CLIQ Web Manager

User Manual

V 5.0

The global leader in
door opening solutions

Program version: 5.0
Document number: ST-002716
Date: 2014-11-27
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
Section 1 *“Overview”*, page 9	✓	✓	A brief introduction to CLIQ and this manual.
Section 3 *“Getting Started with CWM”*, page 12	✓	✓	Describes how to get started when working with CWM for the first time.
Section 4 *“Working with CWM”*, page 22	✓	✓	Describes how to execute all relevant tasks for administrators when working with a locking system.
Section 2 *“Setting Up CWM Clients”*, page 11	✓	✓	Describes how to set up a CWM client.
Section 5 *“Setting Up Locking Systems”*, page 70		✓	Describes how to set up a new locking system.
Section 6 *“Configuring Locking Systems”*, page 72		✓	Describes how to configure various aspects of a locking system.
Section 7 *“CLIQ Hardware”*, page 101	✓	✓	Describes the CLIQ architecture and components.
Section 8 *“CLIQ Concepts and Features”*, page 107	✓	✓	Describes how authorisation works, and the concepts of CWM features. Some concepts are very technical and intended for Super Administrators only.
Section 9 *“Appendix”*, page 127	✓	✓	Contains reference information.

Terminology

For a definition of terms and acronyms used in this manual, see Section 9.1.1 *“Terms”*, page 127 and Section 9.1.2 *“Acronyms”*, page 128.

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

2 Setting Up CWM Clients

2.1 CWM Client Setup Overview

1) Install the Local PD.

   See Section 2.2 *“Installing Local PDs”*, page 11.

2) Install Java.

   See Section 2.3 *“Installing Java”*, page 11.

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.

4) If the drivers are not installed automatically, navigate to http://www.ftdichip.com/Drivers/D2XX.htm, and download the applicable driver for the operating system in the client PC.

   Read the documentation on the web page for more information on how to install the driver.

2.3 Installing Java

1) Ensure that the Windows user account currently logged in has Administrator access rights.

2) Download and install the latest Java JRE from http://www.java.com/download.

   NOTE!
   It is recommended to install the latest Java JRE even if a supported version is already installed.

   For information about supported Java versions, see Section 9.8 *“Client PC Requirements”*, page 138.

3) Restart the computer.

Verify the Java JRE installation and get help with troubleshooting at http://www.java.com/verify.

3 Getting Started with CWM

3.1 Getting Started with CWM Overview

1) Install the C-Key certificate.

   See Section 3.2.1 *“C-Key Certificate Installation and Renewal Overview”*, page 12.

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 20.

3.2 Installing and Renewing C-Key Certificates

3.2.1 C-Key Certificate Installation and Renewal Overview

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

The procedure to install a certificate depends on the Internet browser and whether **DCS Integration** is enabled or not.

If DCS Integration is enabled, the C-Key holder has received an e-mail with a link to the Enrolment Application.

Certificate Installation with DCS Integration

- Internet Explorer: Section 3.2.2 *“Installing C-Key Certificate with DCS (Internet Explorer)”*, page 13
- Firefox: Section 3.2.3 *“Installing C-Key Certificate with DCS (Firefox)”*, page 14

With DCS Integration, the C-Key certificate can be generated directly in the Internet browser. There is no need to obtain the certificate separately.

Certificate Installation without DCS Integration

- Internet Explorer: Section 3.2.4 *“Installing C-Key Certificate Manually (Internet Explorer)”*, page 15
- Firefox: Section 3.2.5 *“Installing C-Key Certificate Manually (Firefox)”*, page 15

To install the C-Key certificate without DCS Integration, a certificate file must be available.

Certificate Renewal

See Section 3.2.6 *“Renewing C-Key Certificate”*, page 16

3.2.2 Installing C-Key Certificate with DCS (Internet Explorer)

Prerequisites:

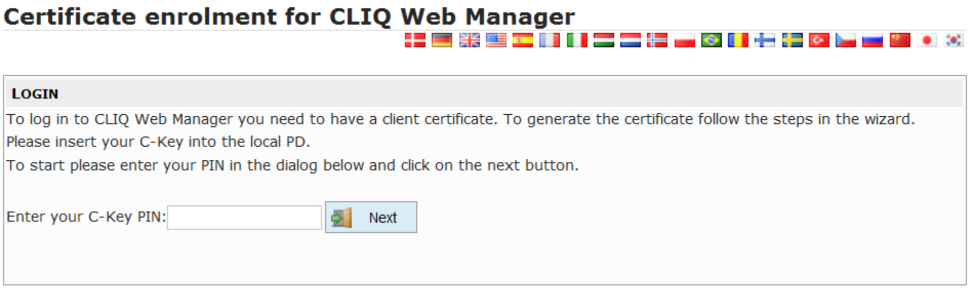
- The Local PD is installed.
- The C-Key is handed out in CWM.

  This has generated an e-mail with a link to the Enrolment Application sent to the employee's e-mail address.
- 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 6.11.3 *“Editing C-Key Information”*, page 90.
- The following is available:
  - The C-Key and the C-Key PIN code.
  - The e-mail with the link to the Enrolment Application.

1) Insert the C-Key in the left slot of the Local PD.

2) Click in the link in the e-mail or open Internet Explorer and enter the link into the navigation bar.



Certificate enrolment for CLIQ Web Manager

LOGIN

To log in to CLIQ Web Manager you need to have a client certificate. To generate the certificate follow the steps in the wizard.
Please insert your C-Key into the local PD.
To start please enter your PIN in the dialog below and click on the next button.

Enter your C-Key PIN:

3) Enter the C-Key PIN code and click **Next**.

   The C-key is authenticated and a One Time Password (OTP) is sent to the e-mail address of the C-Key holder. This might take a while.

4) Enter the one time password included in the e-mail and click **Next**.

5) Click **Generate certificate**.

   Internet Explorer displays a warning that a certificate operation is being performed.

6) Click **Yes** to allow the certificate operation.

7) If a warning is displayed again, click **Yes** once more.

   The certificate in now installed in Internet Explorer and a link to CWM is displayed.

> **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.)

8) Click on the link to open CWM.

3.2.3 Installing C-Key Certificate with DCS (Firefox)

Prerequisites:

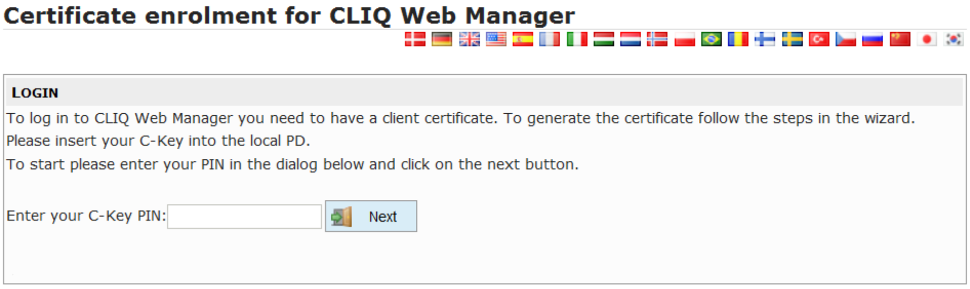
- The Local PD is installed.
- The C-Key is handed out in CWM.

  This has generated an e-mail with a link to the Enrolment Application sent to the employee's e-mail address.
- 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 6.11.3 *"Editing C-Key Information"*, page 90.
- The following is available:
  - The C-Key and the C-Key PIN code.
  - The e-mail with the link to the Enrolment Application.

1) Insert the C-Key in the left slot of the Local PD.

2) Click in the link in the e-mail or open Firefox and enter the link into the navigation bar.



Certificate enrolment for CLIQ Web Manager

LOGIN

To log in to CLIQ Web Manager you need to have a client certificate. To generate the certificate follow the steps in the wizard.

Please insert your C-Key into the local PD.

To start please enter your PIN in the dialog below and click on the next button.

Enter your C-Key PIN:

3) Enter the C-Key PIN code and click **Next**.

   The C-key is authenticated and a One Time Password (OTP) is sent to the e-mail address of the C-Key holder. This might take a while.

4) Enter the one time password included in the e-mail and click **Next**.

5) Select **High Grade** certificate strength from the drop-down list.

6) Click **Generate certificate**.

7) If a **Choose Token Dialog** is displayed, select **Software Security Device** from the drop-down list and click **OK**.

8) A message that the certificate has been installed is displayed. Continue this procedure to the end to finish the installation. Click **OK**.

9) If a **User Identification Request** is displayed, select the newly created certificate and click **OK**.

   The certificate is named after the Locking System and the key.

10) From the **Tools** menu, select **Options**.

11) Click **Advanced**.

12) Select the **Certificates** tab.

13) Click **View Certificates**.

14) Select the **Your Certificates** tab.

15) Select the newly created certificate.

    It is named after the locking system and the key.

16) Click **Backup**.

17) Select folder, enter a file name and click **Save**.

    The file type must be `.p12`.

18) Enter a **Certificate backup password** and click **OK**.

19) Click **OK** and close the Firefox.

20) From **Windows Start Menu**, click **Control Panel**.

21) Click Java.

22) Select the **Security** tab.

23) Click **Manage Certificates...**

24) Select Certificate type **Client Authentication**.

25) Click **Import**.

26) Select the `.p12` certificate saved in *Step 17* and click **Open**.

27) Enter the password for the certificate and click **OK**.

28) Enter the password for the private keystore and click **OK**.

    By default, the password is `changeme`. It is strongly recommended to change this password.

29) Close the Java Control Panel.

The certificate is now installed.

3.2.4 Installing C-Key Certificate Manually (Internet Explorer)

Installing the certificate requires:

- A `.p12` file for the C-Key along with a password.

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

   The **Certificate Import Wizard** is displayed.

2) Click **Next**.

3) Click **Next**.

4) Enter the password for the certificate and then click **Next**.

5) Select **Automatically select the certificate store based on the type of certificate** and click **Next**.

6) Click **Finish**.

7) Click **OK**.

8) Restart Internet Explorer.

> **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.)

3.2.5 Installing C-Key Certificate Manually (Firefox)

Installing the certificate requires:

- A .p12 file for the C-Key along with a password.

1) Open Firefox.
2) From the **Tools** menu, select **Options**.
3) Click **Advanced**.
4) Select the **Certificates** tab.
5) Click **View Certificates**.
6) Select the **Your Certificates** tab.
7) Click **Import**.
8) Select the .p12 certificate file for the C-Key and then click **Open**.
9) Click **OK**.
10) Enter the password for the certificate and click **OK**.
11) Click **OK** and close Firefox.
12) From **Windows Start Menu**, click **Control Panel**.
13) Click **Java**.
14) Select the **Security** tab.
15) Click **Manage Certificates...**
16) Select Certificate type **Client Authentication**.
17) Click **Import**.
18) Select the .p12 certificate file for the C-Key and then click **Open**.
19) Enter the password for the certificate and click **OK**.
20) Enter the password for the private keystore and click **OK**.

    By default, the password is `changeme`. It is strongly recommended to change this password.

21) Close the Java Control Panel.

The certificate is now installed.

3.2.6 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.

If DCS is enabled, the warning message contains the link to the enrolment application, which is used for renewing the certificate. In addition, an e-mail with the link is sent to the C-Key holder.

1) If DCS Integration is enabled:
    a) Navigate to the Enrolment Application.

       The certificate expiration warning message and the e-mail contains the link to the Enrolment Application.

    b) Select the certificate for the C-Key, that is the certificate that is about to expire.
    c) Continue the enrolment procedure:

- For Internet Explorer, follow the instructions in Section 3.2.2 *"Installing C-Key Certificate with DCS (Internet Explorer)"*, page 13

  Start from *Step 3*.
- For Firefox, follow the instructions in Section 3.2.3 *"Installing C-Key Certificate with DCS (Firefox)"*, page 14.

  Start from *Step 3*.

d) A new certificate that can be used from now on is generated and installed. The old certificate will also be available and can be used until it expires.

2) If DCS Integration is **not** enabled:

a) For Internet Explorer, see Section 3.2.4 *"Installing C-Key Certificate Manually (Internet Explorer)"*, page 15.

b) For Firefox, see Section 3.2.5 *"Installing C-Key Certificate Manually (Firefox)"*, page 15.

3.3 Logging In

Prerequisites:

- The Local PD is installed. See Section 2.2 *"Installing Local PDs"*, page 11.
- A supported Internet browser is used. See Section 9.8 *"Client PC Requirements"*, page 138.
- A supported Java version is installed. See Section 2.3 *"Installing Java"*, page 11.
- A C-Key with a PIN code is available. The C-Key must also be handed out to an employee in CWM.
- A valid certificate for the C-Key is installed. See Section 3.2.1 *"C-Key Certificate Installation and Renewal Overview"*, page 12.
- A correct 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 in the Local PD.

4) If prompted, select the **COM port of the PD** (USB Serial Port) where the Local PD is connected, and click **OK**.

   If the port is unknown, try the ports one by one, starting from the highest number. If the selected port is incorrect, the prompt appears again.

   If the prompt disappears before a COM port is selected, refresh the page by pressing **F5** on the keyboard.

5) Click **Login**.

HINT!

- If it takes more than about 10 seconds before the **Login** button becomes enabled, check the Java settings for certificate revocation. The settings are available in **Start Menu » Control Panel » Programs » Java » Advanced**.
  - Under **Check for certificate revocation using**, make sure **Certificate Revocation Lists (CRLs)** is selected.
  - Restart the Internet browser.
- If the **Login** button is continuously disabled, check the Java settings for temporary internet files. The settings are available in **Start Menu » Control Panel » Programs » Java » General » Temporary Internet Files » Settings...**.
  - Make sure that the checkbox **Keep temporary files on my computer.** is checked.
  - Remove old temporary files by clicking **Delete files...** and select **Cached Applications and applets**.

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

7) Click **OK**.

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:

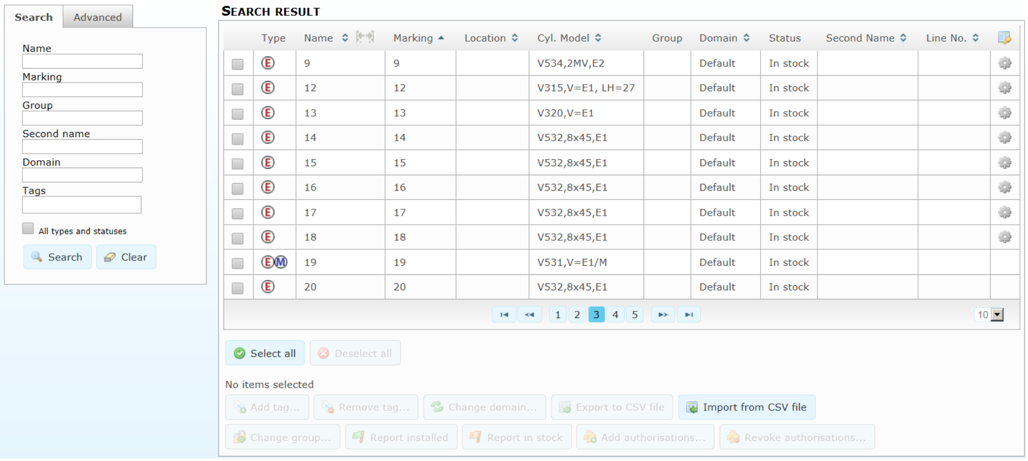
Work	Contains the functions that are most commonly used in daily work.
System Info	Contains functions to administer access rights, employees and visitor information, keys, cylinders and Remote PDs.
Administration	Contains functions to set up and configure the locking system.
Settings	Contains the personal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

3.5.2 Searching for Objects

To search for objects, like cylinders or keys, first select the corresponding menu option.

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.
□	Ⓔ	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		
□	ⒺⓂ	19	19		V531,V=E1/M		Default	In stock		
□	Ⓔ	20	20		V532,8x45,E1		Default	In stock		

No items selected

How to 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 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:

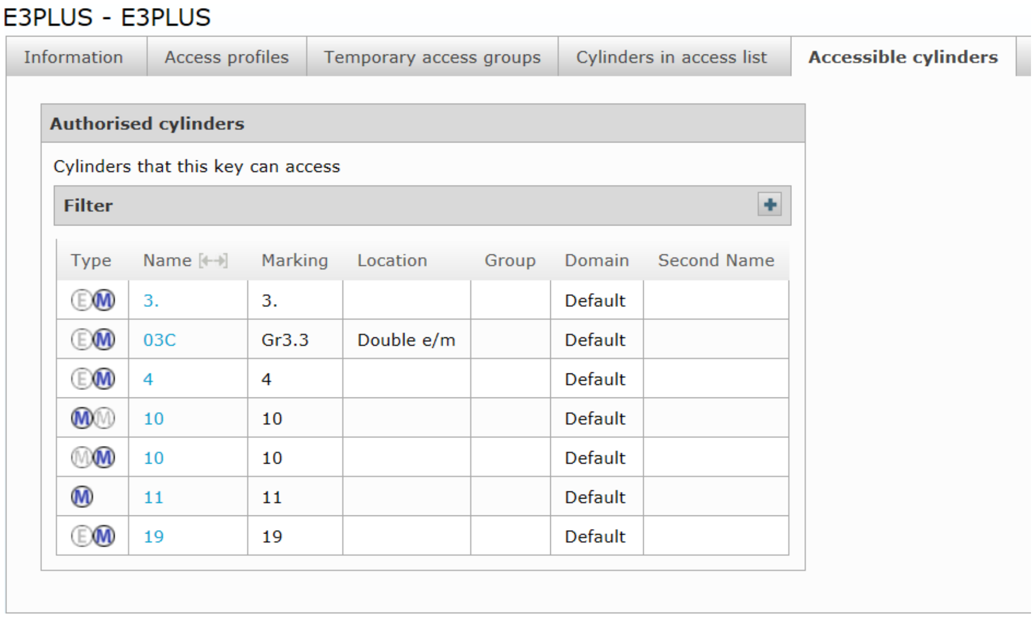
1) Select several individual objects in the leftmost column from one or more search result pages.

   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 **FILTER** banner is visible. See the example below.



E3PLUS - E3PLUS

Authorised cylinders

Cylinders that this key can access

Filter +

Type	Name	Marking	Location	Group	Domain	Second Name
ⒺⓂ	3.	3.			Default	
ⒺⓂ	03C	Gr3.3	Double e/m		Default	
ⒺⓂ	4	4			Default	
ⓂⓂ	10	10			Default	
ⓂⓂ	10	10			Default	
Ⓜ	11	11			Default	
ⒺⓂ	19	19			Default	

Clicking the + symbol opens a box of criteria the list can be filtered by.

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 22

Keys
Handing out keys: Section 4.2.8 *“Handing Out Keys”*, page 29

Receiving keys (Hand-In): Section 4.2.9 *“Receiving Keys (Hand-In)”*, page 30

When keys get lost: Section 4.2.10 *“Reporting Keys Lost Or Broken”*, page 31

Authorisations
Viewing keys that can access a cylinder: Section 4.8.3 *“Viewing Keys With Access to Cylinder”*, page 54

Viewing cylinders where a key has access: Section 4.8.1 *“Viewing Accessible Cylinders for Keys”*, page 53

Changing authorisations on a key: Section 4.9.1 *“Configuring Authorisations in Keys”*, page 55

Changing authorisations on a cylinder: Section 4.9.2 *“Configuring Authorisations in Cylinders”*, page 56

Access Profiles
Associate a key or person with an access profile: Section 4.9.5 *“Selecting Employee or Visitor Access Profiles”*, page 60

Changing authorisations for an access profile: Section 4.9.4 *“Configuring Access Profile Authorisations”*, page 59

Audit Trails
Checking keys that accessed a cylinder: Section 4.11.2 *“Viewing Cylinder Audit Trails”*, page 67

Programming
Programming cylinders: Section 4.4.10.1 *“Programming Cylinders Overview”*, page 40

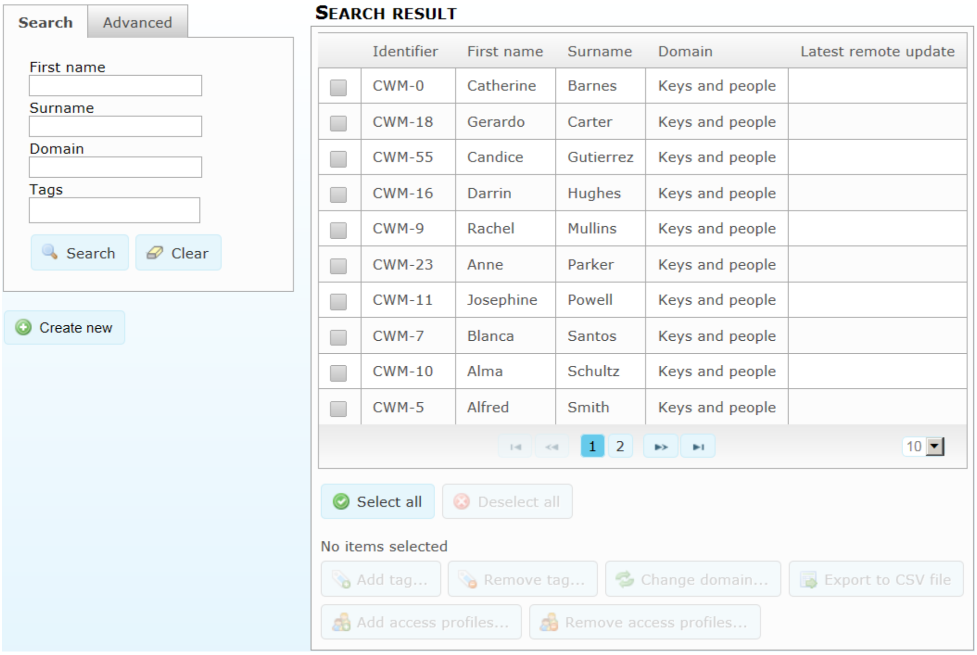
4 Working with CWM

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.



SEARCH RESULT

	Identifier	First name	Surname	Domain	Latest remote update
□	CWM-0	Catherine	Barnes	Keys and people	
□	CWM-18	Gerardo	Carter	Keys and people	
□	CWM-55	Candice	Gutierrez	Keys and people	
□	CWM-16	Darrin	Hughes	Keys and people	
□	CWM-9	Rachel	Mullins	Keys and people	
□	CWM-23	Anne	Parker	Keys and people	
□	CWM-11	Josephine	Powell	Keys and people	
□	CWM-7	Blanca	Santos	Keys and people	
□	CWM-10	Alma	Schultz	Keys and people	
□	CWM-5	Alfred	Smith	Keys and people	

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 employees or visitors.

3) Enter the search criteria.

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.

