dormakaba

Community

User Guide

PK3706 2.6 - 08/2026
Original document

EN

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
T: +1 866-dormakaba (1-866-367-6252)

www.dormakaba.com

Copyright © dormakaba 2026
All rights reserved.

No part of this document may be reproduced or used in any form or by any means without prior written permission of dormakaba Canada .

All names and logos of third-party products and services are the property of their respective owners. MIFARE, MIFARE Classic, MIFARE Plus, and MIFARE Ultralight are registered trademarks of NXP B.V.

Subject to technical changes.

Table of contents

About this document 8
Welcome to Community 9
Configuration 11
Site configuration workflow 13
Configure System Settings 14
Learning about System Settings 15
General Settings 19
Resident Management Settings 20
Security Settings 22
Staff/Vendor Key Settings 33
Failsafe Key Settings 34
Key Expiration Settings 35
Email Configuration Settings 36
Database backup settings 37
Visitor Management Settings 41
Entry System Interface Settings 43
Advanced Settings 44
Community API 48
Licensing Settings 50
Build Your Property 51
Learning about Property Builder 52
Add buildings 58
Add floors 59
Add units 62
Add suites 66
Import units and suites list 71
Add resident common areas 72
Add staff common areas 78
Add restricted areas 84
Add elevators 86
Configure Access 90
Learning about Access Management 91
Add auto-unlatch schedules 95
Add access schedules 97

Add shift schedules 99
Create access point groups 101
Add Credentials 103
Assign schedules 107
Configure access profiles for limited-access common areas 108
Configure Devices 112
Learning about Device Management 113
Add encoders 115
Program Locks 118
Learning about Programming & Auditing 119
Program locks 122
Review & Customize Roles 124
Learning about Role Management 125
Review pre-defined roles 127
Configure custom roles 128
Add Operators 130
Learning about Staff/Vendor Management 131
Configure operators 133
Import staff/vendor list 138
Use Community **140**
Resident Management 143
Learning about Resident Management 144
Add residents 151
Import resident list 153
Assign units 155
Make Resident Keys 162
Modify Resident Access 165
Invalidate resident access 171
Make keys for common area access only 178
Make mobile keys for multiple residents 180
Configure Visitor Management for residents 182
Staff and Vendor Management 184
Learning about Staff/Vendor Management and Staff/Vendor Keys 185
Add staff members/vendors 187
Import staff/vendor list 189
Make Emergency keys 191

Make Staff key (predefined access) 194
Make Staff Keys (variable access) 198
Make Vendor keys 202
Make Limited Use keys 206
Replace Staff/Vendor Keys 210
Invalidate staff/vendor access 212
Configure Visitor Management for staff/vendors 217
Programming/Auditing 218
Reprogram locks 219
Audit locks 221
Audit online access points 222
System Keys 223
Learning about System Keys 224
Block and unblock keys 227
Cancel keys 231
Diagnostic keys 233
Electronic lockout keys 235
Failsafe keys 237
Inhibit keys 238
Latch and unlatch keys 240
Primary and secondary program keys 242
Resequence keys 245
Special function keys 247
Monitoring 248
Learning about Monitoring 249
Monitor keys 250
Monitor digital key usage 251
Reports 253
Access Point Audit Report 254
Credential/Access Point Assignment Report 256
Elevator Configuration Report 257
Key Expiration Report 258
Key/User Assignment Report 259
Operator Report 260
Property Configuration Report 261
Roles and Rights Report 262

Staff/Vendor Access Report 263
System Activity Report 264
Visitor Management Report 267
Toolbar Basics 268
Navigate Community 269
Set operator preferences 271
Install / update Community Client 273
Select default encoder 274
Remote unlock/lock 275
Read key/erase key/access tracking report 277
View notifications 281
Physical keys 283
Digital keys 285
Remote Lock Mgmt 290
Introduction 291
Enable and configure online communication 292
Gateways & Paired Access Points 299
Manage online device configuration 300
Registered gateways and paired access points 302
Program Devices 307
Program devices 308
Notification Management 309
Learning about Notification Management 310
Add notification groups 312
Monitoring (RLM) 314
Learning about Monitoring 315
View metrics 316
Monitor online operations 317
Monitor online events 319
Monitor access point status 322
Reports (RLM) 323
Online Access Points Status Report 324
Online Gateway Status Report 325
Online Paired Access Point Report 326
Troubleshooting 327
Services Manager 328

Troubleshooting encoders 332
Troubleshooting locks 336
Log data 342
Glossary 343
Index 352

About this document

Validity

This document describes the product:

Product designation:	Community
Version:	2.6

Target audience

This document is for all Community Operators: Administrator, Site Configurator, Maintenance Supervisor, Maintenance Technician and Leasing Agent.

Purpose and objective

The purpose of this document is to provide conceptual and instructional information about the features and functions in Community. The document also includes basic troubleshooting topics for common problems.

Additional documents

Community Installation Guide v 2.6 PK3706-EN

Community Release Notes v 2.6 PK3696

Community Enhanced Key Security 2.6 PK3776

Welcome to Community

Community® is flexible and easy-to-use management software for multihousing properties. Developed for security and designed for users, the application streamlines access control management and provides an efficient and user-friendly method to set up and operate apartment buildings, student housing, senior living, and other multi-tenant properties. Flexible configuration and integration options showcase a robust feature set including mobile key access and resident-delegated visitor management. Guided workflows simplify property configuration, staff and vendor management, key issuance, and resident management. Configurable user permissions secure system access. Lock and system data collection supports detailed access point audits and reporting. Remote lock management provides immediate and convenient control of access points. Seamless integration with Keyscan Aurora Access Control extends management to connected perimeter doors and removes the pain of syncing resident and staff data between different systems.

Getting started

Whether you want to take a self-guided tour of your new software or jump straight into configuring your site, the Community workflow is the best place to start. The process to get up and running starts with installation, proceeds to site configuration, then finally arrives at Go Live.

The *Community User Guide* is organized to follow the recommended workflow and provides information and instructions for all Community operators.



An Operator is a staff member who can log in and use Community.

The user guide includes the following sections:

- "Site Configuration" provides an easy-to-follow workflow and step-by-step instructions for setting up Community.
- "Use Community" provides instructions for day-to-day work after Go Live and includes Working with ... topics that address some of the more complicated situations.
- "Remote Lock Management" provides information related to the licensed feature Online Communication and all other features that require Online Communication.
- "Troubleshooting" contains problem-solving information produced by dormakaba field technicians.
- The Glossary defines terms used in the product.
- The Table of Contents and Index provide alternative means of finding information.

Additionally, contextual help is available in the product.

Installation

Installing the Community Server and Community Client is a straightforward wizard-driven process. For detailed instructions, see the *Community Installation Guide* and *Community Release Notes*. For support, an experienced dormakaba technician is available to guide the process and resolve any issues that present.

Site configuration

Site configuration is the process of defining the access controls for the property and creating profiles for the people in your organization who will have access to Community. Use the site configuration workflow and the following modules to configure the site:

- **System Settings** where you configure site-wide options, defaults and preferences.
- **Property Builder** where you create a virtual representation of your site in Community. Add buildings, floors, access points and elevators.
- **Access Management** where you add the credentials that are available to encode on staff/vendor and system keys. You can also configure limited-access common areas and configure and assign schedules to credentials and/or individual access points.
- **Device Management** where you configure encoders. If licensed for online communication, you can also work with gateways and paired access points.

- **Programming & Auditing** where you access the data transfer function required to program and audit locks. If online communication is enabled, you can also audit online access points.
- **Notifications Management** where you create logical groupings of notifications to which operators can subscribe. The module is only active when licensed for online communication.
- **Role Management** where you create and configure Operator roles and the associated rights.
- **Staff/Vendor Management** where you add staff members and configure operators.

Go Live

The Go Live phase starts when site configuration is complete and you begin to perform day-to-day tasks such as adding and making keys for staff and residents. Use the following Community modules to perform daily work:

- **Resident Management** where you manage residents, configure resident access, and encode resident keys.
- **Staff/Vendor Management** where you create and manage profiles for staff/vendors, replace staff/vendor keys, and cancel staff/vendor keys.
- **Staff/Vendor Keys** where you make keys for staff/vendors.
- **Programming & Auditing** where you re-program and audit locks. If online communication is enabled, you can also audit online access points.
- **System Keys** where you encode special purpose keys.
- **Monitoring** where you check the status of all keys made in Community. If licensed for online communication, you can also monitor operations, events and paired access point status.
- **Reports** where you generate current and historical reports for every aspect of your site.

Access to Community features

The features and options that display in Community depend on the rights selected for the role assigned to the active Operator. For example, if the Operator that is currently logged in does not have rights to access the Property Builder module, the module does not display. Likewise, if the only right selected in the *ELO* (Electronic Lockout) key right category is *Make Additional Key*, the only time *ELO* displays as an option when selecting a credential class is when the Operator is making an additional key.

Configuration

This section includes the following subjects:

- Site configuration workflow 13
- Configure System Settings 14
  - Learning about System Settings 15
  - General Settings 19
  - Resident Management Settings 20
  - Security Settings 22
  - Staff/Vendor Key Settings 33
  - Failsafe Key Settings 34
  - Key Expiration Settings 35
  - Email Configuration Settings 36
  - Database backup settings 37
  - Visitor Management Settings 41
  - Entry System Interface Settings 43
  - Advanced Settings 44
  - Community API 48
  - Licensing Settings 50
- Build Your Property 51
  - Learning about Property Builder 52
  - Add buildings 58
  - Add floors 59
  - Add units 62
  - Add suites 66
  - Import units and suites list 71
  - Add resident common areas 72
  - Add staff common areas 78
  - Add restricted areas 84

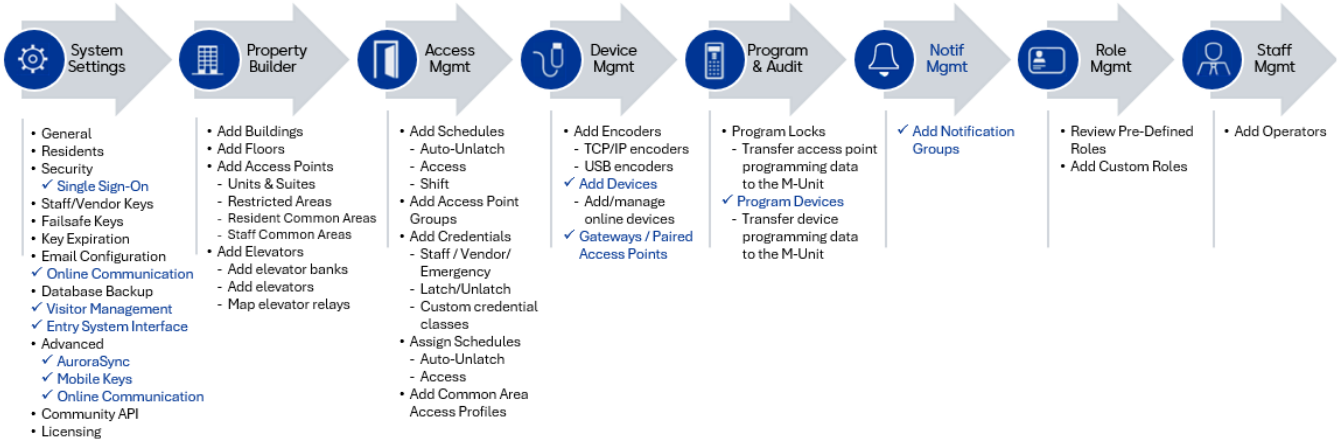
Add elevators 86
Configure Access 90
Learning about Access Management 91
Add auto-unlatch schedules 95
Add access schedules 97
Add shift schedules 99
Create access point groups 101
Add Credentials 103
Assign schedules 107
Configure access profiles for limited-access common areas 108
Configure Devices 112
Learning about Device Management 113
Add encoders 115
Program Locks 118
Learning about Programming & Auditing 119
Program locks 122
Review & Customize Roles 124
Learning about Role Management 125
Review pre-defined roles 127
Configure custom roles 128
Add Operators 130
Learning about Staff/Vendor Management 131
Configure operators 133
Import staff/vendor list 138

Site configuration workflow

The Community Site Configuration Workflow provides an overview of the recommended site configuration process. Each step corresponds to a Community module. Review the process before getting started. Licensed features are indicated by a checkmark.

Refer to *The Property Design and System Configuration Questionnaire* for deployment decisions recorded by the key stakeholders on your team.

Community workflow



After site configuration, remember to ...

- Go to **System Settings > Database Backup** to configure regularly scheduled backups and data retention for the Community SQL Server database (and MongoDB for online systems). The recommendation is to store backups at a secure external location.
- Go to **System Settings > Failsafe Keys** to make backup keys.
- If not licensed for PPK/SPK Storage, go to **System Keys** to make primary and secondary program keys. Store the keys in a secure location.

Step 1

Configure System Settings

This section includes the following subjects:

Learning about System Settings 15
General Settings 19
Resident Management Settings 20
Security Settings 22
Staff/Vendor Key Settings 33
Failsafe Key Settings 34
Key Expiration Settings 35
Email Configuration Settings 36
Database backup settings 37
Visitor Management Settings 41
Entry System Interface Settings 43
Advanced Settings 44
Community API 48
Licensing Settings 50

Learning about System Settings

System Settings is the Community module where you can define system preferences and default values for global options. In some cases, the options in System Settings control whether Community features are enabled and how the features operate. For example, if mobile keys are not enabled in **System Settings**, the option to make mobile keys is not offered during the process of making keys.

Configure System Settings

To configure system settings:

- Go to the **System Settings** module and specify settings for each category.

Configure system-wide defaults and enable licensed options. To make site configuration more efficient, Community populates recommended or moderate values for most system settings. While it's a good idea to review all system settings, you have the option to use the system defaults.

System Settings Categories

You can specify settings for the following categories.

General

Define basic site information and enable phone/mobile number validation override. With the exception of the site name and site image, all settings have system defaults. None of the options in this category require attention.

Residents

Configure defaults for the Resident Management module. All settings have system defaults. However, if you plan to control access to elevators, the option **Display floor access** requires attention.

Security

Configure settings related to account security and lock access, disable/enable enhanced security mode, obtain the Maintenance Unit security password when enhanced security mode is enabled, enable API client certificate authentication, and configure browser certificate options.The following situations require manual configuration:

- Disable authentication for API Integration
- Disable authentication for Maintenance Unit accounts
- Enable client certificate validation for API requests
- Enable/disable Enhanced Security Mode



The following licensed features are also accessible:

- Single Sign-On – Enable and configure single sign-on.

Staff/Vendor Keys

Configure how many times a **Limited Use Key** can be used, disable toggle mode for variable access keys for units, and select whether to display the menu to add common areas when making staff/vendor keys. You can also enable Emergency Keys. Default values are populated. However, this category requires attention if you want to change the defaults.

Failsafe Keys

Configure default values for Failsafe Key options. Failsafe Keys are backup room keys made in advance and maintained in complete sets to be issued in the event of a system or power failure. The recommendation is to create two sets of three keys for each unit and suite door.

Key Expiration

Configure default key expiration for all credential class types and key types. When making a Staff/Vendor Key or System Key, the default expiration date is based on the calculation using the values specified here.

Email

Configure settings used to send emails to staff. No system defaults are populated. This category requires attention so that Community can send automated emails and notifications to staff.

Configure settings used to send emails to staff/vendors. No system defaults are populated. This category requires attention so that Community can send automated emails and notifications to staff/vendors.

Online Communication 

Online Communication is a licensed feature that is disabled by default.

Customize settings for the online communication. Configuring the update time intervals for gateways and wake-up time intervals for paired access points are examples of the settings that you can configure. You can also define whether the gateway network uses a dynamic or static IP address for communication. Lastly, you can customize the settings that trigger intruder alert notifications and enable Rx-Link.

Database Backup



dormakaba strongly recommends scheduling automated backups to a remote server and storing backup and archival data in a secure location off-site.

Database backups are the first priority for disaster preparedness. In the event of data loss or corruption, backups provide a full restore of the Community SQL Server database and, when Online Communication is enabled, the MongoDB database. If the SQL Server database is not backed up, you lose all Community data and must reconfigure the entire site including recreating access points and programming locks. If the MongoDB is not backed up, you lose all data related to Online Communication and must reconfigure the entire online environment including reconfiguring each gateway and pairing locks to gateways.

Database purging and archiving helps maintain sufficient space on the Community Server by deleting or extracting historical records from high-volume database tables, such as the System Activity table. If purging and archiving are not enabled, the database will grow to the system limit and space may become unavailable for normal processing. Purging is processed as scheduled prior to archiving. Because archiving occurs as scheduled immediately after backup, backups must be configured before archiving can be enabled.

Refer to the following table for backup/archive details.

Data	Location Stored	Backup Option	Frequency	Retention
SQL Server	Specified directory (local or remote) Default: C:\Program Files\Microsoft SQL Server\MSSQL16.COMMUNITY\MSSQL\Backup Default for upgrades: existing setting persists	On-demand	On-demand	Current backup
		Per schedule	Per schedule	Per setting
GDPR symmetric key	ProgramData\DormaKaba\Community\Backup (local only)	Per site policy		
MongoDB	MongoDB folder in specified directory (local only) Default for new installations and upgrades with remote SQL Server: none Default for upgrades with local SQL Server: existing setting persists	Per schedule	Per schedule	Latest backup

Data	Location Stored	Backup Option	Frequency	Retention
Archive	Specified directory (local allowed but external hard drive, network drive, or remote server recommended) Default: C:\Program Files\dormakaba\Community Server\Archive Default for upgrades: existing setting persists	Per schedule	Per schedule	Indefinite

In compliance with the GDPR (General Data Protection Regulation), all PII (Personally Identifiable Information) stored in the database is encrypted. Upon taking a backup (on-demand or scheduled) the site-specific encryption key is saved on the Community server at \ProgramData\DormaKaba\Community\Backup. The key is required to restore the database.

Visitor Management

Visitor management is a complimentary feature that works exclusively with AuroraSync and mobile keys. Visitor management provides residents and staff the ability to extend all or part of their access to on-site visitors. Using the dormakaba BlueSky app, residents and staff can generate PIN codes to authorize perimeter and common area access. Residents also have the option to delegate mobile keys for visitors that can work on common doors and the resident's unit if desired.

- A PIN is a 7-digit sequence that can be used at access points where a numeric keypad is installed.
- A delegated mobile key (or PIN code in mobile key format) provides access using the dormakaba BlueSky app.

When Visitor Management is enabled in System Settings for staff/vendors, PIN delegation can be enabled/disabled on the Visitor Management tab in staff/vendor profiles. When Visitor Management is enabled in System Settings for residents, PIN and mobile key delegation can be enabled/disabled on the Visitor Management tab in resident profiles.

Prerequisites include:

- AuroraSync must be enabled and configured.
- Mobile keys must be enabled and configured.
- The resident and/or staff member profile must include a valid mobile number.
- The dormakaba BlueSky app must be installed and registered on the mobile device used to generate PIN code/mobile key.

Advanced

Change key technology settings and enable extended common areas. For more information, see "Learning about Property Builder" on the Help Home page.

The following licensed features are also accessible:

- Mobile keys—Enable mobile keys.
- Online communication—Enable Online Communication. For more information, see "Working with Online Communication" on the Help Home page.
- AuroraSync—For more information, see *Community Aurora Integration* (PK3768).

Entry System Interface

Entry system interface is a licensed feature disabled by default. Enable and configure a third-party entry system to extend resident access management options. The interface gives any third-party entry system the ability to integrate with Resident Management in Community. OATH (Open Authentication) requires third parties to provide required settings to generate a security token.

Community API

Enable and configure the Community REST API, key issuance notification, and the Return UID interface.

Use the REST API for Web Service connections that are secured with token-based authentication. With the Community REST API, you can create and manage virtually all aspects of key issuance for residents, staff, and vendors. The API also supports operations to read and erase keys, and list information about encoders, audits, common areas, active keys, and resident unit assignments. For details about the API, obtain the specification *Community REST API* (PK3781) from a dormakaba Support technician.

Key issuance notification sends a separate notification for every key issued from the user interface, Community REST API, and Community SOAP API . Third parties must first use the Community REST API to register a callback URL and optional security token.

The Return UID interface supports REST-based integration with third-party destination elevator control systems. When enabled, residents and other key holders are directed to the floor associated with their assigned units. Third parties must first use the Community REST API to register at least one callback URL.

Licensing

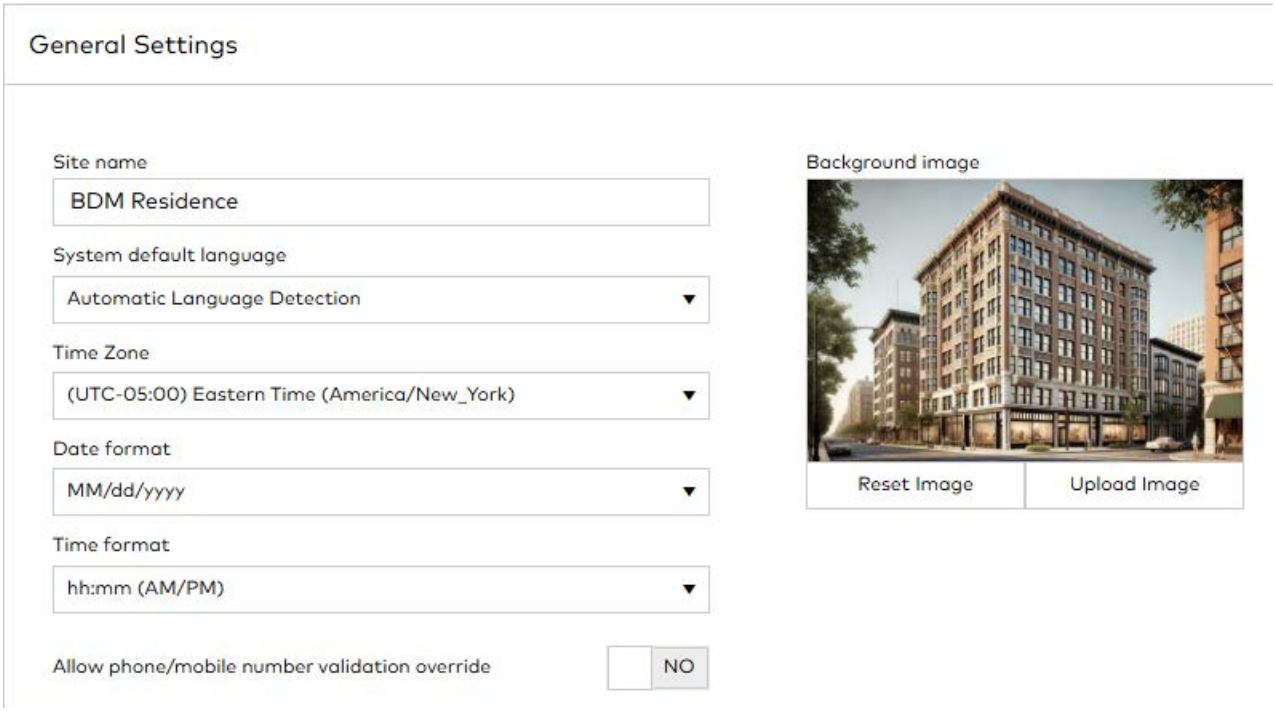
Change the activation key to enable or disable Community features. Licensed features include:

- Mobile keys
- Online communication
- Visitor Management
- Third-party integrations
- PPK/SPK Storage—This option backs up the site PPK/SPK (Primary Program Key/Secondary Program Key) by storing it in the secure internal application used to manage licenses at dormakaba. In the event of database corruption or a total failure, the PPK/SPK backup can be used to reprogram locks and/or reconfigure the Community database.
- Single Sign-On (SSO)

General Settings

Configure basic site settings.

1. Go to **System Settings > General**.



2. For **Site name**, specify the name of the property. Max characters: 30. The site name appears in reports. Default: My Site.
3. For **System default language**, select the default language for the user interface. The default is to detect the browser language. The UI displays in the selected language until a preferred language is selected in **Preferences**. The language selected in **Preferences** takes precedence.
4. For **Time zone**, select the time zone to use for programming locks and encoding keys. Changing the time zone requires reprogramming all access points and remaking / reissuing all keys. The default value reflects the time zone for the Community server.
5. For **Date format**, select the format to display dates site-wide. Default: mm/dd/yyyy.
6. For **Time format**, select the format to display time site-wide. Default: hh:mm (and if available, AM/PM).
7. **Allow phone/mobile number validation override**—Select **YES** to allow phone/mobile numbers that are not recognized. Upon entering a value for a phone number in resident and staff/vendor profiles, validates whether the string adheres to known international standards. If the string is not recognized, the value cannot be saved. (The most common issue is an area code that is not recognized.) The option to override validation allows Operators to save phone numbers that do not meet known standards. Default: NO.
8. For **Background image**, click **Upload image**, navigate to and select an image then click **Open**. Supported file types: gif, jpg, png. The selected image displays on the Community Home page.
9. Click **(Save)** .

Resident Management Settings

Configure system-wide defaults for the **Resident Management** module.

