CLIQ® Web Manager

Bedienungsanleitung

IKON
ASSA ABLOY

assaabloy.com

Experience a safer
and more open world

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

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

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

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

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

ASSA ABLOY
Sicherheitstechnik GmbH

Attilastraße 61–67
12105 Berlin
DEUTSCHLAND
Tel. + 49 30 8106-0
Fax: + 49 30 8106-26 00
berlin@assaabloy.com

www.assaabloy.de

Program version: V 2025.1
Main document number: D001583864
Date published: 2025-05-22
Language: de-DE

1 Überblick

1.1 Einleitung

CLIQ Web Manager (CWM) ist ein webbasiertes Softwaresystem zur Verwaltung und Steuerung der elektromechanischen Schließanlage CLIQ, das eine umfassende Kontrolle von Zugangsberechtigungen und Schlüsselhalteraktivitäten ermöglicht. Das CLIQ-System ist eine leistungsstarke Lösung, die die Zuverlässigkeit mechanischer Schlüssel und Schließzylinder mit der Sicherheit und Flexibilität elektronischer Schlösser verbindet.

1.2 Wesentliche Merkmale

- **Einfacher Einbau** - CLIQ ist ein kostengünstiges Offline-System, das keine elektrische Verdrahtung oder Schließzylinderbatterien benötigt.
- **Ereignislisten** - CLIQ ermöglicht einfachen Zugriff auf präzise Ereignislistendaten für jeden Zylinder und Schlüssel einer Schließanlage.
- **Einzelne Schlüssel** - Jeder Schlüssel wird durch sichere kryptographische Schlüssel geschützt und ist zur Verwendung durch eine einzige Person bestimmt. Bei Verlust eines Schlüssel wird dieser lediglich für ungültig erklärt und an seiner Stelle ein neuer generiert.
- **Zeitgesteuerter Einlass** - CLIQ ermöglicht die Festlegung eines speziellen Zeitplans mit Zeitfenstern, in denen Zugang gewährt wird.
- **Schlüsselverwaltung** - CLIQ Web Manager registriert die Herausgabe von Schlüsseln an verschiedene Schlüsselhalter.
- **Elektronische Ungültigkeitserklärung eines Schlüssels** - Schlüssel können für ungültig erklärt werden, ohne dass der Schlüssel tatsächlich vorliegt.
- **Verlängerung von Berechtigungen** - Erhöht die Sicherheit der Schließanlage, indem sie die Schlüsselhalter zwingt, eine Aktualisierung ihrer Rechte von einem nahe gelegenen Programmiergerät einzuholen. Außerdem wird dadurch sichergestellt, dass die Ereignisliste zum Server hochgeladen wird und den Administratoren der Schließanlage zur Verfügung steht.
- **Gruppenbildungsfunktionen** zur Vereinfachung der Verwaltung. Der CLIQ Web Manager ermöglicht die Gewährung eines Zugangs für Zylindergruppen und Personengruppen z. B. auf der Grundlage ihres geographischen Standorts oder ihrer Funktion im Unternehmen.

1.3 Informationen zu diesem Handbuch

Inhalt des Handbuchs
Dieses Handbuch besteht aus den folgenden Teilen, die für unterschiedliche Zielgruppen bestimmt sind:

Abschnitt	Für Administratoren	Für Super-Administratoren	Beschreibung
1 Überblick	✓	✓	Kurze Einführung in CLIQ und in dieses Handbuch.
2 Einrichtung von CWM-Clients	✓	✓	Beschreibt das Einrichten eines CWM Client.
3 Erste Schritte mit CWM	✓	✓	Beschreibt die ersten Schritte bei der erstmaligen Nutzung des CWM.
4 Arbeiten mit CWM	✓	✓	Beschreibt die Durchführung der verschiedenen Aufgaben der Administratoren bei der Arbeit mit einer Schließanlage.
5 Einrichten von Schließanlagen		✓	Beschreibt die Einrichtung einer neuen Schließanlage.
6 Konfigurieren von Schließanlagen		✓	Beschreibt verschiedene Konfigurationsmöglichkeiten einer Schließanlage.
7 CLIQ-Hardware	✓	✓	Beschreibt die CLIQ-Architektur und ihre Komponenten.
8 CLIQ – Konzepte und Funktionen	✓	✓	Beschreibt das Berechtigungsverfahren und grundsätzliche CWM-Funktionen. Einige Inhalte sind sehr technisch und nur für Super-Administratoren gedacht.
9 Anhang	✓	✓	Enthält Informationen zum Nachschlagen.

Terminologie
Eine Definition der in diesem Handbuch verwendeten Begriffe und Abkürzungen findet sich in *Abschnitt 9.1.1 "Begriffe", Seite 199* und *Abschnitt 9.1.2 "Abkürzungen", Seite 200*.

Menüoptionen des CWM werden **Hauptmenü » Menüoption** geschrieben.

2 Einrichtung von CWM-Clients

2.1 Einrichtung von CWM-Clients - Überblick

1) Lokales PG installieren.

   Siehe *Abschnitt 2.2 "Installieren lokaler PGs", Seite 13*.

2) CLIQ Connect PC installieren.

   Siehe *Abschnitt 2.3 "Installation von CLIQ Connect PC", Seite 13*.

3) CLIQ Connect PC konfigurieren.

   Siehe *Abschnitt 2.4 "Konfigurieren von CLIQ Connect PC", Seite 14*.

2.2 Installieren lokaler PGs

1) Sicherstellen, dass das aktuell angemeldete Windows-Benutzerkonto über Administratorenrechte verfügt.
2) USB-Kabel am lokalen PG und am PC anschließen.
3) Kontrollieren, ob die Treiber automatisch heruntergeladen und installiert werden.

> **HINWEIS!**
> Den zugewiesenen COM-Port notieren, der im Infobereich angezeigt wird. Beim Anmelden bei CLIQ Express oder der CLIQ Go-App wählen Sie den zugewiesenen COM-Port aus, wenn der COM-Port nicht automatisch gefunden wird.
>
> Beispiel: `STMicroelectronics Virtual COM-Port (COM7)`.

4) Wenn die Treiber nicht automatisch installiert werden, wenden Sie sich an den technischen Support.

2.3 Installation von CLIQ Connect PC

CLIQ Connect PC ist eine Software, die die Kommunikation zwischen lokalem PG und CLIQ Web Manager sowie die Generierung von Programmierschlüssel-Zertifikaten handhabt.

Voraussetzungen:

- Das aktuell angemeldete Windows-Benutzerkonto verfügt über Administratorenrechte.
- Der Programmierschlüssel ist bereits ausgegeben, und der Schlüsselhalter hat eine E-Mail von CLIQ Web Manager erhalten.

1) Die CLIQ Connect PC-Installationsdatei herunterladen und ausführen.

   Den Link zur Datei finden Sie in den folgenden Quellen:

   - In der E-Mail von CLIQ Web Manager
   - Auf der CWM-Anmeldeseite
   - Auf der Begrüßungsseite zur Registrierung

2) Nach dem Start der Installationsroutine die **Sprache** auswählen und auf **OK** klicken.

Der CLIQ Connect-Einrichtungsassistent wird geöffnet.

3) Auf **Weiter** klicken.

4) Die Lizenzvereinbarung lesen. Zum Akzeptieren der Vereinbarung das Optionsfeld **Ich akzeptiere die Vereinbarung** auswählen (erforderlich, um mit dem Einrichtungsassistenten fortzufahren) und auf **Weiter** klicken.

> **HINWEIS!**
> Die **Lizenzvereinbarung** genau durchlesen.

5) Einen der folgenden Schritte ausführen:

- Erstmalige Installation von CLIQ Connect PC: Den Zielordner direkt auswählen und auf **Weiter** klicken.
- Zur Aktualisierung einer vorhandenen Installation: **Ja** auswählen, um die vorhandene Installation zu aktualisieren, oder **Nein** auswählen, um die Installation in einem anderen Verzeichnis durchzuführen. Dann zum Fortfahren auf **Weiter** klicken.

6) Die folgenden externen Dienste festlegen:

- Mithilfe von **Automatische Updates aktivieren** kann CLIQ Connect PC automatisch die aktuelle Softwareversion von CLIQ Connect PC herunterladen und installieren.
- Auswahl von **CLIQ Go** aufheben und **CLIQ Web Manager (Programmierschlüssel)** auswählen.

> **HINWEIS!**
> Die zwei oben angeführten Einstellungen können nach der Installation oder dem Aktualisierungsvorgang nicht mehr geändert werden.

- Mithilfe von **Verzeichnisdienst-Integration** kann CLIQ Connect PC automatisch Verbindungsdetails zu CLIQ Remote aus dem zentralen Verzeichnisdienst abrufen. Wenn CLIQ Connect PC keine Verbindung zu einem externen Dienst herstellen soll, die Auswahl von **Verzeichnisdienst-Integration** aufheben. In diesem Fall müssen **CLIQ Remote URL** und **CLIQ Enrolment-URL** manuell bereitgestellt werden.

7) Zum Fortfahren **Weiter** anklicken.

8) Erstmalige Installation von CLIQ Connect PC:

   Einen **Startmenü-Ordner** für die Programmverknüpfungen auswählen bzw. anlegen und zum Fortfahren auf **Weiter** klicken.

9) Warten, während die Dateien extrahiert und installiert werden.

10) Auswählen, ob das Programm nach Fertigstellung der Einrichtung gestartet werden soll oder nicht.

11) Zum Beenden der Einrichtung auf **Abschließen** klicken.

2.4 Konfigurieren von CLIQ Connect PC

2.4.1 Konfigurieren der COM-Auswahl von CLIQ Connect PC

1) Mit der rechten Maustaste auf das Symbol für **CLIQ Connect** im Benachrichtigungsfeld klicken.
2) Auf **COM-Auswahl** klicken.
3) Den COM-Anschluss, an den das Lokale PG angeschlossen ist, auswählen bzw. für automatische Auswahl des COM-Anschlusses auf **Auto** (Standard) klicken.

2.4.2 Anpassen der Serverkonfiguration für CLIQ Connect PC

1) Mit der rechten Maustaste auf das Symbol für **CLIQ Connect** im Benachrichtigungsfeld klicken.
2) Auf **Konfiguration** klicken und den Abschnitt **Serverkonfiguration** suchen.
3) Wenn die Verzeichnisdienst-Integration aktiviert ist:
   a) **Automatisch** auswählen.
   b) Geben Sie **Verzeichnis-URL** ein.
4) Wenn die Verzeichnisdienst-Integration **nicht** aktiviert ist:
   a) **Manuell** auswählen.
   b) **CLIQ Remote URL** und **CLIQ Enrolment-URL** eingeben.
5) Zum Speichern und Beenden auf **OK** klicken.

2.4.3 Konfigurieren der Proxyeinstellungen von CLIQ Connect PC

1) Mit der rechten Maustaste auf das Symbol für **CLIQ Connect** im Benachrichtigungsfeld klicken.
2) Auf **Konfiguration** klicken.
3) Bei **Proxy** die Option **Aktivieren** auswählen.
4) Die geforderten Informationen eingeben und auf **OK** klicken.

3 Erste Schritte mit CWM

3.1 Erste Schritte mit CWM - Überblick

Neue Administratoren: Führen Sie diese Schritte aus, um die Arbeit mit CWM zu beginnen.

Voraussetzungen:

- CWM ist eingerichtet und konfiguriert.
- Ein Programmierschlüssel, ein Programmierschlüsselzertifikat und die Programmierschlüssel-PIN sind verfügbar.

1) Zertifikat für Programmierschlüssel installieren.

   Siehe *Abschnitt 3.2 "Anmelden und Installieren von Programmierschlüssel-Zertifikaten", Seite 16*.

2) Login bei CWM durchführen.

   Siehe *Abschnitt 3.3 "Einloggen", Seite 18*.

3) Gewünschte Sprache für die CWM-Software wählen.

   Siehe *Abschnitt 3.4 "Einstellen der CWM-Sprache", Seite 19*.

4) *Abschnitt 3.5 "Einführung in die CWM-Benutzeroberfläche", Seite 19* durchlesen.

Die üblichsten Aufgaben bei der Arbeit mit CWM sind in *Abschnitt 3.6 "Allgemeine Aufgaben", Seite 23* aufgelistet.

3.2 Anmelden und Installieren von Programmierschlüssel-Zertifikaten

Damit ein Programmierschlüssel mit CWM verwendet werden kann, muss ein eindeutiges Zertifikat auf dem CWM-Client installiert sein.

Die Prozedur zur Installation eines Zertifikats hängt davon ab, ob die **DCS-Integration** verwendet wird.

Zertifikat-Installation mit DCS-Integration
Der Programmierschlüssel wird angemeldet und das Zertifikat wird direkt im Internetbrowser generiert. Das Zertifikat muss nicht separat erstellt werden.

Weitere Informationen siehe *Abschnitt 3.2.1 "Registrierung des Zertifikats für den Programmierschlüssel über CLIQ Connect PC", Seite 17*.

Manuelle Installation des Zertifikats
Zur manuellen Installation des Zertifikats für Programmierschlüssel muss eine Zertifikatdatei zur Verfügung stehen.

Weitere Informationen siehe *Abschnitt 3.2.2 "Manuelle Installation des Programmierschlüssel-Zertifikats", Seite 17*.

3.2.1 Registrierung des Zertifikats für den Programmierschlüssel über CLIQ Connect PC

Voraussetzungen:

- Das lokale PG ist installiert.
- Die CLIQ Connect PC-Software ist auf dem Computer installiert.

  Siehe *Abschnitt 2.3 "Installation von CLIQ Connect PC", Seite 13*.
- Der Programmierschlüssel ist in CWM ausgegeben.
- Der Programmierschlüssel darf angemeldet werden.

  Normalerweise kann ein Programmierschlüssel einmal angemeldet werden, aber diese Einstellung kann von einem Administrator mit den richtigen Rechten geändert werden. Weitere Informationen siehe *Abschnitt 6.11.4 "Bearbeiten von Programmierschlüsselinformationen", Seite 139*.
- Der Programmierschlüssel und der PIN-Code für den Programmierschlüssel sind verfügbar.

1) Programmierschlüssel in den linken Schlitz des lokalen PGs einführen.
2) Mit der rechten Maustaste auf das CLIQ Connect-Symbol im Benachrichtigungsfeld klicken und **Zertifikatsanmeldung starten** auswählen.
3) PIN-Code des Programmierschlüssels eingeben und auf **Weiter** klicken.

   Bei gültiger PIN wird ein Einmalpasswort (OTP) per E-Mail an den Nutzer des Programmierschlüssels gesendet.
4) Das Einmalpasswort (OTP) eingeben und auf **Weiter** klicken.

   Das Programmierschlüsselzertifikat wird automatisch erstellt und in den Webbrowsern hinzugefügt.
5) Zum Abschließen der Programmierschlüsselregistrierung auf **Fertig** klicken.

3.2.2 Manuelle Installation des Programmierschlüssel-Zertifikats

Voraussetzung:

- Eine **.p12** -Datei für den Programmierschlüssel sowie ein Passwort liegen vor.

1) Auf die **.p12**-Datei doppelklicken.

   Der **Zertifikatimport-Assistent** erscheint.
2) **Aktueller Nutzer** auswählen und auf **Weiter** klicken.
3) Überprüfen, ob das korrekte Zertifikat ausgewählt ist, und auf **Weiter** klicken.
4) Das mit der **.p12**-Datei bereitgestellte Passwort eingeben und auf **Weiter** klicken.
5) **Alle Zertifikate an folgendem Speicherort hinterlegen** auswählen und auf **Durchsuchen** klicken.
6) Im Pop-up-Fenster **Persönlich** auswählen und auf **Weiter** klicken.
7) Die Einstellung bestätigen und auf **Abschließen** klicken.

   Das Programmierschlüsselzertifikat wird in den unterstützten Webbrowsern installiert.

HINWEIS!
Das Programmierschlüsselzertifikat muss neu installiert werden, wenn das Passwort des Windows-Benutzerkontos von einem Administrator geändert wird (nicht erforderlich, wenn Nutzer ihre Passwörter selber ändern).

3.2.3 Erneuerung des Programmierschlüssel-Zertifikats

Wenn der Zeitraum bis zum Ablauf des Programmierschlüssel-Zertifikats 60 Tage oder weniger umfasst, wird nach dem Login eine Warnmeldung angezeigt.

- **Mit aktivierter DCS-Integration**:

  Eine E-Mail mit einer Kurzanleitung zur Verlängerung des Zertifikats wird an den Nutzer des Programmierschlüssels gesendet.

  Das Zertifikat wird in CLIQ Connect PC erneuert. Der Vorgang entspricht dem Anmeldevorgang. Siehe *Abschnitt 3.2.1 "Registrierung des Zertifikats für den Programmierschlüssel über CLIQ Connect PC", Seite 17* zu Details.

- **Ohne DCS-Integration**:

  Das neue Zertifikat wird in DCS generiert und dem Nutzer des Programmierschlüssels bereitgestellt.

  Informationen zum Installieren des neuen Zertifikats finden Sie in *Abschnitt 3.2.2 "Manuelle Installation des Programmierschlüssel-Zertifikats", Seite 17*.

Tipp
Es wird empfohlen, das veraltete Zertifikat im Browser zu löschen.

3.3 Einloggen

Voraussetzungen:

- Das lokale PG ist installiert. Siehe *Abschnitt 2.2 "Installieren lokaler PGs", Seite 13*.
- Ein unterstützter Internet-Browser wird verwendet. Siehe *Abschnitt 9.8 "Voraussetzungen für Client-PC", Seite 216*.
- Die CLIQ-Connect-Software ist auf dem Computer installiert und läuft.

  Siehe *Abschnitt 2.3 "Installation von CLIQ Connect PC", Seite 13*.
- Die CLIQ-Connect-Software ist konfiguriert und mit CWM verbunden.

  Siehe *Abschnitt 2.4 "Konfigurieren von CLIQ Connect PC", Seite 14*.
- Ein Programmierschlüssel samt PIN-Code steht zur Verfügung. Der Programmierschlüssel muss auch einem Mitarbeiter im CWM ausgehändigt werden.

HINWEIS!
Bei Anlagen mit Single Sign-on (SSO) ist nach der Installation des Programmierschlüsselzertifikats für bestimmte Vorgänge kein Schlüssel mehr zur Anmeldung erforderlich. Siehe hierzu *Abschnitt 8.10 "Single Sign-on (SSO)", Seite 195*.

- Ein gültiges Zertifikat für den Programmierschlüssel ist installiert. Siehe *Abschnitt 3.2 "Anmelden und Installieren von Programmierschlüssel-Zertifikaten", Seite 16*.
- Eine korrekte URL zu CWM steht zur Verfügung.

3.3.1 Anmeldung mit Programmierschlüssel

1) Programmierschlüssel in den linken Schlitz des lokalen PGs einführen.
2) Zur CWM-Startseite navigieren.
3) Das Zertifikat für den Programmierschlüssel auswählen.

   Die CWM-Anmeldeseite wird angezeigt.
4) Auf **Anmelden** klicken.
5) PIN-Code für den Programmierschlüssel eingeben.

   CLIQ Connect PC bittet um Bestätigung der Verwendung des Schlüssels.
6) Auf **Bestätigen** klicken.

3.3.2 Anmeldung ohne Programmierschlüssel

1) Zur CWM-Startseite navigieren.
2) Das Zertifikat für den Programmierschlüssel auswählen.

   Die CWM-Anmeldeseite wird angezeigt.
3) Auf **SSO-Anmeldung** klicken.

   In den meisten Fällen erfolgt eine automatische Authentifizierung, wenn im Browser bereits eine Anmeldung in der Unternehmensdomäne erfolgt ist, sodass ohne weitere Aktion direkt auf CWM zugegriffen werden kann.

   Wenn nicht, wird das Anmeldefenster des Identitätsanbieters angezeigt.

3.4 Einstellen der CWM-Sprache

1) **Einstellungen » Sprache auswählen** auswählen.
2) Gewünschte Sprache auswählen.

Die Sprache kann auch durch Klicken auf das entsprechende Flaggensymbol im Login-Bildschirm ausgewählt werden.

3.5 Einführung in die CWM-Benutzeroberfläche

3.5.1 Hauptmenüs

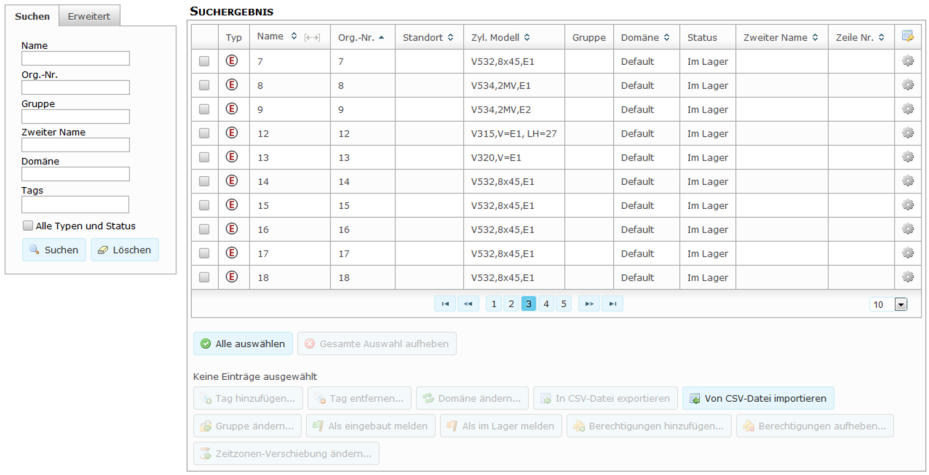
Die CWM-Optionen sind in vier Hauptmenüs unterteilt:

Arbeit	Enthält die bei der täglichen Arbeit am häufigsten verwendeten Funktionen.
Systeminfo	Enthält Funktionen zur Verwaltung von Zugangsrechten, Informationen zu Mitarbeitern und Besuchern, Schlüsseln, Zylindern und Remote-Programmiergeräten.
Verwaltung	Enthält Funktionen zur Einrichtung und Konfiguration der Schließanlage.
Einstellungen	Enthält die persönlichen Einstellungen zum angemeldeten Administrator.

3.5.2 Suchen nach Objekten

Zuerst die standardmäßigen Suchkriterien verwenden
Um nach Objekten wie Zylindern oder Schlüssel zu suchen, zuerst die entsprechende Menüoption auswählen, zum Beispiel **Systeminfo » Zylinder**.

Zuerst wird ein Suchergebnis auf Basis der standardmäßigen Suchkriterien angezeigt.



Dann die Suchfunktionen verwenden

Suchkriterien		Um die Suchkriterien anzupassen, in den linken Suchkasten neue Kriterien eintragen und auf **Suchen** klicken. Im Register **Erweitert** sind weniger häufig verwendete Suchoptionen verfügbar.
Platzhalter		CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.
Tags		Bei Eingabe im Suchfeld **Tags** erscheinen alle passenden Tags in einer Auswahlliste.
Zeilen pro Seite		Bei vielen Suchergebnissen kann mit den Pfeilen unter dem Suchergebnis durch die Seiten geblättert werden. Die Anzahl der pro Seite angezeigten Zeilen lässt sich in der Drop-down-Liste **Zeilen pro Seite** einstellen.
Sortieren		Auf dieses Symbol klicken, um die Suchergebnisse nach der entsprechenden Spalte zu sortieren.
		Die Suchergebnisse werden nach dieser Spalte sortiert (aufsteigend).
		Die Suchergebnisse werden nach dieser Spalte sortiert (absteigend).
Vergrößern einer Spalte		Auf dieses Symbol klicken, um Spalten auszuklappen, in denen Einträge über die Spaltengrenzen hinausgehen.

Um Detailinformationen zum Objekt zu erfahren und das Objekt individuell zu konfigurieren, auf die entsprechende Objektzeile klicken.

3.5.3 Gleichzeitiges Konfigurieren mehrerer Objekte

Bestimmte Befehle lassen sich auf mehrere Objekte gleichzeitig ausführen. Die verfügbaren Befehle hängen vom Typ des Objekts ab.

Um mehrere Objekte gleichzeitig zu konfigurieren:

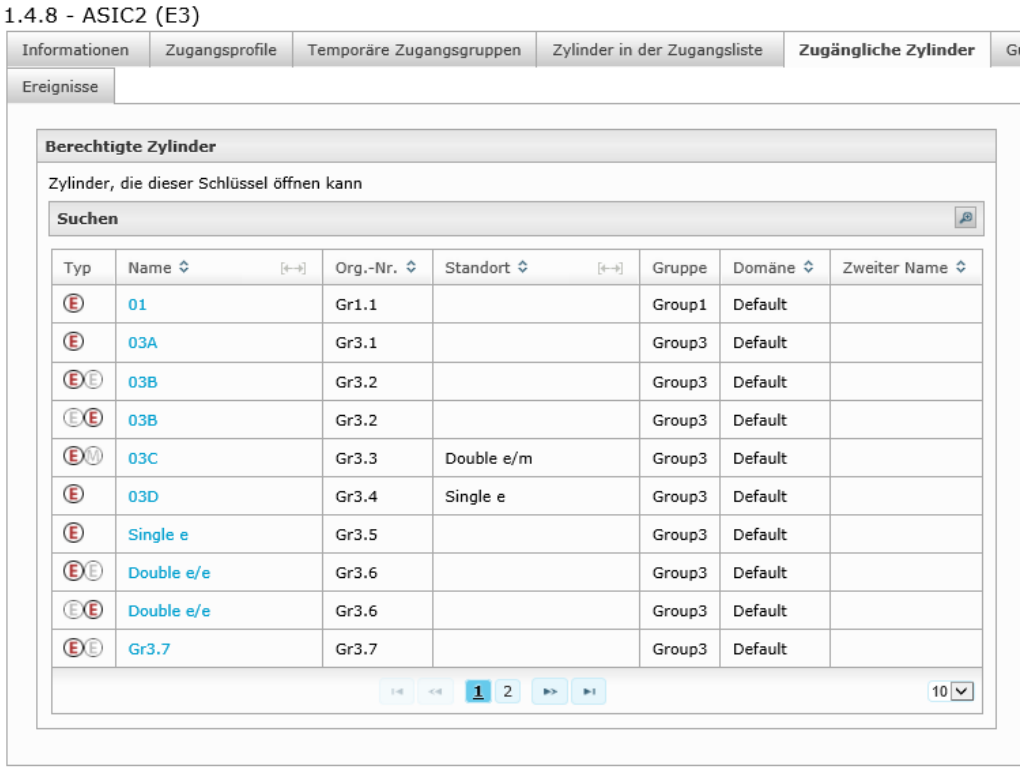
1) Auf einer oder mehreren Suchergebnisseiten mehrere einzelne Objekte in der ersten Spalte auswählen.

   Auf **Alle auswählen** klicken, um sämtliche Objekte auf allen Suchergebnisseiten auszuwählen.

2) Die entsprechende Schaltfläche unter den Suchergebnissen anklicken, um den Befehl auf die ausgewählten Objekte auszuführen.

3.5.4 Filtern langer Listen

Beim Ansehen von Listen mit beispielsweise Zylindern oder Schlüsseln in Zugangslisten ist eine **Suchen**-Leiste zu sehen. Siehe Beispiel unten.



Ein Klick auf das Symbol  öffnet ein Feld mit Suchkriterien.

3.5.5 Bedienung

3.5.5.1 Tastaturbedienung

Für Benutzer, denen keine Maus und kein anderes Zeigegerät zur Verfügung stehen oder die eine Bedienung mit der Tastatur bevorzugen, unterstützt CWM durchgängig eine Navigation mittels Tastatur.

Interaktion	Tasten	Hinweise
Navigation zwischen den meisten Elementen	• **Tabulator** • **Umschalttaste** + **Tabulator** (rückwärts navigieren)	
Schaltflächen	• **Eingabetaste** oder **Leertaste**	
Kontrollkästchen	• **Leertaste**	Aktivierung/Deaktivierung eines Kontrollkästchens.
Comboboxen	• **Leertaste** (Optional. Werteliste öffnen). • **Auf**/**Ab** oder **Links**/**Rechts**	Mit den Pfeiltasten einen Wert auswählen (**Auf**/**Ab** oder **Links**/**Rechts**) und dann mithilfe von **Eingabetaste** akzeptieren.
Tabellen	• **Auf**/**Ab** (navigieren zwischen Tabellenzellen) • **Eingabetaste** (Detailinformationen eingeben und einsehen)	Das Navigieren zwischen den Tabellenzellen erfolgt mit Hilfe der Pfeiltasten (**Auf**/**Ab**).
Optionsfelder	• **Auf**/**Ab** oder **Links**/**Rechts**	Das Auswählen einer Option erfolgt mit Hilfe der Pfeiltasten (**Auf**/**Ab** oder **Links**/**Rechts**), das Navigieren zum nächsten Element mit **Tabulator**.
Hauptmenü	• **Links**/**Rechts** (durch die Optionen des Hauptmenüs navigieren) • **Auf**/**Ab** (Untermenüoption aus-/einklappen) • **Eingabetaste** (Untermenüoption auswählen)	Das Navigieren durch die Optionen des Hauptmenüs und der Untermenüs erfolgt mit Hilfe der Pfeiltasten (**Auf**/**Ab** oder **Links**/**Rechts**).
Seitenansicht	• **Bild Auf** und **Bild Ab**	Aufwärts und abwärts durch die Webseite blättern.
Arbeitsabläufe	• **Alt** + **Links**/**Rechts** • **Alt** + **Q** • **Alt** + **Return**	Zwischen einzelnen Schritten navigieren. Arbeitsablauf abbrechen. Den letzten Schritt bestätigen.
Texteditor	• **Alt** + **Q**	Texteditor beenden.

3.5.5.2 Anzeigemodi

Modus für hohen Kontrast
CWM unterstützt einen Hochkontrastmodus.

200 % Zoom bei 1024x768-Auflösung
Vergrößerung auf bis zu 200 % im Browser ist ohne Funktionsverlust der Benutzeroberfläche möglich.

3.6 Allgemeine Aufgaben

Dies ist eine Liste mit einigen der üblichsten Aufgaben samt Informationen, wo entsprechende Anweisungen zu finden sind.

Einloggen
Abschnitt 3.3 "Einloggen", Seite 18

Personal
Hinzufügen eines Mitarbeiters oder Besuchers: *Abschnitt 4.1.2 "Hinzufügen von Mitarbeitern oder Besuchern", Seite 24*

Nutzerschlüssel
Ausgabe von Schlüsseln: *Abschnitt 4.2.9 "Benutzerschlüssel ausgeben", Seite 40*

Rücknahme von Schlüsseln (Rückgabe): *Abschnitt 4.2.10 "Rücknahme von Benutzerschlüsseln (Rückgabe)", Seite 45*

Verlorene Schlüssel: *Abschnitt 4.2.12.2 "Verlorenen Benutzerschlüssel melden und sperren", Seite 47*

Berechtigungen
Schlüssel mit Berechtigung für einen Zylinder oder eine Zylindergruppe anzeigen: *Abschnitt 3.6 "Allgemeine Aufgaben", Seite 23*

Zylinder anzeigen, für die ein Schlüssel oder eine Schlüsselgruppe über Berechtigungen verfügt: *Abschnitt 4.8.2 "Anzeigen von Schlüsseln mit Berechtigung für bestimmte Zylinder oder Zylindergruppen", Seite 80*

Ändern von Berechtigungen für einen Schlüssel: *Abschnitt 4.9.1 "Konfigurieren von Berechtigungen in Schlüsseln", Seite 81*

Änderung von Berechtigungen für einen Zylinder: *Abschnitt 4.9.2 "Konfigurieren von Berechtigungen in Zylindern", Seite 83*

Zugangsprofile
Verknüpfen eines Schlüssels oder einer Person mit einem Zugangsprofil: *Abschnitt 4.9.5 "Auswählen von Zugangsprofilen von Mitarbeitern oder Besuchern", Seite 87*

Ändern von Berechtigungen für ein Zugangsprofil: *Abschnitt 4.9.4 "Konfigurieren von Berechtigungen in Zugangsprofilen", Seite 86*

Ereignislisten
Kontrollieren von Schlüsseln, die auf einen Zylinder zugegriffen haben: *Abschnitt 4.11.3 "Anzeigen von Ereignislisten für Zylinder", Seite 96*

Programmierung
Programmieren von Zylindern: *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64*

4 Arbeiten mit CWM

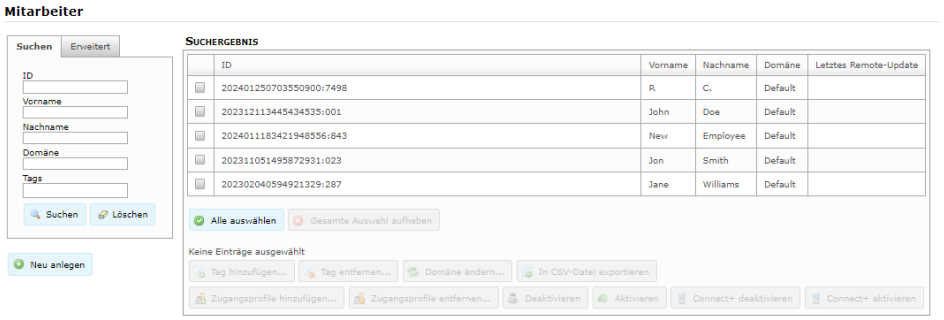
4.1 Verwalten von Mitarbeitern und Besuchern

4.1.1 Suchen nach Mitarbeitern oder Besuchern

1) **Systeminfo » Mitarbeiter** oder **Besucher** auswählen.

   Eine Liste aller Mitarbeiter oder Besucher wird angezeigt.

   Wenn die LDAP-Integration aktiviert ist, ruft CWM alle 24 Stunden automatisch die neuesten Informationen von LDAP ab. Datum und Uhrzeit der letzten Aktualisierung werden angezeigt. Durch Klicken auf **Details anzeigen** werden detaillierte Informationen angezeigt. Um manuell eine Aktualisierung zu initiieren, auf **LDAP-Mitarbeiter aktualisieren** klicken. Weitere Informationen zur LDAP-Integration sind in *Abschnitt 8.12 "LDAP-Integration", Seite 196* verfügbar.



2) Register **Suchen** oder **Erweitert** auswählen.

   Das Register **Erweitert** enthält weitere Suchfelder sowie eine Suchmöglichkeit nach gelöschten oder deaktivierten Mitarbeitern oder Besuchern, abhängig von der CWM-Einstellung für gelöschte Personen. Details siehe *Abschnitt 8.9 "Löschen von Personendaten und DSGVO-Erfüllung", Seite 194*.

3) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

   Bei Eingabe im Suchfeld **Tags** erscheinen alle passenden Tags in einer Auswahlliste.

4) Auf **Suchen** klicken.

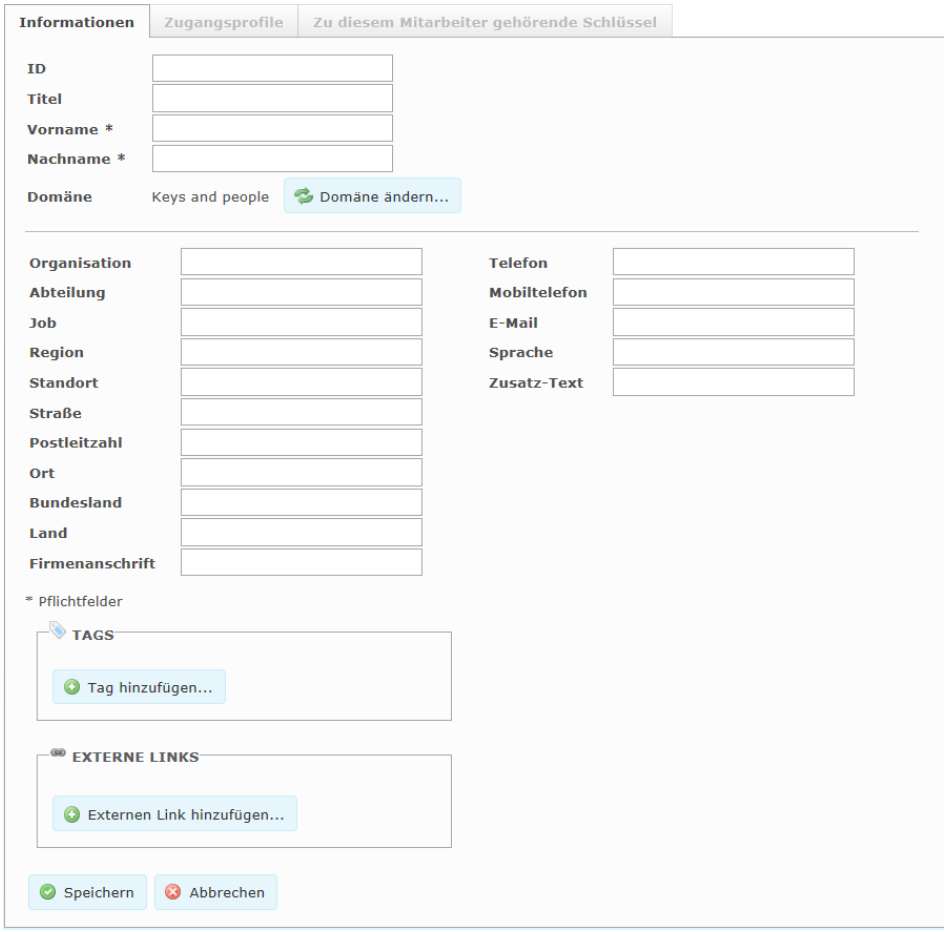
5) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf den entsprechenden Mitarbeiter oder Besucher klicken.

4.1.2 Hinzufügen von Mitarbeitern oder Besuchern

HINWEIS!
Die Mitarbeiterinformationen vom LDAP-Server sind schreibgeschützt. Die neu in CWM erstellten Mitarbeiter werden nicht zum LDAP-Server hinzugefügt.

1) **Systeminfo » Mitarbeiter** oder **Besucher** auswählen.

2) Auf **Neu anlegen** klicken.



3) Die Daten eingeben.

   Vorname und **Nachname** sind Pflichtfelder.

   Die **E-Mail**-Adresse wird benötigt, damit bei verspäteten Schlüsseln eine Erinnerung versandt werden kann, sowie für den Einsatz der DCS-Integrations-Funktionalität für neue Halter von Programmierschlüsseln.

   Wenn die Funktion CLIQ Connect+ für das System aktiviert ist und für den neuen Mitarbeiter oder Besucher aktiviert wird, darf die E-Mail-Adresse nicht mit der E-Mail-Adresse eines bereits in CLIQ Connect+ registrierten Benutzers übereinstimmen.

   Bei Mitarbeitern wird auch das Feld **ID** verwendet. Die ID muss eindeutig sein. Wenn in diesem Feld keine Eingabe vorgenommen wird, wird hier von CWM eine eindeutige ID im Format jjjj-mm-tt:laufende Nr. eingegeben.

4) Um ein Tag hinzuzufügen, auf **Tag hinzufügen...** klicken. Siehe auch *Abschnitt 4.1.7 "Hinzufügen oder Entfernen von Mitarbeiter- oder Besucher-Tags", Seite 32*.

5) Um einen externen Link hinzuzufügen, auf **Externen Link hinzufügen...** klicken. Siehe auch *Abschnitt 4.1.8 "Verwalten externer Links von Mitarbeitern oder Besuchern", Seite 33*.

6) Auf **Speichern** klicken.

4.1.3 Deaktivieren oder Aktivieren von Mitarbeitern oder Besuchern

Voraussetzungen:

- Um Mitarbeiter oder Besucher deaktivieren und deaktivierte Personen suchen und erneut aktivieren zu können, benötigt der Administrator die Berechtigung **Schlüsselhalter: Deaktivieren**.

  Weitere Informationen zum Verwalten von Berechtigungen finden Sie in *Abschnitt 6.7 "Verwalten von Rollen und Rechten", Seite 131*.

- In **Systemeinstellungen** ist **Dauerhaft löschen** im Abschnitt **Beim Löschen von Personen** ausgewählt.

  Weitere Informationen zum Verwalten von **Systemeinstellungen** finden Sie in *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

- Die folgenden Mitarbeiter bzw. Besucher können nicht deaktiviert werden:
  - Mitarbeiter oder Besucher mit ausgegebenen Schlüsseln.
  - Mit LDAP integrierte Mitarbeiter.
  - Aktivierte CLIQ Mobile Manager-Benutzer.

1) **Systeminfo » Mitarbeiter** oder **Systeminfo » Besucher** auswählen.

   Eine Liste aller Mitarbeiter oder Besucher wird angezeigt.

   > **Tipp**
   > Deaktivierte oder aktive Mitarbeiter oder Besucher können über den Filter **Deaktivierte anzeigen** auf der Registerkarte **Erweitert** gefiltert werden.

   Geben Sie bei Bedarf die entsprechenden Suchkriterien ein.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

   Bei Eingabe im Suchfeld **Tags** erscheinen alle passenden Tags in einer Auswahlliste.

   - Um einzelne Mitarbeiter oder Besucher zu aktivieren oder zu deaktivieren, die Anweisungen unter *Schritt 2* befolgen.
   - Um mehrere Mitarbeiter oder Besucher gleichzeitig zu aktivieren oder zu deaktivieren, die Anweisungen unter *Schritt 3* befolgen.

2) **Aktivieren oder Deaktivieren eines einzelnen Mitarbeiters oder Besuchers**

1. Den Mitarbeiter oder Besucher auswählen und die Detailansicht öffnen.
2. **Mitarbeiter oder Besucher deaktivieren**

   a) In der Informationsansicht auf **Deaktivieren** klicken.

   b) Im Pop-up-Fenster auf **Deaktivieren** klicken.

   Mitarbeiter oder Besucher aktivieren

   a) In der Informationsansicht auf **Aktivieren** klicken.

   b) Im Pop-up-Fenster auf **OK** klicken.

3) **Aktivieren oder Deaktivieren mehrerer Mitarbeiter oder Besucher**

1. Die zu deaktivierenden oder aktivierenden Mitarbeiter oder Besucher durch Aktivieren der entsprechenden Kontrollkästchen aus den Suchergebnissen auswählen.
2. **Mehrere Mitarbeiter oder Besucher deaktivieren**

   a) Unter den Suchergebnissen auf **Deaktivieren** klicken.

   b) Im Pop-up-Fenster auf **Deaktivieren** klicken.

   Mehrere Mitarbeiter oder Besucher aktivieren

   a) Unter den Suchergebnissen auf **Aktivieren** klicken.

   b) Im Pop-up-Fenster auf **OK** klicken.

4.1.4 Löschen oder Wiederherstellen von Mitarbeitern oder Besuchern

In den **Systemeinstellungen** kann für das Löschen von Mitarbeitern oder Besuchern zwischen den Optionen **Als gelöscht kennzeichnen** und **Dauerhaft löschen** ausgewählt werden.

- Wenn **Als gelöscht kennzeichnen** ausgewählt ist, lassen sich die gelöschten Mitarbeiter bzw. Besucher bei Bedarf wiederherstellen.
- Wenn **Dauerhaft löschen** aktiviert ist, können gelöschte Mitarbeiter oder Besucher **nicht mehr** wiederhergestellt werden.

Siehe auch *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102* und *Abschnitt 8.9 "Löschen von Personendaten und DSGVO-Erfüllung", Seite 194*.

1) Den Mitarbeiter oder Besucher suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

> **Tipp**
> Gelöschte Benutzer können über den Filter **Gelöschte anzeigen** auf der Registerkarte **Erweitert** gefiltert werden.

2) **Mitarbeiter oder Besucher löschen**

> **HINWEIS!**
> Die folgenden Personen können nicht gelöscht werden:
>
> - Mitarbeiter oder Besucher mit ausgegebenen Schlüsseln.
> - Mit LDAP integrierte Mitarbeiter.
> - In CLIQ Connect+ aktivierter Benutzer.

1. In der Detailanzeige auf **Löschen** klicken.
2. Im Pop-up-Fenster auf **Löschen** klicken.

Mitarbeiter oder Besucher wiederherstellen

1. In der Detailanzeige auf **Wiederherstellen** klicken.
2. Im Pop-up-Fenster auf **Wiederherstellen** klicken.

4.1.5 Aktivieren und Deaktivieren des Zugriffs auf CLIQ Connect+ für Mitarbeiter oder Besucher

Wenn die Funktion CLIQ Connect+ im System aktiviert ist, können Mitarbeiter und Besucher die detaillierten Informationen für ihre Schlüssel über CLIQ Connect überprüfen. Zur Verwendung dieser Funktion muss der Administrator den Benutzer in CLIQ Connect+ aktivieren.

Der Benutzerstatus kann auf zwei verschiedene Weisen aktiviert oder deaktiviert werden:

- Um den Status für einen einzelnen Benutzer zu ändern, befolgen Sie die Anweisungen unter *Abschnitt 4.1.5.1 "Zugriff auf CLIQ Connect+ für einzelnen Benutzer konfigurieren", Seite 28*.
- Um mehrere Mitarbeiter oder Besucher gleichzeitig zu aktivieren oder zu deaktivieren, befolgen Sie die Anweisungen unter *Abschnitt 4.1.5.2 "CLIQ Connect+-Berechtigung für mehrere Mitarbeiter konfigurieren", Seite 29*.

Weitere Details zu CLIQ Connect+ finden Sie in *Abschnitt 8.3.4 "CLIQ Connect und CLIQ Connect+", Seite 187*.

Voraussetzungen:

- Der Administrator hat die Lizenz **CLIQ Connect+** abgerufen und installiert.

  Informationen zum Installieren der neuen Lizenz finden Sie in *Abschnitt 6.1.1 "Installieren von Lizenzen", Seite 101*.
- Die E-Mail-Adresse des Mitarbeiters oder Besuchers darf nicht mit einem anderen Benutzer von CLIQ Connect+ verknüpft sein.

4.1.5.1 Zugriff auf CLIQ Connect+ für einzelnen Benutzer konfigurieren

1) Den Mitarbeiter oder Besucher suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

> **Tipp**
> Deaktivierte oder gelöschte Benutzer können über den Filter auf der Registerkarte **Erweitert** gefiltert werden.

2) Aktivieren oder Deaktivieren des Benutzers in CLIQ Connect+:

Benutzerstatus für CLIQ Connect+ aktivieren:
Auf **Connect+ aktivieren** klicken.

> **HINWEIS!**
> Wenn die E-Mail-Adresse nicht eingegeben wird oder bereits von einem anderen für CLIQ Connect+ aktivierten Mitarbeiter oder Besucher verwendet wird, ist die Schaltfläche **Connect+ aktivieren** deaktiviert.
>
> Klicken Sie auf **Bearbeiten** und geben Sie eine eindeutige E-Mail-Adresse ein.

Eine E-Mail mit Informationen zur Konfiguration von CLIQ Connect wird an die angegebene E-Mail-Adresse gesendet.

Durch Klicken auf die Schaltfläche **E-Mail erneut senden** eines Benutzers von CLIQ Connect+ kann der Administrator auch manuell eine E-Mail senden.

- Wenn CLIQ Connect+ vom Schlüsselhalter nicht aktiviert wurde, enthält die E-Mail Informationen zum Aktivieren des Kontos.
- Wenn CLIQ Connect+ vom Schlüsselhalter aktiviert wurde, enthält die E-Mail Informationen zum Anmelden beim Konto.

Benutzerstatus für CLIQ Connect+ deaktivieren:

1. Deaktivieren: Auf **Connect+ deaktivieren** klicken.
2. Im Popup-Fenster auf **Deaktivieren** klicken.

4.1.5.2 CLIQ Connect+-Berechtigung für mehrere Mitarbeiter konfigurieren

1) Den Mitarbeiter oder Besucher suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

> **Tipp**
> Deaktivierte oder gelöschte Benutzer können über den Filter auf der Registerkarte **Erweitert** gefiltert werden.

2) Wählen Sie die Mitarbeiter und Besucher aus, indem Sie die Kontrollkästchen aktivieren.

> **HINWEIS!**
> Der Benutzerstatus für CLIQ Connect+ kann für bis zu 500 Mitarbeiter oder Besucher gleichzeitig deaktiviert werden.

3) **Benutzerstatus für CLIQ Connect+ aktivieren:**

HINWEIS!
Der Benutzerstatus für CLIQ Connect+ wird nicht für Mitarbeiter oder Besucher aktiviert, die:

- keine registrierte E-Mail-Adresse haben;
- dieselbe E-Mail-Adresse haben wie ein anderer Mitarbeiter oder Besucher, der in CLIQ Connect+ aktiviert ist;
- bereits einen aktivierten Benutzerstatus haben.

1. Auf **Connect+ aktivieren** klicken.

   Ein Popup-Fenster mit Informationen wird geöffnet.

2. Klicken Sie im Popup-Fenster auf **Aktivieren**.

   Eine E-Mail mit Informationen zur Konfiguration von CLIQ Connect wird an die angegebene E-Mail-Adresse gesendet.

   Der Administrator kann die E-Mail auch manuell an einen Benutzer von CLIQ Connect+ senden, indem er in der Ansicht mit den Benutzerinformationen auf die Schaltfläche **E-Mail erneut senden** klickt.

   – Wenn CLIQ Connect+ vom Schlüsselhalter nicht aktiviert wurde, enthält die E-Mail Informationen zum Aktivieren des Kontos.
   – Wenn CLIQ Connect+ vom Schlüsselhalter aktiviert wurde, enthält die E-Mail Informationen zum Anmelden beim Konto.

Benutzerstatus für CLIQ Connect+ deaktivieren:

1. Auf **Connect+ deaktivieren** klicken.

   Ein Popup-Fenster mit Informationen wird geöffnet.

2. Klicken Sie im Popup-Fenster auf **Deaktivieren**.

Das Ergebnis des Vorgangs wird über der Tabelle **SUCHERGEBNIS** angezeigt.

4.1.6 Bearbeiten der Daten zu Mitarbeitern oder Besuchern

Die Vorgehensweise zum Bearbeiten der Mitarbeiter- oder Besucherinformationen in CWM ist in *Abschnitt 4.1.6.2 "Mitarbeiter- oder Besucherinformationen in CWM bearbeiten", Seite 31* beschrieben.

Mitarbeiterinformationen können auch durch Importieren einer aktualisierten CSV-Datei bzw. bei Systemen mit LDAP-Integration über LDAP geändert werden. Weitere Informationen zum Importieren von Mitarbeiterinformationen finden Sie unter *Abschnitt 4.1.11 "Importieren von Mitarbeiterinformationen", Seite 34*. Weitere Informationen zur LDAP-Integration sind in *Abschnitt 8.12 "LDAP-Integration", Seite 196* verfügbar.

HINWEIS!
Für das Bearbeiten oder Löschen einer E-Mail-Adresse eines Mitarbeiters oder Besuchers mit aktiviertem Benutzerstatus für CLIQ Connect+ gelten bestimmte Einschränkungen. Weitere Informationen siehe *Abschnitt 4.1.6.1 "Wichtige Informationen über das Bearbeiten oder Löschen einer E-Mail-Adresse", Seite 31*.

4.1.6.1 Wichtige Informationen über das Bearbeiten oder Löschen einer E-Mail-Adresse

Wenn CLIQ Connect+ aktiviert ist
Mitarbeiter oder Besucher mit aktiviertem Benutzerstatus für CLIQ Connect+ melden sich bei CLIQ Connect mit ihrer in CWM registrierten E-Mail-Adresse an. Das Bearbeiten oder Löschen der E-Mail-Adresse wirkt sich deshalb auf das Anmelden bei CLIQ Connect aus.

Bearbeiten

- Das Ändern der E-Mail-Adresse in eine andere eindeutige E-Mail-Adresse ändert die Anmeldedaten für CLIQ Connect.

  Eine E-Mail mit Informationen zur Konfiguration von CLIQ Connect wird an die angegebene E-Mail-Adresse gesendet.

  – Wenn das Konto für CLIQ Connect+ vom Schlüsselhalter nicht aktiviert wurde, enthält die E-Mail den Kontoaktivierungscode.
  – Wenn das Konto für CLIQ Connect+ vom Schlüsselhalter aktiviert wurde, enthält die E-Mail Informationen zum Anmelden beim Konto.
- Das Ändern der E-Mail-Adresse in eine E-Mail-Adresse, die bereits mit einem anderen Benutzer von CLIQ Connect+ verknüpft ist, ist in CWM nicht zulässig.

  Eine solche Änderung der E-Mail-Adresse über die LDAP-Integration oder eine CSV-Datei wird übersprungen und als Fehler behandelt.

Löschen

- Löschen der E-Mail-Adresse in CWM:

  Durch Löschen wird der Benutzerstatus für CLIQ Connect+ deaktiviert.
- Löschen der E-Mail-Adresse über die LDAP-Integration oder eine CSV-Datei:

  Das Löschen ist nicht zulässig, wenn das Konto für CLIQ Connect+ vom Schlüsselhalter aktiviert wurde.

Wenn die SSO-Anmeldung aktiviert ist
Nachdem einem Mitarbeiter ein Programmierschlüssel zugewiesen wurde, kann die zugehörige E-Mail-Adresse nicht mehr bearbeitet oder gelöscht werden.

4.1.6.2 Mitarbeiter- oder Besucherinformationen in CWM bearbeiten

Dieser Abschnitt beschreibt das Bearbeiten der Mitarbeiter- oder Besucherinformationen in CWM.

Voraussetzungen:

- Der Mitarbeiter oder Besucher, dessen Daten bearbeitet werden sollen, muss aktiv sein.
- Der Mitarbeiter, der bearbeitet werden soll, darf nicht über LDAP integriert sein.

> **HINWEIS!**
> Für Mitarbeiter, die mit LDAP integriert sind, können nur **Domäne** und **TAGS** geändert werden.

1) Den Mitarbeiter oder Besucher suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

2) Auf **Bearbeiten** klicken.

3) Die Felder ändern.

- Bearbeiten von Tags siehe *Abschnitt 4.1.7 "Hinzufügen oder Entfernen von Mitarbeiter- oder Besucher-Tags", Seite 32*.
- Bearbeiten externer Links siehe *Abschnitt 4.1.8 "Verwalten externer Links von Mitarbeitern oder Besuchern", Seite 33*.

4) Auf **Speichern** klicken.

HINWEIS!
Das Ändern dieser Informationen kann zu E-Mail-Benachrichtigungen an den Domänenadministrator führen, damit dieser geeignete Maßnahmen ergreift. Benachrichtigungen werden nur gesendet, wenn sie in den **Systemeinstellungen** aktiviert sind.

Siehe auch *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

4.1.7 Hinzufügen oder Entfernen von Mitarbeiter- oder Besucher-Tags

Informationen zu Tags finden Sie in *Abschnitt 8.2.6 "Tags", Seite 184*.

Voraussetzung:

- Die Mitarbeiter oder Besucher, deren Daten bearbeitet werden sollen, müssen aktiv sein.

1) **Systeminfo » Mitarbeiter** oder **Besucher** auswählen.

Eine Liste aller Mitarbeiter oder Besucher wird angezeigt.

- Um Tags für einzelne Mitarbeiter oder Besucher hinzuzufügen oder zu entfernen, mit *Schritt 2* fortfahren.
- Um Tags für mehrere Mitarbeiter oder Besucher gleichzeitig hinzuzufügen oder zu entfernen, mit *Schritt 3* fortfahren.

2) **Tags für einen einzelnen Mitarbeiter oder Besucher hinzufügen oder entfernen:**

1. Den Mitarbeiter oder Besucher auswählen und die Detailansicht öffnen.
2. Auf **Bearbeiten** klicken.
3. Ein Tag für einen einzelnen Mitarbeiter oder Besucher hinzufügen oder entfernen.

Tag hinzufügen:

a) Auf **Tag hinzufügen...** klicken.
b) Namen für den Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:
Auf den zu entfernenden Tag klicken.

4. Auf **Speichern** klicken.

3) **Tags für mehrere Mitarbeiter oder Besucher hinzufügen oder entfernen:**

1. Mitarbeiter oder Besucher durch Aktivieren der entsprechenden Kontrollkästchen aus den Suchergebnissen auswählen.
2. **Tag hinzufügen:**

a) Auf **Tag hinzufügen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:

a) Auf **Tag entfernen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

4.1.8 Verwalten externer Links von Mitarbeitern oder Besuchern

Informationen über externe Links finden Sie in *Abschnitt 8.4 "Externe Links", Seite 187*.

Voraussetzung:

- Die Mitarbeiter oder Besucher, deren Daten bearbeitet werden sollen, müssen aktiv sein.

1) Den Mitarbeiter oder Besucher suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

2) Auf **Bearbeiten** klicken.
3) **Einen externen Link hinzufügen:**

1. Auf **Hinzufügen.** klicken
2. **Name** für die URL eingeben.
3. **URL** eingeben. Die **URL** muss mit einem Protokoll beginnen (z. B. http:// oder ftp://).

   Wenn in den **Systemeinstellungen** (Eintrag **Externe Links Root-URL**) eine Root-URL festgelegt wurde, muss nur der letzte Teil der URL eingegeben werden. Siehe auch *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.
4. Auf **OK** klicken.

Externen Link bearbeiten:

1. Beim zu bearbeitenden externen Link auf **Bearbeiten** klicken.
2. Die Felder ändern.
3. Auf **OK** klicken.

Einen externen Link entfernen:
Beim zu entfernenden externen Link auf **Entfernen** klicken.

4) Auf **Speichern** klicken.

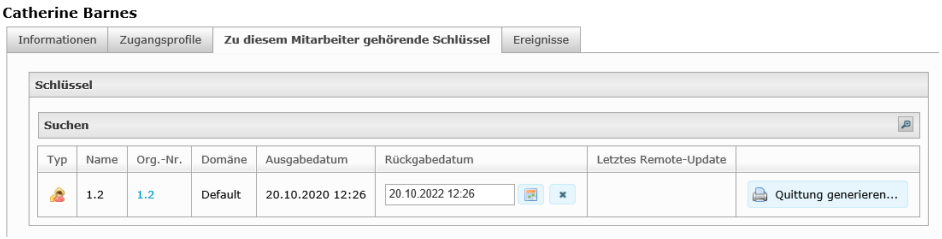
4.1.9 Anzeigen von Mitarbeiter- oder Besucherschlüsseln

1) Den Mitarbeiter oder Besucher suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

2) Register **Zu diesem Mitarbeiter gehörende Schlüssel** oder **Zu diesem Besucher gehörende Schlüssel** auswählen.

   Die aktuell an diesen Mitarbeiter ausgehändigten Schlüssel werden angezeigt.



3)
- Zum Ändern des Rückgabedatums für einen Schlüssel das Feld **Rückgabedatum** bearbeiten.
- Zum Generieren einer Quittung für Ausgabe und Rückgabe des Schlüssels auf **Quittung generieren...** klicken.
- Zur Anzeige der Detailinformationen zum Schlüssel auf die Schlüssel-Org.-Nummer klicken.

4.1.10 Anzeigen von Ereignissen für Mitarbeiter oder Besucher

Die Registerkarte **Ereignisse** enthält eine Aufzeichnung der administrativen Aktivitäten in CWM, einschließlich Aktionen wie das Erstellen eines Mitarbeiters oder Besuchers oder das Aktualisieren des Status von CLIQ Connect+. Außerdem werden hier schlüsselbezogene Ereignisse, die mit einem Mitarbeiter oder Besucher verknüpft sind, protokolliert.

1) Den Mitarbeiter oder Besucher suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

2) In der Detailanzeige das Register **Ereignisse** auswählen.

   Eine Liste von Mitarbeiter- oder Besucherereignissen wird angezeigt.

4.1.11 Importieren von Mitarbeiterinformationen

Durch **Importieren von Mitarbeitern** können neue oder aktualisierte Mitarbeiterdaten im Massenverfahren importiert werden.

> **HINWEIS!**
> Über die LDAP-Integration hinzugefügte Mitarbeiter können nicht durch Importieren einer CSV-Datei bearbeitet werden.

Voraussetzung:

- Beachten Sie beim Erstellen einer CSV-Importdatei die Informationen zum Format in *Abschnitt 9.9 "Dateiformat für Mitarbeiterimport", Seite 216*.

1) **Verwaltung » Mitarbeiter importieren** auswählen.
2) Auf **Auswählen...** klicken.
3) Wählen Sie die hochzuladende Datei und klicken Sie auf **Öffnen**.

4) Auf **Hochladen** klicken.

Es wird angezeigt, wie viele gültige Einträge in der Datei vorhanden sind. Wenn ungültige Einträge vorhanden sind, klicken Sie auf **Details**, um weitere Informationen zu erhalten.

5) Auf **Import** klicken.

4.1.12 Mitarbeiter- oder Besucherinformationen exportieren

1) Die gewünschten Mitarbeiter oder Besucher suchen.

Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

2) In den Suchergebnissen die Mitarbeiter oder Besucher auswählen, deren Informationen exportiert werden sollen.

3) Auf **In CSV-Datei exportieren** klicken.

Informationen zu deaktivierten Mitarbeitern oder Besuchern können nicht exportiert werden.

HINWEIS!
Damit die Excel-Datei korrekt geöffnet werden kann, muss das Trennzeichen entsprechend den regionalen Einstellungen eingestellt sein. Ändern des Trennzeichens siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

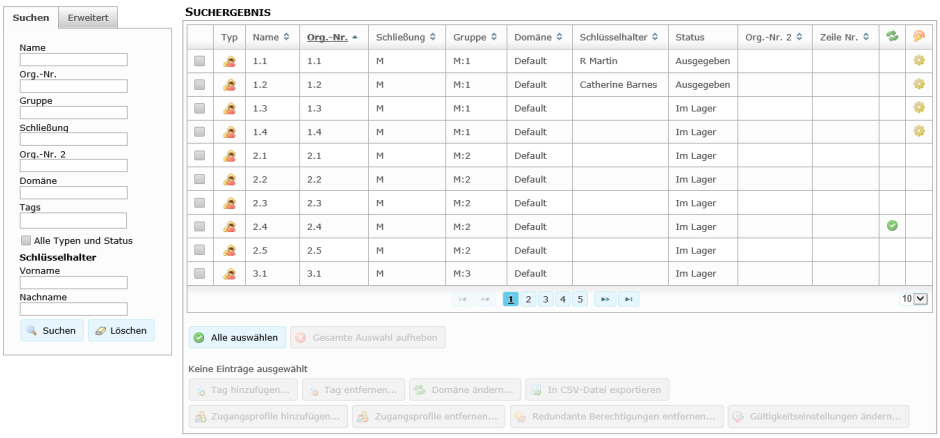
4) Im Pop-up-Fenster Dateidownload auf **Öffnen** oder **Speichern** klicken.

4.2 Verwalten von Schlüsseln

4.2.1 Benutzerschlüssel suchen

1) **Systeminfo » Schlüssel** auswählen.

Eine Liste aller Schlüssel wird angezeigt.



Folgende Symbole werden verwendet:

- Mechanischer Schlüssel
- E1-Schlüssel
- E2-Schlüssel
- CLIQ Connect E2-Schlüssel

- E3-Schlüssel
- CLIQ Connect E3-Schlüssel
- Für den Schlüssel steht ein Remote-Update an

2) Register **Suchen** oder **Erweitert** auswählen.

   Standardmäßig werden mechanische Schlüssel und Schlüssel, die als verloren oder defekt gemeldet wurden, nicht angezeigt. Um auch diese Schlüssel in die Suchergebnisse zu integrieren, **Alle Typen und Status** auswählen.

   Das Register **Erweitert** enthält auch die Suchfelder für Schlüsseltyp, CLIQ Connect-Schlüssel, Inventarstatus und Funktionsstatus.

3) Suchkriterien eingeben.

   Bei Eingabe im Suchfeld **Tags** erscheinen alle passenden Tags in einer Auswahlliste.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

4) Auf **Suchen** klicken.

5) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf die Zeile mit dem entsprechenden Schlüssel klicken.

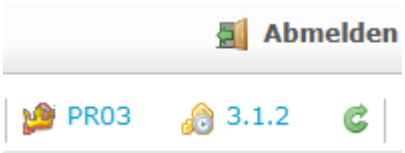
   Informationen zu den Merkmalen des Schlüssels siehe *Abschnitt 9.3.3 "Schlüsselattribute", Seite 203*.

4.2.2 Benutzerschlüssel abfragen

1) Schlüssel in den rechten Schlitz des lokalen PGs einführen.

2) In der oberen rechten Ecke der Seite auf klicken.

   Beide Schlüssel im lokalen Programmiergerät werden unterhalb der Navigationsleiste angezeigt.



3) Auf den Schlüssel im rechten Schlitz des lokalen Programmiergeräts klicken.