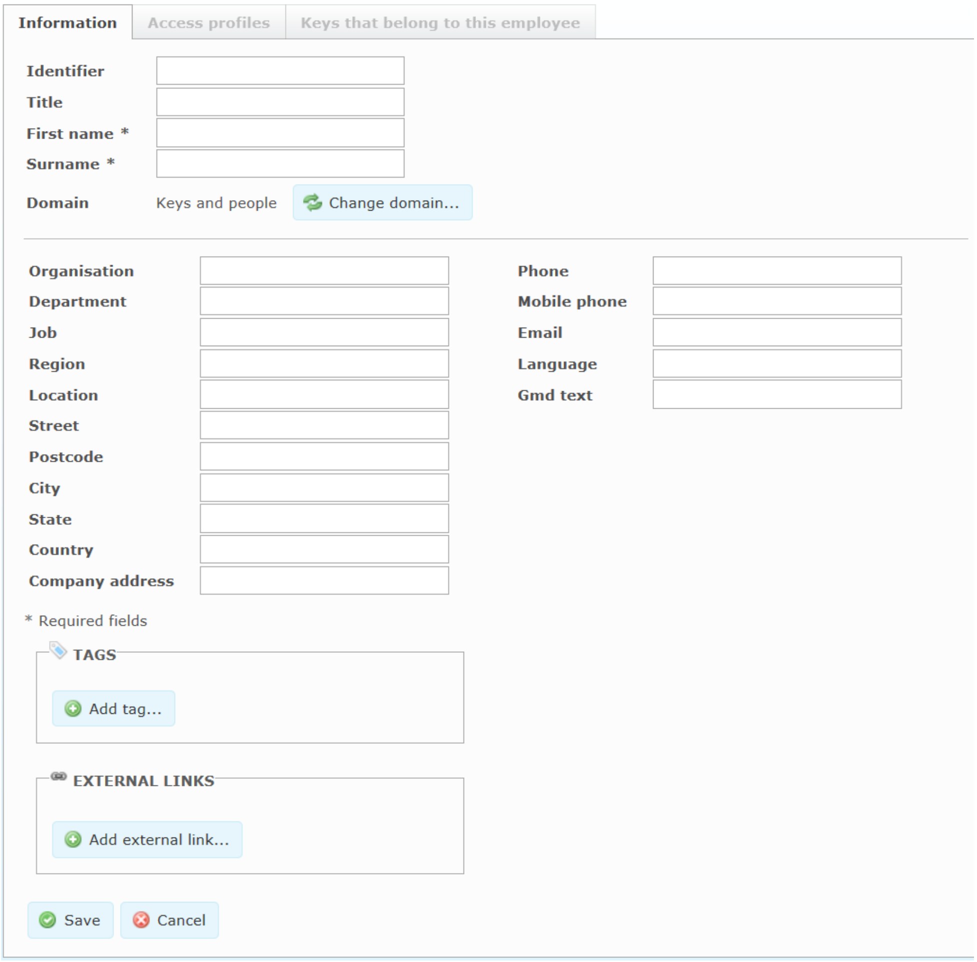
4) Click **Search**.

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

4.1.2 Adding Employees or Visitors

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

2) Click **Create New**.



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.

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 format yyyy-mm-dd:running number.

4) To add a tag, click **Add tag**. See also Section 4.1.5 *"Editing Employee or Visitor Tags"*, page 24.

5) To add an external link, click **Add external link**. See also Section 4.1.6 *"Editing Employee or Visitor External Links"*, page 24.

6) Click **Save**.

4.1.3 Deleting and 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**, see Section 6.4 *"Editing System Settings"*, page 73. When **Mark as deleted** is selected, the deleted employees or visitors can be restored if needed.

1) Find the employee or visitor to delete or restore.

To search for the employee or visitor and view the detailed information, see Section 4.1.1 *"Searching for Employees or Visitors"*, page 22.

2) To delete:

  a) In the detailed information view, click **Delete**.

     Employees or visitors with handed out keys cannot be deleted.

  b) Click **OK**.

3) To restore:

  a) Select the **Advanced** search tab.

  b) Click **Show deleted**.

  c) In the detailed information view, click **Restore**.

4.1.4 Editing Employee or Visitor Information

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 22.

2) Click **Edit**.

3) Update the fields.

4) To edit tags, see Section 4.1.5 *"Editing Employee or Visitor Tags"*, page 24.

5) To edit external links, see Section 4.1.6 *"Editing Employee or Visitor External Links"*, page 24.

6) Click **Save**.

4.1.5 Editing Employee or Visitor Tags

1) Find the employee or visitor.

   To search for the employee or visitor and display the detailed information view, see Section 4.1.1 *"Searching for Employees or Visitors"*, page 22.

2) Click **Edit**.

3) To add a tag:

  a) Click **Add tag**.

  b) Enter a name for the tag.

  c) Click **OK**.

  d) Click **Save**.

4) To remove a tag:

  a) Click the tag to be removed.

  b) Click **OK**.

  c) Click **Save**.

A tag can be simultaneously edited for several employees or visitors. Select the employees or visitors in the search result list and click **Add tags** or **Remove tags**.

See also Section 8.2.6 *"Tags"*, page 119.

4.1.6 Editing Employee or Visitor External Links

1) Find the employee or visitor. To search for the employee or visitor and display the detailed information view, see Section 4.1.1 *"Searching for Employees or Visitors"*, page 22.

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 only necessary to add the last part of the URL. See also Section 6.4 *"Editing System Settings"*, page 73.

   d) Click **OK**.

4) To remove an external link, click **Remove** on 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 121.

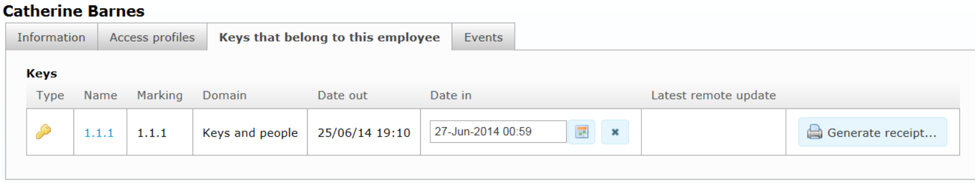
4.1.7 Viewing Employee or Visitor Keys

1) Find the employee or visitor.

   To search for the employee or visitor and display detailed information, see Section 4.1.1 *"Searching for Employees or Visitors"*, page 22.

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

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



Catherine Barnes

Keys

Type	Name	Marking	Domain	Date out	Date in	Latest remote update	
	1.1.1	1.1.1	Keys and people	25/06/14 19:10	27-Jun-2014 00:59		Generate receipt...

3) To change hand-in date for a key, edit the **Date in** field.

4) To generate a receipt of the hand out and hand in of the key, click **Generate Receipt...**.

5) To display the detailed information view of the key, click the key name.

4.1.8 Viewing Employee or Visitor Events

The Events tab is used for traceability of administrator operations in CWM, such as creation of an employee, associating access profiles, etc.

1) Find the employee or visitor.

   To search for the employee or visitor and display detailed information, see Section 4.1.1 *"Searching for Employees or Visitors"*, page 22.

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

   A list of employee or visitor events is displayed.

4.1.9 Exporting Employee Or Visitor Information

1) Search for the employees or visitors.

See Section 4.1.1 *“Searching for Employees or Visitors”*, page 22.

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

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 73.

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

4.2 Managing Keys

4.2.1 Scanning a Key

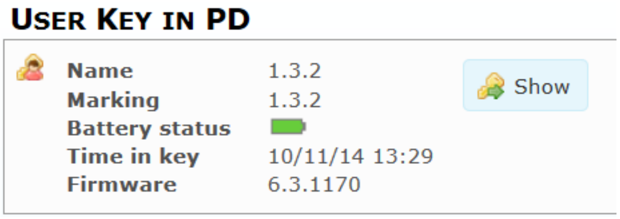
1) Insert the key into the right slot of the Local PD.

2) Select **System Info » Keys**.

A list of all keys is displayed.

3) Under **Programming Device**, click **Scan**.

Basic information about the key is displayed.



USER KEY IN PD

Name	1.3.2
Marking	1.3.2
Battery status	🟩
Time in key	10/11/14 13:29
Firmware	6.3.1170

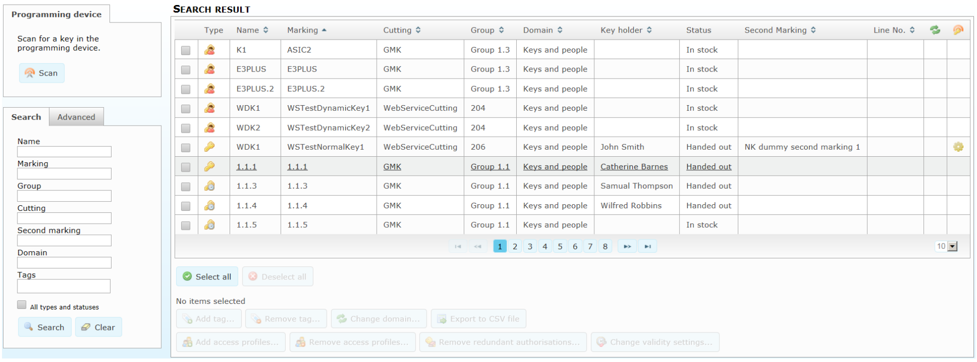
4) To view detailed information about the key , click **Show**.

For information about the key attributes, see Section 9.3.1 *“Key Attributes”*, page 129.

4.2.2 Searching for Keys

1) Select **System Info » Keys**.

A list of all keys is displayed.



Programming device

Scan for a key in the programming device.

Search | Advanced

Name:
Marking:
Group:
Cutting:
Second marking:
Domain:
Tags:
□ All types and statuses

SEARCH RESULT

	Type	Name	Marking	Cutting	Group	Domain	Key holder	Status	Second Marking	Line No.		
□		K1	ASIC2	GMK	Group 1.3	Keys and people		In stock				
□		E3PLUS	E3PLUS	GMK	Group 1.3	Keys and people		In stock				
□		E3PLUS.2	E3PLUS.2	GMK	Group 1.3	Keys and people		In stock				
□		WDK1	WSTestDynamicKey1	WebServiceCutting	204	Keys and people		In stock				
□		WDK2	WSTestDynamicKey2	WebServiceCutting	204	Keys and people		In stock				
□		WDK1	WSTestNormalKey1	WebServiceCutting	206	Keys and people	John Smith	Handed out	NK dummy second marking 1			⚙
□		1.1.1	1.1.1	GMK	Group 1.1	Keys and people	Catherine Barnes	Handed out				
□		1.1.3	1.1.3	GMK	Group 1.1	Keys and people	Samual Thompson	Handed out				
□		1.1.4	1.1.4	GMK	Group 1.1	Keys and people	Wilfred Robbins	Handed out				
□		1.1.5	1.1.5	GMK	Group 1.1	Keys and people		In stock				

No items selected

The following symbols are used:

🔑	Mechanical Key
👤	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, inventory status and operational status.

3) Enter the search criteria.

   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 key.

   For information about the key attributes, see Section 9.3.1 *"Key Attributes"*, page 129.

4.2.3 Editing Key Information

1) Find the key to edit.

   To search for the key and display the detailed information view, see Section 4.2.2 *"Searching for Keys"*, page 26

   To scan the key in the Local PD and display the detailed information view, see Section 4.2.1 *"Scanning a Key"*, page 26

2) Click **Edit**.

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

4) To add a tag, click **Add tag**. See also Section 4.2.4 *"Editing Key Tags"*, page 27

5) To add an external link, click **Add external link**. See also Section 4.2.5 *"Editing Key External Links"*, page 28

6) Click **Save**.

4.2.4 Editing Key Tags

1) Find the key to edit.

   To search for the key and display the detailed information view, see Section 4.2.2 *"Searching for Keys"*, page 26

   To scan the key in the Local PD and display the detailed information view, see Section 4.2.1 *"Scanning a Key"*, page 26

2) Click **Edit**.

   To add a tag:

   a) Click **Add tag**.

   b) Enter a name for the tag.

   c) Click **OK**.

    d) Click **Save**.

3) To remove a tag:

    a) Click the tag to be removed.

    b) Click **OK**.

    c) Click **Save**.

A tag can be edited for several keys simultaneously. Select the keys in the search result list and click **Add tags** or **Remove tags**.

See also Section 8.2.6 *"Tags"*, page 119.

4.2.5 Editing Key External Links

1) Find the key to edit.

    To search for the key and display the detailed information view, see Section 4.2.2 *"Searching for Keys"*, page 26

    To scan the key in the Local PD and display the detailed information view, see Section 4.2.1 *"Scanning a Key"*, page 26

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://).

    d) Click **OK**.

4) To remove an external link, click **Remove** on 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 121.

4.2.6 Viewing Key Update History

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

1) Find the key.

    To search for the key and display the detailed information view, see Section 4.2.2 *"Searching for Keys"*, page 26

    To scan the key in the Local PD and display the detailed information view, see Section 4.2.1 *"Scanning a Key"*, page 26

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

    A list with all key updates is displayed.

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

4.2.7 Viewing Key Events

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.

   To search for the key and display the detailed information view, see Section 4.2.2 *“Searching for Keys”*, page 26

   To scan the key in the Local PD and display the detailed information view, see Section 4.2.1 *“Scanning a Key”*, page 26

2) Select the **Events** tab.

   A list with all key events is displayed.

4.2.8 Handing Out Keys

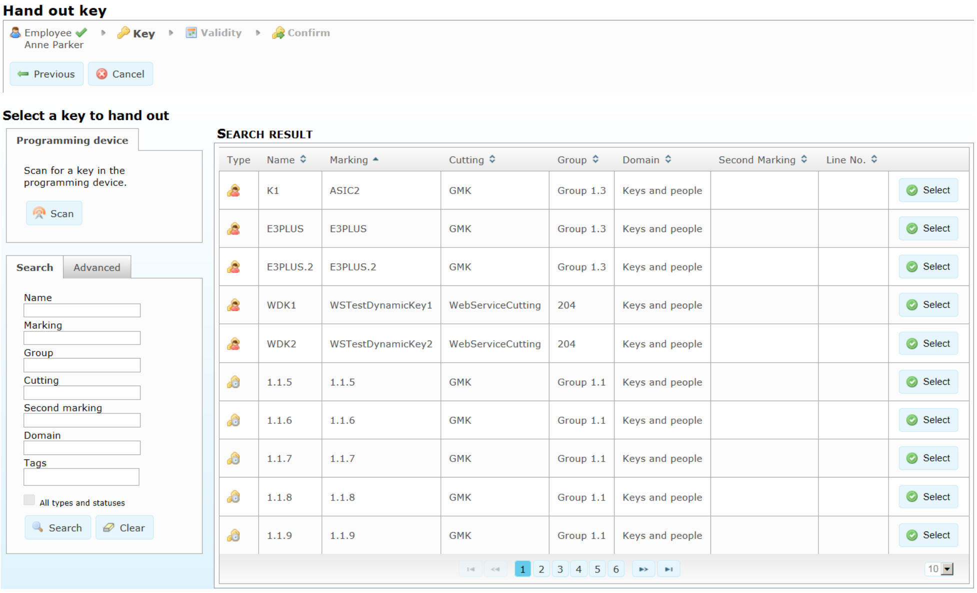
1) Select **Work » Hand out key » To employee** or **To visitor**.

   A list of all employees or visitors is displayed.

2) To search for a specific employee or visitor, see Section 4.1.1 *“Searching for Employees or Visitors”*, page 22.

3) Click **Select**.

   The key selection view is displayed.



SEARCH RESULT

Type	Name	Marking	Cutting	Group	Domain	Second Marking	Line No.	
	K1	ASIC2	GMK	Group 1.3	Keys and people			Select
	E3PLUS	E3PLUS	GMK	Group 1.3	Keys and people			Select
	E3PLUS.2	E3PLUS.2	GMK	Group 1.3	Keys and people			Select
	WDK1	WSTestDynamicKey1	WebServiceCutting	204	Keys and people			Select
	WDK2	WSTestDynamicKey2	WebServiceCutting	204	Keys and people			Select
	1.1.5	1.1.5	GMK	Group 1.1	Keys and people			Select
	1.1.6	1.1.6	GMK	Group 1.1	Keys and people			Select
	1.1.7	1.1.7	GMK	Group 1.1	Keys and people			Select
	1.1.8	1.1.8	GMK	Group 1.1	Keys and people			Select
	1.1.9	1.1.9	GMK	Group 1.1	Keys and people			Select

4) Find and select the key to hand out.

   - To scan the key in the Local PD, click **Scan**.
   - To search for the key, enter the search criteria and click **Search**. See also Section 4.2.2 *“Searching for Keys”*, page 26.
   - Click **Select** for the key to hand out.

   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.

   The following steps and options are applicable for Dynamic Keys in cylinder group remote systems. For other key types and configurations, some of the steps and options are not available.

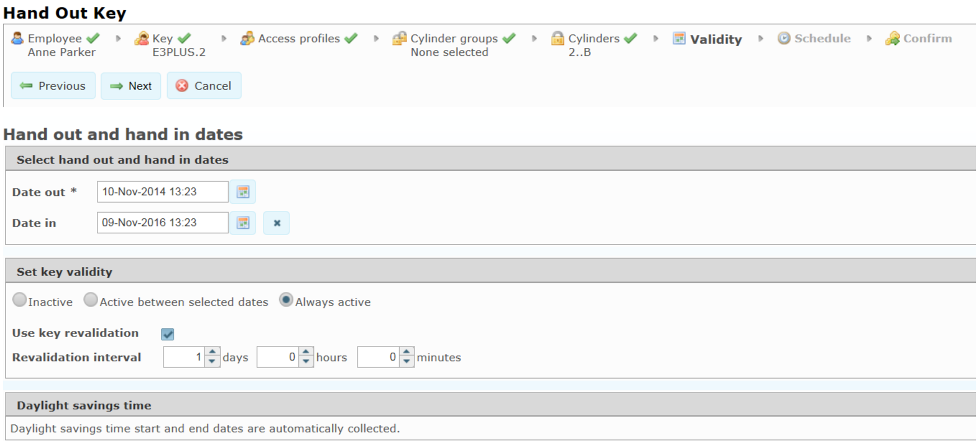
5) Select access profiles for the key and click **Next**.

By default the employee or visitor access profiles are already added.

6) Select the cylinder groups to which the key will have explicit access and click **Next**.

7) Select the cylinders to which the key will have explicit access and click **Next**.

8) Select date and validity information.



Hand Out Key

Employee ✓ Anne Parker ▸ Key ✓ E3PLUS.2 ▸ Access profiles ✓ ▸ Cylinder groups ✓ None selected ▸ Cylinders ✓ 2..B ▸ **Validity** ▸ Schedule ▸ Confirm

Previous | Next | Cancel

Hand out and hand in dates

Select hand out and hand in dates

Date out *	10-Nov-2014 13:23
Date in	09-Nov-2016 13:23

Set key validity

○ Inactive ○ Active between selected dates ● Always active

Use key revalidation ☑

Revalidation interval 1 days 0 hours 0 minutes

Daylight savings time

Daylight savings time start and end dates are automatically collected.

a) Select hand out date (**Date out**) and hand in date (**Date in**).

b) Select if the key will be **Inactive**, **Active between selected dates** or **Always active**.

c) A revalidation interval can be chosen if the key is set as active between selected dates or always active.

- Click **Key revalidation**.
- Select the length of the revalidation interval in days, hours and minutes.

9) Click **Next**.

10) Select the time schedule for when the key will have access, click **Next**.

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

11) To confirm the hand out:

a) For scanned keys, click **Program and Save**.

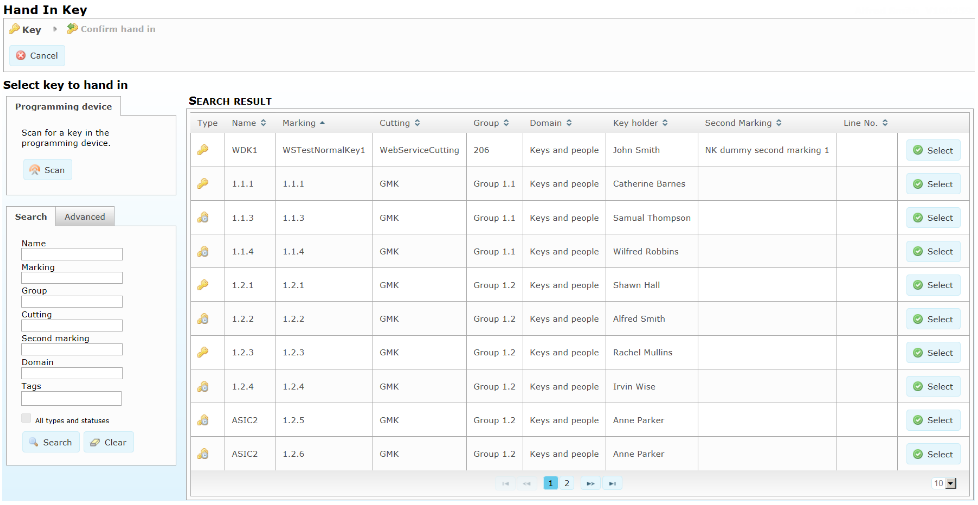
b) For non-scanned keys, click **Apply**.

In remote systems, a remote update job is created.

4.2.9 Receiving Keys (Hand-In)

1) Select **Work » Hand in key**.

A list of all keys handed out is displayed.



SEARCH RESULT

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 the key to hand in.

   To scan the key in the Local PD, click **Scan**.

   To filter the search result, enter the search criteria and click **Search**. See also Section 4.2.2 *“Searching for Keys”*, page 26.

3) Click **Select** for the key to hand in.

4) To hand in a key:

   a) 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.

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

4.2.10 Reporting Keys Lost Or Broken

This section describes how to report user keys lost or broken. See also Section 6.11.10 *“Reporting C-Key Lost, Found or Broken”*, page 93.

1) To report the key as lost:

   a) Select **Work » Report key lost**.

   b) Enter the search criteria to find the owner of the key and click **Search**.

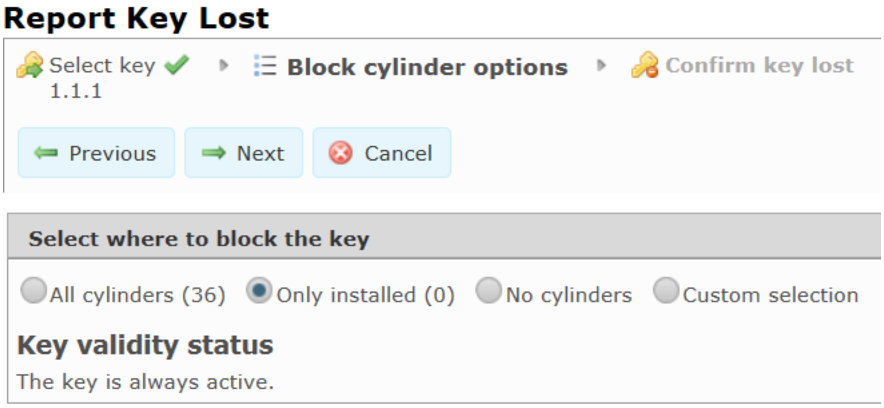
   c) Select the lost key.

      Depending on the urgency of blocking the key, there are three options to proceed:

      - Performing the programming job on the cylinder to immediately block the key.
      - If the key has a revalidation interval, waiting for the current interval to run out after which the key will be blocked.
      - Only have the key reported as lost in CWM but key is not blocked from access.

   d) Select for which cylinders the key will be blocked.

      If no programming of cylinders is planned, select **No cylinders**.



Select where to block the key

○ All cylinders (36) ● Only installed (0) ○ No cylinders ○ Custom selection

Key validity status

The key is always active.

e) Click **Next**.

f) Select **Priority**.

Urgent jobs should have a high priority level.

g) Click **Apply**.

The detailed information view for a key reported as lost will contain the options of removing the lost status as well as changing the cylinders for which the key is blocked.

h) To perform the programming job on the cylinder, see Section 4.4.10.1 *“Programming Cylinders Overview”*, page 40.