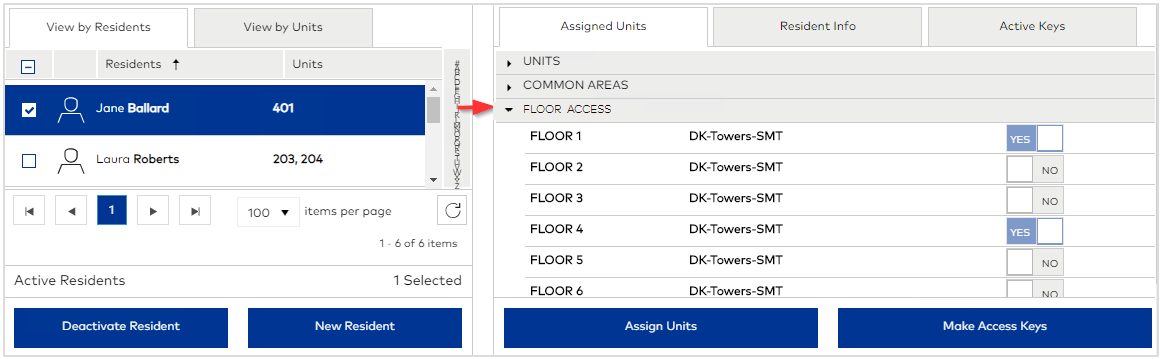
1. Go to System Settings.
2. Click **Residents**.



3. For **Default number of resident keys**, specify the default value for the number of keys to make when making access keys for residents. Valid range: 1-10. Default: 2.
4. For **Default key expiration**, click -/+ to select the number of years and days used to calculate the expiration date that automatically populates when making a key. Default value: 1 year, 0 days.
5. For **Show message details**, select whether you want the system to display messages related to making keys for residents. Default: YES.

   Take caution before deciding to not show message details. When changes to access are made, the messages list the names of residents for whom keys need to be made. The reminders are most useful when residents share access. If you do not make keys as directed by the warning messages, resident keys may be invalid and prevent access.

6. For **Display floor access**, select whether to display the FLOOR ACCESS section in resident profiles in Resident Management. By default, residents have elevator access to floors on which they are assigned units. When the FLOOR ACCESS section is displayed in resident profiles, additional floor access can be enabled. Default: NO. The following figure shows a resident profile that displays floor access.



7. For **Enable deadbolt/privacy switch override for resident keys**—Select whether Resident Keys can override the deadbolt/privacy switch for unit and suite unit doors. If you change this setting, access points may need to be reprogrammed. Default: YES.
8. Click (Save).

Security Settings

Configure settings related to account security.

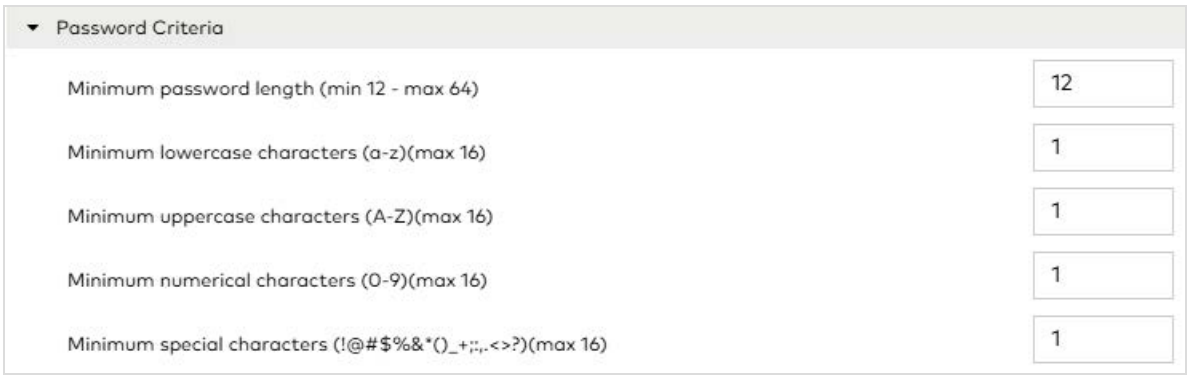
Password settings apply to all passwords with the following exceptions:

- Passwords managed by Identity Provider (IdP) when SSO is enabled
- System-generated one-time passwords, such as when an operator clicks **Forgot your password?** on the login page.

Passwords cannot contain operator first name, last name, user ID, or the current year.

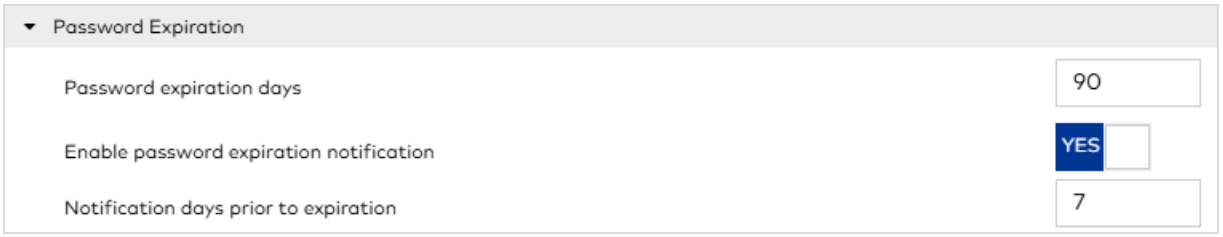
1. Go to **System Settings > Security**.
2. Specify options. Refer to the sections below for details.
3. Click **(Save)**.

Password Criteria



- **Minimum password length**—Specify the minimum number of characters in Community account passwords. Valid values: 12-64, default: 12
- **Minimum lowercase characters**—Specify the minimum number of lowercase characters in Community account passwords. Valid values: a-z, number of characters: 1-16, default: 1
- **Minimum uppercase characters**—Specify the minimum number of uppercase characters in Community account passwords. Valid values: A-Z, number of characters: 1-16, default: 1
- **Minimum numerical characters**—Specify the minimum number of numeric characters in Community account passwords. Valid values: 0-9, number of characters: 1-16, default: 1
- **Minimum special characters**—Specify the minimum number of special characters in Community account passwords. Valid values: !@#$%&*()_+;:,.<>? number of characters: 1-16, default: 1

Password Expiration



- **Password expiration days**—Specify the number of days after which the password for an Operator account expires. Valid values: 1-90, default: 90
- **Enable password expiration notification**—Specify whether to notify Operators when their password is near expiration. Recommended value: YES.

- **Notification days prior to expiration**—Specify the number of days preceding a password expiration that daily notification is displayed after Operator logon. Valid values: 5-30.

Password History



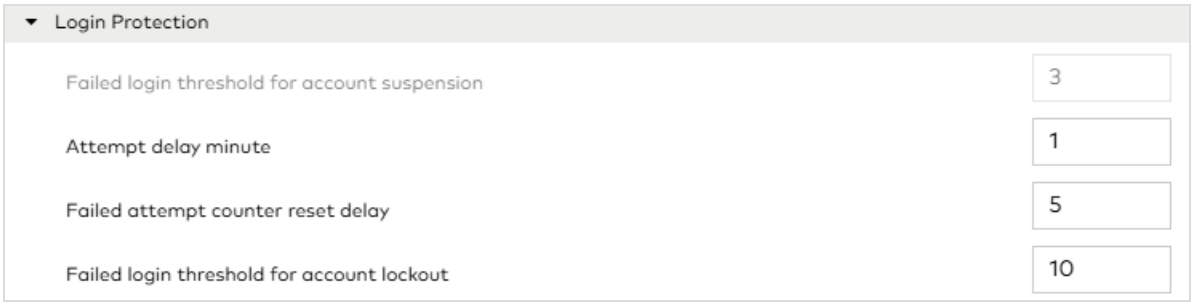
- **Number of previous passwords to check**—Specify the number of most recently used passwords to check when an Operator creates a new password. The new password cannot be the same as any previous password that is checked. Valid values: 4-30.

Password Reset



- **Failed security answers threshold**—Specify the number of times an Operator can fail to provide the correct answer to a security question before the account is blocked. Valid values: 1-10.
- **Password reset expiration delay in hours**—Specify the number of hours the link sent in response to a password reset request is valid. Valid values: 1-24, default: 24
- **Security questions on password change (forgotten password)**—Select whether to prompt the Operator with challenge questions when requesting a password reset. Recommended value: YES.

Login Protection



- **Failed login threshold for account suspension**—Specify the number of failed login attempts before the Community account is temporarily blocked. Accounts that are suspended are blocked for the number of minutes specified in **Attempt delay minute**. Valid values: 3-30.
- **Attempt delay minute**Specify the number of minutes to suspend an account. Valid values: 1-30.
- **Failed attempt counter reset delay**—Specify the number of minutes to suspend an account when the **Failed login threshold for account suspension** is reached. Valid values: 1-30.
- **Failed login threshold for account lockout**—Specify the number of failed login attempts before the Community account is locked out. When the threshold is reached, the Operator cannot log in without administrator support. Valid values: 1-10, default: 10

Account Inactivity



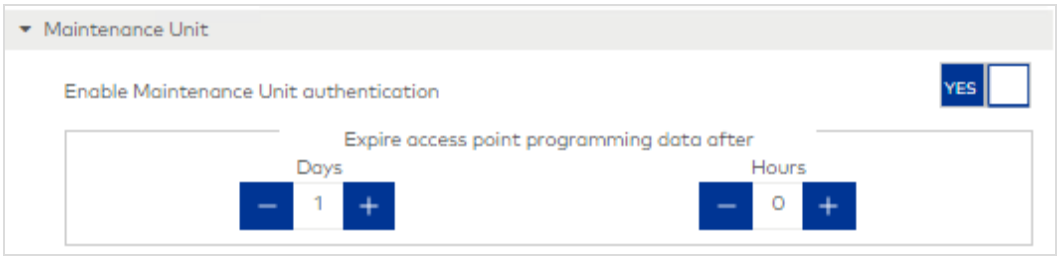
- **Inactivity threshold for account lockout (days)**—Specify the number of days after which an account with no login activity is locked out. When the threshold is reached, the Operator cannot log in without administrator support. Valid values: 1-90, default: 90

Session Inactivity



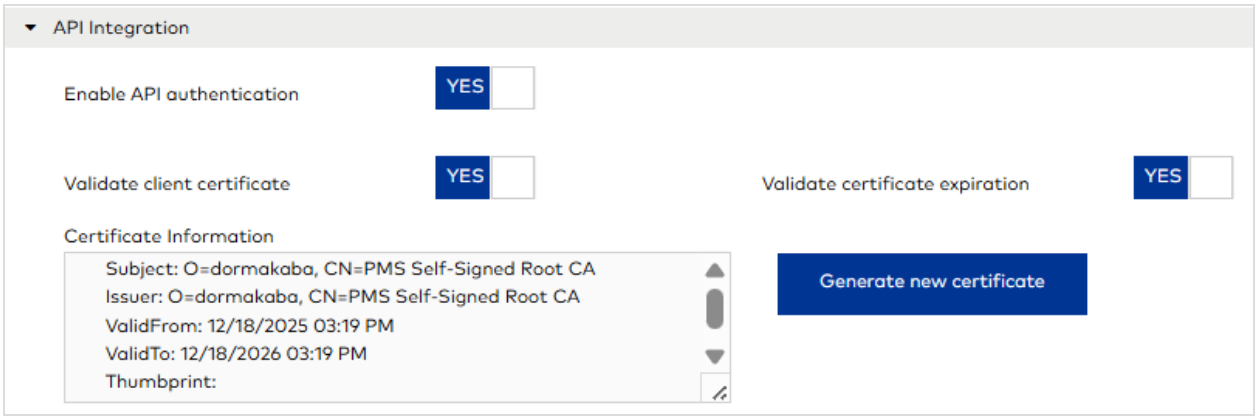
- **Inactivity threshold for session logout (minutes)**—Specify the number of minutes after which an active Community session with no activity ends. When the threshold is reached, the operator must log in again. Valid values: 1-15, default: 15

Maintenance Unit



- Select whether to require M-Unit (Maintenance Unit) authentication. When authentication is enabled, M-Unit credentials are required to program and audit locks. Configure credentials for at least one Operator in Staff/Vendor Management. Defaults: YES, 1 day and 0 hours.
- Specify the number of days and hours after which the data on the M-Unit cannot be transferred. Default: 1 day, 0 hours.

API Integration



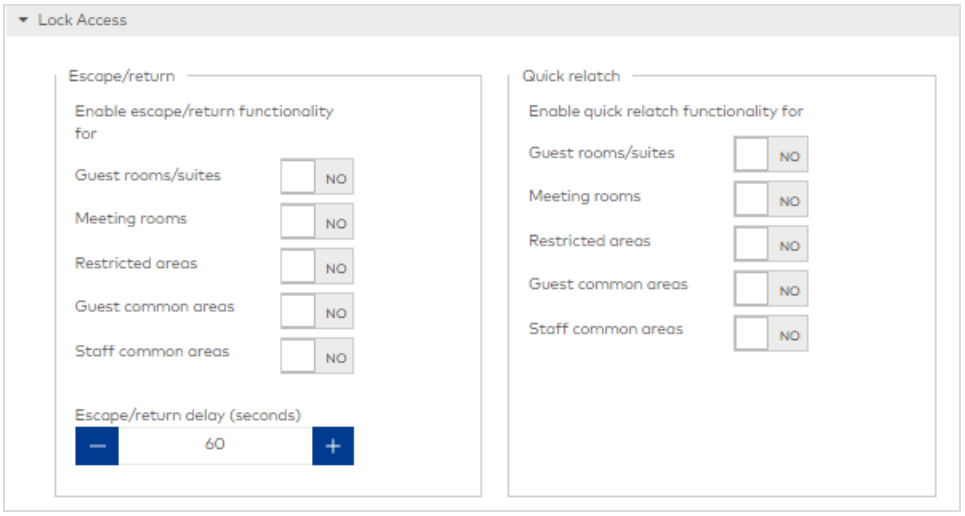
- Select whether to require authentication for API requests. When authentication is enabled, API requests are not processed until the user name and password specified in the request are authenticated against the **API Login** user name

and password configured in **Staff/Vendor Management**. Required for enhanced security mode. Default: YES.

- **Validate client certificate**—(Community SOAP API or Community REST API) Select whether to validate the client certificate for each API request. Required to validate certificate expiration. When this setting is modified, Community reinitializes the API connection. Default: NO. When enabled, the following settings display:
  - **Validate certificate expiration**—Select whether to validate the certificate expiration for each API request. When set to YES and the certificate is expired, API requests are not processed. **Validate client certificate** must be set to **YES**. Default: **YES**.
  - **Generate new certificate**—A certificate is automatically generated for fresh installs. Click to generate a certificate valid for one year. Community generates the certificate regardless of whether the current certificate is current or expired. Certificates are stored in the Personal and Trusted Root Certification Authorities folders on the local machine. For details about exporting/importing the certificate, refer to the API documentation.

Lock Access

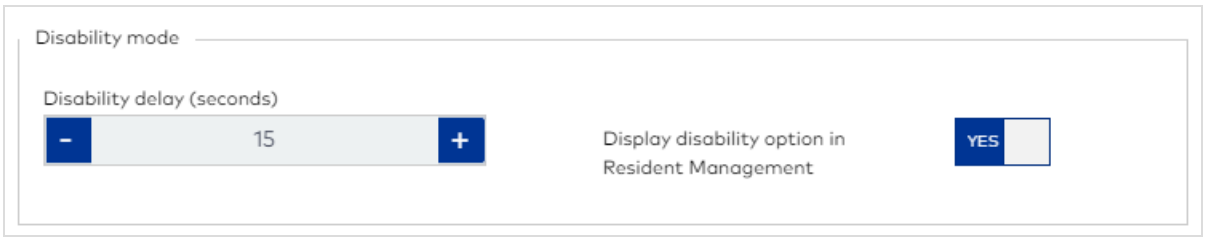
Changes to any settings in this section may require re-programming affected access points.



- **Escape\return**—For each access point type, select whether to allow a grace period during which a lock remains accessible without a key when the door is opened then closed from the inside. If any access point is enabled for Escape/return, specify the number of seconds the lock remains accessible. Defaults: NO / 60. Valid values: 20-300 (increments of 20).
- **Quick relatch**—For each access point type, select whether the lock is relatched immediately after the door is opened. If quick relatch is disabled, the lock is relatched 4 seconds after presenting a valid access key.

Access points can be programmed for both Escape/return and Quick relatch. However, these settings are not allowed for access points that are enabled for toggle mode.

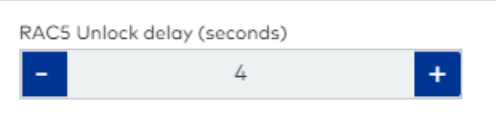
Disability mode



- **Disability delay**—Specify the number of seconds for the access point to remain in an unlocked state after presenting a valid key with the disability option. This option only applies when the **Display disability option inResident Management** is set to **YES**, and **Enable disability option on resident keys** is selected when making resident keys. Default: 15. Valid values: 10-60.
- **Display disability option in Resident Management**—Enable or disable the option to apply the disability delay when making resident keys. The disability delay cannot be applied to resident keys without enabling this option. Default: NO.

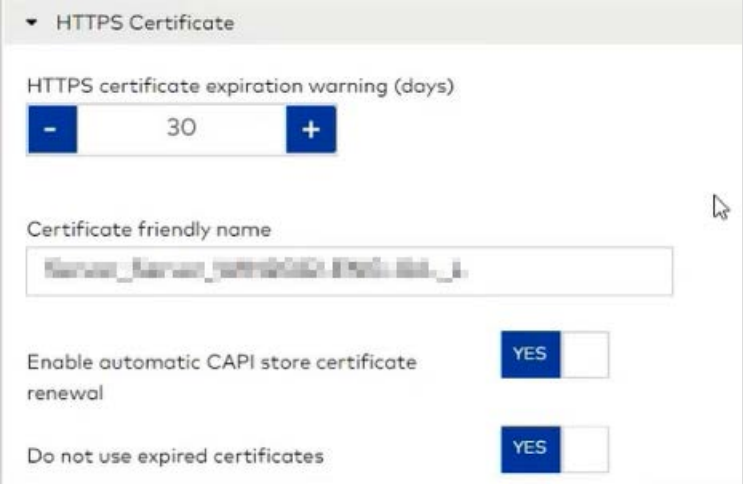
RAC5 option

Changes to this setting may require reprogramming locks.



- **Unlock delay**—Specify the number of seconds for the RAC5 access point to remain in an unlocked state after presenting a valid key. Default: 4. Valid values: 4-60.

HTTPS Certificate



When Community is deployed with an SSL certificate:

- Specify the number of days before the certificate expires to start receiving a daily warning. Default: 30. Valid values: 0-365.

When a certificate from the CAPI store was selected during installation, the additional options are available:

- Modify and save the certificate friendly name.
- Enable automatic CAPI store certificate renewal. When enabled, Community detects a new certificate based on the friendly name and rebinds it to IIS. The detection frequency is one hour. The detection method uses **Valid from** dates. Default: NO.
  - When enabled, the option **Do not use expired certificates** displays. Default: YES. When set to YES, CAPI store certificate is ignored; when set to NO, expired certificate is used.

Enhanced Security Mode

Fresh installations

This option is disabled by default. When ready, refer to the section *Enable enhanced security mode*.

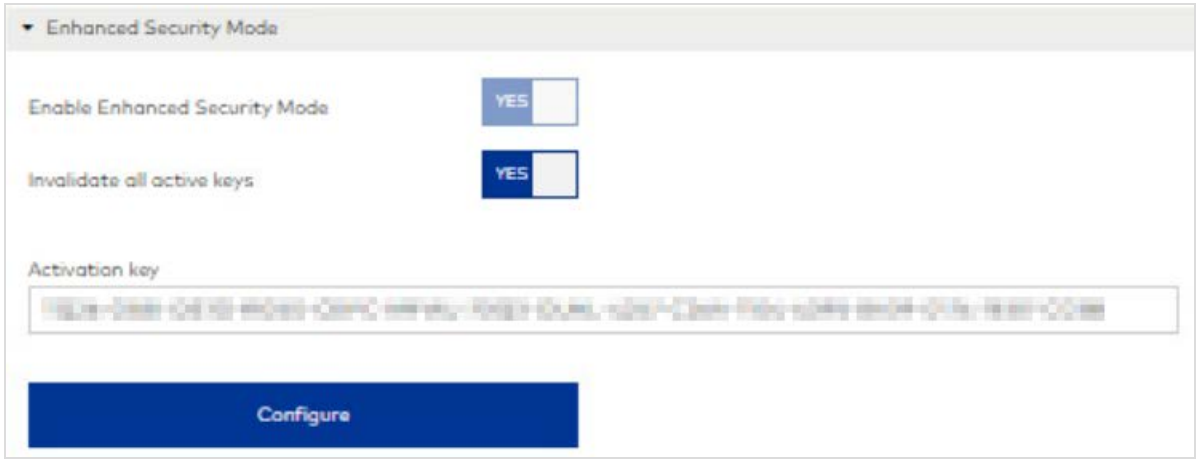
Enabling enhanced security mode (for upgrades and when previously disabled)

For a comprehensive list of requirements and step-by-step instructions to enable enhanced security mode, refer to *Community Enhanced Key Security* (PK3776).

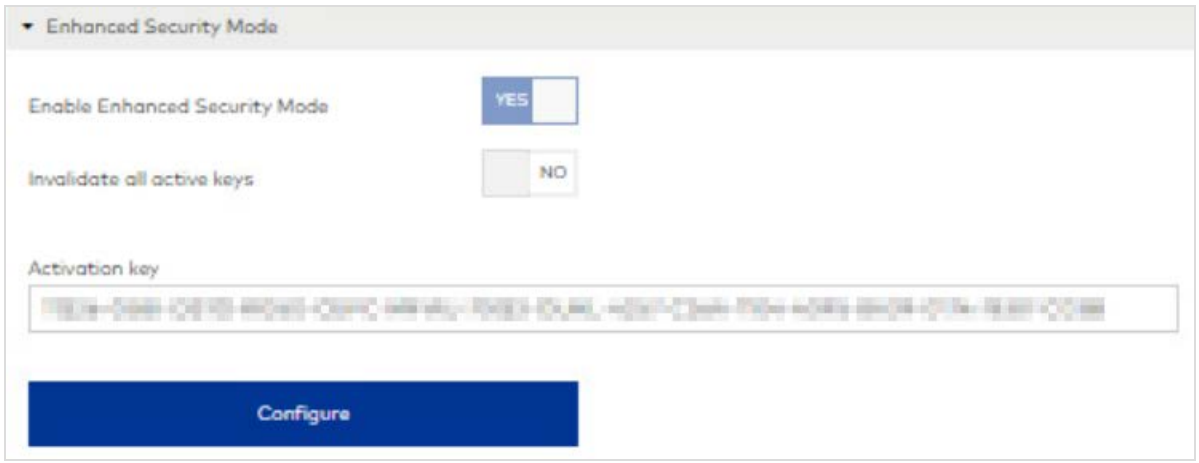
Enabling this option requires specific encoders (part 75720). At least one encoder must be configured before enabling enhanced security mode.

Before enabling enhanced security mode, obtain a valid 64-character activation key from dormakaba Support. Configuration requires that the Community server has access to the internet.

1. Change the **Enhanced Security Mode** switch to **YES**. Read the warning and select **YES** to continue.
2. Select whether to invalidate all active keys:
   - **YES**—Strongly recommended for Community. Select this option to start using enhanced security mode upon reprogramming access points.

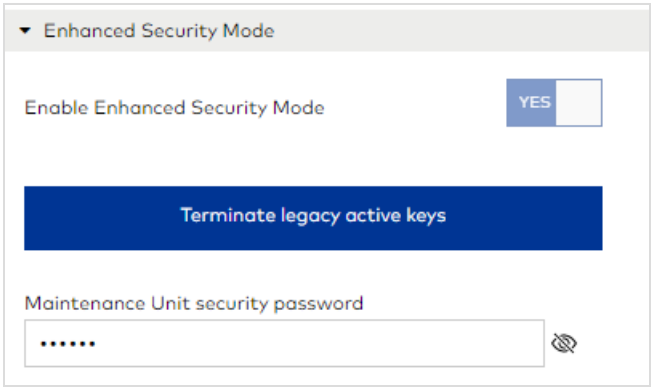


   - **NO**—Select this option to transition to enhanced security mode. Active keys remain valid until the command to terminate all active legacy keys is issued. dormakaba recommends a maximum of two weeks to complete the transition process.



3. Specify the 64-character activation key.
4. Click **Configure**. Read the warning and select **YES** to continue. Community configures the site. The Maintenance Unit security password setting appears. If keys were not invalidated in step 2, the **Terminate active legacy keys** button appears.

Enhanced security mode cannot be disabled after clicking **Configure**.



5. Go to System Keys and re-encode Failsafe Keys.
6. Go to Staff/Vendor Management and make all new RFID keys for active staff/ vendors.
7. Go to Resident Management and make all new RFID keys for active residents.
8. Go to **Programming & Auditing > Programming** and reprogram access points. Specify the M-Unit security password when prompted.
   - If all keys were invalidated in step 2, locks accept only enhanced security keys after reprogramming.
   - If keys were not invalidated in step 2, locks accept enhanced security keys and active legacy keys after reprogramming.
9. Go to Staff/Vendor Management and Resident Management and make all new BLE keys for active staff/vendors and residents, respectively.

If all keys were invalidated in step 2, the process is complete. If keys were not invalidated in step 2, proceed.

10. When ready to finalize the transition to enhanced key security, click **Terminate active legacy keys**.
11. Go to **Programming & Auditing > Programming** and reprogram access points again. Specify the M-Unit security password when prompted. After reprogramming, locks accept only enhanced security keys.

