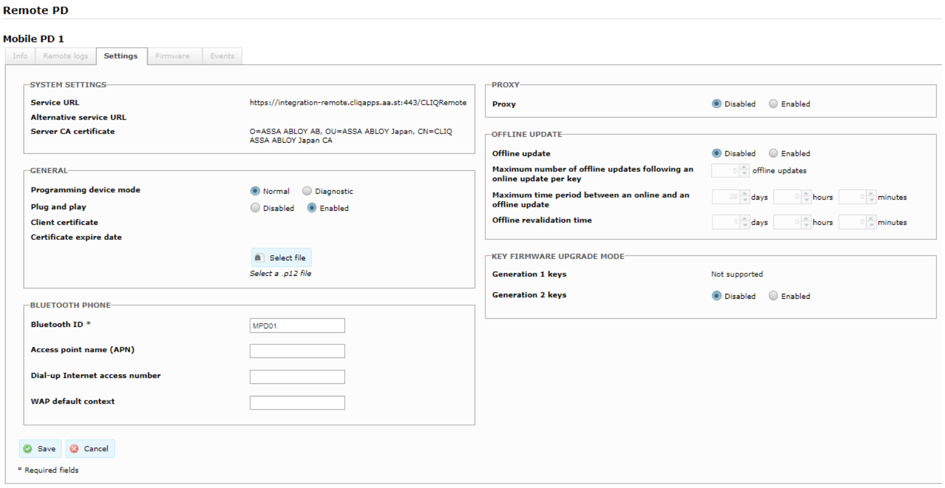
6.5.8.1 Editing CLIQ Mobile PD Settings

1) Find the CLIQ Mobile PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Select the **Settings** tab.

3) Click **Edit**.



Remote PD

Mobile PD 1

SYSTEM SETTINGS

Service URL: https://integration-remote.cliqapps.aa.st:443/CLIQRemote

Alternative service URL

Server CA certificate: O=ASSA ABLOY AB, OU=ASSA ABLOY Japan, CN=CLIQ ASSA ABLOY Japan CA

GENERAL

Programming device mode: ● Normal ○ Diagnostic

Plug and play: ○ Disabled ● Enabled

Client certificate

Certificate expire date

Select a .p12 file

BLUETOOTH PHONE

Bluetooth ID *: MPD01

Access point name (APN)

Dial-up Internet access number

WAP default context

* Required fields

PROXY

Proxy: ● Disabled ○ Enabled

OFFLINE UPDATE

Offline update: ● Disabled ○ Enabled

Maximum number of offline updates following an online update per key: 5 offline updates

Maximum time period between an online and an offline update: 28 days 0 hours 0 minutes

Offline revalidation time: 1 days 0 hours 0 minutes

KEY FIRMWARE UPGRADE MODE

Generation 1 keys: Not supported

Generation 2 keys: ● Disabled ○ Enabled

4) Update the required settings:

GENERAL

- **Programming device mode**

  Select **Normal**. Do not select **Diagnostic** unless advised by technical support.

- **Plug and play**

  NOTE!
  Plug and play requires DCS Integration to be enabled and **Proxy settings** to be disabled in order to function.

  Plug and play enables the Remote PD to automatically receive a certificate from a server, if it does not have one yet. The certificate is downloaded from DCS through the enrolment application.

  Select **Enabled** (recommended default setting) if using the Remote PD in a network connected to the internet without restrictions. Select **Disabled** if loading a certificate to the Remote PD using a USB flash drive.

BLUETOOTH PHONE

Regardless of how the **BLUETOOTH PHONE SETTINGS** are configured, the CLIQ Mobile PD can always be used with a computer connected with a USB cable.

For use with

- iPhone
- Android
- Other mobile phone supporting the PAN Bluetooth profile

Leave all fields in **BLUETOOTH PHONE SETTINGS** except **Bluetooth ID** blank.

For use with a mobile phone that supports the DUN Bluetooth profile, enter the following:

- **Bluetooth ID**

  A name of the CLIQ Mobile PD. This name will be visible in the mobile phone when pairing with the CLIQ Mobile PD.

- **Access point name (APN)**

  The name of the network operator gateway between the mobile network and Internet. An example is: “online.telia.se”. This setting is obtained from the mobile operator.

- **Dial-up Internet access number**

  The number that shall be called to gain network access, for example `*99#`. This setting is obtained from the mobile operator.

- **WAP default context**

  The location in the mobile phone where the Internet connection settings are stored. This is a mobile phone specific setting, and the correct value is obtained from the phone documentation. In most cases the setting can have the value `1`.

PROXY

- **Proxy**

  If **Enabled** is selected, enter **Host**, **Port**, **User name**, and **Password**.

  Host is the address to the proxy server in the network.

  Port is the specific port needed to access the proxy server. Normally these ports are 8080.

OFFLINE UPDATE

> **NOTE!**
> To update a key in offline mode the key must:
>
> - recently have been updated in the same CLIQ Mobile PD (be within the last 10 updated keys).
> - have firmware version 6 or higher.

- **Maximum number of offline updates following an online update**

  Specifies the number of updates that can be made in offline mode before an online update is required. Enter `0` to disable Offline Update.

- **Maximum time period between an online and an offline update**

  Specifies for how long time after the last online update that offline updates are allowed.

- **Offline revalidation time**

  Specifies for how long time the key validity is extended. The revalidation interval set on keys is ignored at offline updates.

KEY FIRMWARE UPGRADE MODE

To enable and disable key upgrades, see *Section 6.5.11 "Enabling and Disabling Key Upgrades in Remote PDs", page 114*.

5) Click **Save**.

6) Transfer the updated configuration to the CLIQ Mobile PD.

   - If the CLIQ Mobile PD has been configured before and can connect with the current settings:

     The updated settings are sent to the CLIQ Mobile PD next time it is used. The PD is configured automatically and connects to the Remote Server. This should take less than a minute.

   - If the PD is configured for the first time with **Plug and play** disabled, or cannot connect with the current settings:

     a) Insert a USB flash drive into the client computer.

     b) Click **Save to file** and save the file to the root folder of the USB flash drive.

> **NOTE!**
> Make sure there are no other files than configuration files in root folder of the USB flash drive.
>
> There can be several configuration files on the same USB flash drive.

c) Connect the USB flash drive to the CLIQ Mobile PD using the appropriate USB cable (see *Section 6.5.8 "Configuring Mobile PDs", page 108*).

d) Insert a user key into the CLIQ Mobile PD.

Configuration of the CLIQ Mobile PD is initiated.

e) When the Download LED lights up continuously, remove the USB flash drive.

⤓

7) To configure a mobile phone to use with the CLIQ Mobile PD, see separate documentation supplied with the CLIQ Mobile PD.

8) To configure a computer for use with the CLIQ Mobile PD:

   a) Install **ASSA ABLOY Network Provider** on the client computer.

   b) Use a Mini USB cable to connect the client computer to the CLIQ Mobile PD. For the appropriate cable, see *Section 6.5.8 "Configuring Mobile PDs", page 108*.

9) To verify that the configuration is correct:

   a) Insert a user key into the CLIQ Mobile PD.

   The PD powers up and connects to the Remote Server. This should not take more than a minute.

   b) Check that CLIQ LED lights up continuously.

   CLIQ

   This means that the PD is online and correctly configured.

See also *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190*.

6.5.8.2 Installing or Renewing a CLIQ Mobile PD Certificate

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Select the **Settings** tab.

3) To install or renew a certificate:

   - If DCS Integration is enabled, click **Generate certificate**.

     The certificate is generated.

   - If DCS Integration is not enabled and the certificate file is provided by the local CLIQ dealer:

     a) Click **Edit** to enter the edit more.

   b) In the **GENERAL** section, click **Select file**.

   c) Click **Select...** and select the certificate file (.p12)

   d) Enter the **Certificate file password**.

   e) Click **Upload**.

   f) Click **Save** to exit the edit mode.

4) Transfer the updated configuration to the PD.

   - If the CLIQ Mobile PD has been configured before and can connect with the current settings:

     Click **Save**.

     The updated settings are sent to the CLIQ Mobile PD next time it is used. The PD is configured automatically and connects to the Remote Server. This should take less than a minute.

   - If the CLIQ Mobile PD is configured for the first time with **Plug and play** disabled, or cannot connect with the current settings:

     a) Insert a USB flash drive into the client computer.

     b) Click **Save to file** and save the file to the root folder of the USB flash drive.

     > **NOTE!**
     > Make sure there are no other files than configuration files in root folder of the USB flash drive.
     >
     > There can be several configuration files on the same USB flash drive.

     c) Connect the USB flash drive to the CLIQ Mobile PD using the appropriate USB cable (see *Section 6.5.8 "Configuring Mobile PDs", page 108*).

     d) Insert a user key into the CLIQ Mobile PD.

     Configuration of the CLIQ Mobile PD is initiated.

     e) When the Download LED lights up continuously, remove the USB flash drive.

5) To configure a mobile phone to use with the CLIQ Mobile PD, see separate documentation supplied with the CLIQ Mobile PD.

6) To configure a computer for use with the CLIQ Mobile PD:

   a) Install **ASSA ABLOY Network Provider** on the client computer.

   b) Use a Mini USB cable to connect the client computer to the CLIQ Mobile PD. For the appropriate cable, see *Section 7.4.2 "Remote PDs", page 148*.

7) To verify that the configuration is correct:

   a) Insert a user key into the CLIQ Mobile PD.

The PD powers up and connects to the Remote Server. This should not take more than a minute.

b) Check that CLIQ LED lights up continuously.

This means that the PD is online and correctly configured.

See also *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190*.

6.5.9 Viewing Remote PD Event Log

The Event Log presents events and issues that the Remote PDs have reported to the CLIQ Web Manager.

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Select the **Event log** tab.

6.5.10 Enabling and Disabling Wall PD Offline Messaging

When a Wall PD stops sending heartbeats for a certain period, the CLIQ Web Manager detects it is offline and sends an email to a specified person. This section explains how to set this feature.

1) Select **Administration » System settings**.

   The system settings are displayed.

2) Click **Edit**.

3) In the SYSTEM section, find **Emails after Wall PD goes offline** under **User messaging**.

4)
   - To stop the email, uncheck the box, and proceed to *Step 8*.
   - To receive the email, check the box, and proceed to the next step.

     The **Configure** button next to the checkbox turns to blue.

5) Click **Configure**.

   Setting window opens.

6) Enter the email address to which the mail is sent when a Wall PD becomes offline.

7) Enter the number of missing heartbeats after which the email is sent.

8) Click **OK**.

6.5.11 Enabling and Disabling Key Upgrades in Remote PDs

For information about how to upgrade keys, including what firmware versions to use, see *Section 6.15.3 "Upgrading Firmware on Keys", page 138*.

1) Find the Remote PD and go to its detailed information view.

   See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) Select the **Settings** tab.

3) For upgrading generation 1 keys:

To Enable Key Upgrades:

Under the **Key firmware upgrade mode settings**, click **Switch to key updater mode**.

This button will only be visible once the necessary firmware files have been imported, see *Section 6.15.3 "Upgrading Firmware on Keys", page 138*.

To Disable Key Upgrades:

Under the **Key firmware upgrade mode settings**, click **Switch to normal mode**.

4) For upgrading generation 2 keys:

To Enable Key Upgrades:

1. Click **Edit**.
2. Under the **Key firmware upgrade mode settings**, select **Enabled**.
3. Click **Save**.

> ℹ **NOTE!**
> Multiple Remote PDs can be selected for upgrading generation 2 keys.
>
> Repeat *Step 5 c* in *Section 6.15.3 "Upgrading Firmware on Keys", page 138* for each Remote PD that is intended for upgrading keys.

To Disable Key Upgrades:

1. Click **Edit**.
2. Under the **Key firmware upgrade mode settings**, select **Disabled**.
3. Click **Save**.

6.5.12 Exporting Remote PD Information

1) Find the Remote PD and go to its detailed information view.

See *Section 6.5.2 "Searching for Remote PDs", page 99*.

2) From the search results, select the Remote PDs whose data should be exported.

3) Click **Export to CSV file**.

4) In the file download pop-up window, click **OK**.

A CSV file is downloaded in the **Downloads** folder.

> ℹ **NOTE!**
> To be able to open the file in Excel in the correct way, the delimiter for the file must be set according to regional settings. To change the delimiter, see *Section 6.4 "Editing System Settings", page 94*.

6.6 Managing Domains

6.6.1 Searching For Domains

1) Select **Administration » Domains**.

   A list of all domains is displayed.

2) Enter the search criteria.

   When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

3) Click **Search**.

4) To display detailed information on a search result, click the row of the specific domain.

6.6.2 Editing Domain Information

1) Find the domain to edit.

   See *Section 6.6.1 "Searching For Domains", page 116*.

2) In the search result list, click the name of the domain.

3) Click **Edit**.

4) Enter the name and description of the domain.

5) Click **Save**.

6.6.3 Setting Initial Domains For New or Imported Objects

New or imported objects are assigned to the corresponding initial domain.

Initial domains exist for the following objects:

- keys
- persons (employees and visitors)
- cylinders (and cylinder groups)

> **NOTE!**
> New or imported cylinders that belong to a cylinder group will be included in the domain of the cylinder group, not in the initial cylinder domain. This means that all cylinders in a cylinder group belong to the same domain. For more information about domains, see *Section 8.2.2 "Domains", page 160*.

New or imported access profiles and temporary access groups are assigned to the initial cylinder domain.

Each initial domain has an editable name. The default name is `default`. The initial domains can share the same domain or have different domains.

To set the initial domains for keys, persons and cylinders:

1) Select **Administration » System settings**.

2) Click **Edit**.

3) Under **ADMINISTRATION**, click **Change domain...** for the specific initial domain.

   A list of domains for which the administrator is authorised is displayed.

4) Click **Select** on the row of the new domain.

5) Click **Save**.

6.6.4 Creating And Deleting Domains

1) Select **Administration » Domains**.

2) To create a domain:

   a) Click **Create New**.

   b) Enter **Name** and an optional **Description**.

   c) Click **Save**.

3) To delete a domain:

> ℹ **NOTE!**
> A domain can only be deleted if no cylinders, cylinder groups, employees, visitors or keys are connected to it. Before deleting, empty the domain by moving the objects to a different domain.
>
> Ensure to move both active and deleted employees or visitors to a different domain. To find deleted employees or visitors, see *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

   a) Find the domain and view the detailed information.

      See *Section 6.6.1 "Searching For Domains", page 116*.

   b) Click **Delete**.

   c) Click **OK**.

6.6.5 Changing Domain For Keys

1) Select **System Info » Keys**.

   A list of all keys is displayed.

2) To search for specific keys, fill in the search criteria and click **Search**.

3) Click the row of the specific key.

4) Click **Edit**.

5) Click **Change domain...**.

   A list of domains for which the administrator is authorised is displayed.

6) Click **Select** on the row of the new domain.

7) Click **Save**.

The domain can be changed for several keys simultaneously. Select the keys in the search result list and click **Change domain...**.

See also *Section 8.2.2 "Domains", page 160*.

6.6.6 Changing Domain For Employees and Visitors

1) Find the employee or visitor to edit.

To search for the employee or visitor and display the detailed information view, see *Section 4.1.1 "Searching for Employees or Visitors", page 23*.

2) Click **Edit**.

3) Click **Change domain...**.

   A list of domains for which the administrator is authorised is displayed.

4) Click **Select** on the row of the new domain.

5) Click **Save**.

The domain can be changed for several employees or visitors simultaneously. Select the employees or visitors in the search result list and click **Change domain...**.

See also *Section 8.2.2 "Domains", page 160*.

6.6.7 Changing Domain For Cylinders

For cylinders that belong to a cylinder group, the domain is changed on cylinder group level. See *Section 6.6.8 "Changing Domain For Cylinder Groups", page 118*.

1) Select **System Info » Cylinders**.

   A list of all cylinders is displayed.

2) To search for specific cylinders, fill in the search criteria and click **Search**.

3) Click the row of the specific cylinder.

4) Click **Edit**.

5) Click **Change domain...**.

   A list of domains for which the administrator is authorised is displayed.

6) Click **Select** on the row of the new domain.

7) Click **Save**.

The domain can be changed for several cylinders simultaneously. Select the cylinders in the search result list and click **Change domain...**.

NOTE!
It is recommended to make sure an access profile and all included cylinders and cylinder groups belong to the same domain. This is to ensure that administrators for a specific domain cannot get indirect access to cylinders in other domains (through access profiles).

See also *Section 8.2.2 "Domains", page 160*.

6.6.8 Changing Domain For Cylinder Groups

For cylinders that do not belong to a cylinder group, the domain is changed on each cylinder individually. See *Section 6.6.7 "Changing Domain For Cylinders", page 118*.

1) Select **System Info » Cylinder groups**.

   A list of all cylinder groups is displayed.

2) To search for specific cylinder groups, fill in the search criteria and click **Search**.

3) Click the row of the specific cylinder group.

4) Click **Edit**.

5) Click **Change domain...**.

A list of domains for which the administrator is authorised is displayed.

6) Click **Select** on the row of the new domain.

7) Click **Save**.

The domain can be changed for several cylinder groups simultaneously. Select the cylinder groups in the search result list and click **Change domain...**.

> **NOTE!**
> It is recommended to make sure an access profile and all included cylinders and cylinder groups belong to the same domain. This is to ensure that administrators for a specific domain cannot get indirect access to cylinders in other domains (through access profiles).

See also *Section 8.2.2 "Domains", page 160*.

6.6.9 Changing Domain for Access Profiles

1) Find the access profile and view the detailed information.

See *Section 4.6.1 "Searching for Access Profiles", page 65*.

2) In the detailed information view, click **Edit**.

3) Click **Change domain**.

4) Click **Select** for the new domain.

5) Click **Save**.

> **NOTE!**
> It is recommended to make sure an access profile and all included cylinders and cylinder groups belong to the same domain. This is to ensure that administrators for a specific domain cannot get indirect access to cylinders in other domains (through access profiles).

6.7 Managing Roles and Permissions

> **NOTE!**
> To assign roles to a C-Key, see *Section 6.11.4 "Editing C-Key Information", page 126*.

1) Select **Administration » Roles**.

A list of existing roles is displayed.

Some of the roles are predefined in CWM.

2) **To Create a Role:**

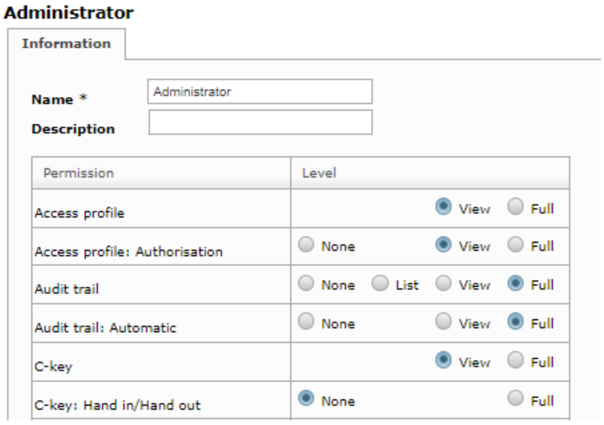
   1. Click **Create new**.
   2. Enter a **Name** and a possible **Description**.
   3. Select permissions in the list.

NOTE!

Restrictions:

- Access to some permissions is dependent upon the level of other permissions. If a specific permission cannot be configured, check the level of related permissions.
- If **Hierarchical administrators** is enabled, the administrator cannot grant a permission level that is higher than their own.