2) To report the key as broken:

a) Select **Work » Report key broken**.

b) Enter the search criteria to find the owner of the key and click **Search**.

c) Select the broken key.

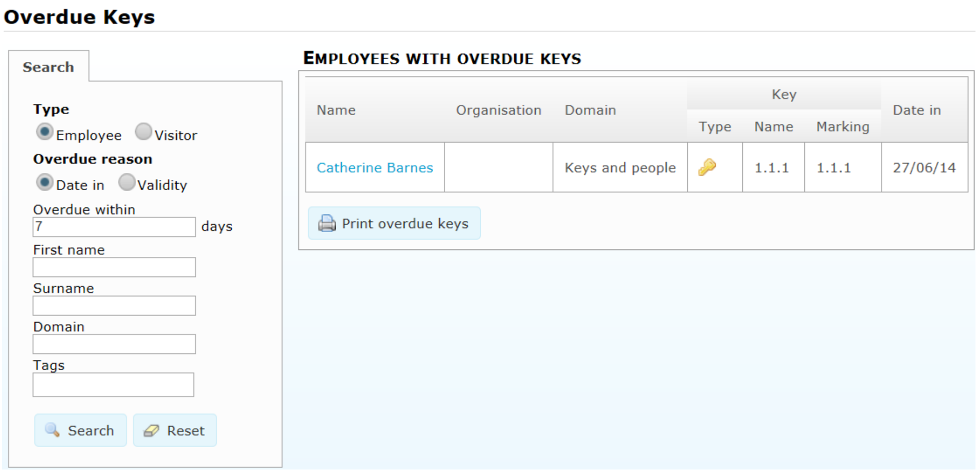
d) Click **Apply**.

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

4.2.11 Viewing Overdue Keys

1) Select **Work » Overdue keys**.

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



Type
● Employee ○ Visitor

Overdue reason
● Date in ○ Validity

Overdue within: 7 days

First name:

Surname:

Domain:

Tags:

Name	Organisation	Domain	Key			Date in
			Type	Name	Marking	
Catherine Barnes		Keys and people	🔑	1.1.1	1.1.1	27/06/14

The default number of days can be edited in the System Settings. See Section 6.4 *"Editing System Settings"*, page 73.

2) To search for overdue keys with other criteria, enter the search criteria and click **Search**.

   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.

3) To print a list of the overdue keys, click **Print overdue keys**.

4) To send an e-mail 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 73.

4.2.12 Copying 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 view the detailed information.

   See Section 4.2.2 *"Searching for Keys"*, page 26.

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.

4.2.13 Exporting Key Information

1) Search for the keys.

   See Section 4.2.2 *"Searching for Keys"*, page 26.

2) From the key search results, select the keys 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 73.

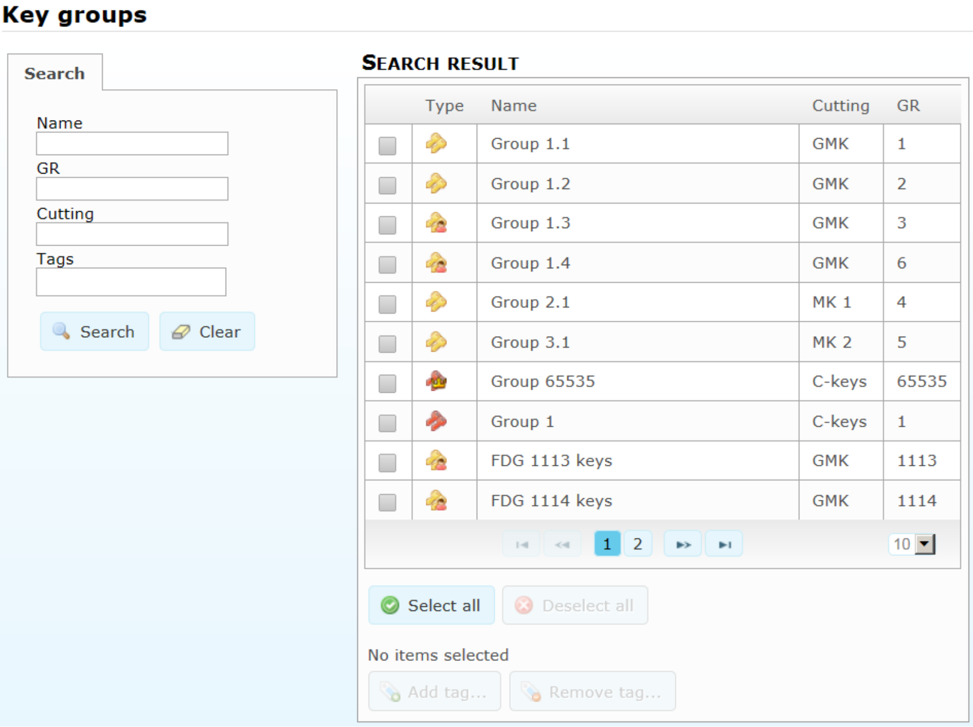
4) In the file download pop-up window, click **Open** or **Save**.

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:

🔑	Dynamic Key Group
🔑	Normal C-Key Group
🔑	Master C-Key Group

2) Enter the search criteria.

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 to edit and view the detailed information.

   See Section 4.2.2 *"Searching for Keys"*, page 26.

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 *"Editing Key Group Tags"*, page 35.

5) Click **Save**.

4.3.3 Editing Key Group Tags

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

   See Section 4.2.2 *"Searching for Keys"*, page 26.

2) Click **Edit**.

3) To add a tag:

   a) Click **Add tag**.

   b) Enter a name for the tag.

   c) Click **OK**.

   d) Click **Save**.

4) To remove a tag:

   a) Click the tag to be removed.

   b) Click **OK**.

   c) Click **Save**.

A tag can be edited for several key groups simultaneously. Select the key groups in the search result list and click **Add tags** or **Remove tags**.

See also Section 8.2.6 *"Tags"*, page 119.

4.3.4 Viewing Key Group Members

1) Find the key group and view the detailed information.

   See Section 4.2.2 *"Searching for Keys"*, page 26.

2) Select the **Members** tab.

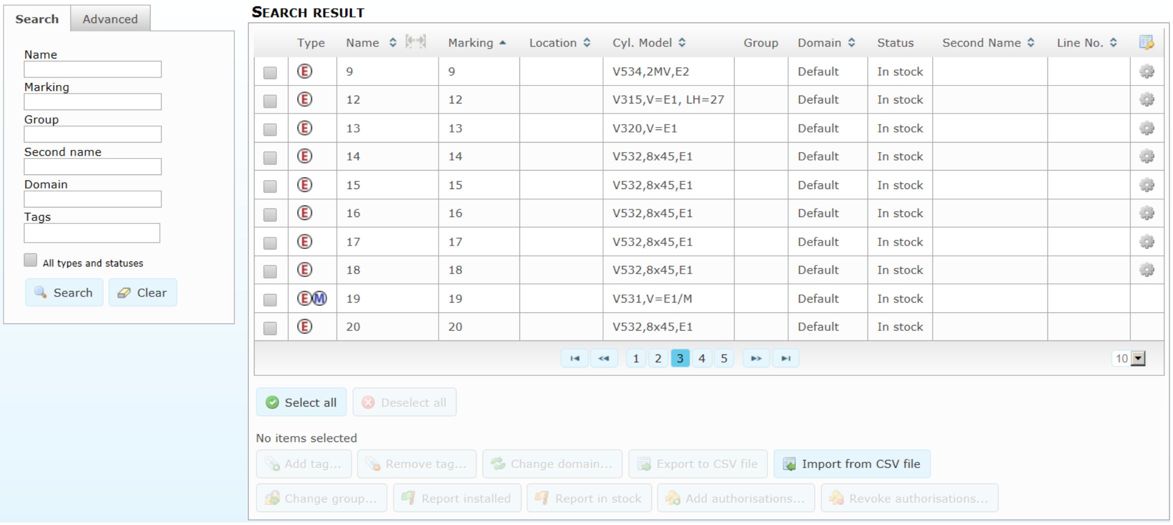
   A list with all keys in that key group is displayed.

4.4 Managing Cylinders

4.4.1 Searching for Cylinders

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

   A list of all cylinders is displayed.



Search | Advanced

Name

Marking

Group

Second name

Domain

Tags

□ All types and statuses

Search Clear

SEARCH RESULT

	Type	Name	Marking	Location	Cyl. Model	Group	Domain	Status	Second Name	Line No.	
□	Ⓔ	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			
□	ⒺⓂ	19	19		V531,V=E1/M		Default	In stock			
□	Ⓔ	20	20		V532,8x45,E1		Default	In stock			

No items selected

The following symbols are used:

Ⓔ Electronic Cylinder

Ⓜ Mechanical Cylinder

ⒺⓂ 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 and operational status.

3) Enter the search criteria.

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 9.3.3 *“Cylinder Attributes”*, page 130.

4.4.2 Editing Cylinder Information

1) Find the cylinder and view the detailed information.

See Section 4.4.1 *“Searching for Cylinders”*, page 35.

2) Click **Edit**.

3) Edit the fields as desired.

For more information about the cylinder attributes, see Section 9.3.3 *“Cylinder Attributes”*, page 130.

4) To add a tag, click **Add tag**. See also Section 4.4.3 *“Editing Cylinder Tags”*, page 37

5) To add an external link, click **Add external link**. See also Section 4.4.4 *"Editing Cylinder External Links"*, page 37

6) Click **Save**.

7) To edit the second name:

   a) Select the **Additional information** tab.

   b) Click **Edit**.

   c) Update the field **Second name**.

   d) Click **Save**.

4.4.3 Editing Cylinder Tags

1) Find the cylinder and view the detailed information.

   See Section 4.4.1 *"Searching for Cylinders"*, page 35

2) Click **Edit**.

3) To add a tag:

   a) Click **Add tag**.

   b) Enter a name for the tag.

   c) Click **OK**.

   d) Click **Save**.

4) To remove a tag:

   a) Click the tag to be removed.

   b) Click **OK**.

   c) Click **Save**.

A tag can be edited for several cylinders simultaneously. Select the cylinders in the search result list and click **Add tags** or **Remove tags**.

See also Section 8.2.6 *"Tags"*, page 119.

4.4.4 Editing Cylinder External Links

1) Find the cylinder and view the detailed information.

   See Section 4.4.1 *"Searching for Cylinders"*, page 35.

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 73.

   d) Click **OK**.

4) To remove an external link, click **Remove** on 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 121.

4.4.5 Viewing Cylinder Update History

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

1) Find the cylinder and view the detailed information.

   See Section 4.4.1 *“Searching for Cylinders”*, page 35.
2) Select the **Update history** tab.

   A list with all cylinder updates is displayed.
3) To display further details on a specific update, click the link in the **Type** column.

4.4.6 Viewing Cylinder Events

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

1) Find the cylinder and view the detailed information.

   See Section 4.4.1 *“Searching for Cylinders”*, page 35.
2) Select the **Events** tab.

   A list with all cylinder events is displayed.

4.4.7 Editing 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 view the detailed information.

   See Section 4.4.1 *“Searching for Cylinders”*, page 35.
2) To report the cylinder installed:
   a) Click **Report installed**.
   b) Click **OK**.

      Several cylinders can be reported installed simultaneously. Select the cylinders in the search result list and click **Report installed**.
3) To report the cylinder in stock:
   a) Click **Report in stock**.
   b) Click **OK**.

      Several cylinders can be reported in stock simultaneously. Select the cylinders in the search result list and click **Report in stock**.
4) To report the cylinder broken:
   a) Click **Report broken**.
   b) Select **Report broken only**.
   c) Click **Next**.
   d) Click **Apply**.

5) To report the cylinder operational:

   a) Click **Report operational**.

   b) Click **OK**.

   A programming job is created.

4.4.8 Replacing Broken Cylinder

1) Find the cylinder to replace and view the detailed information.

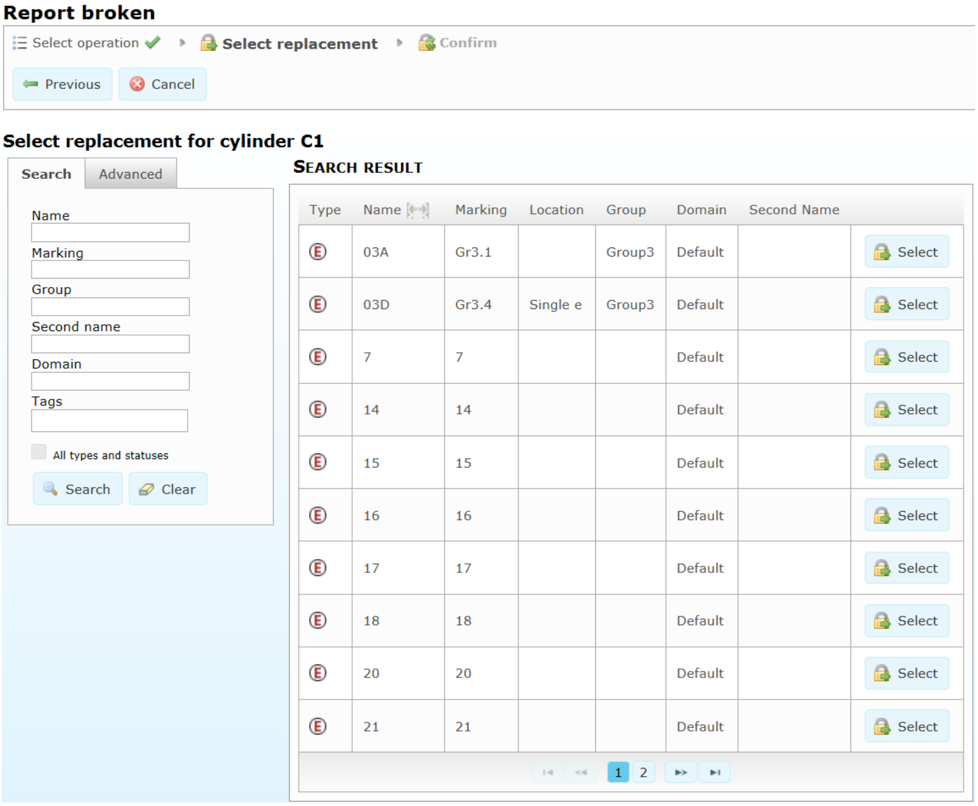
   See Section 4.4.1 *"Searching for Cylinders"*, page 35.

2) Click **Report Broken**.

3) Select **Report broken and replace with another cylinder**.

4) Click **Next**.

   A list with all cylinders of the same type that are in stock is displayed.



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) To select a replacement cylinder, click **Select** for the specific cylinder.

7) Select a **Priority**.

   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.

4.4.9 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 view the detailed information.

   See Section 4.4.1 *"Searching for Cylinders"*, page 35.

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 4.4.10.1 *"Programming Cylinders Overview"*, page 40.

4.4.10 Programming Cylinders

4.4.10.1 Programming Cylinders Overview

Requirements:

- 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 **Cylinder Reprogramming** rights

Programming cylinders involves the following steps:

1) In CWM, **edit the cylinder access list**.

   A cylinder programming job is created.

2) **Assign** the cylinder programming job to a C-Key.

3) **Transfer** the cylinder programming job to the C-Key.

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

5) Once the cylinders are programmed, **update** the status of the programming job in the system.

All cylinder programming jobs are created and assigned to a C-Key in CWM. Transferring and updating programming jobs can either be done with a Local PD or a Remote PD.

The procedure for programming cylinders with a Local PD is described in Section 4.4.10.2 *"Programming Cylinders with Local PD"*, page 40.

The corresponding procedure for Remote PDs is described in Section 4.4.10.3 *"Assigning Cylinder Programming Jobs to C-Key"*, page 42 and Section 4.4.10.4 *"Programming Cylinder Jobs with Remote PD"*, page 42.

For more information about cylinder programming, see Section 8.5 *"Cylinder Programming"*, page 121.

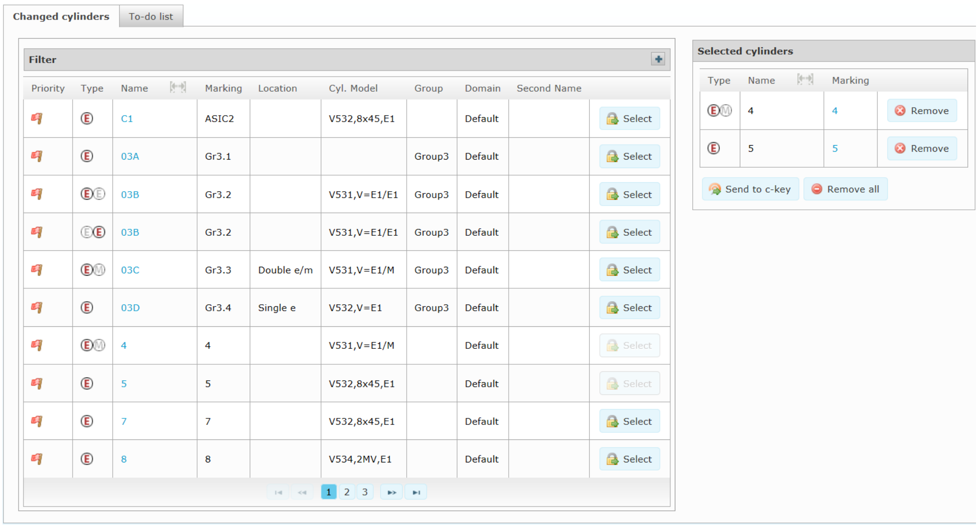
4.4.10.2 Programming Cylinders with Local PD

To program cylinders with a Local PD:

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**.



Priority	Type	Name	Marking	Location	Cyl. Model	Group	Domain	Second Name	
	Ⓔ	C1	ASIC2		V532,8x45,E1		Default		Select
	Ⓔ	03A	Gr3.1			Group3	Default		Select
	ⒺⒺ	03B	Gr3.2		V531,V=E1/E1	Group3	Default		Select
	ⒺⒺ	03B	Gr3.2		V531,V=E1/E1	Group3	Default		Select
	ⒺⓂ	03C	Gr3.3	Double e/m	V531,V=E1/M	Group3	Default		Select
	Ⓔ	03D	Gr3.4	Single e	V532,V=E1	Group3	Default		Select
	ⒺⓂ	4	4		V531,V=E1/M		Default		Select
	Ⓔ	5	5		V532,8x45,E1		Default		Select
	Ⓔ	7	7		V532,8x45,E1		Default		Select
	Ⓔ	8	8		V534,2MV,E1		Default		Select

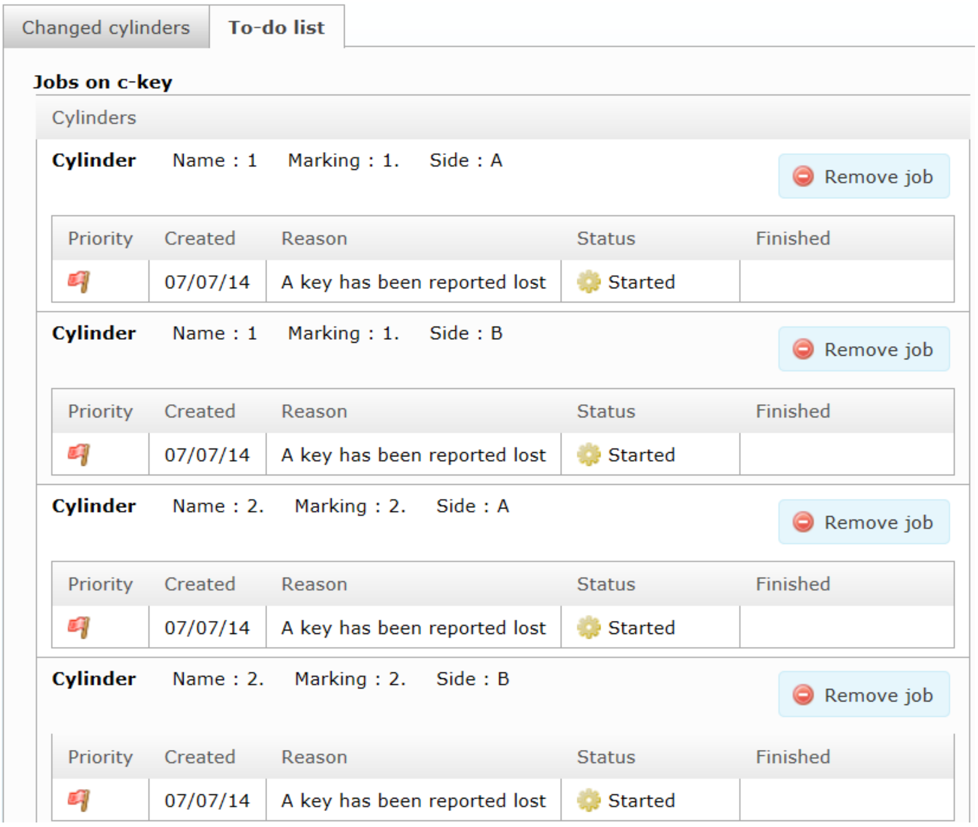
Selected cylinders

Type	Name	Marking	
ⒺⓂ	4	4	Remove
Ⓔ	5	5	Remove

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.

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



Jobs on c-key

Cylinders

Cylinder Name : 1 Marking : 1. Side : A

Priority	Created	Reason	Status	Finished
	07/07/14	A key has been reported lost	Started	

Cylinder Name : 1 Marking : 1. Side : B

Priority	Created	Reason	Status	Finished
	07/07/14	A key has been reported lost	Started	

Cylinder Name : 2. Marking : 2. Side : A

Priority	Created	Reason	Status	Finished
	07/07/14	A key has been reported lost	Started	

Cylinder Name : 2. Marking : 2. Side : B

Priority	Created	Reason	Status	Finished
	07/07/14	A key has been reported lost	Started	

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

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

> **IMPORTANT!**
> Keep the key inserted until the programming job is completed.

7) Log in to CWM again.

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

9) Select the **To-do list** tab.

10) Click **Update**.

    The status of the programming jobs are loaded from the C-Key.

11) Click **Remove finished jobs**.

4.4.10.3 Assigning Cylinder Programming Jobs to C-Key

To assign a cylinder programming job to a C-Key:

1) 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 89

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

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

4) For each cylinder programming job to be executed, click **Select**.

5) Click **Apply**.

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

4.4.10.4 Programming Cylinder Jobs with Remote PD

Throughout the procedure of programming cylinders, the status of the Remote PD interaction is indicated by LEDs, see Section 9.5 *“Remote PD Indications”*, page 136.

To program cylinder jobs with a Remote PD:

1) Insert the C-Key in a Remote PD to pick up (transfer) the cylinder programming job.

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

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

> **IMPORTANT!**
> Keep the key inserted until the programming job is completed.

3) Insert the C-key in a Remote PD to update the status of the programming jobs.

4.4.11 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 4.4.12 *"Exporting Cylinder Information"*, page 43.

> **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 6.15 *"Importing Extensions"*, page 100.

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
>
> Existing cylinder data is overwritten.

> **NOTE!**
> To import cylinder information from a CSV file, the combination of the fields **Marking** and **Second Marking** must exist and be unique. The field **Second Marking** can be omitted.

4.4.12 Exporting Cylinder Information

1) Search for the cylinders.

   See Section 4.4.1 *"Searching for Cylinders"*, page 35.
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 73.