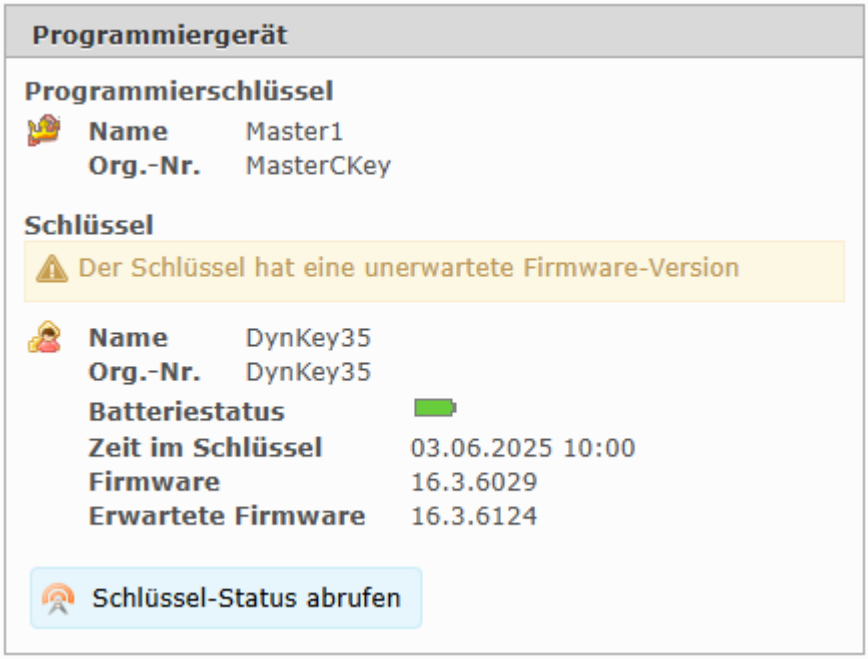
   Die detaillierte Informationsansicht des Schlüssels wird angezeigt. Rechts auf der Seite werden **Name** und **Org.-Nr.** angezeigt.

4.2.3 Schlüsselstatus anzeigen

1) Den Schlüssel abfragen. Siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Auf **Schlüssel-Status abrufen** klicken.

   Grundlegende Informationen zum Schlüssel werden angezeigt. Weitere Informationen über die Batteriestatusanzeige finden Sie unter *Abschnitt 9.6 "Anzeige der Batterieladung", Seite 214*.



4.2.4 Bearbeiten von Informationen für Benutzerschlüssel

1) Den Schlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Auf **Bearbeiten** klicken.

3) Zum Bearbeiten des Schlüsselnamens die Eingabe im Feld **Name** ändern.

4) Um ein Tag hinzuzufügen, auf **Tag hinzufügen** klicken.

   Siehe auch *Abschnitt 4.2.5 "Benutzerschlüssel-Tags hinzufügen oder entfernen", Seite 37*.

5) Um einen externen Link hinzuzufügen, auf **Externen Link hinzufügen** klicken.

   Siehe auch *Abschnitt 4.2.6 "Externe Links für Benutzerschlüssel verwalten", Seite 38*.

6) Auf **Speichern** klicken.

4.2.5 Benutzerschlüssel-Tags hinzufügen oder entfernen

Informationen zu Tags finden Sie in *Abschnitt 8.2.6 "Tags", Seite 184*.

1) Zu bearbeitenden Schlüssel suchen.

   Suche nach einem Schlüssel siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Informationen über das Abfragen des Schlüssels im lokalen Programmiergerät finden Sie in *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) - Um Tags für einzelne Schlüssel hinzuzufügen oder zu entfernen, gehen Sie zu *Schritt 3*.
   - Um Tags für mehrere Schlüssel hinzuzufügen oder zu entfernen, gehen Sie zu *Schritt 4*.

3) **Tags für einen einzelnen Schlüssel hinzufügen oder entfernen:**

1. Den Schlüssel auswählen und die Detailansicht öffnen.
2. Auf **Bearbeiten** klicken.
3. Ein Tag für einen einzelnen Schlüssel hinzufügen oder entfernen.

Tag hinzufügen:

a) Auf **Tag hinzufügen...** klicken.
b) Namen für den Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:
Auf den zu entfernenden Tag klicken.

4. Auf **Speichern** klicken.

4) **Tags für mehrere Schlüssel hinzufügen oder entfernen:**

1. Schlüssel durch Aktivieren der Kontrollkästchen in den Suchergebnissen auswählen.
2. **Tag hinzufügen:**

a) Auf **Tag hinzufügen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:

a) Auf **Tag entfernen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

4.2.6 Externe Links für Benutzerschlüssel verwalten

Informationen über externe Links finden Sie in *Abschnitt 8.4 "Externe Links", Seite 187*.

1) Den Schlüssel suchen und die Detailansicht öffnen.

Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Auf **Bearbeiten** klicken.
3) Hinzufügen eines externen Links:

a) Auf **Hinzufügen** klicken.
b) **Name** für die URL eingeben.
c) **URL** eingeben. Die **URL** muss mit einem Protokoll beginnen (z. B. http:// oder ftp://).

Wenn in den **Systemeinstellungen** (Eintrag **Externe Links Root-URL**) eine Root-URL festgelegt wurde, muss nur der letzte Teil der URL eingegeben

werden. Siehe auch *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

d) Auf **OK** klicken.

4) Bearbeiten eines externen Links:

a) Beim zu bearbeitenden externen Link auf **Bearbeiten** klicken.

b) Die Felder ändern.

c) Auf **OK** klicken.

5) Einen externen Link entfernen: Beim zu entfernenden externen Link auf **Entfernen** klicken.

6) Auf **Speichern** klicken.

4.2.7 Anzeigen der Update-Historie für einen Benutzerschlüssel

Das Register **Update-Historie** wird zur Verfolgung von Schlüsselprogrammierungen verwendet.

Voraussetzungen:

- Die Benutzerberechtigungsstufe muss auf **Anzeige** in der Rolle **Schlüssel: Update-Historie** festgelegt sein.

  Informationen zum Ändern der Berechtigungsstufe finden Sie in *Abschnitt 6.7 "Verwalten von Rollen und Rechten", Seite 131*.

-

1) Den Schlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Register **Update-Historie** auswählen.

   Eine Liste mit allen Schlüssel-Updates wird angezeigt.

   HINWEIS!
   Gemäß Voreinstellung werden Schlüssel-Updates, mit Ausnahme von Firmware-Updates, nach 3 Monaten gelöscht.

   Folgende Symbole werden verwendet:

   - Für ein lokales PG ist ein Programmierungs-Job vorhanden, der jedoch nicht initiiert wurde
   - Für den Schlüssel steht ein Remote-Update an
   - Programmierungs-Job ist abgeschlossen
   - Programmierungs-Job fehlgeschlagen oder abgebrochen
   - Programmierungs-Job wurde durch einen neuen Job ersetzt

3) Zur Anzeige weiterer Details zu einem speziellen Update auf den Link in der Spalte **Grund** klicken.

4.2.8 Anzeigen der Ereignisse für eine Benutzerschlüssel

Das Register Ereignisse wird zur Verfolgung von Administratorvorgängen in CWM verwendet, z. B. das Aushändigen eines Schlüssels, die Verknüpfung von Zugangsprofilen, das Ändern von Schlüssel-Berechtigungen usw.

1) Den Schlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Register **Ereignisse** auswählen.

   Eine Liste mit allen Schlüssel-Ereignissen wird angezeigt.

4.2.9 Benutzerschlüssel ausgeben

Der Ausgabeprozess umfasst zwei Phasen:

1. **Ausgabeeinstellungen**

   In dieser Phase werden die Ausgabeeinstellungen auf drei verschiedenen Seiten konfiguriert: **Allgemein**, **Berechtigungen** und **Zeiteinstellungen**.

   Die Einstellungen auf der Seite **Allgemein** müssen abgeschlossen werden. Die Einstellungen auf den anderen Seiten sind optional.

2. **Zusammenfassung der Ausgabe**

   In dieser Phase werden die Details der Ausgabe bestätigt und der Schlüssel ausgegeben. Wenn der ausgegebene Schlüssel in das PG eingeführt wird, wird er ebenfalls programmiert.

1) Der Prozess der Schlüsselausgabe kann auf zwei Weisen gestartet werden:

   - **Arbeit » Schlüsselausgabe » An Mitarbeiter** oder **An Besucher** auswählen.
   - Über die Detailansicht des Mitarbeiters oder Besuchers:

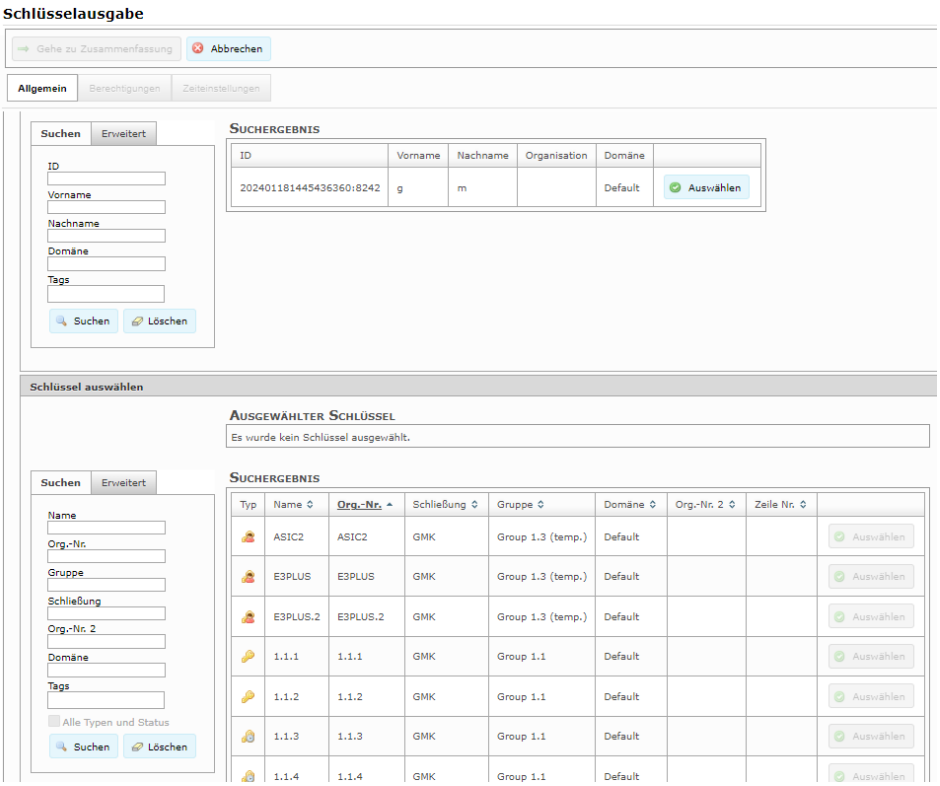
     a) Den Schlüssel suchen und die Detailansicht öffnen.

        Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

        Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

     b) Auf **Schlüsselausgabe** klicken.

   Die Seite **Schlüsselausgabe**, **Allgemein** wird geöffnet.



2) Wenn im Bereich **Mitarbeiter auswählen** oder **Besucher auswählen** kein ausgewählter Mitarbeiter oder Gast vorhanden ist, suchen Sie die Person und klicken Sie auf **Auswählen**.

   Suche nach einem Mitarbeiter oder Besucher siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

3) Wählen Sie den auszugebenden Schlüssel auf eine der folgenden Weisen aus:

   - Wenn der auszugebende Schlüssel vorliegt:

     a) Setzen Sie den Schlüssel in das rechte Schlüsselloch des lokalen PG ein.

     b) Klicken Sie oben rechts auf der Seite auf , um den Schlüssel abzufragen.

     c) Klicken Sie im Feld **Benutzerschlüssel im PG** auf **Auswählen**.

     Normalerweise ist es empfehlenswert, die Ausgabe eines Schlüssels über die Abfragefunktion vorzunehmen, da in diesem Fall die neue Konfiguration direkt auf dem Schlüssel programmiert werden kann. Besonders wichtig ist dies bei Anlagen, die keine Remote-Systeme sind.

   - Wenn der auszugebende Schlüssel nicht vorliegt:

     a) Suchen Sie den Schlüssel in einer der folgenden Listen und klicken Sie auf **Auswählen**.

        - Liste **VORBESTELLTER SCHLÜSSEL**

          Sind mit der ausgewählten Person Schlüsselvorbestellungen verknüpft, wird in der Schlüsselauswahl-Ansicht eine Liste der vorbestellten Schlüsseln angezeigt.

Tipp
Bei einem vorbestellten Schlüssel handelt es sich um einen Schlüssel, der bei Bestellung mit einer bestimmten Person verknüpft wird.

Die Verknüpfung des Schlüssels mit einer bestimmten Person hilft Administratoren dabei, während des Ausgabevorgangs den richtigen Schlüssel für die betreffende Person auszuwählen.

Der Schlüsselstatus bleibt **Im Lager** nach dem Import des Schlüssels in das System, unabhängig davon, ob der Schlüssel vom CLIQ-Händler tatsächlich eingetroffen ist oder nicht.

Der Schlüssel kann an eine beliebige Person ausgegeben werden und verliert den Vorbestellstatus, sobald er ausgegeben wurde.

- Liste **SUCHERGEBNIS**

  Um die Liste einzugrenzen, geben Sie Suchkriterien ein und klicken Sie auf **Suchen**. Siehe auch *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.

4) Legen Sie bei Bedarf die Details auf der Seite **Berechtigungen** und der Seite **Zeiteinstellungen** fest.

   Springen Sie andernfalls direkt zu *Schritt 5*.

HINWEIS!
Alle der folgenden Einstellungen gelten für E3-Schlüssel in Zylindergruppen-Remote-Systemen. Bei anderen Schlüsseltypen und Konfigurationen sind bestimmte Einstellungen nicht verfügbar.

Seite „Berechtigungen“

- **Zugangsprofile auswählen**

  Wählen Sie Zugangsprofile aus der Liste aus.

  Standardmäßig sind die Mitarbeiter- oder Besucherprofile ausgewählt.

- **Zylindergruppen auswählen**

  Wählen Sie die Zylindergruppen aus, zu denen der Schlüssel expliziten Zugang haben soll.

- **Zylinder auswählen**

  Wählen Sie die Zylinder aus, zu denen der Schlüssel expliziten Zugang haben soll.

Seite „Zeiteinstellungen“

- **Schlüsselgültigkeit festlegen**

  – **AUSGABEDATUM UND RÜCKNAHMEDATUM AUSWÄHLEN**

Geben Sie das Ausgabedatum (**Ausgabedatum**) und das Rücknahmedatum (**Rückgabedatum**) ein:

Wenn das Rücknahmedatum noch nicht bekannt ist, klicken Sie auf **X**.

– **SCHLÜSSELGÜLTIGKEIT FESTLEGEN**

Legen Sie die folgenden Einstellungen für die Schlüsselgültigkeit fest.

- Aktivierungseinstellungen aus **Inaktiv**, **Aktiv im festgelegten Zeitraum** und **Immer aktiv** auswählen.

  Wenn **Aktiv im festgelegten Zeitraum** ausgewählt ist, legen Sie das Datum für **Schlüssel aktiv von** und für **Schlüssel aktiv bis** fest.

  Wenn das Datum für **Schlüssel aktiv bis** noch nicht bekannt ist, klicken Sie auf **X**.
- Um die Verlängerungsfunktion zu verwenden, aktivieren Sie das Kontrollkästchen neben **Verlängerung verwenden** und legen Sie das Zeitintervall fest.

  Bei Nutzung dieser Funktion muss der Schlüssel in festgelegten Zeitabständen aktualisiert werden, um aktiv zu bleiben.
- **Nur CLIQ Connect-Schlüssel**:

  Um die **PIN-Validierung** zu verwenden, aktivieren Sie das Kontrollkästchen und legen Sie das Zeitintervall fest.

  Bei Nutzung dieser Funktion muss die PIN des Schlüssels in festgelegten Zeitabständen über CLIQ Connect validiert werden, damit der Schlüssel aktiv bleibt.

Für weitere Informationen zur Gültigkeit des Schlüssels siehe *Abschnitt 8.1.4 "Schlüsselgültigkeit", Seite 170*.

- **Schlüsselzeitplan auswählen**

  SCHLÜSSELZEITPLAN

  Den Schlüsselzeitplan wie folgt einstellen:

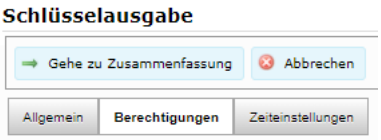
  a) Bei Vorhandensein einer zu nutzenden Zeitplanvorlage Auswahl in der Drop-down-Liste treffen und auf **Anwenden** klicken.

  b) Klicken Sie auf **Zeitraum hinzufügen**, um einen Zeitraum zur ausgewählten Vorlage hinzuzufügen oder den Zeitplan benutzerdefiniert anzupassen.

  c) Auf **Zylinder hinzufügen** klicken, um einen bestimmten Zeitraum für einen Zylinder einzustellen.

  Einen Zylinder aus der angezeigten Liste auswählen und zur Einstellung des Zeitraums auf **Zeitraum hinzufügen** klicken.

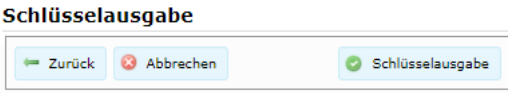
5) Auf **Gehe zu Zusammenfassung** klicken.



Eine Zusammenfassung der Zugangsrechte und der Zeiteinstellungen wird angezeigt.

6) Überprüfen Sie die Einstellungen.

Wenn Sie die Einstellungen ändern möchten, klicken Sie auf **Zurück**, um zur Einstellungsseite zurückzukehren.



7)
- Wenn der auszugebende Schlüssel im lokalen Programmiergerät ist, auf **Programmieren und Speichern** klicken.

  Der Schlüssel wird direkt im Programmiergerät programmiert.
- Wenn der auszugebende Schlüssel nicht im lokalen Programmiergerät ist, auf **Schlüsselausgabe** klicken.

  In den Remote-Systemen wird ein Job zum Remote-Update erstellt.

8) Optional: Eine Quittung erstellen.

Quittungen werden in Form von PDFs erstellt, die gedruckt oder gespeichert werden können.

Zur Erstellung oder Bearbeitung von Quittungsvorlagen siehe *Abschnitt 6.9 "Verwalten von Quittungsvorlagen", Seite 134*.

a) Auf **Quittung generieren...** klicken.

   Das Fenster **Quittungsauswahl** wird geöffnet.

b) Die entsprechende Sprache in der Drop-down-Liste auswählen.

c) Die entsprechende Vorlage in der Drop-down-Liste auswählen.

   In der Drop-down-Liste werden alle Vorlagen für eine Ausgabequittung in der ausgewählten Sprache angezeigt.

d) Auf **Quittung generieren** oder **Herunterladen** klicken.

9) Optional: Stellen Sie einen QR-Code zum Konfigurieren der Server-URL für CLIQ Remote aus und geben Sie ihn zusammen mit dem Schlüssel aus.

Wenn der Schlüsselhalter CLIQ Connect verwenden möchte und das CWM-System nicht mit DCS integriert ist, muss der Schlüsselhalter die Server-URL für CLIQ Remote manuell in CLIQ Connect eingeben. Durch Generieren eines QR-Codes für die CLIQ Remote-Server-URL und Bereitstellen dieses Codes für den Schlüsselhalter lässt sich die App-Konfiguration vereinfachen.

a) Öffnen Sie einen beliebigen, online verfügbaren QR-Generator.

b) Geben Sie die Informationen in dieser Reihenfolge ein: `<ASSA ABLOY-Firmencode>,<MKS-Name>,<URL>`

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

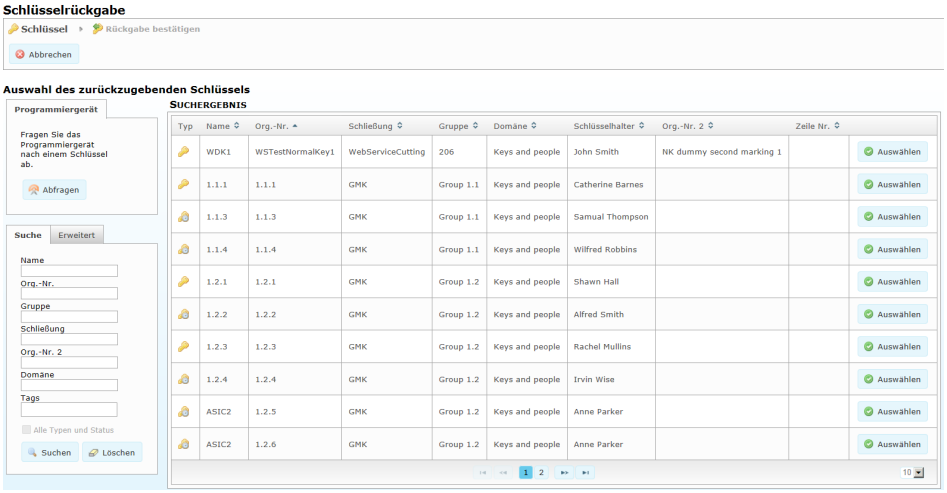
Die ASSA ABLOY-Firmencodes finden Sie in *Abschnitt 9.10 "ASSA ABLOY-Firmencode", Seite 218*.

c) Drucken Sie den QR-Code.

4.2.10 Rücknahme von Benutzerschlüsseln (Rückgabe)

1) **Arbeit » Schlüsselrückgabe** auswählen.

Eine Liste aller ausgegebenen Schlüssel wird angezeigt.



2) Den zurückzunehmenden Schlüssel mit einer der folgenden Vorgehensweisen finden und auswählen:

- In der Liste auf **Auswählen** für den zurückzunehmenden Schlüssel klicken.

  Um den Schlüssel zu suchen, die Suchkriterien eingeben und auf **Suchen** klicken. Siehe auch *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.
- Wenn sich der zurückzunehmende Schlüssel im rechten Schlitz des lokalen PG befindet, auf  in der rechten oberen Ecke der Seite klicken, um den Schlüssel abzufragen.

  Normalerweise ist es empfehlenswert, die Rückgabe eines Schlüssels über die Abfragefunktion vorzunehmen, da in diesem Fall die neue Konfiguration direkt auf dem Schlüssel programmiert werden kann. Besonders wichtig ist dies bei Anlagen, die keine Remote-Systeme sind.

3) Rückgabe eines Schlüssels:

- Wenn der zurückgegebene Schlüssel im lokalen PG abgefragt wird, auf **Schlüssel zurücksetzen und zurückgeben** oder **Schlüsselrückgabe ohne Zurücksetzen** klicken.

  Die Option Zurücksetzen ist nützlich bei Schlüsseln, die bei jeder Ausgabe unterschiedliche Einstellungen haben, und wird für die Mehrheit der Anwendungen empfohlen.
- Wenn der zurückgegebene Schlüssel nicht abgefragt wird, auf **Anwenden** klicken.

4) Optional: Eine Quittung erstellen. Quittungen werden in Form von PDFs erstellt, die gedruckt oder gespeichert werden können.

HINWEIS!

Die Option ist nur bei Auswahl von **Gesonderte Rückgabe- und Ausgabequittungen** in **Systemeinstellungen** verfügbar. Diese Einstellung wird durch Auswahl von **Verwaltung » Systemeinstellungen » VERWALTUNG » Schlüsselquittungen** erreicht.

Weitere Informationen zur Bearbeitung von Systemeinstellungen siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

Informationen über das Erstellen und Bearbeiten von Quittungsvorlagen finden Sie in *Abschnitt 6.9 "Verwalten von Quittungsvorlagen", Seite 134*.

a) Auf **Quittung generieren...** klicken.

   Das Fenster **Quittungsauswahl** wird geöffnet.

b) Die entsprechende Sprache in der Drop-down-Liste auswählen.

c) Die entsprechende Vorlage in der Drop-down-Liste auswählen.

   In der Drop-down-Liste werden alle Vorlagen für eine Rücknahmequittung in der ausgewählten Sprache angezeigt.

d) Auf **Quittung drucken** oder **Herunterladen** klicken.

   Wenn **Herunterladen** ausgewählt wird, wird die Quittung in den Ordner **Downloads** heruntergeladen.

4.2.11 Drucken einer Leerquittung

Bei Ausgabe oder Rücknahme eines Schlüssels wird die Quittung mit den Ausgabe- oder Rücknahmeinformationen im PDF-Format erstellt. Außerdem ist die Generierung von Quittungen möglich, deren Felder zum manuellen Ausfüllen leer gelassen werden.

1) **Arbeit » Quittung**.
2) **Leere Ausgabequittung ausdrucken...** oder **Leere Rückgabequittung ausdrucken...** auswählen.
3) Im Pop-up-Fenster:
   a) Die entsprechende Sprache in der Drop-down-Liste auswählen.
   b) Die zu nutzende Vorlage auswählen.

      Bei Auswahl von **Benutzerdefiniert** werden alle Vorlagen desselben Typs (Quittung für Ausgabe oder Rücknahme) für die ausgewählte Sprache in der Drop-down-Liste angezeigt.
4) Auf **Quittung generieren** oder **Herunterladen** klicken.

4.2.12 Umgang mit einem verlorenen oder defekten Schlüssel

Dieser Abschnitt beschreibt, wie Nutzerschlüssel als verloren oder defekt gemeldet werden. Informationen über das Melden eines verlorenen oder defekten Programmierschlüssels finden Sie in *Abschnitt 6.11.9 "Verlorenen Programmierschlüssel melden und sperren", Seite 142* und *Abschnitt 6.11.10 "Programmierschlüssel als defekt oder funktionsfähig melden", Seite 144*.

4.2.12.1 Defekten Benutzerschlüssel melden

1) Es gibt zwei Möglichkeiten, einen defekten Schlüssel zu melden:

- **Arbeit » Schlüssel als defekt melden** auswählen. Fahren Sie mit *Schritt 2* fort.
- In der Detailansicht des defekten Schlüssels (zum Suchen des Schlüssels siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*) auf die Schaltfläche **Als defekt melden** klicken. Fahren Sie mit *Schritt 4* fort.

2) Suchkriterien eingeben, um den Halter des Schlüssels zu finden, und auf **Suchen** klicken.
3) Defekten Schlüssel auswählen.
4) Auf **Anwenden** klicken.

   Die Detailinformationen für einen als verloren gemeldeten Schlüssel enthalten die Option zum Löschen des Status "defekt".

Wenn der defekte Schlüssel durch einen geklonten Schlüssel ersetzt werden soll, beachten Sie die Anweisungen unter *Abschnitt 4.2.13 "Benutzerschlüssel durch einen Klon aus dem Werk ersetzen", Seite 51*.

4.2.12.2 Verlorenen Benutzerschlüssel melden und sperren

Voraussetzung:

- Wenn Zylinder gesperrt werden müssen und der Zylinderprogrammierjob einem Benutzerschlüssel zugewiesen ist, sicherstellen, dass in den Systemeinstellungen „Verlorenen Schlüssel mit Benutzerschlüsseln sperren“ aktiviert ist. Anweisungen zum Ändern dieser Einstellung finden Sie unter *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*. Dies gilt nur für ein Remote-System.

1) Es gibt zwei Möglichkeiten, einen verlorenen Schlüssel zu melden:

   - **Arbeit » Schlüssel als verloren melden** auswählen. Fahren Sie mit *Schritt 2* fort.
   - In der Detailansicht des verlorenen Schlüssels (zum Suchen des Schlüssels siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*) auf die Schaltfläche **Als verloren melden** klicken. Fahren Sie mit *Schritt 4* fort.

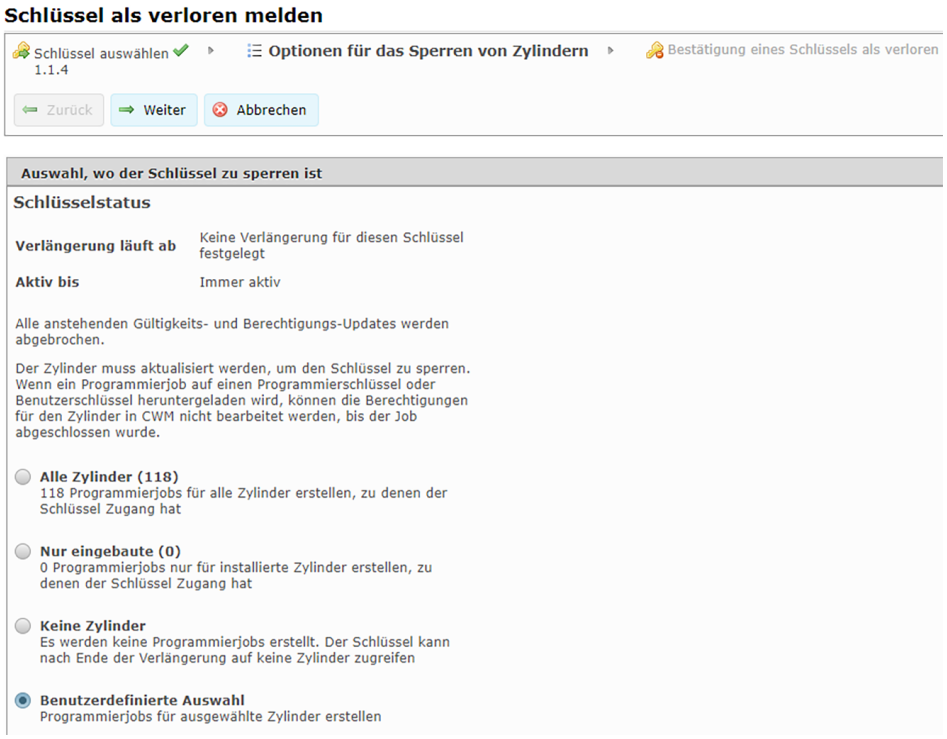
2) Suchkriterien eingeben, um den Halter des Schlüssels zu finden, und auf **Suchen** klicken.
3) Wählen Sie den verlorenen Schlüssel aus und klicken Sie auf **Auswählen**.
4) Wählen Sie die Zylinder aus, für die der Schlüssel gesperrt werden soll:

   - Wenn die Zylinder zum sofortigen Sperren des verlorenen Schlüssels programmiert werden sollen:

     Tipp
     Um das System so zu konfigurieren, dass verlorene Schlüssel in neu hinzugefügten Zylindern gesperrt werden, die Option **Verlorene Schlüssel in neuen Zylindern während des Erweiterungsimports blockieren** in den Systemeinstellungen aktivieren. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

     – Wählen Sie **Alle Zylinder** oder **Nur eingebaute** aus und fahren Sie mit *Schritt 7* fort.

  - Wählen Sie **Benutzerdefinierte Auswahl** aus fahren Sie mit *Schritt 5* fort, um die Zylinder auszuwählen.
- Wenn der Schlüssel in CWM als verloren gemeldet werden soll, ohne den Zugang zu sperren (z. B. während auf den Ablauf des aktuellen Verlängerungsintervalls gewartet wird), wählen Sie **Keine Zylinder** aus, klicken Sie auf **Weiter** und fahren Sie mit *Schritt 11* fort.



5) Auf **Weiter** klicken.
6) Die Zylinder auswählen, für die der verlorene Schlüssel gesperrt werden soll.
7) Auf **Weiter** klicken.

8) Optional: Den Sperrschlüssel durch Klicken auf **Auswählen** aus der Liste auswählen.

> **HINWEIS!**
> Wird dieser Vorgang übersprungen, werden Zylinderprogrammierjobs für Programmierschlüssel erstellt.

Wählen Sie auf der Registerkarte **Suchen** die Option **Alle Typen und Status** aus, um Programmierschlüssel anzuzeigen.

Auf der Registerkarte **Erweitert** unter **Typ** die gewünschten Schlüsseltypen auswählen, um den Listeninhalt anzupassen.

> **HINWEIS!**
> Anforderungen an Sperrschlüssel:
>
> - Der Sperrschlüssel muss der Generation 2 angehören und die Firmwareversion 12.2 oder höher haben.
> - Der Sperrschlüssel muss über ausreichend Speicher verfügen.

9) Wählen Sie auf der Bestätigungsseite unter **Priorität** die Prioritätsstufe aus.

Dringende Jobs sollten hohe Priorität haben.

10)

> **WARNUNG!**
> Auch wenn kein Zylinderprogrammierjob zum Sperren des verlorenen Schlüssels erstellt wird, wird der verlorene Schlüssel in CWM standardmäßig zur **Liste der nicht berechtigten Schlüssel** für die betreffenden Zylinder hinzugefügt. Diese Information ist in CWM jedoch nicht sichtbar. Wenn die betreffenden Zylinder später neu programmiert oder ausgetauscht werden, werden die in CWM gespeicherten Informationen über nicht berechtigte Schlüssel übernommen, sodass der verlorene Schlüssel gesperrt bleibt. Wenn der verlorene Schlüssel später wieder als gefunden gemeldet wird, bleibt er daher in neu programmierten oder ausgetauschten Zylindern gesperrt.
>
> Informationen zum erneuten Autorisieren des gefundenen Schlüssels für diese Zylinder finden Sie in *Abschnitt 4.9.2 "Konfigurieren von Berechtigungen in Zylindern", Seite 83*.
>
> Diese Standardeinstellung kann durch Deaktivieren der Systemeinstellung **Verlorene Schlüssel in Zylinder während des Berechtigungs-Updates unsichtbar blockieren** geändert werden. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

Klicken Sie auf **Als verloren melden**, nachdem Sie alle Informationen überprüft haben.

11) Optional: Klicken Sie auf **Zylinderliste ausdrucken**, um eine PDF-Zusammenfassung zu erstellen.

12) • Wurde für die Programmierung der Zylinder **KEIN** bestimmter Schlüssel ausgewählt, mit *Schritt 4* in *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64* fortfahren.
    • Wenn ein bestimmter Schlüssel für die Programmierung der Zylinder ausgewählt wurde, die nachstehenden Anweisungen befolgen.

13) Die Detailansicht des ausgewählten Sperrschlüssels öffnen.

> **Tipp**
> Durch Klicken auf **Schlüssel-Org.-Nr.** unter **Sperrschlüsselinformationen** wird direkt die Informationsansicht geöffnet.

14) Wechseln Sie zur Registerkarte **Programmierjobs** und bestätigen Sie, dass der Zylinderjob dem Schlüssel zugewiesen ist.

15) • **Programmierung im lokalen PG**

    Den Sperrschlüssel in den rechten Steckplatz des lokalen PG einführen und den Programmierschlüssel aus dem linken Steckplatz des lokalen PG entfernen.

    • **Programmierung in einem Wand-Programmiergerät**

    Den Sperrschlüssel in ein Wand-Programmiergerät einführen.

    Der Zylinderprogrammierjob wird automatisch auf den Sperrschlüssel geschrieben.

16) Jeden Zylinder mit dem Sperrschlüssel neu programmieren.

17) Nach dem Programmieren der Zylinder die abgeschlossenen Zylinderjobs melden. Dazu den Sperrschlüssel in eines der folgenden Geräte einführen:

    • Rechter Steckplatz des lokalen PG (entfernen Sie den Programmierschlüssel aus dem linken Steckplatz)
    • Wand-Programmiergerät

4.2.12.3 Gefundenen Benutzerschlüssel melden

1) Den verlorenen Schlüssel in CWM suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36* oder *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.

> **HINWEIS!**
> Verlorene Schlüssel können mithilfe des Filters **Verloren** auf der Registerkarte **Erweitert** gefiltert werden.

2) Auf **Als gefunden melden** klicken.

   Der Status des Schlüssels ändert sich zu **Im Lager**.

3) Den Schlüssel durch erneutes Programmieren der betroffenen Zylinder wieder autorisieren. Die Anweisungen unter *Abschnitt 4.9.2 "Konfigurieren von Berechtigungen in Zylindern", Seite 83* befolgen.

   Informationen dazu, welche Zylinder betroffen sind, finden Sie unten.

Betroffene Zylinder

Zylinder, die **programmiert werden müssen**, um den Schlüssel wieder zu autorisieren:

- Zylinder, die bereits zur Sperrung des verlorenen Schlüssels programmiert wurden
- Zylinder, die **nicht** zur Sperrung des verlorenen Schlüssels programmiert wurden, müssen im folgenden Fall programmiert werden:
  - Der Zylinder wurde **neu programmiert** oder **ersetzt**.

    UND
  - Die Systemeinstellung **Verlorene Schlüssel in Zylinder während des Berechtigungs-Updates unsichtbar blockieren** ist **aktiviert**.

> **HINWEIS!**
> Dies gilt sowohl für Zylinder, für die keine Programmierjobs erstellt wurden, als der Schlüssel als verloren gemeldet wurde, als auch für Zylinder, für die Programmierjobs zwar erstellt, aber noch nicht ausgeführt wurden.

Alle anderen Zylinder:

Der Schlüssel hat bereits Zugriff und die Zylinder müssen nicht programmiert werden. (Erstellte, aber noch nicht ausgeführte Programmierjobs werden automatisch gelöscht.)

4.2.13 Benutzerschlüssel durch einen Klon aus dem Werk ersetzen

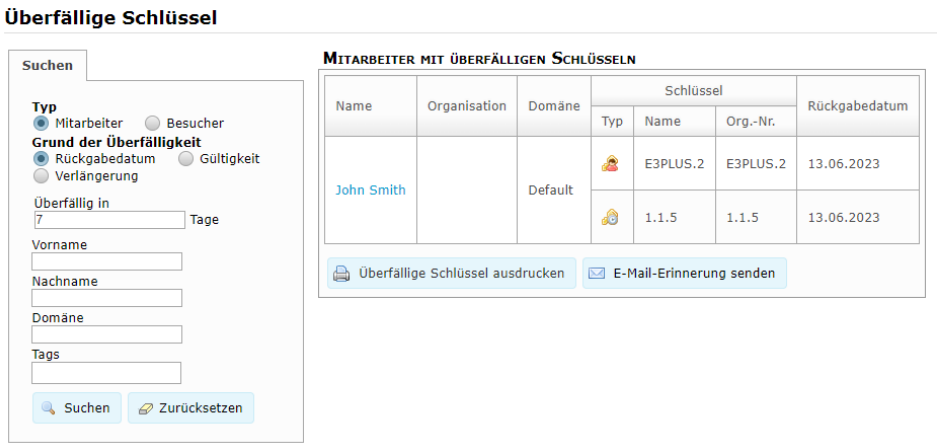
Wenn aufgrund eines defekten Schlüssels ein Austauschklon aus dem Werk geliefert wird, müssen folgende Schritte durchgeführt werden, um die Funktionalität des Schlüssels sicherzustellen.

1) Wenn der Austauschschlüssel aus dem Werk eintrifft, zu **Verwaltung » Erweiterungsimport » Erweiterungsimportdatei(en) hochladen oder holen** wechseln, um entweder die zur Verfügung gestellte CWS-Datei in CWM hochzuladen (bei deaktivierter DCS-Integration) oder die Datei aus DCS abzurufen.
2) Für den Austauschschlüssel einen Berechtigungsjob erstellen und programmieren. Siehe *Abschnitt 4.9.1 "Konfigurieren von Berechtigungen in Schlüsseln", Seite 81*.
3) Für den Austauschschlüssel einen Gültigkeitsjob erstellen und programmieren. *Abschnitt 4.10.1 "Konfigurieren der Schlüsselgültigkeit, Verlängerung und PIN-Validierung", Seite 89*.
4) Alle vorhandenen Zeitplanjobs des alten Schlüssels abbrechen und für den Austauschschlüssel neu erstellen und programmieren. Siehe *Abschnitt 4.10.3 "Konfigurieren des Schlüsselzeitplans", Seite 92*.
5) Der Austauschschlüssel ist einsatzbereit.

4.2.14 Überfällige Benutzerschlüssel anzeigen

1) **Arbeit » Überfällige Schlüssel** auswählen.
2) Auf der Registerkarte **Suchen** durch Auswahl von **Mitarbeiter** oder **Besucher** den Typ des Schlüsselhalters wählen.

   Eine Liste aller an Mitarbeiter oder Besucher ausgegebenen Schlüssel mit einem Rückgabedatum innerhalb einer bestimmten Anzahl von Tagen wird angezeigt.



Die standardmäßig vorgegebene Anzahl von Tagen kann in den Systemeinstellungen geändert werden. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

3) Wählen Sie einen **Grund der Überfälligkeit**, geben Sie weitere Suchkriterien ein und klicken Sie auf **Suchen**.

Grund der Überfälligkeit:

- Wenn **Rückgabedatum** ausgewählt wird, werden alle Schlüssel mit einem Rückgabedatum innerhalb der angegebenen Anzahl von Tagen aufgeführt.
- Wenn **Gültigkeit** ausgewählt wird, werden alle Schlüssel mit dem Ende des Gültigkeitszeitraums innerhalb der angegebenen Anzahl von Tagen aufgeführt.
- Bei Auswahl von **Verlängerung** werden die Schlüssel aufgeführt, deren Verlängerungsintervall im angegebenen Datumsbereich liegt.

4) Klicken Sie auf **Überfällige Schlüssel ausdrucken**, um eine Liste der überfälligen Schlüssel bzw. Schlüssel, die verlängert werden müssen, zu drucken.

5) Um eine E-Mail mit einer Erinnerung an Mitarbeiter oder Besucher mit überfälligen Schlüsseln zu versenden, klicken Sie auf **E-Mail-Erinnerung senden**.

Damit diese Option zur Verfügung steht, muss **Benutzer-Benachrichtigung** unter **Systemeinstellungen** ausgewählt sein. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

4.2.15 Aktualisieren und Revalidieren eines Benutzerschlüssels

Über lokale Programmiergeräte
Ein Schlüssel, der in den rechten Schacht am lokalen Programmiergerät eingeführt wird, wird direkt während des Betriebs in CWM aktualisiert.

Wenn die folgenden Aktionen lokal ausgeführt wurden, wird der Schlüssel im lokalen Programmiergerät gleichzeitig revalidiert:

- **Zeitplan** festlegen
- **Ereignisliste** lesen
- **Zylinder in der Zugangsliste** ändern

Wenn die folgenden Bedingungen erfüllt sind, wird ein Schlüssel im rechten Schacht des lokalen Programmiergeräts **ohne** Programmierschlüssel aktualisiert und/oder revalidiert:

- Schlüssel der Generation 2 mit Firmware-Version 12.3 oder höher
- CLIQ Connect-PC ist aktiviert

> **HINWEIS!**
> Vor der Aktualisierung und Revalidierung muss der Programmierschlüssel aus dem linken Schacht des lokalen Programmiergeräts entfernt werden.

Über Remote-Programmiergeräte
Schlüsselhalter können ihre Schlüssel aktualisieren und/oder revalidieren, indem sie sie in ein Wand-Programmiergerät oder ein mobiles Programmiergerät einführen.

Ein Schlüssel kann auch aktualisiert und/oder revalidiert werden, wenn er über ein mobiles CLIQ Connect-Programmiergerät mit CLIQ Connect verbunden wird.

Weitere Informationen zur Schlüsselverlängerung finden Sie in *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170* und *Abschnitt 8.1.6 "Flexible Verlängerung", Seite 173*.

4.2.16 Benutzerschlüsselkonfiguration kopieren

Die Konfiguration eines Schlüssels kann auf einen anderen Schlüssel kopiert werden, der im lokalen PG abgefragt wird. Folgende Einstellungen werden gegebenenfalls kopiert:

- Gültigkeit
- Zeitplan
- Verlängerungseinstellungen
- Schlüsselzugangsliste
- Zugangsprofile

Bei Schlüsseln, die in Zylinderzugangslisten enthalten sind:

- Zum Update der Zylinderzugangslisten werden Zylinderprogrammierungs-Jobs angelegt.

1) Den Schlüssel suchen, dessen Konfiguration kopiert werden soll, und die Detailansicht des Schlüssels öffnen.

   Siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.
2) Schlüssel, auf den kopiert werden soll, in das lokale PG einführen.
3) Auf **Schlüsselkonfiguration kopieren** klicken.

   Der Schlüssel wird abgefragt.
4) Auf **Auswählen** klicken.
5) Für die erforderlichen Zylinderprogrammierungs-Jobs eine **Priorität** auswählen.

   Dringende Jobs sollten hohe Priorität haben.
6) Auf **Anwenden** klicken.

   Die vorhandene Konfiguration auf dem Zielschlüssel wird überschrieben und Zylinderprogrammierungs-Jobs werden angelegt.

Ein Ereignis mit Datum und Uhrzeit für die Änderung und eine Kennzeichnung aus Quell- und Programmierschlüssel werden erstellt.

4.2.17 Benutzerschlüsselbericht drucken

1) Den Schlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Auf **Schlüsselbericht ausdrucken** klicken.

3) Auswählen, ob die Liste mechanische Zylinder umfassen soll oder nicht und auf **OK** klicken.

4) Im Pop-up-Fenster wird eine Vorschau angezeigt.

   - Zum Speichern auf das Speichersymbol klicken und einen Ordner als Speicherort angeben.
   - Zum Drucken auf **...** klicken und **Ausdrucken** auswählen.

4.2.18 Exportieren von Informationen für Benutzerschlüssel

1) **Systeminfo » Schlüssel** auswählen.

   Eine Liste aller Schlüssel wird angezeigt.

2) Schlüssel suchen.

   Siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.

3) In den Suchergebnissen die Schlüssel, deren Daten exportiert werden sollen, auswählen.

4) Auf **In CSV-Datei exportieren** klicken.

5) Im Pop-up-Fenster für den Dateidownload auf **Speichern** klicken.

   Eine CSV-Datei wird in den Ordner **Downloads** heruntergeladen.

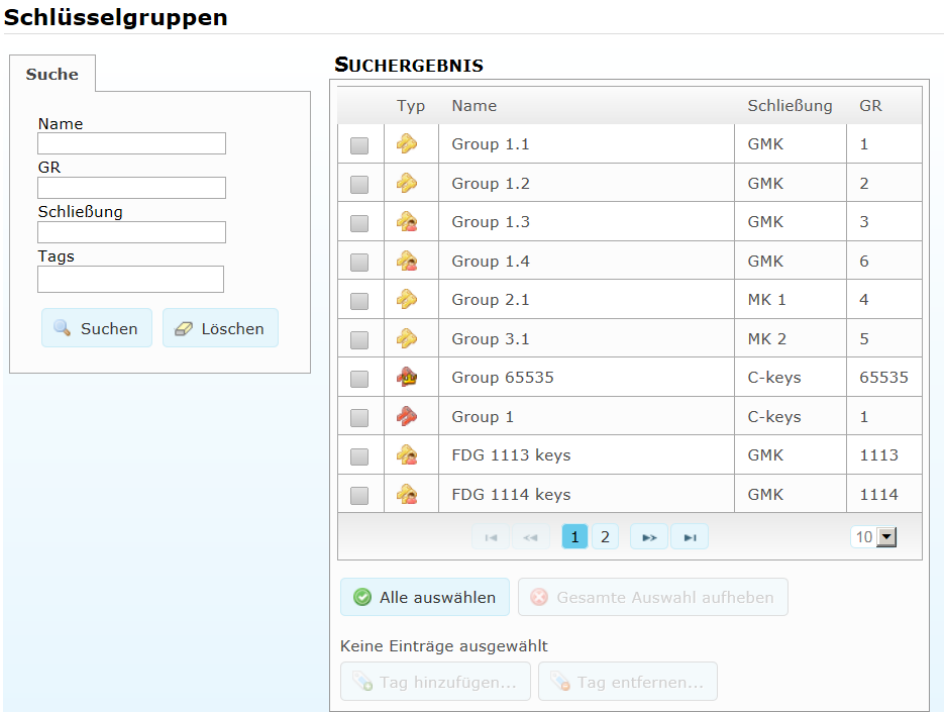
> **HINWEIS!**
> Damit die Excel-Datei korrekt geöffnet werden kann, muss das Trennzeichen entsprechend den regionalen Einstellungen eingestellt sein. Ändern des Trennzeichens siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

4.3 Verwalten von Schlüsselgruppen

4.3.1 Suchen nach Schlüsselgruppen

1) **Systeminfo » Schlüsselgruppen** auswählen.

   Eine Liste aller Schlüsselgruppen wird angezeigt.



Folgende Symbole werden verwendet:

 E1-Schlüssel-Gruppe

 E3-Schlüssel-Gruppe

2) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

   Bei Eingabe im Suchfeld **Tags** erscheinen alle passenden Tags in einer Auswahlliste.

3) Auf **Suchen** klicken.

4) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf die Zeile mit der entsprechenden Schlüsselgruppe klicken.

4.3.2 Bearbeiten von Schlüsselgruppen-Informationen

1) Die Schlüsselgruppe suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.3.1 "Suchen nach Schlüsselgruppen", Seite 54*.

2) Auf **Bearbeiten** klicken.

3) Zum Bearbeiten des Schlüsselgruppennamens den Namen eingeben.

4) Um ein Tag hinzuzufügen, auf **Tag hinzufügen** klicken. Siehe auch *Abschnitt 4.3.3 "Hinzufügen oder Löschen von Schlüsselgruppen-Tags", Seite 56*.

5) Auf **Speichern** klicken.

4.3.3 Hinzufügen oder Löschen von Schlüsselgruppen-Tags

1) Die Schlüsselgruppe suchen.

   Informationen zum Suchen nach einer Schlüsselgruppe finden Sie in *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.

2) - Um Tags für eine einzelne Schlüsselgruppe hinzuzufügen oder zu entfernen, mit *Schritt 3* fortfahren.
   - Um Tags für mehrere Schlüsselgruppen hinzuzufügen oder zu entfernen, mit *Schritt 4* fortfahren.

3) **Tags für eine einzelne Schlüsselgruppe hinzufügen oder entfernen:**

   1. Die Schlüsselgruppe auswählen und die Detailansicht öffnen.
   2. Auf **Bearbeiten** klicken.
   3. Ein Tag für eine einzelne Schlüsselgruppe hinzufügen oder entfernen.

      Tag hinzufügen:

      a) Auf **Tag hinzufügen...** klicken.
      b) Namen für den Tag eingeben.
      c) Auf **OK** klicken.

      Tag entfernen:
      Auf den zu entfernenden Tag klicken.
   4. Auf **Speichern** klicken.

4) **Tags für mehrere Schlüsselgruppen hinzufügen oder entfernen:**

   1. Schlüsselgruppen durch Aktivieren der entsprechenden Kontrollkästchen aus den Suchergebnissen auswählen.
   2. **Tag hinzufügen:**

      a) Auf **Tag hinzufügen...** klicken.
      b) Einen Namen für das Tag eingeben.
      c) Auf **OK** klicken.

      Tag entfernen:

      a) Auf **Tag entfernen...** klicken.
      b) Einen Namen für das Tag eingeben.
      c) Auf **OK** klicken.

Siehe auch *Abschnitt 8.2.6 "Tags", Seite 184*.

4.3.4 Anzeigen der Mitglieder von Schlüsselgruppen

1) Die Schlüsselgruppe suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.3.1 "Suchen nach Schlüsselgruppen", Seite 54*.

2) Register **Mitglieder** auswählen.

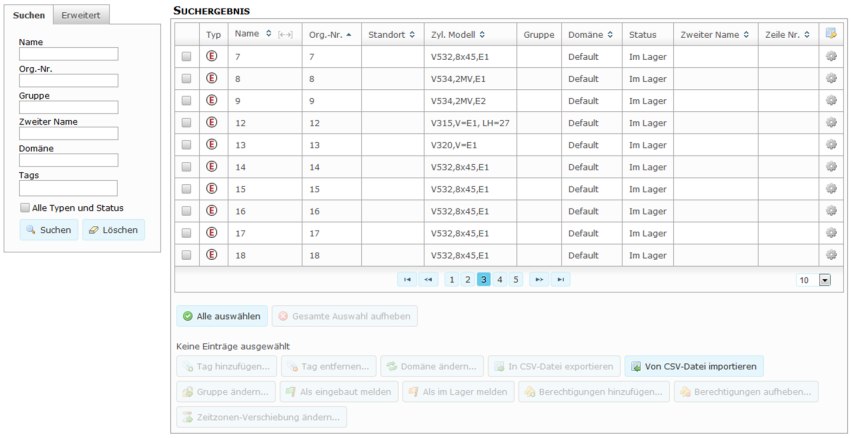
   Eine Liste mit allen Schlüsseln in dieser Schlüsselgruppe wird angezeigt.

4.4 Verwalten von Zylindern

4.4.1 Suchen nach Zylindern

1) **Systeminfo » Zylinder** auswählen.

   Eine Liste aller Zylinder wird angezeigt, mit Ausnahme mechanischer oder defekter Zylinder.



   Folgende Symbole werden verwendet:

   - Elektronischer Zylinder
   - Mechanischer Zylinder
   - Doppelzylinder (hier verwendetes Beispiel: A-Seite elektronisch; B-Seite mechanisch)

2) Register **Suchen** oder **Erweitert** auswählen.

   Mechanische und defekte Zylinder werden standardmäßig nicht angezeigt. Um auch diese Zylinder in die Suchergebnisse zu integrieren, **Alle Typen und Status** auswählen.

   Die Registerkarte **Erweitert** enthält auch die Suchfelder „Zylindertyp“, „Bestandsstatus“, „Status funktionsfähig“ und „Org.-Nr. 2“ sowie eine Dropdownliste mit benutzerdefinierten Feldern (sofern in den **Systemeinstellungen** definiert). Diese Einstellung wird durch Auswahl von **Verwaltung » Systemeinstellungen » VERWALTUNG » Benutzerdefinierte Felder Zylinder** erreicht.).

3) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

   Bei Eingabe im Suchfeld **Tags** erscheinen alle passenden Tags in einer Auswahlliste.

4) Auf **Suchen** klicken.

5) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf die Zeile mit dem entsprechenden Zylinder klicken.

   Weitere Informationen zu den Merkmalen des Zylinders siehe *Abschnitt 9.3.5 "Zylinderattribute", Seite 205*.

4.4.2 Bearbeiten von Zylinderinformationen

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

   Wenn **Zweiter Name** oder **Benutzerdefinierte Felder** bearbeitet werden müssen, mit *Schritt 6* fortfahren.

2) Auf **Bearbeiten** klicken.

3) Die Felder bearbeiten.

   Weitere Informationen zu den Merkmalen des Zylinders siehe *Abschnitt 9.3.5 "Zylinderattribute", Seite 205*.

4)
   - Um ein Tag hinzuzufügen, auf **Tag hinzufügen** klicken. Siehe auch *Abschnitt 4.4.3 "Zylinder-Tags hinzufügen oder entfernen", Seite 58*
   - Um einen externen Link hinzuzufügen, auf **Externen Link hinzufügen** klicken. Siehe auch *Abschnitt 4.4.4 "Externe Links für Zylinder verwalten", Seite 59*

5) Auf **Speichern** klicken.

6) **Zweiter Name** und **Benutzerdefinierte Felder** werden auf der Registerkarte **Zusätzliche Informationen** bearbeitet.

   HINWEIS!
   Benutzerdefinierte Felder werden in den **Systemeinstellungen** definiert. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

   a) Register **Zusätzliche Informationen** auswählen.

   b) Auf **Bearbeiten** klicken.

   c) Das Feld ändern.

   d) Auf **Speichern** klicken.

4.4.3 Zylinder-Tags hinzufügen oder entfernen

Informationen zu Tags finden Sie in *Abschnitt 8.2.6 "Tags", Seite 184*.

1) **Systeminfo » Zylinder** auswählen.

   Eine Liste aller Zylinder wird angezeigt.

   - Um Tags für einzelne Zylinder hinzuzufügen oder zu entfernen, gehen Sie zu *Schritt 2*.
   - Um Tags für mehrere Zylinder gleichzeitig hinzuzufügen oder zu entfernen, gehen Sie zu *Schritt 3*.

2) **Tags für einen einzelnen Zylinder hinzufügen oder entfernen:**

   1. Den Zylinder auswählen und seine Detailansicht öffnen.
   2. Auf **Bearbeiten** klicken.
   3. Ein Tag für einen einzelnen Zylinder hinzufügen oder entfernen.

Tag hinzufügen:

a) Auf **Tag hinzufügen...** klicken.
b) Namen für den Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:
Auf den zu entfernenden Tag klicken.

4. Auf **Speichern** klicken.

3) **Tags für mehrere Zylinder hinzufügen oder entfernen:**

1. Die Zylinder durch Aktivieren der Kontrollkästchen aus den Suchergebnissen auswählen.
2. **Tag hinzufügen:**

a) Auf **Tag hinzufügen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:

a) Auf **Tag entfernen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

4.4.4 Externe Links für Zylinder verwalten

Informationen über externe Links finden Sie in *Abschnitt 8.4 "Externe Links", Seite 187*.

1) Den Zylinder suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Auf **Bearbeiten** klicken.
3) **Einen externen Link hinzufügen:**

1. Auf **Hinzufügen.** klicken
2. **Name** für die URL eingeben.
3. **URL** eingeben. Die **URL** muss mit einem Protokoll beginnen (z. B. http:// oder ftp://).

   Wenn in den **Systemeinstellungen** (Eintrag **Externe Links Root-URL**) eine Root-URL festgelegt wurde, muss nur der letzte Teil der URL eingegeben werden. Siehe auch *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.
4. Auf **OK** klicken.

Externen Link bearbeiten:

1. Beim zu bearbeitenden externen Link auf **Bearbeiten** klicken.
2. Die Felder ändern.
3. Auf **OK** klicken.

Einen externen Link entfernen:

Beim zu entfernenden externen Link auf **Entfernen** klicken.

4) Auf **Speichern** klicken.

4.4.5 Anzeigen von Schlüsselgruppen und Ausnahmen in einer Zylinderzugangsliste

Das Register **Schlüssel in der Zugangsliste** wird verwendet, um Schlüsselgruppen und Ausnahmen in der Zylinderzugangsliste anzuzeigen.

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Register **Schlüssel in der Zugangsliste** auswählen.

   Es wird eine Liste mit allen Schlüsselgruppen und Ausnahmen in der Zugangsliste dieses Zylinders angezeigt. Informationen zur Bearbeitung finden Sie in *Abschnitt 4.9.2 "Konfigurieren von Berechtigungen in Zylindern", Seite 83*.

4.4.6 Anzeigen der Update-Historie für einen Zylinder

Das Register Update-Historie wird zur Verfolgung von Schlüsselprogrammierungen verwendet.

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Register **Update-Historie** auswählen.

   Eine Liste mit allen Zylinder-Updates wird angezeigt.

   Folgende Symbole werden verwendet:

   - Programmierungs-Job vorhanden, der jedoch nicht initiiert wurde
   - Programmierungs-Job wurde auf Programmierschlüssel übertragen
   - Programmierungs-Job ist abgeschlossen
   - Programmierungs-Job fehlgeschlagen oder abgebrochen
   - Programmierungs-Job wurde durch einen neuen Job ersetzt

3) Zur Anzeige weiterer Details zu einem speziellen Update auf den Link in der Spalte **Typ** klicken.

4.4.7 Anzeigen von Ereignissen für einen Zylinder

Auf der Registerkarte **Ereignisse** können Administratorvorgänge in CWM nachverfolgt werden, z. B. Meldungen defekter Zylinder.

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Register **Ereignisse** auswählen.

   Eine Liste mit allen Zylinder-Ereignissen wird angezeigt.

4.4.8 Zeitzonen-Verschiebung des Zylinders bearbeiten

Wenn sich die Zylinder einer Domäne in verschiedenen Zeitzonen befinden, lässt sich deren Zeitzone anpassen. Diese Einstellung ist nur für Generation-2-Zylinder verfügbar.

Weitere Informationen zu den Schlüsselgenerationen siehe *Abschnitt 7.2.5 "Schlüsselgenerationen", Seite 163*.

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Auf **Zeitzonen-Verschiebung ändern...** klicken.

3) **Zeitzonen-Verschiebung** auf die gewünschte Anzahl Minuten einstellen.

4) Einstellen der Jobpriorität

5) Auf **OK** klicken.

   Ein Zylinderprogrammier-Job wird angelegt. Informationen zum Programmieren des Zylinders finden Sie in *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64*.

> **HINWEIS!**
> Während der Programmierjob auf die Ausführung wartet, wird in den Detailinformationen des Zylinders die Schaltfläche **Zeitzonen-Verschiebung abbrechen** angezeigt.
>
> Auf die Schaltfläche klicken, um während der Bearbeitung die Anpassung der Zeitzonen-Verschiebung abzubrechen.

Die Zeitzonen-Verschiebung lässt sich für mehrere Zylinder gleichzeitig anpassen. Die Zylinder in der Liste der Suchergebnisse auswählen und auf **Zeitzonen-Verschiebung** klicken.

4.4.9 Zylinderstatus ändern

Zylinder haben einen Bestandsstatus, der entweder **Im Lager** oder **Installiert** lauten kann, sowie einen Funktionsstatus, der entweder **Funktionsfähig** oder **Defekt** lauten kann.

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) **Status auf „Installiert“ festlegen**

   1. Auf **Als eingebaut melden** klicken.
   2. Auf **OK** klicken.

      Mehrere Zylinder können gleichzeitig als installiert gemeldet werden. Die Zylinder in der Liste der Suchergebnisse auswählen und auf **Als eingebaut melden** klicken.

   Den Status auf „Im Lager“ festlegen

   1. Auf **Als im Lager melden** klicken.
   2. Auf **OK** klicken.

      Mehrere Zylinder können gleichzeitig als „Im Lager“ gemeldet werden. Die Zylinder in der Liste der Suchergebnisse auswählen und auf **Als im Lager melden** klicken.

Als Defekt melden

1. Auf **Als defekt melden** klicken.
2. **Nur als defekt melden** auswählen.

   Wenn ein Austausch erforderlich ist, siehe *Abschnitt 4.4.10 "Austauschen eines defekten Zylinders", Seite 62*.
3. Auf **Weiter** klicken.
4. Auf **Anwenden** klicken.

Zylinder wieder als funktionsfähig melden

1. Auf **Als funktionsfähig melden** klicken.

   Diese Option ist nur für Zylinder verfügbar, die zuvor als defekt gemeldet wurden.
2. Auf **OK** klicken.
3. Ein Programmier-Job wird angelegt.

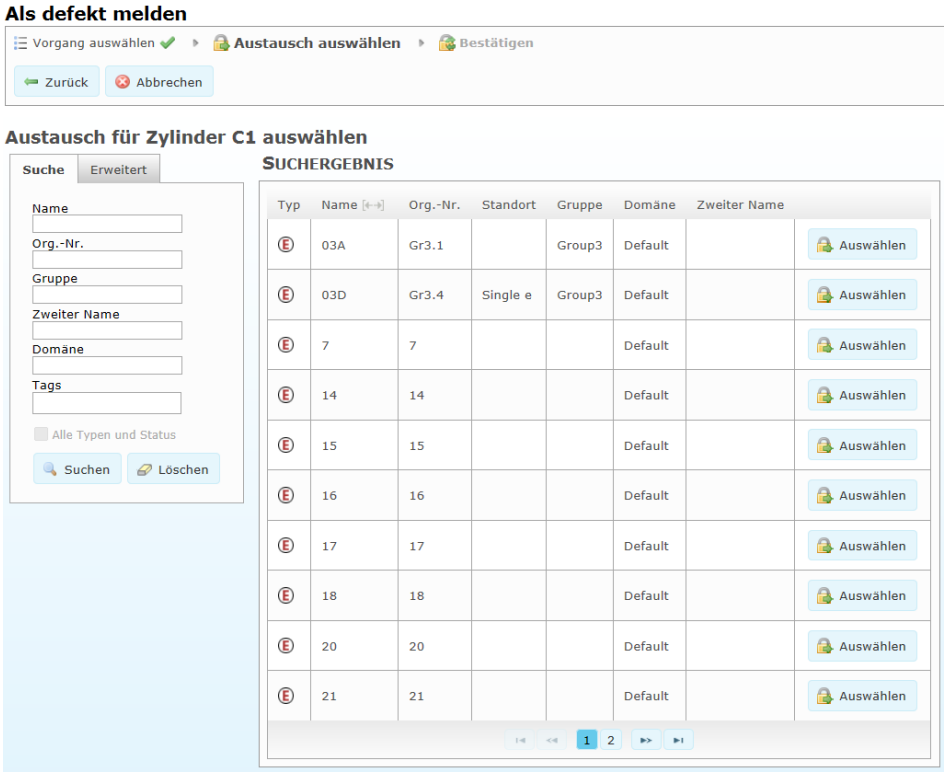
4.4.10 Austauschen eines defekten Zylinders

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.
2) Auf **Als defekt melden** klicken.
3) **Als defekt melden und durch anderen Zylinder ersetzen** auswählen.

4) Auf **Weiter** klicken.

Eine Liste mit allen auf Lager befindlichen Zylindern desselben Typs wie der gemeldete Zylinder wird angezeigt.



5) Um nach bestimmten Zylindern zu suchen, die Suchkriterien eingeben und auf **Suchen** klicken.

6) Durch Klicken auf **Auswählen** einen Austauschzylinder auswählen.

7) Unter **Priorität** eine Prioritätsstufe auswählen.

Dringende Jobs sollten hohe Priorität haben.

8) Auf **Anwenden** klicken.

Die aktuelle Konfiguration einschließlich anstehender Updates für den Ersatzzylinder wird verworfen und durch die Konfiguration des defekten Zylinders ersetzt.

Remote-Update-Jobs werden für die zugehörigen Schlüssel angelegt und Zugangsprofile, die Zugang zum defekten Zylinder gewähren, werden aktualisiert.

4.4.11 Ersetzen eines Zylinders mit einem Klon aus dem Werk

Wenn aufgrund eines defekten Zylinders ein Austauschklon aus dem Werk geliefert wird, müssen folgende Schritte durchgeführt werden, um die Funktionalität des Zylinders sicherzustellen.