  For example, if an administrator is granted the **List** level of the **Cylinder** permission, the administrator cannot grant new roles the **View** or the **Full** level of the **Cylinder** permission.



Administrator

Name * Administrator

Description

Permission	Level
Access profile	● View ○ Full
Access profile: Authorisation	○ None ● View ○ Full
Audit trail	○ None ○ List ○ View ● Full
Audit trail: Automatic	○ None ○ View ● Full
C-key	● View ○ Full
C-key: Hand in/Hand out	● None ○ Full

To Edit an Existing Role:

NOTE!

Restrictions:

- An administrator cannot edit their own role; only the **Description** field is editable.
- If **Hierarchical administrators** is enabled, the administrator cannot edit the role of an administrator with higher permissions.
- If **Hierarchical administrators** is enabled, the administrator cannot grant a permission level that is higher than their own.
- The **Super administrator**, **Approver** and **CLIQ Connect+** roles are read-only and cannot be edited.

1. Click the row of a specific role.
2. Click **Edit** to update the **Name**, **Description** or **Permissions** of the role.
3. Click **Save**.

To Delete a Role

NOTE!

Restrictions:

- Roles that are associated with one or more members cannot be deleted.
- The **Super administrator**, **Approver** and **CLIQ Connect+** roles are read-only and cannot be deleted
- If **Hierarchical administrators** is enabled, the administrator cannot delete roles with a permission level that is higher than their own.

1. Click the row of a specific role.
2. Click **Delete**.
3. Click **OK**.

To View C-Key Members of a Role

1. Click the row of a specific role.
2. Select the **Members** tab.

See also:

- *Section 8.8 "CWM Roles and Permissions", page 173*
- *Section 9.4 "Permissions", page 185*

6.8 Importing Employee Information

The employee information to be imported must be stored in a CSV-file following certain specifications. See *Section 9.9 "Employee Import File Format", page 193*. The exact specifications are subject to change and it is therefore recommended to upload the file for validation.

NOTE!
The following employees are not added or updated to CWM during the importing process:

- The deactivated employees.
- LDAP integrated employees.

1) Select **Administration » Import employees**.
2) Click **Select** to find the locally saved file on the computer.
3) Click **Open**.
4) Click **Upload** to validate the file.

   Information on how many valid entries the file contains is displayed. If the file does not follow the specifications, import is not possible.
5) Click **Import** to import the valid file.

6.9 Managing Receipt Templates

The template text and logo in hand in or hand out receipts can be created and edited. Receipts are created in PDF format which can either be printed or saved.

> **NOTE!**
> In order to manage the receipt templates, the user permission level should be **Full** in the role **Receipt templates**. To change the permission level, refer to *Section 6.7 "Managing Roles and Permissions", page 119*.

6.9.1 Creating a Receipt Template

It is possible to add a new receipt templates to the system and set them either the default or non-default template.

1) Select **Administration » Receipt templates**.

   The list of receipt templates is displayed.

2) Click **Create new** which is located under the list.

3) Enter the following fields:

   - **Name**: It is used as a template name.
   - **Type**: Select either **Hand out** or **Hand in**.
   - **Default for**: If the creating template is used as a default, check either or both boxes.
   - **Language**: Select the appropriate language from the drop-down list.
   - **Title**: It is printed in the receipt as the heading of the content.

4) Select the logotype:

   - System logo: The default organisation logo. To change the system logo, see *Section 6.9.3 "Changing the System Logo", page 123*.
   - Custom logo: A separate company logo instead of the system logo.

     a) Select **Use custom logo**.

     b) Click **Select**.

     c) Click **Select...** and select the file.

        The image to upload must be less than 2 MB and in JPEG, JPG, PNG, BMP or GIF format.

     d) Click **Upload**.

        The logo appears on the pop-up screen.

     e) Click **Close** to exit.

5) Enter sentences in the **Text** box.

   In creating a new template based on the standard text, it is recommended to click **Use standard text** and edit the content.

   The text box has basic edit buttons to format the texts. To apply these styles to a new text, click the button and start typing. To apply these styles to existing content in the editor select the text and click the appropriate button. The following tables shows the list of available buttons.

B	Bold
I	Italic
<u>U</u>	Underline
~~S~~	Strikethrough
x^2	Superscript
X_2	Subscript
☰	Unordered list
1☰	Ordered list
H_1	First level header
H_2	Second level header
T_x	Clear formatting

6) Optional: Click **Preview template** to check the receipt.
7) Click **Save**.

6.9.2 Editing a Receipt Template

1) Select **Administration » Receipt templates**.

   The list of receipt templates is displayed.
2) Click the template to edit.
3) Click **Edit**.
4) Edit the following fields:
   - **Name**: It is used as a template name.
   - **Type**: Select either **Hand out** or **Hand in**.
   - **Default for**: If the editing template is used as a default, check either or both boxes.
   - **Language**: Select the appropriate language from the drop-down list.
   - **Title**: It is printed in the receipt as the heading of the content.
5) Edit the logotype:
   - To change the system logo, see *Section 6.9.3 "Changing the System Logo", page 123*.
   - To change the custom logo, click **Select** to upload the new logo.
6) Edit the sentences in the **Text** box.

   For more information on how to format texts, see *Section 6.9.1 "Creating a Receipt Template", page 122*, *Step 5*.
7) Optional: Click **Preview template** to check the receipt.
8) Click **Save**.

6.9.3 Changing the System Logo

Receipt templates contain the brand logo as a default but it is possible to customise the default logo.

Prerequisites:

- The logo is an image file with an RGB colour profile (CMYK is not supported).
- The logo has to be less than 2 MB. Recommended size is about 120 x 60 pixels.

1) Select **Administration » Receipt templates**.
2) Click **Change system logo** which locates under the list.
3) - To change to the customised logo:
     a) Click **Select...**.
     b) Select the file to upload and click **Open**.
     c) Click **Upload**.
   - To change to the default logo, click **Restore default**.
4) Click **Close**.

6.9.4 Deleting a Receipt Template

1) Select **Administration » Receipt templates**.

   The list of receipt templates is displayed.
2) Click the template to delete.
3) Click **Delete**.
4) In the pop-up window, click **OK**.

6.10 Managing Schedule Templates

There are two types of schedule templates, **Basic template** and **Multi time period template**.

- A basic template allows for one time period to be set per day of the week.
- A multi time period template allows for days and time periods to be freely set. Multiple time periods can be set for the same day of the week.

The two templates are supported by different key firmware versions. For information about which key firmware versions support which template, see *Section 9.7 "Firmware Dependent Functionality", page 192*.

1) Select **Administration » Schedule templates**.
2) To create a Basic Schedule template:
   a) Click **Create basic template**.

      By default the time periods are set to all day.
   b) Enter **Name** and optional **Description**.
   c) To change from the default time periods, click **Edit** on the row of that specific day.
   d) Select **All day**, **Never** or **Custom**.
   e) If the custom option is selected, fill in the period values **From time** and **To time**.
   f) Click **Save**.

If necessary, repeat *Step 2 c* - *Step 2 f* for other days.

g) Click **Save**.

3) To create a Multi Time Period Schedule template:

   a) Click **Create multi time period template**.

   b) Enter **Name** and optional **Description**.

   c) Click **Add period**.

   d) Fill in the period values **From date** and **To date**.

   e) Fill in the period values **From time** and **To time**.

   f) Click **Save**.

   g) Add more time periods as required.

   h) Click **Save**.

4) To edit a template:

   a) Click the row of the specific template.

   b) Click **Edit**.

   c) Update the fields and click **Save**.

5) To delete a template:

   a) Click the row of the specific template.

   b) Click **Delete**.

   c) Click **OK**.

See also *Section 8.1.8 "Key Schedules", page 158*.

6.11 Managing C-Keys

6.11.1 Searching for C-Keys

1) Select **Administration » C-keys**.

2) Enter the search criteria.

   When typing in search fields CWM accepts the first part of a search string as well as an asterisk (*). If the search is for "Laboratory 1", writing "Lab", "*1", or "Lab*1" will give search results including "Laboratory 1".

3) Click **Search**.

4) To display detailed information on a search result, click the row of the specific C-Key.

   For information about the C-Key attributes, see *Section 9.3.4 "C-Key Attributes", page 183*.

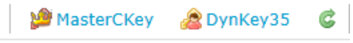
6.11.2 Scanning a C-Key

1) Insert the C-Key to scan into the right slot of the Local PD.

> **NOTE!**
> The C-Key used for login must remain in the left slot of the Local PD.

2) Click ↻ in the upper right corner of the page.

Both C-Keys in the Local PD are shown below the navigation bar.



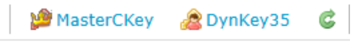
6.11.3 Viewing C-Key Status

1) Insert the C-Key to view into the right slot of the Local PD.

> **NOTE!**
> The C-Key used for login must remain in the left slot of the Local PD.

2) Click ↻ in the upper right corner of the page.

Both keys in the Local PD are shown below the navigation bar.

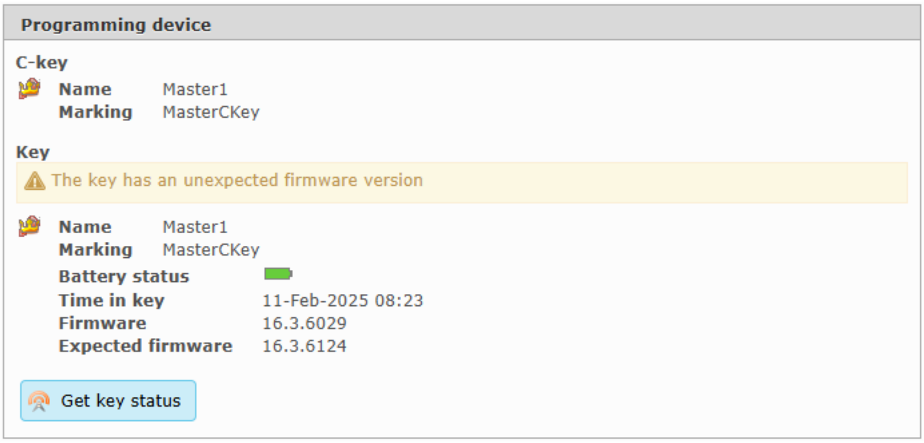


3) Click the C-Key in the right slot of the Local PD.

The C-Key's detailed information view is displayed, with the C-Key's **Name** and **Marking** shown on the right-hand side of the page.

4) Click **Get key status**.

Basic information about the C-Key in the right slot is displayed. For more information about the battery status indicator, see *Section 9.6 "Battery Level Indications", page 191*.



Programming device

C-key

Name Master1
Marking MasterCKey

Key

⚠ The key has an unexpected firmware version

Name Master1
Marking MasterCKey
Battery status 🟩
Time in key 11-Feb-2025 08:23
Firmware 16.3.6029
Expected firmware 16.3.6124

6.11.4 Editing C-Key Information

1) Find the C-Key and go to its detailed information view.

To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

2) Click **Edit**.

- To edit the C-Key name, update the field **Name**.
- To block the C-Key, select **Block**.
- To change if certificate enrolment is allowed, select **Always Allowed**, **Allowed once**, or **Not Allowed**.

  See also *Section 8.11 "DCS Integration", page 176*.
- To assign or change the C-Key authorisation roles, select one or more roles.

> **NOTE!**
>
> **Restrictions:**
>
> – It is not possible to change the role of the C-Key that is currently used to log in.
>
> – The Approver role cannot be combined with other roles.
>
> – If **Hierarchical administrators** is enabled, the administrator cannot assign roles with a permission level that is higher than their own.

3) Click **Save**.

6.11.5 Selecting C-Key Domains

1) Find the C-Key and go to its detailed information view.

To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

2) Find the C-Key.

To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

3) Select the **Domain authorisations** tab.

4) Click **Edit** to change domains.

5) To add domains:

   a) Click **Add domain...**.

   The search result list displays all domains.

   b) To filter the domains, enter search criteria and click **Search**.

   c) Click **Select** for the domains to add or click **Select all**.

   d) Click **Done**.

6) To remove a domain, click **Remove** for the domain to remove or click **Remove all**.

7) Click **Save**.

The change of domain will take effect at next login.

6.11.6 Viewing C-Key Events

The Events tab is used for traceability of some administrator operations in CWM, such as when the C-Key was handed out.

1) Find the C-Key and go to its detailed information view.

   To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

   To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

2) Select the **Events** tab.

   A list with all C-Key events is displayed.

6.11.7 Handing Out C-Keys

Prerequisite:

- The administrator has been fully granted the permission; **C-key: Hand in/Hand out**.
- The employee receiving a C-Key must have a valid email address.

1) Find the C-Key and go to its detailed information view.

   To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

   To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

2) Click **Hand out to employee**.

   The list of employee is displayed.

3) Select the employee from the list and click **Select**.

   An email is sent to the employee's registered email address, containing instructions on where to download CLIQ Connect PC and the URL for the locking system.

   To be able to log in to CWM, the employee must install a certificate for the key. For more information about how to install the certificate, see *Section 3.2 "Enrolling and Installing C-Key Certificates", page 15*.

> **HINT!**
> It is strongly recommended that the employee changes the C-Key PIN code. For instructions, see *Section 6.11.11 "Changing C-Key PIN Code", page 131*.

6.11.8 Handing In C-Keys

Prerequisite:

- The administrator has been fully granted the permission; **C-key: Hand in/Hand out**.

1) Find the C-Key and go to its detailed information view.

   To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

   To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

2) Click **Hand in C-key**.

   The C-Key can no longer be used to log in to CWM.

6.11.9 Reporting and Blocking a Lost C-Key

1) Find the C-Key and display the detailed information view.

   See *Section 6.11.1 "Searching for C-Keys", page 125*.

2) Click **Report lost**.

3) Lost C-Keys that contain cylinder programming jobs need to be blocked in order to prevent unauthorised cylinder programming.

   - To block a C-Key that contains cylinder programming jobs, select the cylinders to block the C-Key in:

     – Select **All cylinders** or **Only installed** and proceed to *Step 6*.

     – Select **Custom selection** and proceed to proceed to *Step 4* to select the cylinders.

   - To report the C-Key lost without blocking any cylinders, select **No cylinders**, click **Next** and proceed to *Step 9*.

4) Click **Next**.

5) Select the cylinders for which the lost C-Key will be blocked.

6) Click **Next**.

7) Optional: Select the cylinder programming key from the list by clicking **Select**.

   ℹ **NOTE!**
   If this process is skipped, cylinder programming jobs are created for C-Keys.

   In the **Search** tab, select **All types and statuses** to show C-Keys.

   In the **Advanced** tab, under **Type**, select either user keys or C-Keys to change what is shown in the list.

   ℹ **NOTE!**
   The cylinder programming key must have sufficient memory.

8) In the confirmation page, select the priority level under **Priority**.

   Urgent jobs should have a high priority level.

9) After verifying all information, click **Report lost**.

- If **no** jobs are created to block the lost C-Key, the programming jobs assigned to the lost C-Key are cancelled and listed under **Work » Cylinder programming**.
- If jobs are created to block the lost C-Key, the key used for blocking will also inherit the cylinder blocking jobs originally assigned to the lost C-Key. Other cylinder programming jobs that were originally assigned to the lost C-Key are cancelled and listed under **Work » Cylinder programming**.

> ⚠ **WARNING!**
> By default, even if no cylinder programming job is created to block the lost C-Key, the lost C-Key is still added in CWM to the list of **Unauthorised Keys** for the affected cylinders. This information is, however, not visible in CWM. If these cylinders are later reprogrammed or replaced, the information about unathorised keys stored in CWM is applied to these cylinders, in effect blocking the lost C-Key. Therefore, even if the lost C-Key is later reported found, it will still be blocked by any reprogrammed or replaced cylinders.
>
> In order to reauthorise the found C-Key in those cylinder access list, see *Section 4.9.2 "Configuring Authorisations in Cylinders", page 76*.
>
> In order to change this default setting, **Silently block lost keys in cylinder during authorisation update** needs to be turned off. See *Section 6.4 "Editing System Settings", page 94*.

10) - If a specific key was **NOT** selected to program the cylinders, continue from *Step 4* in *Section 4.4.13 "Programming Cylinders", page 59*.
    - If a specific key was selected to program the cylinders, follow the instructions below.
11) Go to the information view of the selected user key.

> **HINT!**
> Clicking **Key Marking** under **Blocking Key Information** leads directly to the information view.

12) Go to the **Programming jobs** tab and confirm that the cylinder job is assigned to the key.
13) - **Programming in the Local PD**

      Insert the user key into the right slot of the Local PD and remove the C-Key from the left slot of the Local PD.
    - **Programming in a Wall PD**

      Insert the user key into a Wall PD.

    The cylinder programming job is automatically written to the user key.
14) Reprogram each cylinder using the user key.
15) After programming the cylinders, report the completed cylinder jobs by inserting the user key into one of the following devices:

- The right slot of the Local PD (remove the C-Key from the left slot)
- A Wall PD

After finding the C-Key, report it by clicking **Report found** in the detailed information view.

6.11.10 Reporting Broken or Operational C-Key

1) Find the C-Key and display the detailed information view.

   See *Section 6.11.1 "Searching for C-Keys", page 125*.

2) **To Report Broken**

   1. Click **Report broken**.
   2. Click **OK**.

   To Report Operational

   1. Click **Report operational**.
   2. Click **OK**.

6.11.11 Changing C-Key PIN Code

> **NOTE!**
> The PIN Code must have 6 characters. The following characters are allowed:
>
> - Upper-case (A, B, C, ...)
> - Lower-case (a, b, c, ...)
> - Digits (0, 1, 2, ...)
> - Minus (-)
> - Underscore (_)
> - Space ( )
> - Special (!, $, %, &, ...)
> - Brackets ([,], {, }, (,), <, >)
>
> Non-English characters are not allowed.

1) To change any normal C-Key PIN using the master C-Key or C-Key with Super administrator role:

   a) Select **Administration » C-keys**.
   b) Insert the C-Key in the right port of the Local PD.
   c) Click **Scan**.
   d) Click **Show** by the C-Key.
   e) Click **Set new PIN**.
   f) Enter **Master C-key PIN**.
   g) Enter the new PIN in **New PIN**.
   h) Enter the new PIN again in **Confirm new PIN**.

2) To change the normal C-Key PIN of the same key used to log in:

a) Select **Settings » C-key settings**.

b) Click **Change C-key PIN**.

c) Enter **Current PIN**.

d) Enter **New PIN**.

e) Enter the new PIN in **Confirm new PIN**.

3) Click **OK**.

6.11.12 Unlocking C-Keys

After 5 attempts to login with the wrong PIN, the C-Key is locked and has to be unlocked by entering the PUK code provided by the CLIQ dealer. See *Section 6.11.12.1 "Unlocking C-Keys by Using PUK Code", page 132* for more information.

> **NOTE!**
> After 25 attempts of entering the wrong PUK, the C-Key becomes unusable and has to be replaced with a new C-Key.

If the administrator does not have the PUK code, the Master C-Key holder can unlock the C-Key. See *Section 6.11.12.2 "Unlocking C-Keys Using Master C-Key", page 132* for more information.

6.11.12.1 Unlocking C-Keys by Using PUK Code

1) Select **Settings » C-key settings**.

2) Click **Unlock C-key**.

3) Enter **PUK**.

If the administrator does not have the PUK code, contact a Master C-Key holder.

4) Enter **New PIN**.

5) Enter **Confirm new PIN**.