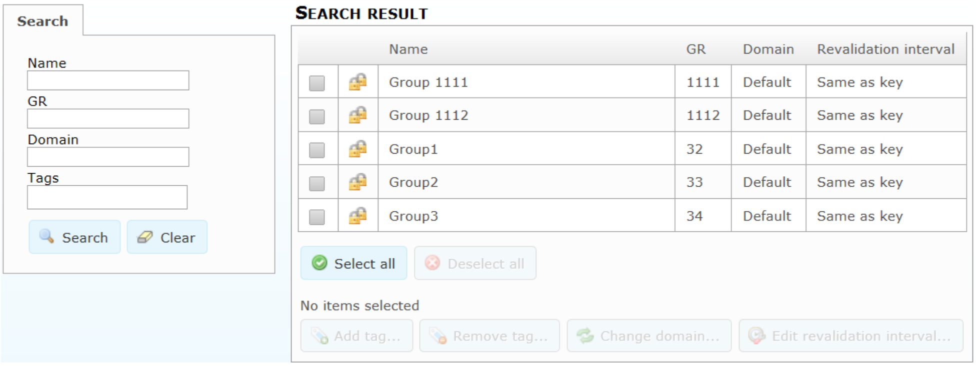
4) In the file download pop-up window, click **Open** or **Save**.

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 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

No items selected

2) Enter the search criteria.

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.

See Section 4.5.1 *“Searching for Cylinder Groups”*, page 44.

2) In the detailed information view, 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 *“Editing Cylinder Group Tags”*, page 44

5) Click **Save**.

6) To change domain, click **Change domain**. See also Section 6.6.8 *“Changing Domain For Cylinder Groups”*, page 86.

4.5.3 Editing Cylinder Group Tags

1) Find the cylinder group.

See Section 4.5.1 *“Searching for Cylinder Groups”*, page 44.

2) Click **Edit**.

3) To add a tag:

   a) Click **Add tag**.

   b) Enter a name for the tag.

   c) Click **OK**.

   d) Click **Save**.

4) To remove a tag:

   a) Click the tag to be removed.

   b) Click **OK**.

   c) Click **Save**.

A tag can be edited for several cylinder groups simultaneously. Select the cylinder groups in the search result list and click **Add tags** or **Remove tags**.

See also Section 8.2.6 *“Tags”*, page 119.

4.5.4 Viewing Cylinder Group Members

1) Find the cylinder group.

   See Section 4.5.1 *“Searching for Cylinder Groups”*, page 44.

2) Select the **Members** tab.

   A list with all cylinders in that group is displayed.

4.5.5 Viewing Cylinder Group Events

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.

   See Section 4.5.1 *“Searching for Cylinder Groups”*, page 44.

2) Select the **Events** tab.

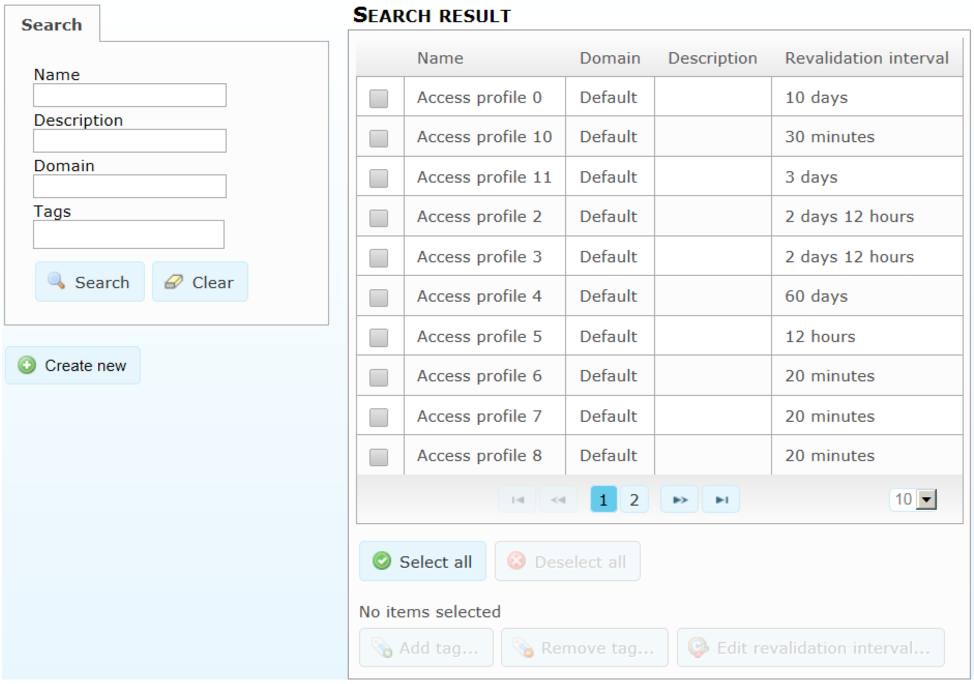
   A list with all cylinder group events is displayed.

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

1 2 10

No items selected

2) Enter the search criteria.

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**.

   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 *“Editing Access Profile Tags”*, page 47

   e) To add an external link, click **Add external link**. See also Section 4.6.5 *“Editing Access Profile External Links”*, page 47

   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 45.

   b) Click **Delete**.

   c) Click **OK**.

See also Section 8.2.4 *“Access Profiles”*, page 115.

4.6.3 Editing Access Profile Information

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

   See Section 4.6.1 *“Searching for Access Profiles”*, page 45.

2) In the detailed information view, click **Edit**.
3) Update the fields.
4) To add tags, click **Add Tag...**. See also Section 4.1.5 *“Editing Employee or Visitor Tags”*, page 24.
5) To add edit external links, click **Add external link...**. See also Section 4.1.6 *“Editing Employee or Visitor External Links”*, page 24.
6) Click **Save**.

4.6.4 Editing Access Profile Tags

1) Find the access profile.

   To search for the access profile and display the detailed information view, see Section 4.6.1 *“Searching for Access Profiles”*, page 45.

2) Click **Edit**.
3) To add a tag:
   a) Click **Add tag**.
   b) Enter a name for the tag.
   c) Click **OK**.
   d) Click **Save**.
4) To remove a tag:
   a) Click the tag to be removed.
   b) Click **OK**.
   c) Click **Save**.

A tag can be edited for several access profiles simultaneously. Select the access profiles in the search result list and click **Add tags** or **Remove tags**.

For more information about tags, see Section 8.2.6 *“Tags”*, page 119.

4.6.5 Editing Access Profile External Links

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

   See Section 4.6.1 *“Searching for Access Profiles”*, page 45.

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 73.

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 121.

4.6.6 Viewing Access Profile Events

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 view the detailed information.

See Section 4.6.1 *"Searching for Access Profiles"*, page 45.

2) Select the **Events** tab.

A list with all access profile events is displayed.

4.6.7 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 4.2.2 *"Searching for Keys"*, page 26.

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

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

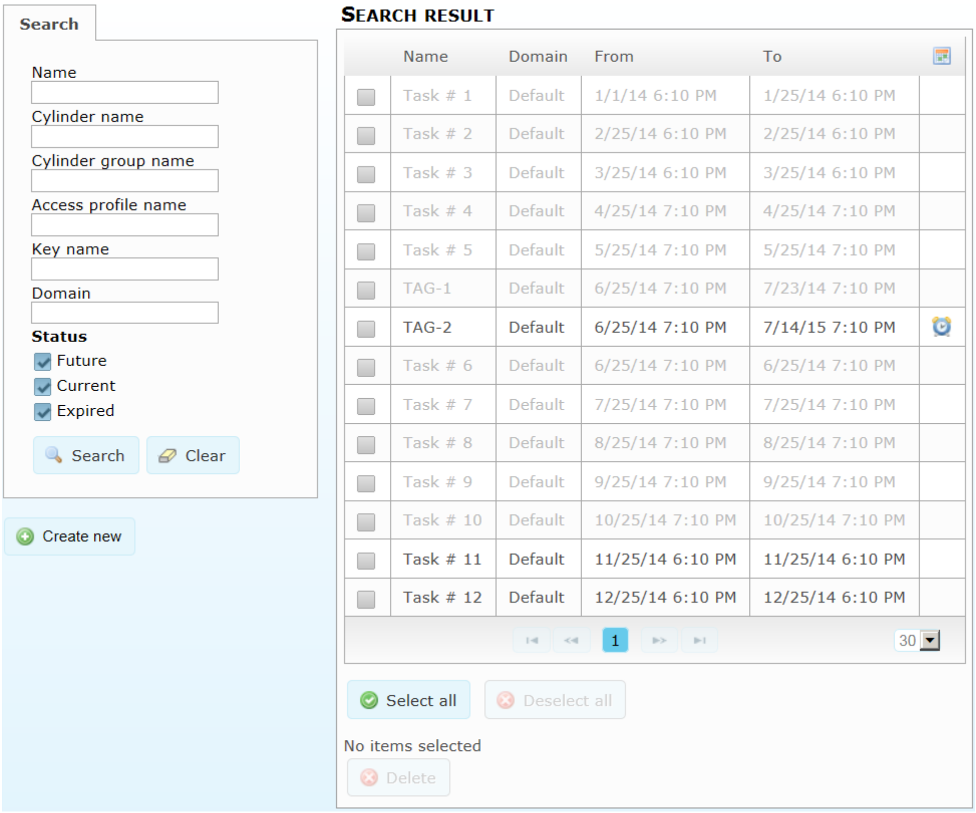
4) Click **OK**.

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.



	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.

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 48.
   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 117.

4.7.3 Editing Temporary Access Groups

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

   See Section 4.7.1 *"Searching for Temporary Access Groups"*, page 48.
2) In the detailed information view, click **Edit**.
3) Update the fields.
4) Click **Save**.

4.7.4 Adding and 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 8.1.5 *"Key Validity"*, page 109.
- Activate key **Revalidation**, see Section 8.1.6 *"Key Revalidation"*, page 109.

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

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

   See Section 4.7.1 *"Searching for Temporary Access Groups"*, page 48.

2) To add keys to a temporary access group:

   a) Select the **Keys** tab.

   b) Click **Edit**.

   c) Click **Add keys...**.

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

   e) Click **Done**.

   f) Click **Save**.

   A remote job is automatically created.

3) To remove keys from a temporary access group:

   a) Select the **Keys** tab.

   b) Click **Edit**.

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

   d) Click **Save**.

4.7.5 Adding and removing access profiles from Temporary Access Groups

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

   See Section 4.7.1 *"Searching for Temporary Access Groups"*, page 48.

2) To add access profiles to a temporary access group:

   a) Select the **Access profiles** tab.

   b) Click **Edit**.

   c) Click **Add access profiles...**.

   d) Click **Select** for individual access profiles to add. Click **Select all** to add all access profiles.

   e) Click **Done**.

   f) Click **Save**.

3) To remove access profiles from a temporary access group:
   a) Select the **Access profiles** tab.
   b) Click **Edit**.
   c) Click **Remove** for individual access profiles to remove. Click **Remove all** to remove all access profiles.
   d) Click **Save**.

4.7.6 Editing Explicit Access for Temporary Access Groups

1) Click **Edit**.
2) 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**.
3) 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**.
4) Click **Save**.

4.7.7 Viewing Temporary Access Group Events

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 view the detailed information.

   See Section 4.7.1 *“Searching for Temporary Access Groups”*, page 48.
2) Select the **Events** tab.

   A list with all temporary access group events is displayed.

4.8 Viewing Authorisations

4.8.1 Viewing Accessible Cylinders for Keys

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.

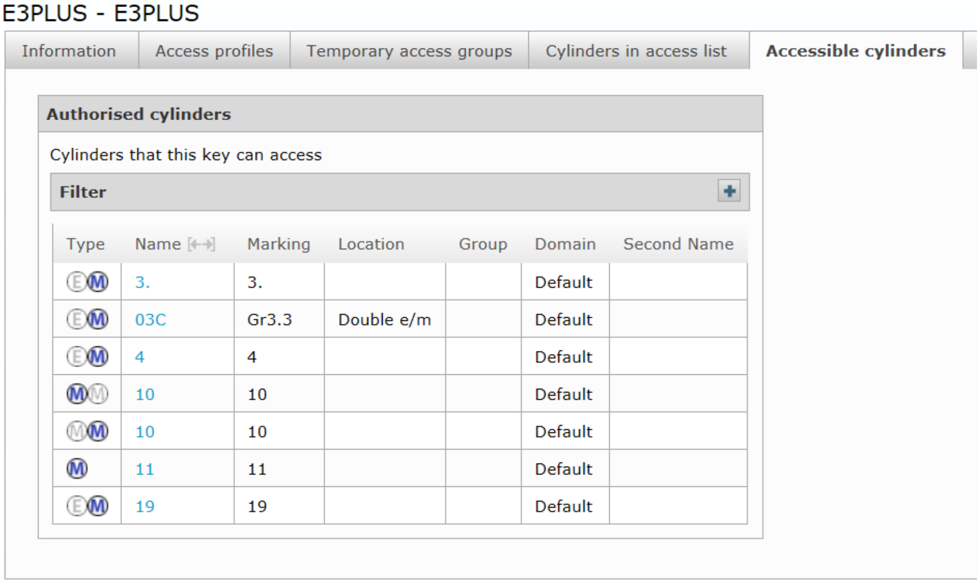
1) Find the key.

   a) To search for the key, see Section 4.2.2 *"Searching for Keys"*, page 26

   b) To scan a key in the Local PD, see Section 4.2.1 *"Scanning a Key"*, page 26

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

   A list of the actually accessible cylinders is displayed.



E3PLUS - E3PLUS

Authorised cylinders

Cylinders that this key can access

Type	Name	Marking	Location	Group	Domain	Second Name
EM	3.	3.			Default	
EM	03C	Gr3.3	Double e/m		Default	
EM	4	4			Default	
MM	10	10			Default	
MM	10	10			Default	
M	11	11			Default	
EM	19	19			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).

E E Information concerns the A-side

E E Information concerns the B-side

4.8.2 Viewing Accessible Cylinders for Key Groups

1) Find the key group and view the detailed information.

   See Section 4.3.1 *"Searching for Key Groups"*, page 34.

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

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

   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).

E E Information concerns the A-side

E E Information concerns the B-side

NOTE!
Individual keys might be excluded from access. See Section 8.1.3 *"Electronic Authorisation"*, page 107.

4.8.3 Viewing Keys With Access to Cylinder

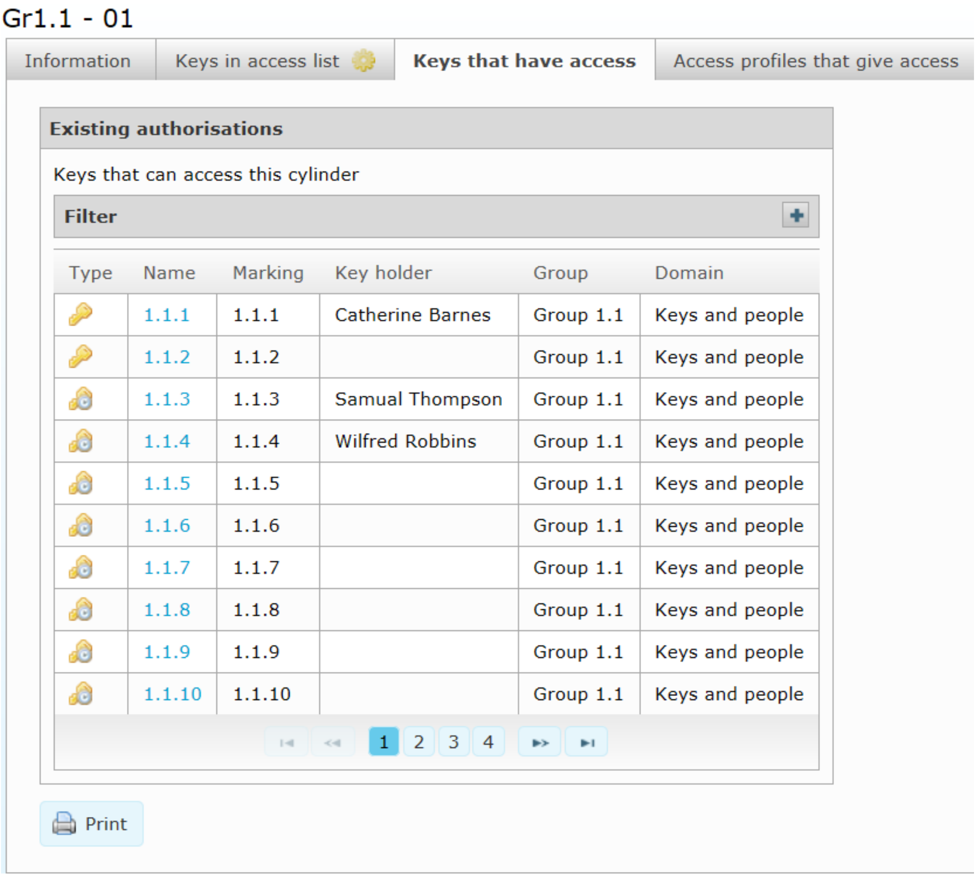
Keys with access means keys that can access the cylinder considering both the key access lists and the cylinder access lists. These are the keys that can actually open the cylinder.

1) Find the cylinder and view the detailed information.

   See Section 4.4.1 *"Searching for Cylinders"*, page 35.

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

   A list of keys with actual access to the cylinder is displayed. Keys belonging to authorised key groups are displayed individually.



Existing authorisations

Keys that can access this cylinder

Type	Name	Marking	Key holder	Group	Domain
🔑	1.1.1	1.1.1	Catherine Barnes	Group 1.1	Keys and people
🔑	1.1.2	1.1.2		Group 1.1	Keys and people
🔑	1.1.3	1.1.3	Samual Thompson	Group 1.1	Keys and people
🔑	1.1.4	1.1.4	Wilfred Robbins	Group 1.1	Keys and people
🔑	1.1.5	1.1.5		Group 1.1	Keys and people
🔑	1.1.6	1.1.6		Group 1.1	Keys and people
🔑	1.1.7	1.1.7		Group 1.1	Keys and people
🔑	1.1.8	1.1.8		Group 1.1	Keys and people
🔑	1.1.9	1.1.9		Group 1.1	Keys and people
🔑	1.1.10	1.1.10		Group 1.1	Keys and people

4.8.4 Viewing Access Profiles That Give Access to Cylinder

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 view the detailed information.

   a) To search for a cylinder, see Section 4.4.1 *"Searching for Cylinders"*, page 35.

   b) To search for a cylinder group, see Section 4.5.1 *"Searching for Cylinder Groups"*, page 44.

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

See also Section 4.9.4 *“Configuring Access Profile Authorisations”*, page 59.

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 59.

Note that the fact that a cylinder is 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”*, page 53.

To remove all access for a cylinder, see Section 4.9.3 *“Removing All Access for a Cylinder”*, page 58.

For more information about authorisation principles, see Section 8.1.3 *“Electronic Authorisation”*, page 107.

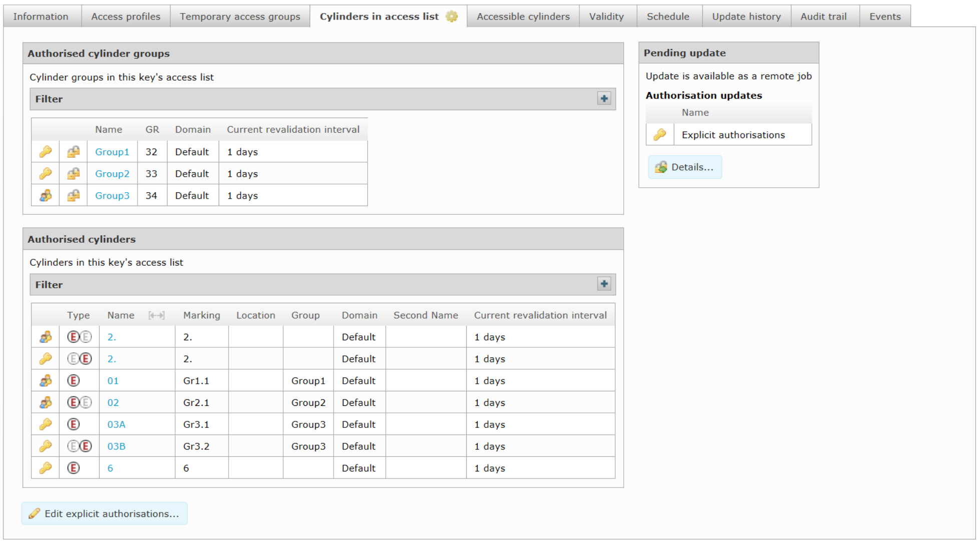
1) Find the key.

   a) To search for the key, see Section 4.2.2 *“Searching for Keys”*, page 26

   b) To scan a key in the Local PD, see Section 4.2.1 *“Scanning a Key”*, page 26

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

   Currently authorised cylinder groups and cylinders are displayed.



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

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 both explicit authorisations and authorisations from access profiles.

🔑 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. In such cases, follow the procedure in *Step 4* or *Step 5*.

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

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

   e) Click **OK**.

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

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

   e) Click **OK**.

6) Click **Save**.

7) If the key is scanned, click **Write access list to key locally** to update the key.

   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.

NOTE!

For Dynamic 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 4.8.3 *"Viewing Keys With Access to Cylinder"*, page 54.

For more information about authorisation principles, see Section 8.1.3 *"Electronic Authorisation"*, page 107.

1) Find the cylinder and view the detailed information.

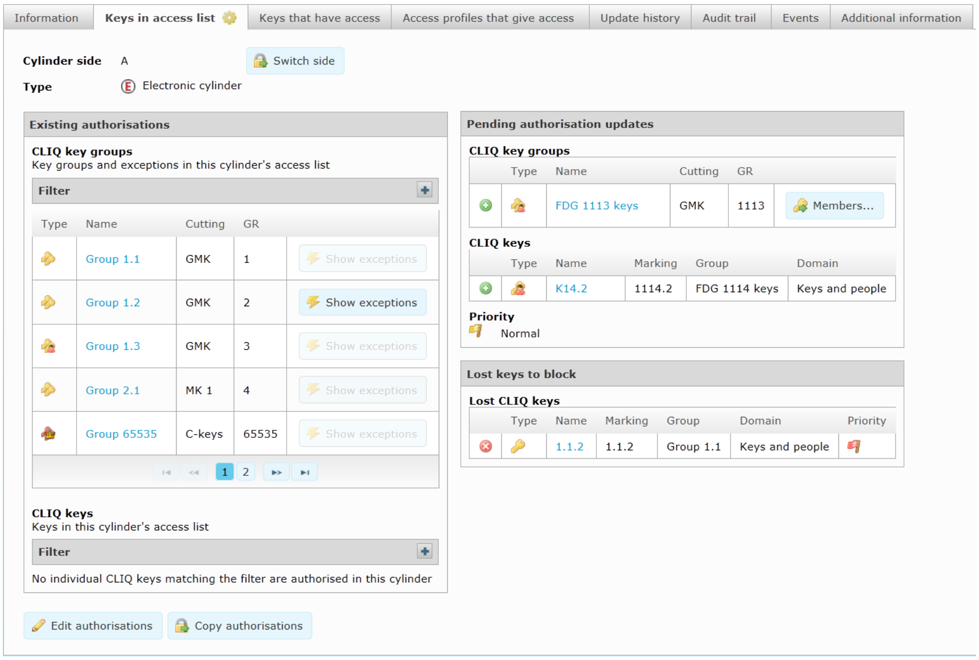
   See Section 4.4.1 *"Searching for Cylinders"*, page 35.