Single Sign-On

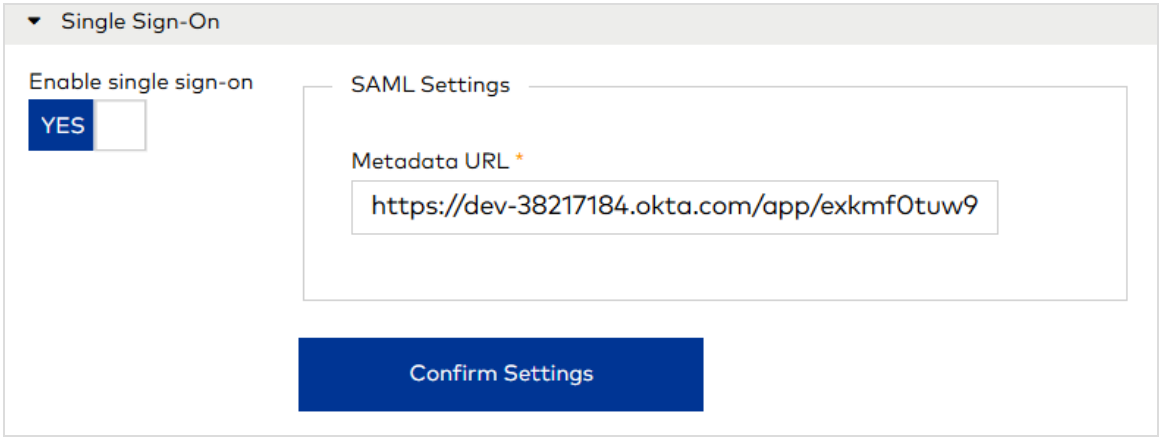
SSO (single sign-on) is a licensed feature that is disabled by default. Some configuration values are provided by dormakaba Support. Some values, as noted, are provided by the identity provider.

Enabling SSO

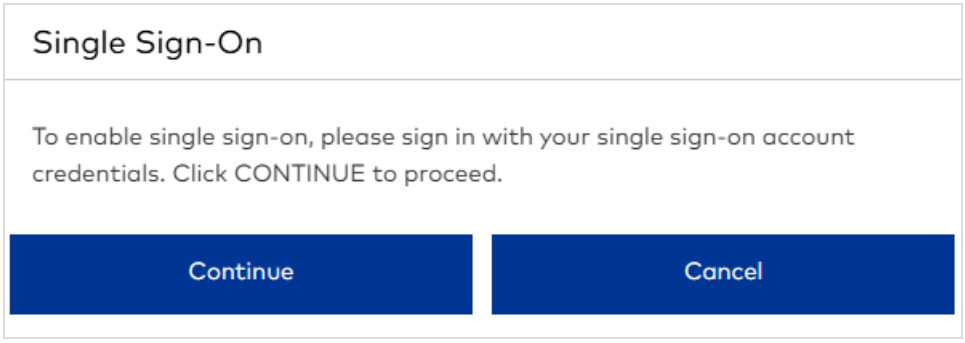
Before enabling SSO, establish the following prerequisites:

- Be prepared to log in to your SSO account during the configuration process.

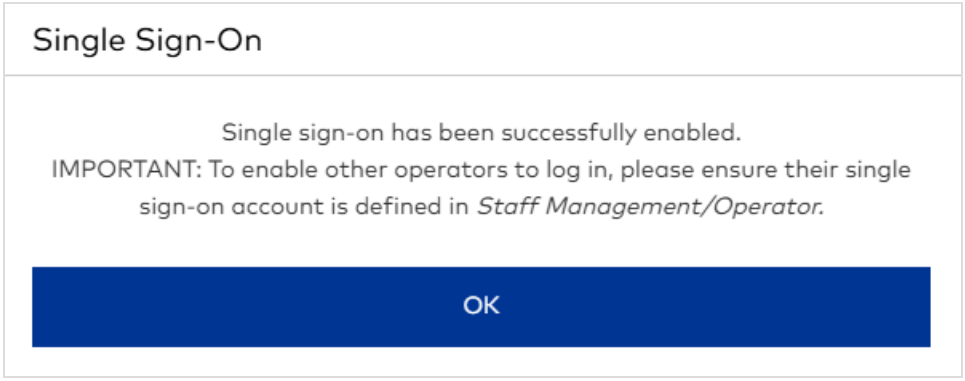
1. To enable SSO, change the **Enable single sign-on** switch to **YES**. At present, only the SAML authentication protocol is supported. SAML uses XML to exchange messages.



2. For **Metadata URL**, specify the location of the XML document containing configuration information about the SAML identity provider (IdP). The value is provided by the IdP.
3. Click **Confirm Settings**.



4. Click **Continue**. Community redirects to the identity provider login page.
5. Log in to your SSO account. The User ID for SSO can be either an email address or EID (Enterprise ID). Community saves the SSO settings and updates the operator's username / User ID in Staff/Vendor Management.



As the operator who switched to SSO, you are now the only operator who can log in to Community. You must now go to Staff/Vendor Management and specify the SSO User ID for each operator.

Identity provider settings

For sites that enable Single Sign-On, all alphabetic characters specified when configuring the SSO Identity provider (IdP) must be lowercase, including server name. For example, using the SAML ID provider Okta, the following fields use the server name:

- Single sign-on URL
- Audience URI
- Other Requestable SSO URLs

Configure your IdP with the applicable protocol settings.

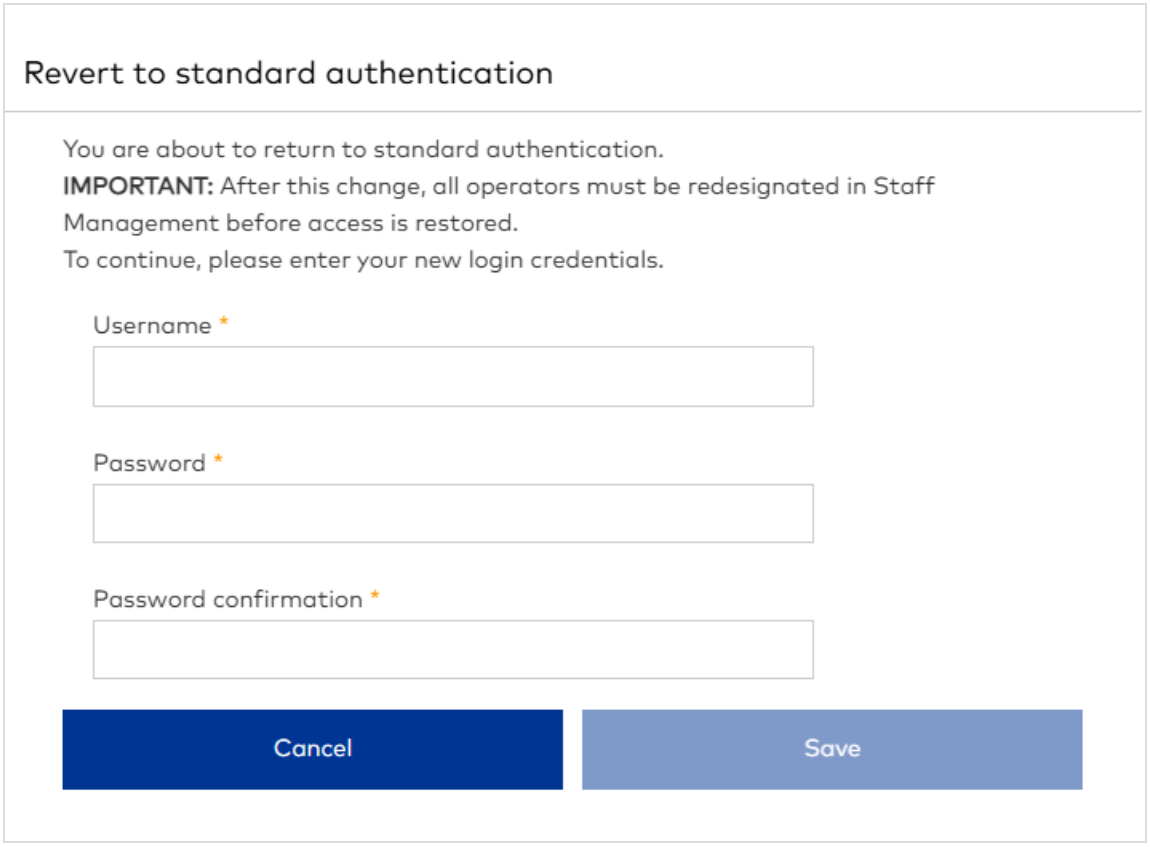
SAML

IdP setting	Value
Assertion Consumer Servcie URL (ACL URL) The on-premises ACS path is provided by the Sustainsys.Saml2 library and cannot be changed. Replace <server> with your server hostname, FQDN, or IP address. Depending on the IdP, terminology differs. Okta=Single sign-on URL, Ping=ACS URL, Microsoft Entra=Reply URL)	https://<community-server>/WebAPI/Saml2/Acs
Service Provider Entity ID (SP ID) Depending on the IdP, terminology differs. Okta=AudienceURI, Ping=Entity ID, Microsoft Entra=Identifier (Entity ID)	https://<community-server>/WebAPI/Saml2
Other Requestable SSO URL (IdP must register this as an additional callback, Index= 1)	https://<community-server>/WebAPI/api/SSO/ValidateSamlResponse
NameID Format	Unspecified
Single Logout (SLO)	Not used

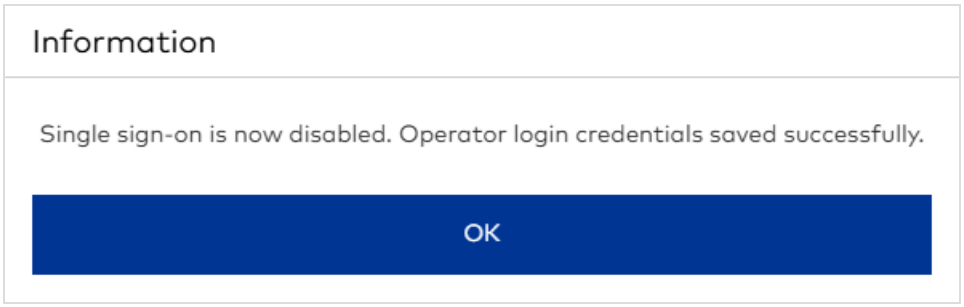
Disabling SSO

After taking this action, all other operators lose operator status and must be re-designated in Staff/Vendor Management to restore access.

1. To disable SSO, change the **Enable single sign-on** switch to **NO**.



2. Specify a new login username.
3. Specify and confirm a new password.
4. Click **Save**.

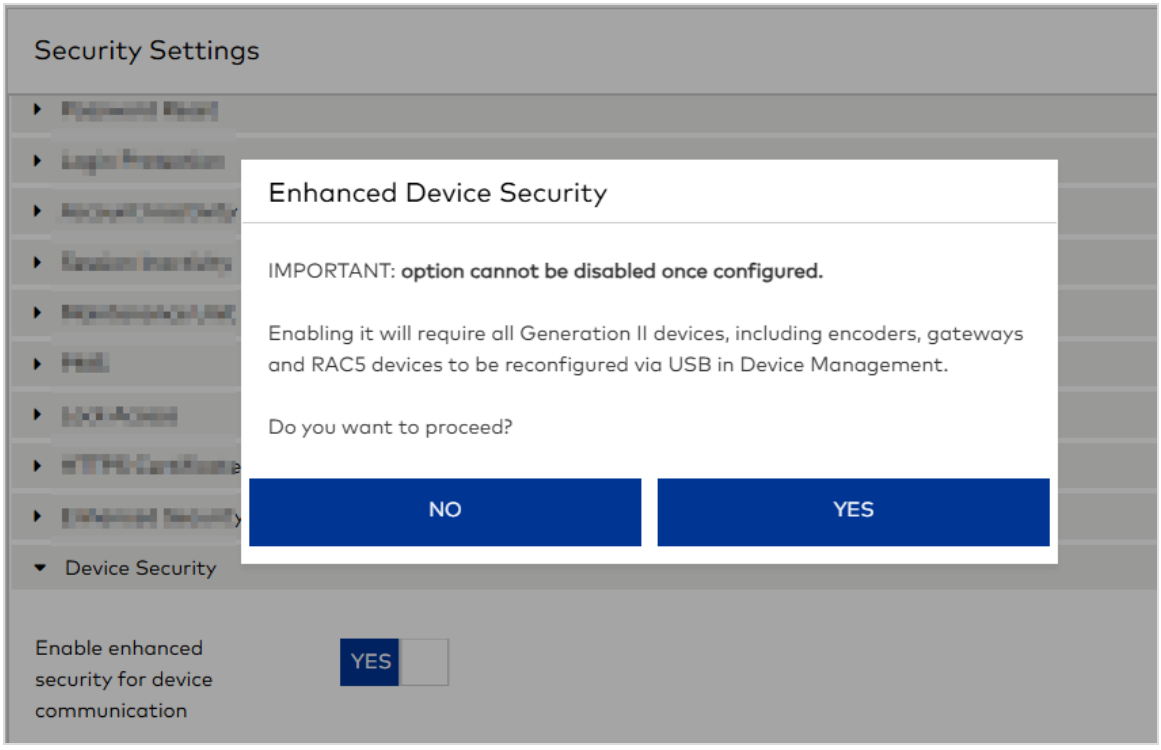


As the operator who reverted to standard authentication, you are now the only operator who can log in to Community. You must now go to Staff/Vendor Management and re-designate operators.

Device Security

Upgrades only. Activate device-specific certificates to enhance security for encoder Gen II and gateway Gen II communication. (The option is enforced by default for new installations.)

1. To enable device security, change the **Enable enhanced security for device communication** switch to **YES**.



2. Read the message that informs all Generation II devices, including encoders, gateways and RAC5 devices, must be reconfigured in **Device Management**.
3. Click **YES** to proceed.

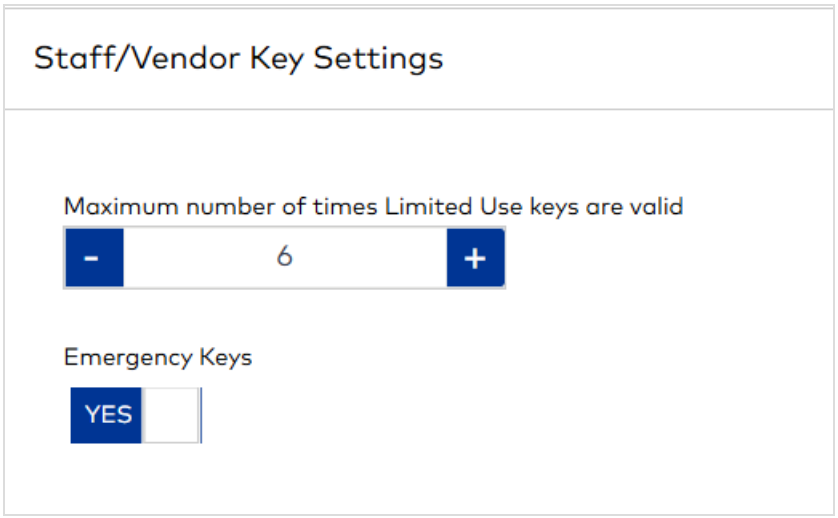
After device security is enabled, Community:

- Generates and stores server-side and client-side IP device certificates.
- Permanently disables the **Enable enhanced security for device communication** switch.
- Takes Generation II devices offline until reconfigured.

Staff/Vendor Key Settings

Configure system-wide defaults for Staff/Vendor Keys.

1. Go to **System Settings > Staff/Vendor Keys**.



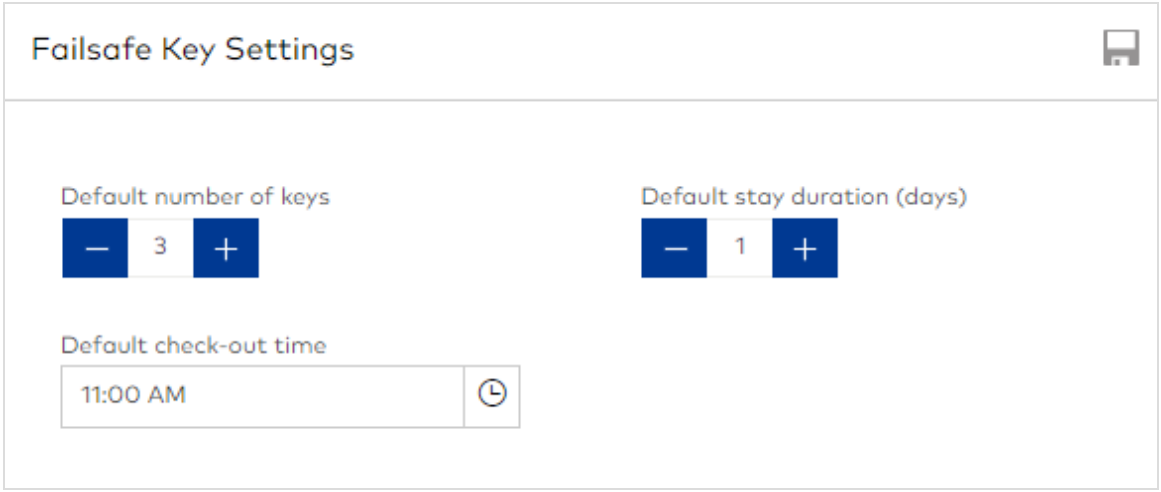
2. Specify the number of times a Limited Use Key can be utilized. Default: 6. Valid values: 1-6.
3. Select whether to enable Emergency Keys. This setting affects the available options in **Role Management**, **Credential Management** and **Staff/Vendor Keys**. When this option is not enabled, no Emergency keys can be made for the site. When Emergency keys are enabled:
   - In **Role Management**, the Emergency credential class is listed and can be selected for Key rights.
   - In **Credential Management**, Emergency credentials can be created (also viewed and deleted).
   - In **Staff/Vendor Keys**, keys can be made using the Emergency credential class.
4. Click **(Save)**.

Failsafe Key Settings

Failsafe Keys are backups of individual unit keys that are made in advance and maintained in complete sets to be issued to residents in the event of a system or power failure. The recommendation is to create and maintain two sets of three keys for each unit and suite door. After one set of Failsafe keys is issued and used, make another set of Failsafe keys to replace the used set. Locks only accept keys from the two most recent Failsafe key sets.

Using a Failsafe Key invalidates previous resident key access to units, suite common doors and suite unit doors.

1. Go to **System Settings > Failsafe Keys**.



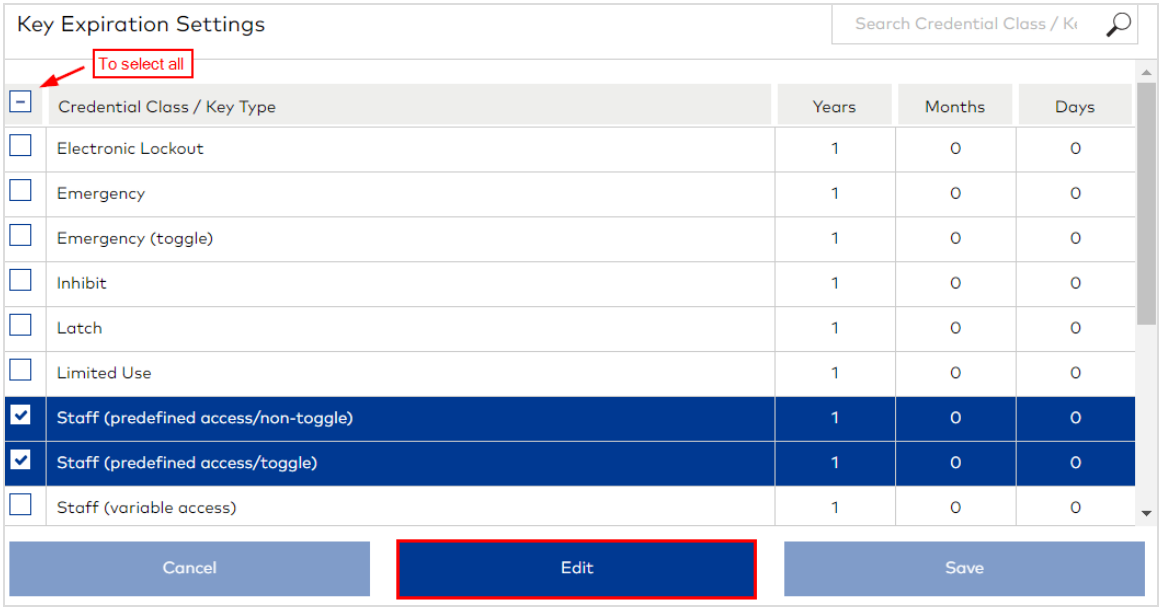
2. Specify the default number of Failsafe Keys to create for each access point. Default: 3.
3. Specify the number of days Failsafe Keys remain valid. After first use, the Failsafe Keys expire after the specified number of days. Default: 1.
4. Select the time after which Failsafe Keys are invalid on the final day of the stay. Default: 11am.
5. Click **(Save)**.

Key Expiration Settings

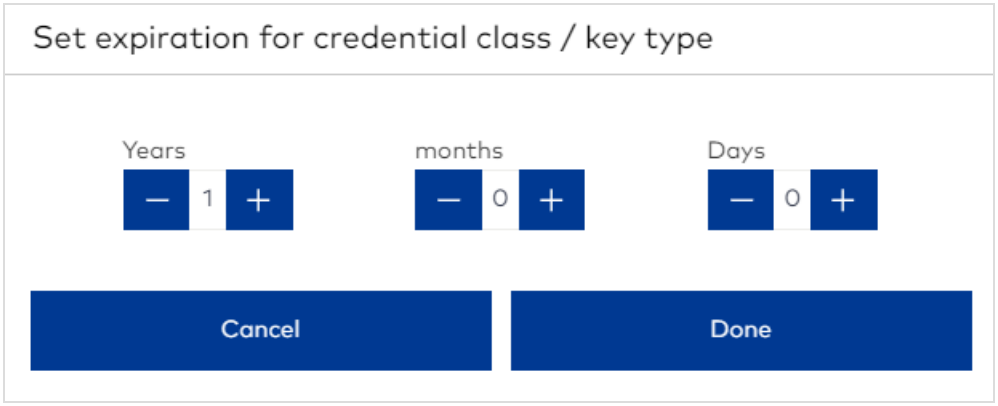
Configure default key expiration dates for credential classes and key types.

Expiration dates can always be changed at key-making time.

1. Go to **System Settings > Key Expiration**.



2. Select the credential class or key types (or the checkbox adjacent to **Credential class/Key type** to select all).
3. Click **Edit**.

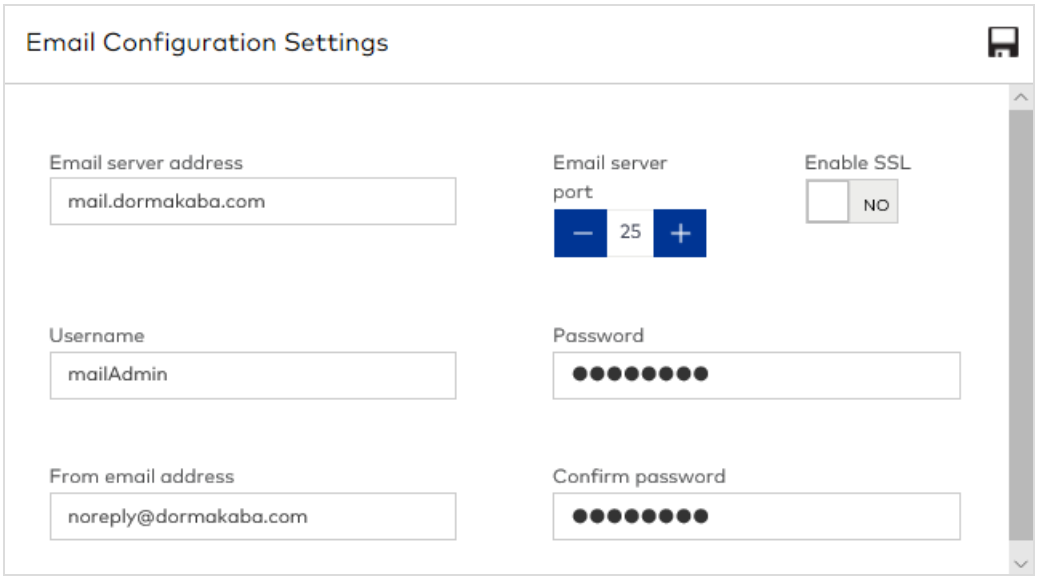


4. Select the number of years, months and days used to calculate the expiration date for the selected credential class/key types. Min: 1 day, Max: 9 years. Default: 1 year.
5. Click **Done**.
6. Click **Save**.

Email Configuration Settings

Configure the email settings used to send automated emails to staff/vendors.

1. Go to **System Settings > Email**.



2. For **Email server address**, specify the IP address or host name of the email server.
3. Specify the communication port on the email server dedicated for automated emails.
4. Select whether to enable SSL (Secure Sockets Layer). When SSL is enabled and security certificates are valid, all email data sent from the email server to mail clients is private and secure. Default: NO. Recommended value: YES.
5. Specify valid account credentials for the account used to send automated email.
6. For **From email address**, specify the email address for the account sending the automated email.
7. Click **(Save)**.

Database backup settings

dormakaba strongly recommends scheduling automated backups to an external hard drive, network drive, or remote server and storing backup data in a secure location off-site.

Refer to the following table for backup details.