1) Wenn der geklonte Zylinder aus dem Werk eintrifft, zu **Verwaltung » Erweiterungsimport » Erweiterungsimportdatei(en) hochladen oder holen** wechseln, um entweder die zur Verfügung gestellte CWS-Datei in CWM hochzuladen (bei deaktivierter DCS-Integration) oder die Datei aus DCS zu holen.

2) Für den Austauschzylinder einen Reprogrammierjob erstellen. Siehe *Abschnitt 4.4.12 "Zylinder-Reprogrammierung anfordern", Seite 64*.

3) Den Austauschzylinder programmieren. Siehe *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64*.

4) Der Austauschzylinder ist einsatzbereit.

4.4.12 Zylinder-Reprogrammierung anfordern

Wenn ein Zylinder reprogrammiert wird, wird der Inhalt seines Speichers gelöscht, einschließlich der Ereignislisten. Die Zugangsliste des Zylinders wird im Rahmen der Reprogrammierung wiederhergestellt. Um den eigentlichen Reprogrammierjob durchzuführen, wird ein Hauptprogrammierschlüssel bzw. ein Normalprogrammierschlüssel mit Berechtigung zur Zylinder-Reprogrammierung benötigt.

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Auf **Reprogrammieren** klicken.

   Bei doppelseitigen Zylindern auf **Seite reprogrammieren A**, **Seite reprogrammieren B** oder beide klicken.

3) **Priorität** auswählen.

   Dringende Jobs sollten hohe Priorität haben.

4) Auf **OK** klicken.

Siehe auch *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64*.

4.4.13 Zylinder mit einem Programmierschlüssel programmieren

Voraussetzungen:

- Ein Programmierschlüssel mit Berechtigung zur **Zylinderprogrammierung**
- Bei Jobs, die den Austausch der Zylindergruppe eines Zylinders umfassen: Ein Programmierschlüssel mit Fähigkeit zur **Zylindergruppenprogrammierung**
- Bei Reprogrammierjobs: Ein Hauptprogrammierschlüssel bzw. ein Normalprogrammierschlüssel mit der Berechtigung **Zylinder-Reprogrammierung**

Wenn der Programmierschlüssel, der für die Programmierung verwendet werden soll, sofort verfügbar ist, das Verfahren unter *Abschnitt 4.4.13.1 "Programmieren von Zylindern mit Programmierschlüssel und lokalem PG", Seite 64* befolgen.

Wenn der Programmierschlüssel, der für die Programmierung verwendet werden soll, nicht sofort verfügbar ist, das Verfahren unter *Abschnitt 4.4.13.2 "Programmieren von Zylindern mit Connect-Programmierschlüssel oder mit Programmierschlüssel und Remote-Programmiergerät", Seite 66* befolgen. Für dieses Verfahren ist ein Remote-Programmiergerät oder ein CLIQ Connect-Programmierschlüssel erforderlich.

Weitere Informationen zur Zylinderprogrammierung siehe *Abschnitt 8.5 "Zylinderprogrammierung", Seite 188*.

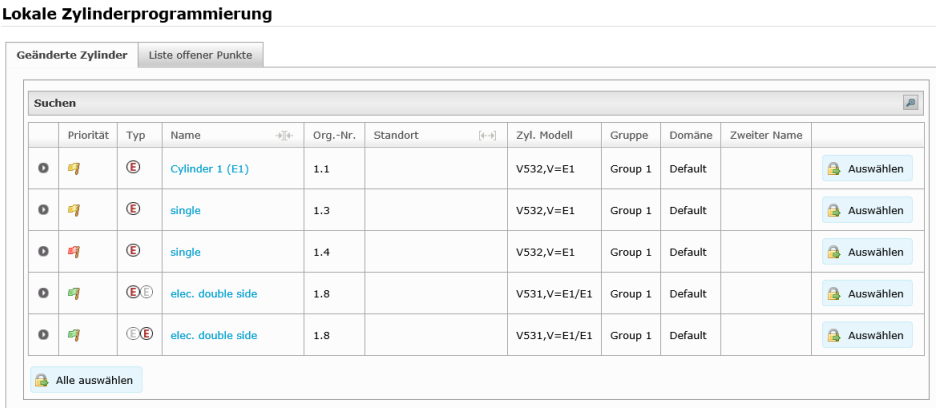
4.4.13.1 Programmieren von Zylindern mit Programmierschlüssel und lokalem PG

Programmierjobs an sofort verfügbare Programmierschlüssel und Programmierzylinder senden:

1) **Arbeit » Zylinderprogrammierung** auswählen.

   Eine Liste der Zylinder, die programmiert werden müssen, wird angezeigt. Prioritätsebenen für die Jobs werden in der Spalte ganz links angezeigt.

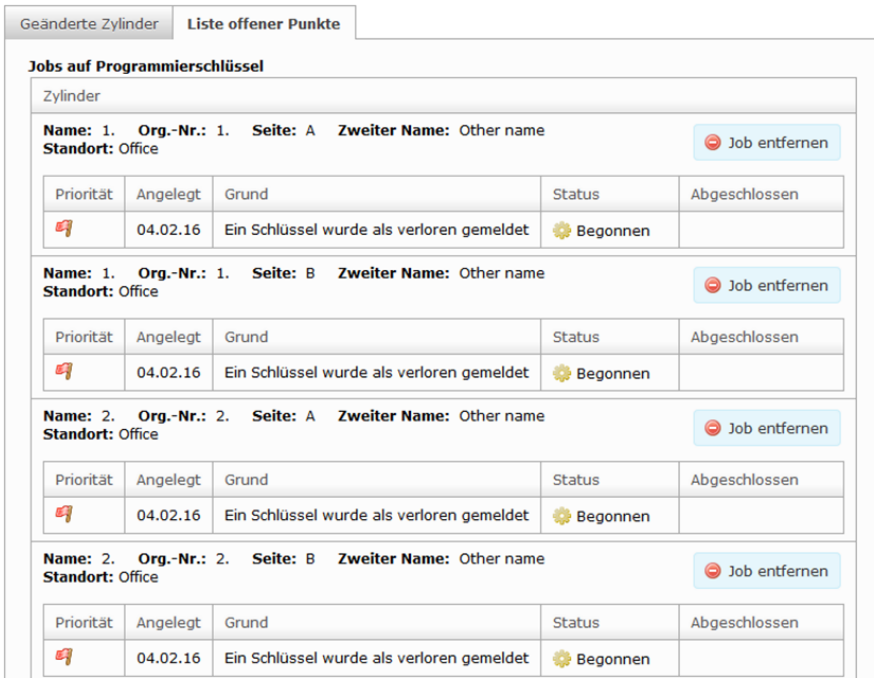
2) Um die auszuführenden Jobs auszuwählen, klicken Sie in der Liste auf **Auswählen** oder unter der Liste auf **Alle auswählen**.



3) Auf **An Programmierschlüssel senden** klicken.

> **HINWEIS!**
> Wenn ein Zylinderprogrammierungs-Job auf einen Programmierschlüssel geladen wird, sind die Berechtigungseinstellungen für diesen Zylinder in der CWM-Software für die Bearbeitung gesperrt.

- Zum Anzeigen der aktuell auf dem Programmierschlüssel vorhandenen Jobs das Register **Liste offener Punkte** auswählen.



- Zum Ausdrucken der Liste auf **Liste offener Punkte ausdrucken** klicken.

4) Den Programmierschlüssel nacheinander in die zu programmierenden Zylinder einführen.

ACHTUNG!
Den Programmierschlüssel eingesteckt lassen, bis der Programmierjob abgeschlossen ist.

Falls der Job fehlschlägt, den Programmierschlüssel in ein mit CWM verbundenes Remote-Programmiergerät einführen, um den Programmierjob wieder im Programmierschlüssel zu laden. Siehe auch *"Reprogrammierung"*.

5) Erneut Login an der CWM-Software durchführen.
6) **Arbeit » Zylinderprogrammierung** auswählen.
7) Register **Liste offener Punkte** auswählen.
8) Auf **Update** klicken.

   Die Statusinformationen der Programmier-Jobs werden vom Programmierschlüssel geladen.
9) Optional: Auf **Abgeschlossene Jobs entfernen** klicken.

4.4.13.2 Programmieren von Zylindern mit Connect-Programmierschlüssel oder mit Programmierschlüssel und Remote-Programmiergerät

Der Status der Interaktion mit dem Remote-Programmiergerät wird während der Zylinderjobprogrammierung mithilfe von LEDs angezeigt. Weitere Informationen über die LED-Anzeige finden Sie in *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen Programmiergeräten", Seite 212* oder *Abschnitt 9.5.2 "Anzeigen eines Wand-Programmiergeräts (Generation 2)", Seite 213*.

1) Zylinderprogrammierjobs einem Programmierschlüssel zuweisen:
   a) Programmierschlüssel suchen.

      Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*
   b) Register **Zylinderprogrammierung** auswählen.
   c) Auf **Zylinder für die Programmierung zuordnen** klicken.
   d) Für jeden auszuführenden Zylinderprogrammierjob auf **Auswählen** klicken.

      WARNUNG!
      Für Jobs mit Änderungen an Zylindergruppen können einem Programmierschlüssel höchstens 100 Jobs zugewiesen werden. Das Zuweisen von mehr Aufträgen kann zu Programmierfehlern führen.
   e) Auf **Anwenden** klicken.

      Nachdem der Zylinderprogrammierjob einem Programmierschlüssel zugewiesen wurde, wird eine E-Mail mit dem Hinweis auf abzurufende Programmierjobs generiert und an den Halter des Programmierschlüssels gesendet.
2) Den Programmierschlüssel in ein Remote-Programmiergerät einführen oder den Connect-Programmierschlüssel mit CLIQ Connect verbinden, um die Zylinderprogrammierjobs zu laden.

Nachdem der Zylinderprogrammierjob übertragen wurde. wird eine E-Mail an den Halter des Programmierschlüssels generiert. Diese enthält Informationen darüber, welche Zylinder zu programmieren sind.

3) Programmierschlüssel in die zu programmierenden Zylinder einführen.

> **ACHTUNG!**
> Schlüssel eingesteckt lassen, bis der Programmier-Job abgeschlossen ist.
>
> Falls der Job fehlschlägt, den Schlüssel in ein mit CWM verbundenes Remote-Programmiergerät einstecken, um den Programmierjob wieder in den Schlüssel zu laden. Siehe auch *"Reprogrammierung"*.

4) Den Programmierschlüssel in ein Remote-Programmiergerät einführen oder den Connect-Programmierschlüssel mit CLIQ Connect verbinden, um den Status der Programmierjobs zu aktualisieren.

4.4.14 Importieren von Zylinderinformationen

Importieren von Zylinderinformationen ermöglicht einen Massenimport von aktualisierten Zylinderdaten. Die Funktion dient lediglich dem Aktualisieren vorhandener Zylinderdaten.

Für den Import wird eine CSV-Datei verwendet. Um möglichst einfach eine neue CSV-Datei zu erstellen, kann eine CSV-Datei mit vorhandenen Zylinderdaten exportiert und anschließend in Excel oder einem Texteditor bearbeitet werden. Siehe *Abschnitt 4.4.15 "Exportieren von Zylinderinformationen", Seite 68*.

> **HINWEIS!**
> Zylinderinformationen lassen sich sowohl aus CSV-Dateien als auch aus **Erweiterungsimportdateien** importieren, die Inhalte sind dabei nicht redundant. CSV-Dateien aktualisieren Zylinderinformationen, die von Benutzern über die Benutzerschnittstelle angepasst werden können. Erweiterungsimportdateien aktualisieren dagegen schreibgeschützte Werksdaten. CSV-Dateien können folglich keine Erweiterungen überschreiben und umgekehrt. Weitere Informationen zu Erweiterungen siehe *Abschnitt 6.16 "Importieren von Erweiterungen", Seite 157*.

1) Auf **Systeminfo » Zylinder** klicken.
2) Auf **Von CSV-Datei importieren** klicken.
3) Auf **Auswählen** klicken und die lokal auf dem Computer gespeicherte Datei suchen.
4) Auf **Öffnen** klicken.
5) Auf **Import** klicken, um die Datei zu importieren und zu validieren.

   Es wird angezeigt, wie viele gültige Einträge in der Datei vorhanden sind. Wenn die Datei nicht den Anforderungen entspricht, ist der Import nicht möglich.

HINWEIS!
Beim Importieren von Zylinderinformationen werden nur die folgenden Spalten in der CSV-Datei aktualisiert.

- Name
- Zweiter Name
- Standort
- Bestandsstatus
- Benutzerdefinierte Felder (falls in den **Systemeinstellungen** definiert)

Die vorhandenen Zylinderdaten werden überschrieben.

HINWEIS!
Um Zylinderinformationen aus einer CSV-Datei zu importieren, müssen die Werte in **Org.-Nr.** bzw. die Kombination der Werte von **Org.-Nr.** und **Org.-Nr. 2** eindeutig sein.

4.4.15 Exportieren von Zylinderinformationen

1) Zylinder suchen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) In den Suchergebnissen die Zylinder, deren Daten exportiert werden sollen, auswählen.

3) Auf **In CSV-Datei exportieren** klicken.

   HINWEIS!
   Damit die Excel-Datei korrekt geöffnet werden kann, muss das Trennzeichen entsprechend den regionalen Einstellungen eingestellt sein. Ändern des Trennzeichens siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

4) Im Pop-up-Fenster Dateidownload auf **Öffnen** oder **Speichern** klicken.

4.5 Verwalten von Zylindergruppen

4.5.1 Suchen nach Zylindergruppen

1) **Systeminfo » Zylindergruppen** auswählen.

   Eine Liste aller Zylindergruppen wird angezeigt.

2) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

   Bei Eingabe im Suchfeld **Tags** erscheinen alle passenden Tags in einer Auswahlliste.

3) Auf **Suchen** klicken.

4) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf die entsprechende Zylindergruppe klicken.

4.5.2 Bearbeiten von Zylindergruppen-Informationen

1) Die Zylindergruppe suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.5.1 "Suchen nach Zylindergruppen", Seite 69*.

2) Auf **Bearbeiten** klicken.

3) Zum Bearbeiten des Zylindergruppennamens die Eingabe im Feld **Name** ändern.

4) Um ein Tag hinzuzufügen, auf **Tag hinzufügen...** klicken. Siehe auch *Abschnitt 4.5.3 "Hinzufügen oder Löschen von Zylindergruppen-Tags", Seite 69*

5) Um die Domäne zu ändern auf **Domäne ändern...** klicken. Siehe auch *Abschnitt 6.6.8 "Ändern der Domäne für Zylindergruppen", Seite 130*.

6) Auf **Speichern** klicken.

4.5.3 Hinzufügen oder Löschen von Zylindergruppen-Tags

1) Zylindergruppe suchen.

   Informationen zum Suchen nach einer Zylindergruppe finden Sie in *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.

2) - Um Tags für eine einzelne Zylindergruppe hinzuzufügen oder zu entfernen, mit *Schritt 3* fortfahren.
   - Um Tags für mehrere Zylindergruppen hinzuzufügen oder zu entfernen, mit *Schritt 4* fortfahren.

3) **Tags für eine einzelne Zylindergruppe hinzufügen oder entfernen:**

1. Die Zylindergruppe auswählen und die Detailansicht öffnen.
2. Auf **Bearbeiten** klicken.
3. Ein Tag für eine einzelne Zylindergruppe hinzufügen oder entfernen.

Tag hinzufügen:

a) Auf **Tag hinzufügen...** klicken.
b) Namen für den Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:
Auf den zu entfernenden Tag klicken.

4. Auf **Speichern** klicken.

4) **Tags für mehrere Zylindergruppen hinzufügen oder entfernen:**

1. Zylindergruppen durch Aktivieren der entsprechenden Kontrollkästchen aus den Suchergebnissen auswählen.
2. **Tag hinzufügen:**

a) Auf **Tag hinzufügen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:

a) Auf **Tag entfernen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

Siehe auch *Abschnitt 8.2.6 "Tags", Seite 184*.

4.5.4 Anzeigen der Mitglieder von Zylindergruppen

1) Die Zylindergruppe suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.5.1 "Suchen nach Zylindergruppen", Seite 69*.

2) Register **Mitglieder** auswählen.

Eine Liste mit allen Zylindern in dieser Gruppe wird angezeigt.

4.5.5 Anzeigen von Ereignissen für eine Zylindergruppe

Das Register Ereignisse wird zur Verfolgung von Administratorvorgängen in CWM verwendet, z. B. das Ändern einer Domäne für eine Zylindergruppe.

1) Die Zylindergruppe suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.5.1 "Suchen nach Zylindergruppen", Seite 69*.

2) Register **Ereignisse** auswählen.

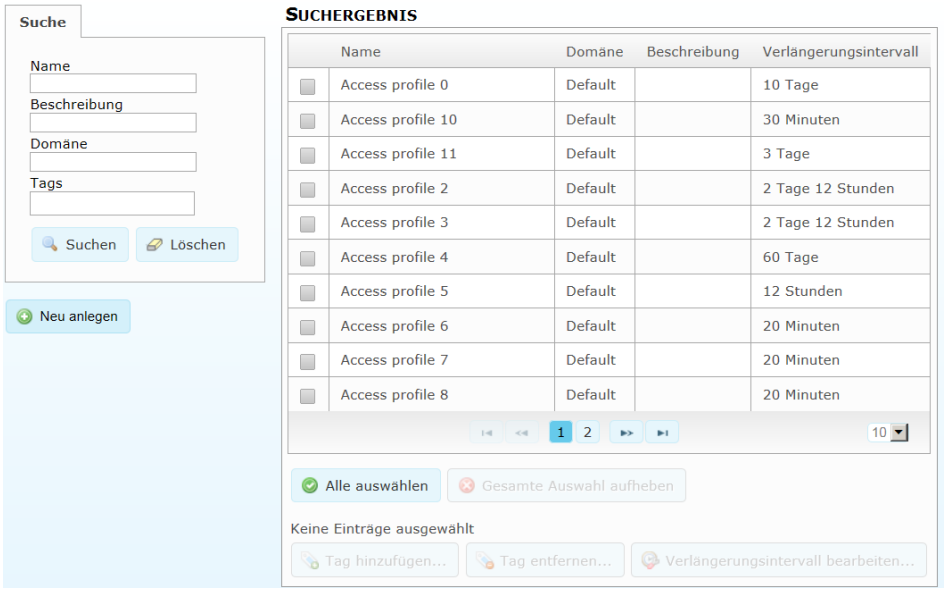
Eine Liste mit allen Zylindergruppen-Ereignissen wird angezeigt.

4.6 Verwalten von Zugangsprofilen

4.6.1 Suchen nach Zugangsprofilen

1) **Systeminfo » Zugangsprofile** auswählen.

   Eine Liste aller Zugangsprofile wird angezeigt.



2) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

3) Auf **Suchen** klicken.

4) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf das entsprechende Zugangsprofil klicken.

4.6.2 Anlegen und Löschen von Zugangsprofilen

Zugangsprofile gelten nur für E3-Schlüssel, die Remote-Updates unterstützen. Sie können auf einen Schlüssel oder eine Person angewendet werden.

1) **Systeminfo » Zugangsprofile** auswählen.
2) Anlegen eines Zugangsprofils:
   a) Auf **Neu anlegen** klicken.
   b) **Name** sowie eine optionale **Beschreibung** eingeben.

      HINWEIS!
      Das Namensfeld muss einen eindeutigen Wert enthalten.

   c) Ändern der Standard-Domäne:

      - Auf **Domäne ändern** klicken
      - Für die gewünschte Domäne auf **Auswählen** klicken.

d) Um ein Tag hinzuzufügen, auf **Tag hinzufügen** klicken. Siehe auch *Abschnitt 4.6.4 "Hinzufügen oder Löschen von Zugangsprofil-Tags", Seite 72*

e) Um einen externen Link hinzuzufügen, auf **Externen Link hinzufügen** klicken. Siehe auch *Abschnitt 4.6.5 "Bearbeiten von externen Links von Zugangsprofilen", Seite 73*

f) Auf **Speichern** klicken.

3) Löschen eines Zugangsprofils:

a) Zugangsprofil suchen und Detailinformationen anzeigen.

Siehe *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.

b) Auf **Löschen** klicken.

c)
- Wenn keine Schlüssel oder Personen mit dem Profil verknüpft sind:

  Auf **Profil löschen** klicken.
- Wenn Schlüssel oder Personen mit dem Profil verknüpft sind:

  a) Das dauerhafte Löschen der Zugangsprofile bestätigen und dann auf das Kontrollkästchen klicken.

  b) Auf **Profil löschen** klicken.

Siehe auch *Abschnitt 8.2.4 "Zugangsprofile", Seite 180*.

4.6.3 Bearbeiten der Angaben im Zugangsprofil

1) Das Zugangsprofil suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.

2) Auf **Bearbeiten** klicken.

3) Die Felder ändern.

4) Um Tags hinzuzufügen, auf **Tag hinzufügen...** klicken. Siehe auch *Abschnitt 4.1.7 "Hinzufügen oder Entfernen von Mitarbeiter- oder Besucher-Tags", Seite 32*.

5) Um externe Links hinzuzufügen und zu bearbeiten, auf **Externen Link hinzufügen...** klicken. Siehe auch *Abschnitt 4.1.8 "Verwalten externer Links von Mitarbeitern oder Besuchern", Seite 33*.

6) Auf **Speichern** klicken.

4.6.4 Hinzufügen oder Löschen von Zugangsprofil-Tags

1) Zugangsprofil suchen.

Informationen zum Suchen nach einem Zugangsprofil finden Sie in *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.

2)
- Um Tags für ein einzelnes Zugangsprofil hinzuzufügen oder zu entfernen, mit *Schritt 3* fortfahren.
- Um Tags für mehrere Zugangsprofile hinzuzufügen oder zu entfernen, mit *Schritt 4* fortfahren.

3) **Tags für ein einzelnes Zugangsprofil hinzufügen oder entfernen:**

1. Das Zugangsprofil auswählen und die Detailansicht öffnen.
2. Auf **Bearbeiten** klicken.
3. Ein Tag für ein einzelnes Zugangsprofil hinzufügen oder entfernen.

Tag hinzufügen:

a) Auf **Tag hinzufügen...** klicken.
b) Namen für den Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:
Auf den zu entfernenden Tag klicken.

4. Auf **Speichern** klicken.

4) **Tags für mehrere Zugangsprofile hinzufügen oder entfernen:**

1. Zugangsprofile durch Aktivieren der entsprechenden Kontrollkästchen aus den Suchergebnissen auswählen.
2. **Tag hinzufügen:**

a) Auf **Tag hinzufügen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

Tag entfernen:

a) Auf **Tag entfernen...** klicken.
b) Einen Namen für das Tag eingeben.
c) Auf **OK** klicken.

Weitere Informationen zu Tags siehe *Abschnitt 8.2.6 "Tags", Seite 184*.

4.6.5 Bearbeiten von externen Links von Zugangsprofilen

1) Das Zugangsprofil suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.

2) Auf **Bearbeiten** klicken.
3) Hinzufügen eines externen Links:

   a) Auf **Hinzufügen.** klicken
   b) **Name** für die URL eingeben.
   c) **URL** eingeben. Die **URL** muss mit einem Protokoll beginnen (z. B. http:// oder ftp://).

      Wenn in den **Systemeinstellungen** eine Root-URL festgelegt wurde, muss nur der letzte Teil der URL eingegeben werden. Siehe auch *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

   d) Auf **OK** klicken.

4) Zum Entfernen eines externen Links beim zu entfernenden Link auf **Entfernen** klicken.

5) Bearbeiten eines externen Links:

   a) Beim zu bearbeitenden externen Link auf **Bearbeiten** klicken.

   b) Die Felder ändern.

   c) Auf **OK** klicken.

6) Auf **Speichern** klicken.

Siehe auch *Abschnitt 8.4 "Externe Links", Seite 187*.

4.6.6 Anzeigen von mit einem Zugangsprofil verknüpfte Schlüssel

Auf der Registerkarte **Schlüssel** werden alle Schlüssel angezeigt, die mit dem ausgewählten Zugangsprofil verknüpft sind. Hier werden auch Schlüssel in abgelaufenen temporären Zugangsgruppen angezeigt, die mit dem ausgewählten Zugangsprofil verknüpft sind.

1) Das Zugangsprofil suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.

2) Register **Schlüssel** auswählen.

   Es wird eine Liste mit allen Schlüsseln angezeigt, die ein Zugangsprofil haben.

4.6.7 Anzeigen von Ereignissen für ein Zugangsprofil

Das Register Ereignisse wird zur Verfolgung von Administratorvorgängen in CWM verwendet, z. B. das Hinzufügen und Entfernen von Zylindern in einem Zugangsprofil.

1) Das Zugangsprofil suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.

2) Register **Ereignisse** auswählen.

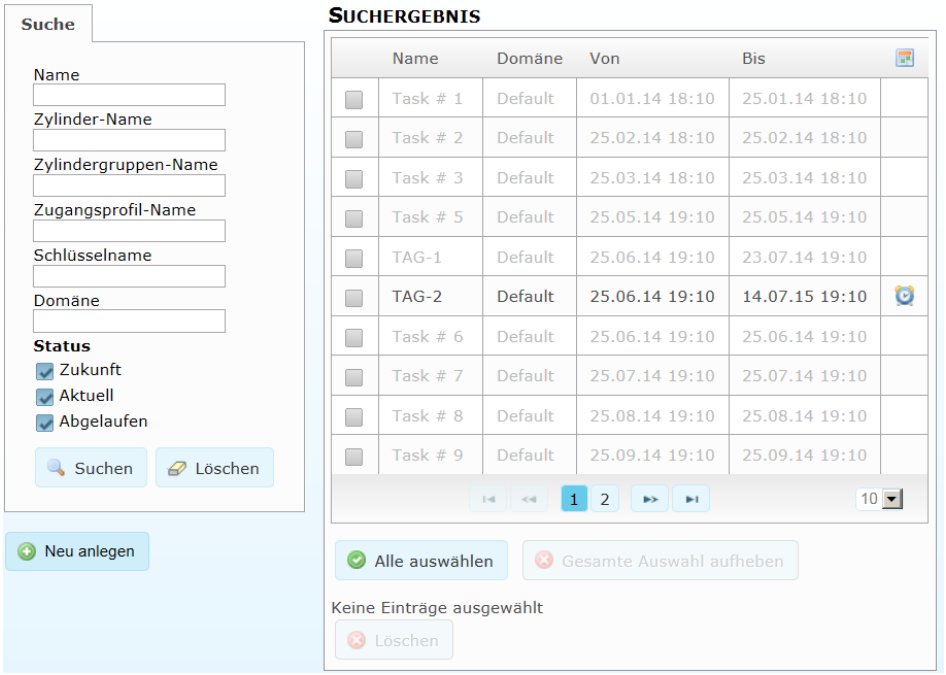
   Eine Liste mit allen Zugangsprofil-Ereignissen wird angezeigt.

4.7 Verwalten von temporären Zugangsgruppen

4.7.1 Suchen nach temporären Zugangsgruppen

1) **Systeminfo » Temporäre Zugangsgruppen** auswählen.

   Eine Liste aller temporären Zugangsgruppen wird angezeigt.



2) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

3) Zum Filtern der Suche:

   a) Das Kästchen **Abgelaufen** markieren, um temporäre Zugangsgruppen anzuzeigen, die nicht länger gültig sind.

      In der Ergebnisliste sind abgelaufene temporäre Zugangsgruppen mit grauem Text formatiert.

   b) Das Kästchen **Aktuell** markieren, um temporäre Zugangsgruppen anzuzeigen, die aktuell gültig sind.

      In der Ergebnisliste sind aktuell gültige temporäre Zugangsgruppen mit schwarzem Text formatiert und mit einem Symbol gekennzeichnet:

   c) Das Kästchen **Zukunft** markieren, um temporäre Zugangsgruppen anzuzeigen, die in der Zukunft gültig sind.

      In der Ergebnisliste sind in der Zukunft gültige temporäre Zugangsgruppen mit schwarzem Text formatiert.

4) Auf **Suchen** klicken.

5) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf die entsprechende temporäre Zugangsgruppe klicken.

4.7.2 Anlegen und Löschen von temporären Zugangsgruppen

Temporäre Zugangsgruppen gelten nur für E3-Schlüssel, die Remote-Updates unterstützen. Sie werden auf einen Schlüssel angewendet.

1) **Systeminfo » Temporäre Zugangsgruppen** auswählen.
2) Anlegen einer temporären Zugangsgruppe:
   a) Auf **Neu anlegen** klicken.
   b) **Name** eingeben.
   c) Die Zeitraumwerte **Von**- und **Bis**-Datum angeben.

> **HINWEIS!**
> Wenn die temporäre Zugangsgruppe nicht länger für einen Schlüssel gültig ist, wird automatisch ein Remote-Job angelegt, um den Zugang der temporären Zugangsgruppe vom Schlüssel zu entfernen. Der Zugang des Schlüssels wird jedoch erst beendet, wenn der Schlüssel in einem Remote-Programmiergerät aktualisiert wird.

   d) Ändern der Standard-Domäne:
      - Auf **Domäne ändern** klicken
      - Für die gewünschte Domäne auf **Auswählen** klicken.
   e) Auf **Speichern** klicken.
3) Löschen einer temporären Zugangsgruppe:
   a) Temporäre Zugangsgruppe suchen und Detailinformationen anzeigen.
      Siehe *Abschnitt 4.7.1 "Suchen nach temporären Zugangsgruppen", Seite 74*.
   b) Auf **Löschen** klicken.
   c) Auf **OK** klicken.

Es ist außerdem möglich, eine temporäre Zugangsgruppe über die Schlüsselansicht anzulegen. In der Detailanzeige das Register **Temporäre Zugangsgruppen** auswählen, auf **Neu anlegen** klicken und die Anweisungen oben befolgen (bei *Schritt 2 b* beginnen).

Siehe auch *Abschnitt 8.2.5 "Temporäre Zugangsgruppen", Seite 182*.

4.7.3 Bearbeiten von temporären Zugangsgruppen

1) Die temporäre Zugangsgruppe suchen und die Detailansicht öffnen.
   Siehe *Abschnitt 4.7.1 "Suchen nach temporären Zugangsgruppen", Seite 74*.
2) In der Detailanzeige auf **Bearbeiten** klicken.
3) Die Felder ändern.
4) Auf **Speichern** klicken.

4.7.4 Hinzufügen oder Entfernen von Schlüsseln in temporären Zugangsgruppen

HINWEIS!
Wenn eine temporäre Zugangsgruppe nicht länger für einen Schlüssel gültig ist, wird automatisch ein Remote-Job angelegt, um den Zugang der temporären Zugangsgruppe vom Schlüssel zu entfernen. Der Zugang des Schlüssels wird jedoch erst beendet, wenn der Schlüssel in einem Remote-Programmiergerät aktualisiert wird. Damit der Schlüsselhalter nach Ablauf der temporären Zugangsgruppe den Schlüssel nicht länger verwenden kann, vor dem Hinzufügen von Schlüsseln einen der folgenden Schritte durchführen:

- In den Aktivierungseinstellungen **Aktiv im festgelegten Zeitraum** einstellen, siehe *Abschnitt 8.1.4 "Schlüsselgültigkeit", Seite 170*.
- Schlüssel-**Verlängerung** aktivieren, siehe *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170*.

Es wird dringend empfohlen, temporäre Zugangsgruppen mit der Schlüssel-Verlängerung zu kombinieren.

1) Die temporäre Zugangsgruppe suchen und die Detailansicht öffnen.
   Siehe *Abschnitt 4.7.1 "Suchen nach temporären Zugangsgruppen", Seite 74*.
2) Register **Schlüssel** auswählen.
3) Auf **Bearbeiten** klicken.
4) Hinzufügen von Schlüsseln zu einer temporären Zugangsgruppe:
   a) Auf **Schlüssel hinzufügen...** klicken.
   b) Um einzelne Schlüssel hinzuzufügen, auf **Auswählen** klicken. Um alle Schlüssel hinzuzufügen, auf **Alle auswählen** klicken.
   c) Auf **Fertig** klicken.
   d) Auf **Speichern** klicken.
      Es wird automatisch ein Remote-Job angelegt.
5) Entfernen von Schlüsseln aus einer temporären Zugangsgruppe:
   a) Um einzelne Schlüssel zu entfernen, auf **Entfernen** klicken. Um alle Schlüssel zu entfernen, auf **Alle entfernen** klicken.
   b) Auf **Speichern** klicken.

4.7.5 Bearbeiten des expliziten Zugangs für temporäre Zugangsgruppen

1) Die temporäre Zugangsgruppe suchen und die Detailansicht öffnen.
   Siehe *Abschnitt 4.7.1 "Suchen nach temporären Zugangsgruppen", Seite 74*.
2) Register **Expliziter Zugang** auswählen.
3) Auf **Bearbeiten** klicken.
4) Hinzufügen oder Entfernen von Zylindergruppen:
   a) Unter **AUSGEWÄHLTE ZYLINDERGRUPPEN** auf **Zylindergruppen hinzufügen...** klicken.
      Alle verfügbaren Zylindergruppen werden angezeigt.

b) Zum Filtern der verfügbaren Zylindergruppen Suchkriterien eingeben und auf **Suchen** klicken.

c) Um Zylindergruppen hinzuzufügen, bei den hinzuzufügenden Zylindern auf **Auswählen** bzw. auf **Alle auswählen** klicken.

d) Auf **OK** klicken.

e) Um Zylindergruppen zu entfernen, bei den zu entfernenden Zylindern auf **Entfernen** bzw. auf **Alle entfernen** klicken.

5) Hinzufügen oder Entfernen von Zylindern:

a) Unter **AUSGEWÄHLTE ZYLINDER** auf **Zylinder hinzufügen...** klicken.

Das Suchergebnis enthält eine Liste der verfügbaren Zylinder.

HINWEIS!
Nur Zylinder, bei denen die Zylinderzugangsliste den gewählten Schlüssel enthält, stehen zur Verfügung.

b) Zum Filtern der verfügbaren Zylinder Suchkriterien eingeben und auf **Suchen** klicken.

c) Um Zylinder hinzuzufügen, bei den hinzuzufügenden Zylindern auf **Auswählen** bzw. auf **Alle auswählen** klicken.

d) Auf **OK** klicken.

e) Um Zylinder zu entfernen, bei den zu entfernenden Zylindern auf **Entfernen** bzw. auf **Alle entfernen** klicken.

6) Auf **Speichern** klicken.

4.7.6 Anzeigen von Ereignissen für eine temporäre Zugangsgruppe

Das Register Ereignisse wird zur Verfolgung von Administratorvorgängen in CWM verwendet, z. B. das Hinzufügen und Entfernen von Schlüsseln in einer temporären Zugangsgruppe.

1) Die temporäre Zugangsgruppe suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.7.1 "Suchen nach temporären Zugangsgruppen", Seite 74*.

2) Register **Ereignisse** auswählen.

Eine Liste mit allen Ereignissen zu temporären Zugangsgruppen wird angezeigt.

4.7.7 Löschen redundanter Schlüssel-Berechtigungen

Das Löschen redundanter Berechtigungen ist von Nutzen, wenn Zugangsprofile in einer Schließanlage eingeführt werden, bei denen die Schlüssel bereits mit expliziten Berechtigungen konfiguriert sind. Explizite Berechtigungen gelten als redundant, wenn der Schlüssel außerdem mit einem Zugangsprofil verknüpft ist, das Zugang zum gleichen Zylinder oder zur gleichen Zylindergruppe gewährt.

Tipp
Wir empfehlen, aus Gründen der besseren Übersichtlichkeit der Berechtigungen redundante Berechtigungen zu löschen.

1) Schlüssel suchen.

Siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.

2) In der Liste der Suchergebnisse die Schlüssel auswählen.

3) Auf **Redundante Berechtigungen entfernen...** klicken.

4) Auf **OK** klicken.

4.8 Anzeigen von Berechtigungen

4.8.1 Anzeigen der zugänglichen Zylinder für bestimmte Schlüssel oder Schlüsselgruppen

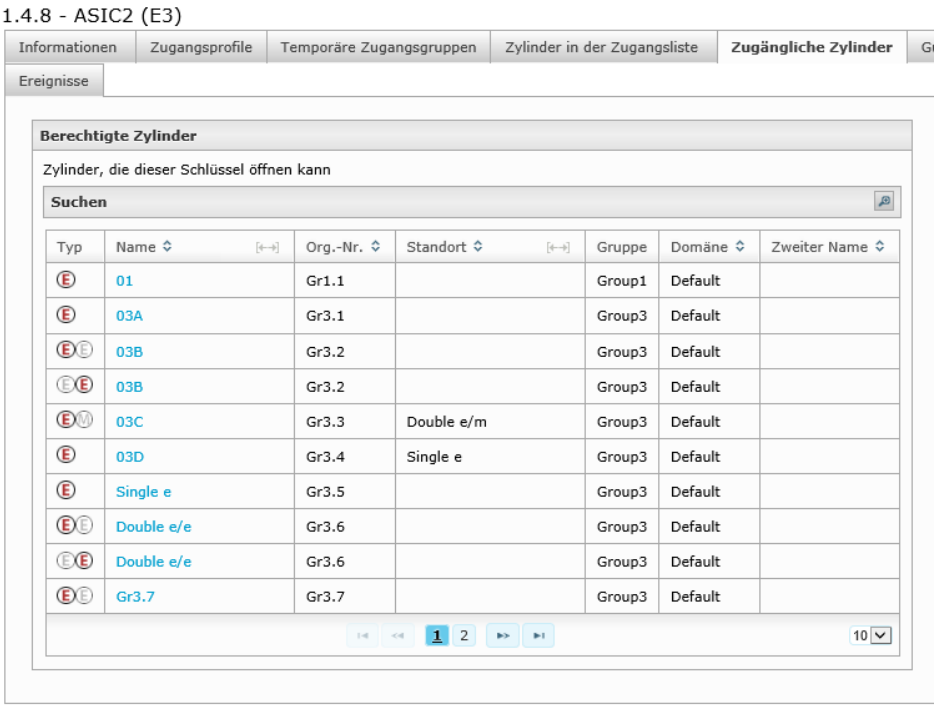
Die tatsächlichen Berechtigungen zeigen, zu welchen Zylindern ein bestimmter Schlüssel Zugang hat, unter Berücksichtigung sowohl der Schlüsselzugangsliste als auch der Zylinderzugangsliste. Dies sind die Zylinder, die ein Schlüssel tatsächlich öffnen kann.

1) Den Schlüssel oder die Schlüsselgruppe suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.3.1 "Suchen nach Schlüsselgruppen", Seite 54*.

2) Register **Zugängliche Zylinder** auswählen.

   Eine Liste aller Zylinder, für die die Schlüsselgruppe eine Berechtigung hat, wird angezeigt.



Bei Doppelzylindern werden A-Seite und B-Seite separat angezeigt. Das Symbol zeigt an, für welche Seite die Angaben gelten (die andere Seite ist ausgegraut)

Angaben gelten für A-Seite

Angaben gelten für B-Seite

HINWEIS!
Einzelne Schlüssel können vom Zugang ausgenommen sein. Siehe *Abschnitt 8.1.2 "Elektronische Berechtigung", Seite 168*.

4.8.2 Anzeigen von Schlüsseln mit Berechtigung für bestimmte Zylinder oder Zylindergruppen

Schlüssel mit Zugang zu einem Zylinder sind Schlüssel, die unter Berücksichtigung der Schlüsselzugangslisten und der Zylinderzugangslisten Zugang zu einem Zylinder haben. Dies sind die Schlüssel, die den Zylinder tatsächlich öffnen können.

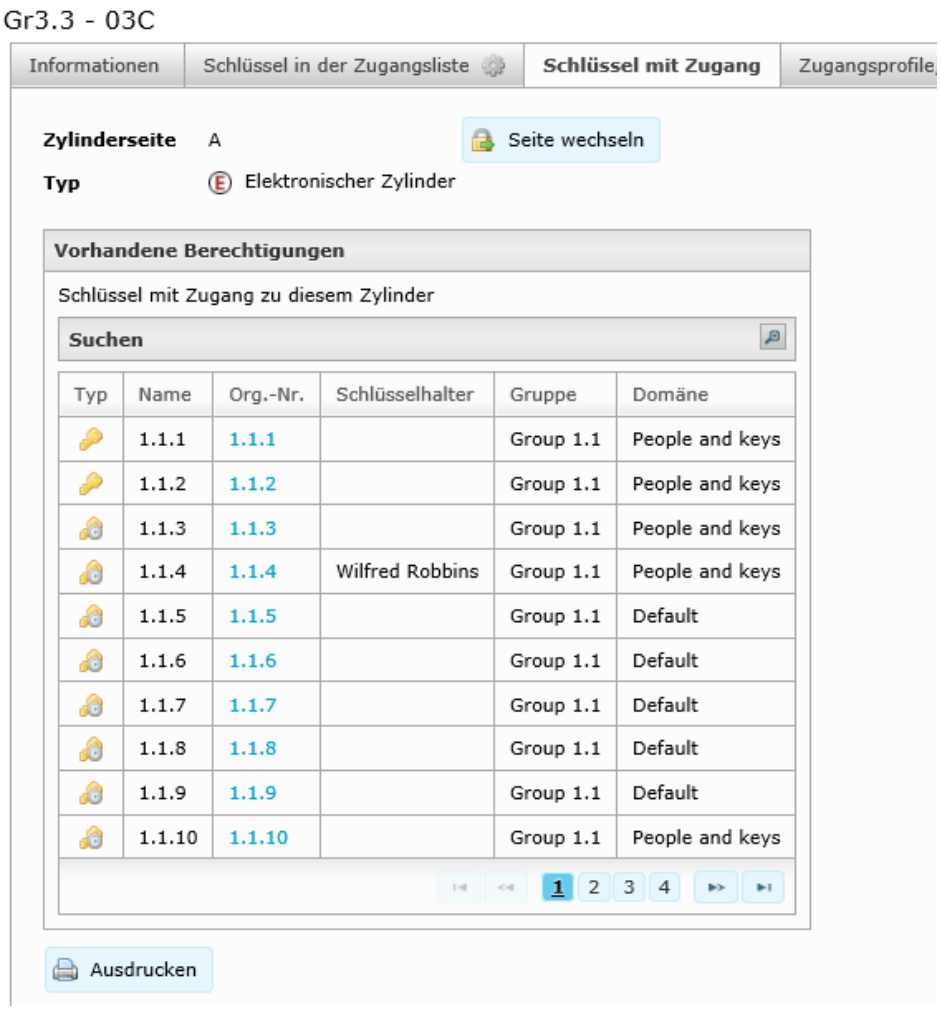
1) Den Schlüssel oder die Zylindergruppe suchen und die Detailansicht öffnen.

   - Suche nach einem Zylinder siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.
   - Suche nach einer Zylindergruppe siehe *Abschnitt 4.5.1 "Suchen nach Zylindergruppen", Seite 69*.

2) Register **Schlüssel mit Zugang** auswählen.

   Eine Liste der Schlüssel, die über die Berechtigung für den Zylinder oder die Zylindergruppe verfügen, wird angezeigt.

   Schlüssel, die berechtigten Schlüsselgruppen angehören, werden einzeln angezeigt.



4.8.3 Anzeigen von Zugangsprofilen, die Zugang zu einem Zylinder oder zu einer Zylindergruppe gewähren

Schlüssel, die mit einem Zugangsprofil verknüpft sind, haben automatisch Zugang zu den Zylindern und Zylindergruppen, die in diesem Zugangsprofil angegeben sind. Achtung:

Dies heißt nicht unbedingt, dass der Schlüssel den Zylinder öffnen kann, da der tatsächliche Zugang auch von der Zugangsliste im Zylinder abhängt.

1) Den Schlüssel oder die Zylindergruppe suchen und die Detailansicht öffnen.

   - Suche nach einem Zylinder siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.
   - Suche nach einer Zylindergruppe siehe *Abschnitt 4.5.1 "Suchen nach Zylindergruppen", Seite 69*.

2) Register **Zugangsprofile, die Zugang gewähren** auswählen.

Siehe auch *Abschnitt 4.9.4 "Konfigurieren von Berechtigungen in Zugangsprofilen", Seite 86*.

4.9 Konfigurieren von Berechtigungen

4.9.1 Konfigurieren von Berechtigungen in Schlüsseln

E3-Schlüssel haben eine Zugangsliste, in der die Zylinder und Zylindergruppen enthalten sind, die der Schlüssel öffnen darf. Berechtigungen in Schlüsseln konfigurieren heißt, die expliziten Berechtigungen in dieser Zugangsliste bearbeiten. Die Zugangsliste kann auch implizite Berechtigungen beinhalten, die aus Zugangsprofilen stammen. Änderung von Berechtigungen in Zugangsprofilen siehe *Abschnitt 4.9.4 "Konfigurieren von Berechtigungen in Zugangsprofilen", Seite 86*.

Die Tatsache, dass ein Zylinder in der Schlüsselzugangsliste enthalten ist, heißt nicht unbedingt, dass der Schlüssel tatsächlich Zugang hat. Der tatsächliche Zugang hängt auch von der Zugangsliste im Zylinder ab. Anzeige der Zylinder, die ein Schlüssel tatsächlich öffnen kann, siehe *Abschnitt 4.8.1 "Anzeigen der zugänglichen Zylinder für bestimmte Schlüssel oder Schlüsselgruppen", Seite 79*.

Zum Entfernen aller Zugänge eines Zylinders siehe *Abschnitt 4.9.3 "Entfernen aller Zugänge eines Zylinders", Seite 85*.

Weitere Informationen zu Berechtigungsprinzipien siehe *Abschnitt 8.1 "Berechtigungsprinzipien", Seite 168*.

1) Den Schlüssel suchen und die Detailansicht öffnen.

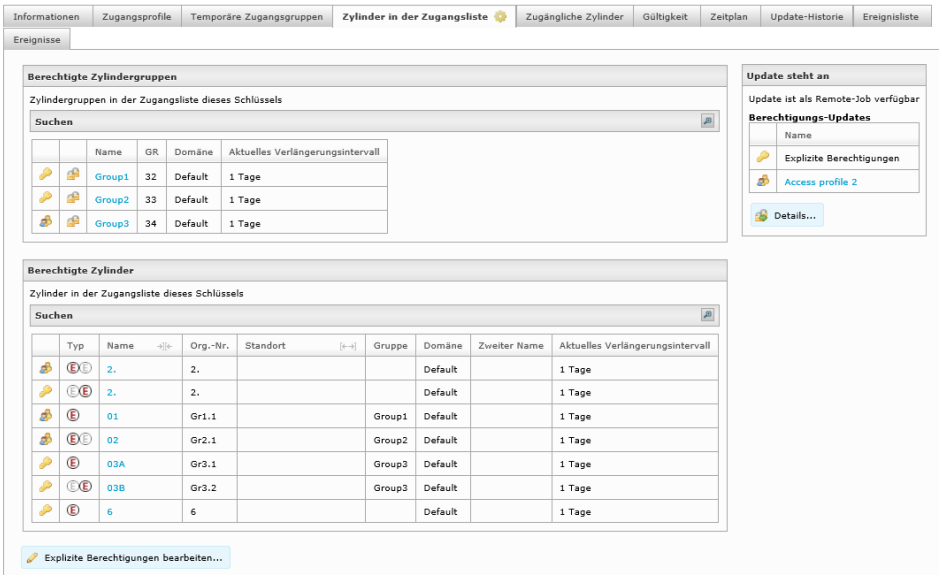
   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Register **Zylinder in der Zugangsliste** auswählen.

   Aktuell berechtigte Zylindergruppen und Zylinder werden angezeigt.

1.3.2 - 1.3.2



Die Zugangsliste enthält explizite Berechtigungen.

 Explizite Berechtigung

 Berechtigung aus Zugangsprofil

Bei Doppelzylindern werden A-Seite und B-Seite separat angezeigt. Das Symbol zeigt an, für welche Seite die Angaben gelten (die andere Seite ist ausgegraut)

 Angaben gelten für A-Seite

 Angaben gelten für B-Seite

Anstehende Remote-Updates werden unter **Update steht an** aufgeführt.

3) Auf **Explizite Berechtigungen bearbeiten...** klicken.

Die festgelegten expliziten Berechtigungen für den Schlüssel werden angezeigt.

Tipp

Zylindergruppen und Zylinder können direkt in dieser Ansicht gelöscht werden, indem bei der zu entfernenden Zylindergruppe bzw. dem zu entfernenden Zylinder auf **Entfernen** geklickt wird.

Beim Entfernen von Schlüsseln mit langen Zugangslisten kann es hilfreich sein, die Zylindergruppen und Zylinder zuerst zu filtern.

4) Hinzufügen oder Entfernen von Zylindergruppen:

a) Unter **Explizite Zylindergruppenberechtigungen** auf **Zylindergruppen ändern...** klicken.

Alle verfügbaren Zylindergruppen werden angezeigt.

b) Zum Filtern der verfügbaren Zylindergruppen Suchkriterien eingeben und auf **Suchen** klicken.

c) Für die hinzuzufügenden Zylindergruppen auf **Auswählen** klicken. Alternativ auf **Alle auswählen** klicken.

d) Für die zu entfernenden Zylindergruppen auf **Entfernen** klicken. Alternativ auf **Alle entfernen** klicken.

e) Auf **OK** klicken.

5) Einzelne Zylinder hinzufügen oder entfernen:

a) Unter **Explizite Zylinderberechtigungen** auf **Zylinder ändern...** klicken.

Das Suchergebnis enthält eine Liste der verfügbaren Zylinder.

> **HINWEIS!**
> Nur Zylinder, bei denen die Zylinderzugangsliste den gewählten Schlüssel enthält, stehen zur Verfügung.

b) Zum Filtern der verfügbaren Zylinder Suchkriterien eingeben und auf **Suchen** klicken.

c) Für die hinzuzufügenden Zylinder auf **Auswählen** klicken. Alternativ auf **Alle auswählen** klicken.

d) Für die zu entfernenden Zylinder auf **Entfernen** klicken. Alternativ auf **Alle entfernen** klicken.

e) Auf **OK** klicken.

6) Auf **Speichern** klicken.

Der Fortschritt und die geschützte Dauer des Vorgangs werden in einem Popup-Fenster angezeigt.

7) Falls der Schlüssel abgefragt ist, für ein Update des Schlüssels auf **Zugangsliste lokal in den Schlüssel schreiben** klicken.

> **HINWEIS!**
> Wenn die Verlängerung für den Schlüssel aktiviert ist, wird der Schlüssel während des Programmiervorgangs im lokalen PG verlängert.

Anderenfalls wird ein Schlüssel-Update-Job angelegt.

4.9.2 Konfigurieren von Berechtigungen in Zylindern

Eine Zylinderzugangsliste wird in Zylindern gespeichert und enthält die Schlüssel und Schlüsselgruppen, die berechtigt sind, den Zylinder zu öffnen. Konfigurieren von Berechtigungen in Zylinder heißt, diese Zugangsliste bearbeiten.

Bei Benutzerschlüsseln: Die Tatsache, dass ein Schlüssel in der Zylinderzugangsliste enthalten ist, bedeutet nicht unbedingt, dass der Schlüssel tatsächlich Zugang hat, da der tatsächliche Zugang auch von der Zugangsliste im Schlüssel abhängt. Anzeige der Schlüssel, die einen Zylinder tatsächlich öffnen können siehe *Abschnitt 4.8.2 "Anzeigen von Schlüsseln mit Berechtigung für bestimmte Zylinder oder Zylindergruppen", Seite 80*.

Weitere Informationen zu Berechtigungsprinzipien siehe *Abschnitt 8.1 "Berechtigungsprinzipien", Seite 168*.

1) Den Zylinder suchen und die Detailansicht öffnen.

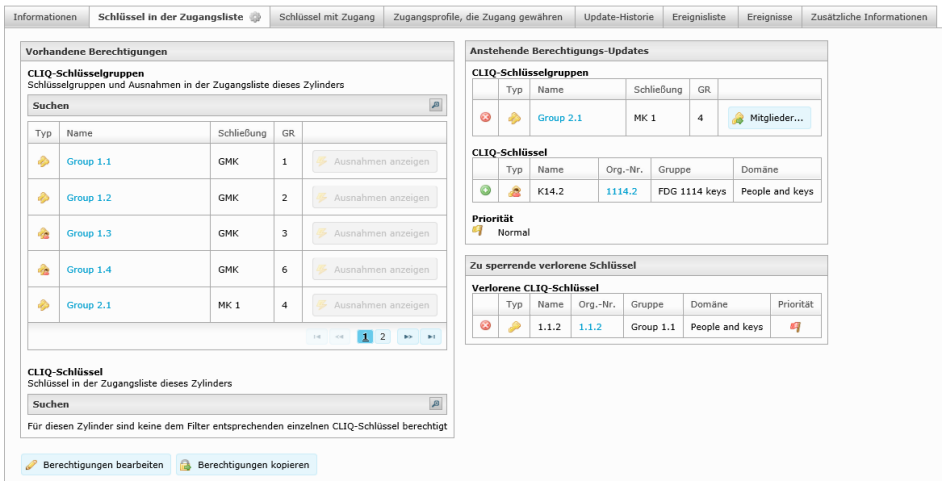
Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Register **Schlüssel in der Zugangsliste** auswählen.

Aktuell berechtigte Schlüsselgruppen und Schlüssel werden angezeigt.

Eventuelle Zylinderprogrammierungs-Jobs mit Berechtigungs-Updates werden unter **Anstehende Berechtigungs-Updates** aufgeführt.

Eventuelle Zylinderprogrammierungs-Jobs aufgrund verlorener Schlüssel werden unter **Zu sperrende verlorene Schlüssel** aufgeführt.



3) Zum Anzeigen von Schlüsseln, die zu einer berechtigten Schlüsselgruppe gehören, jedoch nicht zugangsberechtigt sind, auf **Ausnahmen anzeigen** klicken.

4) Auf **Berechtigungen bearbeiten** klicken.

5) **Schlüsselgruppen oder einzelne Schlüssel hinzufügen**

   1. Auf **CLIQ-Schlüsselgruppe hinzufügen** klicken.

      Das Suchergebnis enthält eine Liste aller verfügbaren Schlüsselgruppen.

   2. Zum Filtern der verfügbaren Schlüsselgruppen Suchkriterien eingeben und auf **Suchen** klicken.

   3. Bei den hinzuzufügenden Schlüsselgruppen auf **Auswählen** klicken.

      HINWEIS!
      Wenn eine Schlüsselgruppe zu einer Zugangsliste hinzugefügt wird, werden alle individuellen Einträge mit Schlüsseln dieser Schlüsselgruppe (jetzt redundant) automatisch entfernt. Das bedeutet: wenn eine Schlüsselgruppe hinzugefügt und später wieder entfernt wird, verlieren alle Schlüssel in dieser Gruppe ihre Zugangsberechtigung, einschließlich der Schlüssel, die zuvor über individuellen Zugang verfügt haben.

   4. Auf **Fertig** klicken.

Schlüssel von der Berechtigung einer Schlüsselgruppe ausschließen

1. Bei der Schlüsselgruppe auf **Bearbeiten** klicken.
2. Um die Zugangsberechtigung von Schlüsseln aufzuheben, auf **Berechtigung aufheben** klicken.

Schlüssel erneut in einer Schlüsselgruppe autorisieren

> **HINWEIS!**
> Bevor der Schlüssel erneut berechtigt werden kann, muss er als gefunden gemeldet werden.
>
> In der Detailansicht des Schlüssels auf **Als gefunden melden** klicken.

1. Bei der Schlüsselgruppe auf **Bearbeiten...** klicken.
2. Auf **Berechtigen** klicken, um den Schlüsseln die Berechtigung für den Zugang zum Zylinder zu erteilen.

Schlüsselgruppen oder einzelne Schlüssel entfernen
Für die zu entfernende Schlüsselgruppe auf „Entfernen“ klicken.

6) Nach Abschluss der Bearbeitung auf **Zur Anzeige** klicken.

Ein Zylinderprogrammier-Job wird angelegt.

Programmieren von Zylindern siehe *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64*.

Berechtigungen können für mehrere Zylinder gleichzeitig bearbeitet werden. Die Zylinder in der Liste der Suchergebnisse auswählen (siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*) und auf **Berechtigungen hinzufügen** oder **Berechtigungen aufheben** klicken.

4.9.3 Entfernen aller Zugänge eines Zylinders

Einzelne Zylinder lassen sich von allen Schlüsseln, Zugangsprofilen und temporären Zugangsgruppen entfernen.

Die Möglichkeit, den gesamten Zugang für einen Zylinder zu entfernen, erfordert eine Schließanlage mit E3-Schlüsseln.

1) Den Zylinder suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) **Schlüsselseitige Berechtigungen entfernen** auswählen.

> **HINWEIS!**
> Um den Zugang zu entfernen, müssen alle Schlüssel mit bisherigem Zugang zum Zylinder aktualisiert werden.

> **HINWEIS!**
> **Schlüsselseitige Berechtigungen entfernen** entfernt den Zylinder nur in solchen Schlüsseln aus der Zugangsliste, die Remote-Updates unterstützen.
>
> Um zu sehen, ob irgendwelche Nicht-Remote-Schlüssel Zugang zum Zylinder haben, das Register **Schlüssel mit Zugang** wählen. Für alle diese Schlüssel den Schlüssel in das lokale PG einsetzen, den Schlüssel abfragen, das Register **Zylinder in der Zugangsliste** auswählen, auf **Explizite Berechtigungen bearbeiten** klicken und den Zylinder entfernen.
>
> Informationen zu Remote-Funktionen siehe *Abschnitt 8.3.1 "Remote-Funktion - Überblick", Seite 184*.

3) Im Pop-up-Fenster auf **OK** klicken.

4.9.4 Konfigurieren von Berechtigungen in Zugangsprofilen

Konfigurieren von Zugangsprofil-Berechtigungen heißt, die impliziten Berechtigungen für mit dem Zugangsprofil verknüpfte Schlüssel und Personen zu bearbeiten.

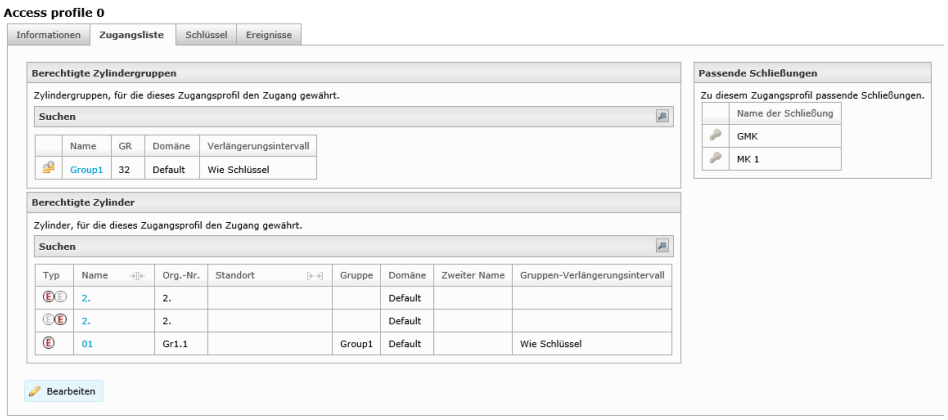
1) Das Zugangsprofil suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.

2) Register **Zugangsliste** auswählen.

   Aktuell berechtigte Zylinder und Zylindergruppen werden angezeigt.

3) Auf **Bearbeiten** klicken.



Bei Doppelzylindern werden A-Seite und B-Seite separat angezeigt. Das Symbol zeigt an, für welche Seite die Angaben gelten (die andere Seite ist ausgegraut)

- Angaben gelten für A-Seite
- Angaben gelten für B-Seite

4) **Hinzufügen von Zylindern oder Zylindergruppen**

1. Auf **Zylinder hinzufügen...** oder **Zylindergruppen hinzufügen...** klicken.

   Im Popup-Fenster wird die Liste der verfügbaren Zylinder oder Zylindergruppen angezeigt.
2. Um das Ergebnis zu filtern, geben Sie Suchkriterien ein und klicken Sie auf **Suchen**.
3. Klicken Sie für die hinzuzufügenden Elemente auf **Auswählen** oder klicken Sie auf **Alle auswählen**.
4. Auf **OK** klicken.

Entfernen von Zylindern oder Zylindergruppen

1. Klicken Sie auf das Suchsymbol und geben Sie die Suchkriterien ein.
2. Auf **Suchen** klicken.

   Das Suchergebnis wird in der Tabelle angezeigt.
3. – Entfernen einzelner Elemente:

     Auf **Entfernen** klicken.
   – Entfernen aller Elemente in den Suchergebnissen:

     Auf **Alle aufgeführten entfernen** klicken.

5) Auch die flexible Verlängerung kann in dieser Ansicht bearbeitet werden. Siehe *Abschnitt 4.10.2 "Konfigurieren der flexiblen Verlängerung", Seite 91*.

6) Klicken Sie auf **Speichern**, um den Bearbeitungsmodus zu beenden.

Siehe auch *Abschnitt 8.2.4 "Zugangsprofile", Seite 180*.

4.9.5 Auswählen von Zugangsprofilen von Mitarbeitern oder Besuchern

Zugangsprofile gelten nur für E3-Schlüssel, andere Schlüssel sind nicht enthalten.

1) Den Mitarbeiter oder Besucher suchen und die Detailansicht öffnen.

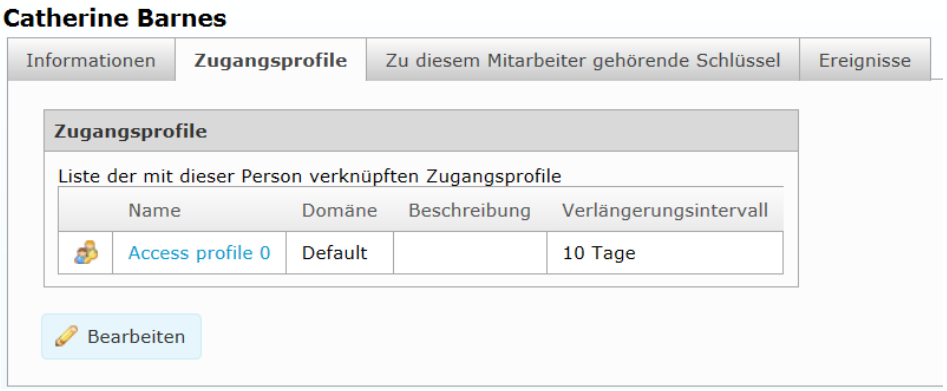
   Siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

2) Register **Zugangsprofile** auswählen.

   Die Liste der Suchergebnisse enthält die Zugangsprofile, die aktuell mit dem Mitarbeiter oder Besucher verknüpft sind.

3) Auf **Bearbeiten** klicken.

   Eine Liste aller zugehörigen Zugangsprofile wird angezeigt.



4) Zugangsprofile hinzufügen:

   a) Auf **Zugangsprofile hinzufügen** klicken.

      Das Suchergebnis enthält eine Liste aller verfügbaren Zugangsprofile.

   b) Zum Filtern der verfügbaren Zugangsprofile **Name**, **Beschreibung**, **Domäne** und/oder **Tags** in das Suchfeld eingeben.

   c) Auf **Auswählen** klicken, um ein Zugangsprofil auszuwählen, bzw. auf **Alle auswählen** klicken.

   d) Auf **Fertig** klicken.

5) Zum Entfernen von Zugangsprofilen auf **Entfernen** klicken, um ein einzelnes Zugangsprofil zu entfernen, bzw. auf **Alle entfernen** klicken.

6) Auf **Speichern** klicken.

Zugangsprofile für mehrere Mitarbeiter oder Besucher können gleichzeitig hinzugefügt oder entfernt werden. Die Mitarbeiter oder Besucher in der Liste der Suchergebnisse auswählen und auf **Zugangsprofile hinzufügen** oder **Zugangsprofile entfernen** klicken.

Siehe auch *Abschnitt 8.2.4 "Zugangsprofile", Seite 180*.

4.9.6 Auswählen von Schlüsselzugangsprofilen

Zugangsprofile gelten nur für E3-Schlüssel.

1) Den Schlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Register **Zugangsprofile** auswählen.

   Die Liste der Suchergebnisse enthält die Zugangsprofile, die aktuell mit dem Schlüssel verknüpft sind.

3) Auf **Bearbeiten** klicken.

4) Zugangsprofile hinzufügen:

   a) Auf **Zugangsprofile hinzufügen** klicken.

      Das Suchergebnis enthält eine Liste aller verfügbaren Zugangsprofile.

   b) Zum Filtern der verfügbaren Zugangsprofile Suchkriterien eingeben und auf **Suchen** klicken.

c) Auf **Auswählen** klicken, um ein Zugangsprofil auszuwählen, bzw. auf **Alle auswählen** klicken.

d) Auf **Fertig** klicken.

5) Zum Entfernen von Zugangsprofilen auf **Entfernen** klicken, um ein einzelnes Zugangsprofil zu entfernen, bzw. auf **Alle entfernen** klicken.

6) Auf **Speichern** klicken.

Zugangsprofile können für mehrere Schlüssel gleichzeitig bearbeitet werden. Die Schlüssel in der Liste der Suchergebnisse auswählen und auf **Zugangsprofile hinzufügen** oder **Zugangsprofile entfernen** klicken.

Siehe auch *Abschnitt 8.2.4 "Zugangsprofile", Seite 180*.