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**.



Cylinder side A

Type Ⓔ Electronic cylinder

Existing authorisations

CLIQ key groups
Key groups and exceptions in this cylinder's access list

Filter +

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 2.1	MK 1	4	Show exceptions
	Group 65535	C-keys	65535	Show exceptions

1 2

CLIQ keys
Keys in this cylinder's access list

Filter +

No individual CLIQ keys matching the filter are authorised in this cylinder

Pending authorisation updates

CLIQ key groups

	Type	Name	Cutting	GR	
⊕		FDG 1113 keys	GMK	1113	Members...

CLIQ keys

	Type	Name	Marking	Group	Domain
⊕		K14.2	1114.2	FDG 1114 keys	Keys and people

Priority
Normal

Lost keys to block

Lost CLIQ keys

	Type	Name	Marking	Group	Domain	Priority
⊗		1.1.2	1.1.2	Group 1.1	Keys and people	

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:

   a) Click **Add CLIQ key group**.

      The search result list displays all available key groups.

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

   c) 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.

d) Click **Done**.

6) To exclude keys from a key group authorisation:

a) Click **Edit** for the key group.

b) Click **Unauthorise** for the keys to exclude from access.

7) To remove key groups, click **Remove** for the key group to remove.

8) To add individual keys, perform *Step 5* for keys.

9) To remove keys, click **Remove** for the key to remove.

10) When done editing click **To view**.

A cylinder programming job is created.

To program cylinders, see Section 4.4.10.1 *"Programming Cylinders Overview"*, page 40.

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 35) 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 view the detailed information.

See Section 4.4.1 *"Searching for Cylinders"*, page 35.

2) Select **Remove key side authorisations**.

> **NOTE!**
> To remove the access, all keys that used to have access to the cylinder must be updated.

> **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 119.

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.

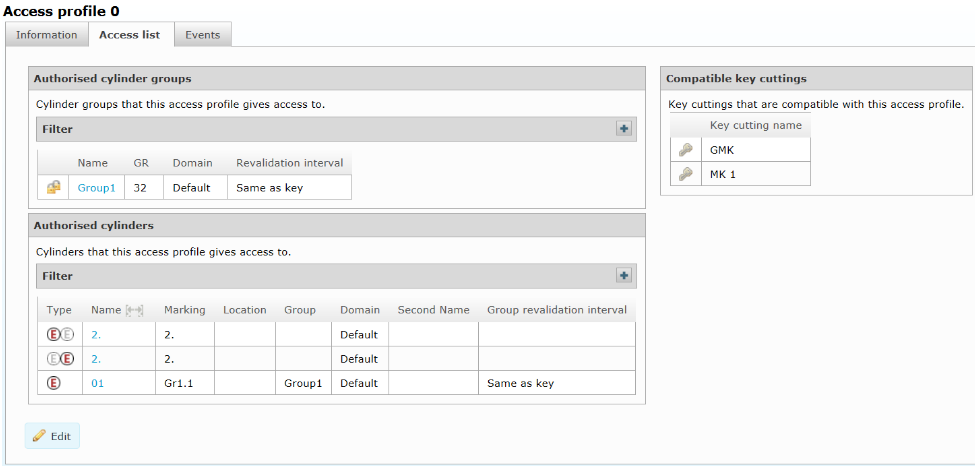
1) Find the access profile and view the detailed information.

   See Section 4.6.1 *“Searching for Access Profiles”*, page 45.

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.

Filter

	Name	GR	Domain	Revalidation interval
	Group1	32	Default	Same as key

Authorised cylinders

Cylinders that this access profile gives access to.

Filter

Type	Name	Marking	Location	Group	Domain	Second Name	Group revalidation interval
ⒺⒺ	2.	2.			Default		
ⒺⒺ	2.	2.			Default		
Ⓔ	01	Gr1.1		Group1	Default		Same as key

Compatible key cuttings

Key cuttings that are compatible with this access profile.

	Key cutting name
	GMK
	MK 1

   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

4) To add cylinders:

   a) Click **Add cylinders**.

      The search result list displays all available cylinders.

   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 **Done**.

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

6) To add cylinder groups, perform *Step 4* for cylinder groups.

7) To remove cylinder groups, click **Remove** for the cylinder group to remove or click **Remove all**.

8) Flexible revalidation can also be edited in this view. See Section 4.10.2 *“Configuring Flexible Revalidation”*, page 64.

9) Click **Save**.

See also Section 8.2.4 *“Access Profiles”*, page 115.

4.9.5 Selecting Employee or Visitor 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 view the detailed information.

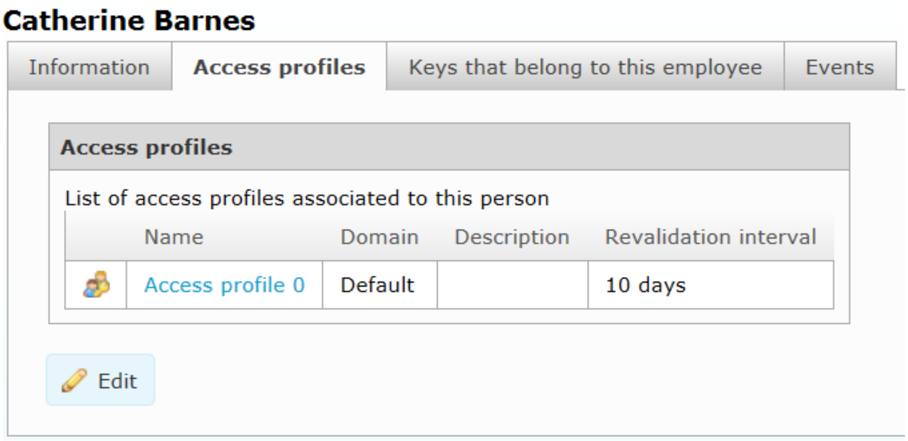
   See Section 4.1.1 *"Searching for Employees or Visitors"*, page 22.

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 115.

4.9.6 Selecting Key Access Profiles

Access profiles are only applicable to dynamic keys.

1) Find the key to edit.

   To search for the key and display the detailed information view, see Section 4.2.2 *"Searching for Keys"*, page 26

To scan the key in the Local PD and display the detailed information view, see Section 4.2.1 *"Scanning a Key"*, page 26

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 115.

4.9.7 Configuring Authorisations Using Lock Chart

The Lock Chart is a matrix that shows what keys have access to what cylinders. It is only available for non-cylinder group systems.

IMPORTANT!
The Lock Chart does only consider the cylinder access lists. For Dynamic Keys, accesses may be limited further by the key access lists, and the Lock Chart might therefore indicate that a key has access even though it does not.

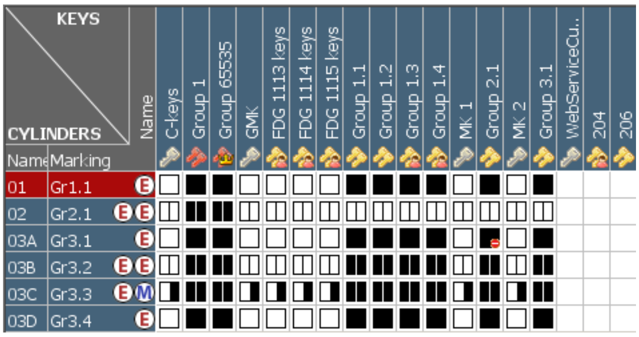
1) Select **Work » Lock chart**.

2) To filter cylinders, enter the cylinder search criteria and then click **Search**.

3) To filter key groups, enter the CLIQ key groups search criteria and click **Search**.

4) Click **Generate lock chart**.

The Lock Chart is displayed. On the left side, the cylinder name and marking appear, and the cylinder type is indicated. On the top, key groups appear.



Name	Marking	Name	C-keys	Group 1	Group 65535	GMK	FDG 1113 keys	FDG 1114 keys	FDG 1115 keys	Group 1.1	Group 1.2	Group 1.3	Group 1.4	MK 1	Group 2.1	MK 2	Group 3.1	WebServiceCu..	204	206
01	Gr1.1	E	□	■	■	□	□	□	□	■	■	■	■	□	■	□	■			
02	Gr2.1	E E	□□	■■	■■	□□	□□	□□	□□	□□	□□	□□	□□	□□	□□	□□	□□			
03A	Gr3.1	E	□	■	■	□	□	□	□	■	■	■	■	□	■⛔	□	■			
03B	Gr3.2	E E	□□	■■	■■	□□	□□	□□	□□	■■	■■	■■	■■	□□	■■	□□	■■			
03C	Gr3.3	E M	□■	■■	■■	□■	□■	□■	□■	■■	■■	■■	■■	□■	■■	□■	■■			
03D	Gr3.4	E	□	■	■	□	□	□	□	■	■	■	■	□	■	□	■			

The access rights appear as follows:

■	Key authorised in cylinder
□	Key not authorised in cylinder
□+	Cylinder Programming Job created to authorise key in cylinder
■⛔	Cylinder Programming Job created to remove authorisation for key in cylinder
◧	Example for double cylinder: Key authorised in cylinder side A but not in side B.

5) To view the individual keys in a key group, click on the key group symbol.

6) To view cylinder or key details, click in the individual key or cylinder symbol.

7) To add access to a cylinder for a specific key, double-click on a square that is marked as not authorised (white).

   A plus sign appears and a cylinder programming job is created.

8) To remove access to a cylinder for a specific key, double-click on a square that is marked as authorised (black).

   A no entry sign appears and a cylinder programming job is created.

9) To program cylinders with the updates, see Section 4.4.10.1 *“Programming Cylinders Overview”*, page 40.

4.10 Configuring Key Validity and Schedule

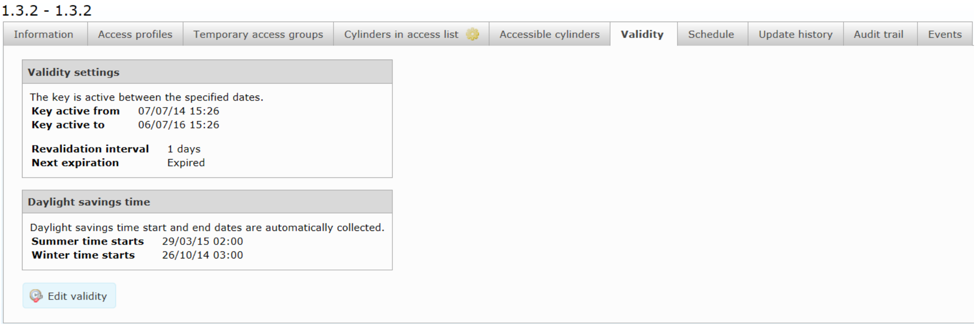
4.10.1 Configuring Key Validity and Revalidation

1) Find the key.

   a) To search for the key, see Section 4.2.2 *“Searching for Keys”*, page 26

   b) To scan a key in the Local PD, see Section 4.2.1 *“Scanning a Key”*, page 26

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:

- Activity setting: 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**, this 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.
- 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) If the key is not scanned, optionally enter a date for **Remote update job expires**.

    After this date, the validity will not be updated when a key is inserted in a Remote PD and the key will work with the old settings.

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 and Revalidation 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 8.1.5 *“Key Validity”*, page 109 and Section 8.1.6 *“Key Revalidation”*, page 109.

4.10.2 Configuring Flexible Revalidation

IMPORTANT!
Since Flexible Revalidation is an advanced and complex feature, it is recommended to read Section 8.1.7 *"Flexible Revalidation"*, page 111 carefully before configuring it.

Prerequisites:

- At least one user key has firmware with Flexible Revalidation support (see Section 9.7 *"Firmware Dependent Functionality"*, page 137).
- The feature is enabled in **System settings** (see Section 6.4 *"Editing System Settings"*, page 73).

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 view the detailed information.

      See Section 4.6.1 *"Searching for Access Profiles"*, page 45.

   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 view the detailed information.

      See Section 4.5.1 *"Searching for Cylinder Groups"*, page 44.

   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 55.

See also Section 8.1.7 *"Flexible Revalidation"*, page 111.

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 112). 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 137

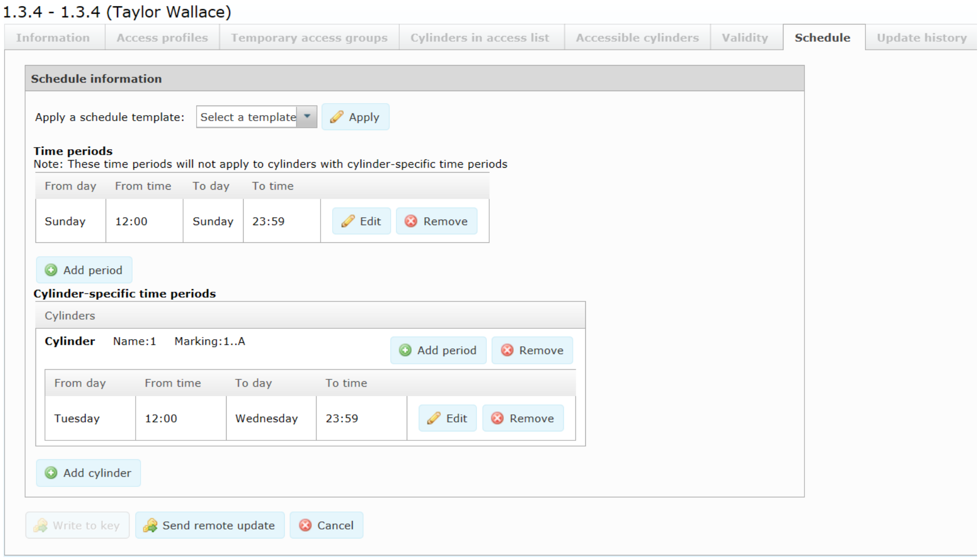
1) Find the key.

   To search for the key, see Section 4.2.2 *"Searching for Keys"*, page 26.

   To scan a key in the Local PD, see Section 4.2.1 *"Scanning a Key"*, page 26.

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	Edit Remove

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	Edit Remove

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.

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 view the detailed information view.

See Section 4.2.2 *“Searching for Keys”*, page 26.

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 65.

6) Click **Next**.

The selected settings are displayed.

7) To confirm the updates, click **Apply**.

Key update jobs are created.

4.11 Viewing Audit Trails

4.11.1 Viewing Key Audit Trails

1) Select **System Info » Keys**.

2) Find and select the key.

   To scan the key in the Local PD, click **Scan**.

   To search for the key, enter the search criteria and click **Search**. For more information, see Section 4.2.2 *"Searching for Keys"*, page 26.

3) For scanned keys:

   a) Click **Select**.

   b) Select the **Audit trail** tab.

   c) Click **Read audit trail**.

      This may take some time.

   d) To view the foreign audit trail, select the **Foreign audit trail** tab.

4) For keys in the search result:

   a) Click the row of a specific search result key.

   b) 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.

   c) To request a new audit trail, click **Request remote audit trail**.

      If **Approvals** is enabled (see Section 6.4 *"Editing System Settings"*, page 73), the request needs to be approved. Enter a comment to the approver and click **Send request**.

      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!
      If Approvals is not enabled, **Request remote audit trail** is automatically turned on at key hand-out and turned off at key hand-in.

See also Section 8.6 *"Audit Trails"*, page 123.

4.11.2 Viewing Cylinder Audit Trails

1) Find the cylinder and view the detailed information.

   See Section 4.4.1 *"Searching for Cylinders"*, page 35.

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 73), 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 4.4.10.1 *"Programming Cylinders Overview"*, page 40.

See also Section 8.6 *"Audit Trails"*, page 123.

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 73.

To view all key interactions with a specific cylinder, a two-step selection can be made by first selecting the keys and then the specific cylinder. All cylinder interactions of a key can be viewed in the same way.

1) Select **System Info » Audit trail archive**.

2) Specify the search criteria and click **Search**.

A list of the audit trail events is displayed containing interactions between keys, Remote PDs and cylinders.

4.11.4 Exporting Audit Trail Information

1) Select **System Info » Audit trail archive**.

A list of archived key and cylinder audit trails is displayed.

2) To search for specific audit trails, enter search criteria and click **Search**.

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 73.

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

4.11.5 Approving Audit Trail Requests

If the CLIQ system has been set up with the approval function enabled, audit trail requests need to be approved before they can be executed. A C-Key with the approver role needs to be used to log into the system to approve pending audit trail requests.

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**.

6) To reject:

   Enter an optional comment, click **Reject**.

   To view already approved or rejected jobs, select the **Approval history** tab.

4.12 Exporting Report Data

Data for employees, visitors, keys, cylinders and audit trail archive can be exported in the respective view. This export option is recommended when exporting information about these objects. For more information, see:

- Section 4.1.9 *“Exporting Employee Or Visitor Information”*, page 25
- Section 4.2.13 *“Exporting Key Information”*, page 33
- Section 4.4.12 *“Exporting Cylinder Information”*, page 43
- Section 4.11.4 *“Exporting Audit Trail Information”*, page 68

The Export report data option described here can be used to export other objects, such as Remote PDs and Key holders.

1) Select **Administration » Export report data**.

2) Select the data to export: Keys, Cylinders, Key holders, Remote PDs and Audit trails.

3) If Audit Trail Archive is selected, select the time interval.

4) Click **Export**.

   The data is opened in Excel automatically when the export is completed.

5 Setting Up Locking Systems

5.1 Locking System Setup Overview

This overview describes the work flow when setting up the locking system.

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 11.

2) Install the Master C-Key Certificate.

   See Section 5.2 *“Installing Master C-Key Certificate”*, page 70.

3) Log in to CWM.

   See Section 3.3 *“Logging In”*, page 17.

4) Set the CWM language.

   See Section 3.4 *“Setting CWM Language”*, page 18.

5) Install a licence.

   See Section 6.1.2 *“Installing Licences”*, page 72.

6) Perform Initial Configuration.

   See Section 5.3 *“Performing Initial Configuration”*, page 70.

5.2 Installing Master C-Key Certificate

If DCS integration is enabled:

- An e-mail address for the Master C-Key holder is specified in DCS. Within an hour of the locking system database preparation, an e-mail with links to the enrolment application and CWM is sent to that e-mail address.
- The number of times a Master C-Key certificate can be generated is determined by a setting in DCS.

1) See Section 3.2.1 *“C-Key Certificate Installation and Renewal Overview”*, page 12.

5.3 Performing Initial Configuration

1) Unlock the locking system. See Section 6.3 *“Unlocking the System”*, page 72.
2) Edit the system settings. See Section 6.4 *“Editing System Settings”*, page 73.
3) Set up the Remote PDs. See Section 6.5.1 *“Setting Up Remote PDs”*, page 74.
4) Create the domains. See Section 6.6.4 *“Creating And Deleting Domains”*, page 84.

5) Specify domain for the cylinders and cylinder groups. See Section 6.6.7 *“Changing Domain For Cylinders”*, page 85 and Section 6.6.8 *“Changing Domain For Cylinder Groups”*, page 86.

6) Set up access profiles. See Section 4.6.2 *“Creating and Deleting Access Profiles”*, page 46.

7) Create receipt templates for hand-out and hand-in receipts. Section 6.9 *“Managing Receipt Templates”*, page 88.

8) Create schedule templates. See Section 6.10 *“Managing Schedule Templates”*, page 89.

9) Add and delete administrator roles and adjust the role permissions as desired. See Section 6.7 *“Managing Roles and Permissions”*, page 87.

10) Issue C-Keys to the locking system administrators. See Section 6.11.7 *“Handing Out C-Keys”*, page 92.

11) Import Employee information to CWM. See Section 6.8 *“Importing Employee Information”*, page 88.

6 Configuring Locking Systems

6.1 Managing Licences

6.1.1 Viewing Licence Status and Features

1) Select **Administration » Licence**.

   Information about the currently installed licence, and the features it contains, is displayed.

To install a new licence, see Section 6.1.2 *"Installing Licences"*, page 72.

6.1.2 Installing Licences

Prerequisites:

- A new licence file is available.
  - For manual installation: Stored on a USB memory 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 » Licence**.

   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 licence automatically**.

   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.

6.2 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 need to be approved before audit trails can be collected.

     Can only be selected when first setting up the locking system.
   - **CLIQ Remote System**. Enables the use of Remote functionality.

     Can only be selected when first setting up the locking system.
   - **Supports Cylinder Groups**. Enables the use of cylinder groups.

     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 e-mails to employees and visitors, for example reminders of overdue keys.
     - **Emails after remote update**. Controls whether an e-mail listing new access information is sent to key holders after a Remote Update.
   - **Flexible revalidation enabled**. Makes it possible to set the revalidation interval per access profile and per cylinder group.

   CLIQ REMOTE

   - **Service URL**. Remote server used by CWM and Remote PDs.
   - **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 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 in the key hand out process is available.
   - **Revalidation interval**. The default setting for the key revalidation 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**. 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.
- **Default key holder language**. The language used when e-mails 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.
- **Remove audit trails older than**. Offers the possibility to automatically remove audit trails from the audit trail archive that are older than a defined number of days. The days are counted from the date when the audit trails were collected. The default value is 0, which disables the function.
- **When deleting key holders**. The option **Mark as deleted** changes the status of the key holder to "deleted" whereas **Delete permanently** removes the key holder from the database altogether. When selecting **Delete permanently** all key holders that have been marked as deleted are removed.
- **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.

6.5 Managing Remote PDs

6.5.1 Setting Up Remote PDs

1) Find the Remote PD to configure and view the detailed information.

   See Section 6.5.2 *“Searching for Remote PDs”*, page 74.

2) Edit the Remote PD information, tags and external links as desired.

   See Section 6.5.3 *“Editing Remote PD Information”*, page 75, Section 6.5.4 *“Editing Remote PD Tags”*, page 75, and Section 6.5.5 *“Editing Remote PD External Links”*, page 76.

3) Edit the Remote PD Settings and load the configuration to the Remote PD. This includes installing the certificate.

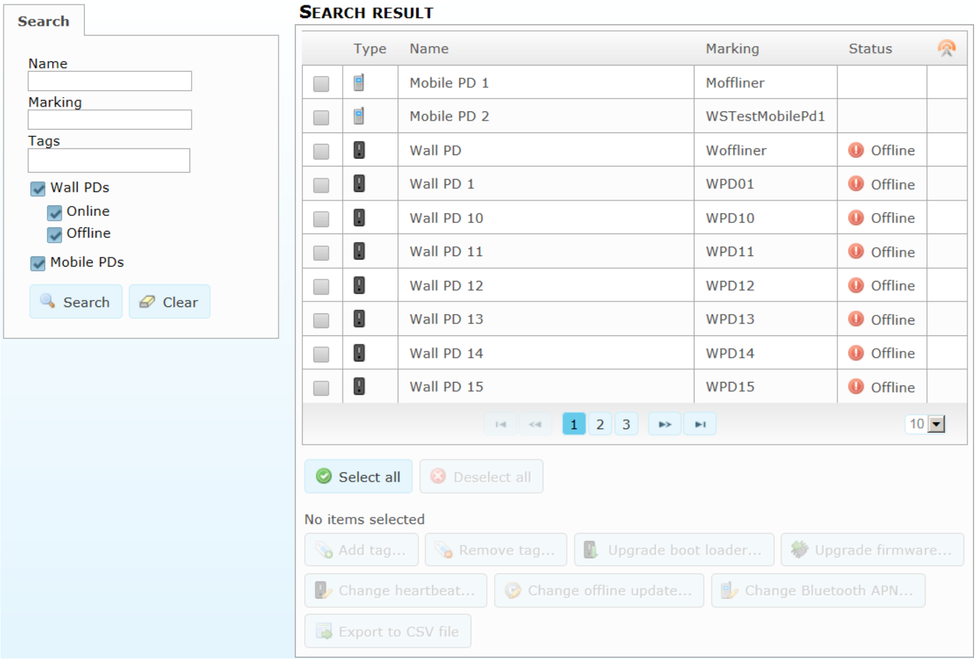
   For Wall PDs, see Section 6.5.6 *“Editing Wall PD Settings and Certificate”*, page 77.