6) Click **OK**.

6.11.12.2 Unlocking C-Keys Using Master C-Key

The following procedure can only be executed by a Master C-Key holder.

1) Insert the C-Key to be unlocked into the right slot of the Local PD.

2) Find the C-Key and go to its detailed information view.

To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

3) Click **Set new PIN**.

4) Enter the **Master C-key PIN**, **New PIN** and **Confirm new PIN** for the locked C-Key.

5) Click **OK** to save.

The new PIN is programmed in the C-Key in the right slot of the PD.

6.11.13 Activate or Deactivate Automatic Audit Trail Retrieval for C-Key

Prerequisites:

- The administrator has permission to enable automatic audit trails.
- A generation 2 C-Key with firmware version 12.6 or higher.
- For activation, the **Approvals** feature must be turned off in **System settings**.

1) Find the C-Key and go to its detailed information view.

   To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

   To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

2) Find the **AUTOMATIC AUDIT TRAIL RETRIEVAL** setting.

3)
   - To activate the automatic audit trail retrieval setting: Click **Enable**.
   - To dectivate the automatic audit trail retrieval setting: Click **Disable**.

4) If the C-Key is in the Local PD, click **Update C-key locally**.

6.11.14 Listing C-Key Certificates

1) Find the C-Key and go to its detailed information view.

   To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

   To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

2) Select the **Certificates** tab.

   The **Last used date** for each certificate is displayed if the system setting **Collect last login date** is enabled. See *Section 6.4 "Editing System Settings", page 94*.

6.11.15 Revoking C-Key Certificates

Revoking C-Key certificates is a security feature and typically used when an administrator's computer with a C-Key certificate is stolen but the C-Key is still in safe hands. In the example with the stolen computer, the installed C-Key certificate is revoked and then enrolled again.

To enrol a C-Key certificate, see *Section 3.2 "Enrolling and Installing C-Key Certificates", page 15*.

1) Find the C-Key and go to its detailed information view.

   To search for the C-Key and display the detailed information view, see *Section 6.11.1 "Searching for C-Keys", page 125*

   To scan the C-Key in the Local PD and display the detailed information view, see *Section 6.11.2 "Scanning a C-Key", page 125*

2) Select the **Certificates** tab.

3) Click **Revoke certificate** for each of the certificates to revoke.

> **HINT!**
> To know which certificate to enrol, look at the column **Last used date**. If any doubts, revoke all certificates and enrol all again.

NOTE!
It is not possible to revoke the certificate that was used to log in to the locking system.

4) Click **OK**.

6.11.16 Replacing Master C-Key

If a Master C-Key is lost or broken a new Master C-Key must be ordered.

Follow these instructions to register the new Master C-Key, and block the lost or broken Master C-Key.

Prerequisites:

- The following is available:
  - A new Master C-Key together with the PIN code.
  - A certificate for the new Master C-Key in case DCS is not integrated.
  - An import file containing the new Master C-Key.

1) Install the Master C-Key Certificate.

   See *Section 5.2 "Installing Master C-Key Certificate", page 90*.

2) Lock CWM for maintenance.

   See *Section 6.2 "Locking the System for Maintenance", page 93*.

3) Import the file containing the new Master C-Key using CLIQ Web Manager Service Tool. For more information, refer to CWM Operation and Maintenance Documentation.

CAUTION!
Log in with the new Master C-Key immediately after importing the file.

Until the new Master C-Key has logged in, the old Master C-Key can still be used and will, if used to log in, block the new Master C-Key.

4) Log in to CWM using the new Master C-Key.

   CWM detects that there are more than one active Master C-Key and automatically blocks the other Master C-Key and marks it as Lost.

   The old Master C-Key can still be used to execute any Cylinder Programming Jobs already stored the key, in the cylinders where it is authorised. CWM now gives the option to create Cylinder Programming Jobs to unauthorise the blocked Master C-Key from cylinders.

5) Click **Yes, create jobs now** or **No, decide later**.

To create unauthorisation jobs later, log in with the new Master C-Key and click **Create blacklisting jobs** from the detailed information view of the blocked Master C-Key.

6.11.17 Exporting C-Key Information

1) Search for the C-Keys.

See *Section 6.11.1 "Searching for C-Keys", page 125*.

2) From the search results, select the C-Keys whose data should be exported by checking the checkboxes.

3) Click **Export to CSV file**.

4) In the file download pop-up window, click **Save**.

A CSV file is downloaded in the **Downloads** folder.

> **NOTE!**
> To be able to open the file in Excel in the correct way, the delimiter for the file must be set according to regional settings. To change the delimiter, see *Section 6.4 "Editing System Settings", page 94*.

6.12 Changing Cylinder Group for Cylinders

> **NOTE!**
> Some cylinders in the cylinder list may represent a potential Free Output on a Wall PD, that is connected to an external device, e.g., a relay controller. In such a case, it is not possible to relocate these cylinders to another cylinder group.
>
> For further information regarding Free Output, contact your local CLIQ dealer.

1) Find the cylinder and view the detailed information.

   See *Section 4.4.1 "Searching for Cylinders", page 52*.

2) Click **Change group**.

3) Click **Select** on the row of the specific cylinder group.

4) Select a **Priority**. Urgent jobs should have a high priority level.

The cylinder group can be changed for several cylinders simultaneously. Select the cylinders in the search result list and click **Change group...**.

6.13 Viewing system status

1) Select **Administration » System status**.

2) Select the **Current status** tab to view the online or offline statuses of Remote PDs, the remote server and email server.

3) Select the **History** tab to view the past changes in online, offline statuses of Remote PDs, the remote server and email server.

   To view past events between certain dates:

   a) Fill in a start date in **Show events from**.

   b) Fill in an end date in **Show events to**.

   c) Click **Search**.

6.14 Viewing Basic Statistics

CWM has a built-in statistics function which provides basic statistics of the locking system, such as number of cylinders and keys.

Prerequisite:

- The administrator has been granted permission to view **Statistics**.

1) Select **Administration » Statistics**.
2) **Statistics** page is opened.
3) Optional: click **Print statistics** or **Export statistics** if required.

6.15 Upgrading Firmware

The firmware version can be checked on the detailed information view of each device.

6.15.1 Upgrading Firmware for Remote PDs

NOTE!
This chapter is not applicable for CLIQ Connect Mobile PD.

To upgrade a Remote PD, CWM must be provided with firmware. When using DCS Integration, firmware files are automatically fetched from DCS. Otherwise, this is done by uploading a local firmware file that is provided by the local CLIQ dealer. Once imported to CWM, Remote PD firmware can either be upgraded through CWM or via a USB flash drive.

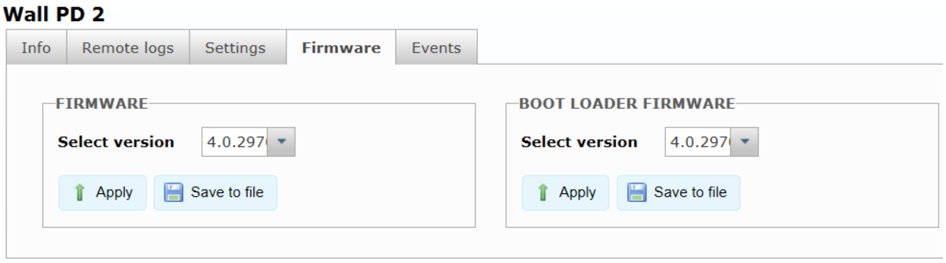
The Remote PD firmware upgrading process differs depending on DCS integration:

- To use DCS integration, start from *Step 2*.
- To use a local firmware file, start from *Step 1*.

1) Upload and import a local firmware file without DCS Integration:
   a) Save the new firmware locally on the computer.
   b) Select **Administration » Firmware**.
   c) Click **Select** to find the new firmware saved on the computer.
   d) Click **Open**.
   e) Click **Upload firmware** to upload the firmware to CWM.

      The firmware is uploaded.
   f) Click **Import firmware** to import the uploaded firmware.

      If successful, a summary of the imported firmware is displayed in a new panel.
2) Select **System info » Remote PDs**.
3) Click the row of the Remote PD to be upgraded.
4) Select the **Firmware** tab and select the version from the **FIRMWARE** or **BOOT LOADER FIRMWARE** section.



NOTE!
The **BOOT LOADER FIRMWARE** section is not displayed for the Generation 2 Wall PD.

5)
- To upgrade firmware for online Remote PDs through CWM:

  a) Select firmware version and click **Apply**.

  b) Activate the upgrade.

  - CLIQ Mobile PDs:

    Insert a user key to power on the CLIQ Mobile PD.

  - Wall PDs:

    The firmware is upgraded at the next heartbeat (next time it connects to the remote server).

- To upgrade firmware for offline Remote PDs via a USB flash drive:

  NOTE!
  The USB flash drive must be formatted with the FAT32 file system and the recommended memory size is 8-16 GB for generation 1 Wall PDs and Mobile PDs. There is no restriction in flash drive size for generation 2 Wall PDs. The USB flash drive must not contain any other files.

  a) Select firmware version and click **Save to file** to save the file to the root of the USB flash drive.

  b) Connect the USB flash drive to the Remote PD using the appropriate USB cable (see *Section 6.5.8 "Configuring Mobile PDs", page 108* or *Section 6.5.7 "Configuring Wall PDs", page 102*).

     The upgrade is initiated automatically.

  c) Activate the upgrade.

  - CLIQ Mobile PDs:

    Insert a user key to power on the CLIQ Mobile PD.

  - Wall PDs:

    The upgrade is initiated automatically.

The firmware upgrade is finished when the download indication LED has stopped flashing and is lit steadily. For information about Remote PD indications, see *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190* and *Section 9.5.2 "Wall PD (Generation 2) Indications", page 191*.

6.15.2 Upgrading Firmware for CLIQ Connect Mobile PDs

1) Connect the CLIQ Connect Mobile PD to the client PC, on which CLIQ Connect PC is installed, using a micro-USB cable.
2) CLIQ Connect PC will automatically check the version of the firmware of the CLIQ Connect Mobile PD.

   If a newer version is available, CLIQ Connect PC suggests upgrading the firmware.
3) Follow the instructions shown on the screen.

6.15.3 Upgrading Firmware on Keys

To upgrade a key, CWM must be provided with firmware. For systems with DCS Integration, firmware files are automatically fetched from DCS. For systems without DCS integration, this is done by uploading a local firmware file that is provided by the local CLIQ dealer. Once imported, the firmware is updated through CWM using a Remote PD.

Table 1. Type of Remote PD to use for upgrading keys

Key version	Remote PD	Remote PD firmware version
User keys, generation 1	Wall PD (Generation 1)	
User keys, generation 2	Wall PD (Generation 1 and 2) or CLIQ Mobile PD	
C-Keys, generation 2, with firmware 12.0 or higher	Wall PD (Generation 1 and 2) or CLIQ Mobile PD	Wall PD or CLIQ Mobile PD firmware 6.3 or higher
C-Keys, generation 2, with firmware lower than 12.0	Cannot be upgraded through CWM	
C-Keys, generation 1	Cannot be upgraded through CWM	

The key generation is visible in the detailed user key and C-Key views, see *Section 4.2.2 "Scanning a User Key", page 34*, *Section 4.2.1 "Searching for User Keys", page 33*, *Section 6.11.2 "Scanning a C-Key", page 125*, or *Section 6.11.1 "Searching for C-Keys", page 125*.

The key firmware upgrading process differs depending on DCS integration:

- For locking systems with DCS integration, skip to *Step 4*.
- For locking systems without DCS integration, continue from *Step 1*.

1) Save the new firmware locally on the computer.
2) Select **Administration » Firmware**.
3) Import the new firmware:
   a) Click **Select** to find the new firmware saved on the computer.
   b) Click **Open**.
   c) Click **Upload firmware** to upload the firmware to CWM.

      If successful, a summary of the uploaded firmware is shown in a new panel.
   d) Click **Import firmware**.

NOTE!
To be able to upgrade generation 1 keys, the following needs to be imported:

- Generation 1 Wall PD boot loader firmware
- Generation 1 Wall PD firmware, version 2.11 or higher
- Generation 1 Wall PD key updater firmware, version 2.11 or higher
- The new key firmware, one for each key type that will be upgraded

NOTE!
For systems with DCS Integration enabled, firmware files are automatically fetched from DCS and listed among the imported firmware that is ready for activation.

4) To upgrade generation 1 user keys:

NOTE!
Generation 2 Wall PDs do not support upgrading the firmware for generation 1 user keys.

a) Select **System Info » Remote PDs**.

b) Find the Wall PD to use for the upgrade and view the detailed information.

See *Section 6.5.2 "Searching for Remote PDs", page 99*.

Among other details, the current boot loader firmware and firmware for the Wall PD is displayed.

c) If the Wall PD boot loader firmware and firmware must be upgraded, see *Section 6.15.1 "Upgrading Firmware for Remote PDs", page 136*.

d) Enable key upgrades in the Wall PD, see *Section 6.5.11 "Enabling and Disabling Key Upgrades in Remote PDs", page 114*.

The key updater firmware is sent to the Wall PD. When the Wall PD has loaded the new firmware and rebooted, it is possible to upgrade keys.

e) For each of the user keys to be upgraded:

- Insert the key in the key updater Wall PD.

  First, pending remote updates for the key will be executed and then the key will be upgraded with the new firmware.

  NOTE!
  The key configuration, including all access rights, is erased during firmware upgrade. It is restored by performing a remote update of the key after the upgrade.

  The Wall PD indicates that updates are finished. For information about Remote PD indications, see *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190*.

- Remove the key from the Wall PD.

  Now a remote update job to restore the key configuration is created in CWM. It will be available after a few minutes.

- Insert the key in any Remote PD to restore the key configuration.

  The upgrade procedure is now completed for this key.

f) Disable key upgrades in the Wall PD, see *Section 6.5.11 "Enabling and Disabling Key Upgrades in Remote PDs", page 114*.

All pending key firmware upgrade jobs are cancelled. The normal Wall PD firmware is sent to the Wall PD and when it has loaded the new firmware and rebooted it will run as an ordinary Wall PD again.

5) To upgrade generation 2 user keys or C-Keys:

a) Select **System Info » Remote PDs**.

b) View the detailed information for the Remote PD to use for the upgrade.

See *Section 6.5.2 "Searching for Remote PDs", page 99*.

- If the Remote PD firmware needs to be upgraded, see *Section 6.15.1 "Upgrading Firmware for Remote PDs", page 136*.

c) In the **Settings** tab, enable key upgrades in the Remote PD. See *Section 6.5.11 "Enabling and Disabling Key Upgrades in Remote PDs", page 114*

d) Select **Administration » Firmware**.

e) Select the **Imported user key firmware** tab or the **Imported C-Key firmware** depending on if updating user keys or C-Keys.

f) Click **Apply** for the imported firmware to upgrade the key.

A remote job is automatically created.

> **NOTE!**
> If the **Apply** button is greyed out for the imported firmware it means there are pending remote upgrades for existing firmware, which are indicated by an icon in the **Status** column. Do the following:
>
> - Click **Cancel** for the firmware with pending remote upgrades.
> - Click **OK**.
> - Click **Apply** for the newest firmware.

> **NOTE!**
> The order of *Step 5 c* and *Step 5 f* can be reversed. It is possible to first apply the imported firmware and then enable key upgrades for a selection of Remote PDs.

g) Upgrade each key in a Remote PD:

> **NOTE!**
> For user keys, any pending remote updates for the key will be executed first and then the key will be upgraded with the new firmware.

- Via **Wall PD** or **CLIQ Mobile PD**

  Insert or connect the key to the devices that has been enabled for key upgrade.

  The Remote PD indicates that updates are finished. For information about Remote PD indications, see *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190* or *Section 9.5.2 "Wall PD (Generation 2) Indications", page 191*.

- Over **Bluetooth protocol in CLIQ Connect App**

  Prerequisites:

  - The firmware version of CLIQ Connect must be 4.1 or later.
  - The firmware version of the key must be 16.3.3 or later.

    Upgrading firmware for keys with older firmware is possible using a Wall PD.

  Connect the key to CLIQ Connect.

  > **NOTE!**
  > If a firmware upgrade is started using the CLIQ Connect and a BLE connection, it must be completed using the same method (i.e., BLE connection to a mobile device). During the intermediate upgrade state, the key will appear non-functional; it will not open any locks and will not respond in any programming device.

6.15.4 Updating Key Firmware Information to CWM Database

When key firmware is upgraded, the CWM database automatically updates the key's firmware information. The key firmware information can be seen in the **Key Information** view.

However, if key firmware is upgraded outside the CWM system, for example at the factory, the CWM database is not updated with the latest key firmware information about the key.

To synchronise the key firmware versions in the CWM database and the physical key, do as follows:

- Scan the upgraded key and get the key status in the Local PD. For more information, see *Section 4.2.2 "Scanning a User Key", page 34*.
- Insert the upgraded key into a remote PD.

> **NOTE!**
> Only generation 2 keys with the firmware version 12.3 or later can update the key firmware information via remote PDs.

NOTE!

C-Keys only:

If a C-Key has an older firmware version than the written one in the CWM database, the CWM database on firmware is not updated. This situation could also result in errors using the C-Key.

6.16 Importing Extensions

To import an extension, CWM must be provided with an extension import file. This is done by uploading a local extension import file.

When using DCS Integration, extension import files are automatically fetched from DCS. Start the extension import process from *Step 2*.

The DCS fetch can also be forced by manually clicking a button. Once uploaded, the extension import must be activated.

Prerequisite:

- If newly added cylinders need to block the lost keys in the system, enable **Block lost keys in new cylinders during extension import** in **System settings**. When enabled, the system automatically creates cylinder programming jobs to block lost keys for these cylinders when cylinder extension import files are activated. For more information. See *Section 6.4 "Editing System Settings", page 94*.

1) Provide an extension import file to CWM.

To Upload a Local Extension Import File

1. Select **Administration » Extension import » Upload or fetch extension import file(s)**.
2. Click **Select...** to find the locally saved extension import file on the computer. Extension import files have the suffix ".cws".
3. Click **Open**.
4. Click **Upload**. The extension import file is uploaded to the Web Manager Server and validated.

To Manually Fetch an Extension Import File from DCS

1. Select **Administration » Extension import » Upload or fetch extension import file(s)**.
2. Click **Fetch extension import file(s)**.

   A status note about the fetching process is displayed.

2) Activate an uploaded or fetched extension import:

NOTE!

It may take a while to process an uploaded or fetched extension import file. Whenever an extension import is ready to be activated, a notification is displayed on the homepage of CWM and sent via email to all administrators that have roles with maintenance permissions.

a) Select **Administration » Extension import » Activate extension import**.

A note about available extension imports is displayed, including information on the number of keys, key groups, cylinders, cylinder groups, and Remote PDs to be activated.

b) Optional: For more detailed information about extension elements, click **Export to CSV file** for each element to create a CSV file and confirm the details within the file.

c) Click **Activate extension import** to activate the available extensions.

> **NOTE!**
> Only uploaded or fetched extension imports that contain new data can be activated. Old or identical data cannot be activated.

Once activated, a confirmation message is displayed on the homepage of CWM.

If the **Block lost keys in new cylinders during extension import** function is activated, cylinder programming jobs are created. To program the cylinders, see *Section 4.4.13 "Programming Cylinders", page 59*.

7 CLIQ Hardware

7.1 CLIQ Architecture

The basic architecture of a CLIQ system is shown in *Figure 1 "CLIQ Architecture", page 144*.