4.9.7 Auswählen von Zugangsprofilen für temporäre Zugriffsgruppen

1) Die temporäre Zugangsgruppe suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.7.1 "Suchen nach temporären Zugangsgruppen", Seite 74*.

2) Register **Zugangsprofile** auswählen.

3) Auf **Bearbeiten** klicken.

4) Hinzufügen von Zugangsprofilen zu einer temporären Zugangsgruppe:

   a) Auf **Zugangsprofile hinzufügen...** klicken.

   b) Um einzelne Zugangsprofile hinzuzufügen, auf **Auswählen** klicken. Um alle Zugangsprofile hinzuzufügen, auf **Alle auswählen** klicken.

   c) Auf **Fertig** klicken.

   d) Auf **Speichern** klicken.

5) Entfernen von Zugangsprofilen von einer temporären Zugangsgruppe:

   a) Um einzelne Zugangsprofile zu entfernen, auf **Entfernen** klicken. Um alle Zugangsprofile zu entfernen, auf **Alle entfernen** klicken.

   b) Auf **Speichern** klicken.

4.10 Konfigurieren von Schlüsselgültigkeit und Zeitplan

4.10.1 Konfigurieren der Schlüsselgültigkeit, Verlängerung und PIN-Validierung

1) Den Schlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Register **Gültigkeit** auswählen.

1.3.2 - 1.3.2

Das Register Gültigkeit zeigt:

- Gültigkeitseinstellungen: Ob der Schlüssel immer aktiv ist, ob er immer inaktiv ist bzw. Datumsangaben, zwischen denen der Schlüssel aktiv ist.
- Bei Verwendung der Verlängerung:
  - **Verlängerungsintervall**: Der Zeitraum, in dem ein Schlüssel nach einer Verlängerung aktiv bleibt, bevor er erneut verlängert werden muss.
  - **Nächstes Ablaufdatum**: Datum und Uhrzeit, wann der Schlüssel ohne Verlängerung inaktiv wird.

    Bei Remote-Verlängerung eines Schlüssels mit Status **Immer aktiv** wird **Der Schlüssel kann immer verlängert werden** angezeigt. Das nächste Ablaufdatum lautet **Niemals**, bis der Schlüssel zum ersten Mal verlängert wird.

    Bei Remote-Verlängerung eines Schlüssels mit Status **Aktiv im Zeitraum** entspricht dieser Wert **Schlüssel aktiv bis**, bis der Schlüssel zum ersten Mal verlängert wird.
- Bei Verwendung der PIN-Validierung:
  - **PIN-Validierungsintervall**: Der Zeitraum, in dem der Schlüssel nach einer PIN-Validierung aktiv bleibt, bis der PIN-Code erneut eingegeben werden muss.
- Sommerzeit-Einstellungen

3) Auf **Gültigkeit bearbeiten** klicken.
4) Auswählen, ob der Schlüssel **Inaktiv**, **Aktiv im festgelegten Zeitraum** oder **Immer aktiv** sein soll.
5) Wenn **Aktiv im festgelegten Zeitraum** gewählt ist, **Schlüssel aktiv von** und **Schlüssel aktiv bis** eingeben.
6) Konfiguration der Verlängerung:
   a) **Schlüssel-Verlängerung verwenden** auswählen.
   b) Tage, Stunden und Minuten für **Verlängerungsintervall** eingeben.

      Dies ist der Zeitraum, über den der Schlüssel nach Gültigkeitsverlängerung in einem Remote-Programmiergerät aktiv bleibt.
   c) Um nur eine einmalige Verlängerung zuzulassen, **Einmaliges Update** auswählen.
7) Zur Konfiguration der PIN-Validierung:
   a) **PIN-Validierung verwenden** auswählen.

b) Tage, Stunden und Minuten für **PIN-Validierungsintervall** eingeben.

Dies ist der Zeitraum, über den der Schlüssel nach einer Validierung mit PIN aktiv bleibt.

Der angegebene Zeitraum muss zwischen einer Minute und 45 Tagen liegen.

c) Für **Neue Anfangs-PIN** wird automatisch eine Zufalls-PIN generiert. Die generierte PIN kann auch überschrieben und manuell eine neue Anfangs-PIN eingegeben werden.

Mit **Wert anzeigen** wird der PIN-Code sichtbar gemacht.

Ist für den Schlüsselhalter eine E-Mail-Adresse eingetragen, wird eine E-Mail mit dem Anfangs-PIN-Code gesendet. Der Benutzer muss diesen PIN-Code bei der ersten Verwendung ändern.

8) Zur Bestätigung der Updates:

a) Wenn der Schlüssel abgefragt ist, auf **In den Schlüssel schreiben** klicken.

Die neuen Einstellungen werden in den Schlüssel geschrieben.

b) Wenn der Schlüssel nicht abgefragt ist, auf **Remote-Update senden** klicken.

Ein Remote Update Job wird angelegt.

Gültigkeit, Verlängerung und PIN-Validierung lassen sich für mehrere Schlüssel gleichzeitig anpassen. Die Schlüssel in der Liste der Suchergebnisse auswählen, auf **Gültigkeitseinstellungen ändern...** klicken und die Anweisungen befolgen.

Siehe auch *Abschnitt 8.1.4 "Schlüsselgültigkeit", Seite 170*, *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170* und *Abschnitt 8.1.7 "PIN-Validierung", Seite 174*.

4.10.2 Konfigurieren der flexiblen Verlängerung

ACHTUNG!
Da die flexible Verlängerung eine komplexe, erweiterte Funktion ist, empfehlen wir, *Abschnitt 8.1.6 "Flexible Verlängerung", Seite 173* vor der Konfiguration sorgfältig zu lesen.

Voraussetzungen:

- Mindestens ein Benutzerschlüssel verfügt über eine Firmware, die die flexible Verlängerung unterstützt (siehe *Abschnitt 9.7 "Firmware-abhängige Funktionen", Seite 215*).
- Die Funktion wird in den **Systemeinstellungen** aktiviert (siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*).

HINWEIS!
Bei Verwendung der flexiblen Verlängerung muss bei allen Schlüsseln, die von den Verlängerungseinstellungen in den Zugangsprofilen oder Zylindergruppen betroffen sind, die Verlängerung aktiviert sein.

1) Einstellung des Verlängerungsintervalls in einem Zugangsprofil:

a) Das Zugangsprofil suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.

b) Auf **Bearbeiten** klicken.

c) Option für **Verlängerung** auswählen.

- Um ein Verlängerungsintervall anzugeben, **Spezifisches Intervall verwenden** auswählen.
- Um ein unbestimmtes Verlängerungsintervall zu belassen, **Verlängerungsintervall von Zylindergruppen verwenden** auswählen.

  Das in den Zylindergruppen eingestellte Verlängerungsintervall wird für Zylindergruppen verwendet, bei denen ein Intervall spezifiziert wurde. Ansonsten wird das auf den Schlüsseln eingestellte Verlängerungsintervall verwendet.

d) Bei Auswahl von **Spezifisches Intervall verwenden** das Intervall als Anzahl von Tagen, Stunden und Minuten eingeben.

e) Auf **Speichern** klicken.

f) Das Verlängerungsintervall kann für mehrere Zugangsprofile gleichzeitig bearbeitet werden. Die Zugangsprofile in der Liste der Suchergebnisse auswählen und auf **Verlängerungsintervall bearbeiten** klicken.

2) Einstellen des Verlängerungsintervalls für eine Zylindergruppe:

a) Die Zylindergruppe suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.5.1 "Suchen nach Zylindergruppen", Seite 69*.

b) Auf **Bearbeiten** klicken.

c) Option für **Verlängerung** auswählen.

- Um ein Verlängerungsintervall anzugeben, **Spezifisches Intervall verwenden** auswählen.
- Um ein unbestimmtes Verlängerungsintervall zu belassen, **Verlängerungsintervall der Schlüssel verwenden** auswählen.

  Das auf den Schlüsseln eingestellte Verlängerungsintervall wird verwendet.

d) Bei Auswahl von **Spezifisches Intervall verwenden** das Intervall als Anzahl von Tagen, Stunden und Minuten eingeben.

e) Auf **Speichern** klicken.

f) Das Verlängerungsintervall kann für mehrere Zylindergruppen gleichzeitig bearbeitet werden. Die Zylindergruppen in der Liste der Suchergebnisse auswählen und auf **Verlängerungsintervall bearbeiten** klicken.

3) Um zu prüfen, ob die Verlängerungsintervalle für einen Schlüssel wie vorgesehen konfiguriert sind, bei jedem Zylinder in der Schlüsselzugangsliste die Spalte **Aktuelles Verlängerungsintervall** ansehen. Siehe *Abschnitt 4.9.1 "Konfigurieren von Berechtigungen in Schlüsseln", Seite 81*.

Siehe auch *Abschnitt 8.1.6 "Flexible Verlängerung", Seite 173*.

4.10.3 Konfigurieren des Schlüsselzeitplans

Es gibt zwei verschiedene Zeitpläne - einen Basiszeitplan und einen Zeitplan mit mehreren Zeitfenster (siehe *Abschnitt 8.1.8 "Schlüssel-Zeitpläne", Seite 175*). Die Firmware des Schlüssels bestimmt, welcher Typ eingesetzt wird. Informationen darüber, welche

Versionen der Schlüsselfirmware welche Art von Zeitplan unterstützt siehe *Abschnitt 9.7 "Firmware-abhängige Funktionen", Seite 215*

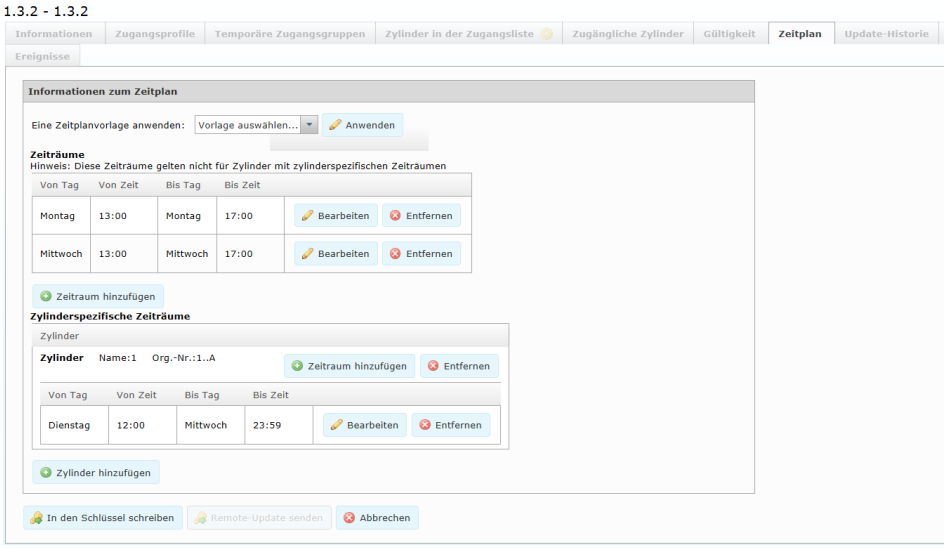
1) Den Schlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Register **Zeitplan** auswählen.

3) Auf **Zeitplan bearbeiten** klicken.



4) Um eine Zeitplanvorlage anzuwenden, eine Vorlage im Drop-down-Menü auswählen und auf **Anwenden** klicken.

   Die Vorlage wird angewendet. Der Zeitplan kann jedoch noch geändert werden.

5) Prüfen, ob der Schlüssel einen Basiszeitplan oder einen Zeitplan mit mehreren Zeitfenstern verwendet.

   Wenn der Schlüssel einen Zeitplan mit mehreren Zeitfenstern verwendet, wird zusätzlich zu **Zeiträume** auch **Zylinderspezifische Zeiträume** angezeigt.

6) Bearbeiten eines Basiszeitplans:

   a) In der Zeile mit dem zu bearbeitenden Tag auf **Bearbeiten** klicken.

   b) **Den ganzen Tag**, **Niemals** oder **Benutzerdefiniert** auswählen.

   c) Wenn die Option Benutzerdefiniert ausgewählt ist, die Zeitraumwerte **Von Zeit** und **Bis Zeit** angeben.

   d) Auf **Speichern** klicken.

7) Bearbeiten eines Zeitplans mit mehreren Zeitfenstern:

   a) Zeitperiode hinzufügen:

      - Auf **Zeitraum hinzufügen** klicken.
      - Die Zeitraumwerte **Von Datum** und **Bis Datum** angeben.
      - Auf **Speichern** klicken.

   b) Um den Zeitraum zu bearbeiten, auf **Zeitraum bearbeiten** klicken.

c) Um einen Zeitraum zu entfernen, auf **Zeitraum entfernen** klicken.

d) Hinzufügen eines Zeitraums für einen speziellen Zylinder:

- Auf **Zylinder hinzufügen** klicken.

  Das Suchergebnis enthält eine Liste aller verfügbaren Zylinder.
- Zum Filtern der verfügbaren Zylinder Suchkriterien eingeben und auf **Suchen** klicken.
- Beim hinzuzufügenden Zylinder auf **Auswählen** klicken.
- Zeitperioden für den Zylinder hinzufügen, bearbeiten und entfernen.

HINWEIS!

Bei Generation-1-Schlüsseln:

– Bei Zylindern, die einzeln (nicht als Teil einer Zylindergruppe) in der Schlüsselzugangsliste enthalten sind, bedeutet die Angabe eines oder mehrerer Zeiträume für einen Zylinder, dass der allgemeine Zeitplan für diesen Zylinder nicht beachtet wird.

– Bei Zylindern, die als Teil einer Zylindergruppe in der Schlüsselzugangsliste enthalten sind, werden die zylinderspezifischen Zeiträume nicht beachtet.

Bei Generation-2-Schlüsseln:

– Die Angabe eines oder mehrerer Zeiträume für einen Zylinder bedeutet, dass der allgemeine Zeitplan für diesen Zylinder nicht beachtet wird.

8) Zur Bestätigung der Updates:

a) Wenn der Schlüssel abgefragt ist, auf **In den Schlüssel schreiben** klicken.

Die neuen Einstellungen werden in den Schlüssel geschrieben. Wenn die Verlängerung für den Schlüssel aktiviert ist, wird der Schlüssel gleichzeitig automatisch verlängert.

b) Wenn der Schlüssel nicht abgefragt ist, auf **Remote-Update senden** klicken.

Ein Schlüssel-Update-Job wird angelegt.

4.10.4 Konfigurieren des Schlüsselgruppenzeitplans

Ein Zeitplan kann für alle Schlüssel in einer Schlüsselgruppe konfiguriert werden.

1) Die Schlüsselgruppe suchen und die Detailansicht öffnen.

Siehe *Abschnitt 4.3.1 "Suchen nach Schlüsselgruppen", Seite 54*.

2) Auf **Schlüssel-Massenkonfiguration** klicken.

3) **Zeitplan einstellen** auswählen.

4) Auf **Weiter** klicken.

5) Zeitplaneinstellungen eingeben. Weitere Informationen siehe *Abschnitt 4.10.3 "Konfigurieren des Schlüsselzeitplans", Seite 92*.

6) Auf **Weiter** klicken.

Die gewählten Einstellungen werden angezeigt.

7) Zur Bestätigung der Updates auf **Anwenden** klicken.

Schlüssel-Update-Jobs werden angelegt.

4.11 Verwalten von Ereignislisten

Für E2-Schlüssel, E3-Schlüssel und Zylinder gibt es eine Ereignislistenfunktion.

Eine Ereignisliste enthält ein Protokoll der Zugriffsversuche, der Schlüsselhalter zum jeweiligen Zeitpunkt und der Programmierdatensätze des Geräts. Weitere Informationen siehe *Abschnitt 8.6 "Ereignislisten", Seite 190*.

4.11.1 Anzeigen von Ereignislisten für Benutzerschlüssel

1) Den Schlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Schlüssel und Anzeige von Detailinformationen siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*

   Abfragen des Schlüssels im lokalen PG und Anzeige der Detailinformationen siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

2) Register **Ereignisliste** auswählen.

   Wenn eine Ereignisliste von einem Remote-Programmiergerät angefordert und gelesen wurde, wird eine Liste der Ereignislisten-Ereignisse angezeigt.

3) Wenn die Funktion **Genehmigungen** aktiviert ist (siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*):

   a) Um eine neue Ereignisliste anzufordern, auf **Remote-Ereignisliste anfordern** klicken.

   b) Einen Kommentar für den Genehmigenden eingeben und auf **Anforderung senden** klicken.

4) Wenn die Funktion **Genehmigungen** deaktiviert ist (siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*):

   - Wenn der Schlüssel im lokalen PG ist, klicken Sie auf **Ereignisliste lesen**. Dies kann eine Weile dauern.
   - Wenn der Schlüssel nicht im lokalen PG ist, klicken Sie auf **Remote-Ereignisliste anfordern**.

     Die Ereignisliste wird beim nächsten Einstecken des Schlüssels in ein Remote-Programmiergerät eingelesen und in der CWM-Software gespeichert. Sie wird dann im Register Ereignisliste angezeigt.

     HINWEIS!

     Remote-Ereignisliste anfordern wird bei der Ausgabe des Schlüssels automatisch eingeschaltet und bei der Rückgabe automatisch ausgeschaltet.

5) Optional: Die Tabelle als PDF-Datei exportieren. Siehe *Abschnitt 4.11.5 "Exportieren von Ereignislisteninformationen", Seite 97*.

Siehe auch *Abschnitt 8.6 "Ereignislisten", Seite 190*.

4.11.2 Anzeigen von Ereignislisten für Zylinder

> **HINWEIS!**
> Die Zylinderereignislisten, die alle Zugangsversuche mit E1-Schlüsseln aufzeichnen, zeigen in der Spalte **Zeit im Schlüssel** nicht die Zeit an.

1) Den Zylinder suchen und die Detailansicht öffnen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Register **Ereignisliste** auswählen.

   Wenn bereits Ereignislisten erfasst wurden, werden diese in Form einer Liste angezeigt.

3) Um eine neue Ereignisliste anzufordern, auf **Ereignisliste anfordern** klicken.

   Wenn **Genehmigungen** aktiviert ist (siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*), Kommentar für den Genehmigenden eingeben.

4) **Priorität** auswählen.

   Dringende Jobs sollten höhere Priorität haben.

5) Auf **OK** klicken.

   Ein Programmier-Job zur Erfassung einer Ereignisliste vom Zylinder wird angelegt.

   Auslesen der Ereignisliste vom Zylinder siehe *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64*.

6) Optional: Die Tabelle als PDF-Datei exportieren. Siehe *Abschnitt 4.11.5 "Exportieren von Ereignislisteninformationen", Seite 97*.

Siehe auch *Abschnitt 8.6 "Ereignislisten", Seite 190*.

4.11.3 Anzeigen des Ereignislistenarchivs

Das Ereignislistenarchiv enthält alle von Schlüsseln und Zylindern der Schließanlage erfassten Ereignislisten. Durch Auswahl eines Schlüssels oder Zylinders können alle erfassten Ereignislisten für diesen Schlüssel oder Zylinder angezeigt werden.

Die Anzahl der Ereignislisten, die im Ereignislistenarchiv Platz finden, ist unbegrenzt. Das Archiv lässt sich so konfigurieren, dass automatisch Ereignislisten entfernt werden, die älter als eine festgelegte Anzahl von Tagen sind, siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

1) **Systeminfo » Ereignislistenarchiv** auswählen.

   Eine Ereignisliste wird angezeigt. Sie enthält die Interaktionen zwischen Schlüsseln, Zylindern, Programmierschlüsseln, Remote-Programmiergeräten und/oder der Software.

   > **HINWEIS!**
   > Aufgrund des großen Umfangs der Ereignislistendaten sind bestimmte erweiterte Informationen wie frühere Schlüsselhalter oder frühere Domänen mit einer Verzögerung verfügbar. Während diese Informationen im Hintergrund verarbeitet werden, wird **Daten werden verarbeitet** in der Liste angezeigt.

2) Suchkriterien eingeben und auf **Suchen** klicken.

So können Sie beispielsweise alle Schlüsselinteraktionen für einen bestimmten Zylinder anzeigen:

Wählen Sie **Schlüssel** unter **Erfasst von** aus und wählen Sie dann **Zylinder** aus und geben Sie **Name** oder **Org.-Nr.** des betreffenden Zylinders unter **Ereignis nach** an.

3) Optional: Die Tabelle als PDF-Datei exportieren. Siehe *Abschnitt 4.11.5 "Exportieren von Ereignislisteninformationen", Seite 97*.

4.11.4 Exportieren von Ereignislisteninformationen

1) Ereignislisten anzeigen:

   - Informationen über das Anzeigen der Ereignisliste für einen bestimmten Schlüssel finden Sie in *Abschnitt 4.11.2 "Anzeigen von Ereignislisten für Benutzerschlüssel", Seite 95*.
   - Informationen über das Anzeigen der Ereignisliste für einen bestimmten Zylinder finden Sie in *Abschnitt 4.11.3 "Anzeigen von Ereignislisten für Zylinder", Seite 96*.
   - Informationen zum Anzeigen des gesamten Ereignislistenarchivs finden Sie unter *Abschnitt 4.11.4 "Anzeigen des Ereignislistenarchivs", Seite 96*.

2) Klicken Sie auf **Vollständige Ereignisliste ausdrucken**, um die Tabelle zu drucken oder im PDF-Format zu speichern.

   Die Tabelle wird in einem Pop-up-Fenster angezeigt.

3) - Zum Speichern auf das Speichersymbol klicken und einen Ordner als Speicherort angeben.
   - Zum Drucken auf **...** klicken und **Ausdrucken** auswählen.

4.11.5 Genehmigung von Ereignislistenanforderungen

Wenn die Funktion **Genehmigungen** aktiviert ist, können Ereignislistenanforderungen erst nach ihrer Genehmigung ausgeführt werden. Um ausstehende Ereignislistenanforderungen genehmigen zu können, muss zur Anmeldung beim System ein Programmierschlüssel mit der Rolle „Genehmiger“ verwendet werden.

Informationen zum Ändern der Einstellung **Genehmigungen** finden Sie in *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

1) Programmierschlüssel mit Funktion "Genehmigender" in den linken Schlitz des lokalen PGs einführen.
2) Am System anmelden.

   Es stehen nur die Menüs **Arbeit** und **Einstellungen** zur Verfügung.

3) **Arbeit » Jobs zur Genehmigung** auswählen.

   Eine Liste mit Jobs, die auf Genehmigung warten, wird angezeigt.

4) Auf **Antworten** klicken.
5) Genehmigen: Optionalen Kommentar eingeben und auf **Genehmigen** klicken.

   Ablehnen: Optionalen Kommentar eingeben und auf **Ablehnen** klicken.

Zur Anzeige bereits genehmigter oder abgelehnter Jobs das Register **Genehmigungshistorie** auswählen.

5 Einrichten von Schließanlagen

5.1 Einrichten einer Schließanlage - Überblick

Im folgenden Überblick wird der Arbeitsablauf zum erstmaligen Einrichten einer Schließanlage beschrieben.

Voraussetzungen:

- Datenbank vorbereitet und Serversoftware auf dem CWM-Server installiert.
- Bei einem Remote-System: Datenbank vorbereitet und Serversoftware auch auf dem Remote Server installiert.
- Firewalls und Proxyserver für SSL-Datenverkehr konfiguriert.
  - Von den Client-PCs zum CWM-Server (Ports 443 und 8443).
  - Von den Remote-PGs zum Remote-Server (Port 443).
  - Vom CWM-Server zum SMTP-Server (Port 25).

1) CWM-Client einrichten.

   Siehe *Abschnitt 2.1 "Einrichtung von CWM-Clients - Überblick", Seite 13*.

2) Zertifikat für Hauptprogrammierschlüssel installieren.

   Siehe *Abschnitt 5.2 "Installieren des Zertifikats für den Hauptprogrammierschlüssel", Seite 98*.

3) Login bei CWM durchführen.

   Siehe *Abschnitt 5.3 "Anmelden bei einer neuen Schließanlage", Seite 99*.

4) Gewünschte Sprache für die CWM-Software wählen.

   Siehe *Abschnitt 3.4 "Einstellen der CWM-Sprache", Seite 19*.

5) Lizenz installieren.

   Siehe *Abschnitt 6.1.1 "Installieren von Lizenzen", Seite 101*.

6) Erstkonfiguration durchführen.

   Siehe *Abschnitt 5.4 "Durchführen der Erstkonfiguration", Seite 100*.

5.2 Installieren des Zertifikats für den Hauptprogrammierschlüssel

Wenn DCS-Integration aktiviert ist:

In DCS ist die E-Mail-Adresse des Hauptprogrammierschlüsselhalters angegeben. Innerhalb einer Stunde nach Vorbereitung der Datenbank der Schließanlage wird eine E-Mail an diese E-Mail-Adresse versandt.

Wie oft ein Zertifikat für einen Hauptprogrammierschlüssel erstellt werden kann, wird durch eine Einstellung in DCS festgelegt.

Das Zertifikat für den Hauptprogrammierschlüssel wird auf dieselbe Weise installiert wie ein Programmierschlüssel-Zertifikat. Weitere Informationen siehe *Abschnitt 3.2.1 "Registrierung des Zertifikats für den Programmierschlüssel über CLIQ Connect PC", Seite 17*.

Wenn DCS-Integration nicht aktiviert ist:

Das Zertifikat für den Hauptprogrammierschlüssel wurde bereits bereitgestellt. Für weitere Informationen zur Installation des Zertifikats siehe *Abschnitt 3.2.2 "Manuelle Installation des Programmierschlüssel-Zertifikats", Seite 17*.

5.3 Anmelden bei einer neuen Schließanlage

Voraussetzungen:

- Das lokale PG ist installiert. Siehe *Abschnitt 2.2 "Installieren lokaler PGs", Seite 13*.
- Ein unterstützter Internet-Browser wird verwendet. Siehe *Abschnitt 9.8 "Voraussetzungen für Client-PC", Seite 216*.
- CLIQ Connect PC ist auf dem Computer installiert und wird ausgeführt.

  Siehe *Abschnitt 2.3 "Installation von CLIQ Connect PC", Seite 13*.
- CLIQ Connect PC ist konfiguriert und mit CWM verbunden.

  Siehe *Abschnitt 2.4 "Konfigurieren von CLIQ Connect PC", Seite 14*.
- Der Hauptprogrammierschlüssel samt PIN-Code steht zur Verfügung.
- Ein gültiges Zertifikat für den Hauptprogrammierschlüssel ist installiert. Siehe *Abschnitt 5.2 "Installieren des Zertifikats für den Hauptprogrammierschlüssel", Seite 98*.
- Die URL zu CWM ist verfügbar.

1) Programmierschlüssel in den linken Schlitz des lokalen PGs einführen.
2) Zur CWM-Startseite navigieren.
3) Das Zertifikat für den Programmierschlüssel auswählen.

   Die CWM-Anmeldeseite wird angezeigt.
4) Auf **Anmelden** klicken.
5) PIN-Code für den Programmierschlüssel eingeben.

   CLIQ Connect PC bittet um Bestätigung der Verwendung des Schlüssels.
6) Auf **Bestätigen** klicken.
7) Wählen Sie **Basiszeitzone** in der Dropdown-Liste aus.

   HINWEIS!
   Diese Einstellung kann nach dem Klicken auf **Bestätigen** nicht mehr geändert werden.

8) Wählen Sie für **Genehmigung von Anfragen von Ereignislisten** aus den folgenden Optionen aus:

   - **Deaktiviert**

     Wenn dies ausgewählt ist, können alle Administratoren Ereignislisten anfordern, ohne eine Genehmigung von einem anderen Administrator zu benötigen.
   - **Aktiviert**

     Wenn dies ausgewählt ist, benötigen alle Administratoren zum Anfordern von Ereignislisten die Genehmigung eines anderen Administrators.

   Für weitere Details zur Genehmigerrolle für Ereignislisten siehe *Abschnitt 4.11.6 "Genehmigung von Ereignislistenanforderungen", Seite 97*.
9) Auf **Erweiterungsimport aktivieren** klicken.

Das Fenster **Bestätigung** wird geöffnet.

10) Überprüfen Sie sorgfältig die Einstellungen.

> **WARNUNG!**
> Die Einstellungen können später nicht geändert werden.

11) Auf **Bestätigen** klicken.

5.4 Durchführen der Erstkonfiguration

1) Schließanlage entriegeln. Siehe *Abschnitt 6.3 "Entsperren des Systems", Seite 102*.
2) Systemeinstellungen bearbeiten. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.
3) Remote-PGs einrichten. Siehe *Abschnitt 6.5.1 "Einrichten von Remote-PGs", Seite 107*.
4) Domänen anlegen. Siehe *Abschnitt 6.6.4 "Anlegen und Löschen von Domänen", Seite 128*.
5) Domäne für Zylinder und Zylindergruppen angeben. Siehe *Abschnitt 6.6.7 "Ändern der Domäne für Zylinder", Seite 129* und *Abschnitt 6.6.8 "Ändern der Domäne für Zylindergruppen", Seite 130*.
6) Zugangsprofile einrichten. Siehe *Abschnitt 4.6.2 "Anlegen und Löschen von Zugangsprofilen", Seite 71*.
7) Quittungsvorlagen für die Ausgabe und Rücknahme von Schlüsseln anlegen. *Abschnitt 6.9 "Verwalten von Quittungsvorlagen", Seite 134*.
8) Vorlagen für Zeitpläne anlegen. Siehe *Abschnitt 6.10 "Verwalten von Zeitplanvorlagen", Seite 136*.
9) Administatorrollen hinzufügen und löschen und die den Rollen zugeordneten Rechte wie gewünscht einstellen. Siehe *Abschnitt 6.7 "Verwalten von Rollen und Rechten", Seite 131*.
10) Programmierschlüssel an die Administratoren der Schließanlage aushändigen. Siehe *Abschnitt 6.11.7 "Ausgeben von Programmierschlüsseln", Seite 141*.
11) Mitarbeiterinformationen in CWM importieren. Siehe *Abschnitt 6.8 "Importieren von Mitarbeiterinformationen", Seite 133*.

6 Konfigurieren von Schließanlagen

6.1 Verwalten von Lizenzen

6.1.1 Installieren von Lizenzen

Voraussetzungen:

- Eine neue Lizenzdatei steht zur Verfügung.
  - Bei manueller Installation: auf einem USB-Speicherstick oder auf der Festplatte des Computers gespeichert.
  - Bei automatischem Abrufen in Systemen mit DCS-Integration: In DCS gespeichert.
- Die Lizenznummer der neuen Lizenzdatei ist höher als die der installierten Lizenz. Eine ältere Lizenz kann nicht installiert werden.

1) **Verwaltung » Lizenz** auswählen.

   Es werden Informationen zur aktuell installierten Lizenz (sowie die enthaltenen Eigenschaften) angezeigt.
2) Bei Systemen mit DCS-Integration und bei Speicherung der Lizenzdatei in DCS:

   Auf **Lizenz holen** klicken.

   Die Lizenz wird heruntergeladen und installiert.
3) Bei Systemen ohne DCS-Integration oder wenn die Lizenzdatei nicht in DCS zur Verfügung steht:
   a) Auf **Auswählen...** klicken.
   b) Lizenzdatei auswählen.
   c) Auf **Hochladen** klicken.

      Die Lizenz wird hochgeladen und installiert.

6.1.2 Lizenzstatus anzeigen

1) **Verwaltung » Lizenz** auswählen.

   Es werden Informationen zur aktuell installierten Lizenz (sowie die enthaltenen Eigenschaften) angezeigt.

Installation einer neuen Lizenz siehe *Abschnitt 6.1.1 "Installieren von Lizenzen", Seite 101*.

6.2 Sperren des Systems zur Wartung

Eine Schließanlage kann zur Durchführung von Wartungsmaßnahmen gesperrt werden.

1) **Verwaltung » Wartung** auswählen.
2) Datum und Zeit auswählen, zu denen das entsprechende System zu Wartungszwecken gesperrt werden soll.

   Die ausgewählte Zeit muss mindestens 10 Minuten in der Zukunft liegen.
3) Auf **Schließanlage sperren** klicken.

6.3 Entsperren des Systems

1) **Verwaltung » Wartung** auswählen.
2) Auf **Schließanlage entsperren** klicken.

6.4 Bearbeiten der Systemeinstellungen

Einige der hier beschriebenen Systemeinstellungen gelten nur für ein Remote-System.

1) **Verwaltung » Systemeinstellungen** auswählen.

   Die gewählten Systemeinstellungen werden angezeigt.
2) Zum Bearbeiten der Systemeinstellungen auf **Bearbeiten** klicken.
3) Die erforderlichen Einstellungen aktualisieren:

SYSTEM

- **Genehmigungen**. Falls dies aktiviert ist, müssen Ereignislistenanforderungen für Zylinder und Schlüssel genehmigt werden, bevor Ereignislisten abgerufen werden können.

  HINWEIS!
  Einschränkungen:
  - Angemeldet mit dem Hauptprogrammierschlüssel.
  - Zum Deaktivieren der Genehmigungsfunktion zunächst sicherstellen, dass alle ausstehenden Ereignislistenjobs abgebrochen oder abgeschlossen sind.
  - Zum Aktivieren der Genehmigungsfunktion zunächst sicherstellen, dass **AUTOMATISCHER EREIGNISLISTENABRUF** in allen Programmierschlüsseln deaktiviert ist. Siehe *Abschnitt 6.11.13 "Automatischen Ereignislistenabruf für Programmierschlüssel aktivieren oder deaktivieren", Seite 146*.

    Vorhandene ausstehende Jobs bleiben von der Aktivierung der Genehmigungsfunktion unberührt und müssen nicht genehmigt werden. Nur neue Ereignislistenjobs müssen genehmigt werden.

- **CLIQ Remote System** zeigt an, ob die Remote-Funktionalität aktiviert ist.

  Dies kann nur beim erstmaligen Einstellen der Schließanlage gewählt werden.
- **Unterstützt Zylindergruppen** zeigt an, ob die Verwendung von Zylindergruppen aktiviert ist.

  Dies kann nur beim erstmaligen Einstellen der Schließanlage gewählt werden.
- **Basiszeitzone**. Für die verschiedenen Ausdrucke in der Anwendung verwendete Zeitzone.

  Dies kann nur beim erstmaligen Einstellen der Schließanlage gewählt werden.

- **Integrierung von Web Services** ermöglicht die Kommunikation mit anderen Systemen, z. B. HR-Systemen.
- **Benutzer-Benachrichtigung** ermöglicht CWM das Versenden von E-Mails an Mitarbeiter und Besucher, z. B. zur Erinnerung an überfällige Schlüssel.

  – **E-Mails nach Remote-Update** steuert, ob nach einem Remote-Update eine E-Mail mit den neuen Berechtigungsdaten an die Schlüsselhalter gesendet wird.

    Das Kontrollkästchen aktivieren und auf **Konfigurieren** klicken, um auszuwählen, ob mechanische Zylinder in die E-Mail einbezogen werden sollen.

  – **E-Mails nach Änderung von Mitarbeiterdaten** steuert, ob eine E-Mail mit einer Liste der an den Mitarbeiterinformationen vorgenommenen Änderungen an den Administrator der Domänen gesendet wird, in denen der Schlüssel des Mitarbeiters eine vorhandene oder ausstehende Berechtigung für mindestens einen Zylinder hat.

    Das Kontrollkästchen aktivieren und auf **Konfigurieren** klicken, um auszuwählen, welche Art von Änderungen zu einer Benachrichtigung führen.

  – **E-Mails nach Änderung von Besucherdaten** steuert, ob eine E-Mail mit einer Liste der an den Besucherinformationen vorgenommenen Änderungen an den Administrator der Domänen gesendet wird, in denen der Schlüssel des Besuchers eine vorhandene oder ausstehende Berechtigung für mindestens einen Zylinder hat.

    Das Kontrollkästchen aktivieren und auf **Konfigurieren** klicken, um auszuwählen, welche Art von Änderungen zu einer Benachrichtigung führen.

  – **E-Mails nach Wechsel von Wand-Programmiergerät in Offline-Status** steuert, ob eine E-Mail an die angegebene Person gesendet wird, wenn ein Wand-Programmiergerät in den Offline-Status wechselt.

    Das Kontrollkästchen aktivieren und auf **Konfigurieren** klicken, um den E-Mail-Empfänger anzugeben und die Anzahl der aufeinanderfolgenden fehlenden Herzschläge einzustellen, nach der eine Benachrichtigung versandt wird.
- **Flexible Verlängerung** ermöglicht das Einstellen des Verlängerungsintervalls je Berechtigungsprofil und je Zylindergruppe.
- **Verlorene Schlüssel während Autorisierungs-Update automatisch im Zylinder sperren**

  Aktivieren Sie das Kontrollkästchen, um zuzulassen, dass das System verlorene Schlüssel automatisch zur Liste der nicht autorisierten Schlüssel hinzufügt, sodass die Schlüssel in den Zylindern gesperrt werden.
- Mit **Verlorene Schlüssel mit Benutzerschlüsseln sperren** können Sie einen Zylindersperrjobs für einen beliebigen Benutzerschlüssel (E3-Schlüssel) programmieren, um einen verlorenen Schlüssel in den Zylindern zu sperren.

  Dies gilt nur für ein Remote-System.

- **Verlorene Schlüssel in neuen Zylindern während des Erweiterungsimports blockieren**: Beim Hinzufügen von Zylindern zu einer Anlage müssen eventuell zuvor als verloren gemeldete Schlüssel in den neuen Zylindern gesperrt werden. Wenn diese Einstellung aktiviert ist, erstellt CWM automatisch Zylinderprogrammierjobs, um die verlorenen Schlüssel beim Aktivieren der Importdatei zu sperren.
- **Hierarchische Administratoren** (können nur von Super-Administratoren bearbeitet werden)

  Aktivieren Sie die Administratorenhierarchie-Funktion durch Aktivieren des Kontrollkästchens, sodass die Benutzer zwischen einer flachen und einer hierarchischen Struktur für Berechtigungen wählen können.

CLIQ REMOTE

- **Service-URL**. Von CWM und Remote-Programmiergeräten verwendeter Remote-Server. Hinweis: Wenn die URL nicht dem Hostnamen entspricht, der im Zertifikat des Remote-Servers festgelegt wurde, wird eine Warnung angezeigt.
- **Alternative Service-URL**: Option zur Festlegung einer alternativen Service-URL zum Remoteserver, die von CWM und Remote-Programmiergeräten verwendet wird. Die URL ist nur dann auf der Registerkarte **Einstellungen** der Ansicht der Remote-Programmiergeräts zu sehen, wenn die Firmwareversion des Wand-Programmiergeräts bzw. des mobilen CLIQ-Programmiergeräts mindestens die Version 4.0 ist. Beachten, dass die **Alternative Service-URL** den gleichen Remote-Server anspricht wie die **Service-URL**.
- **Server-CA-Zertifikat**. Zertifikat der Certificate Authority (CA), die das Serverzertifikat auf dem CLIQ-Remote-Server herausgibt. Der Import des Zertifikats erfordert Super-Administrator-Rechte.

STANDARD-SCHLÜSSELEINSTELLUNGEN

- **Verlängerung bei Ausgabe aktivieren**. Bei Auswahl ist die Verlängerungsoption im Arbeitsablauf für die Schlüsselausgabe verfügbar.
- **Verlängerungsintervall**. Standardeinstellung für das Schlüssel-Verlängerungsintervall.
- **PIN-Validierung bei Ausgabe aktivieren**. Bei Auswahl ist die PIN-Validierungsoption im Arbeitsablauf für die Schlüsselausgabe verfügbar.
- **PIN-Validierungsintervall**. Standardeinstellung für das PIN-Validierungsintervall.
- **Zeit bis Rückgabe**. Standardeinstellung für die Zeit bis zur Rückgabe des Schlüssels, gerechnet ab dem Ausgabedatum. Wenn keine Endzeit angegeben werden soll, `0` eingeben.
- **Gültigkeitseinstellung**. Die Standardeinstellung für die Gültigkeit von Schlüsseln.
- **Gültigkeitsdauer**. Standardeinstellung für die Länge der Schlüsselgültigkeitsdauer bei Auswahl der Gültigkeitsoption **Aktiv im festgelegten Zeitraum**.

VERWALTUNG

- **Standardwert in Tagen für die Suche nach überfälligen Schlüsseln**. Standard-Suchoption für überfällige Schlüssel.
- **Sprache der Benutzer-Benachrichtigung**. Die Sprache, die von CWM für den Versand von E-Mails verwendet wird, z. B. bei überfälligen Schlüsseln.
- **Schlüsselquittungen** legt fest, ob Quittungen für Schlüsselaus- und -rückgabe separat oder gemeinsam gedruckt werden sollen.
- **Externe Links Root-URL**. Eine Root-URL, die zur Bildung externer Links für Schlüssel, Mitarbeiter usw. verwendet wird.
- **CSV-Trennzeichen**. Beim Exportieren von CSV-Dateien wird Semikolon oder Komma als Trennzeichen zwischen den Daten gewählt.
- **Ereignislisten und Ereignisse**. Ereignislisten und Ereignisse, die älter als die festgelegte Anzahl an Tagen sind, werden automatisch aus dem Archiv der Ereignislisten und Ereignisse entfernt. Die Tage werden ab dem Datum gezählt, an dem die Ereignislisten und Ereignisse erfasst wurden.

  Standardmäßig kann der Aufbewahrungszeitraum für Ereignislisten und Ereignisse auf einen Wert zwischen 1 und 366 Tagen festgelegt werden. Mit einer Zusatzlizenz ist ein Zeitraum bis 3660 Tage möglich.

  Ab CWM 11.6 folgt die Löschung dem Erstellungsdatum, d. h. dem Zeitpunkt, an dem der Eintrag auf dem physischen Element erzeugt wurde. Dies ersetzt die frühere Methode, bei der das Analysedatum verwendet wurde, also das Datum, an dem der Eintrag in der CWM-Datenbank gespeichert wurde.
- **Beim Löschen von Personen**. Bei der Einstellung **Als gelöscht kennzeichnen** wird der Status einer gelöschten Person in „gelöscht“ geändert, alle Informationen bleiben jedoch in der Datenbank erhalten. Bei Einstellung **Dauerhaft löschen** (Standardeinstellung für neue Schließanlagen) werden beim Löschen einer Person auch sämtliche zugehörigen Informationen aus der Datenbank gelöscht. Mit der Einstellung **Dauerhaft löschen** wird die DSGVO eingehalten und das Deaktivieren einer Person ermöglicht. Weitere Informationen siehe *Abschnitt 8.9 "Löschen von Personendaten und DSGVO-Erfüllung", Seite 194*.

  Wird die Einstellung von **Als gelöscht kennzeichnen** in **Dauerhaft löschen** geändert, werden alle als gelöscht markierten Personen dauerhaft gelöscht.

  Um die Einstellung von **Dauerhaft löschen** in **Als gelöscht kennzeichnen** ändern zu können, müssen zuerst alle deaktivierten Personen aktiviert werden.
- **Letztes Anmeldedatum erfassen** gibt an, ob das letzte Anmeldedatum für ein Programmierschlüsselzertifikat erfasst werden soll. Wenn die Option aktiviert ist, wird das **Datum der letzten Nutzung** auf der Registerkarte **Zertifikate** in der Detailansicht des Programmierschlüssels angezeigt. Siehe *Abschnitt 6.11.14 "Auflisten von Programmierschlüssel-Zertifikaten", Seite 146*.
- **Benutzerdefinierte Felder Zylinder** bietet die Möglichkeit, benutzerdefinierte Felder zum Speichern zusätzlicher Zylinderinformationen in CWM zu definieren, hinzuzufügen oder zu bearbeiten. Die Werte der benutzerdefinierten Felder lassen sich in den Zylinder-Detailansichten der jeweiligen Zylinder bearbeiten. Sie lassen sich

auch dazu verwenden, Zylinder über die erweiterte Zylindersuche zu ermitteln.

- **Anfängliche Zylinderdomäne** legt die zugeordnete Domäne für neue oder importierte Zylinder fest.
- **Anfängliche Personendomäne** legt die zugeordnete Domäne für neue oder importierte Mitarbeiter oder Besucher fest.
- **Anfängliche Schlüsseldomäne** legt die zugeordnete Domäne für neue oder importierte Schlüssel fest.

NETZWERKAUTHENTIFIZIERUNG FÜR WAND-PROGRAMMIERGERÄT GENERATION 2

- **802.1x-Authentifizierung**

  Bei im System aktivierter Netzwerkauthentifizierung für Wand-Programmiergeräte kann auf Systemeinstellungsebene nicht **Deaktiviert** ausgewählt werden. Klicken Sie auf **Wie kann ich die Authentifizierung deaktivieren?** und rufen Sie die Liste der Wand-Programmiergeräte mit aktivierter Netzwerkauthentifizierung ab. Informationen zum Deaktivieren der Netzwerkauthentifizierung auf Geräteebene finden Sie unter *Abschnitt 6.5.7.1 "Einstellungen von Wand-Programmiergeräten bearbeiten", Seite 112*.

- **Serverhostname für 802.1x-Authentifizierung**

  Geben Sie den Hostnamen des Servers ein.

- **802.1x-Server-CA-Zertifikat**

  Alle Zertifikate sind hier aufgeführt. Wenn ein Zertifikat ungültig ist, wird unter dem Zertifikat eine Meldung angezeigt.

  Es können bis zu 3 Zertifikate im PEM-Format hochgeladen werden.

  So laden Sie ein CA-Zertifikat hoch:

  a) Klicken Sie auf **Neues auswählen...** und wählen Sie ein CA-Zertifikat (`. pem`) aus.

  b) Auf **Zertifikat hochladen** klicken.

  Das CA-Zertifikat wird angezeigt.

LDAP-INTEGRATION

- **Aktiviert**. Wenn dies aktiviert ist, ist die Option der LDAP-Integration verfügbar.
- **LDAP-Servertyp**. Wählen Sie den LDAP-Servertyp in der Dropdown-Liste aus.
- **Verbindungstyp**. Wählen Sie **START TLS** oder **LDAPS** aus.
- **LDAP-Host**. Geben Sie die Adresse zum LDAP-Server im Netzwerk an.
- **LDAP-Port**. Geben Sie den erforderlichen Port für den Zugriff auf den LDAP-Server ein.
- **DN-Benutzer** ist der LDAP-Administrator, der Zugriff auf den Basis-DN hat.

- **Passwort** ist das Passwort des Administrators.
- **Basis-DN** legt den Stamm für Suchen im Active Directory-Verzeichnis fest.
- **Suchfilter** legt Suchkriterien für effizientere Suchen fest.

SINGLE SIGN-ON (SSO)

- **SAML aktiviert**. Durch Aktivieren dieser Option wird die SSO-Anmeldeoption verfügbar. Weitere Informationen über SSO finden Sie in *Abschnitt 8.10 "Single Sign-on (SSO)", Seite 195*.
- **SAML-Konfiguration beim Speichern neu laden**: Wenn eine bereits vorhandene SAML-Konfiguration in der Datenbank geändert wird und diese Option aktiviert ist, wird die Konfiguration beim Klicken auf die Schaltfläche **Speichern** auf dieser Seite neu geladen. Nach dem Speichern wird die Schaltfläche **Verifizierungszertifikat herunterladen** angezeigt.
- **Verifizierungszertifikat neu erstellen**: Wenn für die Anlage bereits eine SAML-Konfiguration vorhanden ist und diese Option aktiviert ist, wird beim Klicken auf die Schaltfläche **Speichern** auf dieser Seite das Zertifikat erstellt. Dies kann notwendig sein, wenn sich das Zertifikat geändert hat oder abgelaufen ist. Nach dem Speichern wird die Schaltfläche **Verifizierungszertifikat herunterladen** angezeigt. Das Zertifikat herunterladen und zum Identitätsanbieterdienst hochladen.

CLIQ CONNECT+

- **Zugängliche Zylinder zeigen**. Wenn dies ausgewählt ist, können Benutzer von CLIQ Connect+ in CLIQ Connect+ sehen, welche Zylinder mit ihrem Schlüssel zugänglich sind.
- **Mechanische Zylinder einbeziehen**. Wenn dies ausgewählt ist, werden in der Liste der zugänglichen Zylinder in CLIQ Connect+ auch die mechanischen Zylinder angezeigt, die dem Schlüsselhalter zugewiesen sind.
- **Zugangsprofile zeigen**. Wenn dies ausgewählt ist, ist in CLIQ Connect+ die Liste der dem Schlüssel zugewiesenen Zugangsprofile sichtbar.

  Zur Aktivierung dieser Funktion muss der Benutzer in der Rolle **Schlüssel: Berechtigung** mindestens die Berechtigungsstufe **Anzeige** haben. Zum Wechsel der Berechtigungsebene siehe *Abschnitt 6.7 "Verwalten von Rollen und Rechten", Seite 131*.

6.5 Verwalten von Remote-PGs

6.5.1 Einrichten von Remote-PGs

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Informationen, Tags und externe Links zum Remote-Programmiergerät wie gewünscht bearbeiten.

   Siehe *Abschnitt 6.5.3 "Bearbeiten von Informationen zum Remote-Programmiergerät", Seite 109*,*Abschnitt 6.5.5 "Tags für Remote-Programmiergeräte hinzufügen oder entfernen", Seite 110* und *Abschnitt 6.5.6 "Externe Links von Remote-Programmiergeräten verwalten", Seite 111*.

3) Einstellungen des Remote-Programmiergeräts bearbeiten und die Konfiguration in das Remote-Programmiergerät laden. Dies beinhaltet die Installation des Zertifikats.

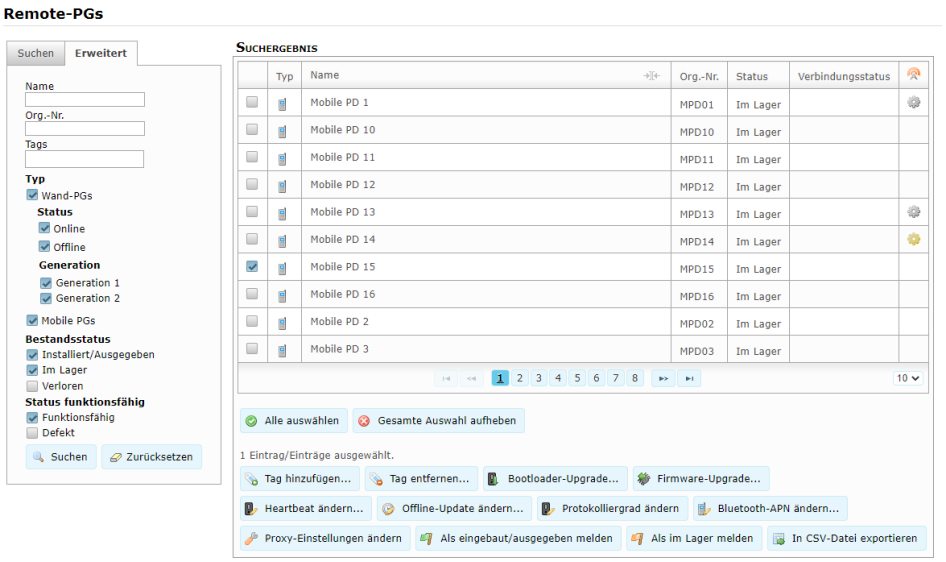
   Wand-PGs siehe *Abschnitt 6.5.7 "Konfigurieren von Wand-Programmiergeräten", Seite 112*.

   Mobile CLIQ-Programmiergeräte siehe *Abschnitt 6.5.8.1 "Einstellungen von mobilen CLIQ-Programmiergeräten bearbeiten", Seite 119*.

6.5.2 Suchen nach Remote-PGs

1) **Systeminfo » Remote-PGs** auswählen.

   Suchergebnis zeigt eine Liste mit Remote-PGs.



   Folgende Symbole werden verwendet:

   Wand-Programmiergerät

   Mobiles CLIQ-Programmiergerät

> **HINWEIS!**
> Mobile CLIQ Connect-Programmiergeräte sind in der Liste nicht enthalten.

2) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

   Um die Suchergebnisliste nach Typ des Remote-Programmiergeräts zu filtern, eines der Kontrollkästchen **Wand-PGs** oder **Mobile PGs** auf der Suchregisterkarte **Erweitert** aktivieren.

   Wand-PGs lassen sich nach Status, **Online** oder **Offline** filtern.

3) Auf **Suchen** klicken.

4) Zur Anzeige von Detailinformationen auf das entsprechende Remote-Programmiergerät klicken.

Es lassen sich mehrere Remote-PGs gleichzeitig konfigurieren. Die Remote-PGs in der Liste der Suchergebnisse auswählen und auf eine der Schaltflächen klicken, um die jeweiligen Einstellungen zu ändern.

6.5.3 Bearbeiten von Informationen zum Remote-Programmiergerät

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Auf **Bearbeiten** klicken.
3) Zum Bearbeiten des Namens des Remote-Programmiergeräts die Eingabe im Feld **Name** ändern.
4) Um Tags hinzuzufügen, auf **Tag hinzufügen...** klicken. Siehe auch *Abschnitt 6.5.5 "Tags für Remote-Programmiergeräte hinzufügen oder entfernen", Seite 110*.
5) Um externe Links hinzuzufügen und zu bearbeiten, auf **Externen Link hinzufügen...** klicken. Siehe auch *Abschnitt 6.5.6 "Externe Links von Remote-Programmiergeräten verwalten", Seite 111*.
6) Auf **Speichern** klicken.

6.5.4 Status des Remote-Programmiergeräts ändern

Remote-PGs haben einen Bestandsstatus, der entweder "Im Lager", "Ausgegeben" oder "Verloren" lauten kann, sowie einen Funktionsstatus, der entweder "Funktionsfähig" oder "Defekt" lauten kann.

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) **Status des Wand-Programmiergeräts ändern**

   - Als **Installiert** melden
     - In der Detailansicht auf **Als Eingebaut melden** und dann auf **OK** klicken.
     - Wenn mehrere Geräte gemeldet werden sollen, in den Suchergebnissen die Wand-Programmiergeräte auswählen. Auf **Als eingebaut/ausgegeben melden** und dann auf **OK** klicken.
   - Als **Im Lager** melden
     - In der Detailansicht auf **Als im Lager melden** und dann auf **OK** klicken.
     - Wenn mehrere Geräte gemeldet werden sollen, in den Suchergebnissen die Wand-Programmiergeräte auswählen. Auf **Als im Lager melden** und dann auf **OK** klicken.
   - Als **Verloren** melden
     - In der Detailansicht auf **Als verloren melden** und dann auf **OK** klicken.
   - Als **Gefunden** melden
     - In der Detailansicht auf **Als gefunden melden** und dann auf **OK** klicken.

- Als **Defekt** melden
  - In der Detailansicht auf **Als defekt melden** und dann auf **OK** klicken.
- Als **Funktionsfähig** melden
  - In der Detailansicht auf **Als funktionsfähig melden** und dann auf **OK** klicken.

3) **Status des mobilen CLIQ-Programmiergeräts ändern**

- Als **Ausgegeben** melden
  - In der Detailansicht auf **Ausgabe** und dann auf **OK** klicken.
  - Wenn mehrere Geräte gemeldet werden sollen, in den Suchergebnissen die Wand-Programmiergeräte auswählen. Auf **Als eingebaut/ausgegeben melden** und dann auf **OK** klicken.
- Als **Im Lager** melden
  - In der Detailansicht auf **Rückgabe** und dann auf **OK** klicken.
  - Wenn mehrere Geräte gemeldet werden sollen, in den Suchergebnissen die Wand-Programmiergeräte auswählen. Auf **Als im Lager melden** und dann auf **OK** klicken.
- Als **Verloren** melden
  - In der Detailansicht auf **Als verloren melden** und dann auf **OK** klicken.
- Als **Gefunden** melden
  - In der Detailansicht auf **Als gefunden melden** und dann auf **OK** klicken.
- Als **Defekt** melden
  - In der Detailansicht auf **Als defekt melden** und dann auf **OK** klicken.
- Als **Funktionsfähig** melden
  - In der Detailansicht auf **Als funktionsfähig melden** und dann auf **OK** klicken.

6.5.5 Tags für Remote-Programmiergeräte hinzufügen oder entfernen

1) **Systeminfo » Remote-PGs** auswählen.

   Eine Liste aller Remote-Programmiergeräte wird angezeigt.

   - Um Tags für einzelne Remote-Programmiergeräte hinzuzufügen oder zu entfernen, gehen Sie zu *Schritt 2*.
   - Um Tags für mehrere Remote-Programmiergeräte gleichzeitig hinzuzufügen oder zu entfernen, gehen Sie zu *Schritt 3*.

2) **Tags für ein einzelnes Remote-Programmiergerät hinzufügen oder entfernen:**

   1. Das Remote-Programmiergerät auswählen und seine Detailansicht öffnen.
   2. Auf **Bearbeiten** klicken.

3. Ein Tag für ein einzelnes Remote-Programmiergerät hinzufügen oder entfernen.

   Tag hinzufügen:

   a) Auf **Tag hinzufügen...** klicken.
   b) Namen für den Tag eingeben.
   c) Auf **OK** klicken.

   Tag löschen:
   Auf den zu entfernenden Tag klicken.

4. Auf **Speichern** klicken.

3) **Tags für mehrere Remote-Programmiergeräte hinzufügen oder entfernen:**

1. Remote-Programmiergeräte durch Aktivieren der Kontrollkästchen in den Suchergebnissen auswählen.
2. **Tag hinzufügen:**

   a) Auf **Tag hinzufügen...** klicken.
   b) Einen Namen für das Tag eingeben.
   c) Auf **OK** klicken.

   Tag löschen:

   a) Auf **Tag entfernen...** klicken.
   b) Einen Namen für das Tag eingeben.
   c) Auf **OK** klicken.

Siehe auch *Abschnitt 8.2.6 "Tags", Seite 184*.

6.5.6 Externe Links von Remote-Programmiergeräten verwalten

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Auf **Bearbeiten** klicken.
3) **Einen externen Link hinzufügen:**

1. Auf **Hinzufügen.** klicken
2. **Name** für die URL eingeben.
3. **URL** eingeben. Die **URL** muss mit einem Protokoll beginnen (z. B. http:// oder ftp://).

   Wenn in den **Systemeinstellungen** (Eintrag **Externe Links Root-URL**) eine Root-URL festgelegt wurde, muss nur der letzte Teil der URL eingegeben werden. Siehe auch *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

4. Auf **OK** klicken.

Externen Link bearbeiten:

1. Beim zu bearbeitenden externen Link auf **Bearbeiten** klicken.
2. Die Felder ändern.
3. Auf **OK** klicken.

Einen externen Link entfernen:
Beim zu entfernenden externen Link auf **Entfernen** klicken.

4) Auf **Speichern** klicken.

Siehe auch *Abschnitt 8.4 "Externe Links", Seite 187*.

6.5.7 Verwalten von Einstellungen und Zertifikaten von Wand-Programmiergeräten

Voraussetzungen:

- Für ein Wand-Programmiergerät, das erstmalig mit deaktiviertem **Plug-and-Play** konfiguriert wird oder mit den aktuellen Einstellungen keine Verbindung herstellen kann:
  - Ein USB-Kabel:
    - **Wand-Programmiergerät Generation 1:** Kabel vom Typ USB On-The-Go (OTG) mit USB-Mini-Stecker (Typen A und B unterstützt) und USB-Standard-Buchse (Typ A).

    - **Wand-Programmiergerät Generation 2:** Kabel mit USB-C-Stecker und USB-Standard-Buchse (Typ A).
  - Ein USB-Speicherstick:
    - **Wand-Programmiergerät Generation 1:** im FAT32-Dateisystemformat formatiert. Empfohlene Speichergröße 8-16 GB.
    - **Wand-Programmiergerät Generation 2:** im FAT32-Dateisystemformat formatiert. Die Größe des USB-Speichersticks ist nicht beschränkt. Verwenden Sie einen Standard-USB-C-Speicherstick oder schließen Sie ein USB-A-Speicherstick mit einem Standardadapter oder -kabel an.
- Verwendung des Offline-Updates:
  - Ein Wand-Programmiergerät Generation 1 mit Firmware 2.11 oder höher oder ein Wand-Programmiergerät Generation 2.
- Installieren oder Erneuern von Zertifikaten **ohne** DCS-Integration:
  - Eine .p12-Zertifikatdatei. Erhältlich beim lokalen CLIQ-Händler.

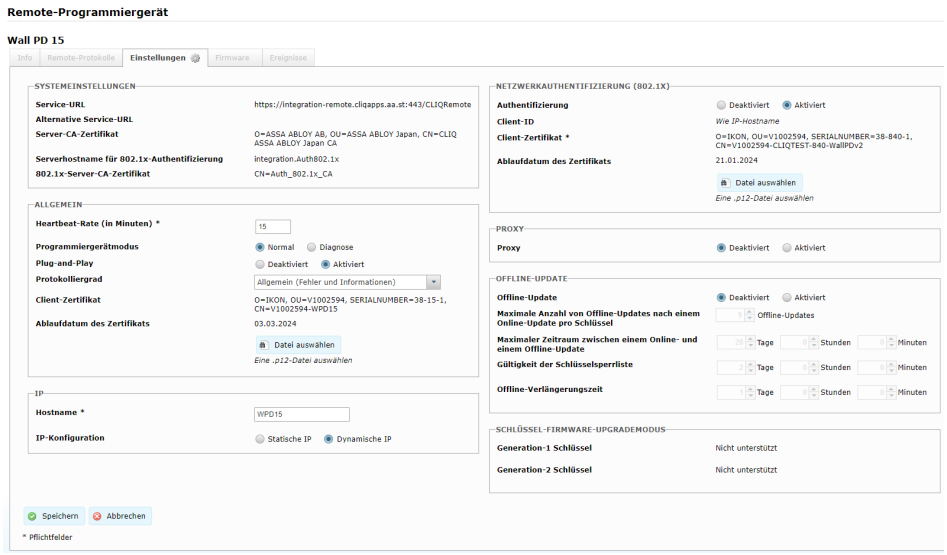
6.5.7.1 Einstellungen von Wand-Programmiergeräten bearbeiten

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Register **Einstellungen** auswählen.

3) Auf **Bearbeiten** klicken.



4) Die erforderlichen Einstellungen aktualisieren:

ALLGEMEIN

- **Heartbeat-Rate (in Minuten)**

  Empfohlener Wert: 15.

  Die Frequenz des Herzschlagsignals ist die Anzahl der Minuten zwischen den vom Wand-Programmiergerät an den CLIQ Remote-Server gesendeten Herzschlagsignalen, die CWM anzeigen, dass das Wand-Programmiergerät online ist. Das Wand-Programmiergerät prüft bei Übertragung des Herzschlagsignals außerdem, ob Updates vorhanden sind (Updates von Firmware oder Konfiguration).

- **Programmiergerätmodus**

  Normal auswählen. Nicht **Diagnose** auswählen, wenn nicht vom technischen Support angewiesen.

- **Plug-and-Play**

  > **HINWEIS!**
  > Damit **Plug-and-Play** funktionieren kann, sind eine aktivierte DCS-Integration sowie deaktivierte **Proxy-Einstellungen** erforderlich.

  Plug-and-Play ermöglicht dem Remote-Programmiergerät, automatisch ein Zertifikat von einem Server zu beziehen, falls es noch keines besitzt. Das Zertifikat wird über die Anmeldeanwendung von DCS heruntergeladen.

  Bei Verwendung des Remote-Programmiergeräts in einem Netzwerk, das ohne Einschränkungen mit dem Internet verbunden ist, die Option **Aktiviert** auswählen (empfohlene Standardeinstellung). Beim Laden eines Zertifikats

in das Remote-Programmiergerät mit Hilfe eines USB-Speichersticks die Option **Deaktiviert** auswählen.

- **Protokolliergrad** (nur Wand-Programmiergerät Generation 2)

  Die Wand-Programmiergeräte senden Fehlerprotokolle an den Remoteserver. Die Protokolle werden 10 Tage lang aufbewahrt. Bei Wand-Programmiergeräten der Generation 2 kann der Protokolliergrad auf eine der folgenden Stufen festgelegt werden:

  - **Kritisch (nur Fehler)**
  - **Allgemein (Fehler und Informationen)**
  - **Detailliert (Fehler, Informationen und Debugging)**
  - **Kein Protokoll**

> **Tipp**
> Der gleiche Protokolliergrad kann auch über die Remote-Programmiergeräte-Liste für mehrere Wand-Programmiergeräte der Generation 2 angewendet werden.

IP

- **Hostname**

  Der Hostname ist der Name des Wand-Programmiergeräts im Netzwerk. Es wird empfohlen, bezeichnende Host-Namen zu verwenden, damit sich das Remote-Programmiergerät bei der Fehlersuche einfacher identifizieren lässt.

- **IP-Konfiguration**

  Statische IP oder **Dynamische IP** auswählen.

  Wenn **Statische IP** gewählt ist, **IP-Adresse**, **Subnetzmaske**, **Gateway** und **DNS** eingeben.

NETZWERKAUTHENTIFIZIERUNG (802.1X) (nur Wand-Programmiergerät Generation 2)

- **Authentifizierung**

  Deaktiviert oder **Aktiviert** auswählen.