Data	Location Stored	Backup Option	Frequency	Retention
SQL Server	Specified directory (local or remote) Default: C:\Program Files\Microsoft SQL Server\MSSQL16.COMMUNITY\MSSQL\Backup Default for upgrades: existing setting persists	On-demand	On-demand	Current backup
		Per schedule	Per schedule	Per setting
GDPR symmetric key	ProgramData\DormaKaba\Community\backup (local only)	Per site policy		
MongoDB	MongoDB folder in specified directory (local only) Default for new installations and upgrades with remote SQL Server: none Default for upgrades with local SQL Server: existing setting persists	Per schedule	Per schedule	Latest backup
Archive	Specified directory (local allowed but external hard drive, network drive, or remote server recommended) Default: C:\Program Files\dormakaba\Community Server\Archive Default for upgrades: existing setting persists	Per schedule	Per schedule	Indefinite

In compliance with the GDPR (General Data Protection Regulation), all PII (Personally Identifiable Information) stored in the database is encrypted. A site-specific encryption key that is required to restore the database is saved on the Community server at \ProgramData\DormaKaba\Community\backup. dormakaba recommends to keep a copy of the key file at a separate secure location.

Storing backups on a remote server

If specifying a remote path for database backups, you must meet the following requirements:

- Community Server and SQL Server may be on the same machine or different machines, but they must be in the same domain.
- The remote backup folder may be on the same or a different machine as SQL Server, but there are no domain requirements.
- The Community Server must have full access to the shared folder. Permissions are set at the folder level on the remote server.

On the Community Server:

1. Create a backup folder with the same name and directory as the remote server. For example, G:\backup must exist on both the Community and remote servers.
2. Open and log in to SQL Server Management Studio.
3. Navigate to **Security** > **Logins** > **NT AUTHORITY\SYSTEM**, right-click and select **Properties**.
4. Select **Server Roles**.
5. Select **sysadmin**.
6. Click **OK**.

On the remote server:

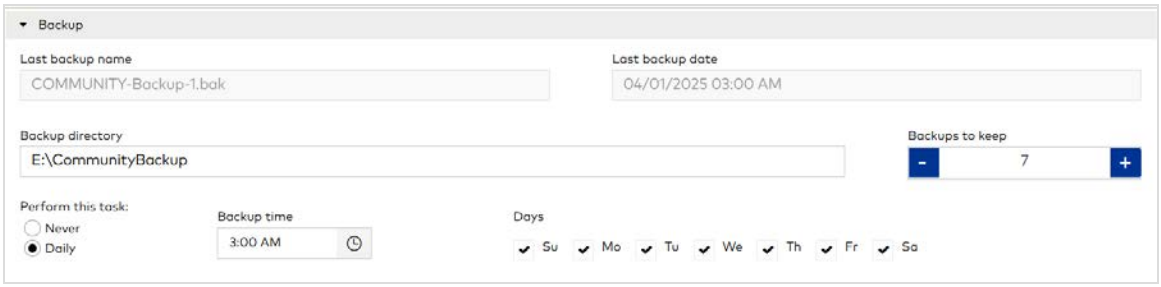
Share the backup folder and add read/write access for the domain user.

To verify the directory path when specifying a remote server, right-click the shared folder, select **Properties**, click the **Sharing** tab, then refer to the value for **Network Path**.

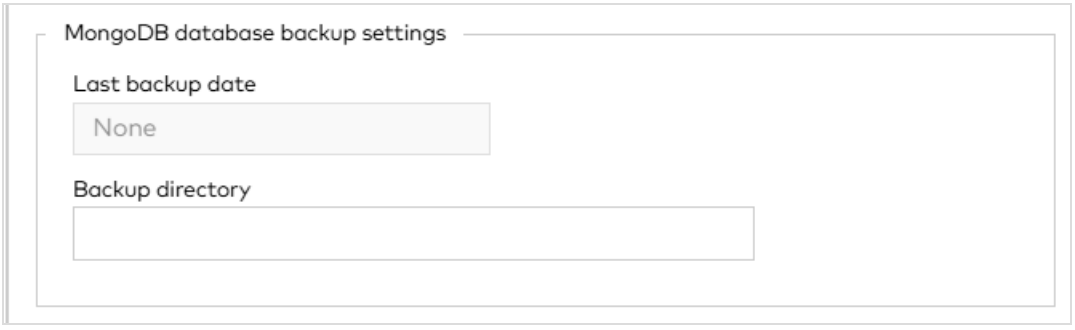
Configure backups

Configure scheduled database backups.

1. Go to **Systems Settings > Database Backup**.



2. SQL Server database backup settings:
   - **Backup name**—Read-only field that shows the name of the most recent SQL Server database backup.
   - **Last backup date**—Read-only field that shows the date of the most recent backup. Blank if never backed up.
   - For **Backup directory**, specify where you want to store database backups. You must specify the full path to a location accessible by the Community server. Although you can specify a local path, **dormakaba strongly recommends saving backups on an external drive, network drive, or remote server**. If specifying the path to a remote server, you must meet the requirements for storing backups on a remote server.
   - For **Backups to keep**, click -/+ to specify the number of SQL Server backups to retain in the backup directory. When the number of backups exceeds the specified number, the oldest backup is deleted from the backup directory. Default: 7. Maximum: 99.
3. Online communication enabled only. MongoDB database backup settings:



   - **Last backup date**—Read-only field that shows the date of the most recent MongoDB database backup. Blank if never backed up.
   - **Backup directory**—Specify where you want to store MongoDB database backups on the local server. Remote paths are not supported.

   Because only the most recent backup of the MongoDB database is retained, establish an external process to back up the MongoDB database if more than the most recent backup is required.

4. General settings:



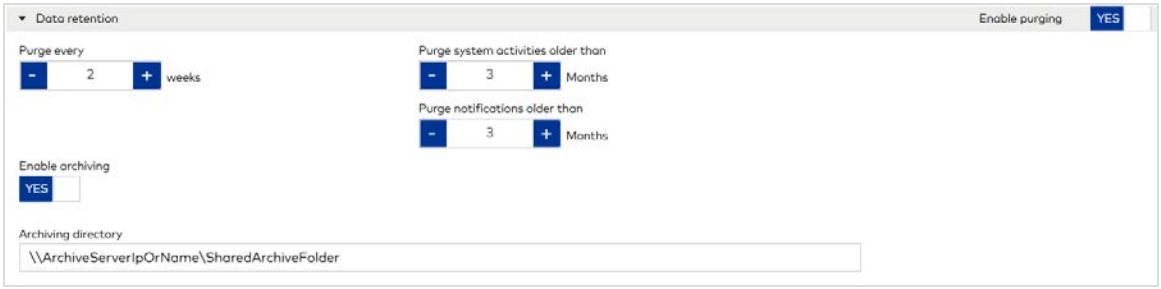
- **Perform this task**—Select one of the following options (Default: Daily):
  - **Never**—No backups are regularly scheduled. You must back up the database manually or use an external process. When you select this option, archiving cannot be enabled.
  - **Daily**—If you select this option, specify when and on which days to perform a scheduled backup.
    - **Backup time**—Click (Clock) and select the time to initiate the backup. Default: 03:00 (3AM).
    - **Days**—Select all days on which to perform a scheduled backup. Default: all days.

5. Click **(Save)**. Upon saving settings, Community validates the specified directory path.

Configure data retention

To configure data retention:

1. Go to **System Settings > Database Backup > Data retention.**



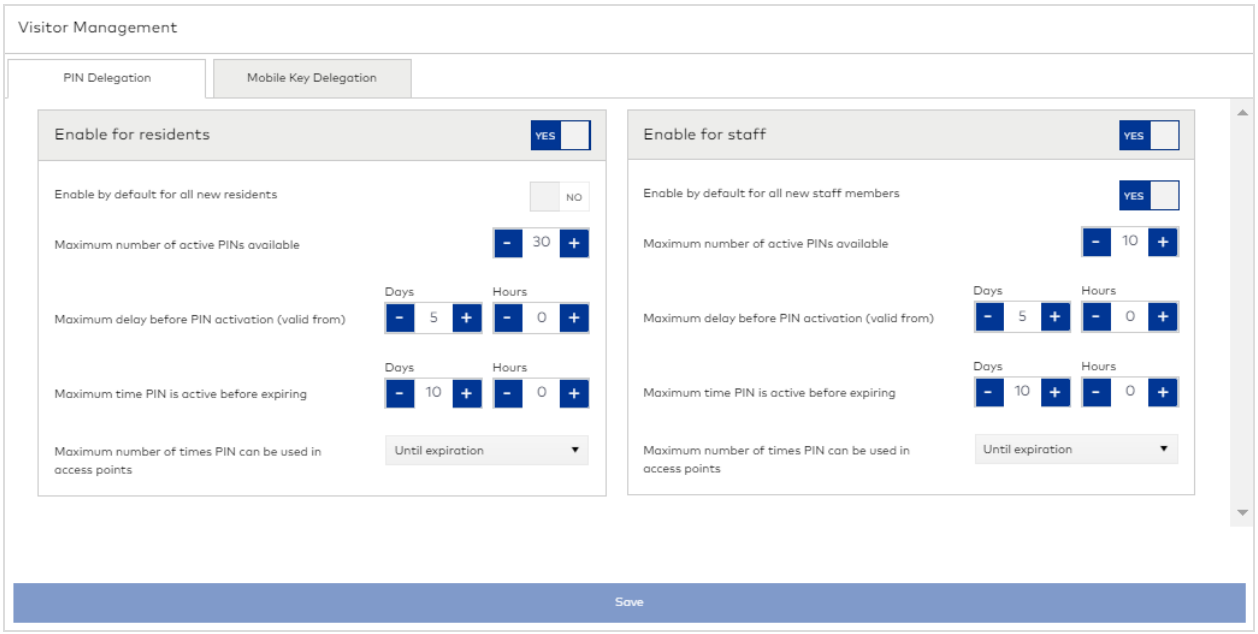
2. For **Enable purging**, select whether to enable purging. Recommended value: YES. If purging is not enabled, the database will grow to the system limit and space will be unavailable for normal processing.
3. For **Purge every**, click -/+ to specify the weekly frequency for purging historical data.
4. For **Purge system activities older than**, click -/+ to select the number of months to retain system activity records in the Community database. All system activity records that go beyond this threshold are deleted. Default: 3.
5. For **Purge historical online operations/events older than**, select the number of months to retain database records for online operations and events. All online records that go beyond this threshold are deleted. Default: 3.
6. For **Purge notifications older than**—Click -/+ to select the number of months to retain notifications in the Community database. All records that go beyond this threshold are deleted regardless of whether the notification has been read. This option only displays if online communication is enabled in **System Settings > Advanced**. Default: 3. Valid values: 1-12.
7. For **Enable archiving**, select whether to enable archiving. Default: **NO**. Recommended value: YES. If archiving is not enabled, the database will grow to the system limit and space will be unavailable for normal processing.
8. For **Archiving directory**, specify the full path to a location accessible by the Community server. **Although you can specify a local path, dormakaba strongly recommends an external hard drive, network drive, or remote server.** If specifying a remote path, you must meet the following requirements:
   - Create and point to a shared folder on the remote server.
   - The Community Server must have full access to the shared folder.
9. Click **(Save)** .

Visitor Management Settings

Configure default values to support PIN and BLE delegation in **Resident Management** and **Staff/Vendor Management**.

» Go to **System Settings > Visitor Management**.

PIN delegation

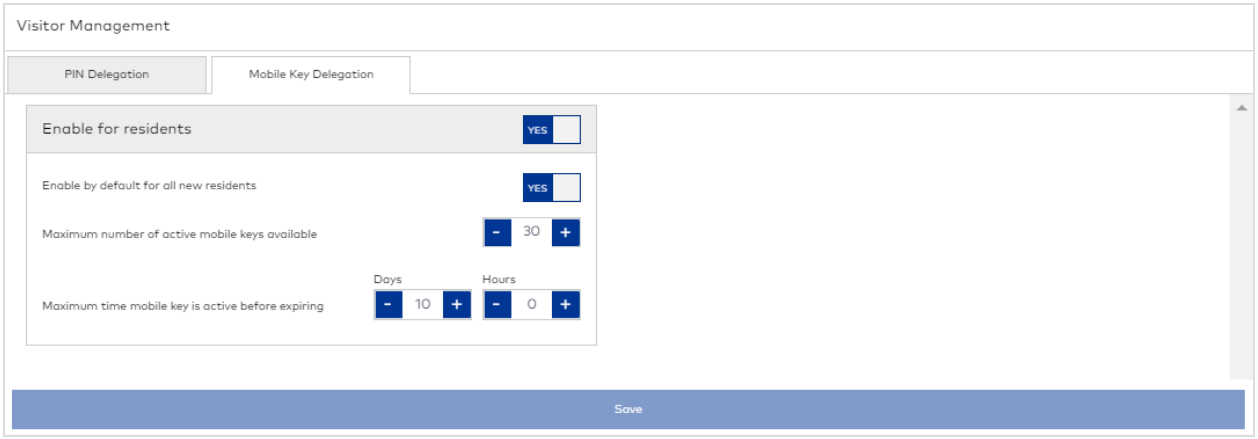


Enable and configure PIN delegation:

- **Enable for residents**—Enable the Visitor Management PIN functionality in **Resident Management**. Default: NO. Upon selecting **YES**, a message box prompts to acknowledge the responsibility of activating the feature. Click **ACCEPT** to continue.
- **Enable for staff**—Enable the Visitor Management PIN functionality in **Staff/Vendor Management**. Default: NO. Upon selecting **YES**, a message box prompts to acknowledge the responsibility of activating the feature. Click **ACCEPT** to continue.
- **Enable by default for all new residents/staff members**—Enable PIN functionality for all new resident and staff/vendor profiles. When the feature is enabled, the PIN section displays on the Visitor Management tab in all new profiles, PIN settings can be customized, and PIN settings can be updated on mobile devices. Default: NO. Upon selecting **YES**, a message box prompts to acknowledge the responsibility of activating the feature. Click **ACCEPT** to continue.
- **Maximum number of active PINs available**—Specify the default value in resident and staff/vendor profiles for the maximum number of PINs that can be active. Valid values: 1-50. Default: 10 .
- **Maximum delay before PIN activation (valid from)**—Specify the default value in resident and staff/vendor profiles for the maximum number of days/hours that a PIN can be created before access authorized by the PIN starts. Range for Residents: 0-15 days/0-23 hours. Range for staff: 0-30 days/0-23 hours. Default: 0 days/0 hours.
- **Maximum time PIN is active before expiring**—Specify the default value in resident and staff/vendor profiles for the maximum number of days/hours that a PIN can be active. Range for residents: 0-15 days/0-23 hours. Range for staff: 0-30 days/0-23 hours. Default: 1 day/0 hours.
- **Maximum number of times PIN can be used in access points**—Specify the default value in resident and staff/vendor profiles for the maximum number of times a PIN can be used in access points. Valid values: Until expiration, 1-5. Default: Until expiration.

- **Authorized common areas**—Select the common areas where access is enabled by default on the Visitor Management tab in resident and staff/vendor profiles.

Mobile key delegation



Enable and configure mobile key delegation:

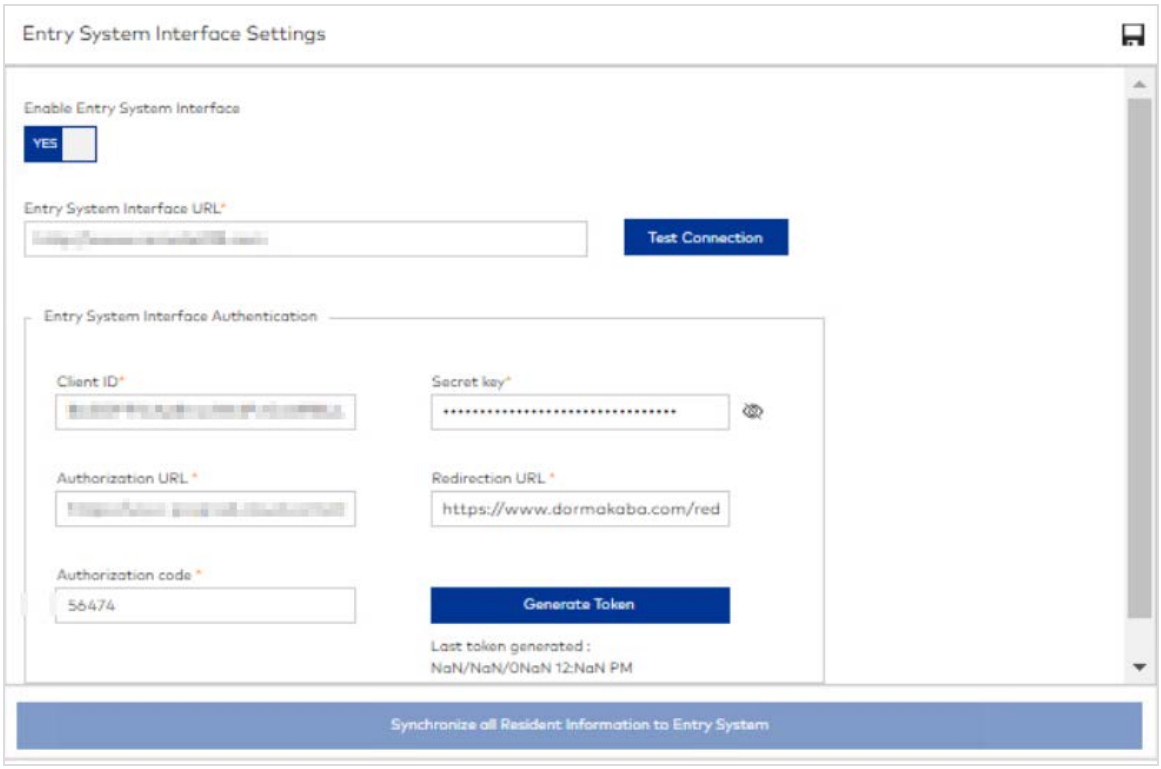
- **Enable for residents**—Enable the Visitor Management mobile key delegation functionality in **Resident Management**. Default: NO. Upon selecting **YES**, a message box prompts to acknowledge the responsibility of activating the feature. Click **ACCEPT** to continue.
- **Enable by default for all new residents**—Enable mobile key delegation for all new resident profiles. When the feature is enabled, the mobile key delegation section displays on the Visitor Management tab in all new profiles, settings can be customized, and settings can be updated on mobile devices. Default: NO. Upon selecting **YES**, a message box prompts to acknowledge the responsibility of activating the feature. Click **ACCEPT** to continue.
- **Maximum number of active mobile keys available**—Specify the maximum number of delegated mobile keys that can be active for the resident. Valid values: 1-50. Default: 10.
- **Maximum time mobile key is active before expiring**—Specify the default value in resident profiles for the maximum number of days/hours that a delegated mobile key can be active. Range: 0-15 days/0-23 hours. Default: 1 day/0 hours.

Entry System Interface Settings

Entry System Interface is a licensed feature that is disabled by default.

Community integrates with third-party entry systems to extend resident access management options. Configuring authentication for the entry system is optional. For implementation details, obtain *Entry System RESTful API Documentation* from dormakaba Support.

1. Go to **System Settings > Entry System Interface**.



2. Enable the entry system interface.
3. Specify the URL to the third-party entry system. Optionally, test the connection.
4. Authentication options—The values for Client ID, Secret key, Authorization URL, Redirection URL and Authorization code are provided by the third party and are required to generate a token.
5. Click **Generate Token**.
6. Click **(Save)**.
7. Click **Synchronize all Resident Information to Entry System**. All resident information is synchronized to the entry system. Future changes to resident profiles are automatically synchronized every two minutes.

Advanced Settings

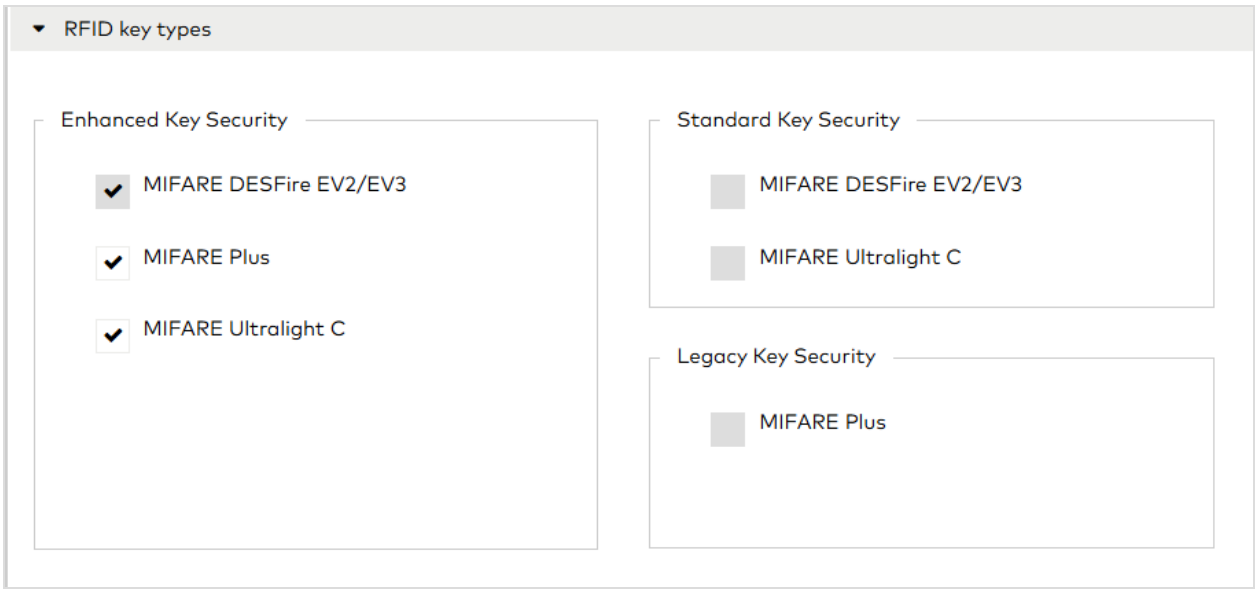
To configure advanced settings:

1. Go to **System Settings > Advanced**.
2. Specify options. Refer to the sections below for details.
3. Click **(Save)** .

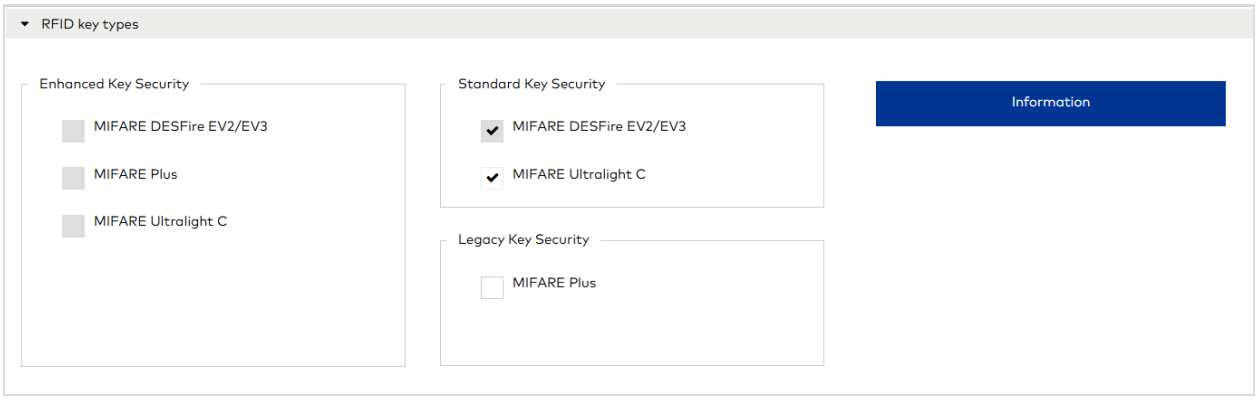
RFID key types

If displayed, click the **Information** button in this section to read the security advisory.

Enhanced Key Security enabled



Enhanced Key Security disabled



Changing the RFID key type is rare and requires reprogramming all locks.

To change the RFID key type, select the option that applies to your deployment then reprogram locks.

- **Enhanced Key Security**—Only available when enhanced security mode is enabled. When this section is enabled, the following key types are available:

  - **MIFARE DESFire EV2/EV3**—Selected and disabled by default.
  - **MIFARE Plus**—Selected and enabled by default. For upgrades, selected if previously selected or upon enabling Enhanced Security Mode if previously selected in Legacy Key Security.
  - **MIFARE Ultralight C**—Selected and enabled by default. For upgrades, selected if previously selected or upon enabling Enhanced Security Mode if previously selected in Standard Key Security.
- **Standard Key Security**—When this section is enabled, the following key types are available:
  - **MIFARE DESFire EV2/EV3**—Selected and disabled by default.
  - **MIFARE Ultralight C**—Selected and enabled by default.
- **Legacy Key Security**—Selecting an option in this section prompts a security reminder message. When this section is enabled, the following key types are available:
  - **MIFARE Plus**—Deselected and enabled by default.
  - **MIFARE Classic**—Not supported for new installations. For upgrades, only displays if previously selected. Contact dormakaba Support.

The selected key technology controls the number of additional access points that can be encoded on keys. Moreover the access points that are considered *additional* differs for resident and staff/vendor keys. (Common areas do not count as additional access points.)

- Resident keys—All access points are considered additional.
- Staff/Vendor keys—All access points that are added at key-encoding time (excluding the access points assigned to the selected credential) are considered additional.