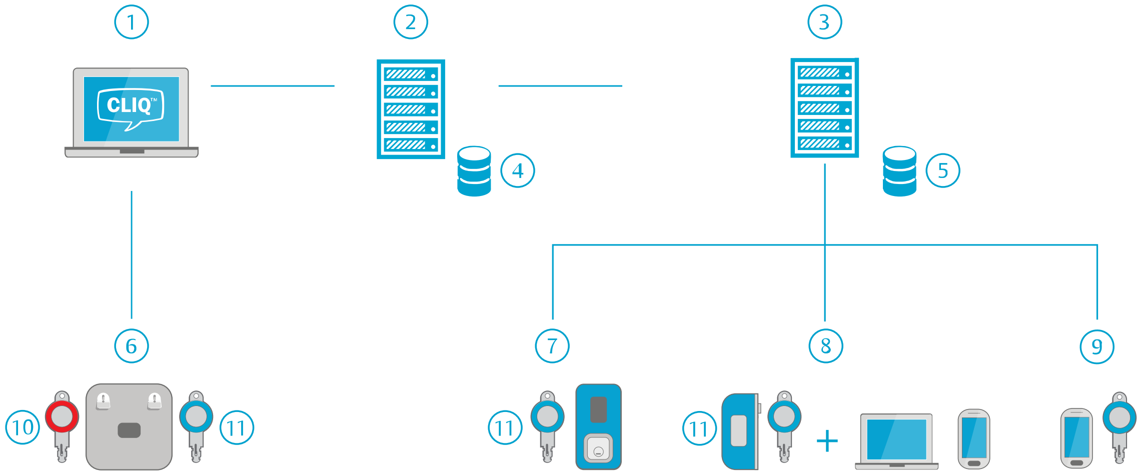


Figure 1. CLIQ Architecture

1. **CWM Client**. Is a computer with an Internet browser used by an administrator to administer a locking system. Several clients can be connected to the server.

2. **Web Manager Server**. Runs the CWM software and is connected to the CLIQ database with information about all CLIQ elements, access lists, audit trails, and so on.

3. **Remote Server**. In a remote system, the Remote Server handles remote update of keys. Key update jobs are sent from the Web Manager server to the Remote server. The update jobs are stored in a database until they are executed from the Remote PD.

4. **Database**. Database for Web Manager Server.

5. **Database**. Database for Remote Server.

6. **Local PDs**. Are connected to the Web Manager client, and are used by the administrator to log in to CWM (using a C-Key) and to program keys locally. For more information, see *Section 7.4.1 "Local PDs", page 147*.

7. **Wall PDs**. A type of Remote PD. By inserting a key in a Wall PD the key update jobs stored in the Remote Server database are executed. See *Section 7.4.2 "Remote PDs", page 148*.

8. **CLIQ Mobile PDs** and **CLIQ Connect Mobile PDs**. Two types of Remote PDs. By inserting a key in a CLIQ Mobile PD or CLIQ Connect Mobile PD the key update jobs stored in the Remote Server database are executed. See *Section 7.4.2 "Remote PDs", page 148*.

9. **CLIQ Connect Keys**. A type of key. By connecting the key to a mobile device with CLIQ Connect the the CLIQ Connect Key can be updated without using a PD. Refer to separate manual for the CLIQ Connect.

10. **C-Keys**. See *Section 7.2.4 "C-Keys", page 145*.

11. **User Keys**. See *Section 7.2.3 "User Keys", page 145*.

7.2 Keys

7.2.1 Key Overview

The CLIQ keys are electromechanical keys that contain electronics and a battery. Each CLIQ key is programmed and can be controlled and managed using CWM.

Keys are either system keys, also called **C-Keys**, used by locking system administrators, or **User Keys**, used by employees and visitors.

7.2.2 CLIQ Connect Keys

Some C-Keys and user keys can be updated via bluetooth technology using a mobile phone or a tablet. These keys are called **CLIQ Connect keys**. Keys that do not have this feature can only be updated in a PD.

7.2.3 User Keys

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

Mechanical Key Is a traditional key without electronic components. Can be managed in CWM but cannot be used with CLIQ cylinders.

Normal Key Is 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 (see *Section 8.1.2 "Electronic Authorisation", page 152*).

Quartz Key In addition to the above, this key type also has a quartz clock function and can be programmed to be active between certain dates and to require revalidation (see *Section 8.1.4 "Key Validity", page 154*). It can also be programmed to have access to cylinders based on a schedule (see *Section 8.1.8 "Key Schedules", page 158*). Keys of this type can also store audit trails (see *Section 8.6 "Audit Trails", page 171*).

Dynamic Key In addition to the above, this key type can also store a key access list of cylinders and cylinder groups that the key is authorised to open (see *Section 8.1.2 "Electronic Authorisation", page 152*). This is useful in remote systems since it enables access to be controlled by keys, which are easily updated in Remote PDs.

A Dynamic key and a Quartz key is either a **CLIQ Connect key** (right icon) or not (left icon). Normal keys are never CLIQ Connect keys. See *Section 7.2.2 "CLIQ Connect Keys", page 145* for more information.

See also *Section 8.1 "Authorisation Principles", page 152*.

7.2.4 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 only used to access CWM and to program cylinders.

There are two types of C-Keys: **Master C-Keys** and **Normal C-Keys**.

Master C-Key

The Master C-Key is used by the Super Administrator to manage the locking system. There is only one Master C-Key per locking system and it must be kept in a secure place.

The Master C-Key has the following unique rights that cannot be given to any other C-Key:

- 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.

Sub Master C-Key

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 has restricted functionality compared to the Master C-Key. For example, it cannot be used to activate initial imports and certain system settings cannot be configured.

Normal C-Key

Normal C-Keys are handed out to the Administrators. Normal C-Keys can be configured to give access to certain functions in CWM, and blocked from other functions. See *Section 8.8 "CWM Roles and Permissions", page 173*).

There is a special kind of Normal C-Key that has the right to execute cylinder reprogramming. Other Normal C-Keys do not have this right. The reprogramming rights are programmed to the key at the factory and cannot be changed. To see whether a Normal C-Key has reprogramming rights, view the detailed C-Key information. See *Section 6.11.1 "Searching for C-Keys", page 125* or *Section 6.11.2 "Scanning a C-Key", page 125*.

Each Normal C-Key is also either a **CLIQ Connect key** (right icon), or not (left icon). See *Section 7.2.2 "CLIQ Connect Keys", page 145* for more information.

NOTE!

The term **C-Key** is used when describing functionality that applies to both Master C-Keys and Normal C-Keys.

Depending on the firmware, C-Keys have **Cylinder group programming** capability. Only C-Keys with this capability can execute Cylinder Programming Jobs involving the change of a cylinder's cylinder group. To see whether a C-Key has the Cylinder group programming capability, view the detailed C-Key information. See *Section 6.11.1 "Searching for C-Keys", page 125* or *Section 6.11.2 "Scanning a C-Key", page 125*. In systems initially delivered as cylinder group systems, all C-Keys have this capability.

In order to use a C-Key in CWM, a unique certificate must be installed in the CWM Client (see *Section 2.1 "CWM Client Setup Overview", page 12*). Each C-Key also has its own PIN code and PUK code.

7.2.5 Key Generations

Two key generations exist:

- Generation 1
- Generation 2

The generation of a key is defined by its hardware. Generation 2 keys are newest and most developed.

All generation 2 keys are backward compatible with generation 1 keys.

The key generation is visible in the detailed key view, see *Section 4.2.2 "Scanning a User Key", page 34* or *Section 4.2.1 "Searching for User Keys", page 33*.

7.3 Cylinders

There are two different cylinder types, mechanical and electronic. Electronic types 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.

When listing cylinders the following symbols are used:

Ⓔ	Electronic Cylinder
Ⓜ	Mechanical Cylinder
ⒺⓂ	Double Cylinder (This example: Electronic A-side and Mechanical B-side)

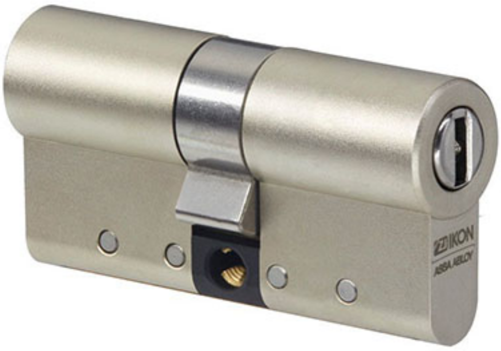


Figure 2. CLIQ Cylinder

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.

7.4 Programming Devices

7.4.1 Local PDs

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

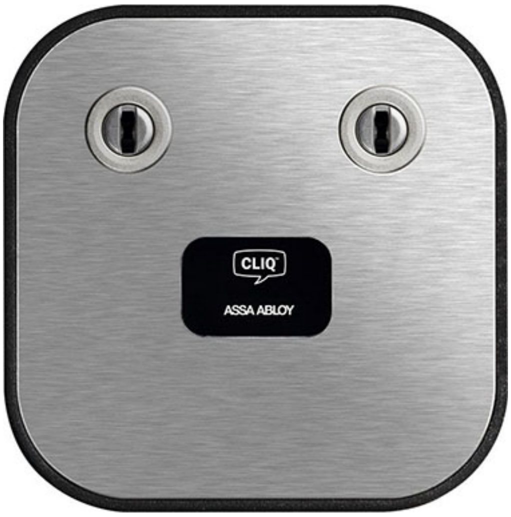


Figure 3. Local Programming Device

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 CWM, a Local PD connected to a CWM 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 CWM)

7.4.2 Remote PDs

Remote PDs are used in remote systems for transferring data between the remote database and the key. Remote PDs can be either Wall PDs or Mobile PDs. Wall PDs and CLIQ Mobile PDs are locking system specific, while CLIQ Connect Mobile PDs can be used with any locking system.

Note that each device supports a different type of USB cables:

Device	USB Cable Type
Wall PD (Generation 1)	mini-USB On-The-Go (OTG) cable
Wall PD (Generation 2)	USB-C cable
CLIQ Mobile PD	mini-USB cable
CLIQ Connect Mobile PD	micro-USB cable

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

- The remote update tasks are executed.
- The time on the key is updated.
- The audit trail is read from the key, if so configured.

See also *Section 9.5.1 "Wall PD (Generation 1) and Mobile PD Indications", page 190* and *Section 9.5.2 "Wall PD (Generation 2) Indications", page 191*.

If **Offline Update** is enabled, a key can be revalidated through a Wall PD or a CLIQ Mobile PD even if it has temporarily lost its network connection. See also *Section 8.1.5 "Key Revalidation", page 154*. Offline update is not available for CLIQ Connect Mobile PDs.

Wall PDs

Two types of Wall PDs are available; Generation 1 and Generation 2. The Generation 2 Wall PD has been added the following features:

- Network Authentication 802.1x can be enabled. To enable or disable it, see *"NETWORK AUTHENTICATION (802.1X) (Generation 2 Wall PD Only)"* and *Section 6.4 "Editing System Settings", page 94*.
- No boot loader is used, i.e. upgrading the boot loader firmware is not necessary.
- The log level for device log is configurable, see *"GENERAL"* for more details.

The Wall PD is typically mounted on the wall and connected to the Remote Server via Ethernet.

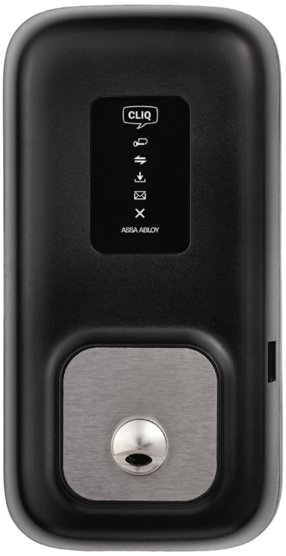


Figure 4. Generation 1 Wall Programming Device

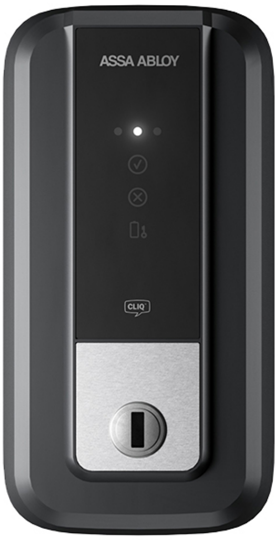


Figure 5. Generation 2 Wall Programming Device

The term **Heartbeat** means that the Wall PD sends a signal to the CLIQ Remote server to notify CLIQ Web Manager that it is online. The Wall PD does also check for Wall PD updates (firmware or configuration updates) when sending the heartbeat. The time between heartbeats is configurable.

When a Wall PD misses some heartbeats, the CLIQ Web Manager assumes that the Wall PD is offline and sends an email to a specified person. For more information on how to enable this feature, see *Section 6.5.10 "Enabling and Disabling Wall PD Offline Messaging", page 114*.

CLIQ Mobile PDs

The CLIQ Mobile PD is a personal programming unit. It can connect either to a computer via a mini-USB cable, or to a mobile phone via Bluetooth Low Energy (BLE) to use the mobile phone's internet connection.

The CLIQ Mobile PD needs battery power when connecting with a mobile phone. When the CLIQ Mobile PD is used with a computer, a special application, **ASSA ABLOY Network Provider**, must be installed on the computer.

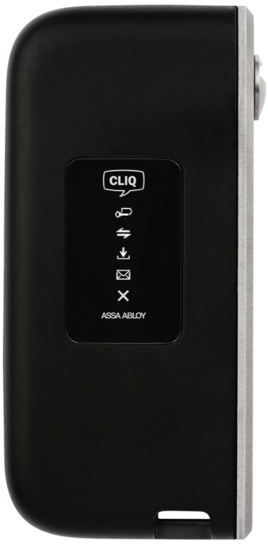


Figure 6. CLIQ Mobile Programming Device

CLIQ Connect Mobile PDs

The CLIQ Connect Mobile PD is used to update keys with CLIQ Connect (Generation 2 keys only) or CLIQ Connect PC.

It can connect to a computer via a micro-USB cable or to a mobile phone via Bluetooth Low Energy (BLE) to use the mobile phone's Internet connection.

The CLIQ Connect Mobile PD needs battery power when connecting with a mobile phone.

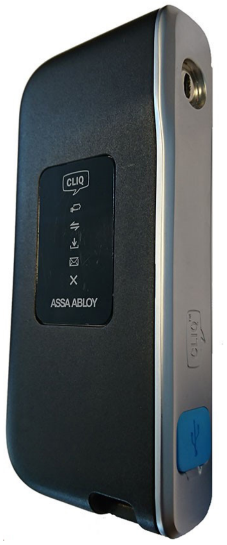


Figure 7. CLIQ Connect Mobile Programming Device

8 CLIQ Concepts and Features

8.1 Authorisation Principles

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

- The mechanical code is correct. See *Section 8.1.1 "Mechanical Authorisation", page 152*.
- The key is Active. This requires that the key is active according to the activation settings and that, if revalidation is used, the key is revalidated within the specified revalidation interval. See *Section 8.1.4 "Key Validity", page 154*.
- The cylinder is electronically programmed to give the key access. See *Section 8.1.2 "Electronic Authorisation", page 152*.
- The key is not blocked in the cylinder. See *Section 8.1.2 "Electronic Authorisation", page 152*.
- For Dynamic Keys: The key has been programmed to have access to the cylinder. See *Section 8.1.2 "Electronic Authorisation", page 152*.
- For Dynamic Keys and Quartz Keys: The key schedule allows access at the current time. See *Section 8.1.8 "Key Schedules", page 158*.

8.1.1 Mechanical Authorisation

As in 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. CWM 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.

8.1.2 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.
- For each key group in the access list, exceptions can be defined, meaning that all keys in the key group except the defined exceptions will have access. This is useful when a cylinder should allow access to all keys in a key group except a few.

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.

For a Dynamic Key to be able to open a cylinder, there must be a match both in the cylinder and in the key. In a typical remote system with Dynamic Keys, the cylinders are programmed to provide access to all keys and the actual access is controlled by the key access list.

Figure 8 "Key access list", page 153 shows the different ways that cylinders or cylinder groups can be included in the access list on the Dynamic Key:

1. directly
2. via an access profile
3. via a user that is associated with an access profile
4. via a temporary access group

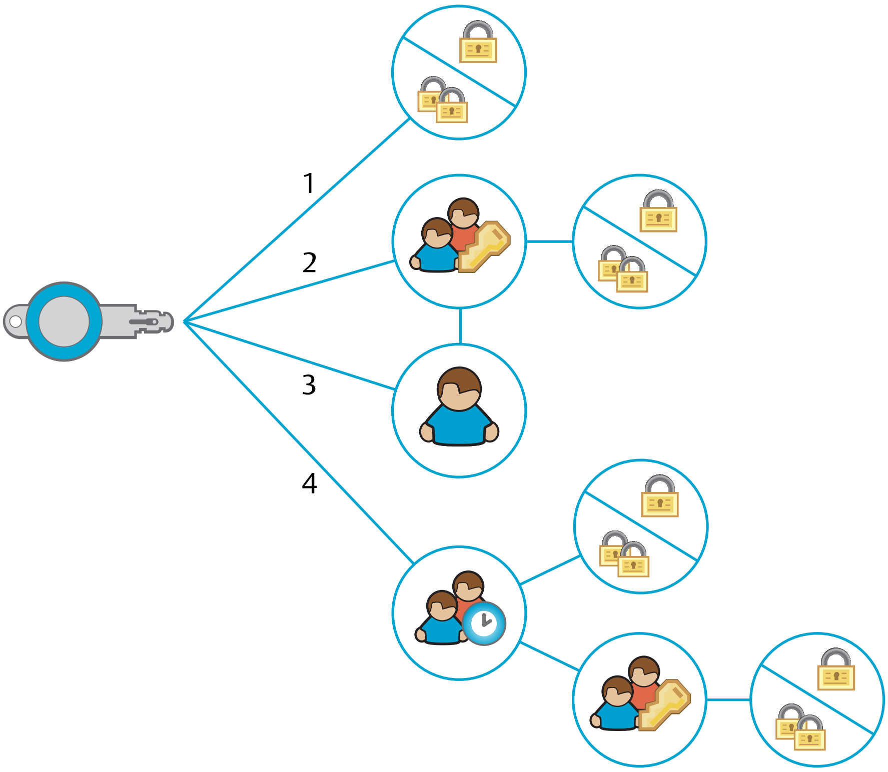


Figure 8. Key access list

The capacity of a Key Access List is limited. The maximum and the currently occupied number of entries can be viewed from the detailed information view of a Dynamic Key. Remote Update Jobs that would exceed the capacity will not be executed. See also *Section 8.3.2 "Remote Update", page 167*.

One difference between Key Access Lists and Cylinder Access Lists is how group entries are handled. In key access lists, cylinders can simultaneously be included both individually and as a part of a cylinder group. This is not the case with Cylinder Access Lists. When a key group is added to a Cylinder Access List, 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.

8.1.3 Explicit and Implicit Access

There are two ways of configuring access lists:

- **Explicit Access** is given by editing the access lists directly on keys, cylinders, and cylinder groups.
- **Implicit Access** is given to keys through access profiles associated with a person or directly with a key. See also *Section 8.2.4 "Access Profiles", page 162*.

Dynamic Keys have an access list that includes the cylinders and cylinder groups that the key is authorised to open. The key's access to a cylinder or a cylinder group can either be explicit or implicit. The access stored in the key access list is the combination of the implicit and explicit accesses.