> **HINWEIS!**
> Nach der erstmaligen Aktivierung der NETZWERKAUTHENTIFIZIERUNG (802.1X) muss das Wand-Programmiergerät mit einem USB-Speicherstick konfiguriert werden.
>
> Siehe *Abschnitt 6.5.7.3 "Wand-Programmiergerät mit NETZWERKAUTHENTIFIZIERUNG (802.1x) konfigurieren", Seite 118* zu weiteren Details.

- **Client-ID** entspricht dem IP-Hostnamen
- **Client-Zertifikat**

Hier wird ein Client-Zertifikat aufgeführt.

Client-Zertifikat hochladen:

a) Auf **Datei auswählen...** klicken.
b) Im Popup-Fenster das Passwort der Zertifikatdatei eingeben und auf **Auswählen...** klicken.
c) Im Popup-Datei-Explorer eine Zertifikatdatei (`. 12`) auswählen.
d) Auf **Hochladen** klicken.

Client-Zertifikat und **Ablaufdatum des Zertifikats** werden angezeigt.

Informationen zum Bearbeiten der systemweiten Einstellungen für 802.1x finden Sie in *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

PROXY

- **Proxy**

  Wenn **Aktiviert** gewählt ist, **Host**, **Port**, **Benutzername** und **Passwort** eingeben.

  Host ist die Adresse zum Proxyserver im Netzwerk.

  Port ist der erforderliche Port für den Zugriff auf den Proxyserver. Im Normalfall lauten diese Ports 8080.

OFFLINE-UPDATE
Siehe auch *Abschnitt 8.3.3 "Offline-Update", Seite 186*.

> **HINWEIS!**
> Für das Update eines Schlüssels im Offline-Modus benötigt der Schlüssel Firmware-Version 6 oder höher.

- **Maximale Anzahl von Offline-Updates nach einem Online-Update pro Schlüssel**

  Gibt die Anzahl von Updates an, die im Offline-Modus pro Schlüssel durchgeführt werden können, bevor ein Online-Update erforderlich ist.

- **Maximaler Zeitraum zwischen einem Online- und einem Offline-Update**

  Gibt den Zeitraum nach dem letzten Online-Update an, während dem Offline-Updates erlaubt sind.

  Der Wert definiert den Zeitraum, innerhalb dem der Schlüssel im Online-Modus verlängert werden muss.

- **Gültigkeit der Schlüsselsperrliste**

  Gibt an, wie lange die Schlüsselsperrliste im Wand-Programmiergerät gespeichert wird und Offline-Updates erlaubt sind. Siehe auch *Abschnitt 8.3.3 "Offline-Update", Seite 186*.

  Der Wert definiert den Zeitraum, in dem das Remote-Programmiergerät eine Offline-Verlängerung erlaubt. Nach Ablauf dieses Zeitraums können

keine Offline-Updates ausgeführt werden. Beispiel: Bei einer erwarteten Serviceunterbrechung von 48 Stunden sollte ein Wert von mindestens 48 Stunden festgelegt werden.

- **Offline-Verlängerungszeit**

  Legt den Zeitraum fest, für den die Schlüsselgültigkeit verlängert wird. Das auf den Schlüsseln eingestellte Verlängerungsintervall wird bei Offline-Updates ignoriert.

SCHLÜSSEL-FIRMWARE-UPGRADEMODUS

> **HINWEIS!**
> Remote-Programmiergeräte der Generation 2 unterstützen keine Firmware-Upgrades für Schlüssel der Generation 1.

Aktivieren und Deaktivieren von Schlüssel-Upgrades siehe *Abschnitt 6.5.11 "Schlüssel-Upgrades in Remote-Programmiergeräten aktivieren und deaktivieren", Seite 125*.

5) Auf **Speichern** klicken.
6) Übertragen der aktualisierten Konfiguration in das PG.

   - Wenn das Wand-Programmiergerät online ist oder mit den aktuellen Einstellungen eine Verbindung herstellen kann:

     Die aktualisierten Einstellungen werden nach dem nächsten Herzschlagsignal an das Wand-Programmiergerät gesendet. Das Wand-Programmiergerät wird automatisch konfiguriert und stellt eine Verbindung zum Remote-Server her.

     Ob ein Wand-Programmiergerät online ist, ist in den Detailinformationen zu finden.

   - Wenn das PG erstmalig mit deaktiviertem **Plug-and-Play** konfiguriert wird oder mit den aktuellen Einstellungen keine Verbindung herstellen kann:

     a) USB-Speicherstick in den Client-Rechner einführen.
     b) Auf **In Datei speichern** klicken und die Datei im Stammverzeichnis des USB-Speichersticks ablegen.

     > **HINWEIS!**
     > Im Stammverzeichnis des USB-Speichersticks dürfen sich nur die Konfigurationsdateien befinden.
     >
     > Auf dem gleichen USB-Speicherstick können sich mehrere Konfigurationsdateien befinden.

     c) Den USB-Speicherstick mit einem geeigneten USB-Kabel am Wand-Programmiergerät anschließen (siehe *Abschnitt 6.5.7 "Konfigurieren von Wand-Programmiergeräten", Seite 112*).

     Das PG wird automatisch konfiguriert und stellt eine Verbindung zum Remote-Server her. Dieser Vorgang sollte weniger als eine Minute dauern.

7) Anhand der CLIQ-LED-Leuchten prüfen, ob das Programmiergerät online und richtig konfiguriert ist.

Siehe *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen Programmiergeräten", Seite 212* oder *Abschnitt 9.5.2 "Anzeigen eines Wand-Programmiergeräts (Generation 2)", Seite 213*.

6.5.7.2 Zertifikat für ein Wand-Programmiergerät installieren oder verlängern

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Register **Einstellungen** auswählen.

3) • Wenn DCS-Integration aktiviert ist, auf **Client-Zertifikat generieren** klicken.

     Das Zertifikat wird erstellt.

   • Wenn DCS-Integration nicht aktiviert ist:

     a) Klicken Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.

     b) Klicken Sie im Bereich **ALLGEMEIN** auf **Datei auswählen**.

     c) Klicken Sie auf **Auswählen...** und wählen Sie die Zertifikatdatei (.p12) aus.

     d) Geben Sie **Passwort der Zertifikatdatei** ein.

     e) Auf **Hochladen** klicken.

     f) Klicken Sie auf **Speichern**, um den Bearbeitungsmodus zu beenden.

4) Übertragen der aktualisierten Konfiguration in das PG.

   • Wenn das Wand-Programmiergerät online ist oder mit den aktuellen Einstellungen eine Verbindung herstellen kann:

     Die aktualisierten Einstellungen werden nach dem nächsten Herzschlagsignal an das Wand-Programmiergerät gesendet. Das Wand-Programmiergerät wird automatisch konfiguriert und stellt eine Verbindung zum Remote-Server her.

     Ob ein Wand-Programmiergerät online ist, ist in den Detailinformationen zu finden.

   • Wenn das PG erstmalig mit deaktiviertem **Plug-and-Play** konfiguriert wird oder mit den aktuellen Einstellungen keine Verbindung herstellen kann:

     a) USB-Speicherstick in den Client-Rechner einführen.

     b) Auf **In Datei speichern** klicken und die Datei im Stammverzeichnis des USB-Speichersticks ablegen.

     HINWEIS!
     Im Stammverzeichnis des USB-Speichersticks dürfen sich nur die Konfigurationsdateien befinden.

     Auf dem gleichen USB-Speicherstick können sich mehrere Konfigurationsdateien befinden.

     c) Den USB-Speicherstick mit einem geeigneten USB-Kabel am Wand-Programmiergerät anschließen (siehe *Abschnitt 6.5.7 "Konfigurieren von Wand-Programmiergeräten", Seite 112*).

Das PG wird automatisch konfiguriert und stellt eine Verbindung zum Remote-Server her. Dieser Vorgang sollte weniger als eine Minute dauern.

5) Anhand der CLIQ-LED-Leuchten prüfen, ob das Programmiergerät online und richtig konfiguriert ist.

   Siehe *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen Programmiergeräten", Seite 212* und *Abschnitt 9.5.2 "Anzeigen eines Wand-Programmiergeräts (Generation 2)", Seite 213*.

6.5.7.3 Wand-Programmiergerät mit NETZWERKAUTHENTIFIZIERUNG (802.1x) konfigurieren

Nach der erstmaligen Aktivierung der NETZWERKAUTHENTIFIZIERUNG (802.1X) muss das Wand-Programmiergerät mit einem USB-Speicherstick konfiguriert werden.

HINWEIS!
Dies gilt nur für Wand-Programmiergeräte der Generation 2.

Voraussetzung:

- **802.1x-Authentifizierung** ist unter **Systemeinstellungen** aktiviert. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Register **Einstellungen** auswählen.
3) Klicken Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.
4) Laden Sie das Client-Zertifikat für die NETZWERKAUTHENTIFIZIERUNG (802.1x) hoch:
   a) Klicken Sie im Bereich **NETZWERKAUTHENTIFIZIERUNG (802.1X)** auf **Datei auswählen...**.
   b) Im Popup-Fenster das Passwort der Zertifikatdatei eingeben und auf **Auswählen...** klicken.
   c) Im Popup-Datei-Explorer eine Zertifikatdatei (`. 12`) auswählen.
   d) Auf **Hochladen** klicken.

      Client-Zertifikat und **Ablaufdatum des Zertifikats** werden angezeigt.
   e) Klicken Sie auf **Speichern**, um den Bearbeitungsmodus zu beenden.
5) Aktualisierte Konfiguration auf das Wand-Programmiergerät übertragen:
   a) USB-Speicherstick in den Client-Rechner einführen.
   b) Auf **In Datei speichern** klicken und die Datei im Stammverzeichnis des USB-Speichersticks ablegen.

      HINWEIS!
      Im Stammverzeichnis des USB-Speichersticks dürfen sich nur die Konfigurationsdateien befinden.

      Auf dem gleichen USB-Speicherstick können sich mehrere Konfigurationsdateien befinden.
   c) Den USB-Speicherstick mit dem Kabel (USB-C-Stecker an USB-Standardbuchse (Typ A)) am Wand-Programmiergerät anschließen.

Das PG wird automatisch konfiguriert und stellt eine Verbindung zum Remote-Server her.

d) Überprüfen, ob die mittlere LED in der Fortschrittsleiste am Wand-Programmiergerät nach Abschluss des Vorgangs dauerhaft leuchtet.

Wenn die LED-Anzeige nicht dauerhaft leuchtet, den Status anhand der Informationen unter *Abschnitt 9.5.2 "Anzeigen eines Wand-Programmiergeräts (Generation 2)", Seite 213* überprüfen.

6.5.8 Verwalten von Einstellungen und Zertifikaten für mobile CLIQ-Programmiergeräte

Voraussetzungen:

- Bei Verwendung mit iPhone oder Android-Mobiltelefon:
  - Ein mobiles CLIQ-Programmiergerät mit Firmwareversion 2.10 oder höher.
  - Wenn das mobile CLIQ-Programmiergerät ohne Bluetooth mit dem Telefon verbunden werden soll, ist ein Mini-USB-Kabel erforderlich. Informationen über geeignete Kabel finden Sie unter *Abschnitt 7.4.2 "Remote-Programmiergeräte", Seite 165*.
- Mobile CLIQ-Programmiergeräte, die erstmalig mit deaktiviertem **Plug-and-Play** konfiguriert werden oder die mit den aktuellen Einstellungen keine Verbindung herstellen können:
  - Ein Kabel vom Typ USB On-The-Go (OTG): USB-Mini-Stecker (Typen A und B unterstützt) an USB-Standard-Buchse (Typ A).

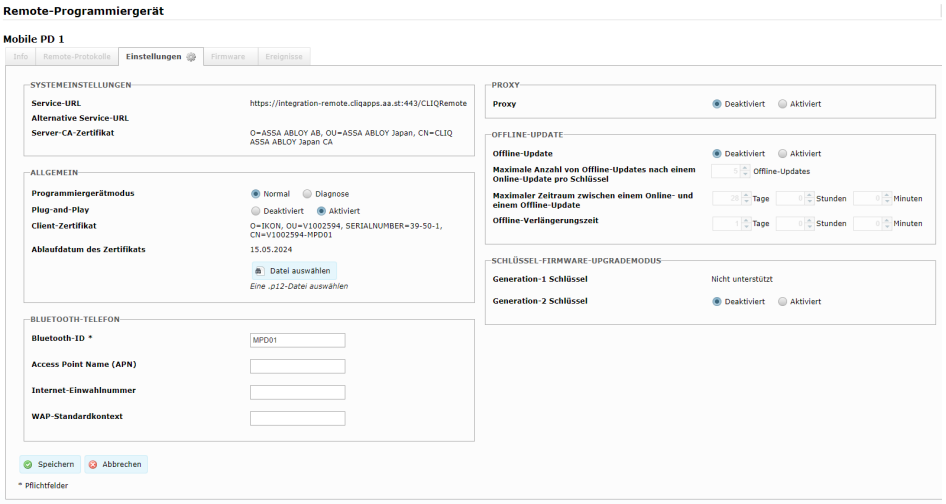
  - Ein im FAT32-Dateisystemformat formatierter USB-Speicherstick. Empfohlene Speichergröße 8-16 GB.
- Verwendung des Offline-Updates:
  - Ein mobiles CLIQ-Programmiergerät mit Firmware 2.10 oder höher.
- Installieren oder Erneuern von Zertifikaten **ohne** DCS-Integration:
  - Eine .p12-Zertifikatdatei. Erhältlich beim lokalen CLIQ-Händler.
- Die mit dem mobilen CLIQ-Programmiergerät mitgelieferte Dokumentation ist verfügbar.

6.5.8.1 Einstellungen von mobilen CLIQ-Programmiergeräten bearbeiten

1) Das mobile CLIQ-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Register **Einstellungen** auswählen.
3) Auf **Bearbeiten** klicken.



4) Die erforderlichen Einstellungen aktualisieren:

ALLGEMEIN

- **Programmiergerätmodus**

  Normal auswählen. Nicht **Diagnose** auswählen, wenn nicht vom technischen Support angewiesen.

- **Plug-and-Play**

> **HINWEIS!**
> Damit **Plug-and-Play** funktionieren kann, sind eine aktivierte DCS-Integration sowie deaktivierte **Proxy-Einstellungen** erforderlich.

  Plug-and-Play ermöglicht dem Remote-Programmiergerät, automatisch ein Zertifikat von einem Server zu beziehen, falls es noch keines besitzt. Das Zertifikat wird über die Anmeldeanwendung von DCS heruntergeladen.

  Bei Verwendung des Remote-Programmiergeräts in einem Netzwerk, das ohne Einschränkungen mit dem Internet verbunden ist, die Option **Aktiviert** auswählen (empfohlene Standardeinstellung). Beim Laden eines Zertifikats in das Remote-Programmiergerät mit Hilfe eines USB-Speichersticks die Option **Deaktiviert** auswählen.

BLUETOOTH-TELEFON

Unabhängig von der Konfiguration der **BLUETOOTH-TELEFON-EINSTELLUNGEN** kann das mobile CLIQ-Programmiergerät immer über ein USB-Kabel zusammen mit einem Computer verwendet werden.

Bei Verwendung mit

- iPhone
- Android
- Anderes Mobiltelefon mit Bluetooth-Profil PAN

Alle Felder in den **BLUETOOTH-TELEFON-EINSTELLUNGEN** mit Ausnahme der **Bluetooth-ID** leer lassen.

Bei Verwendung mit einem Mobiltelefon, das das Bluetooth-Profil DUN unterstützt, Folgendes eingeben:

- **Bluetooth-ID**

  Ein Name des mobilen CLIQ-Programmiergeräts. Dieser Name ist im Mobiltelefon zu sehen, wenn es mit dem mobilen CLIQ-Programmiergerät gekoppelt wird.

- **Access Point Name (APN)**

  Name des Gateways des Netzwerkbetreibers zwischen Mobilfunknetzwerk und Internet. Beispiel: "online.telia.se". Diese Einstellung teilt Ihnen Ihr Mobilfunkbetreiber mit.

- **Internet-Einwahlnummer**

  Die zu wählende Nummer, um Netzzugang zu erhalten, zum Beispiel `*99#`. Diese Einstellung erhalten Sie von Ihrem Mobilfunkbetreiber.

- **WAP-Standardkontext**

  Der Ort im Mobiltelefon, an dem die Internetverbindungseinstellungen gespeichert sind. Dies ist eine mobiltelefonspezifische Einstellung; die richtige Einstellung finden Sie in der Dokumentation des Telefons. In den meisten Fällen kann die Einstellung den Wert `1` haben.

PROXY

- **Proxy**

  Wenn **Aktiviert** gewählt ist, **Host**, **Port**, **Benutzername** und **Passwort** eingeben.

  Host ist die Adresse zum Proxyserver im Netzwerk.

  Port ist der erforderliche Port für den Zugriff auf den Proxyserver. Im Normalfall lauten diese Ports 8080.

OFFLINE-UPDATE

HINWEIS!
Damit ein Schlüssel im Offline-Modus aktualisiert werden kann, muss dieser:

- vor kurzem im gleichen mobilen CLIQ-Programmiergerät aktualisiert worden sein (er muss einer der letzten 10 aktualisierten Schlüssel sein);
- über Firmware-Version 6 oder höher verfügen.

- **Maximale Anzahl von Offline-Updates nach einem Online-Update**

  Gibt die Anzahl von Updates an, die im Offline-Modus durchgeführt werden können, bevor ein Online-Update erforderlich ist. `0` eingeben, um Offline-Update zu deaktivieren.

- **Maximaler Zeitraum zwischen einem Online- und einem Offline-Update**

Gibt an, wie lange nach dem letzten Online-Update Offline-Updates zulässig sind.

- **Offline-Verlängerungszeit**

  Gibt den Zeitraum an, um den die Schlüsselgültigkeit verlängert wird. Das auf den Schlüsseln eingestellte Verlängerungsintervall wird bei Offline-Updates ignoriert.

SCHLÜSSEL-FIRMWARE-UPGRADEMODUS
Aktivieren und Deaktivieren von Schlüssel-Upgrades siehe *Abschnitt 6.5.11 "Schlüssel-Upgrades in Remote-Programmiergeräten aktivieren und deaktivieren", Seite 125*.

5) Auf **Speichern** klicken.

6) Die aktualisierte Konfiguration zum mobilen CLIQ-Programmiergerät übertragen.

- Wenn das mobile CLIQ-Programmiergerät bereits zur einem früheren Zeitpunkt konfiguriert wurde und mit den aktuellen Einstellungen eine Verbindung herstellen kann:

  Die aktualisierten Einstellungen werden bei der nächsten Verwendung an das mobile CLIQ-Programmiergerät gesendet. Das PG wird automatisch konfiguriert und stellt eine Verbindung zum Remote-Server her. Dieser Vorgang sollte weniger als eine Minute dauern.

- Wenn das PG erstmalig mit deaktiviertem **Plug-and-Play** konfiguriert wird oder mit den aktuellen Einstellungen keine Verbindung herstellen kann:

  a) USB-Speicherstick in den Client-Rechner einführen.

  b) Auf **In Datei speichern** klicken und die Datei im Stammverzeichnis des USB-Speichersticks ablegen.

  > **HINWEIS!**
  > Im Stammverzeichnis des USB-Speichersticks dürfen sich nur die Konfigurationsdateien befinden.
  >
  > Auf dem gleichen USB-Speicherstick können sich mehrere Konfigurationsdateien befinden.

  c) Den USB-Speicherstick mit einem geeigneten USB-Kabel am mobilen CLIQ-Programmiergerät anschließen (siehe *Abschnitt 6.5.8 "Konfigurieren von mobile Programmiergeräten", Seite 119*).

  d) Einen Benutzerschlüssel in das mobile CLIQ-Programmiergerät einstecken.

  Die Konfiguration des mobilen CLIQ-Programmiergeräts wird gestartet.

  e) Wenn die Download-LED dauerhaft leuchtet, den USB-Speicherstick entfernen.

7) Die Konfiguration eines Mobiltelefons zur Verwendung mit dem mobilen CLIQ-Programmiergerät ist in der separaten mit dem mobilen CLIQ-Programmiergerät mitgelieferten Dokumentation beschrieben.

8) Einen Computer zur Verwendung mit dem mobilen CLIQ-Programmiergerät konfigurieren:

   a) **ASSA ABLOY Network Provider** auf dem Client-Rechner installieren.

   b) Clientcomputer mit einem Mini-USB-Kabel an das mobile CLIQ-Programmiergerät anschließen. Informationen zum geeigneten Kabel finden Sie in *Abschnitt 6.5.8 "Konfigurieren von mobile Programmiergeräten", Seite 119*.

9) Prüfen auf korrekte Konfiguration:

   a) Einen Benutzerschlüssel in das mobile CLIQ-Programmiergerät einstecken.

   Das PG wird hochgefahren und stellt eine Verbindung zum Remote-Server her. Dieser Vorgang sollte nicht länger als eine Minute dauern.

   b) Prüfen, dass die CLIQ-LED dauerhaft leuchtet.

   Das bedeutet, dass das PG online und korrekt konfiguriert ist.

Siehe auch *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen Programmiergeräten", Seite 212*.

6.5.8.2 Zertifikat für ein mobiles CLIQ-Programmiergerät installieren oder verlängern

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Register **Einstellungen** auswählen.

3) Installation oder Erneuerung eines Zertifikats:

   - Wenn DCS-Integration aktiviert ist, auf **Zertifikat generieren** klicken.

     Das Zertifikat wird erstellt.

   - Wenn die DCS-Integration nicht aktiviert ist und die Zertifikatdatei vom lokalen CLIQ-Händler bereitgestellt wird:

     a) Klicken Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.

     b) Klicken Sie im Bereich **ALLGEMEIN** auf **Datei auswählen**.

     c) Klicken Sie auf **Auswählen...** und wählen Sie die Zertifikatdatei (.p12) aus.

     d) Geben Sie **Passwort der Zertifikatdatei** ein.

     e) Auf **Hochladen** klicken.

     f) Klicken Sie auf **Speichern**, um den Bearbeitungsmodus zu beenden.

4) Übertragen der aktualisierten Konfiguration in das PG.

   - Wenn das mobile CLIQ-Programmiergerät bereits zur einem früheren Zeitpunkt konfiguriert wurde und mit den aktuellen Einstellungen eine Verbindung herstellen kann:

     Auf **Speichern** klicken.

Die aktualisierten Einstellungen werden bei der nächsten Verwendung an das mobile CLIQ-Programmiergerät gesendet. Das PG wird automatisch konfiguriert und stellt eine Verbindung zum Remote-Server her. Dieser Vorgang sollte weniger als eine Minute dauern.

- Wenn das mobile CLIQ-Programmiergerät erstmalig mit deaktiviertem **Plug-and-Play** konfiguriert wird oder mit den aktuellen Einstellungen keine Verbindung herstellen kann:

  a) USB-Speicherstick in den Client-Rechner einführen.

  b) Auf **In Datei speichern** klicken und die Datei im Stammverzeichnis des USB-Speichersticks ablegen.

  > **HINWEIS!**
  > Im Stammverzeichnis des USB-Speichersticks dürfen sich nur die Konfigurationsdateien befinden.
  >
  > Auf dem gleichen USB-Speicherstick können sich mehrere Konfigurationsdateien befinden.

  c) Den USB-Speicherstick mit einem geeigneten USB-Kabel am mobilen CLIQ-Programmiergerät anschließen (siehe *Abschnitt 6.5.8 "Konfigurieren von mobile Programmiergeräten", Seite 119*).

  d) Einen Benutzerschlüssel in das mobile CLIQ-Programmiergerät einstecken.

  Die Konfiguration des mobilen CLIQ-Programmiergeräts wird gestartet.

  e) Wenn die Download-LED dauerhaft leuchtet, den USB-Speicherstick entfernen.

5) Die Konfiguration eines Mobiltelefons zur Verwendung mit dem mobilen CLIQ-Programmiergerät ist in der separaten mit dem mobilen CLIQ-Programmiergerät mitgelieferten Dokumentation beschrieben.

6) Einen Computer zur Verwendung mit dem mobilen CLIQ-Programmiergerät konfigurieren:

   a) **ASSA ABLOY Network Provider** auf dem Client-Rechner installieren.

   b) Clientcomputer mit einem Mini-USB-Kabel an das mobile CLIQ-Programmiergerät anschließen. Informationen zum geeigneten Kabel finden Sie in *Abschnitt 7.4.2 "Remote-Programmiergeräte", Seite 165*.

7) Prüfen auf korrekte Konfiguration:

   a) Einen Benutzerschlüssel in das mobile CLIQ-Programmiergerät einstecken.

   Das PG wird hochgefahren und stellt eine Verbindung zum Remote-Server her. Dieser Vorgang sollte nicht länger als eine Minute dauern.

   b) Prüfen, dass die CLIQ-LED dauerhaft leuchtet.

   Das bedeutet, dass das PG online und korrekt konfiguriert ist.

Siehe auch *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen Programmiergeräten", Seite 212*.

6.5.9 Ereignisprotokoll des Remote-Programmiergeräts anzeigen

Das Ereignisprotokoll enthält Ereignisse und Vorgänge, die von Remote-PGs an den CLIQ Web Manager gemeldet wurden.

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Register **Ereignisprotokoll** auswählen.

6.5.10 Offline-Meldungen für Wand-Programmiergeräte aktivieren oder deaktivieren

Wenn ein Wand-Programmiergerät über einen bestimmten Zeitraum keine Herzschläge mehr sendet, erkennt CLIQ Web Manager, dass es sich im Offline-Status befindet, und sendet eine E-Mail an eine festgelegte Person. Dieser Abschnitt erläutert die Einstellung dieser Funktion.

1) **Verwaltung » Systemeinstellungen** auswählen.

   Die gewählten Systemeinstellungen werden angezeigt.

2) Auf **Bearbeiten** klicken.

3) Im Abschnitt SYSTEM unter **BenutzerBenachrichtigungE-Mails nach Wechsel von Wand-Programmiergerät in Offline-Status** suchen.

4) - Um den E-Mail-Versand einzustellen, das Kontrollkästchen deaktivieren und mit *Schritt 8* fortfahren.
   - Zum Empfang der E-Mail das Kontrollkästchen aktivieren und mit dem nächsten Schritt fortfahren.

     Die Schaltfläche **Konfigurieren** neben dem Kontrollkästchen wird blau gefärbt.

5) Auf **Konfigurieren** klicken.

   Einstellen der Optionen im Fenster.

6) Die E-Mail-Adresse eingeben, an die eine E-Mail gesendet werden soll, wenn ein Wand-Programmiergerät in den Offline-Status wechselt.

7) Die Anzahl der fehlenden Herzschläge eingeben, nach der die E-Mail zu senden ist.

8) Auf **OK** klicken.

6.5.11 Schlüssel-Upgrades in Remote-Programmiergeräten aktivieren und deaktivieren

Informationen zur Durchführung von Schlüssel-Upgrades, einschließlich der zu verwendenden Firmware-Versionen, siehe *Abschnitt 6.15.3 "Upgrade der Firmware in Schlüsseln", Seite 152*.

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) Register **Einstellungen** auswählen.

3) Upgrade von Generation-1-Schlüsseln:

Schlüssel-Upgrades aktivieren:
Unter den **Einstellungen für Schlüssel-Firmware-Upgrademodus** auf **In Schlüssel-Updater-Modus wechseln** klicken.

Diese Schaltfläche wird erst sichtbar, nachdem die erforderlichen Firmware-Dateien importiert wurden, siehe *Abschnitt 6.15.3 "Upgrade der Firmware in Schlüsseln", Seite 152*.

Schlüssel-Upgrades deaktivieren:
Unter den **Einstellungen für Schlüssel-Firmware-Upgrademodus** auf **Umschalten in normalen Modus** klicken.

4) Upgrade von Generation-2-Schlüsseln:

Schlüssel-Upgrades aktivieren:

1. Auf **Bearbeiten** klicken.
2. Unter den **Einstellungen für Schlüssel-Firmware-Upgrademodus** den Punkt **Aktiviert** auswählen.
3. Auf **Speichern** klicken.

> **HINWEIS!**
> Bei einem Upgrade von Generation-2-Schlüsseln lassen sich mehrere Remote-PGs auswählen.
>
> *Schritt 5 c* in *Abschnitt 6.15.3 "Upgrade der Firmware in Schlüsseln", Seite 152* für jedes Remote-Programmiergerät wiederholen, das für Schlüssel-Upgrades verwendet werden soll.

Schlüssel-Upgrades deaktivieren:

1. Auf **Bearbeiten** klicken.
2. Unter den **Einstellungen für Schlüssel-Firmware-Upgrademodus** den Punkt **Deaktiviert** auswählen.
3. Auf **Speichern** klicken.

6.5.12 Informationen zu Remote-Programmiergeräten exportieren

1) Das Remote-Programmiergerät suchen und seine Detailansicht öffnen.

   Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

2) In den Suchergebnissen die Remote-PGs, deren Daten exportiert werden sollen, auswählen.
3) Auf **In CSV-Datei exportieren** klicken.
4) Im Pop-up-Fenster für den Dateidownload auf **OK** klicken.

   Eine CSV-Datei wird in den Ordner **Downloads** heruntergeladen.

HINWEIS!
Damit die Excel-Datei korrekt geöffnet werden kann, muss das Trennzeichen entsprechend den regionalen Einstellungen eingestellt sein. Ändern des Trennzeichens siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

6.6 Verwalten von Domänen

6.6.1 Suchen nach Domänen

1) **Verwaltung » Domänen** auswählen.

   Eine Liste aller Domänen wird angezeigt.

2) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

3) Auf **Suchen** klicken.

4) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf die Zeile mit der entsprechenden Domäne klicken.

6.6.2 Bearbeiten von Domäneninformationen

1) Die zu bearbeitende Domäne suchen.

   Siehe *Abschnitt 6.6.1 "Suchen nach Domänen", Seite 127*.

2) In der Liste der Suchergebnisse auf den Namen der Domäne klicken.

3) Auf **Bearbeiten** klicken.

4) Den Namen und die Beschreibung der Domäne eingeben.

5) Auf **Speichern** klicken.

6.6.3 Einstellen der anfänglichen Domänen für neue oder importierte Objekte

Neue und importierte Objekte werden der entsprechenden anfänglichen Domäne zugeordnet.

Anfängliche Domänen existieren für die folgenden Objekte:

- Schlüssel
- Personen (Mitarbeiter und Besucher)
- Zylinder (und Zylindergruppen)

HINWEIS!
Neue oder importierte Zylinder, die zu einer Zylindergruppe gehören, werden in die Domäne der Zylindergruppe aufgenommen, nicht in die anfängliche Zylinderdomäne. Das bedeutet, dass alle Zylinder einer Zylindergruppe zur selben Domäne gehören. Weitere Informationen zu Domänen finden Sie in *Abschnitt 8.2.2 "Domänen", Seite 178*.

Neue und importierte Zugangsprofile und temporäre Zugangsgruppen werden der anfänglichen Zylinderdomäne zugeordnet.

Jede anfängliche Domäne hat einen veränderbaren Namen. Der Standardname lautet `default`. Die anfänglichen Domänen können dieselbe Domäne oder verschiedene Domänen haben.

Zum Einstellen der anfänglichen Domänen für Schlüssel, Personen und Zylinder:

1) **Verwaltung » Systemeinstellungen** auswählen.
2) Auf **Bearbeiten** klicken.
3) Unter **VERWALTUNG** auf **Domäne ändern...** für die entsprechende anfängliche Domäne klicken.

   Es erscheint eine Liste mit Domänen, für die der Administrator eine Berechtigung besitzt.
4) In der Zeile mit der neuen Domäne auf **Auswählen** klicken.
5) Auf **Speichern** klicken.

6.6.4 Anlegen und Löschen von Domänen

1) **Verwaltung » Domänen** auswählen.
2) Domäne anlegen:
   a) Auf **Neu anlegen** klicken.
   b) **Name** sowie eine optionale **Beschreibung** eingeben.
   c) Auf **Speichern** klicken.
3) Domäne löschen:

> **HINWEIS!**
> Eine Domäne lässt sich nur löschen, wenn keine Zylinder, Zylindergruppen, Mitarbeiter, Besucher oder Schlüssel mit ihr verbunden sind. Vor dem Löschen die Domäne leeren, indem die Objekte in eine andere Domäne verschoben werden.
>
> Sicherstellen, dass sowohl aktive als auch gelöschte Mitarbeiter und Besucher in eine andere Domäne verschoben werden. Zum Auffinden von gelöschten Mitarbeitern und Besuchern siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.

   a) Domäne suchen und Detailinformationen anzeigen.

      Siehe *Abschnitt 6.6.1 "Suchen nach Domänen", Seite 127*.
   b) Auf **Löschen** klicken.
   c) Auf **OK** klicken.

6.6.5 Ändern der Domäne für Schlüssel

1) **Systeminfo » Schlüssel** auswählen.

   Eine Liste aller Schlüssel wird angezeigt.
2) Zur Suche nach bestimmten Schlüsseln die Suchkriterien eingeben und auf **Suchen** klicken.

3) Auf die Zeile mit dem entsprechenden Schlüssel klicken.
4) Auf **Bearbeiten** klicken.
5) Auf **Domäne ändern...** klicken.

   Es erscheint eine Liste mit Domänen, für die der Administrator eine Berechtigung besitzt.
6) In der Zeile mit der neuen Domäne auf **Auswählen** klicken.
7) Auf **Speichern** klicken.

Die Domäne kann für mehrere Schlüssel gleichzeitig geändert werden. Die Schlüssel in der Liste der Suchergebnisse auswählen und auf **Domäne ändern...** klicken.

Siehe auch *Abschnitt 8.2.2 "Domänen", Seite 178*.

6.6.6 Ändern der Domäne für Mitarbeiter und Besucher

1) Zu bearbeitenden Mitarbeiter oder Besucher suchen.

   Suche nach einem Mitarbeiter oder Besucher und Anzeige von Detailinformationen siehe *Abschnitt 4.1.1 "Suchen nach Mitarbeitern oder Besuchern", Seite 24*.
2) Auf **Bearbeiten** klicken.
3) Auf **Domäne ändern...** klicken.

   Es erscheint eine Liste mit Domänen, für die der Administrator eine Berechtigung besitzt.
4) In der Zeile mit der neuen Domäne auf **Auswählen** klicken.
5) Auf **Speichern** klicken.

Die Domäne kann für mehrere Mitarbeiter oder Besucher gleichzeitig geändert werden. Die Mitarbeiter oder Besucher in der Liste der Suchergebnisse auswählen und auf **Domäne ändern...** klicken.

Siehe auch *Abschnitt 8.2.2 "Domänen", Seite 178*.

6.6.7 Ändern der Domäne für Zylinder

Bei Zylindern, die zu einer Zylindergruppe gehören, wird die Domäne auf Zylindergruppenebene geändert. Siehe *Abschnitt 6.6.8 "Ändern der Domäne für Zylindergruppen", Seite 130*.

1) **Systeminfo » Zylinder** auswählen.

   Eine Liste aller Zylinder wird angezeigt.
2) Zur Suche nach bestimmten Zylindern die Suchkriterien eingeben und auf **Suchen** klicken.
3) Auf die Zeile mit dem entsprechenden Zylinder klicken.
4) Auf **Bearbeiten** klicken.
5) Auf **Domäne ändern...** klicken.

   Es erscheint eine Liste mit Domänen, für die der Administrator eine Berechtigung besitzt.
6) In der Zeile mit der neuen Domäne auf **Auswählen** klicken.
7) Auf **Speichern** klicken.

Die Domäne kann für mehrere Zylinder gleichzeitig geändert werden. Die Zylinder in der Liste der Suchergebnisse auswählen und auf **Domäne ändern...** klicken.

HINWEIS!
Es wird empfohlen, dass ein Zugangsprofil sowie alle umfassten Zylinder und Zylindergruppen in derselben Domäne liegen. Dadurch wird sichergestellt, dass Administratoren einer bestimmten Domäne nicht indirekt Zugang zu Zylindern in anderen Domänen erhalten (über Zugangsprofile).

Siehe auch *Abschnitt 8.2.2 "Domänen", Seite 178*.

6.6.8 Ändern der Domäne für Zylindergruppen

Bei Zylindern, die nicht zu einer Zylindergruppe gehören, wird die Domäne individuell je Zylinder geändert. Siehe *Abschnitt 6.6.7 "Ändern der Domäne für Zylinder", Seite 129*.

1) **Systeminfo » Zylindergruppen** auswählen.

   Eine Liste aller Zylindergruppen wird angezeigt.
2) Zur Suche nach bestimmten Zylindergruppen die Suchkriterien eingeben und auf **Suchen** klicken.
3) Auf die Zeile mit der entsprechenden Zylindergruppe klicken.
4) Auf **Bearbeiten** klicken.
5) Auf **Domäne ändern...** klicken.

   Es erscheint eine Liste mit Domänen, für die der Administrator eine Berechtigung besitzt.
6) In der Zeile mit der neuen Domäne auf **Auswählen** klicken.
7) Auf **Speichern** klicken.

Die Domäne kann für mehrere Zylindergruppen gleichzeitig geändert werden. Die Zylindergruppen in der Liste der Suchergebnisse auswählen und auf **Domäne ändern...** klicken.

HINWEIS!
Es wird empfohlen, dass ein Zugangsprofil sowie alle umfassten Zylinder und Zylindergruppen in derselben Domäne liegen. Dadurch wird sichergestellt, dass Administratoren einer bestimmten Domäne nicht indirekt Zugang zu Zylindern in anderen Domänen erhalten (über Zugangsprofile).

Siehe auch *Abschnitt 8.2.2 "Domänen", Seite 178*.

6.6.9 Ändern der Domäne für Zugangsprofile

1) Zugangsprofil suchen und Detailinformationen anzeigen.

   Siehe *Abschnitt 4.6.1 "Suchen nach Zugangsprofilen", Seite 71*.
2) In der Detailanzeige auf **Bearbeiten** klicken.
3) Auf **Domäne ändern** klicken.
4) Bei der neuen Domäne auf **Auswählen** klicken.
5) Auf **Speichern** klicken.

HINWEIS!
Es wird empfohlen, dass ein Zugangsprofil sowie alle umfassten Zylinder und Zylindergruppen in derselben Domäne liegen. Dadurch wird sichergestellt, dass Administratoren einer bestimmten Domäne nicht indirekt Zugang zu Zylindern in anderen Domänen erhalten (über Zugangsprofile).

6.7 Verwalten von Rollen und Rechten

HINWEIS!
Informationen zum Zuweisen von Rollen zu einem Programmierschlüssel finden Sie in *Abschnitt 6.11.4 "Bearbeiten von Programmierschlüsselinformationen", Seite 139*.

1) **Verwaltung » Rollen** auswählen.

   Eine Liste vorhandener Rollen wird angezeigt.

   Einige dieser Rollen sind in der CWM-Software vordefiniert.

2) **Rolle erstellen:**

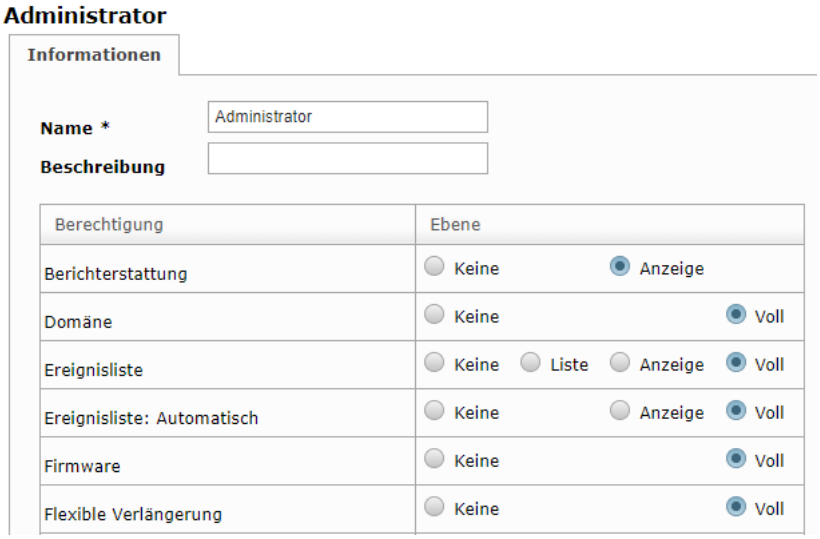
   1. Auf **Neu anlegen** klicken.
   2. **Name** sowie eine eventuelle **Beschreibung** eingeben.
   3. Rechte aus der Liste auswählen.

      HINWEIS!
      Einschränkungen:

      – Der Zugriff auf bestimmte Berechtigungen hängt von der Stufe anderer Berechtigungen ab. Wenn sich eine bestimmte Berechtigung nicht konfigurieren lässt, die Stufe verknüpfter Berechtigungen überprüfen.

      – Wenn **Hierarchische Administratoren** aktiviert ist, kann der Administrator keine Berechtigungsstufen über der eigenen Berechtigungsstufe konfigurieren.

        Ein Administrator, dem die Stufe **Liste** für die Berechtigung **Zylinder** gewährt wurde, kann neuen Rollen beispielsweise nicht die Stufe **Anzeige** oder **Voll** für die Berechtigung **Zylinder** gewähren.



Vorhandene Rolle bearbeiten:

HINWEIS!

Einschränkungen:

- Ein Administrator kann seine eigene Rolle nicht bearbeiten. Nur das Feld **Beschreibung** ist bearbeitbar.
- Wenn **Hierarchische Administratoren** aktiviert ist, kann der Administrator nicht die Rolle eines Administrators mit höheren Berechtigungen bearbeiten.
- Wenn **Hierarchische Administratoren** aktiviert ist, kann der Administrator keine Berechtigungsstufen über der eigenen Berechtigungsstufe konfigurieren.
- Die Rollen **Super-Administrator**, **Genehmigender** und **CLIQ Connect+** sind schreibgeschützt können nicht bearbeitet werden.

1. Auf die Zeile mit der entsprechenden Rolle klicken.
2. Klicken Sie auf **Bearbeiten**, um **Name**, **Beschreibung** oder **Berechtigungen** der Rolle zu aktualisieren.
3. Auf **Speichern** klicken.

Rolle löschen

HINWEIS!

Einschränkungen:

- Rollen, die einem oder mehreren Mitgliedern zugewiesen sind, können nicht gelöscht werden.
- Die Rollen **Super-Administrator**, **Genehmigender** und **CLIQ Connect+** sind schreibgeschützt können nicht gelöscht werden.
- Wenn **Hierarchische Administratoren** aktiviert ist, kann der Administrator keine Rollen löschen, denen eine Berechtigungsstufe über der eigenen Berechtigungsstufe zugewiesen ist.

1. Auf die Zeile mit der entsprechenden Rolle klicken.
2. Auf **Löschen** klicken.
3. Auf **OK** klicken.

Programmierschlüsselmitglieder einer Rolle anzeigen

1. Auf die Zeile mit der entsprechenden Rolle klicken.
2. Register **Mitglieder** auswählen.

Siehe auch:

- *Abschnitt 8.8 "CWM-Rollen und Administratorrechte", Seite 192*
- *Abschnitt 9.4 "Rechte", Seite 206*

6.8 Importieren von Mitarbeiterinformationen

Die zu importierenden Mitarbeiterinformationen müssen in einer CSV-Datei gespeichert sein, die bestimmten Anforderungen entsprechen muss. Siehe *Abschnitt 9.9 "Dateiformat für Mitarbeiterimport", Seite 216*. Da sich die genauen Anforderungen ändern können, wird empfohlen, die Datei zur Kontrolle hochzuladen.

HINWEIS!

Die folgenden Mitarbeiter werden während des Importvorgangs nicht in CWM hinzugefügt oder aktualisiert:

- Deaktivierte Mitarbeiter.
- Mit LDAP integrierte Mitarbeiter.

1) **Verwaltung » Mitarbeiter importieren** auswählen.
2) Auf **Auswählen** klicken und die lokal auf dem Computer gespeicherte Datei suchen.
3) Auf **Öffnen** klicken.
4) Zur Kontrolle der Datei auf **Hochladen** klicken.

   Es wird angezeigt, wie viele gültige Einträge in der Datei vorhanden sind. Wenn die Datei nicht den Anforderungen entspricht, ist der Import nicht möglich.

5) Zum Importieren der gültigen Datei auf **Import** klicken.

6.9 Verwalten von Quittungsvorlagen

Der Text und das Logo in den Vorlagen für Ausgabe- und Rücknahmequittungen können selbst erstellt oder bearbeitet werden. Quittungen werden im PDF-Format erstellt und können gedruckt oder gespeichert werden.

> **HINWEIS!**
> Zur Verwaltung der Quittungsvorlagen ist Berechtigungsebene **Voll** in der Rolle **Quittungsvorlagen** erforderlich. Zum Wechsel der Berechtigungsebene siehe *Abschnitt 6.7 "Verwalten von Rollen und Rechten", Seite 131*.

6.9.1 Erstellen einer Quittungsvorlage

Es ist möglich, neue Quittungsvorlagen zum System hinzuzufügen und diese als voreingestellte oder nicht voreingestellte Vorlagen festzulegen.

1) **Verwaltung » Quittungsvorlagen** auswählen.

   Die Liste der Quittungsvorlagen wird angezeigt.

2) Klicken Sie unterhalb der Liste auf **Neu anlegen**.

3) Die folgenden Felder ausfüllen:

   - **Name**: Dient als Name der Vorlage.
   - **Typ**: **Ausgabe** oder **Rückgabe** auswählen.
   - **Standard für**: Wenn die erstellte Vorlage als voreingestellte Vorlage genutzt werden soll, ein oder beide Kontrollkästchen aktivieren.
   - **Sprache**: Die entsprechende Sprache in der Drop-down-Liste auswählen.
   - **Titel**: Wird als Überschrift für den Inhalt der Vorlage gedruckt.

4) Wählen Sie den Logotyp aus:

   - Systemlogo: das standardmäßige Logo der Organisation. Anweisungen zum Ändern des Systemlogos finden Sie unter *Abschnitt 6.9.3 "Ändern des Systemlogos", Seite 136*.
   - Benutzerdefiniertes Logo: ein eigenes Firmenlogo, das anstelle des Systemlogos verwendet wird.

     a) **Benutzerdefiniertes Logo verwenden** auswählen.

     b) Auf **Auswählen** klicken.

     c) Klicken Sie auf **Auswählen...** und wählen Sie die Datei aus.

     Das hochzuladende Bild muss weniger als 2 MB groß sein und im Format JPEG, JPG, PNG, BMP oder GIF vorliegen.

     d) Auf **Hochladen** klicken.

     Das Logo wird auf dem Pop-up-Bildschirm angezeigt.

     e) Klicken Sie zum Beenden auf **Schließen**.

5) Sätze in das Feld **Text** eingeben.

Bei Erstellung einer neuen Vorlage auf Basis des Standardtexts wird empfohlen, auf **Standardtext verwenden** zu klicken und den Inhalt zu bearbeiten.

Das Textfeld verfügt über einige grundlegende Schaltflächen zur Formatierung des Texts. Um diese Formatierung auf einen neuen Text anzuwenden, auf die Schaltfläche klicken und mit der Eingabe beginnen. Um diese Formatierung auf einen vorhandenen Inhalt im Bearbeitungsfenster anzuwenden, den Inhalt auswählen und auf die gewünschte Schaltfläche klicken. Die folgende Tabelle gibt eine Übersicht über die verfügbaren Schaltflächen:

B	Fett
I	Kursiv
U	Unterstrichen
~~S~~	Durchgestrichen
x^2	Hochgestellt
x_2	Tiefgestellt
	Liste ohne Nummerierung
	Liste mit Nummerierung
H1	Überschrift erste Ebene
H2	Überschrift zweite Ebene
T_x	Formatierung aufheben

6) Optional: Zur Überprüfung der Quittung auf **Vorschauvorlage** klicken.

7) Auf **Speichern** klicken.

6.9.2 Bearbeiten einer Quittungsvorlage

1) **Verwaltung » Quittungsvorlagen** auswählen.

   Die Liste der Quittungsvorlagen wird angezeigt.

2) Auf die zu bearbeitende Vorlage klicken.

3) Auf **Bearbeiten** klicken.

4) Die folgenden Felder bearbeiten:

   - **Name**: Dient als Name der Vorlage.
   - **Typ**: **Ausgabe** oder **Rückgabe** auswählen.
   - **Standard für**: Wenn die bearbeitete Vorlage als voreingestellte Vorlage genutzt werden soll, ein oder beide Kontrollkästchen aktivieren.
   - **Sprache**: Die entsprechende Sprache in der Drop-down-Liste auswählen.
   - **Titel**: Wird als Überschrift für den Inhalt der Vorlage gedruckt.

5) Logotyp bearbeiten:

   - Anweisungen zum Ändern des Systemlogos finden Sie unter *Abschnitt 6.9.3 "Ändern des Systemlogos", Seite 136*.
   - Um das benutzerdefinierte Logo zu ändern, klicken Sie auf **Auswählen** und laden Sie das neue Logo hoch.

6) Die Sätze im Feld **Text** bearbeiten.

Für weitere Informationen zur Formatierung von Texten siehe *Abschnitt 6.9.1 "Erstellen einer Quittungsvorlage", Seite 134, Schritt 5*.

7) Optional: Zur Überprüfung der Quittung auf **Vorschauvorlage** klicken.

8) Auf **Speichern** klicken.

6.9.3 Ändern des Systemlogos

Quittungsvorlagen enthalten ein voreingestelltes Markenlogo. Es ist jedoch möglich, das voreingestellte Logo anzupassen.

Voraussetzungen:

- Das Logo ist eine Bilddatei mit RGB-Farbprofil (CMYK wird nicht unterstützt).
- Das Logo muss kleiner sein als 2 MB. Die empfohlene Größe beträgt ca. 120 x 60 Pixel.

1) **Verwaltung » Quittungsvorlagen** auswählen.
2) Auf **Systemlogo ändern** unter der Liste klicken.
3)
   - Zum Wechsel auf das angepasste Logo:
     a) Auf **Auswählen...** klicken.
     b) Upload-Datei auswählen und auf **Öffnen** klicken.
     c) Auf **Hochladen** klicken.
   - Zum Wechsel auf das voreingestellte Logo auf **Standard wiederherstellen** klicken.
4) Auf **Schließen** klicken.

6.9.4 Löschen einer Quittungsvorlage

1) **Verwaltung » Quittungsvorlagen** auswählen.

   Die Liste der Quittungsvorlagen wird angezeigt.
2) Auf die zu löschende Vorlage klicken.
3) Auf **Löschen** klicken.
4) Im Pop-up-Fenster auf **OK** klicken.

6.10 Verwalten von Zeitplanvorlagen

Es gibt zwei Arten von Zeitplanvorlagen: **Einfache Vorlage** und **Vorlage mit mehreren Zeiträumen**.

- In einer einfachen Vorlage kann ein Zeitraum pro Wochentag festgelegt werden.
- Eine Vorlage mit mehreren Zeiträumen ermöglicht die freie Festlegung von Tagen und Zeiträumen. Es können mehrere Zeiträume für denselben Wochentag festgelegt werden.

Die beiden Vorlagen werden von unterschiedlichen Versionen der Schlüsselfirmware unterstützt. Informationen darüber, welche Versionen der Schlüsselfirmware welche Vorlage unterstützt siehe *Abschnitt 9.7 "Firmware-abhängige Funktionen", Seite 215*.

1) **Verwaltung » Zeitplanvorlagen** auswählen.
2) Zum Anlegen einer grundlegenden Zeitplanvorlage:

a) Auf **Grundlegende Vorlage anlegen** klicken.

   Standardmäßig sind die Zeiträume auf den ganzen Tag eingestellt.

b) **Name** sowie optional **Beschreibung** eingeben.

c) Zum Ändern der standardmäßigen Zeiträume in der Zeile mit dem entsprechenden Tag auf **Bearbeiten** klicken.

d) **Den ganzen Tag**, **Niemals** oder **Benutzerdefiniert** auswählen.

e) Wenn die Option Benutzerdefiniert ausgewählt ist, die Zeitraumwerte **Von Zeit** und **Bis Zeit** eintragen.

f) Auf **Speichern** klicken.

   Falls erforderlich, *Schritt 2 c–Schritt 2 f* für weitere Tage wiederholen.

g) Auf **Speichern** klicken.

3) Zum Anlegen einer Vorlage für einen Zeitplan mit mehreren Zeiträumen:

   a) Auf **Vorlage mit mehreren Zeiträumen anlegen** klicken.

   b) **Name** sowie optional **Beschreibung** eingeben.

   c) Auf **Zeitraum hinzufügen** klicken.

   d) Die Zeitraumwerte **Von Datum** und **Bis Datum** eintragen.

   e) Die Zeitraumwerte **Von Zeit** und **Bis Zeit** eintragen.

   f) Auf **Speichern** klicken.

   g) Falls gewünscht, weitere Zeiträume hinzufügen.

   h) Auf **Speichern** klicken.

4) Vorlage bearbeiten:

   a) Auf die Zeile mit der entsprechenden Vorlage klicken.

   b) Auf **Bearbeiten** klicken.

   c) Die Felder ändern und auf **Speichern** klicken.

5) Vorlage löschen:

   a) Auf die Zeile mit der entsprechenden Vorlage klicken.

   b) Auf **Löschen** klicken.

   c) Auf **OK** klicken.

Siehe auch *Abschnitt 8.1.8 "Schlüssel-Zeitpläne", Seite 175*.

6.11 Verwalten von Programmierschlüsseln

6.11.1 Suchen nach Programmierschlüsseln

1) **Verwaltung » Programmierschlüssel** auswählen.

2) Suchkriterien eingeben.

   CWM akzeptiert bei der Eingabe in Suchfelder auch den ersten Teil eines Suchbegriffs sowie ein Sternchen (*). Wenn beispielsweise nach "Labor 1" gesucht wird, führt die Eingabe von "Lab", "*1" oder "Lab*1" zu Suchergebnissen, die "Labor 1" enthalten.

3) Auf **Suchen** klicken.

4) Zur Anzeige von Detailinformationen zu einem Suchergebnis auf die Zeile mit dem entsprechenden Programmierschlüssel klicken.

Informationen zu den Merkmalen des Programmierschlüssels siehe *Abschnitt 9.3.4 "Programmierschlüsselattribute", Seite 204*.

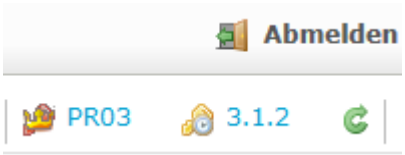
6.11.2 Abfragen eines Programmierschlüssels

1) Den abzurufenden Programmierschlüssel in den rechten Schlitz des lokalen Programmiergeräts einführen.

> **HINWEIS!**
> Der Programmierschlüssel, der für die Anmeldung verwendet wird, muss im linken Schlitz des lokalen Programmiergeräts verbleiben.

2) In der oberen rechten Ecke der Seite auf klicken.

Beide Programmierschlüssel im lokalen Programmiergerät werden unterhalb der Navigationsleiste angezeigt.



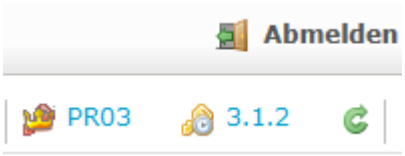
6.11.3 Status des Programmierschlüssels anzeigen

1) Den anzuzeigenden Programmierschlüssel in den rechten Schlitz des lokalen Programmiergeräts einführen.

> **HINWEIS!**
> Der Programmierschlüssel, der für die Anmeldung verwendet wird, muss im linken Schlitz des lokalen Programmiergeräts verbleiben.

2) In der oberen rechten Ecke der Seite auf klicken.

Beide Schlüssel im lokalen Programmiergerät werden unterhalb der Navigationsleiste angezeigt.

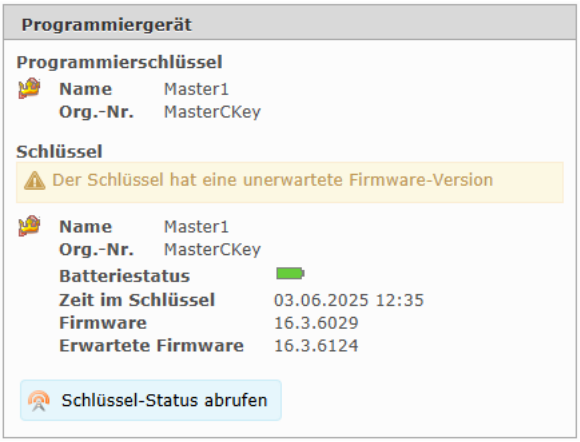


3) Auf den Programmierschlüssel im rechten Schlitz des lokalen Programmiergeräts klicken.

Die detaillierte Informationsansicht des Programmierschlüssels wird angezeigt. Rechts auf der Seite werden **Name** und **Org.-Nr.** des Programmierschlüssels angezeigt.

4) Auf **Schlüssel-Status abrufen** klicken.

Grundlegende Informationen über den Programmierschlüssel im rechten Schlitz werden angezeigt. Weitere Informationen über die Batteriestatusanzeige finden Sie unter *Abschnitt 9.6 "Anzeige der Batterieladung", Seite 214*.



6.11.4 Bearbeiten von Programmierschlüsselinformationen

1) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.

2) Auf **Bearbeiten** klicken.

   - Zum Bearbeiten des Programmierschlüsselnamens das Feld **Name** ändern.
   - Zum Sperren des Programmierschlüssels **Sperren** auswählen.
   - Um zu ändern, ob eine Zertifikatanmeldung zulässig ist, **immer zulässig**, **Einmal zulässig** oder **nicht zulässig** auswählen.

     Siehe auch *Abschnitt 8.11 "DCS-Integration", Seite 196*.
   - Zum Ändern der Berechtigungsrollen für einen Programmierschlüssel eine oder mehrere Rollen auswählen.

   HINWEIS!

   Einschränkungen:

   – Die Rolle des für die aktuelle Anmeldung verwendeten Programmierschlüssels kann nicht geändert werden.

   – Die Rolle des Genehmigenden kann nicht mit anderen Rollen kombiniert werden.

   – Wenn **Hierarchische Administratoren** aktiviert ist, kann der Administrator keine Rollen mit einer Berechtigungsstufe über der eigenen Berechtigungsstufe zuweisen.

3) Auf **Speichern** klicken.

6.11.5 Auswählen von Domänen für Programmierschlüssel

1) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.

2) Programmierschlüssel suchen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.

3) Register **Domänenberechtigungen** auswählen.

4) Zum Ändern von Domänen auf **Bearbeiten** klicken.

5) Hinzufügen von Domänen:

   a) Auf **Domäne hinzufügen...** klicken.

      Das Suchergebnis enthält eine Liste aller Domänen.

   b) Zum Filtern der Domänen die Suchkriterien eingeben und auf **Suchen** klicken.

   c) Bei den hinzuzufügenden Domänen auf **Auswählen** bzw. auf **Alle auswählen** klicken.

   d) Auf **Fertig** klicken.

6) Um eine Domäne zu entfernen, bei der zu entfernenden Domäne auf **Entfernen** bzw. auf **Alle entfernen** klicken.

7) Auf **Speichern** klicken.

   Die Änderung der Domäne wird bei der nächsten Anmeldung wirksam.

6.11.6 Anzeige der Programmierschlüssel-Ereignisse

Das Register Ereignisse wird zur Verfolgung bestimmter Administratorvorgänge in CWM verwendet, z. B. die Ausgabe eines Programmierschlüssels.

1) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.

2) Register **Ereignisse** auswählen.

   Eine Liste mit allen Programmierschlüssel-Ereignissen wird angezeigt.

6.11.7 Ausgeben von Programmierschlüsseln

Voraussetzung:

- Dem Administrator wurde die komplette Berechtigung **Programmierschlüssel: Ausgabe/Rücknahme** zugewiesen.
- Der Mitarbeiter, der einen Programmierschlüssel erhalten soll, muss über eine gültige E-Mail-Adresse verfügen.

1) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.

2) Auf **An Mitarbeiter ausgeben** klicken.

   Die Liste der Mitarbeiter wird angezeigt.

3) Den Mitarbeiter aus der Liste auswählen und auf **Auswählen** klicken.

   An die registrierte E-Mail-Adresse des Mitarbeiters wird eine E-Mail mit Anweisungen zum Herunterladen von CLIQ Connect PC und mit der URL für die Schließanlage gesendet.

   Zur Anmeldung bei CWM muss der Mitarbeiter ein Zertifikat für den Schlüssel installieren. Weitere Informationen zur Installation von Zertifikaten finden Sie unter *Abschnitt 3.2 "Anmelden und Installieren von Programmierschlüssel-Zertifikaten", Seite 16*.

> **Tipp**
> Es wird dringend empfohlen, dass der Mitarbeiter den PIN-Code für den Programmierschlüssel ändert. Eine Anleitung finden Sie unter *Abschnitt 6.11.11 "Ändern des PIN-Codes des Programmierschlüssels", Seite 144*.

6.11.8 Rückgabe von Programmierschlüsseln

Voraussetzung:

- Dem Administrator wurde die komplette Berechtigung **Programmierschlüssel: Ausgabe/Rücknahme** zugewiesen.

1) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.

2) Auf **Programmierschlüssel zurückgeben** klicken.

   Der Programmierschlüssel kann jetzt nicht mehr zum Login an der CWM-Software verwendet werden.

6.11.9 Verlorenen Programmierschlüssel melden und sperren

1) Programmierschlüssel suchen und Detailinformationen anzeigen.

   Siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*.

2) Auf **Als verloren melden** klicken.

3) Verlorene Programmierschlüssel, die Zylinderprogrammierjobs enthalten, müssen gesperrt werden, um eine unbefugte Zylinderprogrammierung zu verhindern.

   - Um einen Programmierschlüssel zu sperren, der Programmierjobs für Zylinder enthält, die Zylinder auswählen, für die der Programmierschlüssel gesperrt werden soll:
     - Wählen Sie **Alle Zylinder** oder **Nur eingebaute** aus und fahren Sie mit *Schritt 6* fort.
     - Wählen Sie **Benutzerdefinierte Auswahl** aus fahren Sie mit *Schritt 4* fort, um die Zylinder auszuwählen.
   - Um den Verlust eines Programmierschlüssels zu melden, ohne einen Zylinder zu sperren, **Keine Zylinder** auswählen, auf **Weiter** klicken und mit *Schritt 9* fortfahren.

4) Auf **Weiter** klicken.

5) Die Zylinder auswählen, für die der verlorene Programmierschlüssel gesperrt werden soll.

6) Auf **Weiter** klicken.

7) Optional: Wählen Sie den Programmierschlüssel für den Zylinder aus der Liste aus, indem Sie auf **Auswählen** klicken.

   HINWEIS!
   Wird dieser Vorgang übersprungen, werden Zylinderprogrammierjobs für Programmierschlüssel erstellt.

   Wählen Sie auf der Registerkarte **Suchen** die Option **Alle Typen und Status** aus, um Programmierschlüssel anzuzeigen.

   Auf der Registerkarte **Erweitert** unter **Typ** entweder Benutzerschlüssel oder Programmierschlüssel auswählen, um den Inhalt der angezeigten Liste zu ändern.

   HINWEIS!
   Der Programmierschlüssel für den Zylinder muss über ausreichend Speicher verfügen.

8) Wählen Sie auf der Bestätigungsseite unter **Priorität** die Prioritätsstufe aus.

   Dringende Jobs sollten hohe Priorität haben.

9) Klicken Sie auf **Als verloren melden**, nachdem Sie alle Informationen überprüft haben.

   - Wenn **keine** Jobs zum Sperren des verlorenen Programmierschlüssels angelegt sind, werden die dem verlorenen Programmierschlüssel zugewiesenen Programmierjobs gelöscht und unter **Arbeit » Zylinderprogrammierung** aufgelistet.

- Wenn Jobs zum Sperren des verlorenen Programmierschlüssels erstellt werden, übernimmt der zum Sperren verwendete Schlüssel auch die Zylindersperrjobs, die dem verlorenen Programmierschlüssel ursprünglich zugewiesenen waren. Andere Zylinderprogrammierjobs, die ursprünglich dem verlorenen Programmierschlüssel zugewiesen waren, werden abgebrochen und unter **Arbeit » Zylinderprogrammierung** aufgeführt.

> **WARNUNG!**
> Auch wenn kein Zylinderprogrammierjob zum Sperren des verlorenen Programmierschlüssels erstellt wird, wird der verlorene Schlüssel in CWM standardmäßig zur **Liste der nicht berechtigten Schlüssel** für die betreffenden Zylinder hinzugefügt. Diese Information ist in CWM jedoch nicht sichtbar. Wenn die betreffenden Zylinder später neu programmiert oder ausgetauscht werden, werden die in CWM gespeicherten Informationen über nicht berechtigte Schlüssel für diese Zylinder übernommen, sodass der verlorene Programmierschlüssel gesperrt bleibt. Wenn der verlorene Programmierschlüssel später wieder als gefunden gemeldet wird, bleibt er daher in neu programmierten oder ausgetauschten Zylindern gesperrt.
>
> Informationen zum erneuten Autorisieren des gefundenen Programmierschlüssel in dieser Zylinderzugangsliste finden Sie in *Abschnitt 4.9.2 "Konfigurieren von Berechtigungen in Zylindern", Seite 83*.
>
> Um diese Standardeinstellung zu ändern, muss **Verlorene Schlüssel in Zylinder während des Berechtigungs-Updates unsichtbar blockieren** deaktiviert werden. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

10)
- Wurde für die Programmierung der Zylinder **KEIN** bestimmter Schlüssel ausgewählt, mit *Schritt 4* in *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64* fortfahren.
- Wenn ein bestimmter Schlüssel für die Programmierung der Zylinder ausgewählt wurde, die nachstehenden Anweisungen befolgen.