   For Mobile PDs, see Section 6.5.7 *“Editing Mobile PD Settings and Certificate”*, page 79.

6.5.2 Searching for Remote PDs

1) Select **System Info » Remote PDs**.

   A list of Remote PDs is displayed.



Search

Name

Marking

Tags

☑ Wall PDs

☑ Online

☑ Offline

☑ Mobile PDs

Search Clear

SEARCH RESULT

	Type	Name	Marking	Status
□	📱	Mobile PD 1	Moffliner	
□	📱	Mobile PD 2	WSTestMobilePd1	
□	▮	Wall PD	Woffliner	Offline
□	▮	Wall PD 1	WPD01	Offline
□	▮	Wall PD 10	WPD10	Offline
□	▮	Wall PD 11	WPD11	Offline
□	▮	Wall PD 12	WPD12	Offline
□	▮	Wall PD 13	WPD13	Offline
□	▮	Wall PD 14	WPD14	Offline
□	▮	Wall PD 15	WPD15	Offline

1 2 3 10

Select all Deselect all

No items selected

Add tag... Remove tag... Upgrade boot loader... Upgrade firmware...

Change heartbeat... Change offline update... Change Bluetooth APN...

Export to CSV file

The following symbols are used:

▮ Wall PD

📱 Mobile PD

2) Enter the search criteria.

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**. 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 view the detailed information.

See Section 6.5.2 *"Searching for Remote PDs"*, page 74.

2) Click **Edit**.

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

4) To add tags, click **Add Tag...**. See also Section 6.5.4 *"Editing Remote PD Tags"*, page 75.

5) To add edit external links, click **Add external link...**. See also Section 6.5.5 *"Editing Remote PD External Links"*, page 76.

6) Click **Save**.

6.5.4 Editing Remote PD Tags

1) Find the Remote PD and view the detailed information.

See Section 6.5.2 *“Searching for Remote PDs”*, page 74.

2) Click **Edit**.

3) To add a tag:

   a) Click **Add tag**.

   b) Enter a name for the tag.

   c) Click **OK**.

   d) Click **Save**.

4) To remove a tag:

   a) Click the tag to be removed.

   b) Click **OK**.

   c) Click **Save**.

A tag can be edited for several Remote PDs simultaneously. Select the Remote PDs in the search result list and click **Add tags** or **Remove tags**.

See also Section 8.2.6 *“Tags”*, page 119.

6.5.5 Editing Remote PD External Links

1) Find the Remote PD and view the detailed information.

   See Section 6.5.2 *“Searching for Remote PDs”*, page 74.

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 https://).

      If a root URL has been defined in **System settings**, it is enough to add the last part of the URL. See Section 6.4 *“Editing System Settings”*, page 73.

   d) Click **OK**.

4) To remove an external link, click **Remove** on 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 121.

6.5.6 Editing Wall PD Settings and Certificate

Prerequisites:

- For a Wall PD that is configured for the first time 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).

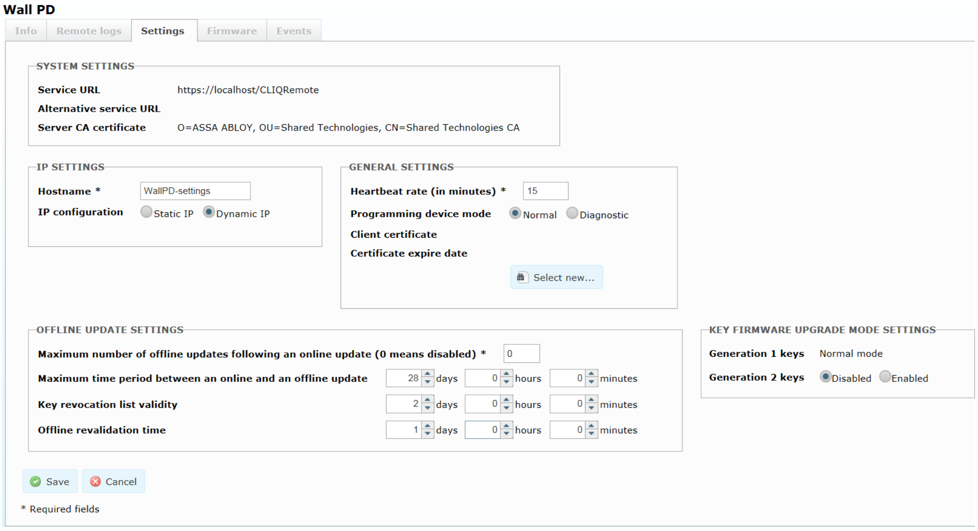
  - A USB memory formatted with the FAT32 file system. Recommended memory size is 8-16 GB.
- To use Offline Update:
  - A Wall PD with firmware 2.11 or higher.
- To install or renew certificates **without** DCS Integration:
  - A .p12 certificate file. This is obtained from the local CLIQ dealer.

1) Find the Wall PD and view the detailed information.

   See Section 6.5.2 *"Searching for Remote PDs"*, page 74.

2) Select the **Settings** tab.

3) Click **Edit**.



Wall PD

SYSTEM SETTINGS

Service URL https://localhost/CLIQRemote
Alternative service URL
Server CA certificate O=ASSA ABLOY, OU=Shared Technologies, CN=Shared Technologies CA

IP SETTINGS

Hostname * WallPD-settings
IP configuration ○ Static IP ● Dynamic IP

GENERAL SETTINGS

Heartbeat rate (in minutes) * 15
Programming device mode ● Normal ○ Diagnostic
Client certificate
Certificate expire date
Select new...

OFFLINE UPDATE SETTINGS

Maximum number of offline updates following an online update (0 means disabled) * 0
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 SETTINGS

Generation 1 keys Normal mode
Generation 2 keys ● Disabled ○ Enabled

Save Cancel

* Required fields

4) Enter **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.

5) Select **Static IP** or **Dynamic IP** for **IP configuration**.

6) If **Static IP** is selected, enter **IP address**, **Subnet mask**, **Gateway**, and **DNS**.

7) Enter **Heartbeat** frequency.

   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.

Recommended value: 15.

8) Select **Programming device mode**.

Select **Normal**. Do not select **Diagnostic** unless advised by technical support.

9) To install or renew a certificate:

a) If DCS Integration is enabled, click **Generate certificate**.

The certificate is generated.

b) If DCS Integration is not enabled:

- Click **Select new...**.
- Select the **Certificate file (.p12)** and enter the **Certificate file password**.
- Click **OK**.

10) To enable and disable key upgrades, see Section 6.5.9 *"Enabling and disabling key upgrades in Remote PDs"*, page 82.

11) Click **Save**.

12) To configure Offline Update:

See also Section 8.3.3 *"Offline Update"*, page 120.

> **NOTE!**
> To update a key in offline mode the key must have firmware version 6 or higher.

a) Enter **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.

b) Enter **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.

c) Enter **Maximum time a key revocation list is valid**.

Specifies how old the Key Revocation List stored in the Wall PD can be and still allow offline updates. See also Section 8.3.3 *"Offline Update"*, page 120.

d) Enter **Offline revalidation time**.

Specifies for how long time the key validity is extended. The revalidation interval set on keys is ignored at offline updates.

13) Transfer the updated configuration to the PD.

a) If the Wall PD is online or can connect with its current settings:

Click **Encrypt and send**.

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.

b) If the PD is configured for the first time, or cannot connect with the current settings:

- Insert a USB memory into the client computer.
- Click **Encrypt and save** and save the file to the root folder of the USB memory.

> **NOTE!**
>
> Make sure there are no other files than configuration files in root folder of the USB memory.
>
> There can be several configuration files on the same USB memory.

- Use the USB OTG cable to connect the USB memory to the Wall PD.

  The PD is configured automatically and connects to the Remote Server. This should take less than a minute.

14) Check that CLIQ LED lights up continuously.

This means that the PD is online and correctly configured.

See also Section 9.5 *“Remote PD Indications”*, page 136.

6.5.7 Editing Mobile PD Settings and Certificate

Prerequisites:

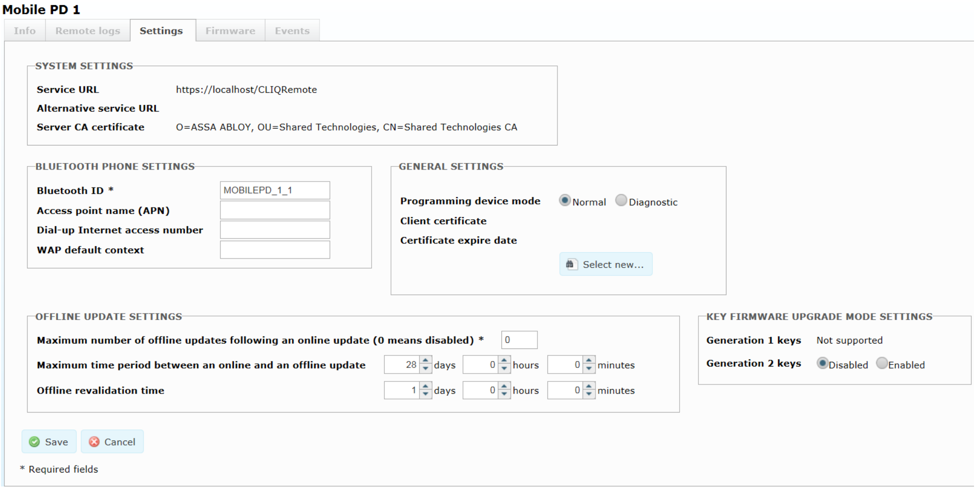
- For use with an iPhone or Android mobile phone:
  - A Mobile PD with firmware version 2.10 or higher.
- For a Mobile PD that is configured for the first time or cannot connect with the existing settings,
  - A USB On-The-Go (OTG) cable: USB Mini Male (both type A and B supported) to USB Standard Female (type A).

  - A USB memory formatted with the FAT32 file system. The recommended memory size is 8-16 GB.
- To use Offline Update:
  - A 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 Mobile PD is available.

1) Find the Mobile PD and view the detailed information.

   See Section 6.5.2 *“Searching for Remote PDs”*, page 74.

2) Select the **Settings** tab.
3) Click **Edit**.



Mobile PD 1

SYSTEM SETTINGS

Service URL https://localhost/CLIQRemote

Alternative service URL

Server CA certificate O=ASSA ABLOY, OU=Shared Technologies, CN=Shared Technologies CA

BLUETOOTH PHONE SETTINGS

Bluetooth ID * MOBILEPD_1_1

Access point name (APN)

Dial-up Internet access number

WAP default context

GENERAL SETTINGS

Programming device mode ● Normal ○ Diagnostic

Client certificate

Certificate expire date

OFFLINE UPDATE SETTINGS

Maximum number of offline updates following an online update (0 means disabled) * 0

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 SETTINGS

Generation 1 keys Not supported

Generation 2 keys ● Disabled ○ Enabled

* Required fields

4) To configure the Mobile PD for use with a mobile phone, configure the **BLUETOOTH PHONE SETTINGS** as described below.

Regardless of how the **BLUETOOTH PHONE SETTINGS** are configured, the Mobile PD can always be used with a computer connected with a USB cable.

a) For use with

- iPhone
- Android
- Other mobile phone supporting the PAN Bluetooth profile

Leave all fields in **BLUETOOTH PHONE SETTINGS** blank.

b) For use with a mobile telephone that supports the DUN Bluetooth profile, enter the following:

- **Bluetooth ID**

  A name of the Mobile PD. This name will be visible in the Mobile Phone when pairing with the 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`.

5) Select **Programming device mode**.

Select **Normal**. Do not select **Diagnostic** unless advised by technical support.

6) To install or renew a certificate:

a) If DCS Integration is enabled, click **Generate certificate**.

The certificate is generated.

b) If DCS Integration is not enabled:

- Click **Select new...**.
- Select the **Certificate file (.p12)** and enter the **Certificate file password**.
- Click **OK**.

7) To configure Offline Update:

> **NOTE!**
> To update a key in offline mode the key must:
>
> - recently have been updated in the same Mobile PD (be within the last 10 updated keys).
> - have firmware version 6 or higher.

a) Enter **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.

b) Enter **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.

c) Enter **Offline revalidation time**.

Specifies for how long time the key validity is extended. The revalidation interval set on keys is ignored at offline updates.

8) To enable and disable key upgrades, see Section 6.5.9 *"Enabling and disabling key upgrades in Remote PDs"*, page 82.

9) Click **Save**.

10) Transfer the updated configuration to the PD.

a) If the Mobile PD has been configured before and can connect with the current settings:

Click **Encrypt and send**.

The updated settings are sent to the 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.

b) If the PD is configured for the first time, or cannot connect with the current settings:

- Insert a USB memory into the client computer.
- Click **Encrypt and save** and save the file to the root folder of the USB memory.

> **NOTE!**
> Make sure there are no other files than configuration files in root folder of the USB memory.
>
> There can be several configuration files on the same USB memory.

- Use the USB OTG cable to connect the USB memory to the Mobile PD.

- Insert a user key into the Mobile PD.
  Configuration of the Mobile PD is initiated.
- When the Download LED lights up continuously, remove the USB memory.

  ⤓

11) To configure a mobile phone to use with the Mobile PD, see separate documentation supplied with the Mobile PD.

12) To configure a computer for use with the 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 Mobile PD.

13) To verify that the configuration is correct:

    a) Insert a user key into the 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 *"Remote PD Indications"*, page 136.

6.5.8 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 view the detailed information.

   See Section 6.5.2 *"Searching for Remote PDs"*, page 74.

2) Select the **Event log** tab.

6.5.9 Enabling and disabling key upgrades in Remote PDs

For information about how to upgrade keys, including what firmware versions to use, see Section 6.14.2 *"Upgrading Firmware on Keys"*, page 97.

1) Find the Remote PD and view the detailed information.

   See Section 6.5.2 *"Searching for Remote PDs"*, page 74.

2) Select the **Settings** tab.

3) For upgrading generation 1 keys:

   a) 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 6.14.2 *"Upgrading Firmware on Keys"*, page 97.

   b) To disable key upgrades:

      - Under the **Key firmware upgrade mode settings**, click **Switch to normal mode**.

4) For upgrading generation 2 keys:

   a) To enable key upgrades:

      - Click **Edit**.
      - Under the **Key firmware upgrade mode settings**, select **Enabled**.
      - Click **Save**.

      > **NOTE!**
      > Multiple Remote PDs can be selected for upgrading generation 2 keys. Repeat *Step 5.d* for each Remote PD that is intended for upgrading keys.

   b) To disable key upgrades:

      - Click **Edit**.
      - Under the **Key firmware upgrade mode settings**, select **Disabled**.
      - Click **Save**.

6.5.10 Exporting Remote PD Information

1) Search for the Remote PDs.

   See Section 6.11.1 *“Searching for C-Keys”*, page 89.

2) From the search results, select the Remote PDs whose data should be exported.

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 73.

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

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.

   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 83.

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)

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:

   > **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 22.

   a) Find the domain and view the detailed information.

      See Section 6.6.1 *“Searching For Domains”*, page 83.

   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 113.

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 22.

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 113.

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 86.

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 113.

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 85.

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 113.

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 45.

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

1) Select **Administration » Roles**.

   A list of existing roles is displayed.

   Some of the roles are predefined in CWM:

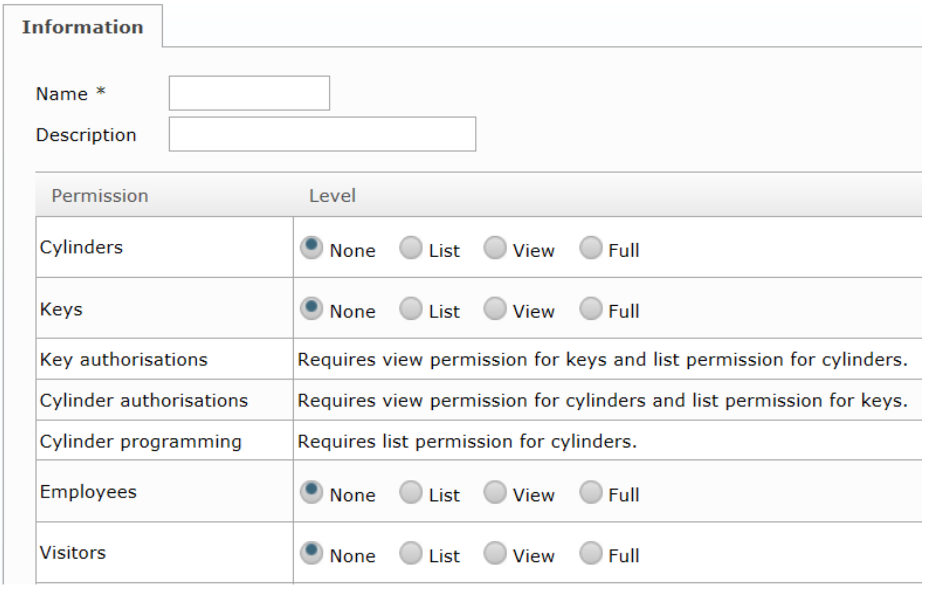
   The **Super administrator**, **Approver** and **WebService** roles are read only and cannot be edited.

2) To create a role:

   a) Click **Create new**.

   b) Enter a **Name** and a possible **Description**.

   c) Select permissions in the list.



Information

Name *

Description

Permission	Level
Cylinders	● None ○ List ○ View ○ Full
Keys	● None ○ List ○ View ○ Full
Key authorisations	Requires view permission for keys and list permission for cylinders.
Cylinder authorisations	Requires view permission for cylinders and list permission for keys.
Cylinder programming	Requires list permission for cylinders.
Employees	● None ○ List ○ View ○ Full
Visitors	● None ○ List ○ View ○ Full

   d) Click **Save**.

3) To edit an existing role:

   a) Click the row of a specific role.

   b) Click Edit to update the **Name**, **Description** or **Permissions** of the role.

   c) Click **Save**.

4) To delete a role:

   a) Click the row of a specific role.

   b) Click **Delete**.

   c) Click **OK**.

      Roles that have members connected to the role cannot be deleted.

5) To view C-Key members of a role:

   a) Click the row of a specific role.

   b) Select the **Members** tab.

See also:

- Section 8.7 *“CWM Roles and Permissions”*, page 124
- Section 9.4 *“Permissions”*, page 131

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 139. The exact specifications are subject to change and it is therefore recommended to upload the file for validation.

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 for receipts printed during hand out and hand in for visitors and employees can be edited. Receipts are created as PDFs which can either be printed or saved.

Prerequisites:

- The logo is an image file with an RGB color profile (CMYK is not supported).

1) Select **Administration » Receipt templates**.

2) To change logo:

   a) Click **Change logo**.

   b) Select a local file.

   c) Click **Upload**.

3) To update the hand out or hand in receipt text for employees:

   a) Select the **Employee hand out** tab or **Employee hand in** tab.

   b) Click **Edit**.

   c) Update the text.

   d) Click **Save**.

4) To update the hand out receipt text for visitors:

   a) Select the **Visitor hand out** tab or **Visitor hand in** tab.

   b) Click **Edit**.

   c) Update the text.

   d) Click **Save**.

5) To preview the receipt, click **Preview**.

6.10 Managing Schedule Templates

There are two types of schedule templates, Basic Schedule template and Multi Time Period Schedule template. 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 137.

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**.
   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 112.

6.11 Managing C-Keys

6.11.1 Searching for C-Keys

1) Select **Administration » C-keys**.
2) Enter the search criteria.

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 9.3.2 *"C-Key Attributes"*, page 130.

6.11.2 Scanning a C-Key

1) Select **Administration » C-keys**.

2) Insert the C-Key into the right slot of the Local PD.

3) Under **Programming Device**, click **Scan**.

Basic information about the C-Key is displayed.

4) To view detailed information about the C-Key, click **Show**.

For information about the C-Key attributes, see Section 9.3.2 *"C-Key Attributes"*, page 130.

6.11.3 Editing C-Key Information

1) 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 89

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 90

2) Click **Edit**.

3) To edit the C-Key name, update the field **Name**.

4) To block the C-Key, select **Block**.

5) To change if certificate enrolment is allowed, select **Always Allowed**, **Allowed once**, or **Not Allowed**.

See also Section 8.8 *"DCS Integration"*, page 125.

6) To change the C-Key authorisation role, select the role.

7) Click **Save**.

6.11.4 Changing C-Key PIN Code

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**.

> **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.

6.11.5 Selecting C-Key Domains

1) Select **Administration » C-keys**.

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 89

   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 90

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.

   To search for the C-Key and display the detailed information view, see Section 6.11.1 *"Searching for C-Keys"*, page 89

   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 90

2) Select the **Events** tab.

   A list with all C-Key events is displayed.

6.11.7 Handing Out C-Keys

1) Select **Administration » C-Keys**.
2) Insert the C-Key to be handed out in the right slot of the Local PD.
3) Click **Scan**.
4) Click **Show** for the C-Key in the right slot (the C-Key to hand out).
5) To set or change authorisation roles:
   a) Click **Edit**.
   b) Select **Authorisation roles**.
   c) Click **Save**.
6) To set a new PIN:
   a) Click **Set new PIN**.
   b) Enter **Master c-key PIN**.
   c) Enter the new PIN in **New PIN**.
   d) Enter the new PIN again in **Confirm new PIN**.
7) Click **Hand out to employee**.
8) Click **Select** for the employee to hand out the key to.

   The C-Key has now been handed out. To be able to log in to CWM, the employee needs to install a certificate for the key. If DCS Integration is enabled, and if the employee has an e-mail address registered, an email will be sent to the employee with a link to the Certificate Enrolment Application.

6.11.8 Handing In C-Keys

1) Find the key.

   To search for the C-Key and display the detailed information view, see Section 6.11.1 *"Searching for C-Keys"*, page 89

   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 90

2) Click **Hand in c-key**.

   The C-Key can no longer be used to log in to CWM.

6.11.9 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. After 25 attempts of entering the wrong PUK, the C-Key becomes unusable and has to be replaced with a new C-Key.

1) Select **Settings » C-key settings**.
2) Enter **PUK**.
3) Enter **New PIN**.
4) Enter **Confirm new PIN**.

6.11.10 Reporting C-Key Lost, Found or Broken

1) Find the C-Key and display the detailed information view.

   See Section 6.11.1 *"Searching for C-Keys"*, page 89.

2) To report the C-Key lost:
   a) Click **Report lost**.
   b) Select in which cylinders to block the key.
   c) Click **Next**.
   d) Select a **Priority**.

      Urgent jobs should have a high priority level.
   e) Click **Apply**.
   f) To perform the Cylinder Programming Jobs, see Section 4.4.10.1 *"Programming Cylinders Overview"*, page 40.