For more information, see *Section 8.2.4 "Access Profiles", page 162* and *Section 8.2.5 "Temporary Access Groups", page 164*.

8.1.4 Key Validity

Key validity means that a key at any given time is either **Active** or **Inactive**. An active key has access according to authorisation and schedule settings, while an inactive key is blocked from all access. Note that key validity and key schedule are two different concepts. See also *Section 8.1.8 "Key Schedules", page 158*.

There are three ways to control the validity of a key:

- **Activation settings**. A key can be set to be **Inactive**, **Always active**, **Active between selected dates**.

  Active between selected dates is only available for Dynamic Keys and Quartz Keys.
- **Revalidation**, an optional feature. With Revalidation, keys must be updated at specified time intervals to stay active.

  When revalidation is selected, **The key can always be revalidated.** is displayed in the **Validity settings** in CWM.

  See also *Section 8.1.5 "Key Revalidation", page 154*.
- **PIN validation**, an optional feature for CLIQ Connect keys. With PIN validation, keys must be PIN validated using CLIQ Connect at specified time intervals to stay active.

  See also *Section 8.1.7 "PIN Validation", page 157*.

For a key to be active, the following must be fulfilled:

- It must be active according to the activation settings.
- It must be revalidated within the specified revalidation interval (if Revalidation is used).
- It must be PIN validated within the specified PIN validation interval (if PIN validation is used).

See also *Section 4.10.1 "Configuring Key Validity, Revalidation, and PIN Validation", page 81*.

8.1.5 Key Revalidation

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

This feature is subject to licence.

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

Figure 9 "Key revalidation", page 155 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 interval (2). When the revalidation interval 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 **Cylinders in access list**

If the following conditions are fulfilled, a key is revalidated in the right slot of the Local PD **without** C-Key:

- Generation 2 key with firmware version 12.3 or later
- CLIQ Connect PC is activated

NOTE!
The C-Key must be removed from the left slot of the Local PD before update and revalidation.

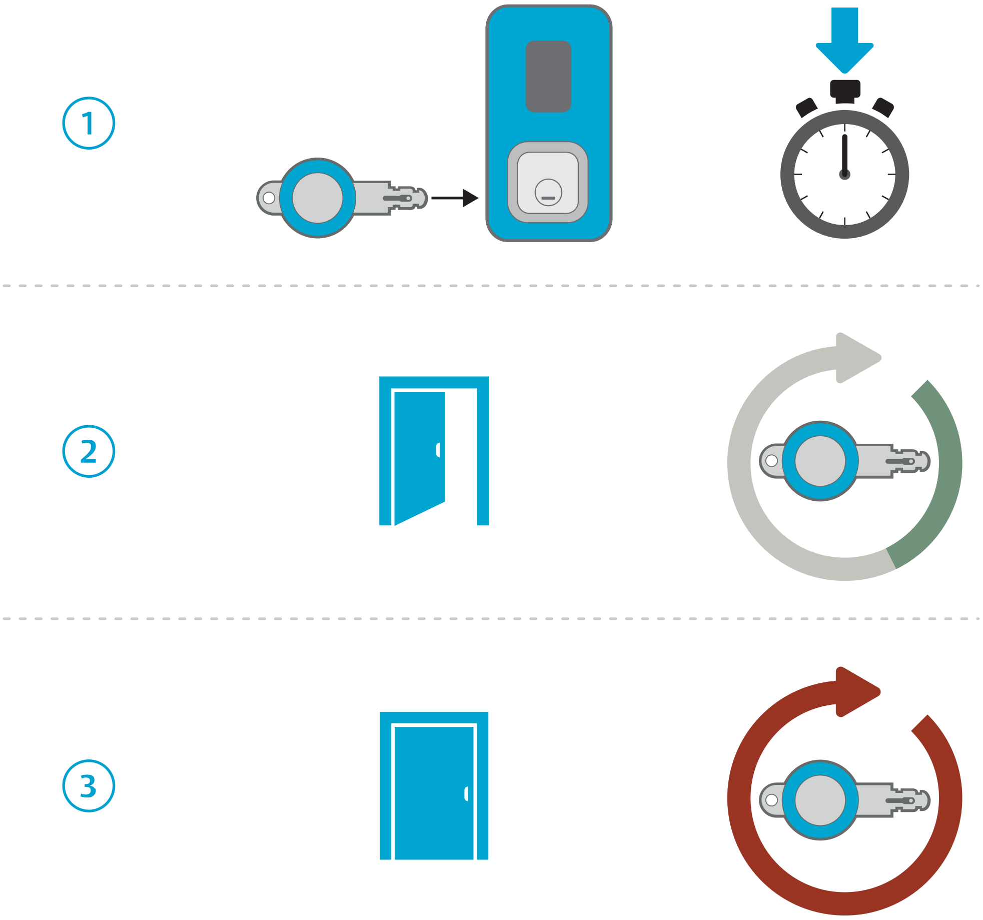


Figure 9. Key revalidation

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 CWM it cannot be revalidated.

Setting the revalidation interval is a trade-off between convenience for the key holder and the locking system security. A short revalidation interval, 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 interval 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.

A way of dealing with this trade-off is using Key revalidation in combination with **PIN validation** (for CLIQ Connect keys). See *Section 8.1.7 "PIN Validation", page 157*.

See also *Section 4.10.1 "Configuring Key Validity, Revalidation, and PIN Validation", page 81*.

Flexible Revalidation is an advanced feature that helps deal with the trade-off issue. See *Section 8.1.6 "Flexible Revalidation", page 156*.

The **Offline Update** function in Remote PDs enables key revalidation even if the Remote PD has temporarily lost its server connection. See *Section 8.3.3 "Offline Update", page 168*.

8.1.6 Flexible Revalidation

Flexible Revalidation is an optional advanced feature that makes it possible to set the key revalidation interval per access profile and per cylinder group. For information about Key Revalidation, see *Section 8.1.5 "Key Revalidation", page 154*.

This feature is subject to licence.

Flexible revalidation is useful in the following situations:

- Cylinders have different sensitivity. For example, access to a server room might be more sensitive than access to a meeting room.
- Roles associated with access profiles have different sensitivity. For example, more frequent revalidation might be required from subcontractors as compared to employees.
- Certain temporary roles may require different revalidation intervals. For example, a person on call duty might need to have a longer revalidation interval, but would be required to be extra careful with the key.

> **CAUTION!**
> When using Flexible Revalidation, all keys that are affected by the revalidation settings on access profiles or cylinder groups must have revalidation enabled.

With Flexible Revalidation, revalidation intervals can be set on three levels:

- **Key setting**. The revalidation interval set on the key constitutes the maximum. No other setting in access profiles or cylinder groups can give a longer revalidation time than this.

  To configure the key revalidation interval, see *Section 4.10.1 "Configuring Key Validity, Revalidation, and PIN Validation", page 81*.
- **Cylinder group setting**. The revalidation interval setting on cylinder groups can be used when cylinder groups have different sensitivity.

  The revalidation interval set on a cylinder group will limit the interval set on the key for that cylinder group. For example, if a key with a revalidation interval of 14 days is given access to a cylinder group with a revalidation interval of 7 days, the setting of 7 days is applied for that cylinder group. But if the cylinder group has a revalidation interval of 30 days, the key setting of 14 days is applied for that cylinder group, since the key setting always constitutes the maximum.

Cylinders in cylinder group systems inherit the revalidation interval set on the cylinder group to which they belong.

Setting a revalidation interval on cylinder groups does not require cylinder programming.

To configure a cylinder group revalidation interval, see *Section 4.10.2 "Configuring Flexible Revalidation", page 83*.

- **Access profile setting**. The revalidation interval setting on access profiles can be used when roles associated with different access profiles have different sensitivity, or when people on call duty temporarily need longer revalidation intervals.

  The revalidation time set on an access profile overrides the setting on cylinder groups. For example, if an access profile with a revalidation interval of 10 days gives access to a cylinder group with a revalidation interval of 7 days, 10 days is applied for that cylinder group for keys associated with the access profile. The Key Setting still constitutes the maximum.

  If a key or a person is associated with more than one access profile with different revalidation intervals, and these access profiles give access to the same cylinder group, the longer interval is applied. For example, if two access profiles, with revalidation intervals of 10 days and 20 days respectively, both give access to the same cylinder group, 20 days is applied for that cylinder group. The cylinder group setting, if specified, is overridden, but the key setting still constitutes the maximum.

  For cylinder groups where both the cylinder group revalidation interval and the access profile revalidation interval is unspecified, the key setting is applied.

  To configure an access profile revalidation interval, see *Section 4.10.2 "Configuring Flexible Revalidation", page 83*.

HINT!
It is strongly recommended to use revalidation settings mainly on **either** cylinder groups **or** access profiles, **not both**. Mixing the two concepts can lead to effects difficult to overview. In the typical case, the setting on cylinder groups is used, with possible exceptions specified on access profiles.

8.1.7 PIN Validation

PIN validation is not available when using CLIQ Connect Mobile PD.

PIN validation is a feature that enables validation offline using a PIN code. It requires using CLIQ Connect and only works with CLIQ Connect user keys.

This feature is subject to licence.

When PIN validation is enabled for a key, the key is disabled after a certain time interval called the **PIN validation interval**. The key holder is then required to enter a PIN code to activate it again. PIN validation is performed in CLIQ Connect, where it is called **Activate**. The mechanism is similar to that of Key revalidation, but PIN validation has a somewhat different purpose:

Key revalidation forces the key holder to update the key at certain intervals to keep the key active. This enables the administrator to make sure the key has the latest updates, and the key will be disabled if reported lost in CWM. Furthermore, when the key is updated, audit trails are fetched from the key if this function is enabled. Key revalidation requires internet connection since it involves fetching updates from the CWM server. No PIN code or password is required to revalidate the key, as it is always preferred that keys have the latest updates. For more information, see *Section 8.1.5 "Key Revalidation", page 154*.

Using PIN validation adds security in several aspects:

- Requires the user to enter a PIN code.
- Protects against lost and stolen keys even though these are not reported as lost in CWM.
- Does not require internet connection. A key can be validated even when the CWM server is down, or the internet connection is lost.
- Since it is rather easy to PIN validate a key, the PIN validation interval can be set to a quite short time, for example 30 minutes, and thus increasing security.

The best security is gained by using a combination of Key revalidation and PIN validation. Key revalidation makes sure the key stays updated, and PIN validation makes sure the key soon becomes unusable for anyone without the PIN code.

In the system settings it is possible to set if PIN validation should be a part of the hand out flow, as well as a default PIN validation interval. See *Section 6.4 "Editing System Settings", page 94*.

See also *Section 8.1.4 "Key Validity", page 154*, *Section 8.1.5 "Key Revalidation", page 154*, and *Section 4.10.1 "Configuring Key Validity, Revalidation, and PIN Validation", page 81*.

8.1.8 Key Schedules

Key Schedules are used to limit key accesses according to a schedule.

If key access needs to be limited to a certain schedule, such as office hours, a schedule can be configured. There are two types of schedules, Basic Schedule and Multiple Time Window Schedule, depending on the firmware version of the key. For more information about key firmware versions, see *Section 9.7 "Firmware Dependent Functionality", page 192*.

- With a Basic Schedule, one time period per day in a week can be specified. The schedule is applied to all cylinders.
- With a Multiple Time Window Schedule, a number of separate time periods per week can be specified and each period can be extended over several days. Schedules can also be set for individual cylinders.

NOTE!

For generation 1 keys:

- For cylinders included in the key access list individually (not as a part of a cylinder group), specifying one or more time periods for a cylinder means that the general schedule is ignored for that cylinder.
- For cylinders included in the key access list as a part of a cylinder group, the cylinder specific time periods are ignored.

For generation 2 keys:

- Specifying one or more time periods for a cylinder means that the general schedule is ignored for that cylinder.

Each key can be configured with a unique schedule or a schedule based on a schedule template.

See also *Section 4.10.3 "Configuring Key Schedule", page 84* and *Section 6.10 "Managing Schedule Templates", page 124*.

8.1.9 Sequence Lock

Sequence Lock is a feature that makes a cylinder require two keys to be unlocked.

Sequence Lock can be configured in the factory on individual cylinders. It can not be configured from CWM.

For cylinders with this feature enabled, unlocking the cylinder requires two keys with access. The keys must be inserted in sequence, within one minute, for the cylinder to open. Cylinders with this feature may optionally be configured to require that the two keys belong to different key groups.

8.1.10 Delay Lock

Delay Lock is a feature that makes a newly revalidated key get access to a cylinder only after a specific time delay.

Delay Lock can be configured in the factory on individual cylinders. It can not be configured from CWM.

For cylinders with this feature enabled, the configured time (for example 15 minutes), is added to the activation and expiration times on any key that accesses the cylinder. For high sensitivity cylinders, it is recommended to use Delay Lock in combination with a short revalidation interval, for example 30 minutes. This ensures that the key is inactive most of the time (if not revalidated very frequently), and that there is a delay after revalidation before someone can actually open the cylinder.

For cases where cylinders have different sensitivity, the feature Flexible Revalidation can be useful. See *Section 8.1.6 "Flexible Revalidation", page 156*.

8.1.11 Online Open

Online Open is a feature used with CLIQ Connect keys that ensures that keys are always updated before opening cylinders. This prevents access for keys with revoked access rights and for keys marked as lost.

Online Open can be configured in the factory on individual cylinders or CLIQ Connect Keys. It can not be configured from CWM.

If Online Open is enabled on a CLIQ Connect key, online opening is required when accessing any cylinder with that key.

If Online Open is enabled on a cylinder, all keys accessing the cylinder are required to perform an online opening. This means that access is limited to CLIQ Connect keys.

When online opening is required, the CLIQ Connect key must be paired with CLIQ Connect before inserting it into the cylinder. Once the key is inserted, CLIQ Connect contacts the CWM Remote Server, fetches the latest updates for the key, and performs a key update. If the key has access to the cylinder after the key update, the cylinder unlocks immediately.

Cylinders with the Online Open feature can be configured to accept **Override keys** without requiring online opening. Keys can be configured as Override keys in factory.

8.2 Grouping Functions

8.2.1 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 groups are mainly used when using access lists in cylinders to control accesses.

Key group benefits:

- Key groups reduce the number of entries required in cylinder access lists.
- Adding a new key to a key group that is allowed in certain cylinders automatically gives access to the new key also. No programming of cylinders is required.
- Key groups can be used for bulk configuration of key schedules.

When a key group is given access to a cylinder, all keys in the key group are automatically given access. It is possible, however, to define exceptions and exclude individual keys from access.

> **NOTE!**
> When a key group is added to an access list, 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.

There are different types of key groups:

Normal Key Group	Can contain Quartz Keys and Normal Keys.
Dynamic Key Group	Can contain Dynamic Keys.
Normal C-Key Group	Can contain Normal C-Keys.
Master C-Key Group	Can contain Master C-Keys.

Mechanical keys cannot belong to a key group.

To bulk configure schedules in a key group, see *Section 4.10.4 "Configuring Key Group Schedule", page 86*.

8.2.2 Domains

The **Domains** feature is an administrative grouping feature that allows administrators to access and control specific regions of a locking system.

This feature is subject to licence.

Domains are used to divide the following elements into administrative regions:

- keys
- employees
- visitors
- cylinders
- cylinder groups
- access profiles
- temporary access groups

Key groups and C-Keys cannot belong to a domain. Therefore, key groups and C-Keys are visible for administrators regardless of their domain.

A domain consists of a set of element groups typically associated with a geographic or organisational region. C-Keys associated with a domain are only given administration rights for the included cylinders.

Domain benefits:

- Convenience: Administrators working with regions of a locking system, such as a geographic region, are not concerned with information about elements in other regions.
- Security: Administrators are not allowed to view or administer elements in other domains.

Domain facts:

- Cylinders that belong to a cylinder group are included in a domain through their cylinder group. That is, all cylinders in a cylinder group belong to the same domain.
- Cylinders that do not belong to a cylinder group, including all mechanical cylinders, are included in a domain individually.
- Elements can only belong to one domain (keys, employees, visitors, cylinders, cylinder groups, access profiles, and temporary access groups).
- For double-sided cylinders, both sides must belong to the same domain.
- An administrator's C-Key can be associated with one or more domains, depending on the assignment.

> **NOTE!**
> Even though C-Keys cannot belong to a domain, each C-Key has a list of domains that the logged in administrator is authorised to access and control.

To associate a C-Key with a domain, see *Section 6.11.5 "Selecting C-Key Domains", page 127*.

8.2.3 Cylinder Groups

A **Cylinder Group** is a set of cylinders that is used to simplify the administration in locking systems with many cylinders.

This feature is subject to licence.

Cylinder groups are used in locking systems that are defined as **Cylinder Group Systems**, for the cylinders that have cylinder group support. See *Section 9.7 "Firmware Dependent Functionality", page 192*.

Cylinder groups are pre-defined from factory, but it is possible to move cylinders between groups afterwards. This, however, requires cylinder programming and it is therefore recommended to plan the groups carefully in advance.

Access can be given to a cylinder group in the same way as to a single cylinder. Combinations of cylinder groups and single cylinders can be used to create high flexibility.

Cylinder group benefits:

- Easier administration of locking systems with many cylinders.
- Since only one entry on the key can give access to many cylinders, a key can get access to a very large number of cylinders.

- When a cylinder is added to or removed from a cylinder group, keys that have access to the cylinder group are immediately affected. Manual update of each key's access list is not required.

Configuring cylinder groups is a trade-off between different considerations:

- Cylinder groups should be configured in such a way that access is normally given to all cylinders in the group.

  It is not possible to give access to all cylinders in a group but omit a few. If it is necessary to do this, the cylinder exceptions should be placed in a separate group.
- Cylinder groups should not be too small, since it is important to limit the number of groups. The fewer the groups, the easier the administration, and the fewer the number of required entries in key access lists.
- Cylinder groups should still be small enough to be stable, that is, it should be unlikely that cylinders need to be moved between groups.

Cylinder group facts:

- Cylinders can only belong to one cylinder group.
- Cylinder groups can only belong to one domain.
- For double cylinders, both sides must belong to the same cylinder group.
- Mechanical cylinders cannot belong to a cylinder group.

8.2.4 Access Profiles

Access Profiles are used to give people that have specific roles the required accesses without having to configure each key individually. Keys can also be directly associated with access profiles.

This feature is subject to licence.

> **NOTE!**
> Roles defined by access profiles must not be confused with the roles defined for administrators working with CWM.

People who have a specific role, such as office cleaning, are associated with a corresponding access profile. The access profile defines a set of cylinders and cylinder groups that must be accessed by people with that particular role. Keys handed out to associated people automatically contain the right accesses as defined in the access profile.

Figure 10 "Access profiles", page 163 shows an example with two access profiles (1, 2), each with access to a number of cylinders or cylinder groups, or both (A, B). The access profiles can be associated with either a person (3) or a key. When associated with a person, the key handed out to that person is automatically given the access of the associated access profiles (C).