11) Die Informationsansicht des ausgewählten Benutzerschlüssels öffnen.

> **Tipp**
> Durch Klicken auf **Org.-Nr. Schlüssel** unter **Sperrschlüsselinformationen** wird direkt die Informationsansicht geöffnet.

12) Wechseln Sie zur Registerkarte **Programmierjobs** und bestätigen Sie, dass der Zylinderjob dem Schlüssel zugewiesen ist.

13)
- **Programmierung im lokalen PG**

  Den Benutzerschlüssel in den rechten Steckplatz des lokalen Programmiergeräts einführen und den Programmierschlüssel aus dem linken Steckplatz des lokalen Programmiergeräts entfernen.
- **Programmierung in einem Wand-Programmiergerät**

  Den Benutzerschlüssel in ein Wand-Programmiergerät einführen.

Der Zylinderprogrammierjob wird automatisch auf den Benutzerschlüssel geschrieben.

14) Jeden Zylinder mit dem Benutzerschlüssel neu programmieren.

15) Nach dem Programmieren der Zylinder die abgeschlossenen Zylinderjobs melden. Dazu den Benutzerschlüssel in eines der folgenden Geräte einführen:

- Rechter Steckplatz des lokalen PG (entfernen Sie den Programmierschlüssel aus dem linken Steckplatz)
- Wand-Programmiergerät

Wenn der Programmierschlüssel wiedergefunden wurde, dies durch Klicken auf **Als gefunden melden** in der Detailansicht melden.

6.11.10 Programmierschlüssel als defekt oder funktionsfähig melden

1) Programmierschlüssel suchen und Detailinformationen anzeigen.

   Siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*.

2) **Als Defekt melden**

   1. Auf **Als defekt melden** klicken.
   2. Auf **OK** klicken.

   Als funktionsfähig melden

   1. Auf **Als funktionsfähig melden** klicken.
   2. Auf **OK** klicken.

6.11.11 Ändern des PIN-Codes des Programmierschlüssels

HINWEIS!
Der PIN-Code muss 6 Zeichen aufweisen. Folgende Zeichen sind zulässig:

- Großbuchstaben (A, B, C, ...)
- Kleinbuchstaben (a, b, c, ...)
- Zahlen (0, 1, 2, ...)
- Minus (-)
- Unterstrich (_)
- Leerzeichen ( )
- Sonderzeichen (!, $, %, &, ...)
- Klammern ([,], {, }, (,), <, >)

Nur Buchstaben aus dem lateinischen Alphabet sind zulässig.

1) Ändern der PIN eines Normalprogrammierschlüssels mit einem Hauptprogrammierschlüssel oder Programmierschlüssel mit Super-Administrator-Rolle:

   a) **Verwaltung » Programmierschlüssel** auswählen.

   b) Programmierschlüssel in den rechten Port des lokalen PGs einführen.

c) Auf **Abfragen** klicken.

d) Neben dem Programmierschlüssel auf **Anzeigen** klicken.

e) Auf **Neue PIN einstellen** klicken.

f) **Hauptprogrammierschlüssel-PIN** eingeben.

g) Unter **Neue PIN** die neue PIN eingeben.

h) Unter **Neue PIN bestätigen** die neue PIN erneut eingeben.

2) Änderung der PIN des Normalprogrammierschlüssels, der auch zum Einloggen verwendet wurde:

a) **Einstellungen » Programmierschlüssel-Einstellungen** auswählen.

b) Auf **Programmierschlüssel-PIN ändern** klicken.

c) **Aktuelle PIN** eingeben.

d) **Neue PIN** eingeben.

e) Unter **Neue PIN bestätigen** die neue PIN eingeben.

3) Auf **OK** klicken.

6.11.12 Entsperren von Programmierschlüsseln

Der Programmierschlüssel wird nach 5 Anmeldeversuchen mit falscher PIN gesperrt und muss durch Eingabe des vom CLIQ-Händler bereitgestellten PUK-Codes entsperrt werden. Weitere Informationen siehe *Abschnitt 6.11.12.1 "Freigeben von Programmierschlüsseln mit dem PUK-Code", Seite 145*.

HINWEIS!
Nach 25 Eingabeversuchen mit dem falschen PUK wird der Programmierschlüssel unbrauchbar. In diesem Fall muss er durch einen neuen Programmierschlüssel ersetzt werden.

Wenn der Administrator nicht über den PUK-Code verfügt, kann der Halter des Hauptprogrammierschlüssels den Programmierschlüssel freigeben. Weitere Informationen siehe *Abschnitt 6.11.12.2 "Freigeben von Programmierschlüsseln mit dem Hauptprogrammierschlüssel", Seite 145*.

6.11.12.1 Freigeben von Programmierschlüsseln mit dem PUK-Code

1) **Einstellungen » Programmierschlüssel-Einstellungen** auswählen.

2) Auf **Programmierschlüssel freigeben** klicken.

3) **PUK** eingeben.

   Wenn der Administrator nicht über den PUK-Code verfügt, wenden Sie sich an einen Halter des Hauptprogrammierschlüssels.

4) **Neue PIN** eingeben.

5) **Neue PIN bestätigen** eingeben.

6) Auf **OK** klicken.

6.11.12.2 Freigeben von Programmierschlüsseln mit dem Hauptprogrammierschlüssel

Die folgende Prozedur kann nur von einem Halter eines Hauptprogrammierschlüssels ausgeführt werden.

1) Führen Sie den freizugebenden Programmierschlüssel in den rechten Schlitz des lokalen PG ein.
2) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.
3) Auf **Neue PIN einstellen** klicken.
4) Füllen Sie die Felder **Hauptprogrammierschlüssel-PIN**, **Neue PIN** und **Neue PIN bestätigen** für den gesperrten Programmierschlüssel aus.
5) Klicken Sie zum Speichern auf **OK**.

   Die neue PIN wird auf den Programmierschlüssel im rechten Schlitz des PG programmiert.

6.11.13 Automatischen Ereignislistenabruf für Programmierschlüssel aktivieren oder deaktivieren

Voraussetzungen:

- Der Administrator hat die Berechtigung, automatische Ereignislisten zu aktivieren.
- Ein Generation-2-Programmierschlüssel mit Firmware-Version 12.6 oder höher.
- Zur Aktivierung muss die Funktion **Genehmigungen** unter **Systemeinstellungen** deaktiviert werden.

1) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.
2) Die Einstellung **AUTOMATISCHER EREIGNISLISTENABRUF** lokalisieren.
3) - Einstellung für den automatischen Abruf von Ereignislisten aktivieren: Auf **Aktivieren** klicken.
   - Einstellung für den automatischen Abruf von Ereignislisten deaktivieren: Auf **Deaktivieren** klicken.
4) Wenn sich der Programmierschlüssel im lokalen Programmiergerät befindet, auf **Programmierschlüssel lokal aktualisieren** klicken.

6.11.14 Auflisten von Programmierschlüssel-Zertifikaten

1) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.
2) Register **Zertifikate** auswählen.

Das **Datum der letzten Nutzung** eines jeden Zertifikats wird angezeigt, wenn die Systemeinstellung **Letztes Anmeldedatum erfassen** aktiviert ist. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

6.11.15 Sperren von Programmierschlüssel-Zertifikaten

Das Sperren von Programmierschlüssel-Zertifikaten ist eine Sicherheitsfunktion und wird im Normalfall verwendet, wenn ein Computer eines Administrators mit einem Programmierschlüssel-Zertifikat gestohlen wird, sich der Programmierschlüssel jedoch noch in sicheren Händen befindet. In dem Beispiel mit dem gestohlenen Computer wird das installierte Programmierschlüssel-Zertifikat gesperrt und wieder angemeldet.

Zur Anmeldung eines Programmierschlüssel-Zertifikats siehe *Abschnitt 3.2 "Anmelden und Installieren von Programmierschlüssel-Zertifikaten", Seite 16*.

1) Den Programmierschlüssel suchen und die Detailansicht öffnen.

   Suche nach einem Programmierschlüssel und Anzeige von Detailinformationen siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*

   Abfrage des Programmierschlüssels im lokalen Programmiergerät und Anzeige der Detailinformationen siehe *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.

2) Register **Zertifikate** auswählen.

3) Bei allen zu sperrenden Zertifikaten auf **Zertifikat sperren** klicken.

   Tipp
   Um festzustellen, welches Zertifikat anzumelden ist, siehe Spalte **Datum der letzten Nutzung**. Im Zweifelsfall alle Zertifikate sperren und wieder anmelden.

   HINWEIS!
   Das Sperren des Zertifikats, das bei der Anmeldung an der Schließanlage verwendet wurde, ist nicht möglich.

4) Auf **OK** klicken.

6.11.16 Ersetzen des Hauptprogrammierschlüssels

Wenn ein Hauptprogrammierschlüssel verloren oder defekt ist, muss ein neuer Hauptprogrammierschlüssel bestellt werden.

Diese Anweisungen befolgen, um den neuen Hauptprogrammierschlüssel zu registrieren und den verlorenen bzw. defekten Hauptprogrammierschlüssel zu sperren.

Voraussetzungen:

- Folgendes steht zur Verfügung:
  - Ein neuer Hauptprogrammierschlüssel samt PIN-Code.
  - Ein Zertifikat für den neuen Hauptprogrammierschlüssel, wenn die DCS-Integration nicht aktiviert ist.
  - Eine Importdatei mit dem neuen Hauptprogrammierschlüssel.

1) Zertifikat für Hauptprogrammierschlüssel installieren.

Siehe *Abschnitt 5.2 "Installieren des Zertifikats für den Hauptprogrammierschlüssel", Seite 98*.

2) CWM für Wartung sperren.

   Siehe *Abschnitt 6.2 "Sperren des Systems zur Wartung", Seite 101*.

3) Die Datei mit dem neuen Hauptprogrammierschlüssel mit Hilfe des Service-Tools CLIQ Web Manager importieren. Zu weiteren Informationen siehe Betriebs- und Wartungsdokumentation für CWM.

   ACHTUNG!
   Unmittelbar nach dem Importieren der Datei mit dem neuen Hauptprogrammierschlüssel anmelden.

   Vor der ersten Anmeldung mit dem neuen Hauptprogrammierschlüssel kann nach wie vor der alte Hauptprogrammierschlüssel verwendet werden. Durch eine Anmeldung mit dem alten Hauptprogrammierschlüssel wird in diesem Fall der neue Hauptprogrammierschlüssel gesperrt.

4) Sich mit dem neuen Hauptprogrammierschlüssel bei CWM anmelden.

   CWM erkennt, dass mehrere Hauptprogrammierschlüssel aktiv sind, und sorgt dafür, dass der andere Hauptprogrammierschlüssel automatisch gesperrt und als verloren gekennzeichnet wird.

   Der alte Hauptprogrammierschlüssel kann weiterhin dazu verwendet werden, um in Zylindern, für die eine Berechtigung vorliegt, alle im Schlüssel bereits gespeicherten Zylinderprogrammierungs-Jobs auszuführen. CWM stellt hier die Möglichkeit zur Verfügung, Zylinderprogrammierungs-Jobs anzulegen, um die Berechtigung des gesperrten Hauptprogrammierschlüssels in Zylindern aufzuheben.

5) Auf **Ja, Jobs jetzt anlegen** oder **Nein, später entscheiden** klicken.

Um Jobs zur Aufhebung der Berechtigungen später anzulegen, mit dem neuen Hauptprogrammierschlüssel anmelden und in der Detailanzeige des gesperrten Hauptprogrammierschlüssels auf **Sperrlisten-Jobs erstellen** klicken.

6.11.17 Exportieren von Programmierschlüssel-Informationen

1) Die Programmierschlüssel suchen.

   Siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*.

2) In den Suchergebnissen durch Aktivieren der Kontrollkästchen die Programmierschlüssel auswählen, deren Daten exportiert werden sollen.

3) Auf **In CSV-Datei exportieren** klicken.

4) Im Pop-up-Fenster für den Dateidownload auf **Speichern** klicken.

   Eine CSV-Datei wird in den Ordner **Downloads** heruntergeladen.

   HINWEIS!
   Damit die Excel-Datei korrekt geöffnet werden kann, muss das Trennzeichen entsprechend den regionalen Einstellungen eingestellt sein. Ändern des Trennzeichens siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

6.12 Ändern der Zylindergruppe von Zylindern

HINWEIS!
Bestimmte Zylinder in der Zylinderliste können einen möglichen freien Ausgang in einem Wand-Programmiergerät darstellen, der mit einem externen Gerät wie einem Relaiscontroller verbunden ist. In einem solchen Fall können dies betreffenden Zylinder nicht in eine andere Zylindergruppe verschoben werden.

Weitere Informationen zum potentialfreien Ausgang erhalten Sie von Ihrem örtlichen CLIQ-Händler.

1) Zylinder suchen und Detailinformationen anzeigen.

   Siehe *Abschnitt 4.4.1 "Suchen nach Zylindern", Seite 57*.

2) Auf **Gruppenänderung** klicken.
3) In der Zeile mit der entsprechenden Zylindergruppe auf **Auswählen** klicken.
4) Eine **Priorität** auswählen. Dringende Jobs sollten hohe Priorität haben.

Die Zylindergruppe kann für mehrere Zylinder gleichzeitig geändert werden. Die Zylinder in der Liste der Suchergebnisse auswählen und auf **Gruppe ändern...** klicken.

6.13 Anzeigen des Systemstatus

1) **Verwaltung » Systemstatus** auswählen.
2) Zur Anzeige der Online- oder Offline-Status der Remote-Programmiergeräte, des Remoteservers und des E-Mail-Servers die Registerkarte **Aktueller Status** auswählen.
3) Zur Anzeige der vergangenen Änderungen in den Online- oder Offline-Status der Remote-Programmiergeräte, des Remoteservers und des E-Mail-Servers die Registerkarte **Historie** auswählen.

   Anzeige vergangener Ereignisse zwischen bestimmten Tagen:

   a) Bei **Ereignisse anzeigen von** ein Startdatum angeben.
   b) Bei **Ereignisse anzeigen bis** ein Enddatum angeben.
   c) Auf **Suchen** klicken.

6.14 Anzeigen grundlegender Statistikdaten

CWM verfügt über eine integrierte Statistikfunktion, die grundlegende Statistikdaten zur Schließanlage bereitstellt, wie Anzahl der Zylinder und Schlüssel.

Voraussetzung:

- Dem Administrator wurden Anzeigeberechtigung für **Statistik** gewährt.

1) **Verwaltung » Statistik** auswählen.
2) Die Seite **Statistik** wird geöffnet.
3) Optional: Klicken Sie je nach Bedarf auf **Statistik ausdrucken** oder **Statistik exportieren**.

6.15 Firmware-Upgrade

Die Firmwareversion kann in der Detailansicht jedes Geräts überprüft werden.

6.15.1 Upgrade der Firmware in Remote-PGs

> **HINWEIS!**
> Dieses Kapitel gilt nicht für mobile CLIQ Connect-Programmiergeräte.

Um ein Upgrade eines Remote-Programmiergeräts durchzuführen, muss Firmware für CWM bereitgestellt werden. Bei Verwendung der DCS-Integration werden die Firmwaredateien automatisch von DCS abgerufen. Andernfalls geschieht dies durch Hochladen einer lokalen Firmwaredatei, die vom lokalen CLIQ-Händler zur Verfügung gestellt wird. Nach dem Import zu CWM kann die Firmware des Remote-Programmiergeräts entweder über CWM oder über einen USB-Speicherstick aufgerüstet werden.

Der Prozess zum Aufrüsten der Firmware des Remote-Programmiergeräts hängt von der DCS-Integration ab:

- Zum Verwenden der DCS-Integration mit *Schritt 2* beginnen.
- Zum Verwenden einer lokalen Firmwaredatei mit *Schritt 1* beginnen.

1) Lokale Firmwaredatei ohne DCS-Integration hochladen und importieren:
   a) Neue Firmware lokal auf dem Computer speichern.
   b) **Verwaltung » Firmware** auswählen.
   c) Auf **Auswählen** klicken, um die auf dem Computer gespeicherte neue Firmware zu suchen.
   d) Auf **Öffnen** klicken.
   e) Zum Hochladen der Firmware in CWM auf **Firmware hochladen** klicken.

      Die Firmware wird hochgeladen.
   f) Klicken Sie auf **Firmware importieren**, um die hochgeladene Firmware zu importieren.

      Nach erfolgreicher Durchführung erscheint in einem neuen Fenster eine Zusammenfassung der importierten Firmware.
2) **Systeminfo » Remote-PGs** auswählen.
3) Auf die Zeile mit dem Remote-Programmiergerät klicken, bei dem das Upgrade durchgeführt werden soll.
4) Wählen Sie das Register **Firmware** aus und wählen Sie die Version im Bereich **FIRMWARE** oder **BOOTLADER-FIRMWARE** aus.

> **HINWEIS!**
> Der Bereich **BOOTLADER-FIRMWARE** wird für Wand-Programmiergeräte der Generation 2 nicht angezeigt.

5) • Upgrade der Firmware für Online-Remote-PGs über CWM:

   a) Wählen Sie die Firmware-Version aus und klicken Sie auf **Anwenden**.

   b) Aktivieren Sie die Aufrüstung.

      • Mobile CLIQ-Programmiergeräte:

        Einen Benutzerschlüssel einführen, um das mobile CLIQ-Programmiergerät einzuschalten.

      • Wand-PGs:

        Die Firmware wird beim nächsten Heartbeat-Signal (wenn sich das PG das nächste Mal mit dem Remoteserver verbindet) aktualisiert.

• Firmware-Upgrade für Offline-Remote-Programmiergeräte über einen USB-Speicherstick:

> **HINWEIS!**
> Der USB-Speicherstick muss im FAT32-Dateisystemformat formatiert sein. Für Wand-Programmiergeräte der Generation 1 und mobile Programmiergeräte wird eine Speichergröße von 8–16 GB empfohlen. Für Wand-Programmiergerät der Generation 2 gilt keine Einschränkung in Bezug auf die Speichergröße. Der USB-Speicherstick darf keine anderen Dateien enthalten.

   a) Wählen Sie die Firmware-Version aus und klicken Sie auf **In Datei speichern**, um die Datei im Stammverzeichnis des USB-Speichersticks zu speichern.

   b) Den USB-Speicherstick mit einem geeigneten USB-Kabel am Remote-Programmiergerät anschließen (siehe *Abschnitt 6.5.8 "Konfigurieren von mobile Programmiergeräten", Seite 119* oder *Abschnitt 6.5.7 "Konfigurieren von Wand-Programmiergeräten", Seite 112*).

      Die Aufrüstung wird automatisch initiiert.

   c) Aktivieren Sie die Aufrüstung.

      • Mobile CLIQ-Programmiergeräte:

        Einen Benutzerschlüssel einführen, um das mobile CLIQ-Programmiergerät einzuschalten.

      • Wand-PGs:

        Die Aufrüstung wird automatisch initiiert.

Das Firmware-Upgrade ist beendet, wenn die Download-Anzeige-LED nicht mehr blinkt, sondern ständig leuchtet. Informationen zu Anzeigen des Remote-Programmiergeräts finden Sie unter *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und*

mobilen Programmiergeräten", Seite 212 und *Abschnitt 9.5.2 "Anzeigen eines Wand-Programmiergeräts (Generation 2)", Seite 213*.

6.15.2 Firmware-Upgrade für mobile CLIQ Connect-Programmiergeräte durchführen

1) Verbinden Sie das mobile CLIQ Connect-Programmiergerät mit einem Micro-USB-Kabel mit dem Clientcomputer, auf dem der CLIQ Connect-PC installiert ist.
2) CLIQ Connect-PC erkennt die Firmware-Version des mobilen CLIQ Connect-Programmiergeräts automatisch.

   Ist eine neuere Version verfügbar, empfiehlt CLIQ Connect-PC ein Firmware-Upgrade.
3) Hierfür die Anweisungen auf dem Display befolgen.

6.15.3 Upgrade der Firmware in Schlüsseln

Um ein Upgrade eines Schlüssels durchzuführen, muss CWM mit der Firmware versehen werden. Bei Systemen mit DCS-Integration werden die Firmware-Dateien automatisch von DCS abgerufen. Bei Systemen ohne DCS-Integration geschieht dies durch Hochladen einer lokalen Firmware-Datei die vom lokalen CLIQ-Händler zur Verfügung gestellt wird. Nach dem Import wird die Firmware über ein Remote-Programmiergerät über CWM aktualisiert.

Tabelle 1. Typ des zu verwendenden Remote-Programmiergeräts bei Schlüssel-Upgrades

Schlüsselversion	Remote-Programmiergerät	Firmwareversion des Remote-Programmiergeräts
Benutzerschlüssel, Generation 1	Wand-Programmiergerät (Generation 1)	
Benutzerschlüssel, Generation 2	Wand-Programmiergerät (Generation 1 oder 2) oder mobiles CLIQ-Programmiergerät	
Programmierschlüssel, Generation 2, mit Firmware 12.0 oder höher	Wand-Programmiergerät (Generation 1 oder 2) oder mobiles CLIQ-Programmiergerät	Firmware 6.3 oder höher für Wand-Programmiergerät oder mobiles CLIQ-Programmiergerät
Programmierschlüssel, Generation 2, mit Firmware unter 12.0	Kein Upgrade über CWM möglich	
Programmierschlüssel, Generation 1	Kein Upgrade über CWM möglich	

Die Schlüsselgeneration ist in der Detailansicht des Benutzerschlüssels und den Ansichten des Programmierschlüssels sichtbar. Siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*, *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*, *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138* oder *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137*.

Der Prozess zum Aufrüsten der Schlüsselfirmware variiert je nach DCS-Integration:

- Bei Schließanlagen mit DCS-Integration weiter bei *Schritt 4*.
- Bei Schließanlagen ohne DCS-Integration weiter bei *Schritt 1*.

1) Neue Firmware lokal auf dem Computer speichern.

2) **Verwaltung » Firmware** auswählen.
3) Importieren Sie die neue Firmware:
   a) Auf **Auswählen** klicken, um die auf dem Computer gespeicherte neue Firmware zu suchen.
   b) Auf **Öffnen** klicken.
   c) Zum Hochladen der Firmware in CWM auf **Firmware hochladen** klicken.

      Nach erfolgreicher Durchführung erscheint eine Zusammenfassung der hochgeladenen Firmware in einem neuen Fenster.
   d) Auf **Firmware importieren** klicken.

> **HINWEIS!**
> Damit ein Upgrade von Generation-1-Schlüsseln durchgeführt werden kann, muss Folgendes importiert werden:
>
> - Bootloader-Firmware für Wand-Programmiergerät der Generation 1
> - Firmware für Wand-Programmiergerät der Generation 1, Version 2.11 oder höher
> - Schlüssel-Updater-Firmware für Wand-Programmiergerät der Generation 1, Version 2.11 oder höher
> - Die neue Schlüsselfirmware, je eine für jeden Schlüsseltyp, für den ein Upgrade durchgeführt werden soll.

> **HINWEIS!**
> Bei Systemen mit aktivierter DCS-Integration werden die Firmware-Dateien automatisch von DCS abgefragt und zusammen mit der importierten Firmware, die zur Aktivierung bereit ist, aufgelistet.

4) Upgrade von Benutzerschlüsseln Generation 1:

> **HINWEIS!**
> Wand-Programmiergeräte der Generation 2 unterstützen keine Firmware-Upgrades für Benutzerschlüssel der Generation 1.

   a) **Systeminfo » Remote-PGs** auswählen.
   b) Das für das Upgrade zu verwendende Wand-Programmiergerät suchen und Detailinformationen anzeigen.

      Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

      Neben anderen Informationen werden die aktuelle Bootloader-Firmware und die Firmware des Wand-Programmiergeräts angezeigt.
   c) Wenn ein Upgrade der Bootloader-Firmware und Firmware des Wand-Programmiergeräts erforderlich ist, siehe *Abschnitt 6.15.1 "Upgrade der Firmware in Remote-PGs", Seite 150*.

d) Schlüssel-Upgrades im Wand-Programmiergerät aktivieren, siehe *Abschnitt 6.5.11 "Schlüssel-Upgrades in Remote-Programmiergeräten aktivieren und deaktivieren", Seite 125*.

Die Schlüssel-Updater-Firmware wird zum Wand-Programmiergerät gesendet. Wenn das Wand-Programmiergerät die neue Firmware geladen und einen Neustart durchgeführt hat, kann das Upgrade von Schlüsseln durchgeführt werden.

e) Für jeden Nutzerschlüssel, für den ein Upgrade durchgeführt werden soll:

- Schlüssel in das Schlüssel-Updater-Wand-Programmiergerät einstecken.

  Zunächst werden anstehende Remote-Updates für den Schlüssel ausgeführt, anschließend wird der Upgrade mit der neuen Firmware durchgeführt.

  HINWEIS!
  Die Schlüsselkonfiguration einschließlich aller Zugangsrechte wird beim Firmware-Upgrade gelöscht. Sie wird durch Durchführung eines Remote-Updates des Schlüssels nach dem Upgrade wiederhergestellt.

  Das Wand-Programmiergerät zeigt an, dass die Updates beendet sind. Informationen zu Anzeigen des Remote-Programmiergeräts finden Sie unter *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen Programmiergeräten", Seite 212*.
- Schlüssel aus dem Wand-Programmiergerät ziehen.

  Jetzt wird ein Remote Update Job zur Wiederherstellung der Schlüsselkonfiguration in CWM angelegt. Dieser steht nach ein paar Minuten zur Verfügung.
- Schlüssel zur Wiederherstellung der Schlüsselkonfiguration in beliebiges Remote-Programmiergerät einstecken.

  Der Upgrade-Prozess ist jetzt für diesen Schlüssel beendet.

f) Schlüssel-Upgrades im Wand-Programmiergerät deaktivieren, siehe *Abschnitt 6.5.11 "Schlüssel-Upgrades in Remote-Programmiergeräten aktivieren und deaktivieren", Seite 125*.

Alle anstehenden Upgrade-Jobs für die Schlüsselfirmware werden abgebrochen. Die normale Wand-Programmiergerät-Firmware wird zum Wand-Programmiergerät gesendet, und nach dem Laden der neuen Firmware und dem Neustart arbeitet das Gerät wieder als normales Wand-Programmiergerät.

5) Upgrade von Benutzerschlüsseln Generation 2 oder von Programmierschlüsseln:

a) **Systeminfo » Remote-PGs** auswählen.

b) Anzeige der Detailinformationen des Remote-Programmiergerät, das für das Upgrade genutzt werden soll.

Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

- Falls ein Upgrade der Firmware im Remote-Programmiergerät erforderlich ist, siehe *Abschnitt 6.15.1 "Upgrade der Firmware in Remote-PGs", Seite 150*.

c) Auf der Registerkarte **Einstellungen** die Schlüssel-Upgrades im Remote-Programmiergerät aktivieren. Siehe *Abschnitt 6.5.11 "Schlüssel-Upgrades in Remote-Programmiergeräten aktivieren und deaktivieren", Seite 125*

d) **Verwaltung » Firmware** auswählen.

e) Register **Importierte Benutzerschlüssel-Firmware** oder **Importierte Programmierschlüssel-Firmware** auswählen, je nachdem, ob Benutzer- oder Programmierschlüssel aktualisiert werden.

f) Zur Durchführung des Schlüssel-Upgrades die importierte Firmware mit **Anwenden** bestätigen.

Es wird automatisch ein Remote-Job angelegt.

HINWEIS!
Sollte die Schaltfläche **Anwenden** bei der importierten Firmware ausgegraut sein, liegen anstehende Remote-Upgrades für die vorhandene Firmware vor. Dies wird durch ein Symbol in der Spalte **Status** angezeigt. Wie folgt vorgehen:

- Bei der Firmware mit anstehenden Remote-Upgrades auf **Abbrechen** klicken.
- Auf **OK** klicken.
- Bei der neuesten Firmware auf **Anwenden** klicken.

HINWEIS!
Die Reihenfolge von *Schritt 5 c* und *Schritt 5 f* kann umgekehrt werden. Es ist möglich, zuerst die importierte Firmware anzuwenden und anschließend Schlüssel-Upgrades für eine Auswahl von Remote-PGs zu aktivieren.

g) Upgrade für jeden Schlüssel in einem Remote-Programmiergerät durchführen:

HINWEIS!
Bei Benutzerschlüsseln werden zunächst anstehende Remote-Updates für den Schlüssel ausgeführt, anschließend wird das Upgrade mit der neuen Firmware durchgeführt.

- Über **Wand-Programmiergerät** oder **Mobiles CLIQ-Programmiergerät**

  Führen Sie den Schlüssel in die Geräte ein, die für das Schlüssel-Upgrade aktiviert wurden, oder verbinden Sie den Schlüssel damit.

  Das Remote-Programmiergerät zeigt an, dass die Updates beendet sind. Informationen zu Anzeigen des Remote-Programmiergeräts finden Sie unter *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen*

Programmiergeräten", Seite 212 oder *Abschnitt 9.5.2 "Anzeigen eines Wand-Programmiergeräts (Generation 2)", Seite 213*.

- Über das **Bluetooth-Protokoll in der CLIQ Connect-App**

  Voraussetzungen:

  – Die Firmwareversion von CLIQ Connect muss 4.1 oder höher sein.
  – Die Firmwareversion des Schlüssels muss 16.3.3 oder höher sein.

  Ein Upgrade der Firmware für Schlüssel mit älterer Firmware ist mit einem Wand-Programmiergerät möglich.

  Verbinden Sie den Schlüssel mit CLIQ Connect.

  HINWEIS!
  Wenn ein Upgrade der Firmware über CLIQ Connect und eine BLE-Verbindung gestartet wird, muss es mit der gleichen Methode abgeschlossen werden (d. h. BLE-Verbindung mit einem mobilen Gerät). Während des Zwischenstadiums des Upgrades ist der Schlüssel nicht funktionsfähig; er öffnet keine Schlösser und reagiert in keinem Programmiergerät.

6.15.4 Aktualisieren der Schlüsselfirmware-Informationen in der CWM-Datenbank

Beim Aufrüsten der Schlüsselfirmware aktualisiert die CWM-Datenbank automatisch die Firmware-Informationen des Schlüssels. Informationen zur Firmware des Schlüssels können auf in der Ansicht **Schlüsselinformationen** angezeigt werden.

Wenn die Schlüsselfirmware jedoch außerhalb des CWM-Systems aufgerüstet wird, zum Beispiel im Werk, wird die CWM-Datenbank nicht mit den neuesten Informationen zur Schlüsselfirmware aktualisiert.

Gehen Sie wie folgt vor, um die Version der Schlüsselfirmware in der CWM-Datenbank und im physischen Schlüssel zu synchronisieren:

- Fragen Sie den aufgerüsteten Schlüssel ab und rufen Sie den Schlüsselstatus im lokalen PG ab. Weitere Informationen hierzu finden Sie in *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.
- Führen Sie den aufgerüsteten Schlüssel in ein Remote-Programmiergerät ein.

  HINWEIS!
  Nur Schlüssel der Generation 2 mit Firmwareversion 12.3 oder höher können die Schlüsselfirmware-Informationen über ein Remote-Programmiergerät aktualisieren.

HINWEIS!

Nur Programmierschlüssel:

Wenn ein Programmierschlüssel eine ältere Firmwareversion hat als die in der CWM-Datenbank angegebene Version, wird die CWM-Datenbank auf der Firmware nicht aktualisiert. Diese Situation kann auch zu Fehlern bei der Verwendung des Programmierschlüssels führen.

6.16 Importieren von Erweiterungen

Um eine Erweiterung zu importieren, muss CWM mit einer Erweiterungsimportdatei versehen werden. Dies erfolgt durch Hochladen einer lokalen Erweiterungsimportdatei.

Bei Verwendung der DCS-Integration werden die Erweiterungsimportdateien automatisch aus DCS abgerufen. Den Erweiterungsimportprozess ab *Schritt 2* durchführen.

Das Abrufen der Daten von DCS kann auch durch manuelles Klicken auf eine Schaltfläche erzwungen werden. Nach dem Hochladen muss der Erweiterungsimport aktiviert werden.

Voraussetzung:

- Wenn neu hinzugefügte Zylinder die verlorenen Schlüssel in der Anlage sperren sollen, **Verlorene Schlüssel in neuen Zylindern während des Erweiterungsimports blockieren** unter **Systemeinstellungen** aktivieren. Wenn diese Option aktiviert ist, erstellt die Anlage automatisch Zylinderprogrammierjobs, mit denen verlorene Schlüssel beim Aktivieren der Erweiterungsimportdateien für diese Zylinder gesperrt werden. Weitere Informationen hierzu finden Sie in *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

1) Geben Sie eine Erweiterungsimportdatei für CWM an.

Lokale Erweiterungsimportdatei hochladen

1. **Verwaltung » Erweiterungsimport » Erweiterungsimportdatei(en) hochladen oder holen** auswählen.
2. Auf **Auswählen...** klicken und die lokal auf dem Computer gespeicherte Erweiterungsimportdatei suchen. Erweiterungsimportdateien haben die Endung ".cws".
3. Auf **Öffnen** klicken.
4. Auf **Hochladen** klicken. Die Erweiterungsimportdatei wird zum Web Manager Server hochgeladen und validiert.

Erweiterungsimportdatei manuell von DCS abrufen

1. **Verwaltung » Erweiterungsimport » Erweiterungsimportdatei(en) hochladen oder holen** auswählen.
2. Auf **Erweiterungsimportdatei(en) holen** klicken.

   Es wird ein Statushinweis zum Abfragevorgang angezeigt.

2) Aktivieren eines hochgeladenen oder abgerufenen Erweiterungsimports:

> **HINWEIS!**
> Die Verarbeitung einer hochgeladenen oder abgefragten Erweiterungsimportdatei kann etwas Zeit in Anspruch nehmen. Sobald ein Erweiterungsimport zur Aktivierung bereit ist, wird auf der CWM-Startseite eine entsprechende Meldung angezeigt. Die Meldung wird außerdem per E-Mail an alle Administratoren gesendet, die Rollen mit Wartungsberechtigungen haben.

a) **Verwaltung » Erweiterungsimport » Erweiterungsimport aktivieren** auswählen.

Ein Hinweis über verfügbare Erweiterungsimporte und mit Informationen über die Anzahl der zu aktivierenden Schlüssel, Schlüsselgruppen, Zylinder, Zylindergruppen und Remote-Programmiergeräte wird angezeigt.

b) Optional: Um ausführlichere Informationen zu Erweiterungselementen zu erhalten, klicken Sie für jedes Element auf **In CSV-Datei exportieren**. Daraufhin wird eine CSV-Datei erstellt, in der Sie die Details überprüfen können.

c) Auf **Erweiterungsimport aktivieren** klicken, um die verfügbaren Erweiterungen zu aktivieren.

> **HINWEIS!**
> Nur hochgeladene bzw. abgefragte Erweiterungsimporte, die neue Daten enthalten, lassen sich aktivieren. Alte oder identische Daten können nicht aktiviert werden.

Nach der Aktivierung wird auf der CWM-Startseite eine Bestätigungsmeldung angezeigt.

Wenn die Funktion **Verlorene Schlüssel in neuen Zylindern während des Erweiterungsimports blockieren** aktiviert ist, werden Zylinderprogrammierjobs erstellt. Informationen zum Programmieren der Zylinder finden Sie in *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64*.

7 CLIQ-Hardware

7.1 CLIQ-Architektur

Die grundlegende Architektur eines CLIQ-Systems zeigt *Abbildung 1 "CLIQ-Architektur", Seite 159*

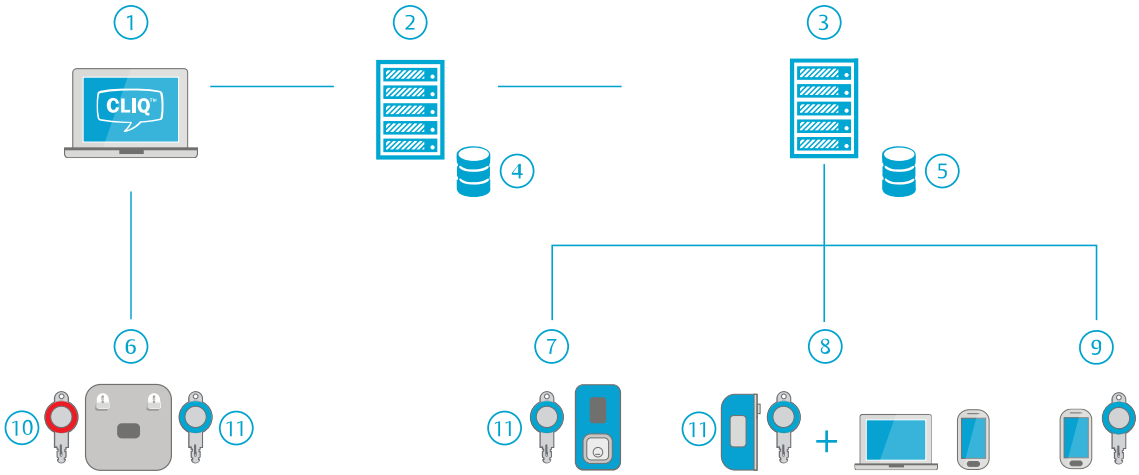


Abbildung 1. CLIQ-Architektur

1. **CWM Client**. Dabei handelt es sich um einen Rechner mit Internet-Browser, der von einem Administrator zur Verwaltung einer Schließanlage genutzt wird. An den Server können mehrere Clients angeschlossen sein.

2. **Web Manager Server**. Auf diesem Server läuft die CWM-Software. An diesen Server ist die CLIQ-Datenbank angeschlossen, die Informationen zu allen CLIQ-Elementen, Zugangslisten, Ereignislisten usw. enthält.

3. **Remote-Server**. Bei einem Remote-System wird über den Remote Server der standortferne Update der Schlüssel abgewickelt. Die Schlüssel-Update-Jobs werden vom Web Manager Server zum Remote Server übertragen. Die Update-Jobs werden in einer Datenbank gespeichert, bis sie von dem Remote-Programmiergerät ausgeführt werden.

4. **Datenbank**. Datenbank des Web Manager Server.

5. **Datenbank**. Datenbank des Remote Server.

6. **Lokale PG**. Diese sind mit dem Web Manager Client verbunden und werden vom Administrator für die Anmeldung an CWM (mit einem Programmierschlüssel) und das lokale Programmieren von Schlüsseln verwendet. Weitere Informationen siehe *Abschnitt 7.4.1 "Lokale PGs", Seite 164*.

7. **Wand-Programmiergeräte**. Eine Art Remote-Programmiergerät. Durch Einstecken eines Schlüssels in ein Wand-Programmiergerät werden die in der Datenbank des Remote-Servers gespeicherten Update-Jobs ausgeführt. Siehe *Abschnitt 7.4.2 "Remote-Programmiergeräte", Seite 165*.

8. **Mobile CLIQ-Programmiergeräte** und **mobile CLIQ Connect-Programmiergeräte**. Zwei Arten von Remote-Programmiergeräten. Die in der Datenbank des Remote-Servers gespeicherten Jobs für Schlüssel-Updates werden ausgeführt, wenn ein Schlüssel in ein mobiles CLIQ-Programmiergerät oder in ein mobiles CLIQ Connect-Programmiergerät eingesteckt wird. Siehe *Abschnitt 7.4.2 "Remote-Programmiergeräte", Seite 165*.

9. **CLIQ Connect-Schlüssel**. Ein Schlüsseltyp. Der CLIQ Connect-Schlüssel kann ohne ein Programmiergerät aktualisiert werden, indem der Schlüssel mithilfe von CLIQ Connect mit einem mobilen Gerät verbunden wird. Weitere Informationen hierzu finden Sie im separaten Handbuch zu CLIQ Connect.

10. **Programmierschlüssel**. Siehe *Abschnitt 7.2.4 "Programmierschlüssel", Seite 161*.

11. **Benutzerschlüssel**. Siehe *Abschnitt 7.2.3 "Nutzerschlüssel", Seite 160*.

7.2 Schlüssel

7.2.1 Überblick über die Schlüssel

Die CLIQ-Schlüssel sind elektromechanische Schlüssel, die Elektronik und eine Batterie enthalten. Jeder CLIQ-Schlüssel ist programmiert und kann mit der CWM-Software gesteuert und verwaltet werden.

Bei den Schlüsseln handelt es sich entweder um Systemschlüssel, auch als **Programmierschlüssel** bezeichnet, die von den Administratoren der Schließanlage verwendet werden, oder um **Benutzerschlüssel**, die von Mitarbeitern und Besuchern verwendet werden.

7.2.2 CLIQ Connect-Schlüssel

Manche Programmierschlüssel und Benutzerschlüssel können per Bluetooth über ein Mobiltelefon oder Tablet aktualisiert werden. Diese Schlüssel werden als **CLIQ Connect-Schlüssel** bezeichnet. Schlüssel ohne diese Funktion können nur per PG aktualisiert werden.

7.2.3 Nutzerschlüssel

Nutzerschlüssel werden von Mitarbeitern und Besuchern für den Zugang zu den Einrichtungen verwendet. Es gibt verschiedene Arten von Nutzerschlüsseln.

	**Mechanischer Schlüssel**	Herkömmlicher Schlüssel ohne elektronische Komponenten. Kann mit CWM verwaltet, jedoch nicht mit CLIQ-Zylindern genutzt werden.
	**E1-Schlüssel**	Elektromechanischer Schlüssel, mit dem mechanische Zylinder mit kompatibler Schließung geöffnet werden können und der bei Einrichtung entsprechender Berechtigungen CLIQ-Zylinder auf Grundlage der Zylinderzugangsliste öffnen kann (siehe *Abschnitt 8.1.2 "Elektronische Berechtigung", Seite 168*).
	**E2-Schlüssel**	Zusätzlich zu den oben genannten besitzt dieser Schlüsseltyp außerdem eine Quarzuhrfunktion und lässt sich so programmieren, dass er in bestimmten Datumsbereichen aktiv ist und eine Verlängerung erfordert (siehe *Abschnitt 8.1.4 "Schlüsselgültigkeit", Seite 170*). Er kann auch so programmiert werden, dass er auf Basis eines Zeitplans Zugang zu Zylindern hat (siehe *Abschnitt 8.1.8 "Schlüssel-Zeitpläne", Seite 175*). Schlüssel von diesem Typ können auch Ereignislisten speichern (siehe *Abschnitt 8.6 "Ereignislisten", Seite 190*).
	**E3-Schlüssel**	Zusätzlich zu den oben genannten kann dieser Schlüsseltyp auch eine Schlüsselzugangsliste von Zylindern und Zylindergruppen, die mit diesem Schlüssel geöffnet werden können, abspeichern (siehe *Abschnitt 8.1.2 "Elektronische Berechtigung", Seite 168*). Dies ist bei Remote-Systemen nützlich, da es die Zugangssteuerung über Schlüssel ermöglicht, die in Remote-PGs problemlos aktualisiert werden können.

Ein E3-Schlüssel und ein E2-Schlüssel sind entweder ein **CLIQ Connect-Schlüssel** (rechtes Symbol) oder nicht (linkes Symbol). E1-Schlüssel sind niemals CLIQ Connect-Schlüssel. Weitere Informationen siehe *Abschnitt 7.2.2 "CLIQ Connect-Schlüssel", Seite 160*.

Siehe auch *Abschnitt 8.1 "Berechtigungsprinzipien", Seite 168*.

7.2.4 Programmierschlüssel

Systemschlüssel, auch als **Programmierschlüssel** bezeichnet, sind Schlüssel, die von den Administratoren der Schließanlage verwendet werden. Programmierschlüssel öffnen keine Zylinder, sondern werden nur zum Zugriff auf CWM und zur Programmierung von Zylindern verwendet.

Es gibt zwei Arten von Programmierschlüsseln: **Hauptprogrammierschlüssel** und **normale Programmierschlüssel**.

Hauptprogrammierschlüssel

Der Hauptprogrammierschlüssel wird vom Superadministrator zur Verwaltung der Schließanlage verwendet. Es gibt nur einen Hauptprogrammierschlüssel pro Schließanlage, und dieser muss an einem sicheren Ort aufbewahrt werden.

Der Hauptprogrammierschlüssel besitzt die folgenden einzigartigen Berechtigungen, die keinem anderen Programmierschlüssel zugewiesen werden können:

- Ändern des PIN-Codes anderer Programmierschlüssel.
- Ausführen von Zylinderprogrammierungs-Jobs, die aktualisierten Zugang für Programmierschlüssel umfassen.
- Melden eines verlorenen Programmierschlüssels als gefunden.

Sub-Hauptprogrammierschlüssel

Sub-Hauptprogrammierschlüssel werden von Administratoren verwendet. In einer Anlage kann es mehrere Sub-Hauptprogrammierschlüssel geben.

Ein Sub-Hauptprogrammierschlüssel hat im Vergleich zum Hauptprogrammierschlüssel eine eingeschränkte Funktionalität. So können beispielsweise keine Erstimporte aktiviert und bestimmte Systemeinstellungen nicht konfiguriert werden.

Normalprogrammierschlüssel

Normale Programmierschlüssel werden an die Administratoren ausgegeben. Normale Programmierschlüssel können so konfiguriert werden, dass sie Zugriff auf bestimmte Funktionen in CWM ermöglichen. Sie können außerdem für andere Funktionen gesperrt werden. Siehe *Abschnitt 8.8 "CWM-Rollen und Administratorrechte", Seite 192*).

Es gibt eine spezielle Version des Normalprogrammierschlüssels die die Berechtigung zur Durchführung einer Zylinder-Reprogrammierung besitzt. Andere normale Programmierschlüssel verfügen nicht über diese Berechtigung. Die Berechtigung zur Reprogrammierung wird werksseitig im Schlüssel programmiert und lässt sich nicht ändern. Ob ein Normalprogrammierschlüssel die Berechtigung zur Reprogrammierung hat, steht in den Detailinformationen des Programmierschlüssels. Siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137* oder *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*.

Jeder normale Programmierschlüssel ist ebenfalls entweder ein **CLIQ Connect-Schlüssel** (rechtes Symbol) oder nicht (linkes Symbol). Weitere Informationen siehe *Abschnitt 7.2.2 "CLIQ Connect-Schlüssel", Seite 160*.

HINWEIS!
Bei der Beschreibung von Funktionen, die sowohl für den Hauptprogrammierschlüssel als auch für normale Programmierschlüssel gelten, wird der Begriff **Programmierschlüssel** verwendet.

Programmierschlüssel haben je nach Firmware die Fähigkeit zur **Zylindergruppenprogrammierung**. Nur Programmierschlüssel mit dieser Fähigkeit können Zylinderprogrammierungs-Jobs ausführen, die eine Änderung der Zylindergruppe eines Zylinders umfassen. Ob ein Programmierschlüssel die Fähigkeit zur Zylindergruppenprogrammierung hat, steht in den Detailinformationen des Programmierschlüssels. Siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137* oder *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*. In Systemen, die ursprünglich als Zylindergruppensysteme geliefert wurden, haben alle Programmierschlüssel diese Fähigkeit.

Um einen Programmierschlüssel in CWM zu verwenden, muss im CWM-Client ein eindeutiges Zertifikat installiert sein (siehe *Abschnitt 2.1 "Einrichtung von CWM-Clients - Überblick", Seite 13*). Jeder Programmierschlüssel hat einen eigenen PIN- und PUK-Code.

7.2.5 Schlüsselgenerationen

Es gibt zwei Schlüsselgenerationen:

- Generation 1
- Generation 2

Die Generation eines Schlüssels wird von dessen Hardware bestimmt. Generation-2-Schlüssel sind neuer und weiterentwickelt.

Alle Generation-2-Schlüssel sind rückwärtskompatibel zu Generation-1-Schlüsseln.

Die Schlüsselgeneration ist in der Detailanzeige des Schlüssels zu sehen, siehe *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36* oder *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35*.

7.3 Zylinder

Es gibt zwei verschiedene Zylindertypen - mechanische und elektronische. Elektronische Typen können Zugangsrechte für Schlüssel und Schlüsselgruppen sowie Ereignislistendaten speichern.

Zylinder können ein- oder doppelseitig sein. Bei doppelseitigen Zylindern können die Seiten vom gleichen Typ sein, müssen aber nicht.

Bei der Auflistung von Zylindern werden folgende Symbole verwendet:

- Elektronischer Zylinder
- Mechanischer Zylinder
- Doppelzylinder (hier verwendetes Beispiel: A-Seite elektronisch; B-Seite mechanisch)

Abbildung 2. CLIQ-Zylinder

Ein Zylinder kann in unterschiedlichen Schlössern, Türen, Vorhängeschlössern, Schranktüren usw. eingebaut werden. Auf jedem Zylinderkörper ist eine Kennnummer vermerkt.

In einem elektronischen Zylinder sind folgende Daten gespeichert:

- Berechtigte Schlüsselgruppen und Schlüsselhalter
- Gesperrte Schlüssel
- Normale Ereignislisten: Ereignislisten für Schlüsseleinführungen mit Schlüsseln der gleichen Schließanlage
- Fremde Ereignislisten: Ereignislisten für Schlüsseleinführungen mit Schlüsseln anderer Schließanlagen

Unterschiedliche Zylinderkonfigurationen haben unterschiedliche Speicherkapazitäten. Weitere Informationen finden Sie in den Produktinformationen.

7.4 Programmiergeräte

7.4.1 Lokale PGs

Das lokale PG wird zum Verbinden von Programmierschlüsseln und Nutzerschlüsseln mit CWM verwendet.

Abbildung 3. Lokales Programmiergerät

Das lokale Programmiergerät wird von den Administratoren einer Schließanlage verwendet. Es hat zwei Schlüsselschlitze; der linke ist für Programmierschlüssel bestimmt, der rechte für Benutzerschlüssel. Zur Anmeldung bei CWM werden ein lokales Programmiergerät, das mit einem CWM-Client verbunden ist, und ein Programmierschlüssel benötigt. Das PG kann über den USB-Anschluss angeschlossen werden.

Das Lokale PG besitzt zwei Anschlüsse:

- Eine USB-Schnittstelle
- Eine Schnittstelle zum Anschluss von Zylindern (wird bei CWM nicht verwendet)

7.4.2 Remote-Programmiergeräte

Remote-PGs werden bei Remote-Systemen zur Übertragung von Daten zwischen der Remote-Datenbank und dem Schlüssel benötigt. Remote-Programmiergeräte können entweder Wand-Programmiergeräte oder mobile Programmiergeräte sein. Wand-Programmiergeräte und mobile CLIQ-Programmiergeräte sind für bestimmte Schließanlagen vorgesehen. Mobile CLIQ Connect-Programmiergeräte können hingegen mit jeder Schließanlage verwendet werden.

Der zu verwendende USB-Kabeltyp hängt vom Gerätetyp ab:

Gerät	USB-Kabeltyp
Wand-Programmiergerät (Generation 1)	mini-USB On-The-Go (OTG)
Wand-Programmiergerät (Generation 2)	USB-C
Mobiles CLIQ-Programmiergerät	mini-USB
Mobiles CLIQ Connect-Programmiergerät	micro-USB

Wenn ein Schlüssel in ein Remote-Programmiergerät eingesteckt wird, werden folgende Vorgänge ausgeführt:

- Die Remote Update Tasks werden ausgeführt.
- Die Zeit auf dem Schlüssel wird aktualisiert.
- Die Ereignisliste wird bei entsprechender Konfiguration aus dem Schlüssel ausgelesen.

Siehe auch *Abschnitt 9.5.1 "Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen Programmiergeräten", Seite 212* und *Abschnitt 9.5.2 "Anzeigen eines Wand-Programmiergeräts (Generation 2)", Seite 213*.

Bei aktivierter Option **Offline-Update** kann ein Schlüssel auch dann über ein Wand-Programmiergerät oder ein mobiles CLIQ-Programmiergerät verlängert werden, wenn vorübergehend keine Netzwerkverbindung besteht. Siehe auch *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170*. Offline-Update ist nicht für mobile CLIQ Connect-Programmiergeräte verfügbar.

Wand-PGs

Es gibt zwei Arten von Wand-Programmiergeräten: Geräte der Generation 1 und Geräte der Generation 2. Wand-Programmiergeräte der Generation 2 bieten die folgenden zusätzlichen Funktionen:

- Die Netzwerkauthentifizierung 802.1x kann aktiviert werden. Informationen zum Aktivieren und Deaktivieren finden Sie in *"NETZWERKAUTHENTIFIZIERUNG (802.1X) (nur Wand-Programmiergerät Generation 2)"* und *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.
- Es wird kein Bootloader verwendet, d. h. es ist kein Upgrade der Bootloader-Firmware erforderlich.
- Der Protokolliergrad für das Geräteprotokoll ist konfigurierbar. Weitere Informationen hierzu finden Sie unter *"ALLGEMEIN"*.

Wand-Programmiergeräte werden üblicherweise an einer Wand montiert und über Ethernet mit dem Remoteserver verbunden.

Abbildung 4. Wand-Programmiergerät der Generation 1

Abbildung 5. Wand-Programmiergerät der Generation 2

Der Begriff **Herzschlag** bezeichnet ein Signal, das ein Wand-Programmiergerät an einen CLIQ Remote-Server sendet, um der CLIQ Web Manager-Software mitzuteilen, dass es online ist. Das Wand-Programmiergerät fragt bei Übertragung des Herzschlagsignals außerdem ab, ob Updates vorhanden sind (Updates von Firmware oder Konfiguration). Die Zeit zwischen den Herzschlag-Signalen ist konfigurierbar.

Wenn der Herzschlag eines Wand-Programmiergeräts aussetzt, nimmt CLIQ Web Manager an, dass das Wand-Programmiergerät in den Offline-Status gewechselt ist und sendet eine E-Mail an eine festgelegte Person. Für weitere Informationen zur Aktivierung dieser Funktion siehe *Abschnitt 6.5.10 "Offline-Meldungen für Wand-Programmiergeräte aktivieren oder deaktivieren", Seite 125*.

Mobile CLIQ-Programmiergeräte

Das mobile CLIQ-Programmiergerät ist ein persönliches Programmiergerät. Es kann entweder über ein Mini-USB-Kabel mit einem Computer oder über Bluetooth Low Energy (BLE) mit einem Mobiltelefon verbunden werden und so die Internetverbindung des Telefons nutzen.

Das mobile CLIQ-Programmiergerät muss zur Verbindung mit einem Mobiltelefon über Batterie betrieben werden. Wenn das mobile CLIQ-Programmiergerät mit einem Rechner verwendet wird, muss eine spezielle Anwendung, **ASSA ABLOY Network Provider**, auf dem Rechner installiert sein.

Abbildung 6. CLIQ Mobiles Programmiergerät

Mobile CLIQ Connect-Programmiergeräte
Das mobile CLIQ Connect-Programmiergerät wird verwendet, um Schlüssel mithilfe von CLIQ Connect (nur Schlüssel der 2. Generation) oder mithilfe von CLIQ Connect PC zu aktualisieren.

Es kann über ein Micro-USB-Kabel mit einem Computer oder über Bluetooth Low Energy (BLE) mit einem Mobiltelefon verbunden werden und damit die Internetverbindung des Telefons nutzen.

Das mobile CLIQ Connect-Programmiergerät muss zur Verbindung mit einem Mobiltelefon über Batterie betrieben werden.

Abbildung 7. Mobiles CLIQ Connect-Programmiergerät

8 CLIQ - Konzepte und Funktionen

8.1 Berechtigungsprinzipien

Damit ein Schlüssel einen Zylinder öffnen kann, müssen folgende Anforderungen erfüllt sein:

- Der mechanische Code muss korrekt sein. Siehe *Abschnitt 8.1.1 "Mechanische Berechtigung", Seite 168*.
- Der Schlüssel muss aktiv sein. Dies bedeutet, dass ein Schlüssel entsprechend den Aktivierungseinstellungen aktiv sein und (bei Verwendung der Verlängerungsfunktion) innerhalb des spezifizierten Verlängerungsintervalls verlängert werden muss. Siehe *Abschnitt 8.1.4 "Schlüsselgültigkeit", Seite 170*.
- Der Zylinder muss elektronisch so programmiert sein, dass er dem Schlüssel Zugang gewährt. Siehe *Abschnitt 8.1.2 "Elektronische Berechtigung", Seite 168*.
- Der Schlüssel darf im Zylinder nicht gesperrt sein. Siehe *Abschnitt 8.1.2 "Elektronische Berechtigung", Seite 168*.
- Bei E3-Schlüsseln: Der Schlüssel muss so programmiert sein, dass er Zugang zum Zylinder hat. Siehe *Abschnitt 8.1.2 "Elektronische Berechtigung", Seite 168*.
- E3-Schlüssel und E2-Schlüssel: Der Schlüsselzeitplan erlaubt zur aktuellen Zeit den Zugang. Siehe *Abschnitt 8.1.8 "Schlüssel-Zeitpläne", Seite 175*.

8.1.1 Mechanische Berechtigung

Wie bei einem traditionellen Hauptschlüsselsystem hat jeder Schlüssel eine mechanische Schließung, und jeder Zylinder ist mit einer oder mehreren Schlüsselschließungen kompatibel. Die CWM-Software verfolgt die Schlüssel, die einen bestimmten Zylinder mechanisch schließen und berücksichtigt dies bei der Festlegung der Möglichkeit der Gewährung eines elektronischen Zugangs.

8.1.2 Elektronische Berechtigung

Die elektronische Berechtigung basiert auf im Zylinder sowie (bei E3-Schlüsseln) im Schlüssel gespeicherten Daten.

Folgende Daten lassen sich in Zylindern speichern:

- Eine **Zylinderzugangsliste** mit den Schlüsseln und Schlüsselgruppen, die Zugang zum Zylinder haben.
- Für jede Schlüsselgruppe in der Zugangsliste können Ausnahmen festgelegt werden, d. h. alle Schlüssel in der Schlüsselgruppe mit Ausnahme der festgelegten Ausnahmen haben Zugang. Dies ist nützlich, wenn ein Zylinder allen Schlüsseln einer Schlüsselgruppe mit Ausnahme einiger weniger Zugang gewähren soll.

Bei E2-Schlüsseln und E1-Schlüsseln bestimmen nur die in den Zylindern gespeicherten Informationen, ob ein Schlüssel Zugang zu einem Zylinder hat.

Bei E3-Schlüsseln können folgende Informationen gespeichert werden:

- Eine **Schlüsselliste** mit den Zylindern und Zylindergruppen, zu denen den Schlüssel Zugang hat.

Damit ein E3-Schlüssel einen Zylinder öffnen kann, müssen die Daten in Zylinder und Schlüssel übereinstimmen. Bei einem typischen Remote-System mit E3-Schlüsseln werden die Zylinder so programmiert, dass sie allen Schlüsseln Zugang gewähren; die tatsächliche Zugangsberechtigung wird über die Schlüsselzugangsliste geregelt.

Abbildung 8 "Schlüsselzugangsliste", Seite 169 zeigt die verschiedenen Vorgehensweisen, wie Zylinder und Zylindergruppen in die Zugangsliste des E3-Schlüssels aufgenommen werden können:

1. direkt
2. über ein Zugangsprofil
3. über einen Benutzer, der einem Zugangsprofil zugeordnet ist
4. über eine temporäre Zugangsgruppe

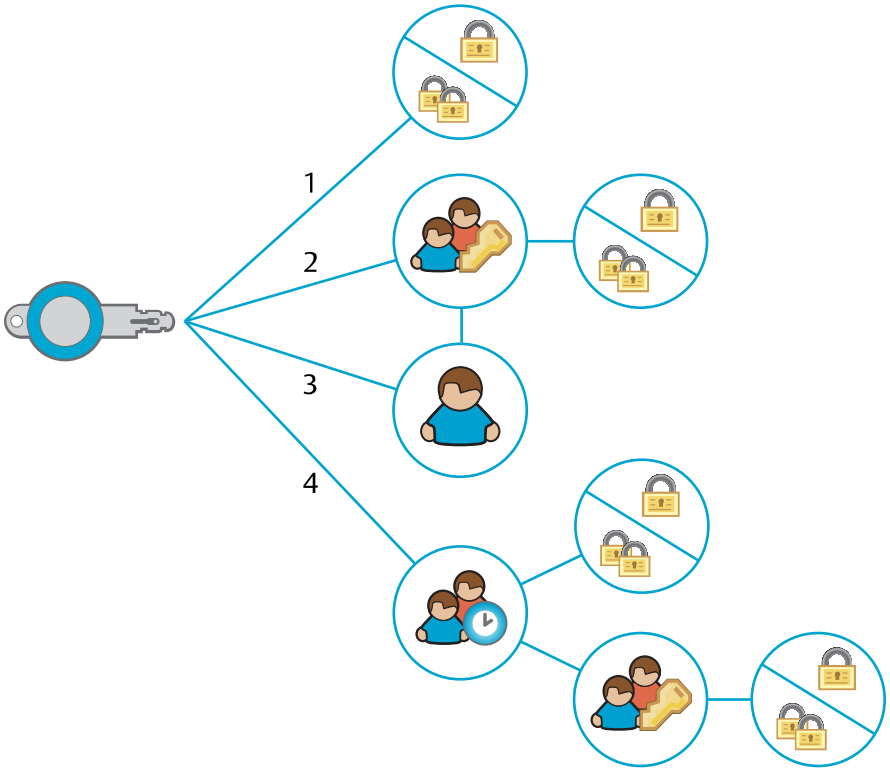


Abbildung 8. Schlüsselzugangsliste

Die Kapazität einer Schlüsselzugangsliste ist begrenzt. Die maximale sowie die aktuell genutzte Anzahl Einträge lässt sich in der Detailanzeige eines E3-Schlüssels sehen. Remote-Update-Jobs, die die Kapazität übersteigen würden, werden nicht ausgeführt. Siehe auch *Abschnitt 8.3.2 "Remote-Update", Seite 185*.

Einer der Unterschiede zwischen Schlüsselzugangslisten und Zylinderzugangslisten ist die Handhabung der Gruppeneinträge. In Schlüsselzugangslisten können Zylinder gleichzeitig sowohl individuell als auch als Teil einer Zylindergruppe umfasst werden. Dies ist bei Zylinderzugangslisten nicht der Fall. Wenn eine Schlüsselgruppe zu einer Zylinderzugangsliste hinzugefügt wird, werden alle individuellen Einträge mit Schlüsseln dieser Schlüsselgruppe (jetzt redundant) automatisch entfernt. Das bedeutet: wenn eine Schlüsselgruppe hinzugefügt und später wieder entfernt wird, verlieren alle Schlüssel in dieser Gruppe ihre Zugangsberechtigung, einschließlich der Schlüssel, die zuvor über individuellen Zugang verfügt haben.

8.1.3 Expliziter und impliziter Zugang

Es gibt zwei Vorgehensweisen bei der Konfiguration von Zugangslisten:

- **Expliziter Zugang** wird durch Bearbeiten der Zugangslisten direkt auf den Schlüsseln, Zylindern und Zylindergruppen gewährt.
- **Impliziter Zugang** wird Schlüsseln über Zugangsprofile gewährt, die mit einer Person oder direkt mit einem Schlüssel verknüpft sind. Siehe auch *Abschnitt 8.2.4 "Zugangsprofile", Seite 180*.

E3-Schlüssel haben eine Zugangsliste, in der die Zylinder und Zylindergruppen enthalten sind, die der Schlüssel öffnen darf. Der Zugang des Schlüssels zu einem Zylinder oder einer Zylindergruppe kann entweder explizit oder implizit sein. Der in der Schlüsselzugangsliste gespeicherte Zugang ist die Kombination aus implizitem und explizitem Zugang.

Weitere Informationen siehe *Abschnitt 8.2.4 "Zugangsprofile", Seite 180* und *Abschnitt 8.2.5 "Temporäre Zugangsgruppen", Seite 182*.

8.1.4 Schlüsselgültigkeit

Schlüsselgültigkeit bedeutet, dass ein Schlüssel zu einem bestimmten Zeitpunkt entweder **Aktiv** oder **Inaktiv** ist. Ein aktiver Schlüssel hat je nach Berechtigung und Zeitplaneinstellungen Zugang, während ein inaktiver Schlüssel keinerlei Zugang hat. Es ist zu beachten, dass Schlüsselgültigkeit und Zeitplan auf zwei verschiedenen Konzepten beruhen. Siehe auch *Abschnitt 8.1.8 "Schlüssel-Zeitpläne", Seite 175*.

Es gibt drei Möglichkeiten, die Gültigkeit eines Schlüssels zu steuern:

- **Aktivierungseinstellungen**. Ein Schlüssel kann so eingestellt werden, dass er **inaktiv**, **immer aktiv** oder **Im gewählten Zeitraum aktiv** ist.