Key technology limits for additional access points:

- MIFARE DESFire EV2/EV3: 94
- MIFARE Ultralight: 6
- MIFARE Mini: 6
- MIFARE Classic & Plus 1k/2k: 94
- MIFARE Classic & Plus 4k: 542
- Mobile key: 25

Property configuration

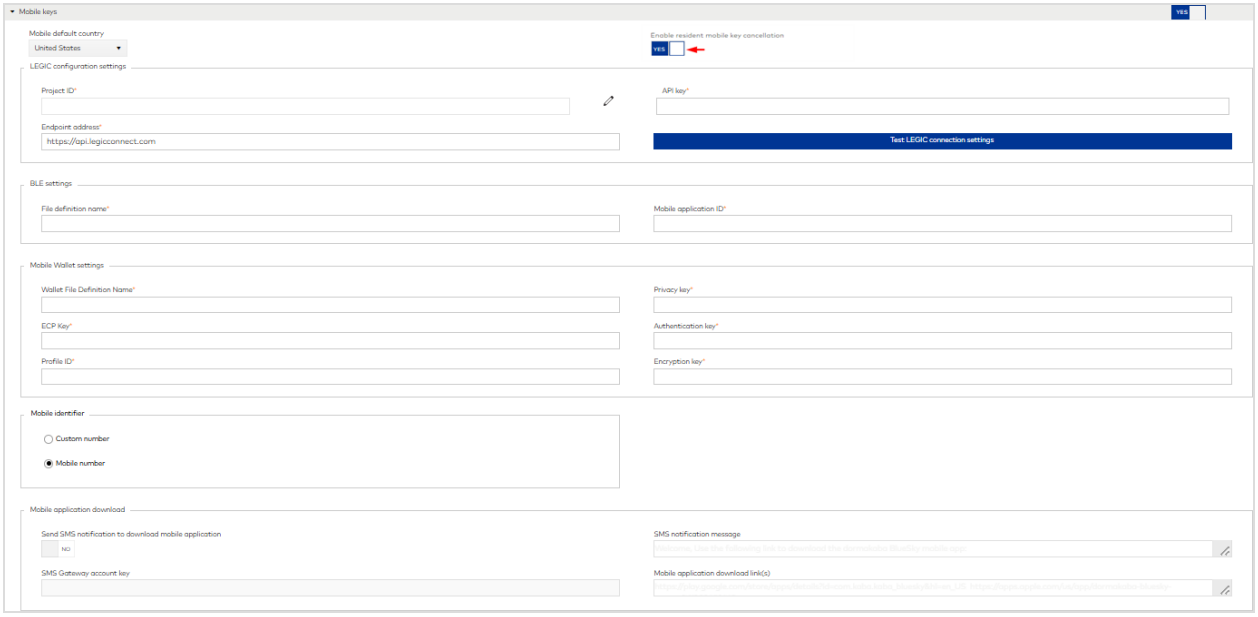


Select whether to enable extended common area configuration. Enabling this option increases the number of limited common areas that can be defined from a combined maximum of 12 (for limited common areas and elevators) to a maximum of 256 for limited common areas and 80 for elevators. When any type of limited common area is defined, changing this option requires deleting then recreating all limited common areas in **Property Builder**, reprogramming the affected access points, and re-encoding all keys (including mobile) on which the limited common areas are encoded. Default: NO. Default: For fresh installations and upgrades with zero limited common areas: YES; for upgrades with any type of limited common area: NO.

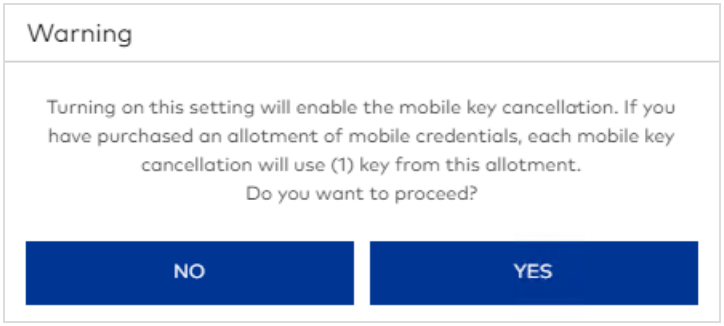
All lock models except RT and Legacy Confidant support extended common areas.

Mobile keys

Mobile keys is a licensed feature that is disabled by default.



1. Set the **Enable mobile keys** switch to **YES**.
2. For **Mobile default country**, select the default country for mobile numbers. The corresponding country code is retrieved for the mobile number.
3. (*conditional, licensed option*) If you want the ability to cancel mobile keys issued to residents and visitors, set the **Enable resident mobile key cancellation** switch to **YES**. If mobile keys are enabled and this option is not enabled, you cannot cancel a mobile key. Instead, the expiration details determine when the mobile key becomes invalid.



4. For **LEGIC configuration/BLE/Mobile Wallet settings**, a dormakaba Customer Service technician provides valid values. Modifying the privacy, authentication and/or encryption keys requires access point reprogramming.
5. For **Mobile identifier**, select one of the following:
   - **Custom number**— When mobile key holders will be using a third-party app integrated to Community, consult your integration solution provider for guidance on whether to configure as **Mobile number** or **Custom number**.
   - **Mobile number**—Select when mobile key holders will be using the dormakaba BlueSky app.
6. Only when mobile identifier is mobile number. For **Mobile application download**, select whether to send a text message to recipients of mobile keys to notify them that their device is not registered with the mobile application. If you select **YES**, you must also specify the message text to send, and an SMS Gateway account key (see note). Use the mobile application download links to download dormakaba BlueSky for Android and Apple devices, respectively. This feature is supported for all mobile keys (staff/vendors,residents, and visitors).

Community supports SMS text notifications through the use of the Swift SMS Gateway service. Information on this third-party service can be found at www.swiftsmsgateway.com.

Online communication

Online communication is a licensed feature that is disabled by default.

If the Community deployment is licensed for Remote Lock Management, set the soft-switch to **YES**. For more information, see Remote Lock Management.

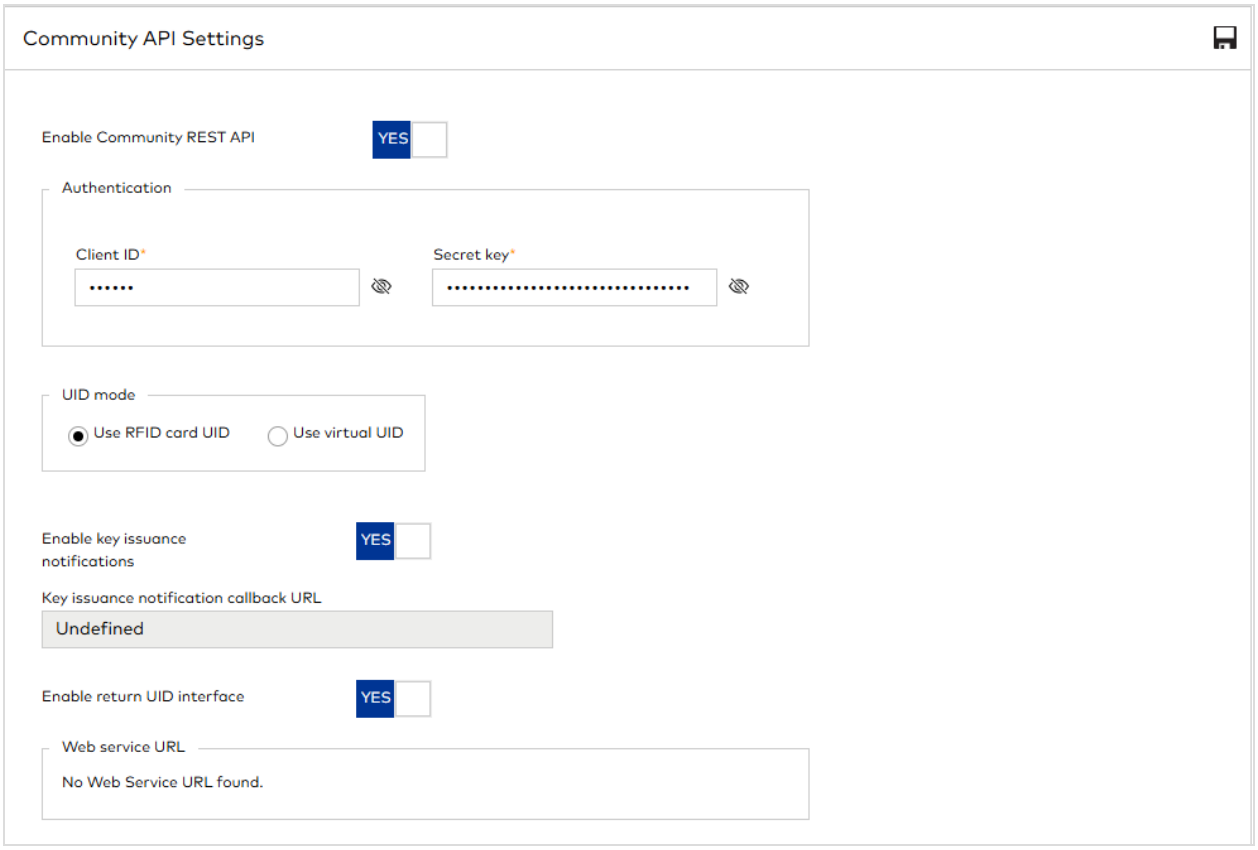
Keyscan Aurora

AuroraSync interface is a licensed feature that is disabled by default. If the Community deployment is connecting with an Aurora server to support Keyscan readers, set the soft-switch to **YES**.

Community API

Enable the Community REST API, key issuance notifications, and the return UID interface.

1. Go to **System Settings > Community API**.



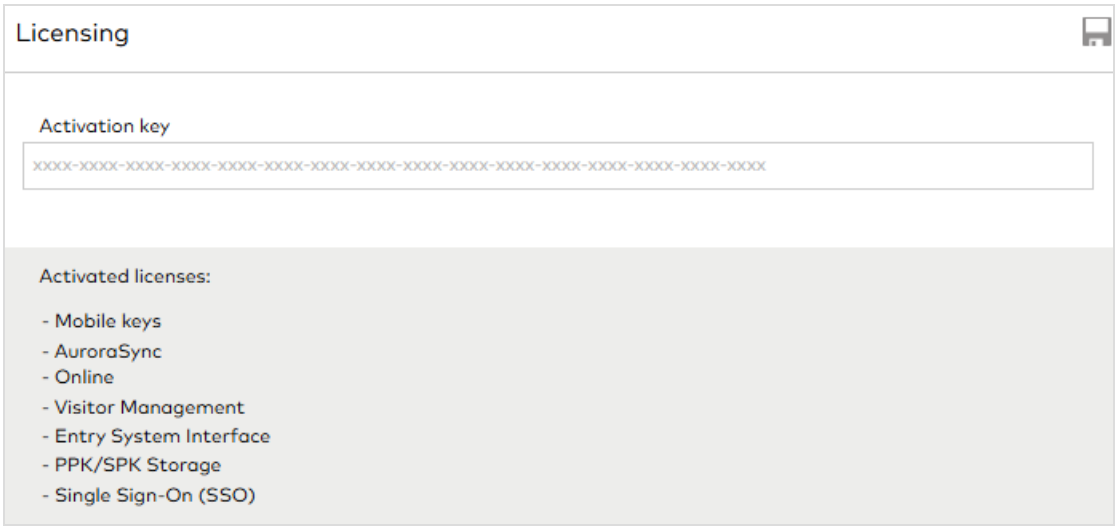
2. Change the **Enable Community REST API** soft-switch to **YES**.
3. Specify the unique client identifier and secret key used to obtain and renew an authentication token. Min chars: 6; max chars: 512 (for both settings).
4. Select the UID mode. This is a global setting.
   - **RFID card UID**—Select this mode when the credential is always encoded on a physical device that uses RFID technology (such as MIFARE keys). The UID is the serial number of the physical key.
     - For notifications, the UID is included in the notifications for all RFID keys. (For mobile keys, the UID is not included in the notification message. For Wallet keys issued from the Community REST API, the notification includes the Wallet card ID.)
     - For key making, the UID is included on all RFID keys issued from the user interface, Community REST API and Community SOAP API. (For mobile keys, the UID is not included. For Wallet keys issued from the Community REST API, the key includes the Wallet card ID.)
   - **Virtual UID**—Select this mode when the credential may be encoded on a device that uses a device/technology other than RFID (such as mobile keys). Community computes a virtual UID for all RFID and mobile keys issued from the user interface, Community REST API and Community SOAP API.
     - For notifications, the UID is included in the notifications for all RFID and mobile keys. (For Wallet keys issued from the Community REST API, the notification includes the Wallet card ID.)
     - For key making, the UID is included on all RFID and mobile keys issued from the user interface, Community REST API and Community SOAP API. (For Wallet keys issued from the Community REST API, the key includes the Wallet card ID.)

5. **Enable key issuance notification**—Select **YES** to enable notifications. Community sends a separate notification to the API each time a key is created. Third parities must first use the Community REST API to register a callback URL and optional security token to receive notification messages.
   - **Key issuance notification callback URL**—Read-only setting. The callback URL to use for sending notifications.
6. **Enable return UID interface**—Select **YES** to enable the Return UID interface. When Community integrates with a third-party elevator system. Third parities must first use the Community REST API to register at least one callback URL.
   - **Web service URL**—Read-only setting. The callback URLs to use for the third-party elevator system.
7. Click **(Save)** .

Licensing Settings

Licensed product features are enabled or disabled depending on the activation key.

1. Go to **System Settings > Licensing**.



2. Specify a valid activation key.
3. Click **(Save)**.

Activated licenses are displayed.

When licensed for PPK/SPK (Primary Program Key and Secondary Program Key) storage, the date and time that the data was stored is listed.

Step 2

Build Your Property

This section includes the following subjects:

Learning about Property Builder 52
Add buildings 58
Add floors 59
Add units 62
Add suites 66
Import units and suites list 71
Add resident common areas 72
Add staff common areas 78
Add restricted areas 84
Add elevators 86

Learning about Property Builder

Setting up your site in Community involves building a virtual representation of all access points on the property. Access points represent points of entry under control by Community. In most cases, an access point corresponds to a lock, such as the lock on a door. However, some access points correspond to different types of hardware such as an elevator reader.

Start by adding the buildings. Then for each building, add all floors. Next, add the individual units, suite units, common areas and restricted areas on each floor. You can also add elevators and configure elevator access.

Access point types

Community supports a maximum of 8,192 access points per site of which 4,095 may be for resident access point types (units and suites).

The following types of access points are created in Property Builder:

- **Unit**—An access point assigned to a resident during unit assignment.
- **Suite**—An access point that is a connected series of units including a common door and one or more suite unit access points.
- **Restricted Area**—And access point type intended for staff only for back-of-the-house access. For example, the Electrical Room would be a restricted area.
- **Resident Common Area**—An access point where general access is configured for residents. Access may be unlimited or limited.
- **Staff Common Area**—An access point where general access is configured for staff. Access may be unlimited (for staff) or limited.
- **Elevator**—An access point that provides access to building floors. An elevator bank is a group of elevators that share the same floor mapping.

Configuring floors and access points

During the process of adding floors and access points in Property Builder, the access point names that you will see in Community are formed. As such, the naming conventions for floors and access points should be descriptive and consistent so that you can create unique names that are easy to recognize when configuring access, making keys and reading reports.

Floor and access point names must not exceed 15 characters including spaces. Valid alphanumeric characters: A-Z, 0-9. Valid special characters: -#%=!,.:_()?*'<>/+.

Name formats

All floor names are formatted using numbers. The numbers that you select are used in the name of the floor. For example, if you select the range 1 to 10 when adding floors, then (using the default prefix FLOOR) you will add ten floors named Floor1, ..., Floor10.

Likewise, access point names are formed the same way with an additional option to format the name using numbers or text. Some access point types, such as common areas, are more suitable for using the text format, *Lobby* for example. If you use the number format, the floor number and unit number are, by default, included in the access point name. For example, if you select the range 1 to 1 when adding a unit to Floor1, then you will add one unit named 101 to Floor1.

Advanced formatting options

The simplest way to create descriptive floor and access point names is to use the advanced formatting options. For example, you can select to exclude the floor number from unit names and/or add a prefix to the unit number. Because access point names must be unique, you can only select numbers that have been used previously if you also specify a unique prefix or suffix. The advanced formatting options are not available for the text format.

When creating floors or access points in **Property Builder**, you can view a dynamic sample of your formatting selections in the **Preview** area.

Batch access point creation

To facilitate quick setup, Community allows batch creation of units and restricted areas. You can add multiple access points to multiple floors simultaneously. For example, if you select the range 1 to 10 when adding units to Floor1, ..., Floor10, then (using the default formatting) you will add ten units on each floor (101, ..., 110, 201, ..., 210, 301, ..., 310, and so on). The total number of access points equals 100.

Include in mobile keys download file

When licensed for mobile keys, the option **Include in mobile keys download file** displays when creating and editing access points. The option serves to identify the locks that are equipped to accept mobile key credentials. Select the option to include in the access point in the mobile keys download file, a report generated from the Buildings context menu in Property Builder.

Lock models

For the most current information about lock models, refer to the release notes.

Community supports the following lock models:

- **Nova**—All access points programmed with this lock profile operate in toggle mode.
- **Saflock Quantum/Saflok Confidant and Confidant NFC/Saflok RT, Saflok RT+/RCU (Remote Controller Unit)/Pixel and Pixel+/Saffire LX (L, M & P)**—For these profiles, toggle mode can be enabled for resident keys. This model also supports toggle mode for keys that are encoded with a credential based on a credential class that either includes toggle by default or is enabled to include toggle.

  Saflok Confidant and Saflok RT do not support extended common areas.

- **Saffire LX (D & I)/Saflok MT**—For these profiles, toggle mode is not supported.
- **RAC5 XT and RAC5 Lite**——For these profiles, toggle mode is supported. RAC5 XT is for online systems; RAC5 Lite does not support Remote Lock Management. Each RAC5 XT device can be mapped to a single access point or two different access points. Manually configure the number of access points to map by modifying the **DEVICES** switch on each RAC5 XT device. For more information, refer to RAC5 documentation.



All lock models for Unit, Suite Common Door and Suite Unit access points support 255 distinct active resident keys. All lock models for Resident Common Areas can manage resident keys (no touring mode) for a site deployed with up to 8,192 access points (combination of all access points).

Toggle Mode

Toggle is a feature that changes the state of a lock between *Latched* and *Unlatched* each time a valid key is presented to the lock. For example, the default state of a lock is *Latched*. The first time a key is presented, the lock changes to an *Unlatched* state. The door is open and remains accessible until the key is presented to the lock again or the interior privacy switch is engaged.

Toggle is enabled in different ways depending on lock type and credential class:

- Toggle may be a mechanical feature of the lock. For example, all Nova locks operate in toggle mode.
- For credentials based on the Emergency, Staff, Staff (variable access), and Vendor classes, toggle is enabled for unit and suite access points by selecting the option **Enable toggle mode** when creating the unit/suite access point in Property Builder. Valid for lock profiles: Saflok Quantum, Saflok Confidant, Saflock RT/RT+, RCU, Pixel and Saffire LX, RAC5 XT, RAC5 Lite.
- For credentials based on the Limited Use class, toggle mode is not supported.

Resident common areas

Resident Common Areas are spaces on your property that are configured for general access by residents and staff/vendors, such as lobbies, parking and recreational facilities. In the hospitality industry, we call these amenities. When you create a Resident Common Area access point, you have the option to enable limited access.

Staff keys only. Access to common areas always remains valid until key expiration. New keys cannot invalidate access to common areas. Cancel keys can only invalidate access to common areas when the key status is Active.

Unlimited resident common areas

When limited access *is not enabled*, the common area is included with all unit assignments and authorized on all Resident Keys. Unlimited Resident Common Areas are also authorized on all Staff/Vendor Keys.

Limited-access resident common areas

When limited access is enabled, access must be configured in **Access Management > Common Area Access**. Essentially, limited Resident Common Areas are associated with units. Resident access depends on the common areas associated with their assigned units/suite units.

When creating the limited common area, you must also select a common area ID. The ID is a numeric value used by the system to synchronize with third-party API (Application Programming Interface) settings. When extended common areas is enabled, there are a maximum of 256 common area IDs to support common areas (resident and staff/vendor). Without extended common areas, the limit is 12 which includes IDs for limited common areas and elevators.

Staff/vendor access to limited Resident Common Areas is also configured in **Access Management > Common Area Access**.

Staff common areas

Staff Common Areas are spaces on your property that are configured for access by staff/vendors, such as an office, kitchen area, and supply closets. When you create a Staff Common Area access point, you have the option to enable limited access.

Access to common areas always remains valid until key expiration. New keys cannot invalidate access to common areas. Cancel keys can only invalidate access to common areas when the key status is Active.

Unlimited staff common areas

When limited access *is not enabled*, the common area is included on all staff/vendor keys.

Limited-access staff common areas

When limited access is enabled, the following options are available:

- limit access based on credential—access must be configured in **Access Management > Credential Management**.
- limit access based on common area access profile—access must be configured in **Access Management > Common Area Access**.

When creating the limited common area, you must also select a common area ID. The ID is a numeric value used by the system to synchronize with third-party API (Application Programming Interface) settings.

When extended common areas is enabled, there are a maximum of 256 common area IDs to support common areas (resident and staff/vendor). Without extended common areas, the limit is 12 which includes IDs for limited common areas and elevators.

Elevators

Configuring elevators to control building floor access involves an elevator technician and Community Site Configurator. dormakaba provides the elevator control box and readers. The elevator technician is responsible for all device installation and wiring. The Site Configurator works in **Property Builder** to establish elevator access points.

The basic process for the Site Configurator is:

1. Add one or more elevator banks.
2. Add one or more elevators.
3. Map floor access (for each elevator bank).

Elevator banks

An elevator bank is a group of elevators that share the same floor mapping. The elevators must be in the same building, but they do not need to be co-located. The Site Configurator needs to obtain the control box model before adding an elevator bank because the model affects floor mapping.

Elevators

Elevators are added to an elevator bank. You provide a name for the elevator and a name for at least one reader. Readers are devices that interpret the floor access configuration data encoded on a key and communicate with the control box to allow access.

Although we refer to the elevator as the access point, it is actually the reader that controls access.

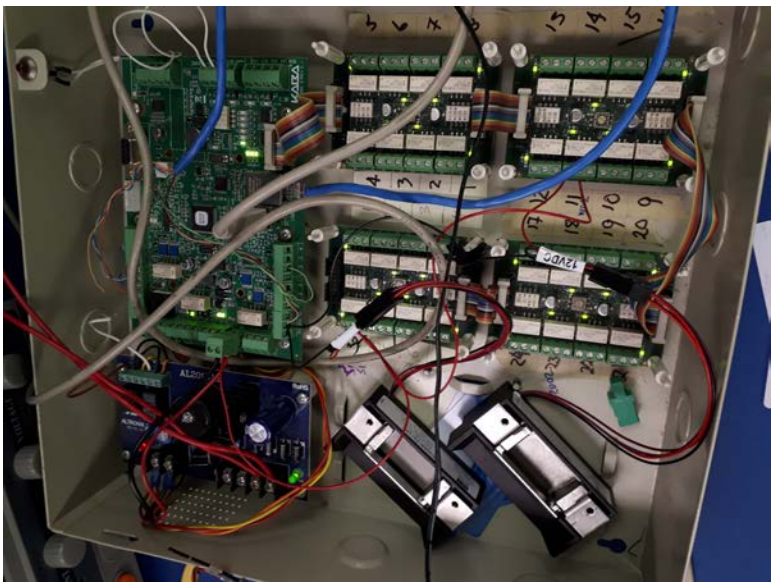
Floor mapping

The Site Configurator maps floor access for each elevator bank. While all floor mapping works the same, the control box model selected when adding the elevator bank affects the options available. Generally, as the number of floors that need to be independently controlled increases, the size of the control box increases.