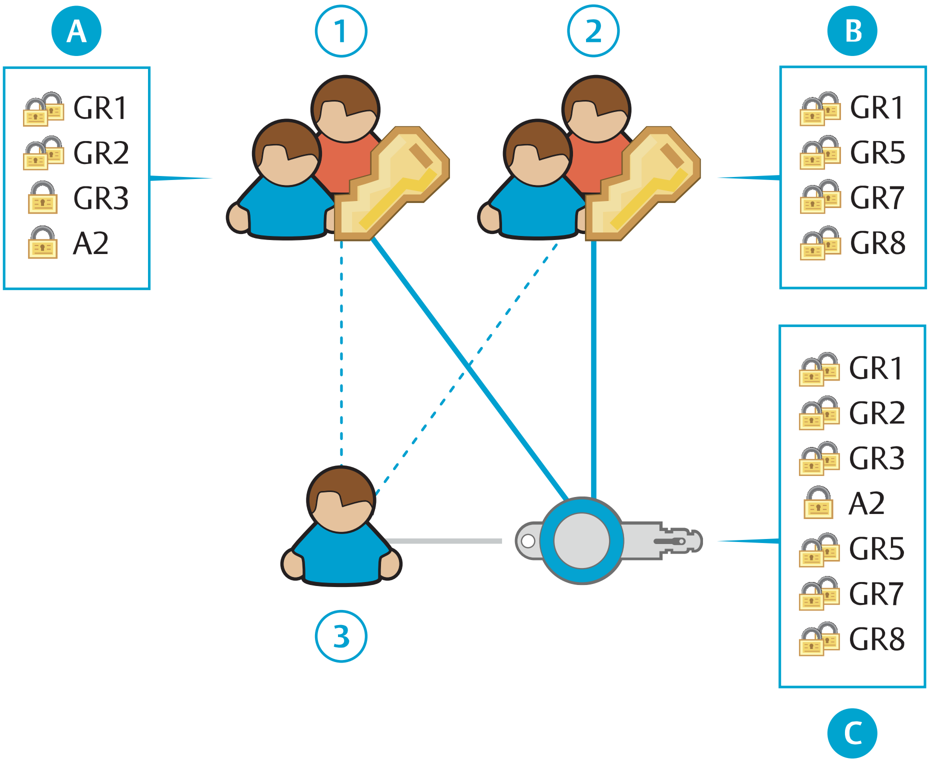


Figure 10. Access profiles

If an access profile is directly associated with a key, other keys belonging to the same key holder do not inherit that access profile.

Access profiles are dynamic in the sense that a change in the access profile automatically updates the state of key authorisations, as they are defined in CWM (also called **Defined State**). A change in the access profile generates remote update jobs for associated keys. No cylinder programming is required. For information about **Defined State** and **Actual State**, see *Section 9.1.1 "Terms", page 179*.

Access profiles defines the **Implicit Access** for keys, while the authorised cylinders and cylinder groups directly defined for the key make up the **Explicit Access**. The actual access stored in the key access list is the combination of the implicit and explicit accesses. That is, the key can access both the cylinders defined in the access profile and the cylinders defined explicitly for the key.

Access profile benefits:

- Possible to simultaneously manage access for several people or keys.
- Possible to define profiles corresponding to roles, and give access to people who have one or more roles.
- When an access profile is changed, associated remote update jobs are automatically created.

Access profile facts:

- A key or a person can have several roles and therefore be associated with more than one access profile.
- Both individual cylinders and cylinder groups can be included in an access profile.

- An access profile belongs to one single domain and only cylinders and cylinder groups that belong to that domain can be added.

NOTE!
It is recommended to make sure an access profile and all included cylinders and cylinder groups belong to the same domain. This is to ensure that administrators for a specific domain cannot get indirect access to cylinders in other domains (through access profiles).

- When introducing access profiles in a locking system where authorisations in key access lists are already used, the key access lists may include multiple entries of the same cylinder or cylinder group. To remove redundant entries, see *Section 4.7.7 "Removing Redundant Key Authorisations", page 72*.

HINT!
To keep a better overview when using access profiles, it is recommended to minimise the use of explicit accesses.

8.2.5 Temporary Access Groups

Temporary Access Groups are used to temporarily expand the access of keys by associating them with a selection of access profiles. The access of a temporary access group is the combined access of the included access profiles during a time period that is defined with a start date and an end date.

Keys in the temporary access group are given implicit access to the cylinders and cylinders groups that are assigned to the included access profiles. In addition, keys can be given explicit access to individual cylinders and cylinder groups that are assigned to the the temporary access group.

Figure 11 "Temporary Access Groups", page 165 shows a key that is added to a temporary access group (1) with three access profiles (2, 3, 4) and one set of individual cylinders and cylinder groups (4). Each access profile has access to a number of cylinders or cylinder groups, or both (A, B, C). During a defined time period the key is granted access to all cylinders and cylinder groups (D).

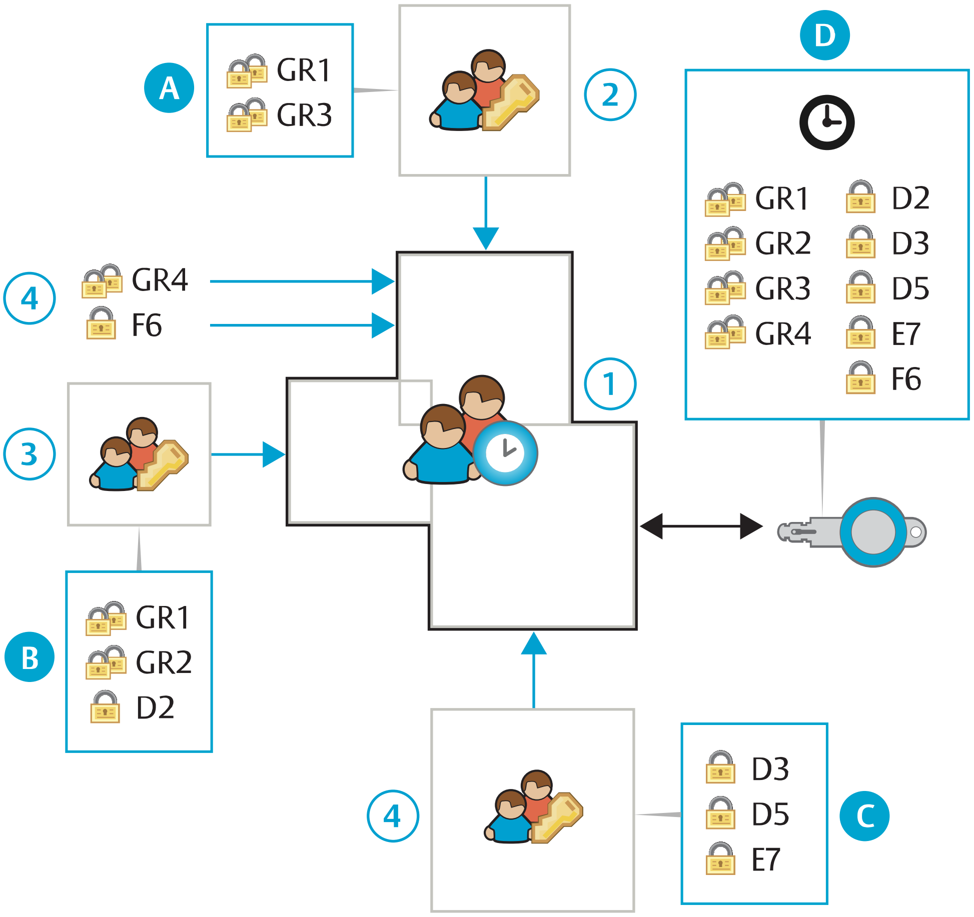


Figure 11. Temporary Access Groups

An example of usage is when one or several service technicians are on call and need access to a number of access profiles during the on call period.

In practice, the key is added to a temporary access group and programmed in a local or Remote PD. When the temporary access group is no longer valid for a key, a remote job will automatically be created to remove the access of the temporary access group from the key.

NOTE!
Cancellation of the key's access will not take effect until the key is updated in a Remote PD. To cancel the key holder's possibility to use the key after the temporary access group has expired, do one of the following prior to handing out the key:

- Set **Active between selected dates** in the activation settings, see *Section 8.1.4 "Key Validity", page 154*.
- Activate key **Revalidation**, see *Section 8.1.5 "Key Revalidation", page 154*.

It is strongly recommended to combine temporary access groups with key revalidation.

Temporary access group benefits:

- Possible to temporarily give one or several keys access to a group of access profiles, individual cylinders, and cylinder groups.

Temporary access group facts:

- All access profiles within a temporary access group must be part of the same domain.
- Users assigned to the default domain can see temporary access groups from all domains. Logged in users for other domains can only see temporary access groups within their own domains.

8.2.6 Tags

A **Tag** is a text string that can be used to label objects to make them easier to find and administrate.

For example, access profiles can be grouped by the type of role they are associated with, and cylinders can be grouped by the building where they are installed.

When searching for objects, tags can be entered as a search criteria.

Tags are sometimes already added in extension files and available when the files are imported to CWM. It is also possible to add or delete tags manually for the following objects:

- Employees (see *Section 4.1.7 "Adding or Removing Employee or Visitor Tags", page 30*)
- Visitors (see *Section 4.1.7 "Adding or Removing Employee or Visitor Tags", page 30*)
- Keys (see *Section 4.2.5 "Adding or Removing User Key Tags", page 35*)
- Key groups (see *Section 4.3.3 "Adding or Removing Key Group Tags", page 52*)
- Cylinders (see *Section 4.4.3 "Adding or Removing Cylinder Tags", page 54*)
- Cylinder groups (see *Section 4.5.3 "Adding or Deleting Cylinder Group Tags", page 64*)
- Access profiles (see *Section 4.6.4 "Adding or Deleting Access Profile Tags", page 66*)
- Remote PDs (see *Section 6.5.5 "Adding or Removing Remote PD Tags", page 101*)

More than one tag can be added to each object.

8.3 Remote Feature

8.3.1 Remote Feature Overview

The remote feature enables remote updates of key configurations. It also enables revalidation and retrieval of audit trails from a remote site.

This feature is subject to licence.

- **Remote update of key configurations**

  The administrator configures authorisations and other settings on keys without the key being present. The new key configuration is stored in the remote server database as a **Remote Update Job**. When the key is inserted in a Remote PD, the update job is executed and the key is programmed with the new configuration.
- **Remote update of current key time setting**

  The current key time setting is updated at each key update.
- **Remote retrieval of audit trails**

The key audit trail is retrieved at each key update, unless Approvals in System settings is enabled.

- **Revalidation**.

  Revalidation ensures that keys are updated at certain time intervals. For more information about revalidation, see *Section 8.1.5 "Key Revalidation", page 154*.

See also *Section 8.3.2 "Remote Update", page 167*.

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.

8.3.2 Remote Update

Remote Update Jobs are pending key updates. This should not be confused with **Cylinder Programming Jobs**, that are pending cylinder updates. For more information about Cylinder Programming Jobs, see *Section 8.5 "Cylinder Programming", page 169*.

Unless the key is scanned in the Local PD, all actions that require updates of the information on the key will result in a Remote Update Job, which includes updating authorisations, validity, schedule, and so on. The Remote Update Job will be executed the next time the key is inserted in a Remote PD.

The Remote PD is normally online but can be configured to allow key updates under certain conditions also when it is offline. See *Section 8.3.3 "Offline Update", page 168*.

Throughout CWM, the following symbol is used for Remote Update Jobs:

⚙ Pending remote update exists for the key

To view pending remote authorisation updates, see *Section 4.9.1 "Configuring Authorisations in Keys", page 74*.

Exceeding Key Capacity

Remote Update Jobs that would exceed the capacity of a Key Access List cannot be executed. When such a job is created in CWM, an email about this is sent to all administrators that have the full **Key authorisations** permission and that have an email address specified. The job is also marked with the following symbol in CWM:

⚙ Pending remote update exists that exceeds key capacity

When performing operations on a single key from the key view, a Remote Update Job is created instantly and the administrator can immediately see if it exceeds key capacity. However, when performing operations on keys from other views, Remote Update Jobs are not created instantly and the administrator does not get immediate feedback.

Operations that may generate Remote Update Jobs exceeding key capacity and where the administrator does not get immediate feedback include:

- Adding accesses to an access profile
- Adding access profiles to multiple keys
- Adding access profiles to a person

To resolve the situation, the number of entries in the Key Access List must be reduced. This is done by reducing the number of explicit accesses, by reducing the number of accesses in associated access profiles, or by removing associated access profiles. The Remote Update Job is automatically adjusted accordingly.

8.3.3 Offline Update

Offline Update is not available when using CLIQ Connect Mobile PD.

Offline Update is a function that enables keys to be revalidated through a Remote PD even if it has temporarily lost its network connection. This is useful in situations where it is critical that a key can get its validity extended even if the network connection is unstable. Updates of accesses cannot be made in offline mode. Offline Update is configurable per Remote PD.

To limit the risks and the exposure of lost keys, a number of conditions can be set for an offline update to be allowed. The following is configurable:

- The number of consecutive updates that can be made in offline mode before an online update is required.
- For how long time offline updates are allowed after the last online update.
- How much the key validity is extended at an offline update. The revalidation interval set on keys is ignored at offline updates.

Specific for Wall PDs

The key is not allowed an offline update if it is included in the **Key Revocation List** stored in each Wall PD. This list contains the keys that have been reported lost and therefore should not be allowed offline updates. The Wall PD checks for new versions of the Key Revocation List at each heartbeat and only allows offline updates if the version of the list stored in the Wall PD is not too old. The time a Key Revocation List is valid is configurable with a Wall PD parameter.

Specific for CLIQ Mobile PDs

Only keys that have recently been updated in the same CLIQ Mobile PD (keys that are within the last 10 updated keys) may be revalidated in offline mode.

See also *Section 8.1.5 "Key Revalidation", page 154*.

To configure Offline Update, see *Section 6.5.7 "Configuring Wall PDs", page 102* and *Section 6.5.8.1 "Editing CLIQ Mobile PD Settings", page 109*.

8.3.4 CLIQ Connect and CLIQ Connect+

CLIQ Connect is an application installed on a mobile device such as a mobile phone or a tablet. It enables user key holders, that means visitors and employees, to easily manage their user keys. CLIQ Connect is available for Android and iOS.

CLIQ Connect offers the following functions:

- Validate and change the PIN code of a Connect key.
- Update Connect keys via the key's Bluetooth connection
- Update the other types of user keys via a CLIQ Connect Mobile PD.

CLIQ Connect+

CLIQ Connect+ can be used with CLIQ Connect **version 4.0 or later**. With this feature, any registered key holders can see more details of their keys, such as validity, schedule, or accessible cylinders, for both connect keys and non-connect keys.

Once activated, the key holder follows the email instructions from CWM to complete the setup. The app is configured using a QR code included in the email.

This functionality requires the following conditions:

- CWM System version 11.2 or later.
- The licence **CLIQ Connect+** is granted to the system.

  To install the licence, see *Section 6.1 "Managing Licences", page 93*.
- The key holder is an activated CLIQ Connect+ user.

  To enable key holders to access the CLIQ Connect+, see *Section 4.1.5 "Activating or Deactivating CLIQ Connect+ for Employees or Visitors", page 27*.
- The key holder activates the CLIQ Connect+ account following the email instruction sent by CWM.

8.4 External Links

An **External Link** is a URL, an Internet address, that can be used to link an object, such as an employee or a cylinder, to more information.

For example, an employee can be linked to the employee's page on the company Intranet and a cylinder or a Wall PD can be linked to a map of its location.

External Links can be added to the following objects:

- Employees (see *Section 4.1.8 "Managing Employee or Visitor External Links", page 31*)
- Visitors (see *Section 4.1.8 "Managing Employee or Visitor External Links", page 31*)
- Keys (see *Section 4.2.6 "Managing User Key External Links", page 36*)
- Cylinders (see *Section 4.4.4 "Managing Cylinder External Links", page 55*)
- Access profiles (see *Section 4.6.5 "Editing Access Profile External Links", page 67*)
- Remote PDs (see *Section 6.5.6 "Managing Remote PD External Links", page 102*)

More than one external link can be added to each object.

8.5 Cylinder Programming

Cylinder programming includes updating a cylinder's access list or retrieving cylinder audit trails.

A **Cylinder Programming Job** is created in CWM in these situations:

- The authorised keys for a cylinder are updated.
- A key included in the cylinders' access list is reported as lost or broken.
- Reprogramming of a cylinder is selected.
- A cylinder audit trail retrieval is selected.
- The cylinder group to which a cylinder belongs is changed.

When the Cylinder Programming Jobs are to be executed, they are first loaded onto a C-Key in the Local PD or Remote PD. By inserting the C-Key in the cylinder, the Programming Job is executed and, if applicable, the audit trails from the cylinder are loaded onto the C-Key. Once the programming job is executed, the C-Key is once again inserted in the Local PD or Remote PD and the locking system can be updated with information about the completed programming jobs and the retrieved audit trails.

Figure 12 "Cylinder programming", page 170 shows two ways of executing cylinder programming jobs:

- In the first case (1) the cylinder programming job is loaded onto the administrator's C-Key (A) via a Local PD. The C-Key is then transported and inserted to the cylinder that needs programming and returned when the job is done to update the locking system.

- In the second case (2) an administrator logs in to CWM using a C-Key (A) and prepares cylinder programming jobs that other administrators pick up with their C-Keys (B) in a Remote PD. The C-Keys are then inserted to the cylinders and returned to the Remote PD to update the locking system.

  The option to pick up, execute and confirm cylinder programming jobs via a Remote PD makes it possible to have one administrator preparing the jobs in CWM and another administrator programming the cylinders without ever logging in to CWM.

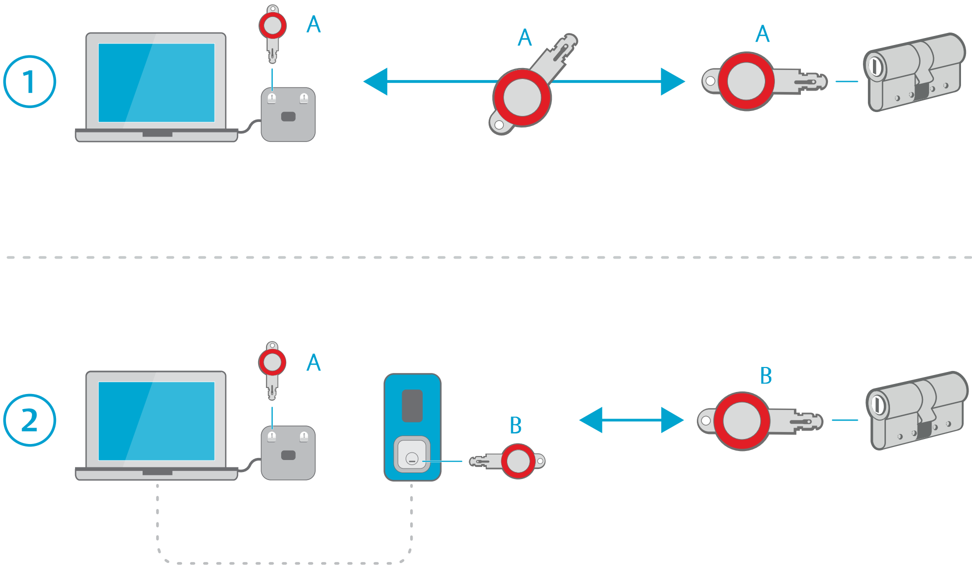


Figure 12. Cylinder programming

Throughout CWM, the following symbols are used for Cylinder Programming Jobs:

⚙ Cylinder programming job exists

⚙ Cylinder programming job needs approval

⚙ Cylinder programming job has been programmed to C-Key

⚙ Cylinder programming job has been finished

⚙ Cylinder programming job has failed or been cancelled

⚙ Cylinder programming job has been replaced with a new job

Cylinder Programming Jobs can only be loaded onto C-Keys with the **Cylinder programming** permission.