3) To report the C-Key found:

   NOTE!
   To report a C-Key found the Master C-Key must be used.

   a) Click **Report found**.
   b) Click **OK**.

      Any existing Cylinder Programming Jobs to unauthorise the C-Key that are not yet executed are removed. The C-Key authorisations that have been removed from cylinders through executed Cylinder Programming Jobs need to be programmed to the cylinders again.

4) To report C-Key broken:
   a) Click **Report broken**.
   b) Click **OK**.

6.11.11 Listing C-Key Certificates

1) Find the C-Key with the certificates to show.

   To search for the C-Key and display the detailed information view, see Section 6.11.1 *"Searching for C-Keys"*, page 89

   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 90

2) Select the **Certificates** tab.

6.11.12 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 3.2.1 *"C-Key Certificate Installation and Renewal Overview"*, page 12.

1) Find the C-Key with the certificates to revoke.

   To search for the C-Key and display the detailed information view, see Section 6.11.1 *"Searching for C-Keys"*, page 89

   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 90

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.

6.11.13 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, or an e-mail from DCS with a link to the Enrolment application.
  - 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 70.

2) Lock CWM for maintenance.

   See Section 6.2 *"Locking the System for Maintenance"*, page 72.

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.

   IMPORTANT!
   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.

6.11.14 Exporting C-Key Information

1) Search for the C-Keys.

   See Section 6.11.1 *"Searching for C-Keys"*, page 89.

2) From the search results, select the C-Keys whose data should be exported.

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 73.

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

6.12 Changing Cylinder Group for Cylinders

1) Find the cylinder and view the detailed information.

   See Section 4.4.1 *"Searching for Cylinders"*, page 35.

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 Checking 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 e-mail server.

3) Select the **History** tab to view the past changes in online, offline statuses of Remote PDs, the remote server and e-mail 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 Upgrading Firmware

6.14.1 Upgrading Firmware for Remote PDs

To upgrade a Remote PD, CWM must be provided with firmware. This is done by uploading a local firmware file that is provided by the local CLIQ dealer. For systems with DCS Integration, firmware files are automatically fetched from DCS. Once imported to CWM, Remote PD firmware can either be upgraded through CWM or via a USB memory.

1) To upload a local firmware file to a system 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.

2) To import the new firmware:

   a) Select **Administration » Firmware**.

   b) Click **Import firmware**.

   If successful, a summary of the imported firmware is displayed in a new panel.

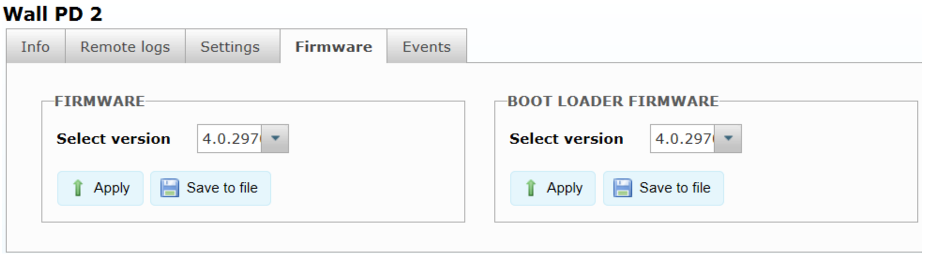
> **NOTE!**
> For systems with DCS Integration enabled, firmware files are automatically fetched from DCS and listed among the imported firmware that is ready for activation.

3) To upgrade firmware for online Remote PDs through CWM:

   a) Select **System info » Remote PDs**.

   b) Click the row of the Remote PD to be upgraded.

   c) Select the **Firmware** tab.



FIRMWARE: Select version 4.0.297

BOOT LOADER FIRMWARE: Select version 4.0.297

   d) For boot loader firmware upgrade: Under **BOOT LOADER FIRMWARE**, select firmware version and click **Apply**.

   e) For firmware upgrade: Under **FIRMWARE**, select firmware version and click **Apply**.

   f) For Mobile PDs, insert a user key to power on the Mobile PD and activate the upgrade.

   The Wall PD firmware is upgraded at the next heartbeat (next time it connects to the remote server).

   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 *"Remote PD Indications"*, page 136.

4) To upgrade firmware for offline Remote PDs via a USB memory:

> **NOTE!**
> The USB memory must be formatted with the FAT32 file system and the recommended memory size is 8-16 GB. It must not contain any other files.

a) Select **System info » Remote PDs**.

b) Click the row of the Remote PD to be upgraded.

c) Select the **Firmware** tab.

d) For boot loader firmware upgrade: Under **BOOT LOADER FIRMWARE**, select firmware version and click **Save to file**.

Save the file to the root of the USB memory.

e) For firmware upgrade: Under **FIRMWARE**, select firmware version and click **Save to file**.

Save the file to the root of the USB memory.

f) Connect the USB to the Remote PD using a USB On-The-Go cable.

g) For Mobile PDs, insert a user key to power on the Mobile PD and activate the upgrade.

For 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 more information about Remote PD indications, see Section 9.5 *“Remote PD Indications”*, page 136.

6.14.2 Upgrading Firmware on Keys

To upgrade a key, CWM must be provided with firmware. This is done by uploading a local firmware file that is provided by the local CLIQ dealer. For systems with DCS Integration, firmware files are automatically fetched from DCS. Once imported, the firmware is updated through CWM using a Remote PD configured as an updater PD.

Table 1. Type of Remote PD to use for upgrading keys

Key version	Remote PD	Remote PD firmware version
Generation 1	Wall PD	Wall PD firmware 2.9 or higher Wall PD key updater firmware 2.9 or higher
Generation 2	Wall PD or Mobile PD	Wall PD or Mobile PD firmware 4.0 or higher

The key generation is visible in the detailed key view, see Section 4.2.1 *“Scanning a Key”*, page 26 or Section 4.2.2 *“Searching for Keys”*, page 26.

To upgrade firmware on keys:

1) Save the new firmware locally on the computer.

2) Select **Administration » Firmware**.

3) To 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 imported 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:
>
> - Wall PD boot loader firmware
> - Wall PD firmware, version 2.9 or higher
> - Wall PD key updater firmware, version 2.9 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 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 74.

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 6.14.1 *“Upgrading Firmware for Remote PDs”*, page 96.

d) Enable key upgrades in the Wall PD, see Section 6.5.9 *“Enabling and disabling key upgrades in Remote PDs”*, page 82.

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 *“Remote PD Indications”*, page 136.

- 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 6.5.9 *"Enabling and disabling key upgrades in Remote PDs"*, page 82.

   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 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 74.

   c) If the Remote PD firmware needs to be upgraded, see Section 6.14.1 *"Upgrading Firmware for Remote PDs"*, page 96.

   d) Enable key upgrades in the Remote PD, see Section 6.5.9 *"Enabling and disabling key upgrades in Remote PDs"*, page 82.

   e) Select **Administration » Firmware**.

   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.d* 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) For each of the user keys to be upgraded:

      - Insert the key in the Remote PD that has been enabled for key upgrade.
        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 Remote PD indicates that updates are finished. For information about Remote PD indications, see Section 9.5 *"Remote PD Indications"*, page 136.
      - Remove the key from the Remote 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.

6.15 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. For systems with DCS Integration, extension import files are automatically fetched from DCS. The DCS fetch can also be forced by manually clicking a button. Once uploaded, the extension import must be activated.

1) To upload a local extension import file:

    a) Select **Administration » Extension import » Upload or fetch extension import file(s)**.

    b) Click **Select** to find the locally saved extension import file on the computer.

    > **NOTE!**
    > Extension import files have the suffix ".cws".

    c) Click **Open**.

    d) Click **Upload**.

    The extension import file is uploaded to the Web Manager Server and validated.

2) To manually fetch an extension import file from DCS, click **Fetch extension import file(s)**.

    A status note about the fetching process is displayed.

3) To 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 e-mail 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 along with information on how many keys, key groups, cylinders, cylinder groups and Remote PDs there are to activate.

    b) 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 note is displayed on the homepage of CWM.

7 CLIQ Hardware

7.1 CLIQ Architecture

The basic architecture of a CLIQ system is shown in Figure 1 *"CLIQ Architecture"*, page 101.

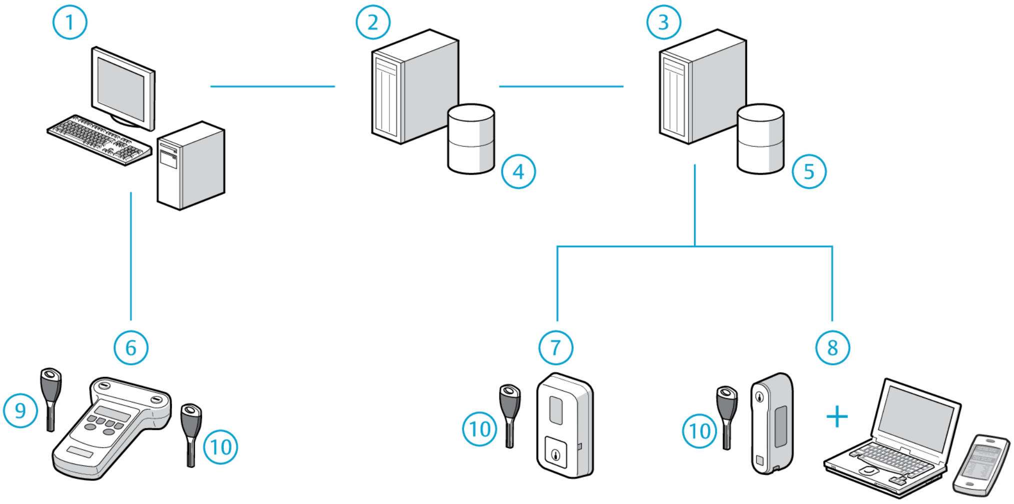


Figure 1. CLIQ Architecture

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 104.
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 105.
8. **Mobile 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 105.
9. **C-Keys**. See Section 7.2.3 *"C-Keys"*, page 102.
10. **User Keys**. See Section 7.2.2 *"User Keys"*, page 102.

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.

See also Section 7.2.2 *"User Keys"*, page 102 and Section 7.2.3 *"C-Keys"*, page 102.

7.2.2 User Keys

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

Mechanical Key

Is a traditional key without electronic components. Can be managed in CWM but cannot be used with CLIQ cylinders.

Dynamic 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 8.1.3 *"Electronic Authorisation"*, page 107).

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 8.1.5 *"Key Validity"*, page 109). It can also be programmed to have access to cylinders based on a schedule (see Section 8.1.8 *"Key Schedules"*, page 112).

This key type can also store a key access list of cylinders and cylinder groups that the key is authorised to open (see Section 8.1.3 *"Electronic Authorisation"*, page 107). This is useful in remote systems since it enables access to be controlled by keys, which are easily updated in Remote PDs.

See also Section 8.1 *"Authorisation Principles"*, page 107.

7.2.3 C-Keys

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

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 8.7 *"CWM Roles and Permissions"*, page 124).

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 89 or Section 6.11.2 *"Scanning a C-Key"*, page 90.

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 89 or Section 6.11.2 *"Scanning a C-Key"*, page 90. 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 11). Each C-Key also has its own PIN code and PUK code.

7.2.4 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 4.2.1 *"Scanning a Key"*, page 26 or Section 4.2.2 *"Searching for Keys"*, page 26.

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)

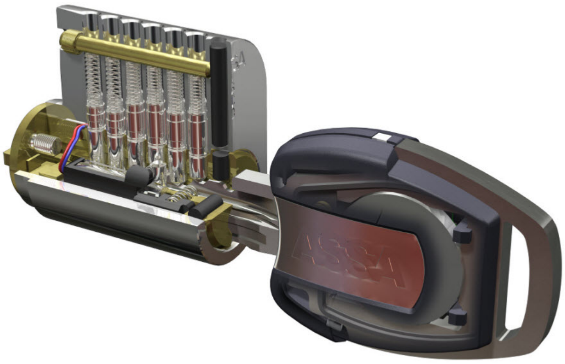


Figure 2. CLIQ Cylinder

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.

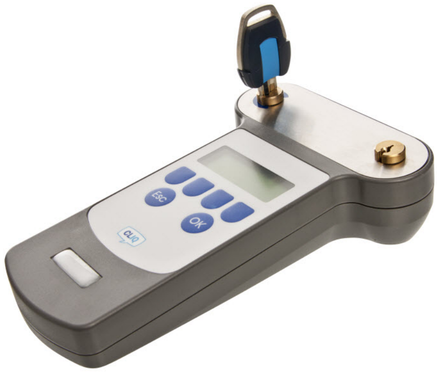


Figure 3. Local Programming Device

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 either the USB port or the serial port.

The Local PD has four ports:

- A serial port
- A USB port
- A port for external power supply (not needed when connecting the Local PD with USB)
- 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 and they are locking system specific.

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 *"Remote PD Indications"*, page 136.

If **Offline Update** is enabled, a key can be revalidated through a Remote PD even if it has temporarily lost its network connection. See also Section 8.1.6 *"Key Revalidation"*, page 109.

Wall PDs
The Wall PD is typically mounted on the wall. It is connected to the remote server via Ethernet.

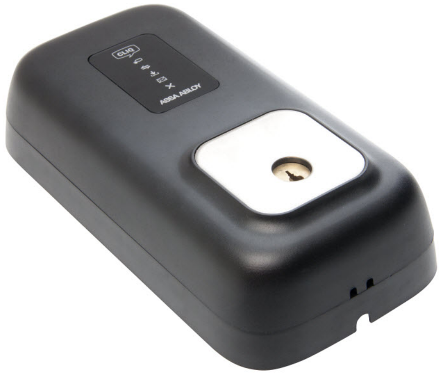


Figure 4. Wall Programming Device

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.

Mobile PDs
The Mobile PD is a personal programming unit. There are two types of Mobile PDs:

- Mobile PDs that connect to a computer via a USB cable to use the computer's Internet connection.
- Mobile PDs that can connect either to a computer via a USB cable, or to a mobile phone via Bluetooth to use the mobile phone's Internet connection.

The Mobile PD needs battery power when connecting with a mobile phone. When the Mobile PD is used with a computer, a special application, **ASSA ABLOY Network Provider**, must be installed on the computer.

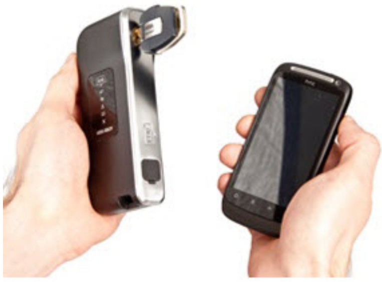


Figure 5. Mobile Programming Device

8 CLIQ Concepts and Features

8.1 Authorisation Principles

8.1.1 Authorisation Principles Overview

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

- The mechanical code is correct. See Section 8.1.2 *"Mechanical Authorisation"*, page 107.
- 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 8.1.5 *"Key Validity"*, page 109.
- The cylinder is electronically programmed to give the key access. See Section 8.1.3 *"Electronic Authorisation"*, page 107.
- For Dynamic Keys: The key has been programmed to have access to the cylinder. See Section 8.1.3 *"Electronic Authorisation"*, page 107.
- For Dynamic Keys: The key schedule allows access at the current time. See Section 8.1.8 *"Key Schedules"*, page 112.

8.1.2 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.

8.1.3 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.

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 6 *"Key access list"*, page 108 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

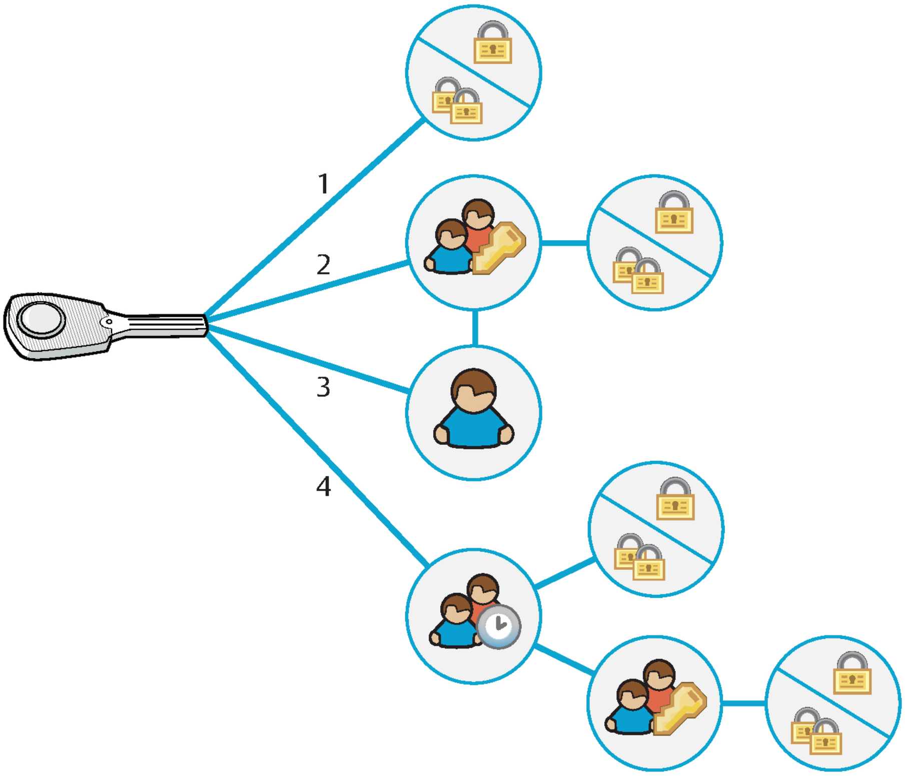


Figure 6. Key access list

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 120.

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.

8.1.4 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 115.

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 115 and Section 8.2.5 *"Temporary Access Groups"*, page 117.

8.1.5 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 112.

There are two ways to control the validity of a key:

- **Activation settings**. A key can be set to be **Inactive**, **Always active**, or **Active between selected dates**.

  Active between selected dates is only available for Dynamic Keys.

  See also Section 4.10.1 *“Configuring Key Validity and Revalidation”*, page 62.
- **Revalidation**, an optional feature. With Revalidation, keys must be inserted in a Remote PD at specified time intervals to stay active.

  See also Section 8.1.6 *“Key Revalidation”*, page 109.

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).

8.1.6 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 inserted in a Remote PD ("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 7 *“Key revalidation”*, page 110 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.

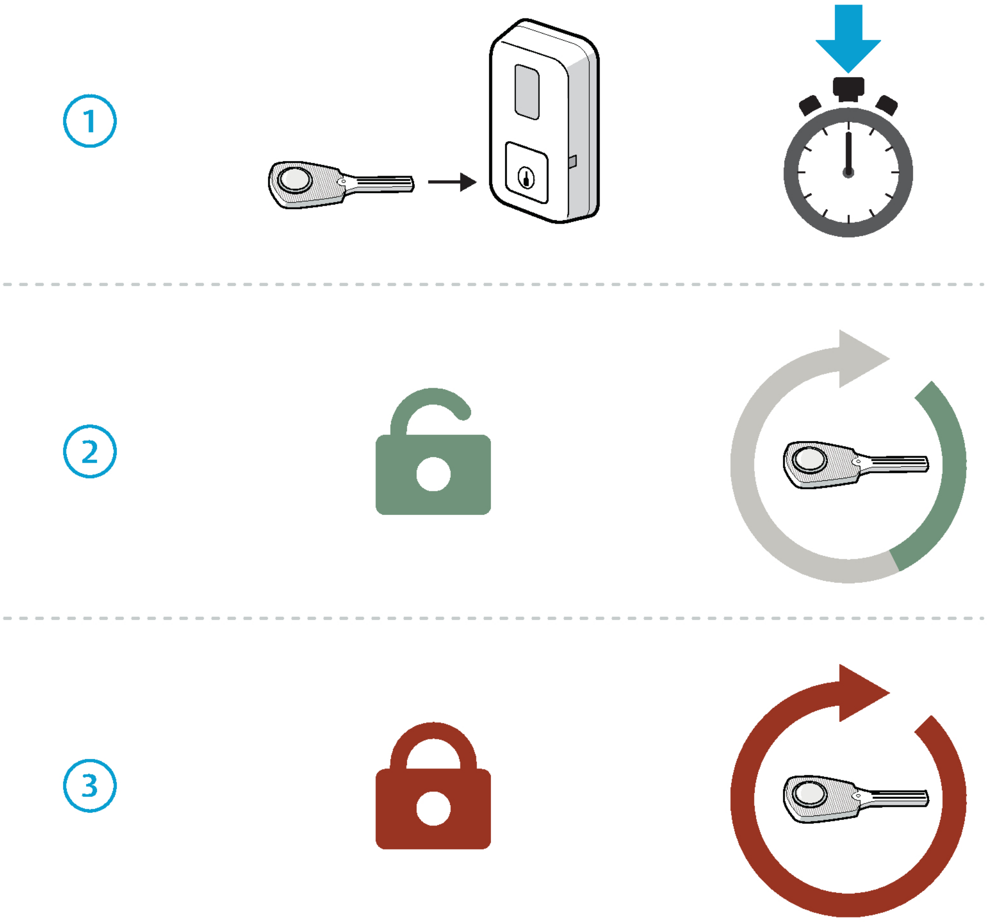


Figure 7. Key revalidation

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.

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.

See also Section 4.10.1 *“Configuring Key Validity and Revalidation”*, page 62.

Flexible Revalidation is an advanced feature that helps deal with the trade-off issue. See Section 8.1.7 *“Flexible Revalidation”*, page 111.

The **Offline Update** function in Remote PDs enables key revalidation even if the Remote PD has temporarily lost its Internet connection. See Section 8.3.3 *“Offline Update”*, page 120.

8.1.7 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 8.1.6 *“Key Revalidation”*, page 109.

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.

IMPORTANT!

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 and Revalidation”*, page 62.
- **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 64.

- **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 64.

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.

8.1.8 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 137.

- 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 65 and Section 6.10 *"Managing Schedule Templates"*, page 89.

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:

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 66.

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 6.11.7 *“Handing Out C-Keys”*, page 92.

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 137.

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 8 *"Access profiles"*, page 116 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).

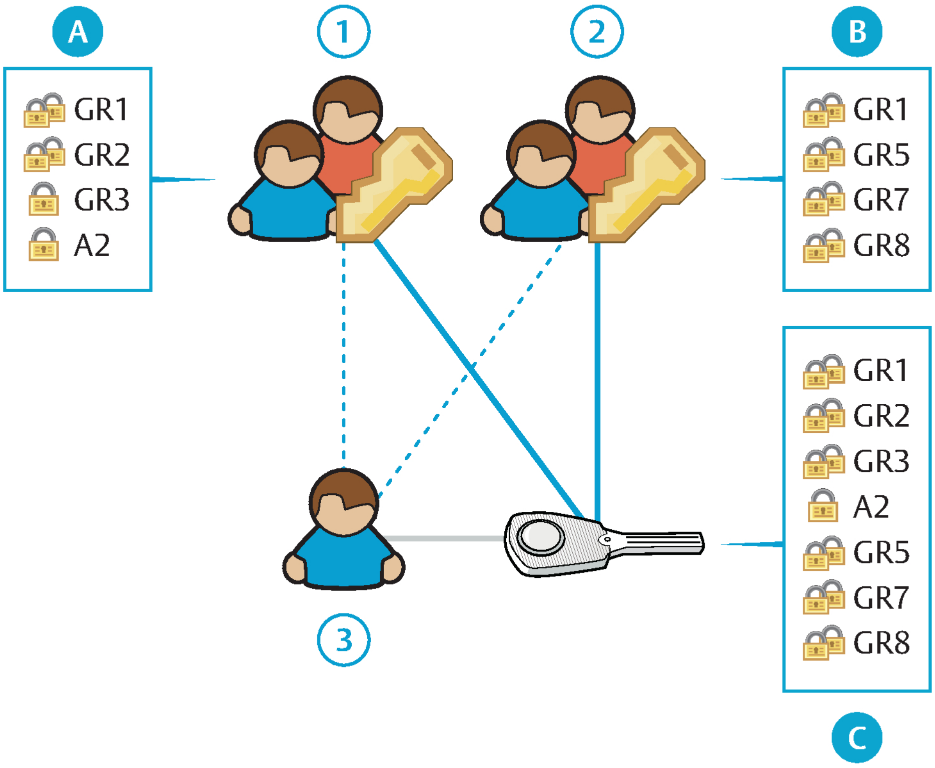


Figure 8. Access profiles

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 127.