A control box is a device that contains one or more electrical panels with one or more relay switches. Your site will use one of the following models:

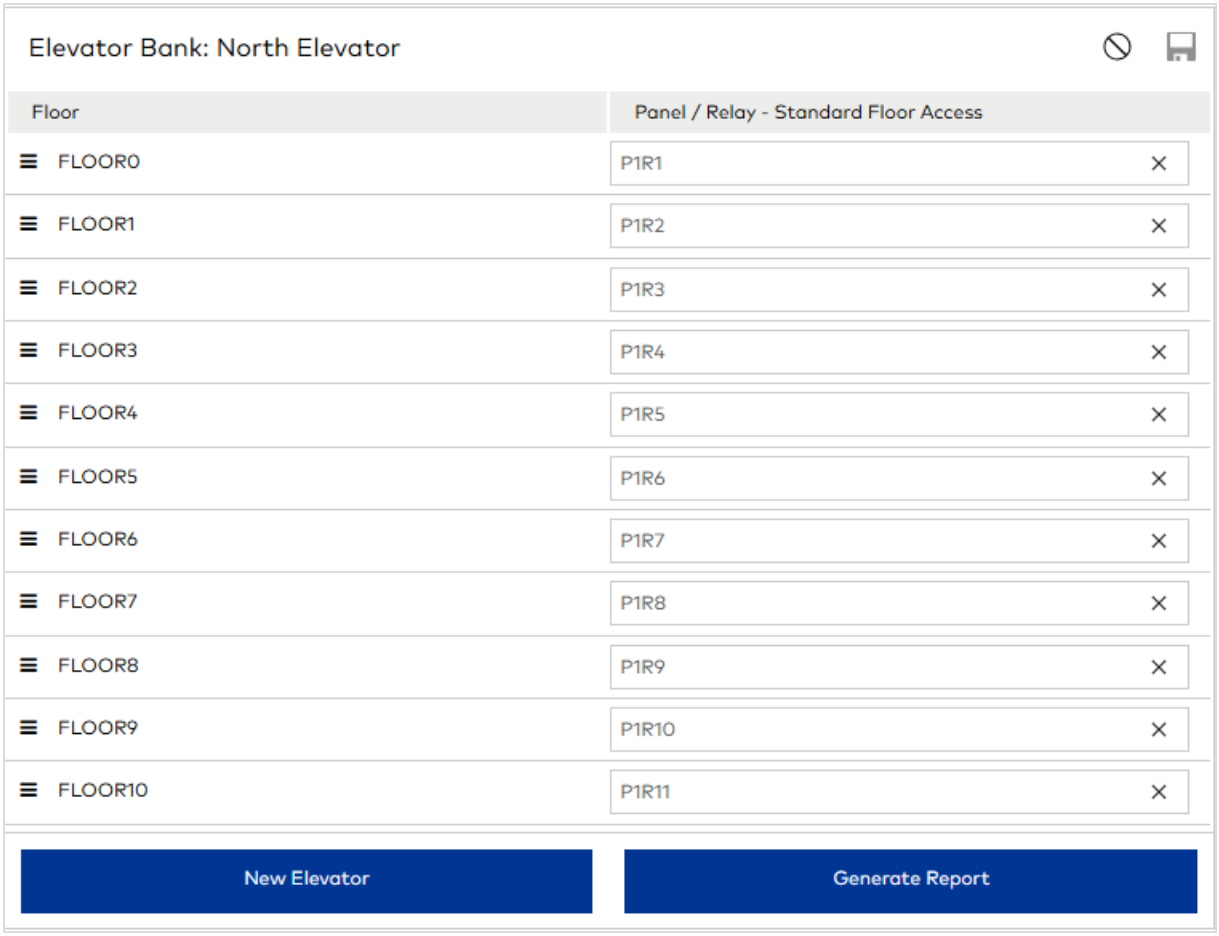
- **EMCC - Expanded Multi-Channel Controller**—Eight panels with 16 relays per panel.
- **MCC 12 - Multi-Channel Controller** (Legacy mode supported)—One panel with 12 relays.
- **MCC 8 - Multi-Channel Controller** (Legacy mode supported)—One panel with 8 relays.
- **ECU - Elevator Controller Unit**—One panel with one relay.
- **MFC - Multiple Floor Controller**—Four panels with eight relays per panel.
- **RAC 5 - Remote Access Controller**—(Non-MFC) Eight panels with eight relays per panel. For online environments, RAC5 gateways must be configured in **Device Management**.

The following figure shows the interior of an MFC control box with four panels, eight relays each.



The relays on three of the panels are labeled 1-24. When mapping floor access in Community, relay switches are mapped to floors.

The following figure shows Community floor mapping. Floors 1-3 are mapped to Relay1 (P1R1). All other floors are mapped to a separate relay.



When a Key Holder presents a key to the reader, the reader detects the access configuration encoded on the key, communicates to the control box which relays to open, and illuminates the buttons on the elevator panel that the Key Holder is authorized to access. In some cases, a reader is outside of the elevator to control access to the **Up** and **Down** call buttons.

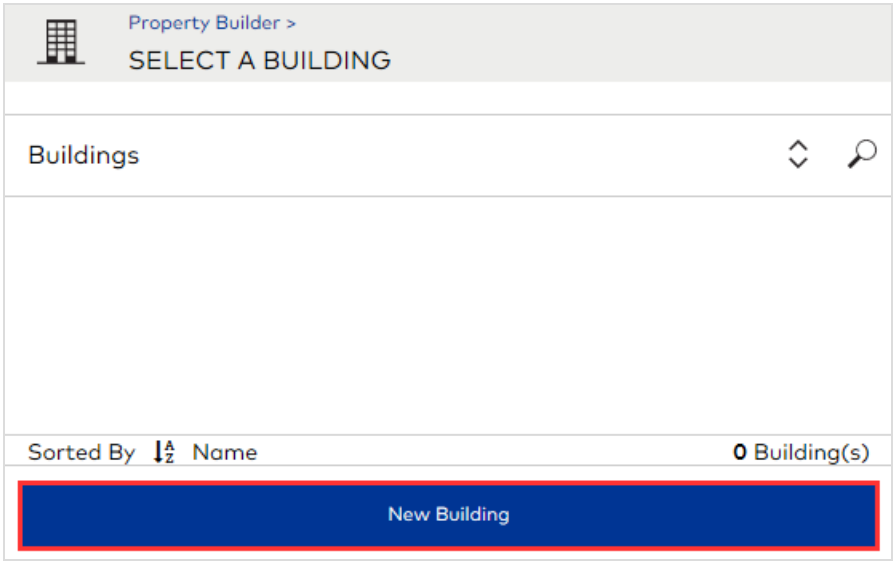
Aside from the basic rule, *a floor can be mapped to only one relay*, relay-to-floor mapping is entirely configurable. The important thing to remember is that a signal from the reader to open the relay opens access to all floors mapped to the relay. For example, if Floors1-3 are mapped to Relay1 and the floor access encoded on a key is authorized for Floor1 only, the Key Holder will be able to access Floors1-3. Therefore, for maximum control the recommendation is to map one floor to one relay. A reason why you might want to map more than one floor to a relay is if access to two or more floors is always authorized together.

Add buildings

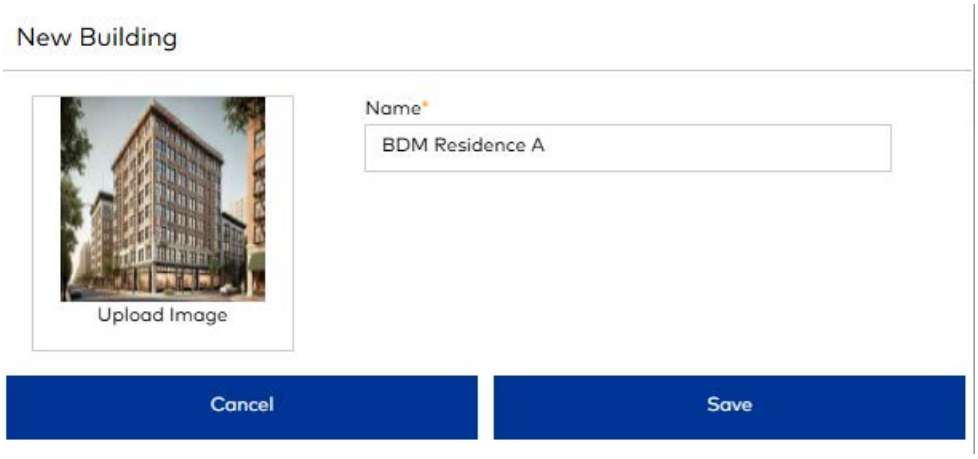
Buildings are the independent structures on your site.

To add buildings:

1. Go to **Property Builder**.



2. Click **New Building**.



3. Specify a unique name.
4. (*optional*) Select an image to represent your site. Click **Upload image**, navigate to and select an image then click **Open**. Supported file types: gif, jpg, png.
5. Click **Save**. The building displays in the list.

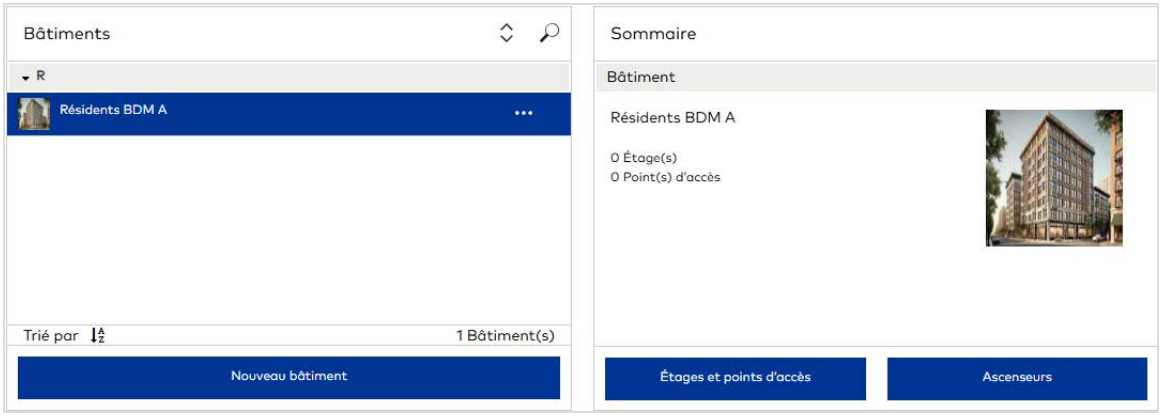


Add floors

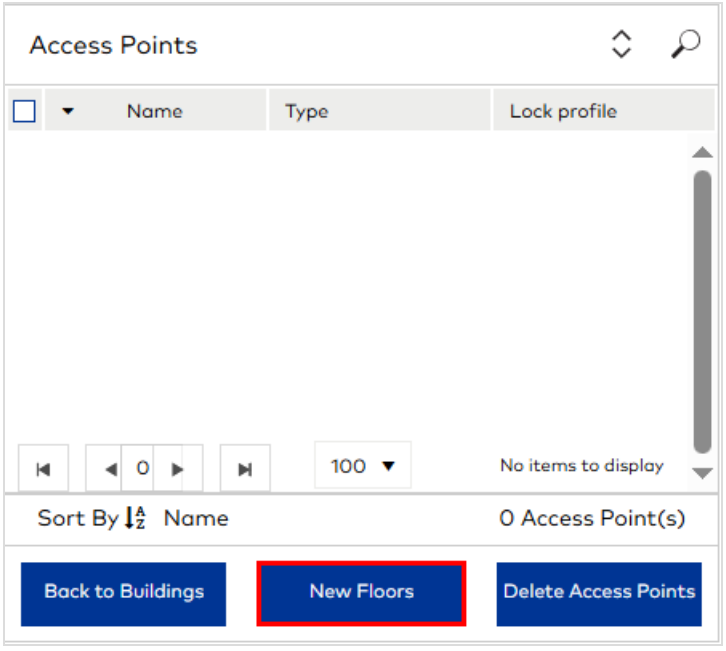
Floors are the levels in a building. You must add floors before adding access points.

To add floors:

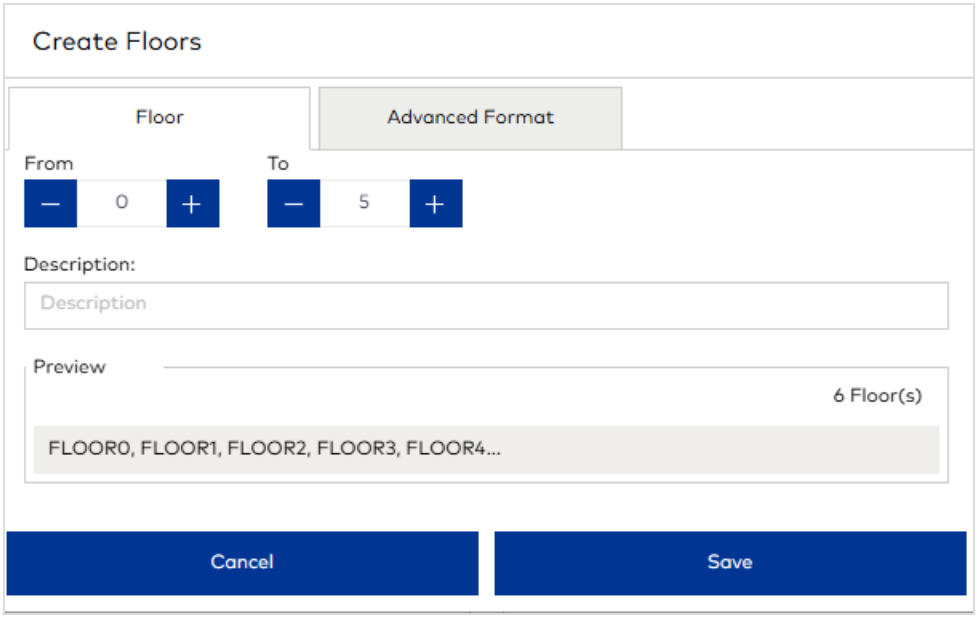
1. Go to **Property Builder**.
2. Select a building.



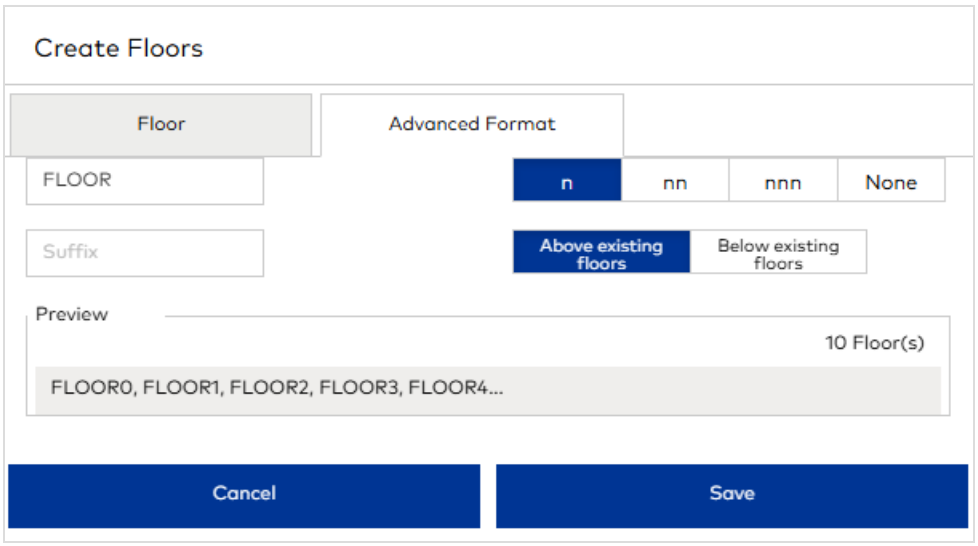
3. Click **Floors & Access Points**.



4. Click **New Floors**.

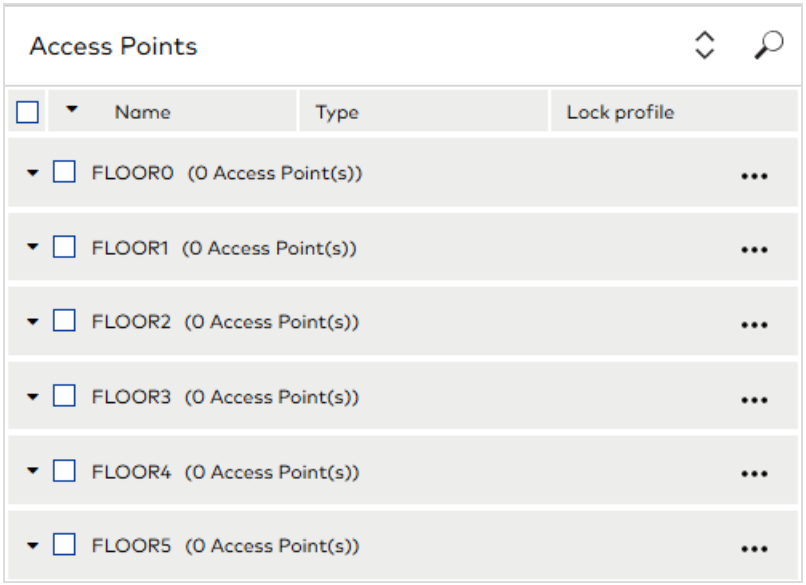


5. Specify the range of floors to add. Because floor names must be unique, you can only select numbers that have been used previously if you also specify a unique prefix or suffix.
6. (*optional*) Add a description for the floor or range of floors.
7. (*optional*) Specify any of the following options on the **Advanced Format** tab:



- **Prefix**—Specify text to display before the floor number. Include spaces where appropriate. Default: FLOOR.
- **Suffix**—Specify text to display after the floor number or access point. Include spaces where appropriate. Default: none.
- **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for FLOOR 1, **nn** for FLOOR 01, **nnn** for FLOOR 001. To hide the floor number in the name, select **None**. Default: n.
- **Add floors(s)**—Select whether to add the floors to the list before or after existing floors. Default: Above existing floor(s).

8. Click **Save**.


Access Points
Name
Type
Lock profile
FLOOR0 (0 Access Point(s))
FLOOR1 (0 Access Point(s))
FLOOR2 (0 Access Point(s))
FLOOR3 (0 Access Point(s))
FLOOR4 (0 Access Point(s))
FLOOR5 (0 Access Point(s))

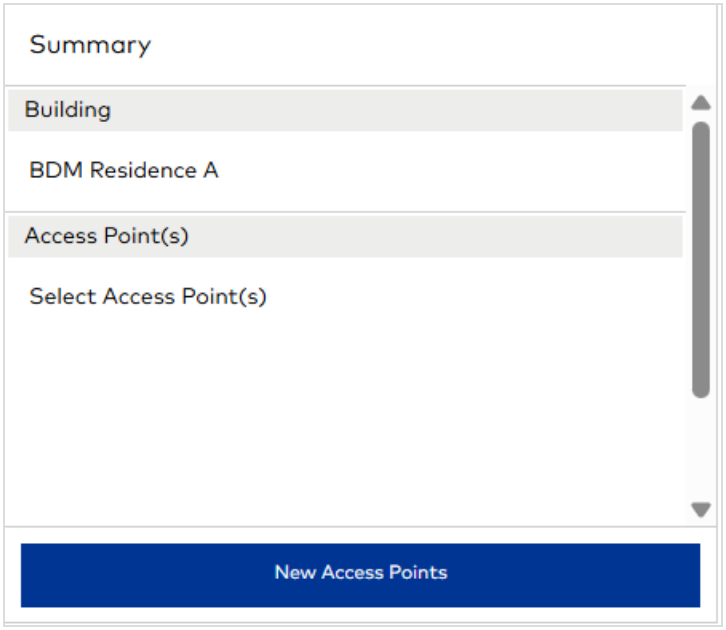
Add units

Units are the type of access points assigned to residents during unit assignment.

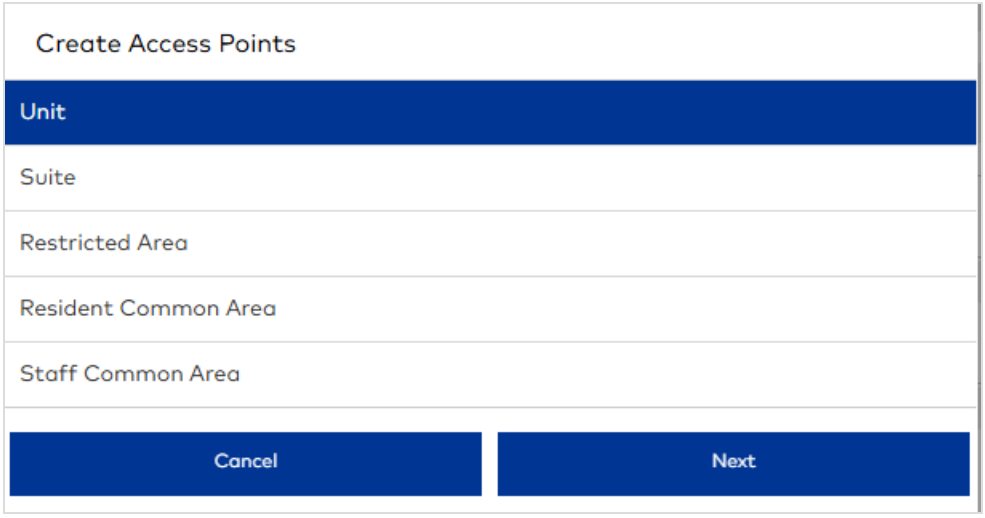
To import unit and suite access point types, see Import units and suites list.

To add units:

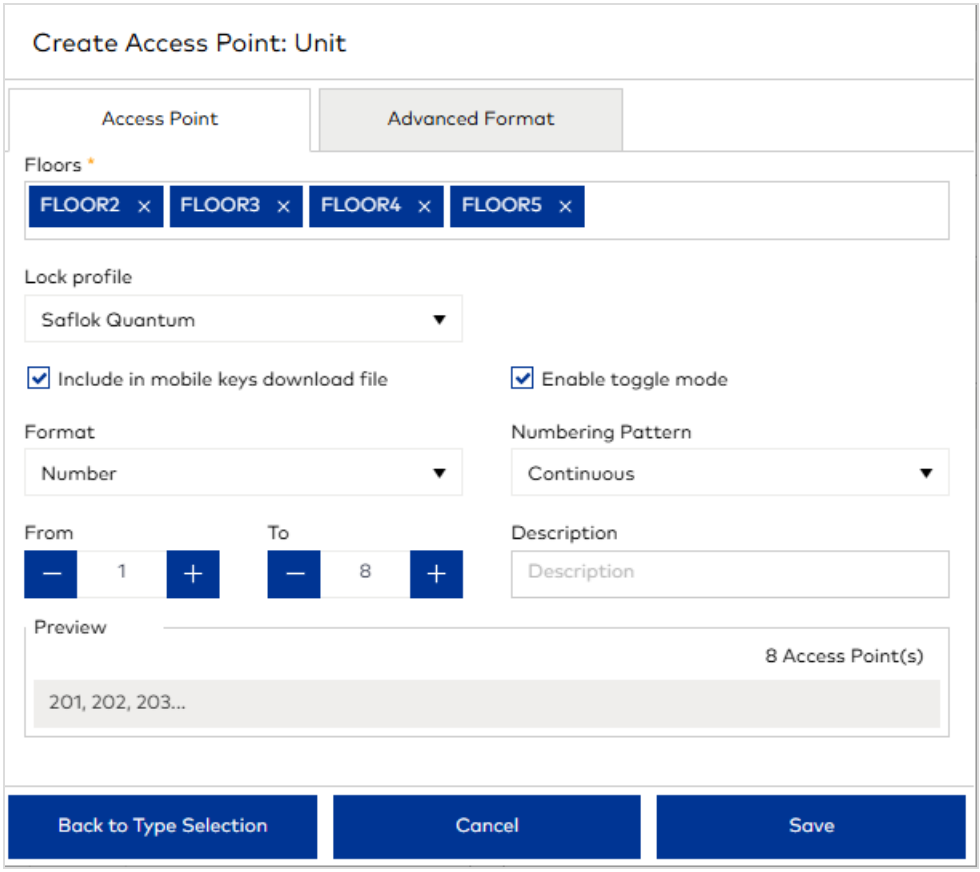
1. Go to **Property Builder**.
2. Select a building.
3. Click **Floors & Access Points**.



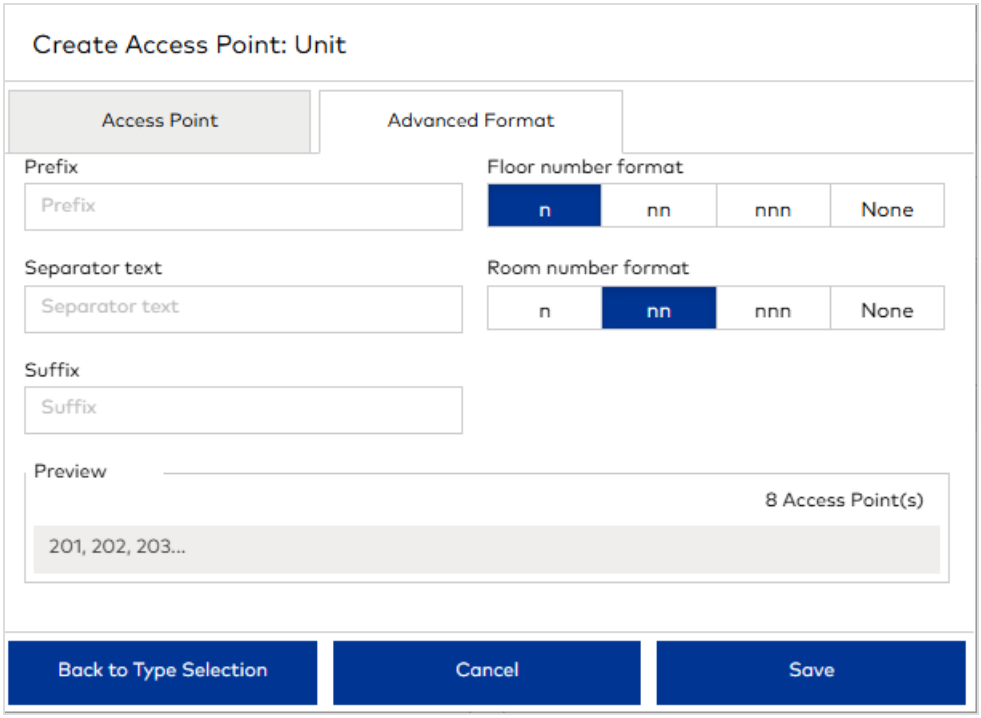
4. Click **New Access Points**.