Jobs involving the change of a cylinder's cylinder group also require a C-Key with the **Cylinder group programming** capability. To see whether a C-Key has the Cylinder group programming capability, view the detailed C-Key information. See *Section 6.11.1 "Searching* *for C-Keys", page 125* or *Section 6.11.2 "Scanning a C-Key", page 125*. In systems initially delivered as cylinder group systems, all C-Keys have this capability.

See also *Section 4.4.13 "Programming Cylinders", page 59* and *Section 8.8 "CWM Roles and Permissions", page 173*.

Reprogramming
Reprogramming can be used as a first troubleshooting measure if a cylinder does not work as expected. For example, if the C-Key is removed too early when programming a cylinder, the cylinder will not work properly and reprogramming resolves the problem.

When the C-Key with a failed programming job is inserted into a Remote PD, CWM automatically recreates the programming job and sends it to the key again. This enables the key holder to redo the programming job.

CWM also notifies the administrator, via email, with information about which key was used, the affected cylinder, and the reason of programming when failing. This function is always on and cannot be deactivated.

When a cylinder is reprogrammed, its memory content is deleted, including the audit trails. The cylinder access list is then restored as part of the reprogramming. This is different from normal cylinder programming, when the cylinder access list is only updated and the audit trail is left untouched.

A Master C-Key or a Normal C-Key with Cylinder Reprogramming rights is needed to perform the actual reprogramming job.

See also *Section 4.4.12 "Requesting Cylinder Reprogramming", page 58*.

8.6 Audit Trails

Both cylinders and keys have an audit trail feature. An Audit Trail is a list of events involving keys requesting access in a cylinder as well as keys and cylinders being programmed. There are two types of audit trails:

- **Normal audit trails** contain events where involved devices belong to the same locking system.
- **Foreign audit trails** contain events where involved devices belong to different locking systems.

Key Audit Trails
Only Quartz Keys and Dynamic Keys can store the audit trails.

The key audit trail records the 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 to access the cylinder, 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. Note that the audit trail does not record cylinder access attempts by a Mechanical Key.

Automatic Audit Trail Retrieval
If a user key belongs to a remote system, supports remote updates, is a Quartz or dynamic key, and audit trail approvals are disabled, handing out the user key triggers the creation of a remote read audit trail job.

A C-Key can be programmed to retrieve cylinder audit trails automatically. This function enables the key holder to easily and quickly retrieve audit trails from arbitrary cylinders within the domain. See also *Section 6.11.13 "Activate or Deactivate Automatic Audit Trail Retrieval for C-Key", page 133*.

Automatic Audit Trail Archive Removal

The audit trail archive can be configured to automatically remove audit trails older than a defined number of days. This deletion process is based on the creation date—the date when the entry was generated on the physical element—rather than the parse date, which is when the entry was stored in the CWM database.

If the **Extended audit trail and event archive** licence is not granted, the automatic removal period can be set up to 366 days.

If the **Extended audit trail and event archive** licence is granted, the automatic removal period can be set up to 3660 days.

Approvals

In locking systems where the **Approvals** feature is enabled, all audit trail requests for keys and cylinders need to be approved by an administrator with the **Approver** role. Once the audit trail is read from a key or a cylinder, it can be viewed by any administrator with view permission for **Audit Trails**. See also *Section 8.8 "CWM Roles and Permissions", page 173*.

The feature is enabled or disabled in **System settings**. See *Section 6.4 "Editing System Settings", page 94*.

8.7 Events

Operations performed by the administrator on the following CWM components are stored as events and viewed on the **Events** tab of each component.

- **Employee or visitor**

  To view employee or visitor events, see *Section 4.1.10 "Viewing Events for Employee or Visitor", page 32*.
- **Key**

  To view key events, see *Section 4.2.8 "Viewing Events for User Key", page 37*.
- **Cylinder**

  To view cylinder events, see *Section 4.4.7 "Viewing Events for Cylinder", page 56*.
- **Cylinder group**

  To view cylinder group events, see *Section 4.5.5 "Viewing Events for Cylinder Group", page 64*.
- **Access profile**: such as adding and removing cylinders in an access profile.

  To view access profile events, see *Section 4.6.7 "Viewing Events for Access Profile", page 68*.
- **Temporary access group**

  To view access profile events, see *Section 4.7.6 "Viewing Events for Temporary Access Group", page 71*.
- **Remote PD**.

To view Remote PD events, see *Section 6.5.9 "Viewing Remote PD Event Log", page 114*.

- **C-Key**

  To view C-Key events, see *Section 6.11.6 "Viewing C-Key Events", page 128*.

Automatic Event Archive Removal
The event archive can be configured to automatically remove audit trails older than a defined number of days.

If the **Extended audit trail and event archive** licence is not granted, the automatic removal period can be set up to 366 days.

If the **Extended audit trail and event archive** licence is granted, the automatic removal period can be set up to 3660 days.

> **NOTE!**
> The following events are not subject to automatic removal and remain in the history even after the retention period has passed:
>
> - Key, cylinder and Remote PD activation
> - The latest key handout event in the employee or visitor events and the key events.

8.8 CWM Roles and Permissions

Roles are defined by the combination of the given permissions and assigned to C-Keys.

Each permission gives roles different levels of right to perform a certain CWM function.

Roles
The functions visible in CWM depend on the role assigned to the C-Key used by the administrator who is logged in. It is highly recommended that administrators only have access to functions they need in their work. For example, an administrator performing only programming tasks for cylinders may only have access to that function. An administrator responsible for key management may only have access to the hand out/hand in and the key lost/broken procedures.

> **NOTE!**
> Roles defined for administrators working with CWM must not be confused with the roles defined by access profiles.

The following roles are pre-defined in CWM:

Table 2. Pre-defined Roles

Role	Description
Super Administrator	Full permissions except the permission to approve audit trail requests.
Administrator	Permissions for major tasks, such as configuring authorisations, editing templates, and so on.
Receptionist	Permissions needed for simpler daily tasks, such as key hand-out and hand-in.
Approver	Permissions only to approve audit trail requests.

Role	Description
Cylinder Programmer	Permissions only to execute cylinder programming.
WebService	Used for Web services integration.

The Super Administrator and the Approver roles cannot be deleted or edited. The WebService role can be edited but not deleted.

More than one role can be assigned to a C-Key, but the Approver role cannot be combined with other roles. For more information about how to assign roles, see *Section 6.11.4 "Editing C-Key Information", page 126*.

NOTE!
Some rights for C-Keys depend on the C-Key type and are not configurable through roles and permissions. See *Section 7.2.4 "C-Keys", page 145*.

By default, the roles described above are in a flat structure. Administrators can create or edit roles with higher permissions than what they are granted, and can assign or unassign these roles on C-Key.

When the hierarchical administrators function is turned on, the hierarchy of the roles is formed, and the following restrictions are applied:

- the administrator cannot grant a permission level that is higher than their own.
- the administrator cannot assign or delete roles with a permission level that is higher than their own.

The rank of the roles in the hierarchy is determined by the permission level. If a role is granted a higher permission level than what the administrator is granted, the role is assumed as a higher role than the administrator's role and cannot be edited or deleted by the administrator.

The hierarchical administrators function can be enabled by the Super Administrator from the **System settings** page.

Permissions

For each role, permissions are given per specific CWM function, such as handling keys, cylinders, employees, firmware, system settings, C-Keys, and so on.

Permission for a CWM function is set to one of the following levels:

Table 3. Permission Levels

Level	Description
None	Allows no access.
List	Allows searching and listing.
View	Also allows viewing details.
Full	Also allows editing information.

For a full list of permissions and what is allowed at each level, see *Section 9.4 "Permissions", page 185*.

See also *Section 6.7 "Managing Roles and Permissions", page 119*.

8.9 Deletion of Personal Data and GDPR Compliance

CWM can be set to handle deleted employees and visitors in two different ways: **Delete permanently** or **Mark as deleted**. The behaviour is controlled by the system setting **When deleting persons**.

Delete Permanently

In order to support GDPR, the Deletion of Personal Data setting needs to be set to **Delete permanently**. When set to this, the following applies:

- When deleting a person, the corresponding data is deleted permanently from the database and cannot be restored. References to a deleted person in event logs and audit trails are permanently replaced with **N/A**.
- In addition to **Delete**, there is also a function to **Deactivate** a person. Deactivation means that all personal data is hidden and is not processed in any way as long as the person is deactivated. References to a deactivated person in event logs and audit trails are temporarily replaced with **N/A**. These references are restored if a person is reactivated. Only administrators with the **Deactivate key holder** permission can deactivate persons, as well as view and reactivate deactivated persons.
- Information about deactivated persons cannot be edited, deleted, exported or processed in any other way.
- When importing employees from a file, employees that are deactivated in CWM are ignored even if their data is modified in the CSV file.

See also *Section 4.1.3 "Deactivating or Activating Employees or Visitors", page 25*.

Mark as Deleted

Set to **Marked as Deleted** the Deletion of Personal Data does not follow GDPR.

Deleted persons are not removed from the database and a deleted person may still be referenced in for example events and audit trails. Deleted persons can be restored according to *Section 4.1.4 "Deleting or Restoring Employees or Visitors", page 26*. A person that is not marked to be deleted is in CWM described as **Active** (not to be confused with deactivated or activated persons when the system setting is set to **Delete permanently**).

8.10 Single Sign-On (SSO)

Single Sign-On (SSO) allows administrators to access the system without its C-Key.

SSO functionality must be configured individually in each system. When SSO is supported, the Super Administrator can enable or disable the feature as needed. For more details, see *"SINGLE SIGN ON (SSO)"* in *Section 6.4 "Editing System Settings", page 94*.

When it is enabled, an administrator who has been issued a new C-Key must first enrol a certificate using the CCPC and the C-Key. Once the certificate enrolment is successfully completed, the administrator can log in to the system without the C-Key.

Note that certain operations within the system, such as programming jobs that require secure data stored on the C-Key, still require the administrator to log in with the C-Key. In these cases, a pop-up message will prompt the user to insert the C-Key and authenticate accordingly.

The following functions require C-Key login:

- Local cylinder programming: sending tasks to the C-Key, updating its status, and removing finished or unfinished tasks

- Copy key configuration
- Activate extension import
- Enable or disable automatic audit trail retrieval on the C-Key
- Unlock the C-Key
- Change C-Key PIN
- Refresh the status of user key inserted into the local PD via the top bar of the page

8.11 DCS Integration

DCS is a server application for managing certificates and licences in a CLIQ locking system.

DCS Integration enables automatic certificate generation for C-Keys and Remote PDs, and thereby eliminates the need to distribute these certificates separately. It also enables fetching licence files, firmware files and extension files from DCS.

DCS Integration must be activated during the system installation.

With DCS Integration, Remote PD certificates are generated from within CWM, while C-Key certificates are generated through **CLIQ Connect PC**.

C-Key certificate enrolment can be set to be **Always Allowed** (recommended), **Allowed once**, or **Not Allowed**. For the Master C-Key this is set in DCS and for Normal C-Keys settings are made in CWM (see *Section 6.11.4 "Editing C-Key Information", page 126*).

Table 4. Certificate Enrolment Setting

Setting	Description
Always Allowed	The C-Key certificate can be enrolled many times. This is useful if the C-Key holder needs to access CWM from more than one computer.
Allowed once	The C-Key certificate can be enrolled only once.
Not Allowed	Enrolment is not allowed.

NOTE!
Certificate renewal is allowed regardless of this setting.

To generate C-Key certificates, see *Section 3.2.1 "Enrolling C-Key Certificate via CLIQ Connect PC", page 16*.

To generate Remote PD certificates, see *Section 6.5.7 "Configuring Wall PDs", page 102* or *Section 6.5.8 "Configuring Mobile PDs", page 108*.

To fetch a licence file from DCS, see *Section 6.1.1 "Installing Licences", page 93*.

To fetch an extension file from DCS, see *Section 6.16 "Importing Extensions", page 142*.

8.12 LDAP Integration

LDAP stands for Lightweight Directory Access Protocol, and is a software protocol which enables access to the directory services. In the context of CWM, LDAP is used as the master source of employees information by integrating with CWM. CWM supports OpenLDAP, Microsoft Active Directory and Apache Directory.

When LDAP is integrated, employees added in a particular active directory are automatically (once per 24 hours) or manually synchronised to CWM. In CWM, the employees from LDAP coexist with employees in CWM, and their first names, surnames, emails and mobile phone numbers are visible and searchable.

If the CLIQ Connect+ feature is enabled and the employee is an activated CLIQ Connect+ user, deactivating or deleting the employee or deleting the employee email address is not possible. For more information about the CLIQ Connect+ feature, see *Section 8.3.4 "CLIQ Connect and CLIQ Connect+", page 168*.

Since information from LDAP is read-only, there are some restrictions in managing the employee in CWM when LDAP integration is enabled. *Table 34 "The available activities in CWM when LDAP is integrated", page 177* shows which management administrators can handle.

Table 5. The available activities in CWM when LDAP is integrated

	Employee	
	LDAP integrated	**non LDAP integrated**
Add	n/a	✓
Edit	✓* *Only **Domain** and **TAGS** can be changed from GUI.	✓
Delete/Deactivate	n/a	✓

LDAP integration is enabled or disabled in the **System settings** page. See *Section 6.4 "Editing System Settings", page 94* for setting LDAP integration. As prerequisites both the licence and the permission for LDAP integration have to be granted to the administrators. See *Section 6.1 "Managing Licences", page 93* to install the licence and *Section 6.7 "Managing Roles and Permissions", page 119* to grant the permission.

8.13 Licensing

To be able to use CWM, a licence is required. Licences are issued per locking system by the local CLIQ dealer.

A valid licence always gives access to the basic functions in CWM. In addition, the availability of the following features are controlled by licence content:

- Remote
- Domains
- Access profiles
- Temporary access groups
- Revalidation
- Flexible Revalidation
- Cylinder groups
- Web services
- PIN validation
- LDAP integration
- Extended audit trail and event archive
- CLIQ Connect+

To view available licensed features, see *Section 6.1.2 "Viewing Licence Status", page 93*.

For systems with **DCS Integration** enabled, CWM automatically checks for available licences in DCS every 24 hours and at CWM start-up. If there is no licence available in DCS or if DCS Integration is not enabled, licences must be installed manually. See *Section 6.1.1 "Installing Licences", page 93*.

Licence files are assigned a licence number in the order they are created. It is only possible to install a licence file which is created later than the currently installed file.

Licence expiry and email notification

A licence has a **Soft Expire Date** and a **Hard Expire Date**.

After the Soft Expire Date has passed, notification emails are sent to **Super Administrator** every Monday until the licence is renewed. For example, if the Soft Expire Date is a Tuesday, the first email is sent on the following Monday. In order to receive the emails, the adminstrators must have a registered email address. A warning message is also displayed in the CWM user interface. Contact your local CLIQ dealer to obtain a new licence.

If the Hard Expire Date has passed, CWM is locked from use on start-up. A warning message is displayed in the start page, and an email is sent to notify of the expiry date. Contact your local CLIQ dealer to obtain a new licence.

For more information about how to install licences, see *Section 6.1.1 "Installing Licences", page 93*.

When licences are controlled by external software (not by DCS), licence renewal is usually done on the Soft Expire Date. In this case, no notification email is sent.

9 Appendix

9.1 Terms and Acronyms

9.1.1 Terms

Actual State
Describes the state of the key authorisations actually programmed to keys and cylinders. See also **Defined State**.

Cylinder Access List
List of authorised keys, stored in cylinders.

Cylinder Group System
A Locking System pre-defined to support cylinder groups.

Cylinder Programming Job
Job that contains updates to a cylinder, which can be executed on the cylinder using a C-Key.

Cylinder Reprogramming
This operation clears a cylinder's memory content and then restores the cylinder access list, list of unauthorised keys, and other configurations, such as the time zone offset, from the database.

DCS Integration
A feature in CWM that enables automatic certificate generation for C-Keys and Remote PDs.

Defined State
Describes the state of key authorisations as defined in CWM. This is not necessarily the same as the Actual State, since some authorisations may not have been programmed to keys and cylinders yet. See also **Actual State**.

Element
CLIQ Keys and cylinders make up the CLIQ elements.

Explicit Access
Entry in the Dynamic Key Access List that is added explicitly for that key. See also **Implicit Access**.

Extension
An addition to a locking system that contains new keys, key groups, cylinders, cylinder groups, and Remote PDs.

Implicit Access
Entry in the Dynamic Key Access List that is added through access profiles associated with a person or directly with a key. See also **Explicit Access**.

Key Access List
List of authorised cylinders, stored in Dynamic Keys.

List of unauthorised keys
List of keys that have been blocked from access to a cylinder, after being reported lost.

Locking System
A system of cylinders and keys that are administrated together. In this manual the term is also associated to related PDs and the related information defined in CWM (such as electronic authorisations, employee and visitor data, administrator role definitions, system settings, and so on).

Object
Entities that can be administrated through CWM, such as keys, key groups, cylinders, cylinder groups, access profiles, Remote PDs, employees and visitors.

Remote System A locking system with remote functionality enabled.

Remote Update Job Job that contains updates to a key, which can be executed on the key by inserting it into a Remote PD.

USB On-The-Go A USB standard that allows USB devices to act as a host.

9.1.2 Acronyms

CSV	Comma Separated Values (a file format)
CWM	CLIQ Web Manager
DCS	Digital Content Server
GDPR	General Data Protection Regulation (an EU regulation that concerns processing of personal data)
PD	Programming Device
USB OTG	USB On-The-Go

9.2 CWM Symbols

User Keys

Mechanical Key

Normal Key

Quartz Key

CLIQ Connect Quartz Key

Dynamic Key

CLIQ Connect Dynamic Key

Normal Key Group

Dynamic Key Group

Pending remote update exists for the key

Pending remote update exists that exceeds key capacity

C-Keys

Master C-Key

Normal C-Key

CLIQ Connect Normal C-Key

Normal C-Key Group

Master C-Key Group

Programming job has not been sent to a C-Key

Programming job has been sent to a C-Key but not initiated yet

⚙	Some programming jobs have been sent to a C-Key while some have not
⚙	Programming job has been finished
⚙	Programming job has failed or been cancelled
⚙	Programming job has been replaced with a new job

Cylinders

Ⓔ	Electronic Cylinder
Ⓜ	Mechanical Cylinder
ⒺⓂ	Double Cylinder (This example: Electronic A-side and Mechanical B-side)
ⒺⒺ	Information concerns the A-side
ⒺⒺ	Information concerns the B-side
⚙	Cylinder programming job exists
⚙	Cylinder programming job needs approval
⚙	Cylinder programming job has been programmed to C-Key
⚙	Cylinder programming job has been finished
⚙	Cylinder programming job has failed or been cancelled
⚙	Cylinder programming job has been replaced with a new job

Authorisations

🔑	Explicit authorisation
👥	Authorisation from access profile

Remote PDs

▮	Wall PD
📱	CLIQ Mobile PD

9.3 Object Attributes

9.3.1 Employee Attribute

Identifier A unique code or ID used to distinguish this individual person from others in a system

Title A courtesy prefix used before the name, such as Mr., Ms., Dr.

First name The given name of the person.

Surname The family or last name of the person.

Domain The domain the person belongs to.

Organisation The company or institution the person is affiliated with.

Phone The person's contact telephone number.