  Aktiv im festgelegten Zeitraum ist nur für E3-Schlüssel und E2-Schlüssel verfügbar.
- **Verlängerung**, eine optionale Funktion. Schlüssel mit Verlängerung müssen in festgelegten Zeitabständen aktualisiert werden, um aktiv zu bleiben.

  Bei Auswahl der Verlängerung wird **Der Schlüssel kann immer verlängert werden.** in den **Gültigkeitseinstellungen** in CWM angezeigt.

  Siehe auch *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170*.
- **PIN-Validierung**, eine optionale Funktion für CLIQ Connect-Schlüssel. Die PIN von Schlüsseln mit PIN-Validierung muss in festgelegten Zeitabständen über CLIQ Connect validiert werden, damit die Schlüssel aktiv zu bleiben.

  Siehe auch *Abschnitt 8.1.7 "PIN-Validierung", Seite 174*.

Damit ein Schlüssel aktiv ist, müssen folgende Bedingungen erfüllt sein:

- Er muss entsprechend den Aktivierungseinstellungen aktiviert sein.
- Er muss innerhalb des spezifizierten Verlängerungsintervalls verlängert werden (bei Verwendung der Verlängerungsfunktion).
- Die PIN muss im vorgegebenen PIN-Validierungsintervall validiert werden (falls die PIN-Validierung verwendet wird).

Siehe auch *Abschnitt 4.10.1 "Konfigurieren der Schlüsselgültigkeit, Verlängerung und PIN-Validierung", Seite 89*.

8.1.5 Schlüssel-Verlängerung

Die Funktion **Schlüssel-Verlängerung** stellt sicher, dass Schlüssel in bestimmten Zeitabständen aktualisiert werden.

Diese Funktion erfordert eine Lizenz.

Schlüssel mit Schlüsselverlängerung müssen in festgelegten Zeitabständen aktualisiert („verlängert“) werden, um aktiv zu bleiben. Nach der Verlängerung bleibt der Schlüssel ab dem Zeitpunkt der Verlängerung für die als Verlängerungsintervall angegebene Anzahl von Tagen, Stunden und Minuten aktiv. Wird die Gültigkeit eines Schlüssels nicht innerhalb der angegebenen Zeit verlängert, wird er inaktiv, bis er wieder verlängert wird.

Abbildung 9 "Schlüssel-Verlängerung", Seite 172 zeigt das Prinzip der Schlüssel-Verlängerung. Wenn ein Schlüssel in einem Remote-Programmiergerät verlängert wird, startet ein Timer (1). Der Schlüssel hat Zugang, solange er innerhalb des Verlängerungsintervalls verwendet wird (2). Nach Ablauf des Verlängerungsintervalls (3) muss der Schlüssel in einem Remote-Programmiergerät verlängert werden (1). Durch die Verlängerung des Schlüssels wird der Timer zurückgesetzt.

Schlüssel werden außerdem in einem lokalen PG verlängert, wenn die folgenden Aktionen lokal ausgeführt wurden:

- **Zeitplan** festlegen
- **Ereignisliste** lesen
- **Zylinder in der Zugangsliste** ändern

Wenn die folgenden Bedingungen erfüllt sind, wird ein Schlüssel im rechten Schacht des lokalen Programmiergeräts **ohne** Programmierschlüssel revalidiert:

- Schlüssel der Generation 2 mit Firmware-Version 12.3 oder höher
- CLIQ Connect-PC ist aktiviert

HINWEIS!
Vor der Aktualisierung und Revalidierung muss der Programmierschlüssel aus dem linken Schacht des lokalen Programmiergeräts entfernt werden.

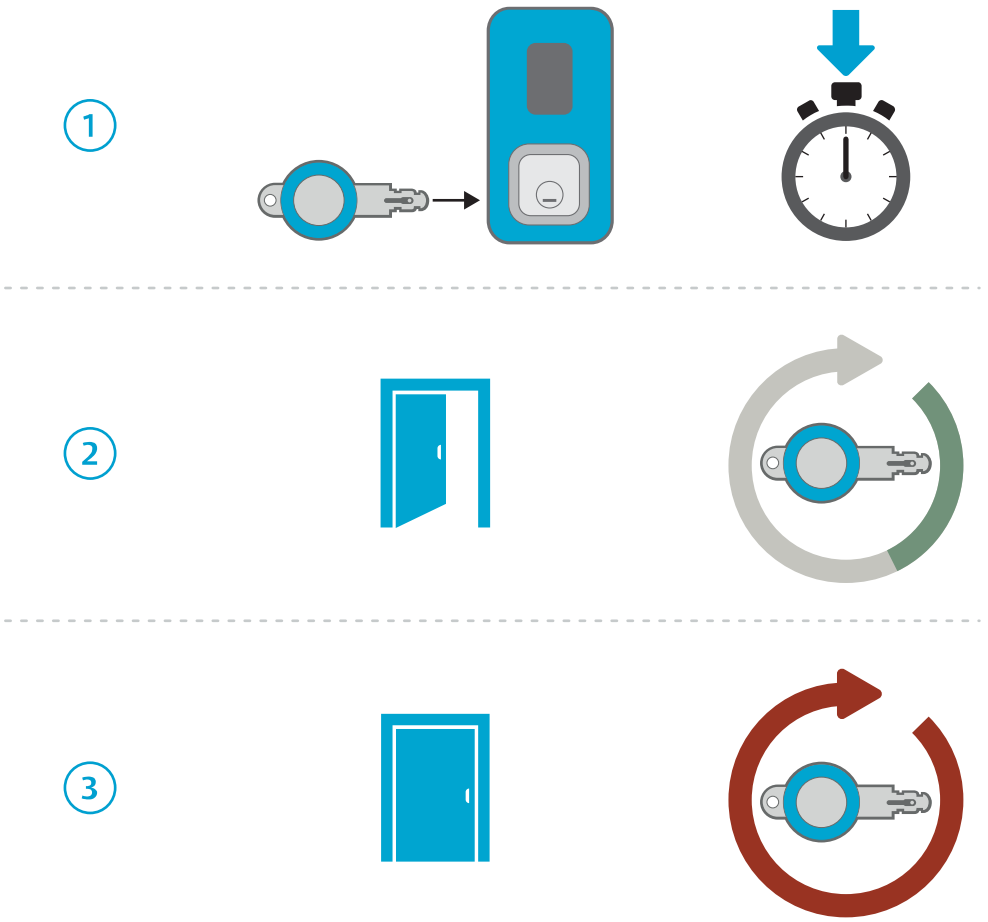


Abbildung 9. Schlüssel-Verlängerung

Die Verlängerung hat folgende Vorteile:

- Es wird sichergestellt, dass anstehende Schlüssel-Updates auf den Schlüsseln regelmäßig durchgeführt werden.
- Die Ereignislisten werden in kurzen Abständen ausgelesen.
- Das Risiko bei Schlüsselverlust wird reduziert. Ein verlorener Schlüssel verliert nach Ablauf des festgelegten Zeitraums sämtliche Zugangsrechte. Wird er in CWM als verloren gemeldet, kann er auch nicht mehr verlängert werden.

Bei der Einstellung des Verlängerungsintervalls muss ein Kompromiss zwischen Praktikabilität für den Schlüsselhalter und Sicherheit der Schließanlage gefunden werden. Ein kurzes Verlängerungsintervall von beispielsweise 24 Stunden gewährleistet häufige Updates und begrenzt das Risiko bei verlorenen Schlüsseln; andererseits muss der Schlüsselhalter den Schlüssel täglich aktualisieren. Ein langes Verlängerungsintervall ist für den Schlüsselhalter bequemer, erhöht aber das Risiko bei verloren gegangenen Schlüsseln und führt zu einem weniger häufigen Update von Zugangslisten und Ereignislisten.

Eine Möglichkeit zum Umgang mit dieser Einschränkung ist die Verwendung der Schlüsselverlängerung in Verbindung mit **PIN-Validierung** (bei CLIQ Connect-Schlüsseln). Siehe *Abschnitt 8.1.7 "PIN-Validierung", Seite 174*.

Siehe auch *Abschnitt 4.10.1 "Konfigurieren der Schlüsselgültigkeit, Verlängerung und PIN-Validierung", Seite 89*.

Die **flexible Verlängerung** ist eine erweiterte Funktion, die die Festlegung eines geeigneten Kompromisses unterstützt. Siehe *Abschnitt 8.1.6 "Flexible Verlängerung", Seite 173*.

Die Funktion **Offline-Update** bei Remote-Programmiergeräten ermöglicht das Verlängern der Schlüsselgültigkeit auch dann, wenn das Remote-Programmiergerät vorübergehend die Serververbindung verloren hat. Siehe *Abschnitt 8.3.3 "Offline-Update", Seite 186*.

8.1.6 Flexible Verlängerung

Die **flexible Verlängerung** ist eine optionale erweiterte Funktion, die die Festlegung eines Schlüssel-Verlängerungsintervalls je Zugangsprofil und je Zylindergruppe ermöglicht. Informationen zur Schlüssel-Verlängerung siehe *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170*.

Diese Funktion erfordert eine Lizenz.

Die flexible Verlängerung ist unter den folgenden Umständen nützlich:

- Wenn die Zylinder unterschiedlichen Sicherheitsanforderungen genügen müssen. Zum Beispiel kann der Zugang zu einem Serverraum sicherheitskritischer sein als der Zugang zu einem Besprechungszimmer.
- Wenn die mit den Zugangsprofilen verknüpften Rollen unterschiedlichen Sicherheitsanforderungen genügen müssen. Zum Beispiel kann bei Lieferanten eine häufigere Verlängerung erforderlich sein als bei Mitarbeitern.
- Wenn bestimmte zeitlich begrenzte Rollen unterschiedliche Verlängerungsintervalle erfordern. Eine Person im Bereitschaftsdienst kann beispielsweise unter Umständen ein längeres Verlängerungsintervall benötigen, muss aber besonders sorgfältig auf den Schlüssel aufpassen.

ACHTUNG!
Bei Verwendung der flexiblen Verlängerung muss bei allen Schlüsseln, die von den Verlängerungseinstellungen in den Zugangsprofilen oder Zylindergruppen betroffen sind, die Verlängerung aktiviert sein.

Bei der flexiblen Verlängerung können die Verlängerungsintervalle auf drei Ebenen eingestellt werden:

- **Schlüsseleinstellung**. Das auf dem Schlüssel eingestellte Verlängerungsintervall ist das Maximum. Einstellungen in Zugangsprofilen oder für Zylindergruppen können in keinem Falle zu einem Verlängerungsintervall führen, das länger ist als der hier eingestellte Wert.

  Konfiguration des Schlüssel-Verlängerungsintervalls siehe *Abschnitt 4.10.1 "Konfigurieren der Schlüsselgültigkeit, Verlängerung und PIN-Validierung", Seite 89*.

- **Zylindergruppeneinstellung**. Die Einstellung des Verlängerungsintervalls für Zylindergruppen kann verwendet werden, wenn Zylindergruppen unterschiedlichen Sicherheitsanforderungen genügen müssen.

  Das für eine Zylindergruppe eingegebene Verlängerungsintervall beschränkt das auf dem Schlüssel angegebene Intervall für diese Zylindergruppe. Wenn z. B. ein Schlüssel mit einem Verlängerungsintervall von 14 Tagen Zugang zur einer Zylindergruppe mit einem Verlängerungsintervall von 7 Tagen erhält, dann gilt für diese Zylindergruppe die Einstellung von 7 Tagen. Wenn andererseits die Zylindergruppe ein Verlängerungsintervall von 30 Tagen hat, dann gilt für diese Zylindergruppe die auf dem Schlüssel vorhandene Einstellung von 14 Tagen, da die Einstellung auf dem Schlüssel stets das Maximum festlegt.

Zylinder in Zylindergruppensystemen übernehmen das eingestellte Verlängerungsintervall der Zylindergruppe, zu der sie gehören.

Die Einstellung eines Verlängerungsintervalls für Zylindergruppen erfordert keine Zylinderprogrammierung.

Konfiguration eines Zylindergruppen-Verlängerungsintervalls siehe *Abschnitt 4.10.2 "Konfigurieren der flexiblen Verlängerung", Seite 91*.

- **Zugangsprofileinstellung**. Die Einstellung des Verlängerungsintervalls in Zugangsprofilen kann verwendet werden, wenn die mit den verschiedenen Zugangsprofilen verknüpften Rollen unterschiedlichen Sicherheitsanforderungen entsprechen müssen oder wenn Personen im Bereitschaftsdienst vorübergehend längere Verlängerungsintervalle benötigen.

  Die in einem Zugangsprofil festgelegte Verlängerungszeit hat Vorrang vor den Zylindergruppeneinstellungen. Wenn z. B. ein Zugangsprofil mit einem Verlängerungsintervall von 10 Tagen Zugang zu einer Zylindergruppe mit einem Verlängerungsintervall von 7 Tagen gewährt, dann gilt für diese Zylindergruppe 10 Tage für Schlüssel, die mit dem Zugangsprofil verknüpft sind. Die Schlüsseleinstellung ist weiterhin das Maximum.

  Wenn ein Schlüssel oder eine Person mit mehr als einem Zugangsprofil mit unterschiedlichen Verlängerungsintervallen verknüpft ist und diese Zugangsprofile Zugang zur selben Zylindergruppe gewähren, dann gilt das längere Intervall. Wenn z. B. zwei Zugangsprofile mit Verlängerungsintervallen von 10 Tagen bzw. 20 Tagen Zugang zur selben Zylindergruppe gewähren, dann gilt für diese Zylindergruppe 20 Tage. Die Zylindergruppeneinstellung (sofern angegeben) wird umgangen, aber die Schlüsseleinstellung stellt weiterhin das Maximum dar.

  Bei Zylindergruppen, für die weder ein Zylindergruppen-Verlängerungsintervall noch ein Zugangsprofil-Verlängerungsintervall spezifiziert ist, gilt die Schlüsseleinstellung.

  Konfiguration eines Zugangsprofil-Verlängerungsintervalls siehe *Abschnitt 4.10.2 "Konfigurieren der flexiblen Verlängerung", Seite 91*.

Tipp
Es wird dringend empfohlen, Einstellungen von Verlängerungsintervallen hauptsächlich **entweder** über Zylindergruppen **oder** über Zugangsprofile vorzunehmen, **nicht über beide**. Die Vermischung beider Konzepte kann zu Unübersichtlichkeit führen. Im typischen Fall wird die Einstellung für Zylindergruppen verwendet und mögliche Ausnahmen werden in den Zugangsprofilen spezifiziert.

8.1.7 PIN-Validierung

PIN-Validierung ist bei Verwendung von mobilen CLIQ Connect-Programmiergeräten nicht verfügbar.

PIN-Validierung ist eine Funktion, die eine Offline-Validierung per PIN-Code ermöglicht. Hierfür ist CLIQ Connect erforderlich. Dies funktioniert nur mit CLIQ Connect-Benutzerschlüsseln.

Diese Funktion erfordert eine Lizenz.

Wenn die PIN-Validierung für einen Schlüssel aktiviert ist, wird der Schlüssel nach einem bestimmten Zeitraum deaktiviert, dem so genannten **PIN-Validierungsintervall**. Dann

muss der Schlüsselhalter einen PIN-Code eingeben, um ihn erneut zu aktivieren. Die PIN-Validierung erfolgt in CLIQ Connect, wo sie als **Aktivieren** bezeichnet wird. Der Mechanismus ähnelt einer Schlüsselverlängerung, doch die PIN-Validierung verfolgt ein etwas anderes Ziel:

Bei der Schlüssel-Verlängerung muss der Schlüsselhalter den Schlüssel in bestimmten Zeitabständen aktualisieren, damit der Schlüssel aktiv bleibt. So kann der Administrator sicherstellen, dass der Schlüssel die neusten Updates hat und ein in CWM als verloren gemeldeter Schlüssel wird deaktiviert. Außerdem werden bei der Aktualisierung des Schlüssels Ereignislisten vom Schlüssel gelesen, falls diese Funktion aktiviert ist. Für die Schlüssel-Verlängerung ist eine Internetverbindung erforderlich, weil dabei Updates vom CWM-Server abgerufen werden. Zur Verlängerung des Schlüssels ist kein PIN-Code oder Passwort erforderlich, da Schlüssel vorzugsweise immer die neuesten Updates haben sollten. Weitere Informationen siehe *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170*.

Eine PIN-Validierung erhöht die Sicherheit in mehrfacher Hinsicht:

- Der Benutzer muss einen PIN-Code eingeben.
- Schutz gegenüber verlorenen und gestohlenen Schlüsseln, auch wenn diese nicht in CWM als verloren gemeldet werden.
- Keine Internetverbindung erforderlich. Ein Schlüssel kann auch dann validiert werden, wenn der CWM-Server oder die Internetverbindung ausgefallen ist.
- Da die PIN-Validierung eines Schlüssels sehr leicht geht, kann das PIN-Validierungsintervall auf eine sehr kurze Zeit wie z. B. 30 Minuten eingestellt werden, was die Sicherheit erhöht.

Die größtmögliche Sicherheit wird durch eine Kombination aus Schlüssel-Verlängerung und PIN-Validierung erreicht. Durch die Schlüssel-Verlängerung werden die Schlüssel-Updates sichergestellt, und durch die PIN-Validierung wird der Schlüssel für jeden ohne PIN-Code schnell nutzlos.

In den Systemeinstellungen kann festgelegt werden, ob die PIN-Validierung Teil des Arbeitsablaufs für die Schlüsselausgabe sein soll, ebenso wie ein Standardintervall für die PIN-Validierung. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

Siehe auch *Abschnitt 8.1.4 "Schlüsselgültigkeit", Seite 170*, *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170* und *Abschnitt 4.10.1 "Konfigurieren der Schlüsselgültigkeit, Verlängerung und PIN-Validierung", Seite 89*.

8.1.8 Schlüssel-Zeitpläne

Schlüssel-Zeitpläne werden verwendet, um den Zugang mit einem Schlüssel auf eine bestimmten Zeit zu beschränken.

Wenn der Zugang mit einem Schlüssel nach einem bestimmten Zeitplan beschränkt werden muss, z. B. auf die Bürozeiten, kann ein Zeitplan konfiguriert werden. Je nach Firmwareversion des Schlüssels gibt es zwei Arten von Zeitplänen: den einfachen Zeitplan und den Zeitplan mit mehreren Zeiträumen. Weitere Informationen zu den Firmwareversionen der Schlüssel finden Sie unter *Abschnitt 9.7 "Firmware-abhängige Funktionen", Seite 215*.

- Bei einem Basiszeitplan kann ein einziger Zeitraum pro Wochentag spezifiziert werden. Dieser Zeitplan gilt für alle Zylinder.
- Bei einem Zeitplan mit mehreren Zeitfenstern können verschiedene Zeiträume pro Woche angegeben werden, und jeder Zeitraum kann sich über mehrere Tage erstrecken. Es können auch Zeitpläne für einzelne Zylinder angelegt werden.

HINWEIS!

Bei Generation-1-Schlüsseln:

- Bei Zylindern, die einzeln (nicht als Teil einer Zylindergruppe) in der Schlüsselzugangsliste enthalten sind, bedeutet die Angabe eines oder mehrerer Zeiträume für einen Zylinder, dass der allgemeine Zeitplan für diesen Zylinder nicht beachtet wird.
- Bei Zylindern, die als Teil einer Zylindergruppe in der Schlüsselzugangsliste enthalten sind, werden die zylinderspezifischen Zeiträume nicht beachtet.

Bei Generation-2-Schlüsseln:

- Die Angabe eines oder mehrerer Zeiträume für einen Zylinder bedeutet, dass der allgemeine Zeitplan für diesen Zylinder nicht beachtet wird.

Alle Schlüssel können mit einem spezifischen Zeitplan oder mit einem Zeitplan auf Grundlage einer Zeitplanvorlage konfiguriert werden.

Siehe auch *Abschnitt 4.10.3 "Konfigurieren des Schlüsselzeitplans", Seite 92* und *Abschnitt 6.10 "Verwalten von Zeitplanvorlagen", Seite 136*.

8.1.9 Zylinder mit 4-Augen-Prinzip

Die Funktion **Zylinder mit 4-Augen-Prinzip** erfordert zwei Schlüssel, um einen Zylinder zu entriegeln.

Das 4-Augen-Prinzip kann im Werk bei einzelnen Zylindern konfiguriert werden. Sie kann nicht über CWM konfiguriert werden.

Bei Zylindern, bei denen diese Funktion aktiviert ist, sind zwei Zugangsschlüssel zum Entriegeln erforderlich. Die Schlüssel müssen der Reihe nach innerhalb von einer Minute eingesteckt werden, um den Zylinder zu öffnen. Optional können Zylinder mit dieser Funktion so konfiguriert werden, dass die beiden Schlüssel zu unterschiedlichen Schlüsselgruppen gehören müssen.

8.1.10 Verzögerungsschloss

Durch die Funktion **Verzögerungsschloss**erhält ein gerade neu verlängerter Schlüssel erst nach einer bestimmten Zeitverzögerung Zugang zu einem Zylinder.

Die Funktion Verzögerungsschloss kann im Werk bei einzelnen Zylindern konfiguriert werden. Sie kann nicht über CWM konfiguriert werden.

Bei Zylindern, bei denen diese Funktion aktiviert ist, wird die konfigurierte Zeit (zum Beispiel 15 Minuten) zur Aktivierungs- und Ablaufzeit jedes Schlüssels, der auf den Zylinder zugreift, addiert. Bei Zylindern mit hohen Sicherheitsanforderungen wird empfohlen, die Verzögerungsschloss-Funktion in Kombination mit einem kurzen Verlängerungsintervall (zum Beispiel 30 Minuten) zu verwenden. Dadurch ist sichergestellt, dass der Schlüssel die meiste Zeit über inaktiv ist (wenn er nicht sehr häufig verlängert wird) und der Zylinder nach einer Verlängerung des Schlüssels erst nach einer Verzögerungszeit geöffnet werden kann.

Bei Zylindern mit unterschiedlichen Sicherheitsanforderungen kann die flexible Verlängerung nützlich sein. Siehe *Abschnitt 8.1.6 "Flexible Verlängerung", Seite 173*.

8.1.11 Online öffnen

Online öffnen ist eine bei CLIQ Connect-Schlüsseln verwendete Funktion, mit der gewährleistet ist, dass Schlüssel vor dem Öffnen von Zylindern immer aktualisiert werden. Dadurch wird verhindert, dass Schlüssel Zugang erhalten, deren Zugangsrechte aufgehoben wurden oder die als verloren gekennzeichnet sind.

Die Funktion „Online öffnen“ kann im Werk für einzelne Zylinder oder CLIQ Connect-Schlüssel konfiguriert werden. Sie kann nicht über CWM konfiguriert werden.

Ist die Funktion „Online öffnen“ für einen CLIQ Connect-Schlüssel aktiviert, muss eine Online-Öffnung durchgeführt werden, wenn mit dem Schlüssel auf einen Zylinder zugegriffen wird.

Ist Online öffnen bei einem Zylinder aktiviert, muss bei allen Schlüsseln, die auf diesen Zylinder zugreifen eine Online-Öffnung durchgeführt werden. Damit ist der Zugang auf CLIQ Connect-Schlüssel beschränkt.

Wenn eine Online-Öffnung erforderlich ist, muss der CLIQ Connect-Schlüssel mit CLIQ Connect gekoppelt werden (Pairing), bevor er in den Zylinder eingesteckt werden kann. Sobald der Schlüssel eingesteckt ist, stellt CLIQ Connect eine Verbindung mit dem CWM-Remote-Server her, ruft die neuesten Aktualisierungen für den Schlüssel ab und führt eine Schlüsselaktualisierung durch. Wenn der Schlüssel nach dem Schlüssel-Update Zugang zum Zylinder hat, wird der Zylinder sofort entriegelt.

Zylinder mit Online-Öffnung sind so konfiguriert, dass sie **Überbrückungsschlüssel** akzeptieren, ohne dass eine Online-Öffnung erforderlich ist. Alle nicht Connect Schlüssel werden im Werk als Überbrückungsschlüssel konfiguriert.

8.2 Gruppenbildungsfunktionen

8.2.1 Schlüsselgruppen

Schlüsselgruppen werden verwendet, um Zugangsrechte und sonstige Merkmale nicht nur für einen einzelnen Schlüssel, sondern für eine Schlüsselgruppe festzulegen.

Schlüsselgruppen werden hauptsächlich dann verwendet, wenn für die Zugangssteuerung Zugangslisten in den Zylindern verwendet werden.

Vorteile von Schlüsselgruppen:

- Schlüsselgruppen reduzieren die Anzahl der erforderlichen Einträge in Zylinderzugangslisten.
- Wenn ein neuer Schlüssel zu einer Schlüsselgruppe hinzugefügt wird, die bestimmte Zylinder schließt, dann schließt automatisch auch der neue Schlüssel. Eine Programmierung der Zylinder ist nicht erforderlich.
- Schlüsselgruppen können zur Massenkonfiguration von Schlüsselzeitplänen verwendet werden.

Wenn eine Schlüsselgruppe Zugang zu einem Zylinder erhält, dann schließen automatisch alle Schlüssel in der Schlüsselgruppe. Es können aber Ausnahmen festgelegt und einzelne Schlüssel vom Zugang ausgeschlossen werden.

HINWEIS!
Wenn eine Schlüsselgruppe zu einer Zugangsliste hinzugefügt wird, werden alle individuellen Einträge mit Schlüsseln dieser Schlüsselgruppe (jetzt redundant) automatisch entfernt. Das bedeutet: wenn eine Schlüsselgruppe hinzugefügt und später wieder entfernt wird, verlieren alle Schlüssel in dieser Gruppe ihre Zugangsberechtigung, einschließlich der Schlüssel, die zuvor über individuellen Zugang verfügt haben.

Es gibt verschiedene Arten von Schlüsselgruppen:


E1-Schlüssel-Gruppe Kann E2-Schlüsseln und E1-Schlüsseln enthalten.


E3-Schlüssel-Gruppe Kann E3-Schlüssel enthalten.


Normalprogrammierschlüssel-Gruppe Kann normale Programmierschlüssel enthalten.


Hauptprogrammierschlüssel-Gruppe Kann Hauptprogrammierschlüssel enthalten.

Mechanische Schlüssel können keiner Schlüsselgruppe angehören.

Massenkonfiguration von Zeitplänen in einer Schlüsselgruppe siehe *Abschnitt 4.10.4 "Konfigurieren des Schlüsselgruppenzeitplans", Seite 94*.

8.2.2 Domänen

Die Funktion **Domänen** ist eine administrative Gruppierfunktion, die Administratoren ermöglicht, zu bestimmten Bereichen einer Schließanlage Zugang zu erhalten und diese Bereiche zu steuern.

Diese Funktion erfordert eine Lizenz.

Domänen werden verwendet, um folgende Elemente in administrative Bereiche zu unterteilen:

- Schlüssel
- Mitarbeiter
- Besucher
- Zylinder
- Zylindergruppen
- Zugangsprofile
- temporäre Zugangsgruppen

Schlüsselgruppen und Programmierschlüssel können nicht einer Domäne angehören. Daher sind Schlüsselgruppen und Programmierschlüssel ungeachtet ihrer Domäne für Administratoren sichtbar.

Eine Domäne besteht aus einer Anzahl von Elementgruppen, die typischerweise zu einem geographischen oder organisatorischen Bereich gehören. Programmierschlüssel, die zu einer bestimmten Domäne gehören, erhalten lediglich Administrationsrechte für die enthaltenden Zylinder.

Vorteile von Domänen:

- Komfort: Administratoren, die mit Bereichen einer Schließanlage arbeiten, z. B. einer bestimmten geographischen Region, werden nicht mit Informationen zu Elementen in anderen Regionen behelligt.
- Sicherheit: Administratoren dürfen Elemente in anderen Domänen weder sehen noch administrieren.

Fakten zu Domänen:

- Zylinder, die zu einer Zylindergruppe gehören, werden über ihre Zylindergruppe von einer Domäne umfasst. Das bedeutet, dass alle Zylinder einer Zylindergruppe zur selben Domäne gehören.
- Zylinder, die nicht zu einer Zylindergruppe gehören, einschließlich aller mechanischen Zylinder, sind individuell Teil einer Domäne.
- Elemente können nur einer Domäne angehören (Schlüssel, Mitarbeiter, Besucher, Zylinder, Zylindergruppen, Zugangsprofile und temporäre Zugangsgruppen).
- Bei doppelseitigen Zylindern müssen beide Seiten derselben Domäne angehören.
- Der Programmierschlüssel eines Administrators kann je nach Zuweisung zu einer oder mehreren Domänen gehören.

HINWEIS!
Obwohl Programmierschlüssel nicht einer Domäne angehören können, besitzt jeder Programmierschlüssel eine Liste mit Domänen, für die der angemeldete Administrator Zugangs- und Steuerberechtigung hat.

Informationen zum Verknüpfen eines Programmierschlüssels mit einer Domäne finden Sie in *Abschnitt 6.11.5 "Auswählen von Domänen für Programmierschlüssel", Seite 140*.

8.2.3 Zylindergruppen

Eine **Zylindergruppe** ist eine Menge von Zylindern, die herangezogen wird, um die Verwaltung von Schließanlagen mit zahlreichen Zylindern zu vereinfachen.

Diese Funktion erfordert eine Lizenz.

Zylindergruppen werden in Schließanlagen verwendet, die als **Zylindergruppensysteme** definiert sind. Dies gilt für Zylinder mit Zylindergruppenunterstützung. Siehe *Abschnitt 9.7 "Firmware-abhängige Funktionen", Seite 215*.

Zylindergruppen werden vorab im Werk festgelegt, es können aber nachträglich Zylinder von einer Gruppe in eine andere übertragen werden. Dazu ist jedoch eine Zylinderprogrammierung erforderlich, und es wird empfohlen, die Gruppen vorab sorgfältig zu planen.

Einer Zylindergruppe kann Zugang genau wie einem Einzelzylinder gewährt werden. Kombinationen aus Zylindergruppen und Einzelzylindern bietet ein hohes Maß an Flexibilität.

Vorteile von Zylindergruppen:

- Einfachere Verwaltung von Schließanlagen mit einer Vielzahl von Zylindern.
- Da mit einem einzigen Eintrag Zugang zu zahlreichen Zylindern gewährt werden kann, kann mit einem einzigen Schlüssel eine Vielzahl von Zylindern geschlossen werden.
- Wenn ein Zylinder zu einer Zylindergruppe hinzugefügt oder aus einer solchen entfernt wird, wirkt sich dies unmittelbar auf die Schlüssel mit Zugang zu dieser

Zylindergruppe aus. Ein manuelles Update der Zugangsliste jedes einzelnen Schlüssels ist nicht erforderlich.

Das Konfigurieren von Zylindergruppen ist ein Kompromiss aus unterschiedlichen Erwägungen:

- Zylindergruppen sollten so konfiguriert werden, dass normalerweise allen Zylindern in der Gruppe Zugang gewährt wird.

  Es ist nicht möglich, allen Zylindern in einer Gruppe Zugang zu gewähren und einige wenige als Ausnahme zu definieren. Wenn dies erforderlich ist, sollten die entsprechenden Zylinder als separate Gruppe angelegt werden.
- Die Zylindergruppen sollten nicht zu klein sein, da es wichtig ist, die Anzahl der Gruppen zu begrenzen. Je weniger Gruppen vorhanden sind, desto einfacher wird die Verwaltung und desto geringer ist die Anzahl erforderlicher Einträge in den Schlüsselzugangslisten.
- Zylindergruppen sollten andererseits so klein sein, dass sie stabil sind, d. h. eine notwendige Übertragung von Zylindern zwischen Gruppen sollte möglichst unwahrscheinlich sein.

Fakten zu Zylindergruppen:

- Zylinder können nur zu einer Zylindergruppe gehören.
- Zylindergruppen können nur zu einer Domäne gehören.
- Bei doppelten Zylindern müssen beide Seiten derselben Zylindergruppe angehören.
- Mechanische Zylinder können keiner Zylindergruppe angehören.

8.2.4 Zugangsprofile

Zugangsprofile werden verwendet, um Personen mit speziellen Rollen den erforderlichen Zugang zu gewähren, ohne dass jeder Schlüssel einzeln konfiguriert werden muss. Schlüssel können ebenfalls direkt mit Zugangsprofilen verknüpft werden.

Diese Funktion erfordert eine Lizenz.

HINWEIS!
Die von Zugangsprofilen definierten Nutzerrollen sind nicht mit den Rollen zu verwechseln, die für die mit CWM arbeitenden Administratoren festgelegt werden.

Personen mit einer bestimmten Rolle, z. B. Büroreinigung, sind mit einem entsprechenden Zugangsprofil verknüpft. Das Zugangsprofil definiert eine Reihe von Zylindern und Zylindergruppen, zu denen Personen mit dieser bestimmten Rolle Zugang haben sollen. Schlüssel, die an die zugeordneten Personen ausgegeben werden, enthalten automatisch die richtigen Zugangsrechte, wie sie im Zugangsprofil festlegt wurden.

Abbildung 10 "Zugangsprofile", Seite 181 zeigt ein Beispiel mit zwei Zugangsprofilen (1, 2), jeweils mit Zugang zu mehreren Zylindern bzw. Zylindergruppen oder beidem (A, B). Die Zugangsprofile lassen sich entweder mit einer Person (3) oder mit einem Schlüssel verknüpfen. Bei Verknüpfung mit einer Person erhält der an diese Person ausgegebene Schlüssel automatisch Zugang zu den verknüpften Zugangsprofilen (C).

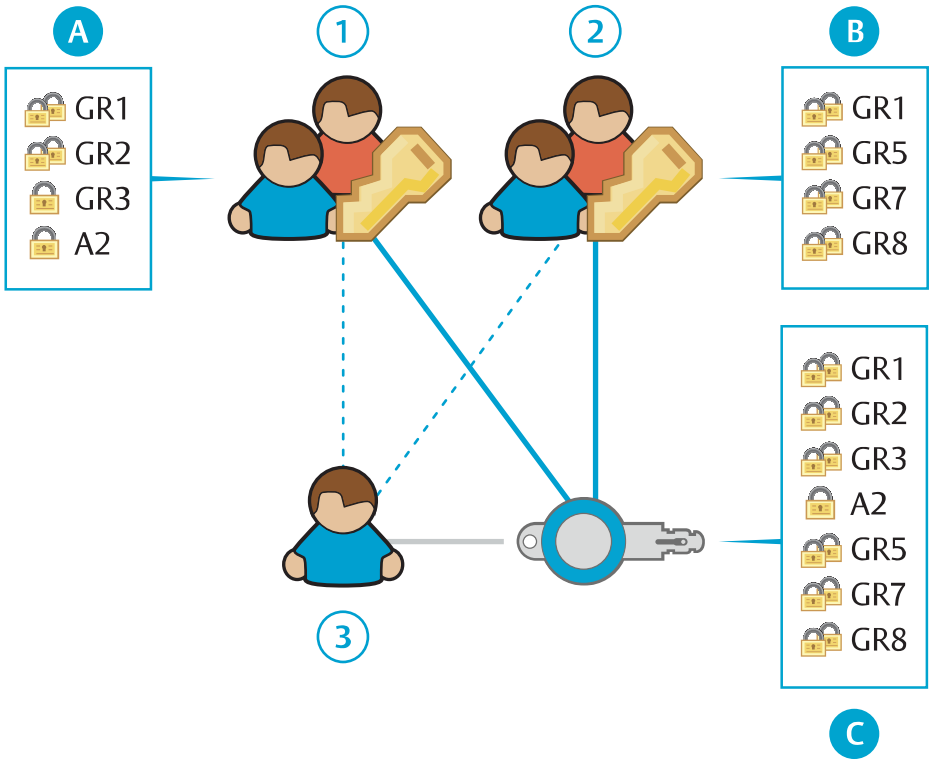


Abbildung 10. Zugangsprofile

Wenn ein Zugangsprofil direkt mit einem Schlüssel verknüpft ist, wird dieses Zugangsprofil nicht von anderen Schlüsseln übernommen, die dem gleichen Schlüsselhalter gehören.

Zugangsprofile sind insofern dynamisch, dass eine Änderung im Zugangsprofil automatisch den Status der Schlüssel-Berechtigungen laut Festlegung in CWM aktualisiert (auch **Definierter Status** genannt). Durch eine Änderung im Zugangsprofil werden Remote-Update-Jobs für verknüpfte Schlüssel generiert. Eine Programmierung von Zylindern ist nicht erforderlich. Informationen zu **Definierter Status** und **Tatsächlicher Status** siehe *Abschnitt 9.1.1 "Begriffe", Seite 199*.

Zugangsprofile legen den **impliziten Zugang** für Schlüssel fest, während die berechtigten Zylinder und Zylindergruppen, die direkt für den Schlüssel definiert wurden, den **expliziten Zugang** darstellen. Der in der Schlüsselzugangsliste gespeicherte tatsächliche Zugang ist die Kombination aus implizitem und explizitem Zugang, d. h. der Schlüssel schließt sowohl die im Zugangsprofil enthaltenen als auch die explizit für den Schlüssel festgelegten Zylinder.

Vorteile von Zugangsprofilen:

- Es ist möglich, den Zugang für mehrere Personen oder Schlüssel gleichzeitig zu verwalten.
- Es ist möglich, Profile entsprechend bestimmten Rollen zu definieren und Personen mit einer oder mehreren Rollen Zugang zu gewähren.
- Bei Änderung eines Zugangsprofils werden die entsprechenden Remote Update Jobs automatisch erzeugt.

Fakten zu Zugangsprofilen:

- Ein Schlüssel oder eine Person kann mehrere Rollen haben und daher mit mehr als einem Zugangsprofil verknüpft sein.

- In einem Zugangsprofil können sowohl Einzelzylinder als auch Zylindergruppen enthalten sein.
- Ein Zugangsprofil gehört nur zu einer einzigen Domäne, und es können nur Zylinder oder Zylindergruppen hinzugefügt werden, die zu dieser Domäne gehören.

> **HINWEIS!**
> Es wird empfohlen, dass ein Zugangsprofil sowie alle umfassten Zylinder und Zylindergruppen in derselben Domäne liegen. Dadurch wird sichergestellt, dass Administratoren einer bestimmten Domäne nicht indirekt Zugang zu Zylindern in anderen Domänen erhalten (über Zugangsprofile).

- Bei der Einführung von Zugangsprofilen in einer Schließanlage, bei der bereits Berechtigungen in Schlüsselzugangslisten verwendet werden, können die Schlüsselzugangslisten mehrere Einträge mit dem gleichen Zylinder oder der gleichen Zylindergruppen enthalten. Informationen zum Löschen redundanter Einträge siehe *Abschnitt 4.7.7 "Löschen redundanter Schlüssel-Berechtigungen", Seite 78*.

> **Tipp**
> Um beim Einsatz von Zugangsprofilen besseren Überblick zu behalten, wird empfohlen, die Verwendung von expliziten Zugängen zu minimieren.

8.2.5 Temporäre Zugangsgruppen

Temporäre Zugangsgruppen werden verwendet, um den Zugang von Schlüsseln vorübergehend zu erweitern, indem sie mit einer Auswahl von Zugangsprofilen verknüpft werden. Der Zugang einer temporären Zugangsgruppe stellt sich aus den kombinierten Zugängen der umfassten Zugangsprofile in einem durch Start- und Enddatum festgelegten Zeitraum zusammen.

Schlüssel in der temporären Zugangsgruppe erhalten impliziten Zugang zu den Zylindern und Zylindergruppen, die den enthaltenen Zugangsprofilen zugeordnet sind. Zusätzlich können Schlüssel expliziten Zugang zu einzelnen Zylindern und Zylindergruppen erhalten, die der temporären Zugangsgruppe zugeordnet sind.

Abbildung 11 "Temporäre Zugangsgruppen", Seite 183 zeigt einen Schlüssel, der zu einer temporären Zugangsgruppe (1) mit drei Zugangsprofilen (2, 3, 4) und einem Satz mit einzelnen Zylindern und Zylindergruppen (4) hinzugefügt wurde. Jedes Zugangsprofil hat Zugang zu mehreren Zylindern bzw. Zylindergruppen oder beidem (A, B, C). In einem festgelegten Zeitraum erhält der Schlüssel Zugang zu allen Zylindern und Zylindergruppen (D).

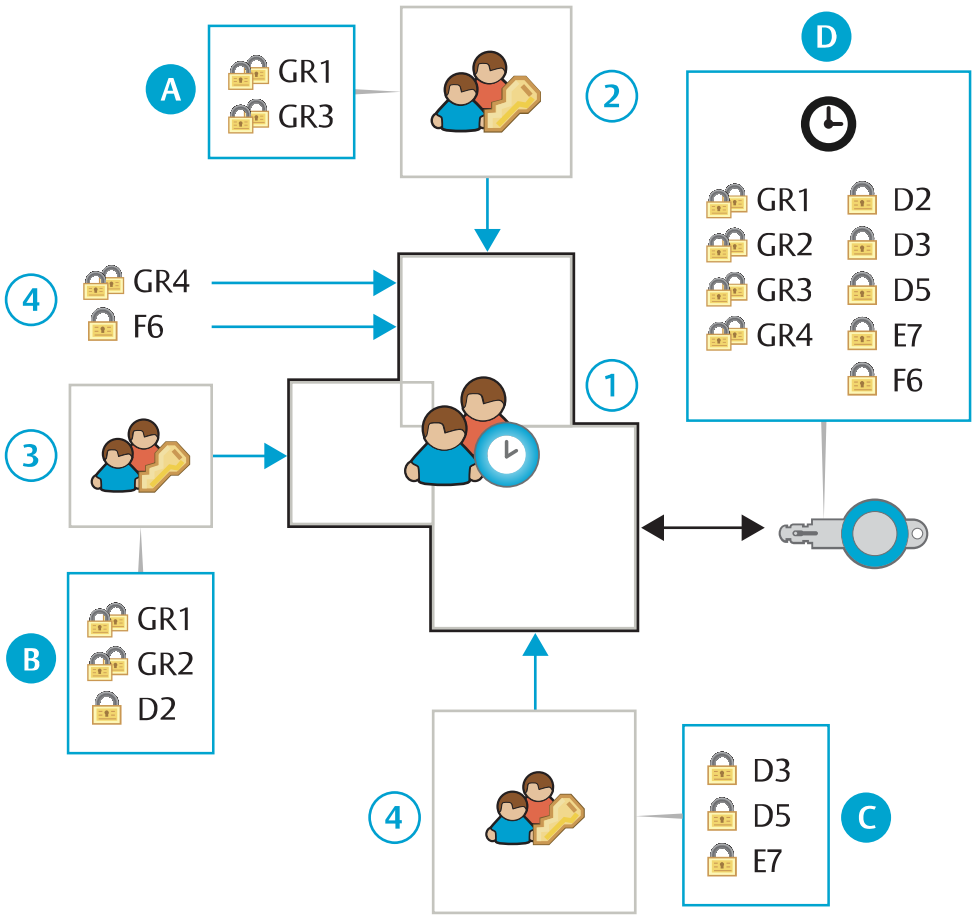


Abbildung 11. Temporäre Zugangsgruppen

Ein Verwendungsbeispiel ist, wenn ein oder mehrere Wartungstechniker Bereitschaftsdienst haben und während ihrer Bereitschaft Zugang zu verschiedenen Zugangsprofilen benötigen.

In der Praxis wird der Schlüssel zu einer temporären Zugangsgruppe hinzugefügt und in einem lokalen oder Remote-Programmiergerät programmiert. Wenn die temporäre Zugangsgruppe nicht länger für einen Schlüssel gültig ist, wird automatisch ein Remote-Job angelegt, um den Zugang der temporären Zugangsgruppe vom Schlüssel zu entfernen.

HINWEIS!
Der Zugang des Schlüssels wird erst beendet, wenn der Schlüssel in einem Remote-Programmiergerät aktualisiert wird. Damit der Schlüsselhalter nach Ablauf der temporären Zugangsgruppe den Schlüssel nicht länger verwenden kann, vor dem Aushändigen des Schlüssels einen der folgenden Schritte durchführen:

- In den Aktivierungseinstellungen **Aktiv im festgelegten Zeitraum** einstellen, siehe *Abschnitt 8.1.4 "Schlüsselgültigkeit", Seite 170*.
- Schlüssel-**Verlängerung** aktivieren, siehe *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170*.

Es wird dringend empfohlen, temporäre Zugangsgruppen mit der Schlüssel-Verlängerung zu kombinieren.

Nutzen temporärer Zugangsgruppen:

- Einem oder mehreren Schlüsseln können vorübergehend Zugang zu einer Gruppe mit Zugangsprofilen, einzelnen Zylindern und Zylindergruppen gewährt werden.

Fakten zu temporären Zugangsgruppen:

- Alle Zugangsprofile innerhalb einer temporären Zugangsgruppe müssen zur selben Domäne gehören.
- Benutzer, die mit der Standard-Domäne verknüpft sind, können temporäre Zugangsgruppen aus allen Domänen sehen. Angemeldete Benutzer anderer Domänen können nur temporäre Zugangsgruppen innerhalb ihrer eigenen Domänen sehen.

8.2.6 Tags

Ein **Tag** ist eine Zeichenkette, mit der Objekte zum leichteren Auffinden und Verwalten gekennzeichnet werden können.

Zum Beispiel können Zugangsprofile nach der Art der Rolle, mit der sie verknüpft sind, oder Zylinder nach dem Gebäude, in dem sie installiert sind, gruppiert werden.

Bei der Suche nach Objekten können Tags als Suchkriterium eingegeben werden.

In einigen Fällen wurden Tags bereits in den Erweiterungsdateien hinzugefügt und sind bei Import der Dateien in CWM verfügbar. Für die folgenden Objekte können Tags außerdem manuell hinzugefügt oder gelöscht werden:

- Mitarbeiter (siehe *Abschnitt 4.1.7 "Hinzufügen oder Entfernen von Mitarbeiter- oder Besucher-Tags", Seite 32*)
- Besucher (siehe *Abschnitt 4.1.7 "Hinzufügen oder Entfernen von Mitarbeiter- oder Besucher-Tags", Seite 32*)
- Schlüssel (siehe *Abschnitt 4.2.5 "Benutzerschlüssel-Tags hinzufügen oder entfernen", Seite 37*)
- Schlüsselgruppen (siehe *Abschnitt 4.3.3 "Hinzufügen oder Löschen von Schlüsselgruppen-Tags", Seite 56*)
- Zylinder (siehe *Abschnitt 4.4.3 "Zylinder-Tags hinzufügen oder entfernen", Seite 58*)
- Zylindergruppen (siehe *Abschnitt 4.5.3 "Hinzufügen oder Löschen von Zylindergruppen-Tags", Seite 69*)
- Zugangsprofile (siehe *Abschnitt 4.6.4 "Hinzufügen oder Löschen von Zugangsprofil-Tags", Seite 72*)
- Remote-PGs (siehe *Abschnitt 6.5.5 "Tags für Remote-Programmiergeräte hinzufügen oder entfernen", Seite 110*)

Jedem Objekt können mehrere Tags zugeordnet werden.

8.3 Remote-Funktion

8.3.1 Remote-Funktion - Überblick

Die Remote-Funktion ermöglicht Remote-Updates von Schlüsselkonfigurationen. Sie ermöglicht auch das Verlängern und das Abrufen von Ereignislisten von einem entfernten Standort aus.

Diese Funktion erfordert eine Lizenz.

- **Remote Update von Schlüsselkonfigurationen**

Der Administrator konfiguriert Berechtigungen und sonstige Einstellungen auf Schlüsseln, ohne dass der Schlüssel vorliegt. Die neue Schlüsselkonfiguration wird in der Datenbank des Remote Server als **Remote Update Job** gespeichert. Wenn der Schlüssel in ein Remote-Programmiergerät eingesteckt wird, wird der Update-Job ausgeführt und der Schlüssel mit der neuen Konfiguration programmiert.

- **Remote Update der aktuellen Zeiteinstellung eines Schlüssels**

  Die aktuelle Zeiteinstellung des Schlüssels wird bei jedem Schlüssel-Update aktualisiert.

- **Remote-Auslesen von Ereignislisten**

  Die Ereignisliste des Schlüssels wird bei jedem Schlüssel-Update ausgelesen, es sei denn in den Systemeinstellungen ist "Genehmigungen" aktiviert.

- **Verlängerung**.

  Die Verlängerung gewährleistet, dass Schlüssel in bestimmten Zeitabständen aktualisiert werden. Weitere Informationen zur Verlängerung der Schlüsselgültigkeit siehe *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170*.

Siehe auch *Abschnitt 8.3.2 "Remote-Update", Seite 185*.

Systeme werden entweder als Remote- oder Nicht-Remote-Systeme geliefert. Ein Nicht-Remote-System, das später in ein Remote-System umgewandelt wird, kann sowohl Schlüssel enthalten, die Remote-Updates unterstützen, als auch solche, die Remote-Updates nicht unterstützen. In einem System, das anfänglich als Remote-System geliefert wurde, unterstützen alle Schlüssel bei Lieferung Remote-Updates.

8.3.2 Remote-Update

Remote Update Jobs sind anstehende Schlüsselaktualisierungen. Diese sind nicht zu verwechseln mit **Zylinderprogrammierungs-Jobs**, bei denen es sich um anstehende Zylinderaktualisierungen handelt. Weitere Informationen zu Zylinderprogrammierungs-Jobs siehe *Abschnitt 8.5 "Zylinderprogrammierung", Seite 188*.

Außer wenn der Schlüssel im lokalen PG abgefragt wird, führen alle Vorgänge, die eine Aktualisierung der Daten auf dem Schlüssel erfordern, zu einem Remote Update Job. Dazu gehört das Update von Berechtigungen, Gültigkeit, Zeitplan usw. Der Remote-Update-Job wird beim nächsten Einstecken des Schlüssels in ein Remote-Programmiergerät ausgeführt.

Das Remote-Programmiergerät ist im Normalfall online, kann jedoch auch so konfiguriert werden, dass es Schlüssel-Updates unter bestimmten Bedingungen offline zulässt. Siehe *Abschnitt 8.3.3 "Offline-Update", Seite 186*.

Für Remote-Update-Jobs wird in CWM durchgängig folgendes Symbol verwendet:

 Für den Schlüssel steht ein Remote-Update an

Anzeige der anstehenden Remote-Berechtigungs-Updates siehe *Abschnitt 4.9.1 "Konfigurieren von Berechtigungen in Schlüsseln", Seite 81*.

Überschreitung der Schlüsselkapazität
Remote-Update-Jobs, die zur Kapazitätsüberschreitung einer Schlüsselzugangsliste führen würden, können nicht ausgeführt werden. Wenn ein solcher Job in CWM angelegt wird, wird an alle Administratoren, die vollständig für **Schlüsselberechtigungen** berechtigt sind und für die E-Mail-Adressen registriert wurden, eine E-Mail zu diesem Ereignis gesendet. Der Job wird in CWM außerdem mit folgendem Symbol gekennzeichnet:

 Anstehendes Remote-Update überschreitet Schlüsselkapazität

Bei Aktionen an einem einzelnen Schlüssel in der Schlüsselansicht wird direkt ein Remote-Update-Job erstellt, und der Administrator kann sofort sehen, ob dieser die Schlüsselkapazität überschreitet. Bei Aktionen an Schlüsseln in anderen Ansichten werden jedoch Remote-Update-Jobs nicht direkt erstellt, d. h. der Administrator erhält keine sofortige Rückmeldung.

Zu den Aktionen, die beim Generieren von Remote-Update-Jobs die Schlüsselkapazität überschreiten können und bei denen der Administrator keine sofortige Rückmeldung erhält, gehören:

- Hinzufügen von Zugängen zu einem Zugangsprofil
- Hinzufügen von Zugangsprofilen zu mehreren Schlüsseln
- Hinzufügen von Zugangsprofilen zu einer Person

Um das Problem zu beheben, muss die Anzahl der Einträge in der Schlüsselzugangsliste reduziert werden. Dies erfolgt durch Reduzierung der Anzahl expliziter Zugänge, durch Reduzierung der Anzahl der Zugänge in verknüpften Zugangsprofilen oder durch Entfernen von verknüpften Zugangsprofilen. Der Remote-Update-Job wird automatisch entsprechend angepasst.

8.3.3 Offline-Update

Offline-Update ist bei Verwendung von mobilen CLIQ Connect-Programmiergeräten nicht verfügbar.

Mit der Funktion **Offline-Update** kann ein Schlüssel auch dann über ein Remote-Programmiergerät verlängert werden, wenn vorübergehend keine Netzwerkverbindung besteht. Dies ist in Situationen nützlich, wenn es von entscheidender Bedeutung ist, dass ein Schlüssel auch bei instabiler Netzwerkverbindung seine Gültigkeit verlängert bekommen kann. Zugänge lassen sich nicht im Offline-Modus aktualisieren. Offline-Update ist pro Remote-Programmiergerät konfigurierbar.

Um das Risiko bei verlorenen Schlüsseln zu begrenzen, lassen sich mehrere Bedingungen für das Zulassen eines Offline-Updates einstellen. Folgendes ist konfigurierbar:

- Die Anzahl von aufeinander folgenden Updates, die im Offline-Modus durchgeführt werden können, bevor ein Online-Update erforderlich ist.
- In welchen Zeitraum Offline-Updates nach dem vergangenen Online-Update zulässig sind.
- Um wie viel die Schlüsselgültigkeit durch ein Offline-Update verlängert wird. Das auf den Schlüsseln eingestellte Verlängerungsintervall wird bei Offline-Updates ignoriert.

Spezifisch für Wand-PGs
Wenn der Schlüssel in der in jedem Wand-Programmiergerät gespeicherten **Schlüsselsperrliste** enthalten ist, darf er kein Offline-Update erhalten. Diese Liste enthält die Schlüssel, die als verloren gemeldet wurden und für die daher keine Offline-Updates zulässig sind. Das Wand-Programmiergerät prüft bei jedem Herzschlag auf neue Versionen der Schlüsselsperrliste und erlaubt nur dann Offline-Updates, wenn die Version der im Wand-Programmiergerät gespeicherten Liste nicht zu alt ist. Die Gültigkeitsdauer einer Schlüsselsperrliste lässt sich über einen Wand-Programmiergerät-Parameter konfigurieren.

Spezifisch für mobile CLIQ-Programmiergeräte
Nur Schlüssel, die vor kürzerer Zeit im gleichen mobilen CLIQ-Programmiergerät aktualisiert wurden (Schlüssel, die zu den letzten 10 aktualisierten Schlüsseln gehören), können aktualisiert werden.

Siehe auch *Abschnitt 8.1.5 "Schlüssel-Verlängerung", Seite 170*.

Konfiguration von Offline-Update siehe *Abschnitt 6.5.7 "Konfigurieren von Wand-Programmiergeräten", Seite 112* und *Abschnitt 6.5.8.1 "Einstellungen von mobilen CLIQ-Programmiergeräten bearbeiten", Seite 119*.

8.3.4 CLIQ Connect und CLIQ Connect+

CLIQ Connect ist eine Anwendung, die auf einem mobilen Gerät wie einem Mobiltelefon oder einem Tablet installiert wird. Mit CLIQ Connect können Benutzer, d. h. Besucher oder Mitarbeiter, ihre Benutzerschlüssel einfach verwalten. CLIQ Connect ist für Android und iOS verfügbar.

CLIQ Connect bietet die folgenden Funktionen:

- Validierung und Änderung des PIN-Codes eines Connect-Schlüssels.
- Aktualisieren von Connect-Schlüsseln über die Bluetooth-Verbindung des Schlüssels
- Aktualisieren anderer Arten von Benutzerschlüsseln über ein mobiles CLIQ Connect-Programmiergerät.

CLIQ Connect+
CLIQ Connect+ kann mit CLIQ Connect **Version 4.0 oder höher** verwendet werden. Mit dieser Funktion können alle registrierten Schlüsselhalter weitere Details zu ihren Connect-Schlüsseln oder anderen Schlüsseln anzeigen, z. B. Gültigkeit, Zeitplan oder zugängliche Zylinder.

Nach der Aktivierung befolgt der Schlüsselhalter die Anweisungen in der von CWM erhaltenen E-Mail, um die Einrichtung abzuschließen. Die Konfiguration der App erfolgt über einen in der E-Mail enthaltenen QR-Code.

Für diese Funktion müssen die folgenden Bedingungen erfüllt sein:

- CWM-Systemversion 11.2 oder höher.
- Die Lizenz **CLIQ Connect+** wurde für das System erteilt.

  Informationen zum Installieren der Lizenz finden Sie in *Abschnitt 6.1 "Verwalten von Lizenzen", Seite 101*.
- Der Schlüsselhalter ist ein in CLIQ Connect+ aktivierter Benutzer.

  Informationen zum Gewähren von Zugriff für Schlüsselhalter auf CLIQ Connect+ finden Sie in *Abschnitt 4.1.5 "Aktivieren und Deaktivieren von CLIQ Connect+ für Mitarbeiter oder Besucher", Seite 28*.
- Der Schlüsselhalter aktiviert das CLIQ Connect+-Konto durch Befolgen der Anweisungen in der von CWM erhaltenen E-Mail.

8.4 Externe Links

Ein **externer Link** ist eine URL oder Internetadresse, die verwendet werden kann, um ein Objekt, z. B. einen Mitarbeiter oder Zylinder, mit zusätzlichen Informationen zu verknüpfen.

Es kann zum Beispiel ein Mitarbeiter mit seiner Seite im Intranet des Unternehmens verlinkt werden oder ein Zylinder bzw. Wand-Programmiergerät mit einem Übersichtsplan, auf dem sein Standort zu sehen ist.

Externe Links können für folgende Objekte definiert werden:

- Mitarbeiter (siehe *Abschnitt 4.1.8 "Verwalten externer Links von Mitarbeitern oder Besuchern", Seite 33*)
- Besucher (siehe *Abschnitt 4.1.8 "Verwalten externer Links von Mitarbeitern oder Besuchern", Seite 33*)
- Schlüssel (siehe *Abschnitt 4.2.6 "Externe Links für Benutzerschlüssel verwalten", Seite 38*)
- Zylinder (siehe *Abschnitt 4.4.4 "Externe Links für Zylinder verwalten", Seite 59*)
- Zugangsprofile (siehe *Abschnitt 4.6.5 "Bearbeiten von externen Links von Zugangsprofilen", Seite 73*)
- Remote-PGs (siehe *Abschnitt 6.5.6 "Externe Links von Remote-Programmiergeräten verwalten", Seite 111*)

Jedem Objekt können mehrere externe Links zugeordnet werden.

8.5 Zylinderprogrammierung

Zur Zylinderprogrammierung gehört das Update einer Zylinder-Zugangsliste oder das Auslesen von Zylinder-Ereignislisten.

Ein **Zylinderprogrammierungs-Job** wird in CWM unter den folgenden Umständen angelegt:

- Wenn die berechtigten Schlüssel für einen Zylinder aktualisiert werden.
- Wenn ein Schlüssel in der Zugangsliste des Zylinders als verloren oder defekt gemeldet wird.
- Wenn die Reprogrammierung eines Zylinders gewählt wurde.
- Wenn das Auslesen einer Zylinder-Ereignisliste gewählt wurde.
- Wenn die Zylindergruppe, zu der ein Zylinder gehört, geändert wird.

Wenn die Aufträge zur Zylinderprogrammierung ausgeführt werden sollen, werden sie zuerst in einen Programmierschlüssel im lokalen PG oder im Remote-Programmiergerät geladen. Beim Einführen des Programmierschlüssels in den Zylinder wird der Programmierauftrag ausgeführt und werden ggf. die Ereignislisten des Zylinders auf den Programmierschlüssel geladen. Nach Ausführung des Programmierauftrags wird der Programmierschlüssel erneut in das lokale PG oder in das Remote-Programmiergerät eingesteckt und die Schließanlage kann mit Informationen über die abgeschlossenen Programmieraufträge und abgerufenen Ereignislisten aktualisiert werden.

Abbildung 12 "Zylinderprogrammierung", Seite 189 zeigt zwei Vorgehensweisen bei der Ausführung von Zylinderprogrammier-Jobs:

- Im ersten Fall (1) wird der Zylinderprogrammierjob über ein lokales Programmiergerät auf den Programmierschlüssel des Administrators (A) geladen. Der Programmierschlüssel wird anschließend zum zu programmierenden Zylinder gebracht und dort eingesteckt. Nach Ausführung des Jobs wird der Schlüssel zurückgebracht, um die Schließanlage zu aktualisieren.
- Im zweiten Fall (2) meldet sich ein Administrator mithilfe eines Programmierschlüssels (A) bei CWM an, um Zylinderprogrammierjobs vorzubereiten, die andere Administratoren mit ihren Programmierschlüsseln (B)

mit einem Remote-Programmiergerät abrufen. Die Programmierschlüssel werden anschließend in die Zylinder eingesteckt und zum Remote-Programmiergerät zurückgebracht, um die Schließanlage zu aktualisieren.

Die Option, Zylinderprogrammier-Jobs über ein Remote-Programmiergerät aufzunehmen, auszuführen und zu bestätigen, ermöglicht, dass ein Administrator die Jobs in CWM vorbereitet und ein anderer Administrator die Zylinder programmiert, ohne am CWM angemeldet zu sein.

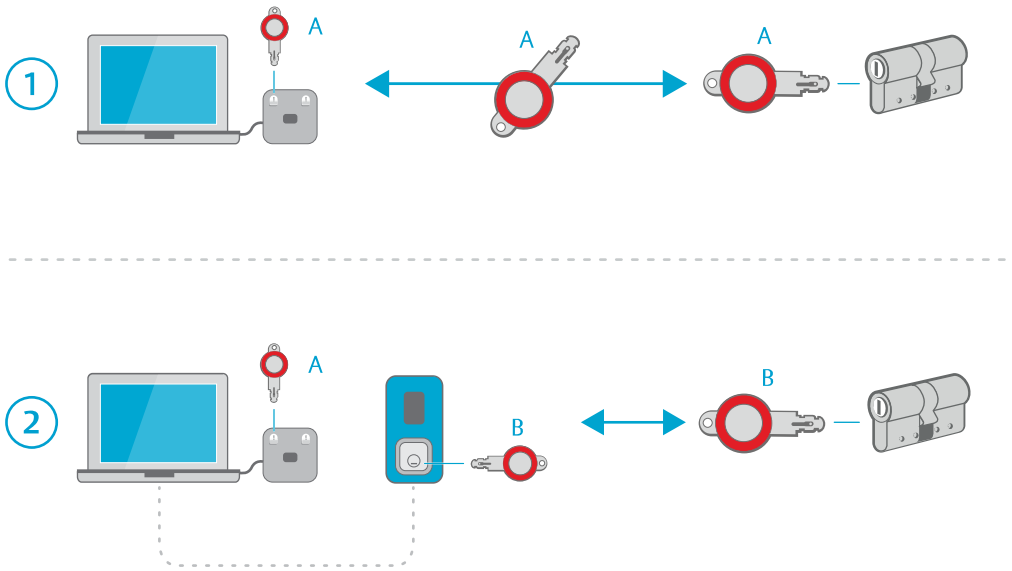


Abbildung 12. Zylinderprogrammierung

In CWM werden durchgängig folgende Symbole für Zylinderprogrammierungs-Jobs verwendet:

- Zylinderprogrammierungs-Job vorhanden
- Zylinderprogrammierungs-Job muss genehmigt werden
- Zylinderprogrammierungs-Job wurde auf Programmierschlüssel übertragen
- Zylinderprogrammierungs-Job ist abgeschlossen
- Zylinderprogrammierungs-Job fehlgeschlagen oder abgebrochen
- Zylinderprogrammierungs-Job wurde durch einen neuen Job ersetzt

Zylinderprogrammierungs-Jobs können nur auf Programmierschlüssel mit **Zylinderprogrammierungs-Recht** geladen werden.

Jobs, die den Austausch der Zylindergruppe eines Zylinders umfassen, erfordern auch einen Programmierschlüssel mit Fähigkeit zur **Zylindergruppenprogrammierung**. Ob ein Programmierschlüssel die Fähigkeit zur Zylindergruppenprogrammierung hat, steht in den Detailinformationen des Programmierschlüssels. Siehe *Abschnitt 6.11.1 "Suchen nach Programmierschlüsseln", Seite 137* oder *Abschnitt 6.11.2 "Abfragen eines Programmierschlüssels", Seite 138*. In Systemen, die ursprünglich als

Zylindergruppensysteme geliefert wurden, haben alle Programmierschlüssel diese Fähigkeit.

Siehe auch *Abschnitt 4.4.13 "Programmieren von Zylindern", Seite 64* und *Abschnitt 8.8 "CWM-Rollen und Administratorrechte", Seite 192*.

Reprogrammierung
Die Reprogrammierung lässt sich als erste Fehlerbehebungsmaßnahme einsetzen, wenn ein Zylinder nicht wie erwartet funktioniert. Wenn beispielsweise ein Programmierschlüssel bei der Zylinderprogrammierung zu früh abgezogen wird, funktioniert der Zylinder nicht korrekt. Dieses Problem wird durch eine erneute Programmierung behoben.

Wenn der Programmierschlüssel mit einem fehlgeschlagenen Programmierjob in ein Remote-Programmiergerät eingesteckt wird, erstellt CWM automatisch den Programmierjob neu, um ihn anschließend wieder an den Schlüssel zu senden. Dadurch kann der Schlüsselhalter den Programmierjob erneut durchführen.