5. Select **Unit**, then click **Next**.

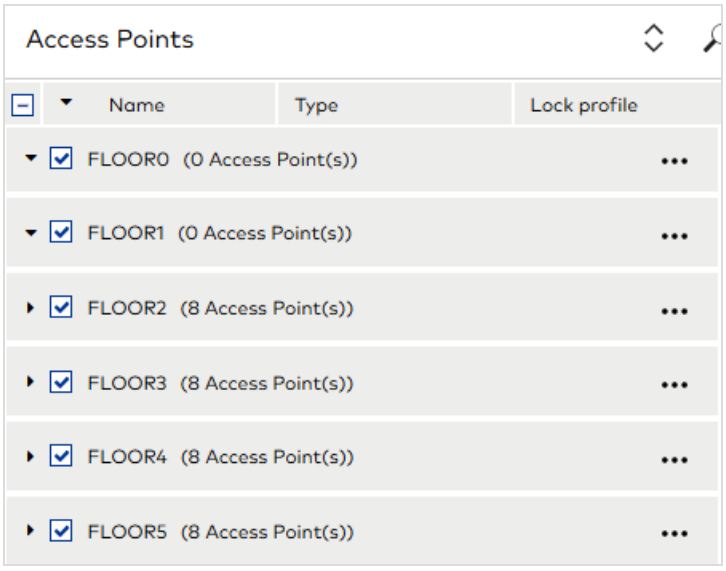


6. For **Floors**, select one or more floors where you want to add the access points.
7. For **Lock profile**, select the lock model. All Nova locks include the toggle feature. For all other lock types that support toggle, the **Enable toggle mode** option is displayed. Each time a valid key is presented to a lock that includes or is enabled for toggle mode, the state of the lock alternates between *Latched* and *Unlatched*. For example, Unit 100 is programmed using a Nova lock profile. The lock is in a *Latched* (secure) state. The first time the resident presents a key, the lock changes to an *Unlatched* state. The door is open and remains accessible until the key is presented to the lock again or the interior privacy switch is engaged. When this option is not selected, locks remain in a Latched state except for the brief time when a valid key is presented allowing access.
8. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
9. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
10. For **Format**, select whether to identify the access points using numbers or text.
    - If you select **Number**, specify the range of access points to add and, if adding more than one access point, select a numbering pattern for incrementing the numbers.
    - If you select **Text**, specify a unique access point name.
11. (*optional*) Add a description for the access point or range of access points.
12. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the **Advanced Format** tab:



- **Prefix**—Specify the text to display before the main number. Include spaces where appropriate.
- **Separator text**—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
- **Suffix**—Specify the text to display after the main number. Include spaces where appropriate.
- **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the floor number in the access point name, select **None**.
- **Unit number format**—Select how many digit positions to display for unit numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the unit number in the access point name, select **None**.

13. Click **Save**.



14. When prompted, select a lock profile for the access points.
15. When notified the import is successful, click **OK**. The following figure shows the import of access points using the .csv created in Notepad.

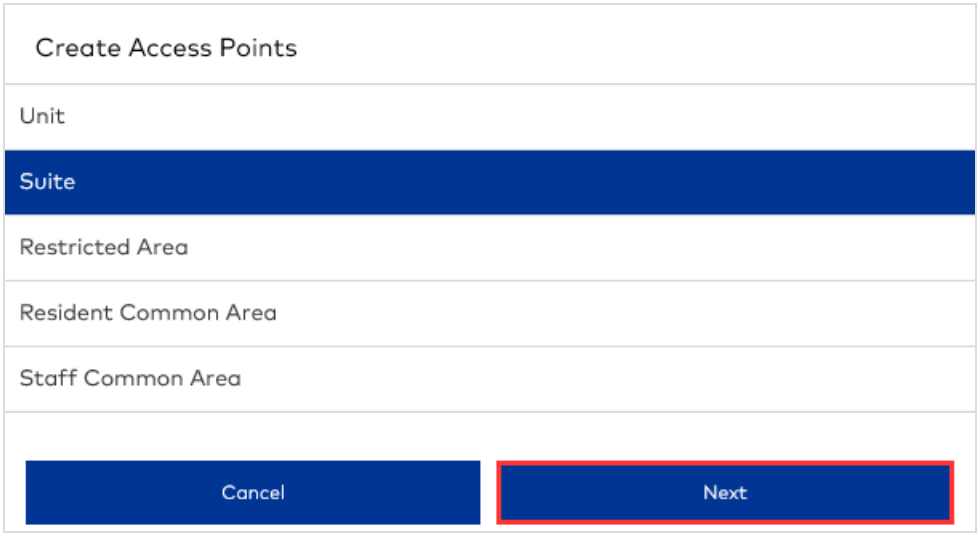
Add suites

A suite is a connected series of units that includes a common door and one or more suite units.

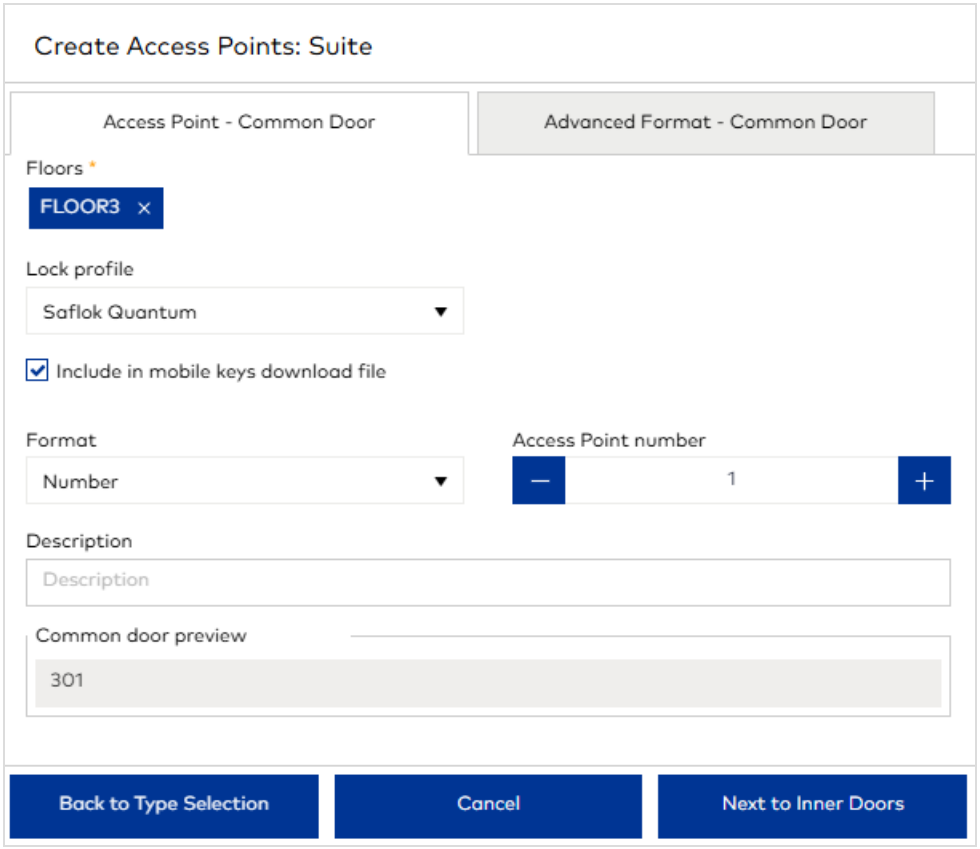
To import unit and suite access point types, see Import units and suites list.

To add suites:

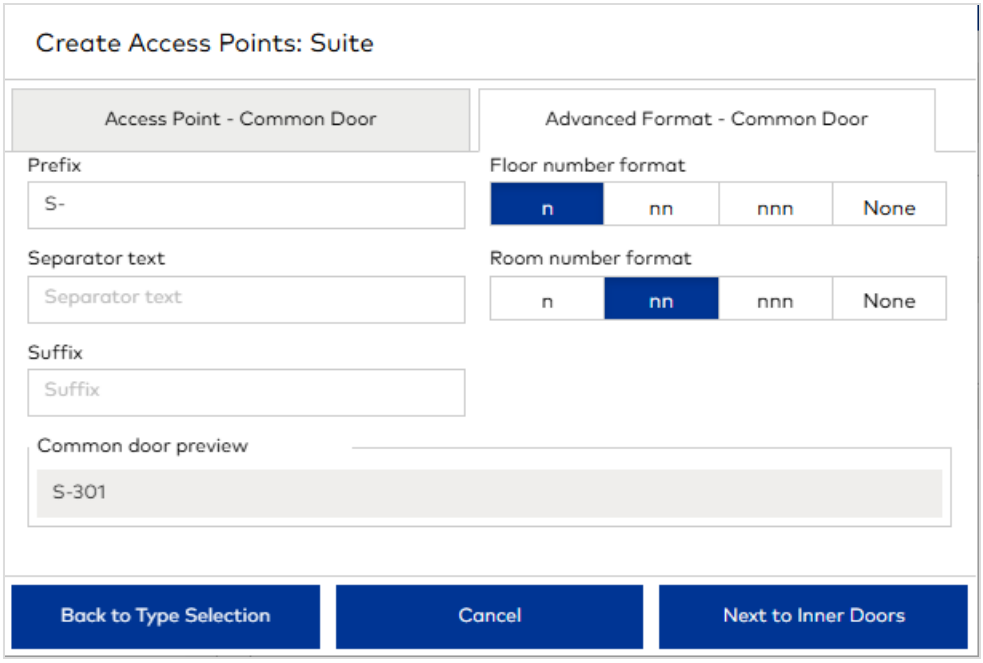
1. Go to **Property Builder**.
2. Select a building.
3. Click **Floors & Access Points**.
4. Click **New Access Points**.



5. Select **Suite**, then click **Next**. The first options that you define are for the Common Door.

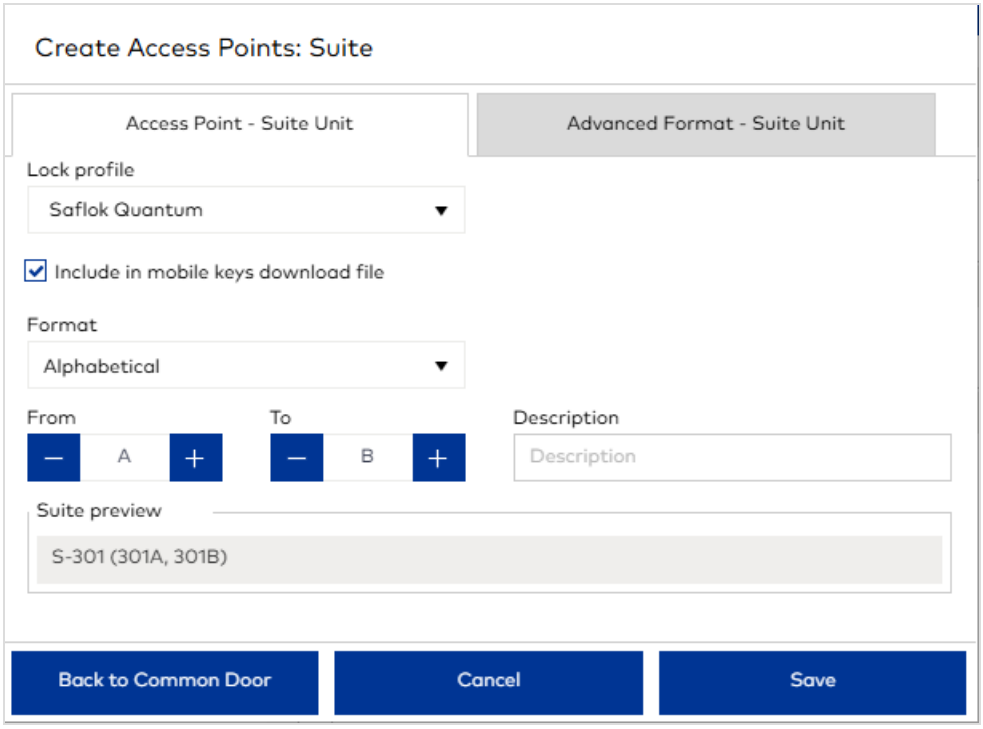


6. For **Floors**, select the floor where you want to add the access points.
7. For **Lock profile**, select the lock model. If the selected lock model does not include the built-in toggle feature but allows the feature to be added programmatically, the option **Enable toggle mode** displays. If you want the key behavior to alternate from lock to unlock each time the key is presented, select **Enable toggle mode**. When this option is deselected, the key only unlocks.
8. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
9. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
10. For **Format**, select whether to identify the access points using numbers or text.
    - If you select **Number**, specify a number for the Common Door.
    - If you select **Text**, specify a unique access point name.
11. (*optional*) Add a description for the access point or range of access points.
12. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the **Advanced Format** tab:

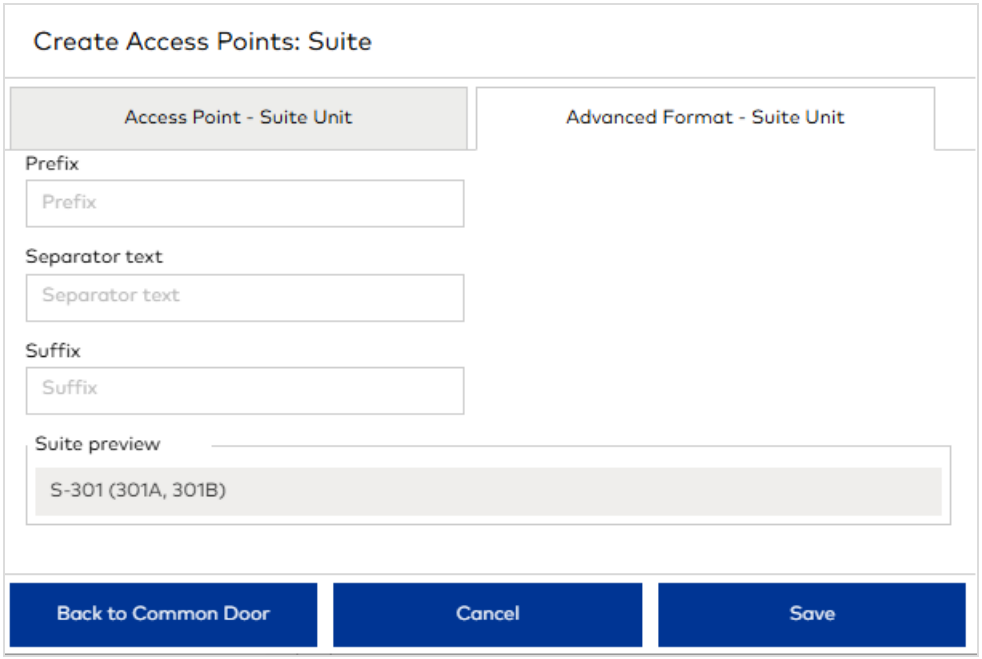


- **Prefix**—Specify the text to display before the main number. Include spaces where appropriate.
- **Separator text**—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
- **Suffix**—Specify the text to display after the main number. Include spaces where appropriate.
- **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the floor number in the access point name, select **None**.
- **Unit number format**—Select how many digit positions to display for unit numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the unit number in the access point name, select **None**.

13. Click **Next to Inner Doors**.

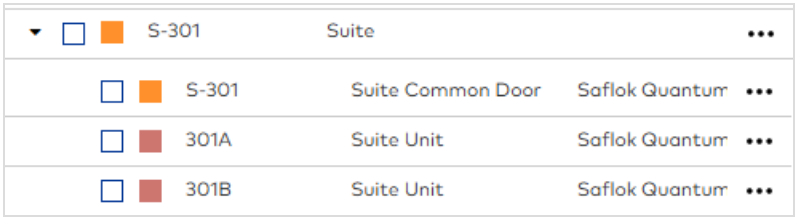


14. For **Lock profile**, select the lock model. If the selected lock model does not include toggle mode, an additional option to enable/disable toggle mode is displayed. If you want the key behavior to alternate from lock to unlock each time the key is presented, select the **Enable toggle mode**. When this option is deselected, the key only unlocks.
15. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
16. For **Format**, select whether to identify the access points using alphabetic characters, numbers, or text. If using letters or numbers, specify the range of access points to add; and, if adding more than one access point, select a numbering pattern for incrementing numbers.
17. (*optional*) Add a description for the access point or range of access points.
18. (*optional*) If you selected to format access point names using alphabetic characters or numbers, specify any of the following options on the **Advanced Format** tab:



- **Prefix**—Specify the text to display before the main number. Include spaces where appropriate.
- **Separator text**—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
- **Suffix**—Specify the text to display after the main number. Include spaces where appropriate.
- **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the floor number in the access point name, select **None**.
- **Unit number format**—Select how many digit positions to display for unit numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the unit number in the access point name, select **None**.

19. Click **Save**.



Import units and suites list

Unit and suite access point types can be added to Community by batch import. This menu option is only available when the *Import access point list* system right is enabled in **Role Management > Property Builder**.

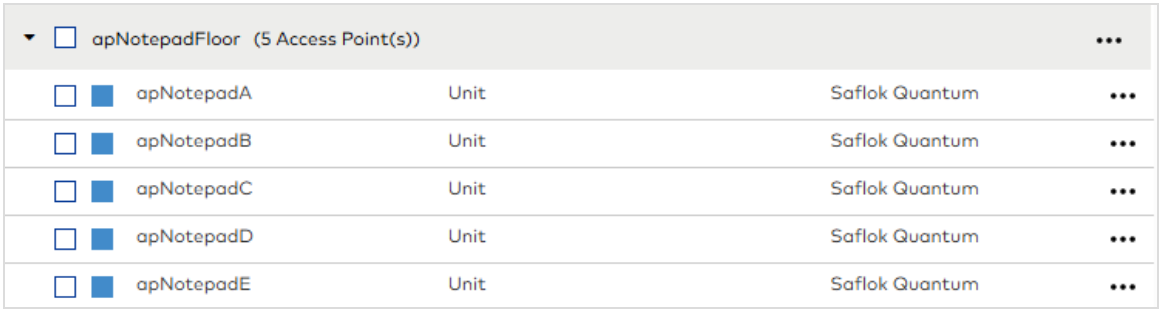
Use the provided import template to ensure format requirements. Download the template from the Context Help / Property Builder home page.

To import unit and suite access points:

1. Prepare the import file.
2. Go to **Property Builder**.
3. For the building where you want to add units, click and select **(More) ▪▪▪ Import Access Point List**.
4. Navigate to and select the file that you want to import, then click **Open**. The following rules apply:
   - The file type must be .csv (.csv UTF-8 for non-English languages).
   - ACCESSPOINT and FLOORNAME are required.
   - If the floor name in the csv file is an exact match to an existing floor name, the access point is added to the existing floor.

If units have already been created, you are prompted to proceed. Click **YES** to proceed.

5. When notified the import is successful, click **OK**. The following figure shows the import of access points using the .csv created in Notepad.



Add resident common areas

Resident Common Areas are spaces on your property that are configured for general access by residents and staff, such as lobbies, parking and recreational facilities. When you create a common area, you have the option to limit access.

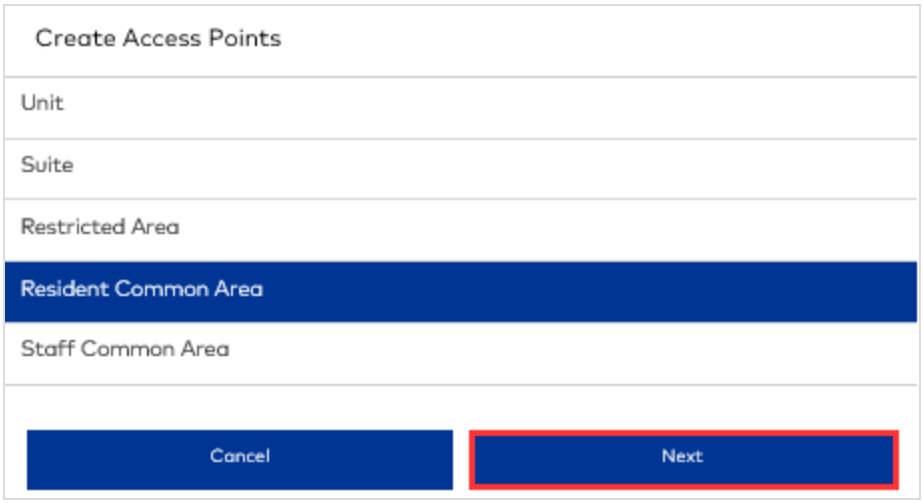
To learn more about common areas and how limited access affects the configuration, see Resident common areas in "Learning about Property Builder."

This topic provides instructions for adding the following types of common area access points:

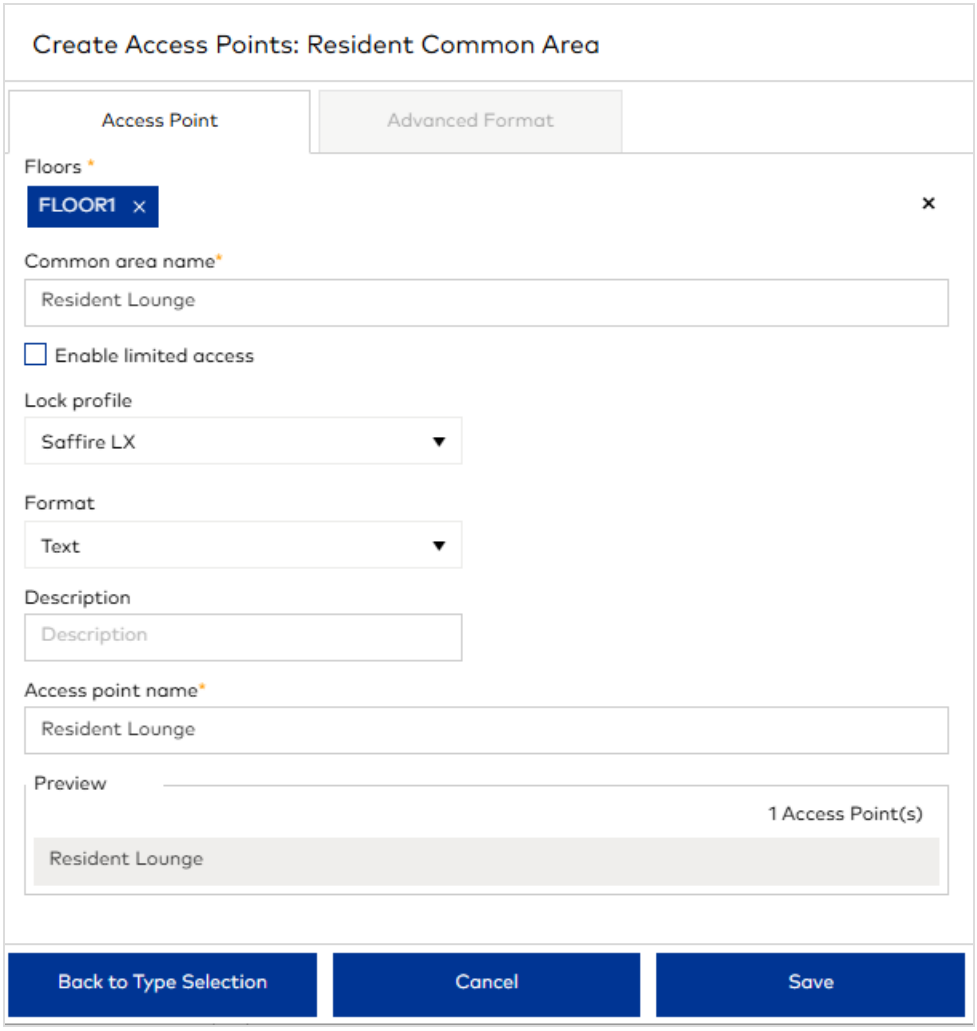
- Adding Unlimited Resident Common Areas
- Adding Limited-Access Resident Common Areas
- Adding Common Areas to Common Area Groups

Adding unlimited resident common areas

1. Go to **Property Builder**.
2. Select a building.
3. Click **Floors & Access Points**.
4. Click **New Access Points**.



5. Select **Resident Common Area**, then click **Next**.



6. For **Floors**, select the floor where you want to add the access point.
7. For **Common area name**, specify a unique name that does not exceed 20 characters. This is the name of the common area group. You can add additional common areas to the group.

   When limited access is not enabled, this common area and related access points can be implicitly accessed by all resident keys.

8. For **Lock profile**, select the lock model.

   Toggle mode is only supported for units and suite units.

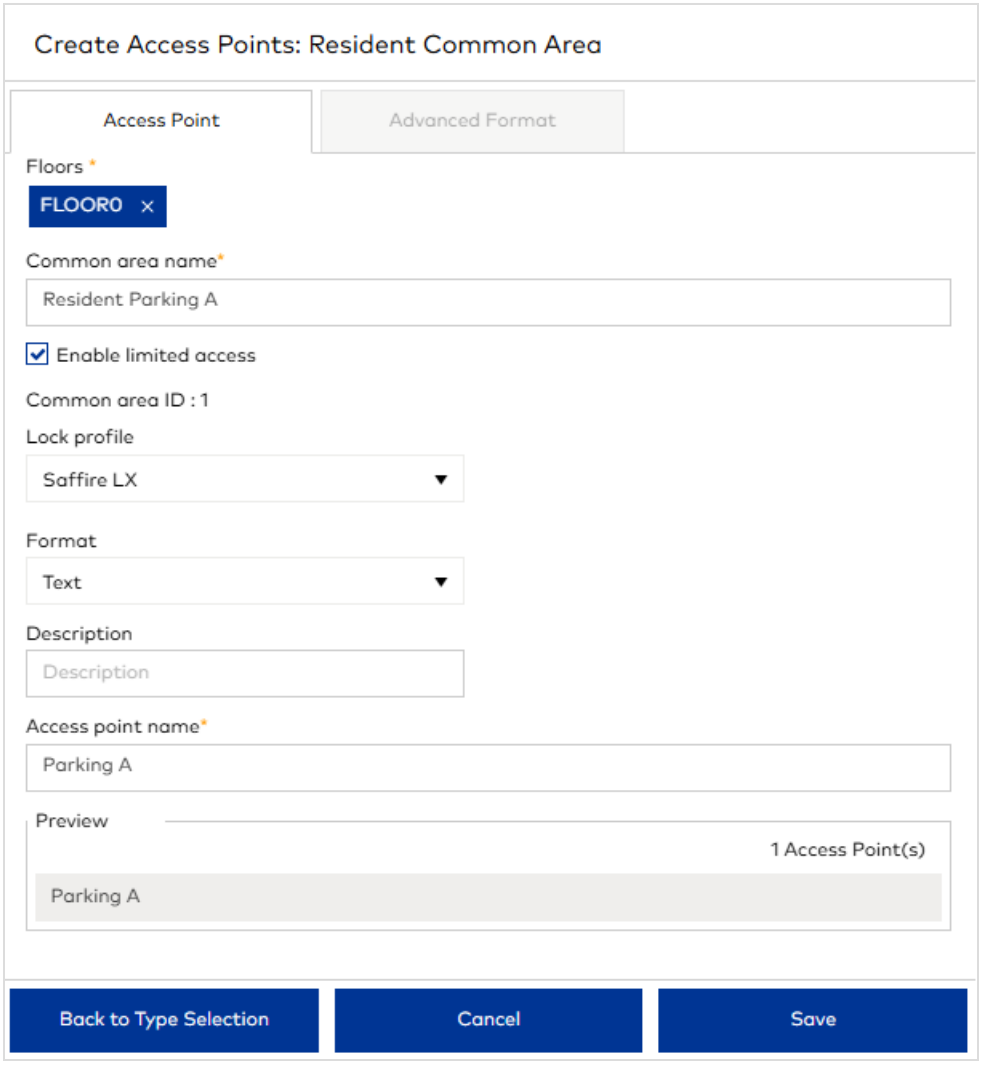
9. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
10. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
11. For **Format**, select whether to identify the access points using numbers or text.
    - If you select **Number**, specify the range of access points to add and, if adding more than one access point, select a numbering pattern for incrementing the numbers.
    - If you select **Text**, specify a unique access point name.