Department The specific division or unit within the organisation the person works in.

Job The person’s job title or role within the organisation.

Email The person's email address.

Region A broader geographic area the person is located in (e.g., EMEA, APAC).

Language The primary language the person uses for communication.

Location General description of the place the person is based (can overlap with **City** or **State**).

Gmd text

Street The street address where the organisation or person is located.

Postcode The postal code for the address.

City The city where the person or organisation is located.

State The state, province, or region within a country.

Company address The full address of the person’s organisation or workplace.

9.3.2 Visitor Attribute

Identifier A unique code or ID used to distinguish this individual person from others in a system

Title A courtesy prefix used before the name, such as Mr., Ms., Dr.

First name The given name of the person.

Surname The family or last name of the person.

Domain The domain the person belongs to.

Organisation The company or institution the person is affiliated with.

Phone The person's contact telephone number.

Department The specific division or unit within the organisation the person works in.

Job The person’s job title or role within the organisation.

Email The person's email address.

Region A broader geographic area the person is located in (e.g., EMEA, APAC).

Language The primary language the person uses for communication.

Location General description of the place the person is based (can overlap with **City** or **State**).

Street The street address where the organisation or person is located.

Postcode The postal code for the address.

City The city where the person or organisation is located.

State The state, province, or region within a country.

Company address The full address of the person's organisation or workplace.

9.3.3 Key Attributes

Name Name of the key.

Key holder The person the key is currently handed out to.

Marking The key marking.

Second marking Alternative marking (not always used).

Key cutting The mechanical cutting of the key.

Group The key group the key belongs to.

Type The key type. For more information, see *Section 7.2.3 "User Keys", page 145*.

Firmware The firmware version.

Generation The key generation.

Status The key status (**In stock**, **Handed out**, **Lost** or **Broken**).

Line number Not used.

Last remote update Date and time of the last update through a Remote PD.

Access list size Used entries / Maximum entries in the Key Access List.

Time zone offset support Show whether the time zone offset support functionality is supported.

Tags Tags defined for the key.

External Links URLs associated with the key.

9.3.4 C-Key Attributes

Name Name of the C-Key.

Key holder The employee the C-Key is currently handed out to.

Marking The C-Key marking.

Second marking Alternative marking (not always used).

Group The key group the C-Key belongs to.

Type The C-Key type. For more information, see *Section 7.2.4 "C-Keys", page 145*.

Firmware The firmware version.

Generation The C-Key generation.

Remote support

Cylinder reprogramming Whether the C-Key has the right to execute Cylinder Reprogramming Jobs.

Cylinder group programming Whether the C-Key can execute Cylinder Programming Jobs that change a cylinder's cylinder group.

Cylinder firmware upgrade Whether the C-Key can upgrader the cylinder firmware or not (in development).

Status The C-Key status (**In stock**, **Handed out**, **Lost** or **Broken**).

Blocked Whether the C-Key is blocked from all access.

Validity settings C-Key validity setting.

Certificate enrolment Whether certificate enrolment is allowed.

Roles Which roles that are associated with the C-Key.

9.3.5 Cylinder Attributes

Name Name of the cylinder.

Marking The cylinder marking.

Status The cylinder status (**In stock**, **Installed** or **Broken**).

Location The location of the cylinder.

Base time zone The time zone at the cylinder location.

Cylinder model The cylinder model.

Length The physical length of the cylinder. For double cylinders, the length is represented by one number for each side. For a cylinder with a blind or a knob, the length is represented by one number for the cylinder length and one number for the blind/knob side length.

Line number Not used.

Locked by The C-Key to which pending cylinder programming jobs are loaded. While a cylinder programming job is loaded to a C-Key, the settings for that cylinder are locked from editing in CWM.

Cylinder side **A** or **B** (for double cylinders)

Type **E** (Electronic) or **M** (Mechanical).

Group The cylinder group to which the cylinder belongs.

Firmware The firmware version of the cylinder.

Time zone offset The offset of the cylinder's time zone, compared to the base time zone.

Domain The domain to which the cylinder belongs.

Tags Tags defined for the cylinder.

External Links URLs associated with the cylinder.

9.3.6 Remote PD Attributes

Name Name of the Remote PD.

Marking The Remote PD marking.

Type **Mobile PD** or **Wall PD**.

Generation The Wall PD generation.

MAC address The physical address of the Remote PD.

GR Group ID (for internal use only).

UID Unique ID (for internal use only).

Firmware Firmware version.

Boot loader (Generation 1 only) Boot loader firmware version.

Status Inventory status (**In stock**, **Installed**, **Handed out** or **Lost**).

Operational status (**Broken**).

Connection status **Offline** or **Online**.

Last connection Mobile PD: The time and date when the Mobile PD was last online.

Last known IP address The IP address from which Remote PD was online last time.

Tags Tags defined for the Remote PD.

External Links URLs associated with the Remote PD.

9.4 Permissions

For each permission, **None**, **List**, **View** or **Full** can be selected. **View** automatically includes **List**, and **Full** automatically includes **View** and **List**.

If there are dependencies between permissions, these are listed in the **Dependencies** column. For example, to be able to grant permissions for Key Authorisations, View permission for Keys and List permission for Cylinders is required.

Permission	**None**	**List** **Elements are listed**	**View** **Details for listed elements can be accessed**	**Full** **Details for listed elements can be accessed and manipulated**	**Dependencies**
Access profiles Controls administration of access profiles (create, delete, edit)		❌	Can view access profile details.	Can create new access profiles and edit existing ones, except for the access list which is controlled by the access profile authorisation permission.	
Access profile: Authorisation Controls setting authorisations for an access profile		❌	Can view authorisations in access profile.	Can add or remove authorisations in access profile.	Requires View permission for **Access profile**.
Approvals		**Jobs for approval** menu option available. Can view a list of audit trail requests for approval.	❌	Can approve audit trail requests. Approver role only and cannot be edited.	Only applicable if approval setting is activated during initial installation.
Audit trail			Audit trail tab is visible in key view and cylinder view.	Can request audit trails for cylinders and keys via the audit trail tab.	
Audit Trail: Automatic		❌	Permission to view automatic audit trails retrieval status for C-Keys.	Permission to view automatic audit trails retrieval status for C-Keys.	Requires at least View permission for **C-key**.
C-key	❌	❌	Can view C-Key details.	Can edit C-Key details and hand out C-Keys.	
C-key: Hand in/Hand out		❌	❌	Can hand in and hand out C-Keys.	Requires List permission for **Key holder: Employee** and View permission for **C-key**.

Permission	**None**	**List** **Elements are listed**	**View** **Details for listed elements can be accessed**	**Full** **Details for listed elements can be accessed and manipulated**	**Dependencies**
Cylinder		Selectable when **Cylinder: Authorisation** is None.	Can view cylinder details.	Can edit cylinder details and change cylinder status.	
Cylinder: Authorisation			Can view authorisations for a cylinder.	Can edit authorisations for a cylinder and request cylinder reprogramming.	Requires View permission for **Cylinder** and List permission for **Key**.
Cylinder: Programming		❌	❌	Can send programming jobs to C-Keys.	Requires List permission for **Cylinder**.
Domain (No permission required to view domain memberships and domain authorisations for C-Keys.)		❌	❌	Can administrate domains (add, remove, edit), and change domain authorisations for C-Keys.	
Firmware		❌	❌	Can import firmware.	Firmware upgrade requires Full permission for **Remote PDs**.
Flexible revalidation (Can see revalidation intervals if flexible revalidation is enabled.)		❌	❌	Can edit revalidation intervals for access profiles and cylinder groups.	
Key	Selectable when **Cylinder: Authorisation** is None.	Can list keys indirectly.	**Keys** menu option available. Can view key details.	Can edit key details, inventory and operational status.	
Key: Authorisation		Selectable when **Key: Authorisation** is None.	Can view authorisations for a key.	Can edit authorisations for a key.	Requires View permission for **Key** and List permission for **Cylinder**.

Permission	**None**	**List** **Elements are listed**	**View** **Details for listed elements can be accessed**	**Full** **Details for listed elements can be accessed and manipulated**	**Dependencies**
Key: Hand in/Hand out		⊗	⊗	**Hand in key** and **Hand out key** menu options available. Can perform hand in and hand outs.	Requires List permissions for **Key holder: Employee**, **Key holder: Visitor**, **Key** and **Cylinder** and Full permissions for **Key: Authorisation**.
Key: Schedule	⊗	⊗		Can edit schedule for a key, configure schedule in bulk for a key group, and set schedule while handing out the key.	Requires Full permission for **Template: Apply schedule by template** and View permission for **Key**.
Key: Update history		⊗	Can view key update history under the **Update history** tab.	⊗	Requires View permission for **Key**.
Key: Validity	⊗	⊗		Can edit bulk validity settings for keys, edit key validity settings, and set validity while handing out a key.	Requires View permission for **Key**.
Key holder: Deactivate		⊗	⊗	Can deactivate persons as well as search for and activate deactivated persons.	Requires Full permission for **Key holder: Employee** and **Key holder: Visitor**
Key holder: Employee	⊗	⊗	⊗	Can edit employee details.	
Key holder: Employee import		⊗	⊗	Can import employee data.	Requires Full permission for **Key holder: Employee**.
Key holder: Visitor	⊗	⊗	⊗	Can edit visitor details.	

Permission	**None**	**List** **Elements are listed**	**View** **Details for listed elements can be accessed**	**Full** **Details for listed elements can be accessed and manipulated**	**Dependencies**
LDAP integration		❌	Can view **LDAP Integration** settings in the system settings page.	Can edit **LDAP Integration** settings in the system settings page.	Requires View permission for **System settings**.
Maintenance		❌	❌	Can lock and unlock the system.	
Remote PDs		Can list Remote PDs indirectly.	**Remote PDs** menu option available. Can view Remote PD details.	Can edit Remote PD settings, upgrade Remote PD firmware and switch a Wall PD to key updater mode to use for key firmware upgrade.	
Roles	❌		**Roles** menu option available. Can view list of roles and see details of a role.	Can administer roles (create, edit, delete) and assign roles to C-Keys.	
Statistics		❌	Can view system statistics.	❌	
System settings	❌	❌			
System status		❌	**System status** menu option available. Can view system status.	❌	Requires List permission for **Remote PDs**.
Template: Apply schedule by template	❌	❌	❌	Can apply schedule template for a key and apply schedule template while handing out the key.	Requires View permission for **Key**.
Template: Receipt			**Receipt templates** menu option available. Can print receipts and preview receipt templates.	Can create, edit and delete the receipt templates	
Template: Schedule	❌		Can view schedule templates.	Can edit schedule templates.	
Temporary access group		❌	Can view temporary access groups.	Can edit temporary access groups.	

9.5 Remote PD Indications

9.5.1 Wall PD (Generation 1) and Mobile PD Indications

LED Indications		Buzzer	Interpretation
CLIQ Solid white			**Power On and Online**
CLIQ Fast white blinking			**Wall PD: Acquiring IP Address** **Mobile PD: Initialising Bluetooth or USB Connection**
CLIQ Slow white blinking			**Connecting to Remote Server during Startup Sequence**
	⬇ Solid	1 long beep	**Offline Update Finished OK**
CLIQ Solid red			**Mobile PD Battery Low**
CLIQ One red blink	✗ One blink		**Mobile PD Battery Critical Low**
🔑 Solid			**Key Battery Low**
⇆ Blinking			**Connecting during Remote Update**
⇆ Solid			**Connected during Remote Update**
⬇ Solid			**Firmware Upgrade Finished**
		1 beep	**Operation Finished OK** **Remote PD Settings Updated**
⬇ Blinking			**Downloading and Processing**
✉ Solid		1 beep	**Email Sent**
✗ Solid		3 beeps	**Operation finished with error**

For operations involving a key, beeps are repeated every three seconds until the key is removed.

9.5.2 Wall PD (Generation 2) Indications

LED Indications		Buzzer	Interpretation
✺ ● ●	Left: Blue pulse Middle: Off Right: Off		**Checking 802.1x Settings**
● ✺ ●	Left: Solid Blue Middle: Blue pulse Right: Off		**Acquiring IP Address**
● ● ✺	Left: Solid Blue Middle: Solid Blue Right: Blue pulse		**Establishing Server Connection**
● ○ ●	Left: Off Middle: Solid White Right: Off		**Connected and Ready to Use**
● ☼ ●	Left: Off Middle: White pulse Right: Off		**Lost Connection**
☼ ☼ ☼ →	LEDs start flashing white from the left		**Key Update is in Progress**
✺ ✺ ✺ →	LEDs start flashing blue from the left		**Firmware or a Parameter Update is in Progress**
✓	Green check mark	2 increasing beeps	**Operation Finished OK**
✗	Red cross	2 decreasing beeps	**Operation finished with error For operations**
🔋	Red battery		**Key Battery Low**

9.6 Battery Level Indications

The battery level of the currently scanned key in the right slot is indicated with the following symbols.

Battery Level Indication	Interpretation
🔋	**Battery level excellent**
🔋	**Battery level good**

Battery Level Indication	Interpretation
🪫	**Battery level low**
🪫	**Battery level critical**

9.7 Firmware Dependent Functionality

Table 51 "Firmware Requirements", page 192 lists CWM features and the lowest firmware version required for PDs, keys and cylinders.

Table 6. Firmware Requirements

Feature	Lowest supported FW	
Automatic audit trail retrieval	Key and C-Key	12.7.0
C-Key FW upgrade	Wall PD and CLIQ Mobile PD	6.3
	C-Key	12.0.0
CLIQ Connect Mobile PD compatibility	Key	12.3
Cylinder group support	Key	6.3.1
	Cylinder	5.3.1
Flexible revalidation	Key	6.3.1
Key firmware information update via remote PD	Key	12.3
Offline update	Key	6.3.1
PIN Validation	Key	16.0.0
Remote PD Plug & Play	Wall PD and CLIQ Mobile PD	6.2.1
Remote PD Proxy support	Wall PD and CLIQ Mobile PD	6.2.1
Remote C-Key update	C-Key	12.0.0
Remote support	Key	3.0
	C-Key	12.0.0
Revalidation	Key	3.0
Schedule type - Basic	Key	Only 1.x ,3.x, 5.x
Schedule type - Multiple Time Window	Key	2.x ,4.x, 6.x, 10 or higher
Time Zone Offset	Key, C-Key and Cylinder	10.0.0
User key FW upgrade (generation 2)	Key	10.1

To view the firmware version of a key, view the detailed information. See *Section 4.2.1 "Searching for User Keys", page 33* or *Section 4.2.2 "Scanning a User Key", page 34*.

To view the firmware version of a Wall PD, view the detailed information. See *Section 6.5.2 "Searching for Remote PDs", page 99*.

To view the firmware version of a CLIQ Mobile PD, view the detailed information. See *Section 6.5.2 "Searching for Remote PDs", page 99*.

9.8 Client PC Requirements

Product	Requirement
Operating System	• Windows 10 (64-bit) • Windows 11
Internet Browser	• Firefox ESR 138 or later • Firefox 138 or later • Google Chrome 136 or later • Microsoft Edge 136 or later *Support for Internet Explorer is being discontinued due to end-of-life support for this browser.
PDF Reader	Any (Tested with Adobe Reader)

9.9 Employee Import File Format

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**.

HINT!

To make sure that the CSV file has the correct encoding **Windows Notepad** can be used. Open the CSV file in Notepad, select **File » Save As...**, select **UTF-8** encoding and click **Save**.

File Size

The maximum file size allowed to be imported to CWM is 7.0MB.

File Content

The required delimiter is either comma (,) or semicolon (;). The system setting **CSV delimiter** does not affect importing.

The first row is a header that represents all the comma-separated field names (a description of the fields). The header is validated and language specific, that is, the text in the header has to be according to the definitions of the selected language.

HINT!

A correct header can be fetched by exporting employees to a CSV file and then remove all information except the first row. When exporting employees, an extra field, **Tags**, is added after the other fields. This field can be kept in the file but will be ignored during import.

See *Section 4.1.12 "Exporting Employee or Visitor Information", page 33*.

Each of the following rows represents an employee. The field values are separated with the delimiter and the order of the fields must correspond to the header. If a field must include the delimiter character (comma or semicolon), the whole field data must be placed within quotation marks ("), for example `"11 Wall St, New York, NY"`.

NOTE!
If a field is empty, the delimiter must still be present.

The fields and the requirements are listed in *Table 53 "CSV File Structure", page 194*.

Table 7. CSV File Structure

Field No	Name	Mandatory	No of Characters
1	Identifier		1-50
2	Title		0-100
3	First name	✓	1-49
4	Last name	✓	1-49
5	Domain		0-100
6	Email		0-100
7	Phone		0-100
8	Organisation		0-100
9	Department		0-100
10	Street		0-100
11	Postcode		0-100
12	Language		0-100
13	Region		0-100
14	Job		0-100
15	City		0-100
16	State		0-100
17	Country		0-100
18	Company address		0-100
19	Location		0-100
20	Mobile phone		0-100
21	Gmd text		0-100

Identifier must be unique. For employees in the file that have identical **Identifier** to an employee already in the system, the information in the system is replaced by the information in the file. However, if an employee is added in CWM and then imported without the **Identifier** being specified in the file, the result will be duplicate entries of that employee.

NOTE!
Employees in the CSV file with the same identifier as a deactivated employee in CWM are ignored and not imported.

Email must be specified in a correct email format.

NOTE!
There are limitations in editing or deleting the email address for an employee or visitor with the CLIQ Connect+ user status activated. For more information, see *Section 4.1.6.1 "Important information about Editing or Deleting Email Address", page 29*.

Maximum number of employees in one file is 10 000.

Example File

```
Identifier,Title,First name,Last_name,Domain,Email,Phone,Organi
sation,Department,Street,Postcode,Language,Region,Job,City,Stat
e,Country,Company address,Location,Mobile phone,Gmd text

P0,Professor,George,Whitmore,Stockholm,George.Whitmore@assaablo
y.com,37192537299732677730,ASSA ABLOY,Shared Technologies,,,Swed
ish,,System Developer,Stockholm,,Sweden,"Formansvagen 11, 117 4
3 Stockholm",,070-69721357838660652822,GmdText
```

9.10 ASSA ABLOY Operating Company Code

Code	Operating Company
0	No company specified
1	ASSA ABLOY Opening Solutions Sweden (ASSA)
2	ABLOY
3	IKON
4	VACHETTE
6	MEDECO
7	SARGENT
8	ARROW
9	LAPERCHE
10	ASSA ABLOY Opening Solutions Norway (TRIOVING)
11	ASSA ABLOY Opening Solutions Denmark (RUKO)
12	MUL-T-LOCK
13	ASSA US
14	ASSA UK
15	ASSA BALT
16	MEDECO CANADA
17	FAB
18	AA Japan
19	TESA
20	AA New Zealand
21	AA Australia
22	AA Singapole
23	AA Hong Kong
24	AA China

Code	Operating Company
25	AA India
26	KESO
27	Corbin Russwin
28	ABLOY UK
29	ABLOY US

9.11 Software Support Information

9.11.1 Contacting Software Support

If you have problems using CLIQ Web Manager or any of the hardware devices like keys, cylinders or programming devices, please contact your local CLIQ dealer. Please have your master key system number and the Web Manager version in use ready for all service related communication. When writing emails please always add the master key system number to the header of the email.

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

Subject to technical changes. Program version: V 2025.1. Document number: PB00023 00017 0EN. Language: en-GB. Published: 2025-05-22.