CWM benachrichtigt außerdem den Administrator mit einer E-Mail, die Informationen über den verwendeten Schlüssel, den betroffenen Zylinder und den Grund für die Programmierung zum Zeitpunkt des Fehlers enthält. Diese Funktion ist immer eingeschaltet und lässt sich nicht deaktivieren.

Wenn ein Zylinder reprogrammiert wird, wird der Inhalt seines Speichers gelöscht, einschließlich der Ereignislisten. Als Teil der Reprogrammierung wird die Zylinderzugangsliste wiederhergestellt. Dies unterscheidet sich von der herkömmlichen Zylinderprogrammierung, bei der die Zylinderzugangsliste nur aktualisiert wird und die Ereignisliste unberührt bleibt.

Um den eigentlichen Reprogrammierjob durchzuführen, wird ein Hauptprogrammierschlüssel bzw. ein Normalprogrammierschlüssel mit Berechtigung zur Zylinder-Reprogrammierung benötigt.

Siehe auch *Abschnitt 4.4.12 "Zylinder-Reprogrammierung anfordern", Seite 64*.

8.6 Ereignislisten

Sowohl Zylinder als auch Schlüssel verfügen über eine Ereignislisten-Funktion. Eine Ereignisliste listet alle Schlüssel auf, die Zugang zu einem Zylinder angefordert haben, sowie Schlüssel und Zylinder, die programmiert wurden. Es gibt zwei Arten von Ereignislisten:

- **Normale Ereignislisten** enthalten Ereignisse, bei denen die betroffenen Geräte zur gleichen Schließanlage gehören.
- **Fremde Ereignislisten** enthalten Ereignisse, bei denen die betroffenen Geräte zu anderen Schließanlagen gehören.

Schlüssel-Ereignislisten
Nur E2-Schlüssel und E3-Schlüssel können Ereignislisten speichern.

Die Schlüssel-Ereignisliste protokolliert die Zylinder, in denen der Schlüssel einen Zugang versucht hat, den Schlüsselhalter zum betreffenden Zeitpunkt (falls nicht dauerhaft gelöscht oder deaktiviert) sowie Programmierjobs, die auf dem Schlüssel ausgeführt wurden. Außerdem sind die Zeit und das Ergebnis dieser Vorgänge aufgeführt.

Zylinder-Ereignislisten
Die Zylinder-Ereignisliste protokolliert, mit welchen Schlüsseln versucht wurde, auf den Zylinder zuzugreifen, den Schlüsselhalter zum entsprechenden Zeitpunkt (falls nicht

dauerhaft gelöscht) sowie ausgeführte Programmierjobs. Außerdem sind die Zeit und das Ergebnis dieser Vorgänge aufgeführt. Beachten Sie, dass die Ereignislisten keine Zylinderzugriffsversuche mit mechanischen Schlüsseln aufzeichnet.

Automatischer Ereignislistenabruf
Wenn ein Benutzerschlüssel zu einer Remoteanlage gehört, Remote-Updates unterstützt, ein E2-Schlüssel oder ein dynamischer Schlüssel ist und Genehmigungen für Ereignislisten deaktiviert sind, löst die Ausgabe des Benutzerschlüssels die Erstellung eines Remote-Jobs zum Lesen der Ereignisliste aus.

Ein Programmierschlüssel lässt sich so programmieren, dass er Zylinder-Ereignislisten automatisch abruft. Dadurch kann der Schlüsselhalter einfach und schnell Ereignislisten aus beliebigen Zylindern innerhalb der Domäne abrufen. Siehe auch *Abschnitt 6.11.13 "Automatischen Ereignislistenabruf für Programmierschlüssel aktivieren oder deaktivieren", Seite 146*.

Automatisches Entfernen des Ereignislistenarchivs
Das Ereignislistenarchiv lässt sich so konfigurieren, dass Ereignislisten, die älter als eine festgelegte Anzahl von Tagen sind, automatisch entfernt werden. Dieser Löschvorgang basiert auf dem Erstellungsdatum, d. h. dem Datum, an dem der Eintrag auf dem physischen Element erzeugt wurde, und nicht auf dem Analysedatum, d. h. dem Datum, an dem der Eintrag in der CWM-Datenbank gespeichert wurde.

Sofern nicht die Lizenz **Erweiterte Ereignisliste und Ereignisarchiv** erteilt wurde, kann für das automatische Entfernen ein Zeitraum von bis zu 366 Tagen festgelegt werden.

Wenn die Lizenz **Erweiterte Ereignisliste und Ereignisarchiv** erteilt wurde, kann für das automatische Entfernen ein Zeitraum von bis zu 3660 Tagen festgelegt werden.

Genehmigungen
Bei Schließanlagen, in denen die Funktion **Genehmigungen** aktiviert ist, müssen alle Ereignislistenanforderungen für Schlüssel und Zylinder von einem Administrator mit der Rolle **Genehmigender** genehmigt werden. Nach dem Auslesen einer Ereignisliste aus einem Schlüssel oder Zylinder kann diese von jedem beliebigen Administrator mit Anzeigeberechtigung für **Ereignislisten** angezeigt werden. Siehe auch *Abschnitt 8.8 "CWM-Rollen und Administratorrechte", Seite 192*.

Die Funktion wird unter **Systemeinstellungen** aktiviert oder deaktiviert. Siehe *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

8.7 Ereignisse

Vom Administrator in den folgenden CWM-Komponenten ausgeführte Vorgänge werden als Ereignisse gespeichert und auf der Registerkarte **Ereignisse** jeder Komponente angezeigt.

- **Mitarbeiter oder Besucher**

  Informationen zum Anzeigen von Mitarbeiter- oder Besucherereignissen finden Sie in *Abschnitt 4.1.10 "Anzeigen von Ereignissen für Mitarbeiter oder Besucher", Seite 34*.

- **Schlüssel**

  Informationen zum Anzeigen von Schlüsselereignissen finden Sie in *Abschnitt 4.2.8 "Anzeigen der Ereignisse für eine Benutzerschlüssel", Seite 40*.

- **Zylinder**

Informationen zum Anzeigen von Zylinderereignissen finden Sie in *Abschnitt 4.4.7 "Anzeigen von Ereignissen für einen Zylinder", Seite 60*.

- **Zylindergruppe**

  Informationen zum Anzeigen von Zylindergruppenereignissen finden Sie in *Abschnitt 4.5.5 "Anzeigen von Ereignissen für eine Zylindergruppe", Seite 70*.

- **Zugangsprofil**: zum Beispiel Hinzufügen und Entfernen von Zylinder in einem Zugangsprofil.

  Informationen zum Anzeigen von Ereignissen in Bezug auf Zugangsprofile finden Sie in *Abschnitt 4.6.7 "Anzeigen von Ereignissen für ein Zugangsprofil", Seite 74*.

- **Temporäre Zugangsgruppe**

  Informationen zum Anzeigen von Ereignissen in Bezug auf Zugangsprofile finden Sie in *Abschnitt 4.7.6 "Anzeigen von Ereignissen für eine temporäre Zugangsgruppe", Seite 78*.

- **Remote-Programmiergerät**

  Informationen zum Anzeigen von Ereignissen zu Remote-Programmiergeräten finden Sie in *Abschnitt 6.5.9 "Ereignisprotokoll des Remote-Programmiergeräts anzeigen", Seite 125*.

- **Programmierschlüssel**

  Informationen zum Anzeigen von Ereignissen in Bezug auf Programmierschlüssel finden Sie in *Abschnitt 6.11.6 "Anzeige der Programmierschlüssel-Ereignisse", Seite 140*.

Automatische Bereinigung des Ereignisarchivs
Das Ereignisarchiv lässt sich so konfigurieren, dass Ereignislisten, die älter als eine festgelegte Anzahl von Tagen sind, automatisch entfernt werden.

Sofern nicht die Lizenz **Erweiterte Ereignisliste und Ereignisarchiv** erteilt wurde, kann für das automatische Entfernen ein Zeitraum von bis zu 366 Tagen festgelegt werden.

Wenn die Lizenz **Erweiterte Ereignisliste und Ereignisarchiv** erteilt wurde, kann für das automatische Entfernen ein Zeitraum von bis zu 3660 Tagen festgelegt werden.

HINWEIS!
Die folgenden Ereignisse werden nicht automatisch entfernt und verbleiben auch nach Ablauf des Beibehaltungszeitraums in der Historie:

- Aktivierung von Schlüsseln, Zylindern und Remote-Programmiergeräten
- Das neueste Schlüsselausgabeereignis in den Mitarbeiter- oder Besuchereignissen und in den Schlüsselereignissen.

8.8 CWM-Rollen und Administratorrechte

Rollen werden durch die Kombination der erteilten Berechtigungen definiert und Programmierschlüsseln zugewiesen.

Jede Berechtigung gewährt einer Rolle bestimmte Rechte zum Ausführen der verschiedenen CWM-Funktionen.

Rollen

Die in CWM sichtbaren Funktionen hängen von der Rolle ab, die dem Programmierschlüssel zugewiesen ist, der vom angemeldeten Administrator verwendet wird. Wir empfehlen, dass Administratoren nur Zugriff auf Funktionen haben sollten, die sie für ihre Arbeit benötigen. Beispielsweise kann ein Administrator, der nur Programmieraufgaben für Zylinder durchführt, nur Zugriff auf diese Funktion haben. Ein Administrator, der für das Schlüsselmanagement zuständig ist, kann nur Zugriff auf die Funktionen für Schlüsselausgabe/-rückgabe und verlorene/defekte Schlüssel haben.

HINWEIS!
Die für Administratoren festgelegten Rollen sind nicht mit den von den Zugangsprofilen definierten Nutzerrollen zu verwechseln.

In CWM sind folgende Rollen vordefiniert:

Tabelle 2. Vordefinierte Rollen

Rolle	Beschreibung
Super-Administrator	Vollständige Rechte mit Ausnahme der Berechtigung zur Genehmigung von Ereignislistenanforderungen.
Administrator	Rechte für wichtige Aufgaben wie die Konfiguration von Berechtigungen, Bearbeiten von Vorlagen usw.
Schlüsselausgabestelle	Rechte, die für einfachere, alltägliche Aufgaben benötigt werden, z. B. Schlüsselausgabe und -rücknahme.
Genehmigender	Hat nur das Recht zur Genehmigung der Anforderung von Ereignislisten.
Zylinderprogrammierer	Hat nur das Recht zur Zylinderprogrammierung.
WebService	Dient der Integrierung von Web Services.

Die Rollen Super-Administrator und Genehmigender können nicht gelöscht oder bearbeitet werden. Die WebService-Rolle kann bearbeitet, aber nicht gelöscht werden.

Einem Programmierschlüssel können mehrere Rollen zugewiesen werden, aber die Rolle des Genehmigenden kann nicht mit anderen Rollen kombiniert werden. Weitere Informationen zum Zuweisen von Rollen finden Sie unter *Abschnitt 6.11.4 "Bearbeiten von Programmierschlüsselinformationen", Seite 139*.

HINWEIS!
Bestimmte Rechte für Programmierschlüssel hängen vom Typ des Programmierschlüssels ab und lassen sich nicht über Rollen und Berechtigungen konfigurieren. Siehe *Abschnitt 7.2.4 "Programmierschlüssel", Seite 161*.

Standardmäßig sind die oben beschriebenen Rollen in einer flachen Struktur organisiert. Administratoren können Rollen mit höheren Berechtigungen als den eigenen Berechtigungen erstellen oder bearbeiten und können diese Rollen einem Programmierschlüssel zuweisen oder Zuweisungen aufheben.

Wenn die Funktion der hierarchischen Administratoren aktiviert ist, werden die Rollen hierarchisch organisiert und gelten die folgenden Einschränkungen:

- Ein Administrator kann keine Berechtigungsstufen über der eigenen Berechtigungsstufe konfigurieren.

- Ein Administrator kann keine Rollen mit einer höheren als der eigenen Berechtigungsstufe zuweisen oder löschen.

Die Rangordnung der Rollen in der Hierarchie wird von der Berechtigungsstufe bestimmt. Eine Rolle mit höherer Berechtigungsstufe als der Berechtigungsstufe des Administrators wird als der Administratorrolle übergeordnete Rolle betrachtet und kann vom Administrator nicht bearbeitet oder gelöscht werden.

Die Funktion der hierarchischen Administratoren wird vom Super-Administrator auf der Seite **Systemeinstellungen** aktiviert.

Rechte
Für jede Rolle werden Berechtigungen nach CWM-Funktion erteilt, z. B. die Verwaltung von Schlüsseln, Zylindern, Mitarbeitern, Firmware, Systemeinstellungen oder Programmierschlüsseln.

Die Rechte für eine CWM-Funktion werden auf eine der folgenden Ebenen festgesetzt:

Tabelle 3. Ebenen für Administratorrechte

Ebene	Beschreibung
Keine	Kein Zugriff
Liste	Erlaubt das Suchen und Auflisten.
Anzeige	Erlaubt die Anzeige von Einzelheiten.
Voll	Erlaubt auch die Bearbeitung von Daten.

Für eine vollständige Liste der Rechte und der erlaubten Vorgänge auf jeder Ebene siehe *Abschnitt 9.4 "Rechte", Seite 206*.

Siehe auch *Abschnitt 6.7 "Verwalten von Rollen und Rechten", Seite 131*.

8.9 Löschen von Personendaten und DSGVO-Erfüllung

In CWM gibt es zwei mögliche Einstellungen für das Löschen von Mitarbeitern und Besuchern: **Dauerhaft löschen** und **Als gelöscht kennzeichnen**. Das Verhalten wird über die Systemeinstellung **Beim Löschen von Personen** bestimmt.

Dauerhaft löschen
Zur Einhaltung der DSGVO muss die Einstellung zum Löschen personenbezogener Daten auf **Dauerhaft löschen** gesetzt sein. Bei dieser Einstellung gilt Folgendes:

- Personen werden zusammen mit allen zugehörigen Daten dauerhaft aus der Datenbank gelöscht und können nicht mehr wiederhergestellt werden. Verweise auf eine gelöschte Person in Ereignisprotokollen und Ereignislisten werden dauerhaft durch **Keine Angabe** ersetzt.
- Neben dem **Löschen** gibt es auch eine Funktion zum **Deaktivieren** einer Person. Deaktivieren bedeutet, dass sämtliche Personendaten verborgen sind und auf keinerlei Weise verarbeitet werden, so lange die Person deaktiviert ist. Verweise auf deaktivierte Personen in Ereignisprotokollen und Ereignislisten werden vorübergehend durch **Keine Angabe** ersetzt. Diese Verweise werden bei der Reaktivierung einer Person wiederhergestellt. Nur Administratoren mit der Berechtigung **Schlüsselhalter deaktivieren** können Personen deaktivieren sowie deaktivierte Personen einsehen und reaktivieren.
- Dies ist die einzige Möglichkeit zum Bearbeiten, Löschen, Exportieren oder Verarbeiten von Informationen.

- Beim Import von Mitarbeitern aus einer Datei werden in CWM deaktivierte Mitarbeiter ignoriert, auch wenn ihre Daten in der CSV-Datei geändert werden.

Siehe auch *Abschnitt 4.1.3 "Deaktivieren oder Aktivieren von Mitarbeitern oder Besuchern", Seite 26*.

Als gelöscht kennzeichnen

Bei der Einstellung **Als gelöscht markiert** erfolgt das Löschen personenbezogener Daten nicht gemäß DSGVO.

Gelöschte Personen werden nicht aus der Datenbank gelöscht und es könnte weiterhin beispielsweise in Ereignissen und Ereignislisten auf eine gelöschte Person verwiesen werden. Gelöschte Personen können gemäß *Abschnitt 4.1.4 "Löschen oder Wiederherstellen von Mitarbeitern oder Besuchern", Seite 27* wiederhergestellt werden. Eine Person, die nicht zum Löschen vorgemerkt ist, wird in CWM als **Aktiv** beschrieben (nicht zu verwechseln mit deaktivierten oder aktivierten Personen in der Systemeinstellung **Dauerhaft löschen**).

8.10 Single Sign-on (SSO)

Mit Single Sign-on (SSO) können Administratoren ohne Programmierschlüssel auf die Anlage zugreifen.

Die SSO-Funktionalität muss in jeder Anlage individuell konfiguriert werden. Wenn SSO unterstützt wird, kann der Superadministrator die Funktion je nach Bedarf aktivieren oder deaktivieren. Weitere Details finden Sie unter *"SINGLE SIGN-ON (SSO)"* in *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102*.

Wenn diese Funktion aktiviert ist, muss ein Administrator, der einen neuen Programmierschlüssel erhalten hat, zunächst mit CCPC und dem Programmierschlüssel ein Zertifikat registrieren. Nach erfolgreicher Registrierung des Zertifikats kann sich der Administrator ohne Programmierschlüssel an der Anlage anmelden.

Bestimmte Vorgänge innerhalb der Anlage, zum Beispiel Programmierjobs, die auf dem Programmierschlüssel gespeicherte sichere Daten benötigen, erfordern weiterhin die Anmeldung des Administrators mit dem Programmierschlüssel. In diesen Fällen wird eine Popup-Meldung angezeigt, die den Benutzer auffordert, den Programmierschlüssel einzufügen und sich entsprechend zu authentifizieren.

Für die folgenden Funktionen ist eine Anmeldung mit dem Programmierschlüssel erforderlich:

- Lokale Zylinderprogrammierung: Senden von Aufgaben an den Programmierschlüssel, Aktualisieren seines Status und Entfernen beendeter oder nicht beendeter Aufgaben
- Kopieren einer Schlüsselkonfiguration
- Aktivieren des Erweiterungsimports
- Aktivieren oder Deaktivieren des automatischen Abrufens von Ereignislisten auf dem Programmierschlüssel
- Entsperren des Programmierschlüssels
- PIN des Programmierschlüssels ändern
- Status eines in das lokale Programmiergerät eingesteckten Benutzerschlüssels über die obere Leiste der Seite aktualisieren

8.11 DCS-Integration

DCS ist eine Serveranwendung zur Verwaltung von Zertifikaten und Lizenzen in einer CLIQ-Schließanlage.

Die **DCS-Integration** ermöglicht die automatische Erstellung von Zertifikaten für Programmierschlüssel und Remote-PGs, wodurch sich die separate Verteilung dieser Zertifikate erübrigt. Sie ermöglicht auch das Abrufen von Lizenz-, Firmware- und Erweiterungsdateien von DCS.

Die DCS-Integration muss während der Installation der Anlage aktiviert werden.

Wenn die DCS-Integration aktiviert ist, werden Zertifikate für Remote-Programmiergeräte aus CWM heraus erstellt; Zertifikate für Programmierschlüssel werden hingegen über **CLIQ Connect PC** erstellt.

Die Zertifikatanmeldung für Programmierschlüssel kann auf **immer zulässig** (empfohlen), **Einmal zulässig** oder **nicht zulässig** eingestellt werden. Die Einstellung erfolgt für den Hauptprogrammierschlüssel in DCS und für normale Programmierschlüssel in CWM (siehe *Abschnitt 6.11.4 "Bearbeiten von Programmierschlüsselinformationen", Seite 139*).

Tabelle 4. Einstellung der Zertifikatanmeldung

Einstellung	Beschreibung
Immer zulässig	Das Programmierschlüssel-Zertifikat kann vielfach erstellt werden. Dies ist hilfreich, wenn der Programmierschlüsselhalter vom mehreren Computern aus Zugang zu CWM benötigt.
Einmal zulässig	Das Programmierschlüssel-Zertifikat kann nur einmal erstellt werden.
Nicht zulässig	Eine Anmeldung ist nicht zulässig.

HINWEIS!
Die Zertifikat-Erneuerung ist unabhängig von dieser Einstellung zulässig.

Informationen zum Generieren von Zertifikaten für Programmierschlüssel finden Sie unter *Abschnitt 3.2.1 "Registrierung des Zertifikats für den Programmierschlüssel über CLIQ Connect PC", Seite 17*.

Informationen zum Erstellen von Zertifikaten für Remote-Programmiergeräte finden Sie in *Abschnitt 6.5.7 "Konfigurieren von Wand-Programmiergeräten", Seite 112* oder *Abschnitt 6.5.8 "Konfigurieren von mobile Programmiergeräten", Seite 119*.

Abfragen einer Lizenzdatei aus DCS siehe *Abschnitt 6.1.1 "Installieren von Lizenzen", Seite 101*.

Abfragen einer Erweiterungsdatei aus DCS siehe *Abschnitt 6.16 "Importieren von Erweiterungen", Seite 157*.

8.12 LDAP-Integration

LDAP steht für „Lightweight Directory Access Protocol“ und ist ein Softwareprotokoll für den Zugriff auf Verzeichnisdienste. Im Kontext von CWM wird LDAP als Hauptquelle für Mitarbeiterinformationen verwendet, indem es mit CWM integriert wird. CWM unterstützt OpenLDAP, Microsoft Active Directory und Apache Directory.

Bei bestehender LDAP-Integration werden die in einem bestimmten Verzeichnis hinzugefügten Mitarbeiter automatisch (alle 24 Stunden) oder manuell mit CWM

synchronisiert. In CWM werden die aus LDAP abgerufenen Mitarbeiter neben den Mitarbeiter aus CWM angezeigt. Vorname, Nachname, E-Mail-Adresse und Telefonnummer der Mitarbeiter aus LDAP werden angezeigt und können durchsucht werden.

Wenn die Funktion CLIQ Connect+ aktiviert ist und der Mitarbeiter ein in CLIQ Connect+ aktivierter Benutzer ist, ist es nicht möglich, den Mitarbeiter zu deaktivieren oder zu löschen oder die E-Mail-Adresse zu löschen. Weitere Informationen zu CLIQ Connect+ finden Sie unter *Abschnitt 8.3.4 "CLIQ Connect und CLIQ Connect+", Seite 187*.

Weil die Information aus LDAP schreibgeschützt sind, gelten bei der Verwaltung von Mitarbeitern in CWM bestimmte Einschränkungen, wenn die LDAP-Integration aktiviert ist. *Tabelle 33 "Verfügbare Aktivitäten in CWM bei Integration mit LDAP", Seite 197* zeigt, welche Verwaltungsaufgaben die Administratoren ausführen können.

Tabelle 5. Verfügbare Aktivitäten in CWM bei Integration mit LDAP

	Mitarbeiter	
	aus LDAP-Integration	**ohne LDAP-Integration**
Hinzufügen	Keine Angabe	✓
Bearbeiten	✓* * Nur **Domäne** und **TAGS** können über die Benutzeroberfläche geändert werden.	✓
Löschen/Deaktivieren	Keine Angabe	✓

Die LDAP-Integration wird auf der Seite **Systemeinstellungen** aktiviert bzw. deaktiviert. Informationen zur Einstellung der LDAP-Integration sind in *Abschnitt 6.4 "Bearbeiten der Systemeinstellungen", Seite 102* verfügbar. Als Voraussetzung müssen den Administratoren die Lizenz und die Rechte für die LDAP-Integration erteilt werden. Informationen zum Installieren der Lizenz sind in *Abschnitt 6.1 "Verwalten von Lizenzen", Seite 101* und Informationen zum Erteilen der Rechte in *Abschnitt 6.7 "Verwalten von Rollen und Rechten", Seite 131* verfügbar.

8.13 Lizenzierung

Die Verwendung von CWM erfordert eine Lizenz. Lizenzen werden je Schließanlage vom lokalen CLIQ-Händler herausgegeben.

Eine gültige Lizenz ermöglicht immer Zugriff auf die grundlegenden CWM-Funktionen. Zusätzlich regelt der Lizenzumfang die Verfügbarkeit folgender Funktionen:

- Remote
- Domänen
- Zugangsprofile
- Temporäre Zugangsgruppen
- Verlängerung
- Flexible Verlängerung
- Zylindergruppen
- Web-Dienste
- PIN-Validierung

- LDAP-Integration
- Erweiterte Ereignisliste und Ereignisarchiv
- CLIQ Connect+

Die verfügbaren lizenzierten Funktionen sind in *Abschnitt 6.1.2 "Lizenzstatus anzeigen", Seite 101* beschrieben.

Für Systeme mit aktivierter **DCS-Integration** sucht CWM alle 24 Stunden und beim Starten von CWM automatisch nach verfügbaren Lizenzen. Wenn keine Lizenz in DCS verfügbar ist oder die DCS-Integration nicht aktiviert wurden, müssen die Lizenzen manuell installiert werden. Siehe *Abschnitt 6.1.1 "Installieren von Lizenzen", Seite 101*.

Lizenzdateien erhalten in der Reihenfolge ihrer Erstellung eine Lizenznummer. Es kann nur eine Lizenzdatei installiert werden, die später als die aktuell installierte Datei erstellt wurde.

Lizenzablauf und E-Mail-Benachrichtigung

Eine Lizenz hat ein **reguläres Ablaufdatum** und ein **Kulanzablaufdatum**.

Nach Verstreichen des regulären Ablaufdatums werden jeden Montag Benachrichtigungs-E-Mails an den **Super-Administrator** gesendet, bis die Lizenz verlängert wurde. Wenn das reguläre Ablaufdatum beispielsweise auf einen Dienstag fällt, wird die erste Benachrichtigungs-E-Mail am folgenden Montag gesendet. Damit der Administrator die E-Mails empfängt, muss eine E-Mail-Adresse für ihn registriert sein. Zusätzlich wird in der CWM-Benutzeroberfläche eine Warnmeldung angezeigt. Wenden Sie sich an Ihren örtlichen CLIQ-Händler, um eine neue Lizenz zu erhalten.

Nach Verstreichen des Kulanzablaufdatums wird CWM beim Starten gesperrt. Auf der Startseite wird eine Warnmeldung angezeigt und eine E-Mail mit der Benachrichtigung über das Ablaufdatum wird gesendet. Wenden Sie sich an Ihren örtlichen CLIQ-Händler, um eine neue Lizenz zu erhalten.

Weitere Informationen zur Installation von Lizenzen finden Sie unter *Abschnitt 6.1.1 "Installieren von Lizenzen", Seite 101*.

Wenn die Lizenzen mit einer externen Software (nicht DCS) verwaltet werden, erfolgt die Lizenzverlängerung üblicherweise am regulären Ablaufdatum. In diesem Fall wird keine Benachrichtigungs-E-Mail gesendet.

9 Anhang

9.1 Begriffe und Abkürzungen

9.1.1 Begriffe

Tatsächlicher Status Beschreibt den Status der Schlüssel-Berechtigungen, wie sie tatsächlich in Schlüsseln und Zylindern programmiert sind. Siehe auch **Definierter Status**.

Zylinderzugangsliste In Zylindern gespeicherte Liste berechtigter Schlüssel.

Zylindergruppensystem Eine Schließanlage, die für die Unterstützung von Zylindergruppen vordefiniert ist.

Zylinderprogammier-Job Ein Job, der Updates für einen Zylinder enthält und mit Hilfe eines Programmierschlüssels im Zylinder durchgeführt werden kann.

Zylinder-Reprogrammierung Dieser Vorgang löscht den Speicherinhalt eines Zylinders und stellt anschließend die Zugangsliste für den Zylinder, die Liste der nicht berechtigten Schlüssel und andere Konfigurationen, z. B. die Zeitzonen-Verschiebung, aus der Datenbank wieder her.

DCS-Integration Eine Funktion in CWM, die die automatische Erstellung von Zertifikaten für Programmierschlüssel und Remote-Programmiergeräte ermöglicht.

Definierter Status Beschreibt den Status der Schlüssel-Berechtigungen, wie er in CWM definiert ist. Dieser muss nicht unbedingt dem tatsächlichen Status entsprechen, da einige der Berechtigungen unter Umständen noch nicht in den Schlüsseln und Zylindern programmiert wurden. Siehe auch **Tatsächlicher Status**.

Element CLIQ-Elemente sind CLIQ-Schlüssel und -Zylinder.

Expliziter Zugang Eintrag in der Zugangsliste für E3-Schlüssel, der explizit für einen bestimmten Schlüssel hinzugefügt wird. Siehe auch **Impliziter Zugang**.

Erweiterung Ein Zusatz zu einer Schließanlage, der neue Schlüssel, Schlüsselgruppen, Zylinder, Zylindergruppen und Remote-Programmiergeräte enthält.

Impliziter Zugang Eintrag in der Zugangsliste für E3-Schlüssel, der über Zugangsprofile hinzugefügt wird, die mit einer Person oder direkt mit einem Schlüssel verknüpft sind. Siehe auch **Expliziter Zugang**.

Schlüsselzugangsliste In E3-Schlüsseln gespeicherte Liste berechtigter Zylinder.

Liste der nicht berechtigten Schlüssel Liste der Schlüssel, die für den Zugang zu einem Zylinder gesperrt wurden, nachdem sie als verloren gemeldet wurden.

Schließanlage Ein System von Zylindern und Schlüsseln, die gemeinsam verwaltet werden. In diesem Handbuch umfasst diese Bezeichnung auch die zugehörigen PGs und die zugehörigen Informationen, die in CWM

	definiert sind (z. B. die elektronischen Berechtigungen, Mitarbeiter- und Besucherdaten, Definitionen von Administratorrollen, Systemeinstellungen usw.).
Objekt	Einheiten, die über CWM verwaltet werden können, z. B. Schlüssel, Schlüsselgruppen, Zylinder, Zylindergruppen, Zugangsprofile, Remote-PGs, Mitarbeiter und Besucher.
Remote-System	Eine Schließanlage, bei der die Remote-Funktionalität aktiviert ist.
Remote Update Job	Ein Job, der Updates für einen Schlüssel enthält und durch Einstecken in ein Remote-Programmiergerät auf dem Schlüssel ausgeführt werden kann.
USB On-The-Go	Ein USB-Standard, der USB-Geräten die Funktion als Host ermöglicht.

9.1.2 Abkürzungen

CSV	Comma Separated Values (ein Dateiformat)
CWM	CLIQ Web Manager
DCS	Digital Content Server
DSGVO	Datenschutz-Grundverordnung (eine EU-Verordnung zur Verarbeitung von Personendaten)
PG	Programmiergerät
USB OTG	USB On-The-Go

9.2 In CWM verwendete Symbole

Nutzerschlüssel


Mechanischer Schlüssel


E1-Schlüssel


E2-Schlüssel


CLIQ Connect E2-Schlüssel


E3-Schlüssel


CLIQ Connect E3-Schlüssel


E1-Schlüssel-Gruppe


E3-Schlüssel-Gruppe


Für den Schlüssel steht ein Remote-Update an


Anstehendes Remote-Update überschreitet Schlüsselkapazität

Programmierschlüssel

 Hauptprogrammierschlüssel

 Normalprogrammierschlüssel

 Normale CLIQ Connect-Programmierschlüssel

 Normalprogrammierschlüssel-Gruppe

 Hauptprogrammierschlüssel-Gruppe

 Programmierungs-Job wurde nicht an einen Programmierschlüssel gesendet

 Programmierungs-Job wurde an einen Programmierschlüssel gesendet, aber noch nicht initiiert

 Bestimmte Programmierungs-Jobs wurden an einen Programmierschlüssel gesendet, aber nicht alle

 Programmierungs-Job ist abgeschlossen

 Programmierungs-Job fehlgeschlagen oder abgebrochen

 Programmierungs-Job wurde durch einen neuen Job ersetzt

Zylinder

 Elektronischer Zylinder

 Mechanischer Zylinder

 Doppelzylinder (hier verwendetes Beispiel: A-Seite elektronisch; B-Seite mechanisch)

 Angaben gelten für A-Seite

 Angaben gelten für B-Seite

 Zylinderprogrammierungs-Job vorhanden

 Zylinderprogrammierungs-Job muss genehmigt werden

 Zylinderprogrammierungs-Job wurde auf Programmierschlüssel übertragen

 Zylinderprogrammierungs-Job ist abgeschlossen

 Zylinderprogrammierungs-Job fehlgeschlagen oder abgebrochen

 Zylinderprogrammierungs-Job wurde durch einen neuen Job ersetzt

Berechtigungen

 Explizite Berechtigung

 Berechtigung aus Zugangsprofil

Remote-Programmiergeräte

 Wand-Programmiergerät

 Mobiles CLIQ-Programmiergerät

9.3 Objektattribute

9.3.1 Mitarbeiterattribut

ID	Ein eindeutiger Code oder eine ID zur Identifizierung einer Person in der Anlage.
Anrede	Eine vor dem Namen verwendete Anrede wie Frau, Herr oder Dr.
Vorname	Der Vorname der Person.
Nachname	Der Nachname der Person.
Domäne	Die Domäne, zu der die Person gehört.
Organisation	Das Unternehmen oder die Institution, dem/der die Person angehört.
Telefon	Die Telefonnummer der Person.
Abteilung	Die spezifische Abteilung oder Einheit innerhalb der Organisation, in der die Person arbeitet.
Job	Die Berufsbezeichnung oder Funktion der Person innerhalb der Organisation.
E-Mail	Die E-Mail-Adresse der Person.
Region	Ein größeres geografisches Gebiet, in dem sich die Person befindet (z. B. EMEA, APAC).
Sprache	Die Hauptsprache, in der die Person kommuniziert.
Standort	Eine allgemeine Beschreibung des Ortes, an dem sich die Person befindet (kann sich mit **Ort** oder **Bundesland** überschneiden).
Zusatz-Text	
Straße	Die Straße (Teil der Adresse) der Organisation oder Person.
Postleitzahl	Die Postleitzahl der Adresse.
Ort	Der Ort (Teil der Adresse) der Person oder Organisation.
Bundesland	Das Bundesland, die Provinz oder die Region innerhalb eines Landes.
Firmenanschrift	Die vollständige Adresse der Organisation oder des Arbeitsplatzes der Person.

9.3.2 Besucherattribut

ID	Ein eindeutiger Code oder eine ID zur Identifizierung einer Person in der Anlage.
Anrede	Eine vor dem Namen verwendete Anrede wie Frau, Herr oder Dr.
Vorname	Der Vorname der Person.

Nachname	Der Nachname der Person.
Domäne	Die Domäne, zu der die Person gehört.
Organisation	Das Unternehmen oder die Institution, dem/der die Person angehört.
Telefon	Die Telefonnummer der Person.
Abteilung	Die spezifische Abteilung oder Einheit innerhalb der Organisation, in der die Person arbeitet.
Job	Die Berufsbezeichnung oder Funktion der Person innerhalb der Organisation.
E-Mail	Die E-Mail-Adresse der Person.
Region	Ein größeres geografisches Gebiet, in dem sich die Person befindet (z. B. EMEA, APAC).
Sprache	Die Hauptsprache, in der die Person kommuniziert.
Standort	Eine allgemeine Beschreibung des Ortes, an dem sich die Person befindet (kann sich mit **Ort** oder **Bundesland** überschneiden).
Straße	Die Straße (Teil der Adresse) der Organisation oder Person.
Postleitzahl	Die Postleitzahl der Adresse.
Ort	Der Ort (Teil der Adresse) der Person oder Organisation.
Bundesland	Das Bundesland, die Provinz oder die Region innerhalb eines Landes.
Firmenanschrift	Die vollständige Adresse der Organisation oder des Arbeitsplatzes der Person.

9.3.3 Schlüsselattribute

Name	Name des Schlüssels.
Schlüsselhalter	Die Person, an die ein Schlüssel aktuell ausgegeben ist.
Kennzeichnung	Die Schlüssel-Kennzeichnung.
Zweitkennzeichnung	Alternative Kennzeichnung (wird nicht in allen Fällen verwendet).
Schließung	Der mechanische Schnitt des Schlüssels
Gruppe	Die Schlüsselgruppe, zu der der Schlüssel gehört.
Typ	Schlüsseltyp. Weitere Informationen siehe *Abschnitt 7.2.3 "Nutzerschlüssel", Seite 160*.
Firmware	Firmware-Version.
Generation	Die Schlüsselgeneration.

Status	Schlüsselstatus (**Im Lager**, **Ausgegeben**, **Verloren** oder **Defekt**).
Zeile Nummer	Nicht verwendet.
Letztes Remote Update	Datum und Zeit des letzten Updates über ein Remote-Programmiergerät.
Größe der Zugangsliste	Verwendete Einträge / maximale Anzahl Einträge in der Schlüsselzugangsliste.
Unterstützung für Zeitzonen-Verschiebung	Zeigt an, ob die Funktion der Zeitzonen-Verschiebung unterstützt wird.
Tags	Für den Schlüssel definierte Tags.
Externe Links	Mit dem Schlüssel verknüpfte URLs.

9.3.4 Programmierschlüsselattribute

Name	Name des Programmierschlüssels.
Schlüsselhalter	Der Mitarbeiter, an den ein Programmierschlüssel aktuell ausgegeben ist.
Kennzeichnung	Die Programmierschlüssel-Kennzeichnung.
Zweitkennzeichnung	Alternative Kennzeichnung (wird nicht in allen Fällen verwendet).
Gruppe	Die Schlüsselgruppe, zu der der Programmierschlüssel gehört.
Typ	Der Programmierschlüssel-Typ. Weitere Informationen siehe *Abschnitt 7.2.4 "Programmierschlüssel", Seite 161*.
Firmware	Firmware-Version.
Generation	Die Generation des Programmierschlüssels.
Remote-Support	
Zylinder-Reprogrammierung	Ob der Programmierschlüssel die Berechtigung zur Ausführung von Zylinder-Reprogrammierjobs hat.
Zylindergruppenprogrammierung	Ob der Programmierschlüssel Zylinderprogrammierungs-Jobs ausführen kann, die die Zylindergruppe eines Zylinders ändern.
Zylinder-Firmware-Upgrade	Ob der Programmierschlüssel ein Upgrade der Zylinderfirmware durchführen kann (in Entwicklung).
Status	Programmierschlüsselstatus (**Im Lager**, **Ausgegeben**, **Verloren** oder **Defekt**).
Gesperrt	Ob der Programmierschlüssel gegen jeglichen Zugang gesperrt ist.
Gültigkeitseinstellungen	Einstellung zur Gültigkeit des Programmierschlüssels.

Zertifikatanmeldung	Ob die Zertifikatanmeldung zulässig ist.
Rollen	Welche Rollen mit dem Programmierschlüssel verknüpft sind.

9.3.5 Zylinderattribute

Name	Name des Zylinders.
Kennzeichnung	Die Zylinder-Kennzeichnung.
Status	Zylinderstatus (**Im Lager**, **Eingebaut** oder **Defekt**).
Standort	Der Standort des Zylinders.
Basiszeitzone	Zeitzone am Standort des Zylinders.
Zylindermodell	Modell des Zylinders.
Länge	Physikalische Länge des Zylinders. Bei Doppelzylinder wird die Länge durch eine Zahl auf jeder Seite angegeben. Bei einem Zylinder mit einer Blende oder einem Knauf wird die Länge durch eine Zahl für die Zylinderlänge und eine Zahl für die Länge der Blenden-/Knaufseite angegeben.
Zeile Nummer	Nicht verwendet.
Gesperrt von	Programmierschlüssel, auf den anstehende Zylinderprogrammier-Jobs geladen werden. Wenn ein Zylinderprogrammier-Job auf einen Programmierschlüssel geladen wird, sind die Einstellungen für diesen Zylinder in der CWM-Software für die Bearbeitung gesperrt.
Zylinderseite	**A** oder **B** (bei doppelseitigen Zylindern)
Typ	**E** (Elektronisch) oder **M** (Mechanisch).
Gruppe	Zylindergruppe, zu der ein Zylinder gehört.
Firmware	Die Firmwareversion des Zylinders.
Zeitzonen-Verschiebung	Der Versatz der Zylinder-Zeitzone gegenüber der Basiszeitzone.
Domäne	Domäne, zu der ein Zylinder gehört.
Tags	Für einen Zylinder definierte Tags.
Externe Links	Mit einem Zylinder verknüpfte URLs.

9.3.6 Remote-Programmiergerät-Attribute

Name	Name des Remote-Programmiergeräts.
Kennzeichnung	Die Organisationsnummer des Remote-Programmiergeräts.
Typ	**Mobiles Programmiergerät** oder **Wand-Programmiergerät**.

Generation	Die Generation des Wand-Programmiergeräts.
MAC-Adresse	Die physische Adresse des Remote-Programmiergeräts.
GR	Gruppen-ID (nur zur internen Verwendung).
UID	Eindeutige ID (nur zur internen Verwendung).
Firmware	Firmware-Version.
Bootloader (nur Generation 1)	Bootlader-Firmware-Version.
Status	Bestandsstatus (**Im Lager**, **Eingebaut**, **Ausgegeben** oder **Verloren**). Funktionsstatus (**Defekt**).
Verbindungsstatus	**Offline** oder **Online**.
Letzte Verbindung	Mobiles Programmiergerät: Uhrzeit und Datum, an dem das mobile Programmiergerät letztmalig online war.
Letzte bekannte IP-Adresse	Die IP-Adresse, von der das Remote-Programmiergerät zum letzten Mal online war.
Tags	Für ein Remote-Programmiergerät definierte Tags.
Externe Links	Mit einem Remote-Programmiergerät verknüpfte URLs.

9.4 Rechte

Für jedes Recht kann **Keine**, **Liste**, **Anzeige** oder **Voll** gewählt werden. **Anzeige** umfasst automatisch **Liste** und **Voll** umfasst automatisch **Anzeige** und **Liste**.

Wenn Abhängigkeiten zwischen den einzelnen Rechten bestehen, sind diese in der Spalte **Abhängigkeiten** aufgeführt. Um z. B. Schlüssel-Berechtigungen gewähren zu können, ist eine Anzeigeberechtigung für Schlüssel und eine Listenberechtigung für Zylinder erforderlich.

Berechtigung	Keine	Liste Elemente werden aufgelistet	Anzeige Zugriff auf Details der aufgelisteten Elemente möglich	Voll Zugriff auf Details der aufgelisteten Elemente einschließlich Bearbeitung möglich	Abhängigkeiten
Zugangsprofile Steuert die Verwaltung von Zugangsprofilen (anlegen, löschen, bearbeiten)		⊗	Kann Zugangsprofildetails anzeigen.	Kann neue Zugangsprofile anlegen und vorhandene ändern, mit Ausnahme der Zugangsliste, die über das Recht zur Zugangsprofil-Berechtigung gesteuert wird.	
Zugangsprofil: Berechtigung Steuert die Einstellung von Berechtigungen für ein Zugangsprofil		⊗	Kann die Berechtigungen in einem Zugangsprofil anzeigen.	Kann Berechtigungen in einem Zugangsprofil hinzufügen oder löschen.	Erfordert Anzeigeberechtigung für **Zugangsprofil**.
Genehmigungen		Menüoption **Jobs zur Genehmigung** verfügbar. Kann eine Liste von Ereignislistenanforderungen zur Genehmigung anzeigen.	⊗	Kann Ereignislistenanforderungen genehmigen. Nur Rolle des Genehmigenden und keine Bearbeitung möglich.	Gilt nur, wenn während der Erstinstallation die Genehmigungseinstellung aktiviert wurde.
Ereignisliste			Register „Ereignisliste“ wird in der Schlüsselansicht und Zylinderansicht angezeigt.	Kann Ereignislisten für Zylinder und Schlüssel über das Register Ereignisliste anfordern.	
Ereignisliste: Automatisch		⊗	Berechtigung zum Anzeigen des Status hinsichtlich des automatischen Abrufens von Ereignislisten für Programmierschlüssel.	Berechtigung zum Anzeigen des Status hinsichtlich des automatischen Abrufens von Ereignislisten für Programmierschlüssel.	Erfordert mindestens Anzeigeberechtigung für **Programmierschlüssel**.

Berechtigung	Keine	Liste Elemente werden aufgelistet	Anzeige Zugriff auf Details der aufgelisteten Elemente möglich	Voll Zugriff auf Details der aufgelisteten Elemente einschließlich Bearbeitung möglich	Abhängigkeiten
Programmierschlüssel	⊗	⊗	Kann Details von Programmierschlüsseln anzeigen.	Kann Details von Programmierschlüsseln bearbeiten und Programmierschlüssel ausgeben.	
Programmierschlüssel: Rückgabe/Ausgabe		⊗	⊗	Kann Programmierschlüssel zurückgeben und ausgeben.	Erfordert Listenberechtigung für **Schlüsselhalter: Mitarbeiter** und Anzeigeberechtigung für **Programmierschlüssel**.
Zylinder		Auswählbar, wenn **Zylinder: Berechtigung** auf „Keine“ festgelegt ist.	Kann Zylinderdetails anzeigen.	Kann Zylinderdetails bearbeiten und Zylinderstatus ändern.	
Zylinder: Berechtigung			Kann die Berechtigungen für einen Zylinder anzeigen.	Kann die Berechtigungen für einen Zylinder bearbeiten und Zylinder-Reprogrammierung anfordern.	Erfordert Anzeigeberechtigung für **Zylinder** und Listenberechtigung für **Schlüssel**.
Zylinder: Programmierung		⊗	⊗	Kann Programmier-Jobs an Programmierschlüssel senden.	Erfordert Listenberechtigung für **Zylinder**.
Domäne (Zur Anzeige von Domänenzugehörigkeiten und Domänenberechtigungen für Programmierschlüssel sind keine Rechte erforderlich.)		⊗	⊗	Kann Domänen verwalten (hinzufügen, löschen, bearbeiten) und Domänenberechtigungen für Programmierschlüssel ändern.	

Berechtigung	Keine	Liste Elemente werden aufgelistet	Anzeige Zugriff auf Details der aufgelisteten Elemente möglich	Voll Zugriff auf Details der aufgelisteten Elemente einschließlich Bearbeitung möglich	Abhängigkeiten
Firmware		⊗	⊗	Kann Firmware importieren.	Firmware-Upgrade erfordert Vollberechtigung für **Remote-PGs**.
Flexible Verlängerung (Kann Verlängerungsintervalle anzeigen, wenn die flexible Verlängerung aktiviert ist.)		⊗	⊗	Kann Verlängerungsintervalle für Zugangsprofile und Zylindergruppen bearbeiten.	
Schlüssel	Auswählbar, wenn **Zylinder: Berechtigung** auf „Keine“ festgelegt ist.	Kann Schlüssel indirekt auflisten	Menüoption **Schlüssel** verfügbar. Kann Schlüsseldetails anzeigen.	Kann Schlüsseldetails, Bestands- und Funktionsstatus bearbeiten.	
Schlüssel: Berechtigung		Auswählbar, wenn **Schlüssel: Berechtigung** auf „Keine“ festgelegt ist.	Kann die Berechtigungen für einen Schlüssel anzeigen.	Kann die Berechtigungen für einen Schlüssel bearbeiten.	Erfordert Anzeigeberechtigung für **Schlüssel** und Listenberechtigung für **Zylinder**.
Schlüssel: Rückgabe/Ausgabe		⊗	⊗	Menüoptionen **Schlüsselrückgabe** und **Schlüsselausgabe** verfügbar. Kann Schlüsselausgabe und -rücknahme durchführen.	Erfordert Listenberechtigungen für **Schlüsselhalter: Mitarbeiter**, **Schlüsselhalter: Besucher**, **Schlüssel** und **Zylinder** und Vollberechtigung für **Schlüssel: Berechtigung**.

Berechtigung	Keine	Liste Elemente werden aufgelistet	Anzeige Zugriff auf Details der aufgelisteten Elemente möglich	Voll Zugriff auf Details der aufgelisteten Elemente einschließlich Bearbeitung möglich	Abhängigkeiten
Schlüssel: Zeitplan	⊗	⊗		Kann Zeitplan für einen Schlüssel bearbeiten, Zeitplan für eine Schlüsselgruppe gesammelt konfigurieren und Zeitplan bei Schlüsselausgabe einstellen.	Erfordert Vollberechtigung für **Vorlage: Zeitplanvorlage anwenden** und Anzeigeberechtigung für **Schlüssel**.
Schlüssel: Update-Historie		⊗	Kann die Update-Historie zum Schlüssel auf der Registerkarte **Update-Historie** anzeigen.	⊗	Erfordert Anzeigeberechtigung für **Schlüssel**.
Schlüssel: Gültigkeit	⊗	⊗		Kann Gültigkeitseinstellungen für Schlüssel gesammelt bearbeiten, Gültigkeitseinstellungen für Schlüssel bearbeiten und Gültigkeit bei Schlüsselausgabe einstellen.	Erfordert Anzeigeberechtigung für **Schlüssel**.
Schlüsselhalter: Deaktivieren		⊗	⊗	Kann Personen deaktivieren sowie deaktivierte Personen suchen und aktivieren.	Erfordert Vollberechtigung für **Schlüsselhalter: Mitarbeiter** und **Schlüsselhalter: Besucher**
Schlüsselhalter: Mitarbeiter	⊗	⊗	⊗	Kann Mitarbeiterdetails bearbeiten.	
Schlüsselhalter: Mitarbeiterimport		⊗	⊗	Kann Mitarbeiterdaten importieren.	Erfordert Vollberechtigung für **Schlüsselhalter: Mitarbeiter**.
Schlüsselhalter: Besucher	⊗	⊗	⊗	Kann Besucherdetails bearbeiten.	

Berechtigung	Keine	Liste Elemente werden aufgelistet	Anzeige Zugriff auf Details der aufgelisteten Elemente möglich	Voll Zugriff auf Details der aufgelisteten Elemente einschließlich Bearbeitung möglich	Abhängigkeiten
LDAP-Integration		⊗	Kann Einstellungen für **LDAP-Integration** auf der Systemeinstellungsseite anzeigen.	Kann Einstellungen für **LDAP-Integration** auf der Systemeinstellungsseite bearbeiten.	Erfordert Anzeigeberechtigung für **Systemeinstellungen**.
Wartung		⊗	⊗	Kann das System sperren und entsperren.	
Remote-Programmiergeräte		Kann Remote-Programmiergeräte indirekt auflisten.	Menüoption **Remote-PGs** verfügbar. Kann Details der Remote-Programmiergeräte anzeigen.	Kann Einstellungen von Remote-Programmiergeräten bearbeiten, Upgrades der Firmware von Remote-Programmiergeräten durchführen und ein Wand-Programmiergerät zum Upgrade der Schlüsselfirmware in den Schlüssel-Updater-Modus umschalten.	
Rollen	⊗		Menüoption **Rollen** verfügbar. Kann eine Liste von Rollen anzeigen und Details einer Rolle sehen.	Kann Rollen verwalten (anlegen, bearbeiten, löschen) und Programmierschlüsseln Rollen zuweisen.	
Statistik		⊗	Kann Systemstatistik anzeigen.	⊗	
Systemeinstellungen	⊗	⊗			
Systemstatus		⊗	Menüoption **Systemstatus** verfügbar. Kann Systemstatus anzeigen.	⊗	Erfordert Listenberechtigung für **Remote-PGs**.

Berechtigung	Keine	Liste Elemente werden aufgelistet	Anzeige Zugriff auf Details der aufgelisteten Elemente möglich	Voll Zugriff auf Details der aufgelisteten Elemente einschließlich Bearbeitung möglich	Abhängigkeiten
Vorlage: Zeitplanvorlage anwenden	⊗	⊗	⊗	Kann Zeitplanvorlage für einen Schlüssel anwenden und Zeitplanvorlage bei Schlüsselausgabe anwenden.	Erfordert Anzeigeberechtigung für **Schlüssel**.
Vorlage: Quittung			Menüoption **Quittungsvorlagen** verfügbar. Kann Quittungen ausdrucken und eine Vorschau der Quittungsvorlagen anzeigen.	Kann Quittungsvorlagen erstellen, bearbeiten und löschen	
Vorlage: Zeitplan	⊗		Kann Zeitplanvorlagen anzeigen.	Kann Zeitplanvorlagen bearbeiten.	
Temporäre Zugangsgruppe		⊗	Kann temporäre Zugangsgruppen anzeigen.	Kann temporäre Zugangsgruppen bearbeiten.	

9.5 Anzeigen auf Remote-Programmiergeräten

9.5.1 Anzeigen auf Wand-Programmiergeräten (Generation 1) und mobilen Programmiergeräten

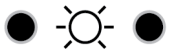
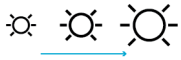
LED-Anzeigen		Summer	Bedeutung
 Weißes Dauerlicht			**Eingeschaltet und online**
 Schnelles weißes Blinken			**Wand-Programmiergerät: Beziehen der IP-Adresse** **Mobiles Programmiergerät: Initialisieren von Bluetooth oder USB-Verbindung**
 Langsames weißes Blinken			**Herstellen der Verbindung zum Remote Server während des Einschaltens**
	 Dauerlicht	1 langer Signalton	**Offline-Update erfolgreich abgeschlossen**

LED-Anzeigen	Summer	Bedeutung
 Rotes Dauerlicht		**Niedriger Batteriestand des mobilen Programmiergeräts**
 Einmaliges rotes Blinken  Einmaliges Blinken		**Extrem niedriger Batteriestand des mobilen Programmiergeräts**
 Dauerlicht		**Niedriger Batteriestand des Schlüssels**
 Blinken		**Herstellen der Verbindung während Remote Update**
 Dauerlicht		**Verbindung während Remote Update hergestellt**
		Upgrade der Firmware abgeschlossen
 Dauerlicht	1 Signalton	**Vorgang erfolgreich abgeschlossen** **Einstellungen des Remote-Programmiergeräts aktualisiert**
 Blinken		**Download und Verarbeitung läuft**
 Dauerlicht	1 Signalton	**E-Mail gesendet**
 Dauerlicht	3 Signaltöne	**Aktion mit Fehler beendet**

Bei Aktionen mit einem Schlüssel werden die Signaltöne alle drei Sekunden wiederholt, bis der Schlüssel abgezogen wird.

9.5.2 Anzeigen eines Wand-Programmiergeräts (Generation 2)

LED-Anzeigen	Summer	Bedeutung
 Links: blinkt blau Mitte: Aus Rechts: Aus		**802.1x-Einstellungen werden überprüft**
 Links: blaues Dauerlicht Mitte: blinkt blau Rechts: Aus		**IP-Adresse wird abgerufen**

LED-Anzeigen	Summer	Bedeutung
 Links: blaues Dauerlicht Mitte: blaues Dauerlicht Rechts: blinkt blau		**Serververbindung wird hergestellt**
 Links: Aus Mitte: weißes Dauerlicht Rechts: Aus		**Verbunden und bereit zur Verwendung**
 Links: Aus Mitte: blinkt weiß Rechts: Aus		**Verbindung getrennt**
 LEDs blinken von links nach rechts weiß		**Schlüssel werden aktualisiert**
 LEDs blinken von links nach rechts blau		**Firmware oder Parameter werden aktualisiert**
 Grünes Häkchen	2 stärker werdende Töne	**Vorgang erfolgreich abgeschlossen**
 Rotes Kreuz	2 schwächer werdende Töne	**Aktion mit Fehler beendet**
 Rotes Batteriesymbol		**Niedriger Batteriestand des Schlüssels**

9.6 Anzeige der Batterieladung

Der Batteriestand des aktuell abgefragten Schlüssels im rechten Schlitz wird mit den folgenden Symbolen angezeigt.

Anzeige der Batterieladung	Bedeutung
	**Batterieladung hervorragend**
	**Batterieladung gut**

Anzeige der Batterieladung	Bedeutung
	**Batterieladung niedrig**
	**Batterieladung kritisch**

9.7 Firmware-abhängige Funktionen

Tabelle 50 "Firmware-Anforderungen", Seite 215 listet die CWM-Funktionen und die erforderliche Firmware-Mindestversion für PGs, Schlüssel und Zylinder auf.

Tabelle 6. Firmware-Anforderungen

Funktion	Niedrigste unterstützte Firmware	
Automatischer Ereignislistenabruf	Schlüssel und Programmierschlüssel	12.7.0
Firmware-Upgrade für Programmierschlüssel	Wand-Programmiergerät und mobiles CLIQ-Programmiergerät	6.3
	Programmierschlüssel	12.0.0
Kompatibilität des mobilen CLIQ Connect-Programmiergeräts	Schlüssel	12.3
Zylindergruppenunterstützung	Schlüssel	6.3.1
	Zylinder	5.3.1
Flexible Verlängerung	Schlüssel	6.3.1
Update der Schlüsselfirmware-Informationen über Remote-Programmiergerät	Schlüssel	12.3
Offline-Update	Schlüssel	6.3.1
PIN-Validierung	Schlüssel	16.0.0
Plug & Play von Remote-Programmiergeräten	Wand-Programmiergerät und mobiles CLIQ-Programmiergerät	6.2.1
Proxyunterstützung für Remote-Programmiergeräte	Wand-Programmiergerät und mobiles CLIQ-Programmiergerät	6.2.1
Remote-Update von Programmierschlüsseln	Programmierschlüssel	12.0.0
Remote-Support	Schlüssel	3.0
	Programmierschlüssel	12.0.0

Funktion	Niedrigste unterstützte Firmware	
Verlängerung	Schlüssel	3.0
Zeitplantyp - Basis	Schlüssel	Nur 1.x, 3.x, 5.x
Zeitplantyp - Mehrere Zeitfenster	Schlüssel	2.x, 4.x, 6.x, 10 oder höher
Zeitzonen-Verschiebung	Schlüssel, Programmierschlüssel und Zylinder	10.0.0
FW-Upgrade für Benutzerschlüssel (Generation 2)	Schlüssel	10.1

Zur Anzeige der Firmware-Version eines Schlüssels Detailinformationen anzeigen. Siehe *Abschnitt 4.2.1 "Benutzerschlüssel suchen", Seite 35* oder *Abschnitt 4.2.2 "Benutzerschlüssel abfragen", Seite 36*.

Zur Anzeige der Firmwareversion eines Wand-Programmiergeräts die Detailansicht öffnen. Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

Zur Anzeige der Firmwareversion eines mobilen CLIQ-Programmiergeräts die Detailansicht öffnen. Siehe *Abschnitt 6.5.2 "Suchen nach Remote-PGs", Seite 108*.

9.8 Voraussetzungen für Client-PC

Produkt	Anforderungen
Betriebssystem	• Windows 10 (64-Bit) • Windows 11
Internet Browser	• Firefox ESR 138 oder höher • Firefox 138 oder höher • Google Chrome 136 oder höher • Microsoft Edge 136 oder höher * Die Unterstützung für Internet Explorer wird aufgrund des angekündigten Supportendes für diesen Browser beendet.
PDF Reader	Beliebiger Reader (mit Adobe Reader getestet)

9.9 Dateiformat für Mitarbeiterimport

Für den Import von Mitarbeiterdaten ist eine Datei mit korrektem Format und korrekten Inhalten erforderlich.

Dateiformat
Das erforderliche Dateiformat ist CSV (Comma Separated Values) mit Zeichenkodierung **Unicode UTF-8**.

Tipp
Um die richtige Kodierung der CSV-Datei sicherzustellen, kann der **Microsoft Editor** in Windows verwendet werden. Die CSV-Datei im Editor öffnen, **Datei » Speichern unter...** auswählen, die Kodierung **UTF-8** auswählen und auf **Speichern** klicken.

Dateigröße
Die maximal zulässige Dateigröße für den Import in CWM beträgt 7,0 MB.

Dateiinhalt
Das erforderliche Trennzeichen ist Komma (,) oder Semikolon (;). Die Systemeinstellung **CSV-Trennzeichen** beeinflusst den Import nicht.

Die erste Zeile ist eine Kopfzeile mit allen Namen der durch Komma getrennten Felder (Feldbeschreibungen). Die Kopfzeile wird überprüft und ist sprachspezifisch, d. h. der Text in der Kopfzeile muss den Definitionen für die gewählte Sprache entsprechen.

Tipp
Eine korrekte Kopfzeile lässt sich erhalten, indem die Mitarbeiter in eine CSV-Datei exportiert und anschließend alle Informationen außer der Kopfzeile gelöscht werden. Beim Exportieren von Mitarbeitern wird nach den übrigen Feldern das zusätzliche Feld **Tags** hinzugefügt. Dieses Feld kann in der Datei beibehalten werden, es wird jedoch beim Importieren ignoriert.

Siehe *Abschnitt 4.1.12 "Mitarbeiter- oder Besucherinformationen exportieren", Seite 35*.

Jede folgende Zeile entspricht einem Mitarbeiter. Feldwerte werden mit dem Trennzeichen voneinander abgetrennt und die Reihenfolge der Felder muss der Kopfzeile entsprechen. Falls ein Feld das Trennzeichen enthalten muss (Komma oder Semikolon), müssen die gesamten Daten in diesem Feld von Anführungsstrichen (") umschlossen werden, z. B. `"11 Wall St, New York, NY"`.

HINWEIS!
Auch bei einem leeren Feld muss das Trennzeichen vorhanden sein.

Felder und Anforderungen sind in *Tabelle 52 "CSV-Dateistruktur", Seite 217* aufgeführt.

Tabelle 7. CSV-Dateistruktur

Feld Nr.	Name	Obligatorisch	Anzahl Zeichen
1	ID		1-50
2	Anrede		0-100
3	Vorname	✓	1-49
4	Nachname	✓	1-49
5	Domäne		0-100
6	E-Mail		0-100
7	Telefon		0-100
8	Organisation		0-100
9	Abteilung		0-100
10	Straße		0-100
11	Postleitzahl		0-100
12	Sprache		0-100
13	Region		0-100
14	Job		0-100
15	Ort		0-100

Feld Nr.	Name	Obligatorisch	Anzahl Zeichen
16	Bundesland		0-100
17	Land		0-100
18	Firmenanschrift		0-100
19	Standort		0-100
20	Mobiltelefon		0-100
21	Zusatz-Text		0-100

Die **ID** muss eindeutig sein. Wenn ein Mitarbeiter in der Datei die gleiche **ID** wie ein Mitarbeiter im System besitzt, werden die Informationen im System durch die Informationen in der Datei ersetzt. Wenn jedoch ein Mitarbeiter in CWM hinzugefügt und anschließend ohne Angabe einer **ID** in der Datei importiert wird, führt dies zu doppelten Einträgen mit diesem Mitarbeiter.

HINWEIS!
Mitarbeiter in der CSV-Datei, deren ID der eines in CWM deaktivierten Mitarbeiters entspricht, werden ignoriert und nicht importiert.

Die **E-Mail** muss ein korrektes E-Mail-Format aufweisen.

HINWEIS!
Für das Bearbeiten oder Löschen einer E-Mail-Adresse eines Mitarbeiters oder Besuchers mit aktiviertem Benutzerstatus für CLIQ Connect+ gelten bestimmte Einschränkungen. Weitere Informationen siehe *Abschnitt 4.1.6.1 "Wichtige Informationen über das Bearbeiten oder Löschen einer E-Mail-Adresse", Seite 31*.

Die maximale Anzahl Mitarbeiter in einer Datei beträgt 10.000.

Beispieldatei

```
ID,Anrede,Vorname,Nachname,Domäne,E-
Mail,Telefon,Organisation,Abteilung,Straße,Postleitzahl,Sprache
,Region,Job,Ort,Bundesland,Land,Firmenadresse,Standort,Mobiltel
efon,Zusatz-Text

P0,Professor,George,Whitmore,Stockholm,George.Whitmore@assaablo
y.com,3719253729973267730,ASSA ABLOY,Shared Technologies,,,Swed
ish,,System Developer,Stockholm,,Sweden,"Formansvagen 11, 117 4
3 Stockholm",,070-6972135783866065282,GmdText
```

9.10 ASSA ABLOY-Firmencode

Code	Firma
0	Keine Firma angegeben
1	ASSA ABLOY Opening Solutions Sweden (ASSA)
2	ABLOY
3	IKON
4	VACHETTE
6	MEDECO

Code	Firma
7	SARGENT
8	ARROW
9	LAPERCHE
10	ASSA ABLOY Opening Solutions Norway (TRIOVING)
11	ASSA ABLOY Opening Solutions Denmark (RUKO)
12	MUL-T-LOCK
13	ASSA US
14	ASSA UK
15	ASSA BALT
16	MEDECO CANADA
17	FAB
18	AA Japan
19	TESA
20	AA Neuseeland
21	AA Australia
22	AA Singapore
23	AA Hong Kong
24	AA China
25	AA India
26	KESO
27	Corbin Russwin
28	ABLOY UK
29	ABLOY US

9.11 Informationen zum Software-Support

9.11.1 Kontakt mit dem Software-Support

Wenn bei der Verwendung des CLIQ Web Managers oder der Hardware wie Schlüssel, Zylinder oder Programmiergeräte Probleme auftreten, bitte mit dem lokalen CLIQ-Händler Kontakt aufnehmen. Bei jeglicher Kommunikation zu Servicezwecken bitte die Hauptschlüsselsystemnummer und die verwendete Version des Web Managers bereithalten. Bei der Kontaktaufnahme per E-Mail bitte stets die Hauptschlüsselsystemnummer in die Betreffzeile der E-Mail eintragen.

ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.

IKON
ASSA ABLOY

ASSA ABLOY Sicherheitstechnik GmbH

Attilastrasse 61-67
12105 Berlin
GERMANY
Tel. + 49 30 8106-0
Fax: + 49 30 8106-26 00
berlin@assaabloy.com

www.assaabloy.de

Technische Änderungen vorbehalten. Program version: V 2025.1. Document number: PB00023 00017 0DE. Language: de-DE. Published: 2025-05-22.