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 4.6.7 *"Removing Redundant Key Authorisations"*, page 48.

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 9 *"Temporary Access Groups"*, page 118 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).

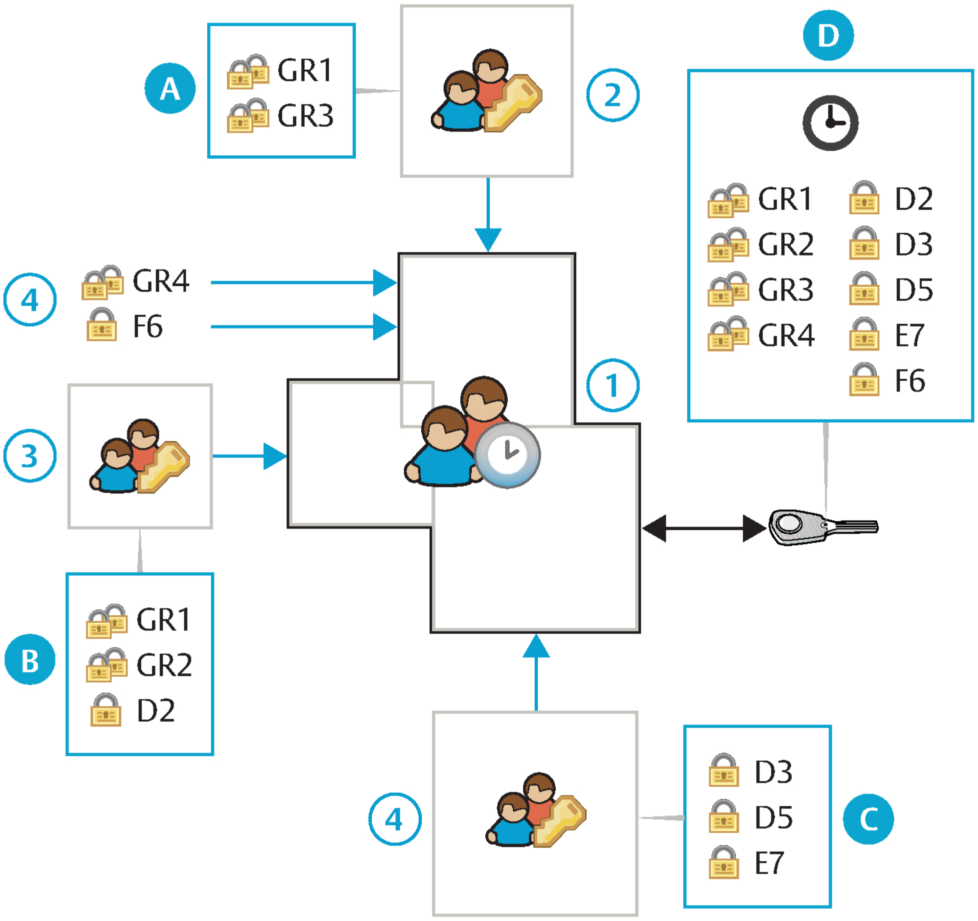


Figure 9. Temporary Access Groups

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 8.1.5 *“Key Validity”*, page 109.
- Activate key **Revalidation**, see Section 8.1.6 *“Key Revalidation”*, page 109.

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 can be used on the following objects:

- Employees (see Section 4.1.5 *"Editing Employee or Visitor Tags"*, page 24)
- Visitors (see Section 4.1.5 *"Editing Employee or Visitor Tags"*, page 24)
- Keys (see Section 4.2.4 *"Editing Key Tags"*, page 27)
- Key groups (see Section 4.3.3 *"Editing Key Group Tags"*, page 35)
- Cylinders (see Section 4.4.3 *"Editing Cylinder Tags"*, page 37)
- Cylinder groups (see Section 4.5.3 *"Editing Cylinder Group Tags"*, page 44)
- Access profiles (see Section 4.6.4 *"Editing Access Profile Tags"*, page 47)
- Remote PDs (see Section 6.5.4 *"Editing Remote PD Tags"*, page 75)

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 the 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 8.1.6 *"Key Revalidation"*, page 109.

See also Section 8.3.2 *"Remote Update"*, page 120.

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 121.

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 120.

Some types of Remote Update Jobs can be set to expire at a specific date. If the key is not updated by that date, the job is cancelled automatically and the key keeps its old configuration.

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 55.

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 e-mail about this is sent to all administrators that have the full **Key authorisations** permission and that have an e-mail 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 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 Mobile PDs

Only keys that have recently been updated in the same Mobile PD (keys that are within the last 10 updated keys) may be revalidated in offline mode.

See also Section 8.1.6 *“Key Revalidation”*, page 109.

To configure Offline Update, see Section 6.5.6 *“Editing Wall PD Settings and Certificate”*, page 77 and Section 6.5.7 *“Editing Mobile PD Settings and Certificate”*, page 79.

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 4.1.6 *“Editing Employee or Visitor External Links”*, page 24)
- Visitors (see Section 4.1.6 *“Editing Employee or Visitor External Links”*, page 24)
- Keys (see Section 4.2.5 *“Editing Key External Links”*, page 28)
- Cylinders (see Section 4.4.4 *“Editing Cylinder External Links”*, page 37)
- Access profiles (see Section 4.6.5 *“Editing Access Profile External Links”*, page 47)
- Remote PDs (see Section 6.5.5 *“Editing Remote PD External Links”*, page 76)

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 10 *"Cylinder programming"*, page 122 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 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 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.

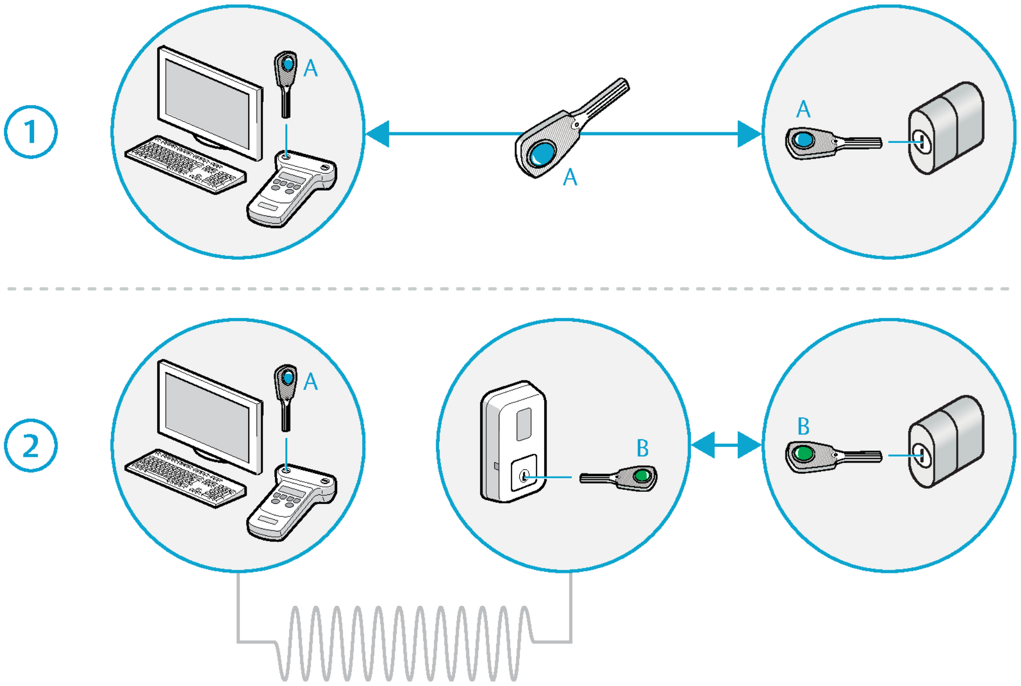


Figure 10. Cylinder programming

Throughout CWM, the following symbols are used for Cylinder Programming Jobs:

⚙ Cylinder Programming Job exists

⚙ Cylinder Programming Job needs approval

⚙ Cylinder Programming Job is programmed to C-Key

⚙ Cylinder Programming Job is finished

⚙ Cylinder Programming Job has failed or been cancelled

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 89 or Section 6.11.2 *"Scanning a C-Key"*, page 90. In systems initially delivered as cylinder group systems, all C-keys have this capability.

See also Section 4.4.10.1 *"Programming Cylinders Overview"*, page 40 and Section 8.7 *"CWM Roles and Permissions"*, page 124.

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 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 4.4.9 *"Requesting Cylinder Reprogramming"*, page 40.

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.

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

Key Audit Trails

The key audit trail records the cylinders the key has attempted to access, as well as the programming jobs that have been performed on the key. It also records the time and the outcome of these events.

Cylinder Audit Trails

The cylinder audit trail records which keys have attempted access, as well as the programming jobs that have been performed. It also records the time and the outcome of these events.

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 8.7 *"CWM Roles and Permissions"*, page 124.

8.7 CWM Roles and Permissions

A **Role** defines the CWM functions a locking system administrator is allowed to perform.

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.
Cylinder Programmer	Permissions only to execute cylinder programming.
WebService	Used for Web services integration.

Roles can be added and removed and the permissions for a role can be edited. The Super Administrator and the Approver roles cannot be deleted or edited. The WebService role can be edited but not deleted.

NOTE!
Some rights for C-Keys depend on the C-Key type and are not configurable through roles and permissions. See Section 7.2.3 *“C-Keys”*, page 102.

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 131.

See also Section 6.7 *“Managing Roles and Permissions”*, page 87.

8.8 DCS Integration

DCS is a server application for managing certificates and licences in a CLIQ locking system.

DCS Integration is an optional feature in CWM. It 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 is activated during the system installation.

With DCS Integration enabled, Remote PD certificates are generated from within CWM, while C-Key certificates are generated through the **Enrolment Application**. The Enrolment Application is a web application that is installed during system installation.

C-Key certificate enrolment can be set to be **Always Allowed**, **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 6.11.3 *"Editing C-Key Information"*, page 90).

Table 4. Certificate Enrolment Setting

Setting	Description
Always Allowed	The enrolment link in the enrolment e-mail can be used to install many certificates. This is useful if the C-Key holder needs to access CWM from more than one computer.
Allowed once	The enrolment link in the enrolment e-mail can be used only once.
Not Allowed	Enrolment is not allowed.

NOTE!
Certificate renewal is allowed regardless of this setting.

To generate C-Key certificates, see Section 3.2.2 *"Installing C-Key Certificate with DCS (Internet Explorer)"*, page 13 or Section 3.2.3 *"Installing C-Key Certificate with DCS (Firefox)"*, page 14.

To generate Remote PD certificates, see Section 6.5.6 *"Editing Wall PD Settings and Certificate"*, page 77 or Section 6.5.7 *"Editing Mobile PD Settings and Certificate"*, page 79.

To fetch a licence file from DCS, see Section 6.1.2 *"Installing Licences"*, page 72.

To fetch an extension file from DCS, see Section 6.15 *"Importing Extensions"*, page 100.

8.9 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
- Revalidation
- Flexible Revalidation
- Cylinder groups
- Web services

To view available licensed features, see Section 6.1.1 *“Viewing Licence Status and Features”*, page 72.

If CWM is started up without a valid licence, CWM is locked from use and a new licence must be installed.

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 6.1.2 *“Installing Licences”*, page 72.

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.

When a licence is about to expire, e-mails are sent to administrators with the **Super Administrator** role, who have a registered e-mail address.

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 An operation that deletes a cylinder's memory content and then restores the cylinder access list from the CWM database.

DCS Integration An optional 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.

Enrolment Application A web application that is used when **DCS Integration** is enabled to generate C-Key certificates.

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.

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

PD Programming Device

USB OTG USB On-The-Go

9.2 CWM Symbols

Keys

🔑 Mechanical Key

🔑 Dynamic Key

🔑 Master C-Key

🔑 Normal C-Key

🔑 Dynamic Key Group

🔑 Normal C-Key Group

🔑 Master C-Key Group

⚙ Pending remote update exists for the key

⚙ Pending remote update exists that exceeds key capacity

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 is programmed to C-Key

⚙ Cylinder Programming Job is finished

⚙ Cylinder Programming Job has failed or been cancelled

Authorisations

🔑	Explicit authorisation
👥	Authorisation from access profile

Lock Chart

■	Key authorised in cylinder
□	Key not authorised in cylinder
⊞	Cylinder Programming Job created to authorise key in cylinder
⊟	Cylinder Programming Job created to remove authorisation for key in cylinder
◧	Example for double cylinder: Key authorised in cylinder side A but not in side B.

Remote PDs

📟	Wall PD
📱	Mobile PD

9.3 Object Attributes

9.3.1 Key Attributes

Name Name of the key.

Marking The key marking.

Second marking Unique number that identifies a key.

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 7.2.2 *“User Keys”*, page 102.

Firmware The firmware version.

Generation The key generation.

Status The key status (**In stock**, **Handed out**, **Lost** or **Broken**).

Line number Line number from the locking plan.

Last remote update Date and time of the last update through a Remote PD.

Tags Tags defined for the key.

External Links URLs associated with the key.

Access list size Used entries / Maximum entries in the Key Access List.

Key holder The person the key is currently handed out to.

9.3.2 C-Key Attributes

Name Name of the C-Key.

Marking The C-Key marking.

Second marking Unique number that identifies a key.

Group The key group the C-Key belongs to.

Type The C-Key type. For more information, see Section 7.2.3 *“C-Keys”*, page 102.

Firmware The firmware version.

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.

Status The C-Key status (**In stock**, **Handed out**, **Lost** or **Broken**).

Blocked Whether the C-Key is blocked from all access.

Certificate enrolment Whether certificate enrolment is allowed.

Authorisation roles Which roles that are associated with the C-Key.

Key holder The person the C-Key is currently handed out to.

9.3.3 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.

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 Line number from the locking plan.

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).
Domain	The domain to which the cylinder belongs.
Tags	Tags defined for the cylinder.
External Links	URLs associated with the cylinder.

9.3.4 Remote PD Attributes

Name	Name of the Remote PD.
Marking	The Remote PD marking.
GR	Group ID (for internal use only).
UID	Unique ID (for internal use only).
Firmware	Firmware version.
Boot loader	Boot loader firmware version.
Status	Connection status (**Offline** or **Online**).
Last connection	Mobile PD: The time and date when the Mobile PD was last online.
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	View	Full	Dependencies
Cylinders		Can list cylinders indirectly. Has effect only in combination with other permissions (see the Dependencies column).	**Cylinders** menu option available. Can view cylinder details.	Can edit cylinder details and change cylinder status.	
Keys		Can list keys indirectly. Has effect only in combination with other permissions (see the Dependencies column).	**Keys** menu option available. Can view key details.	Can edit key details, inventory and operational status.	
Key authorisations			Can view authorisations for a key.	Can edit authorisations for a key.	Requires view permission for keys and list permission for cylinders.
Key schedule		N/A	N/A	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 Apply schedule by template and view permission for keys.
Apply schedule by template		N/A	N/A	Can apply schedule template for a key and apply schedule template while handing out the key.	Requires view permission for keys.
Key validity		N/A	N/A	Can edit bulk validity settings for keys, edit key validity settings, and set validity while handing out a key.	Requires view permission for keys.

Permission	None	List	View	Full	Dependencies
Cylinder authorisations			Can view authorisations for a cylinder.	Can edit authorisations for a cylinder and request cylinder reprogramming.	Requires view permission for cylinders and list permission for keys.
Cylinder programming		N/A	N/A	**Programming** menu option available. Can send programming jobs to C-Keys.	Requires list permission for cylinders.
Employees		Can list employees indirectly. Has effect only in combination with other permissions (see the Dependencies column).	**Employees** menu option available. Can view employee details.	Can edit employee details.	
Visitors		Can list visitor indirectly. Has effect only in combination with other permissions (see the Dependencies column).	**Visitors** menu option available. Can view visitor details.	Can edit visitor details.	
Hand in/ hand out		N/A	N/A	**Hand in key** and **Hand out key** menu options available. Can perform hand in and hand outs.	Requires list permissions for employees, visitors, keys and cylinders and full permissions for key authorisations.
Audit trails			**Audit trails** menu option available. Audit trail tab visible in key view and cylinder view.	Can request audit trails for cylinders and keys via the audit trail tab.	

Permission	None	List	View	Full	Dependencies
Approvals		**Jobs for approval** menu option available. Can view a list of audit trail requests for approval.	N/A	Can approve audit trail requests. This option is given to the default Approver role only, and cannot be edited.	
Remote PDs		Can list Remote PDs indirectly. Has effect only in combination with other permissions (see the Dependencies column).	**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.	
System settings		N/A	**System settings** menu option available. Can view system settings.	Can edit system settings.	
Maintenance		N/A	N/A	Can lock and unlock the system.	
Firmware import		N/A	N/A	Can import firmware.	Firmware upgrades requires full permission for Remote PDs.
Employee import		N/A	N/A	Can import employees.	Requires full permission for employees.
System status		N/A	**System status** menu option available. Can view system status.	N/A	Requires list permission for Remote PDs.
Statistics		N/A	**Statistics** menu option available. Can view system statistics.	N/A	

Permission	**None**	**List**	**View**	**Full**	**Dependencies**
Schedule templates				**Schedule templates** Menu option available. Can view and edit schedule templates.	
Receipt templates		N/A	**Receipt templates** menu option available. Can print receipts and preview receipt templates.	Can edit the receipt templates.	
C-Keys		Can see C-Keys in key listings. (C-Keys are never visible through **Keys** menu option.)	**C-Keys** menu option available. Can view C-Key details.	Can edit C-Key details and hand out C-Keys.	
Roles	(No permission required to see roles on a C-Key.)		**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.	
Export report data		N/A	N/A	Can export report data.	
Domains	(No permission required to view domain memberships and domain authorisations for C-keys.)	N/A	N/A	Can administrate domains (add, remove, edit), and change domain authorisations for C-Keys.	
Access profiles Controls administration of access profiles (create, delete, edit)		N/A	**Access profiles** menu option available. 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.	

Permission	None	List	View	Full	Dependencies
Access profile authorisation Controls setting authorisations for an access profile		N/A	Can see authorisations in access profile.	Can add or remove authorisations in access profile.	Requires view permission for access profiles.
Flexible Revalidation	Can see revalidation intervals if flexible revalidation is enabled.	N/A	N/A	Can edit revalidation intervals for access profiles and cylinder groups.	

9.5 Remote 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 green	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 green			**Firmware Upgrade Finished**
		1 beep	**Operation Finished OK** **Remote PD Settings Updated**

LED Indications	Buzzer	Interpretation
⤓ Blinking		**Downloading and Processing**
✉ Solid	1 beep	**E-mail Sent**
✖ Solid	3 beeps	**Operation finished with error**

For operations involving a key, beeps are repeated every three seconds until the key is removed.

9.6 Battery Level Indications

Battery Level Indication	Interpretation
🟩🟩🟩🟩	**Battery level excellent**
🟩🟩⬜⬜	**Battery level good**
🟨⬜⬜⬜	**Battery level bad**
🟥⬜⬜⬜	**Battery level critical**

9.7 Firmware Dependent Functionality

Key Firmware

Function	Firmware Version
Schedule type - Basic	1.x, 3.x, 5.x
Schedule type - Multiple Time Window	2.x, 4.x, 6.x, 10 or higher
Remote	3 or higher
Cylinder Groups	5 or higher
Offline Update	6 or higher
Flexible Revalidation	6.3 or higher

To view the firmware version of a key, view the detailed information. See Section 4.2.2 *"Searching for Keys"*, page 26 or Section 4.2.1 *"Scanning a Key"*, page 26.

Cylinder Firmware

Function	Firmware Version
Cylinder Groups	5 or higher

Wall PD Firmware

Function	Firmware Version
Key firmware upgrades (generation 1 keys)	Wall PD firmware 2.9 or higher Wall PD key updater firmware 2.9 or higher
Key firmware upgrades (generation 2 keys)	Wall PD firmware 4.0 or higher
Offline Update	Wall PD firmware 2.11 or higher

To view the firmware version of a Wall PD, view the detailed information. See Section 6.5.2 *"Searching for Remote PDs"*, page 74.

Mobile PD Firmware

Function	Firmware Version
Key firmware upgrades (generation 2 keys)	Mobile PD firmware 4.0 or higher
Offline Update	2.10 or higher
Bluetooth PAN support (to use with iPhone or Android)	2.10 or higher

To view the firmware version of a Mobile PD, view the detailed information. See Section 6.5.2 *"Searching for Remote PDs"*, page 74.

9.8 Client PC Requirements

Product	Requirement
Operating System	Windows XP Pro SP 3, Windows Vista, Windows 7 Pro/Enterprise/Ultimate (32- or 64-bit), Windows 8 (64-bit)
Java Runtime Environment (JRE)	• Oracle Java SE 6 JRE 32-bit, update 16 or higher or • Oracle Java SE 7 JRE 32-bit, except update 21
Internet Browser	• Internet Explorer 8 or higher, 32-bit The browser security setting "Do not save encrypted pages to disk" must be disabled or • Firefox 16.0.2 or higher
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 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 4.1.9 *"Exporting Employee Or Visitor Information"*, page 25.

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 5 *"CSV File Structure"*, page 139.

Table 5. CSV File Structure

Field No	Name	Mandatory	No of Characters
1	Identifier		1-50
2	Title		0-100
3	First name	✓	1-49
4	Surname	✓	1-49
5	Email		0-100
6	Phone		0-100
7	Organisation		0-100
8	Department		0-100
9	Street		0-100
10	Postcode		0-100

Field No	Name	Mandatory	No of Characters
11	Language		0-100
12	Region		0-100
13	Job		0-100
14	City		0-100
15	State		0-100
16	Country		0-100
17	Company address		0-100
18	Location		0-100
19	Mobile phone		0-100
20	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.

Email must be specified in a correct e-mail format.

Maximum number of employees in one file is 10 000.

Example File

```
Identifier,Title,First name,Surname,Email,Phone,Organisation,De
partment,Street,Postcode,Language,Region,Job,City,State,Country
,Company address,Location,Mobile phone,Gmd text

P0,Professor,George,Whitmore,George.Whitmore@assaabloy.com,3719
253729973267730,ASSA ABLOY,Shared Technologies,,,Swedish,,Syste
m Developer,Stockholm,,Sweden,"Formansvagen 11, 117 43 Stockhol
m",,070-6972135783866065282,GmdText
```

ASSA®

ASSA ABLOY