12. (*optional*) Add a description for the access point or range of access points.
13. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the **Advanced Format** tab:
    - **Prefix**—Specify the text to display before the main number. Include spaces where appropriate.
    - **Separator text**—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
    - **Suffix**—Specify the text to display after the main number. Include spaces where appropriate.
    - **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the floor number in the access point name, select **None**.
    - **Unit number format**—Select how many digit positions to display for unit numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the unit number in the access point name, select **None**.
14. Click **Save**.



Adding limited-access resident common areas

1. Go to **Property Builder**.
2. Select a building.
3. Click **Floors & Access Points**.
4. Click **New Access Points**.
5. Select **Resident Common Area**, then click **Next**.



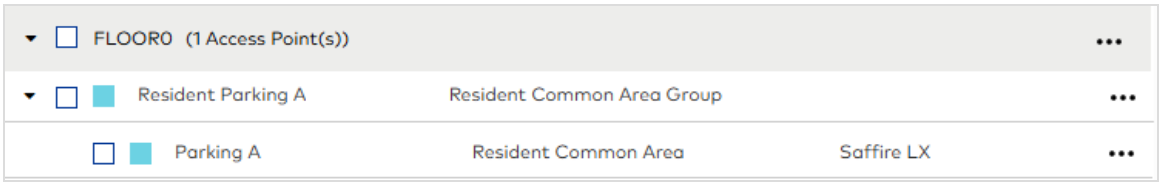
6. For **Floors**, select the floor where you want to add the access point.
7. For **Common area name**, specify a unique name that does not exceed 20 characters. This is the name of the common area group. You can add additional common areas to the group.
8. Select the **Enable limited access** option. The common area must be associated with a profile in **Access Management > Common Area Access**.
9. For **Common area ID**, accept the value that the system automatically populates.
10. For **Lock profile**, select the lock model.

    Toggle mode is only supported for units and suite units.

11. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
12. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
13. For **Format**, select whether to identify the access points using numbers or text.
    - If you select **Number**, specify the range of access points to add and, if adding more than one access point, select a numbering pattern for incrementing the numbers.

- If you select **Text**, specify a unique access point name.

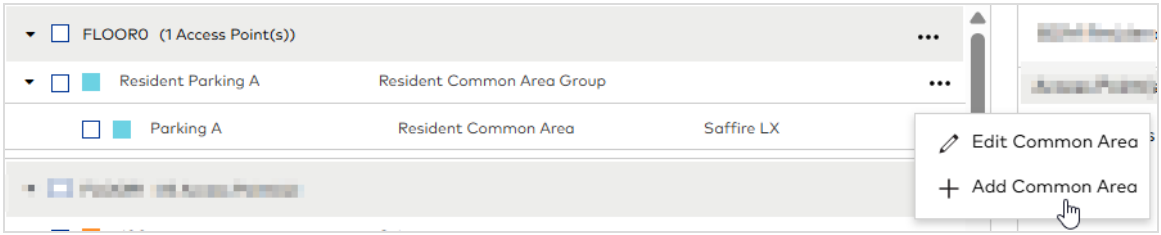
14. (*optional*) Add a description for the access point or range of access points.
15. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the **Advanced Format** tab:
    - **Prefix**—Specify the text to display before the main number. Include spaces where appropriate.
    - **Separator text**—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
    - **Suffix**—Specify the text to display after the main number. Include spaces where appropriate.
    - **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the floor number in the access point name, select **None**.
    - **Unit number format**—Select how many digit positions to display for unit numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the unit number in the access point name, select **None**.
16. Click **Save**.



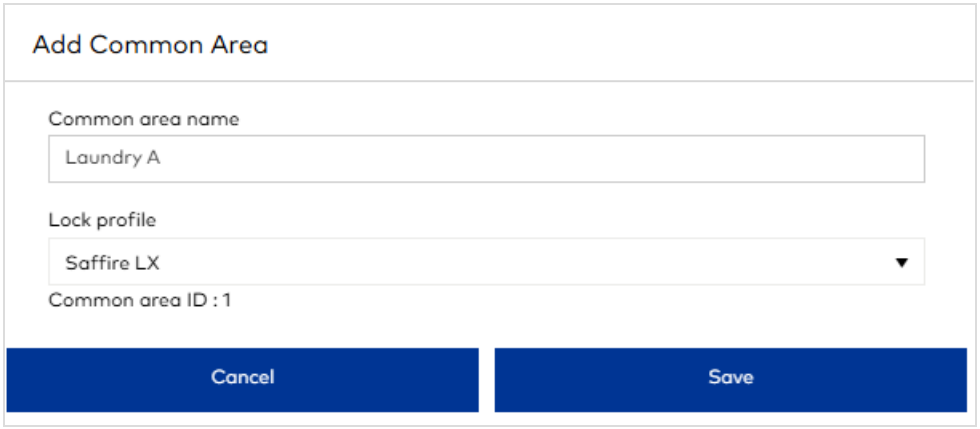
Adding common areas to common area groups

While you can add multiple common areas to the same group, access is enabled at the group level. To add a common area to a common area group:

1. Go to **Property Builder**.
2. Select the common area group where you want to add the common area.



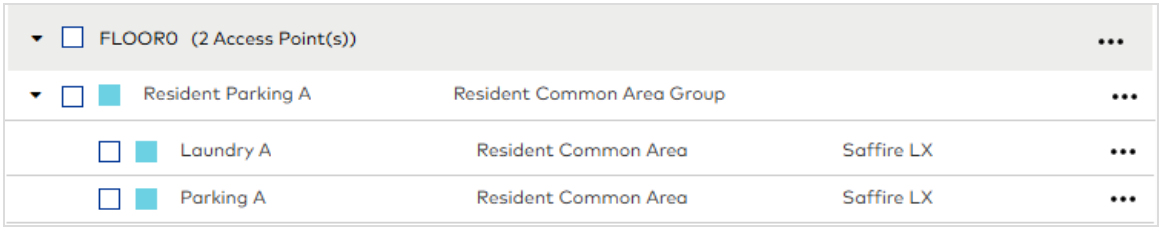
3. Click **(More)** ··· **> Add Common Area**.



4. Specify a unique name for the common area.
5. For **Lock profile**, select the lock model.

   Toggle mode is only supported for units and suite units.

6. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
7. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
8. Click **Save**.



Add staff common areas

Staff Common Areas are the type of access points that are configured for general access by staff, such as break rooms and supply closets. When you create a common area, you have the option to limit access.

To learn more about staff common areas and how limited access affects the configuration, see "Unlimited and Limited-Access Staff Common Areas."

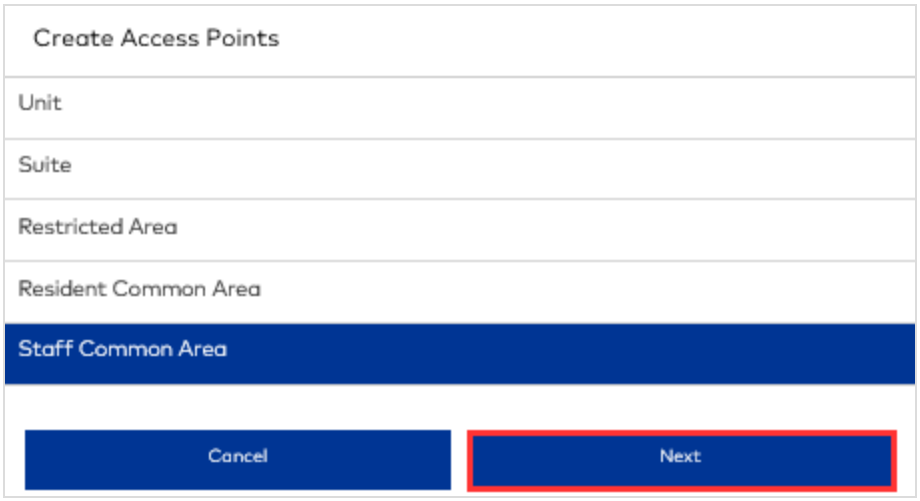
This topic provides instructions for adding the following types of common area access points:

- Adding Unlimited Staff Common Areas
- Adding Limited-Access Staff Common Areas
- Adding Common Areas to Common Area Groups

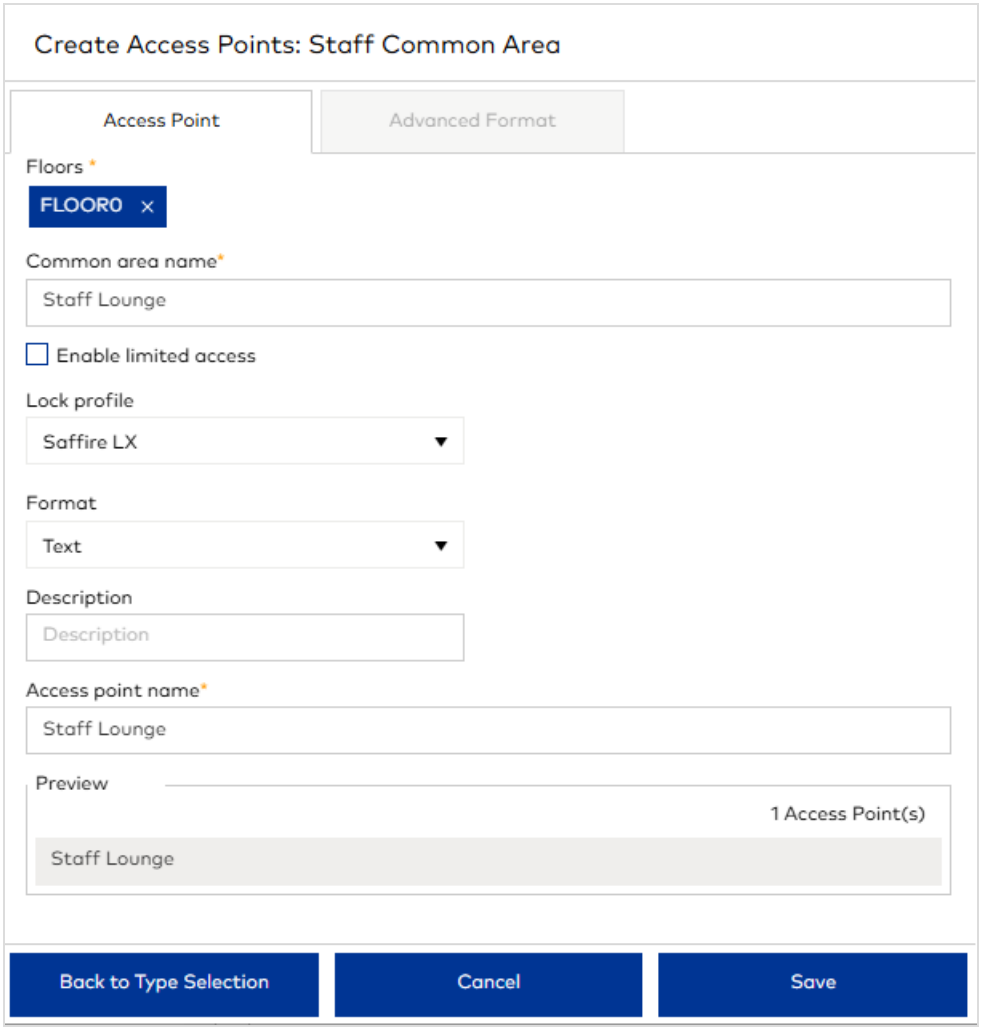
Adding unlimited staff common areas

Unlimited staff common areas are added to every staff/vendor key.

1. Go to **Property Builder**.
2. Select a building.
3. Click **Floors & Access Points**.
4. Click **New Access Points**.



5. Select **Staff Common Area**, then click **Next**.



6. For **Floors**, select the floor where you want to add the access point.
7. For **Common area name**, specify a unique name that does not exceed 20 characters. This is the name of the common area group. You can add additional common areas to the group.
8. For **Lock profile**, select the lock model.

   Toggle mode is only supported for units and suite units.

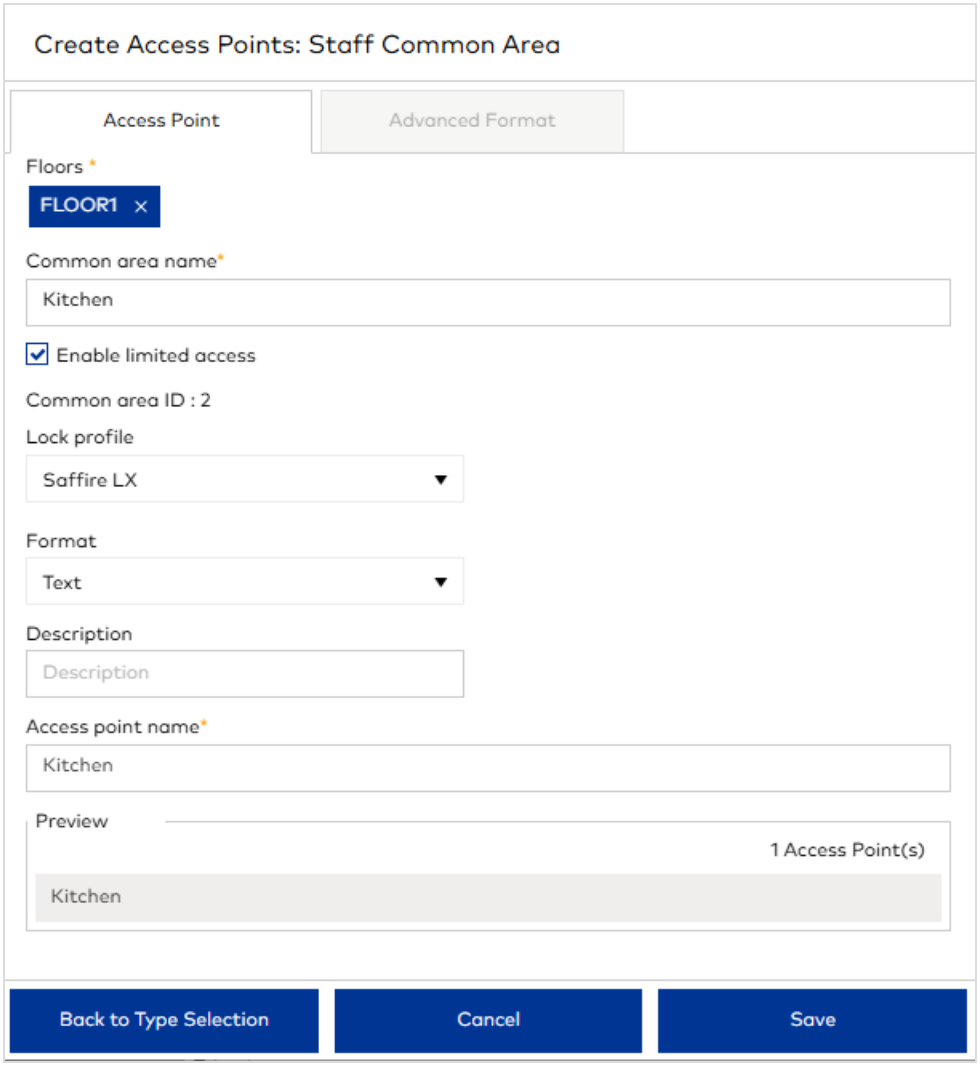
9. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
10. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
11. For **Format**, select whether to identify the access points using numbers or text.
    - If you select **Number**, specify the range of access points to add and, if adding more than one access point, select a numbering pattern for incrementing the numbers.
    - If you select **Text**, specify a unique access point name.

12. (*optional*) Add a description for the access point or range of access points.
13. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the **Advanced Format** tab:
    - **Prefix**—Specify the text to display before the main number. Include spaces where appropriate.
    - **Separator text**—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
    - **Suffix**—Specify the text to display after the main number. Include spaces where appropriate.
    - **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the floor number in the access point name, select **None**.
    - **Unit number format**—Select how many digit positions to display for unit numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the unit number in the access point name, select **None**.
14. Click **Save**.



Adding limited-access staff common areas

1. Go to **Property Builder**.
2. Select a building.
3. Click **Floors & Access Points**.
4. Click **New Access Points**.
5. Select **Staff Common Area**, then click **Next**.



6. For **Floors**, select the floor where you want to add the access point.
7. For **Common area name**, specify a unique name that does not exceed 20 characters. This is the name of the common area group. You can add additional common areas to the group.
8. Select the **Enable limited access** option.
9. For **Lock profile**, select the lock model.

   Toggle mode is only supported for units and suite units.

10. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
11. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
12. For **Format**, select whether to identify the access points using numbers or text.
    - If you select **Number**, specify the range of access points to add and, if adding more than one access point, select a numbering pattern for incrementing the numbers.
    - If you select **Text**, specify a unique access point name.
13. (*optional*) Add a description for the access point or range of access points.

14. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the **Advanced Format** tab:
    - **Prefix**—Specify the text to display before the main number. Include spaces where appropriate.
    - **Separator text**—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
    - **Suffix**—Specify the text to display after the main number. Include spaces where appropriate.
    - **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the floor number in the access point name, select **None**.
    - **Unit number format**—Select how many digit positions to display for unit numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the unit number in the access point name, select **None**.
15. Click **Save**.



Before staff can be issued a key that authorizes access to limited-access staff common areas, you must either add the common area to the assigned staff credential or associate the common area with the assigned staff credential in **Access Management > Common Area Access**.

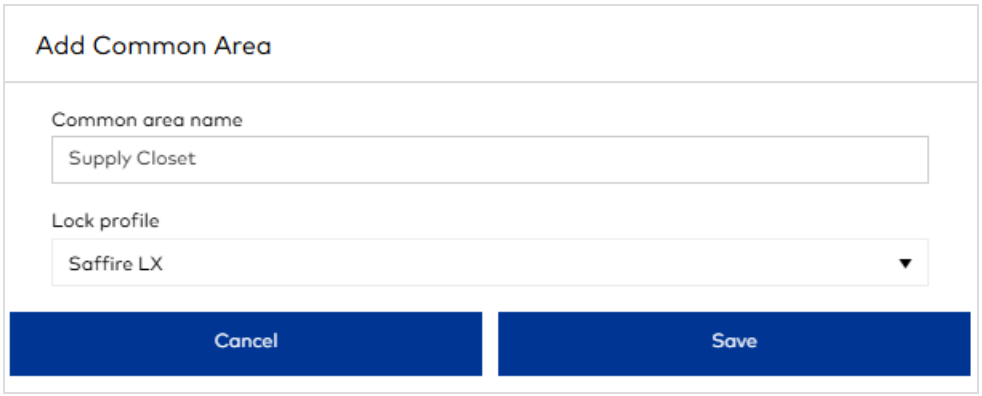
Adding common areas to common area groups

While you can add multiple common areas to the same group, access is enabled at the group level. To add a common area to a common area group:

1. Go to **Property Builder**.
2. Select the common area group where you want to add the common area.



3. Click **(More)** ··· **> Add Common Area**.



4. Specify a unique name for the common area.
5. For **Lock profile**, select the lock model.

Toggle mode is only supported for units and suite units.

6. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
7. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
8. Click **Save**.

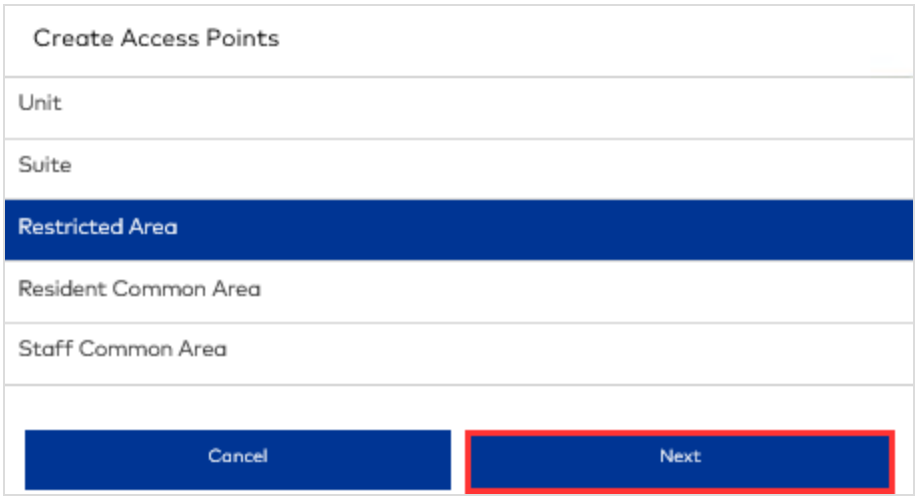


Add restricted areas

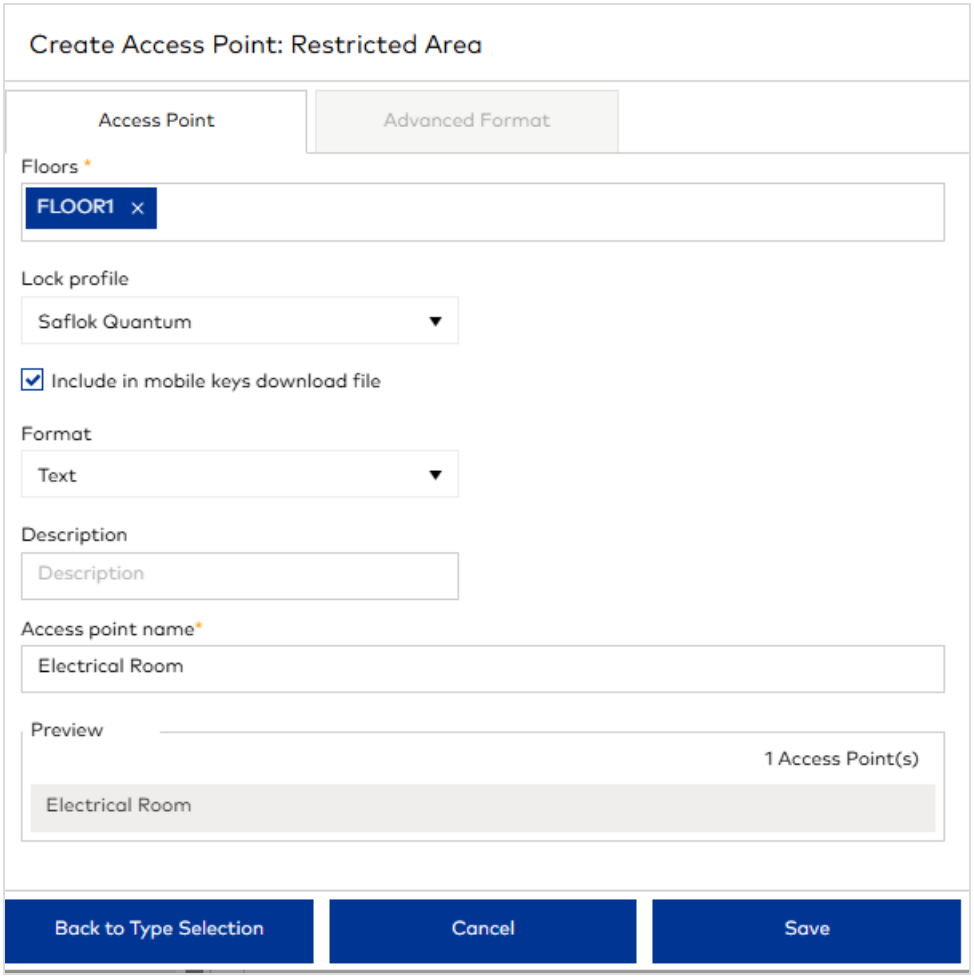
A restricted area is an access point type intended to provide back-of-the-house access for staff only.

To add restricted areas:

1. Go to **Property Builder**.
2. Select a building.
3. Click **Floors & Access Points**.
4. Click **New Access Points**.



5. Select **Restricted Area**, then click **Next**.



6. For **Floors**, select one or more floors where you want to add the access points.
7. For **Lock profile**, select the lock model.

> Toggle mode is only supported for units and suite units.



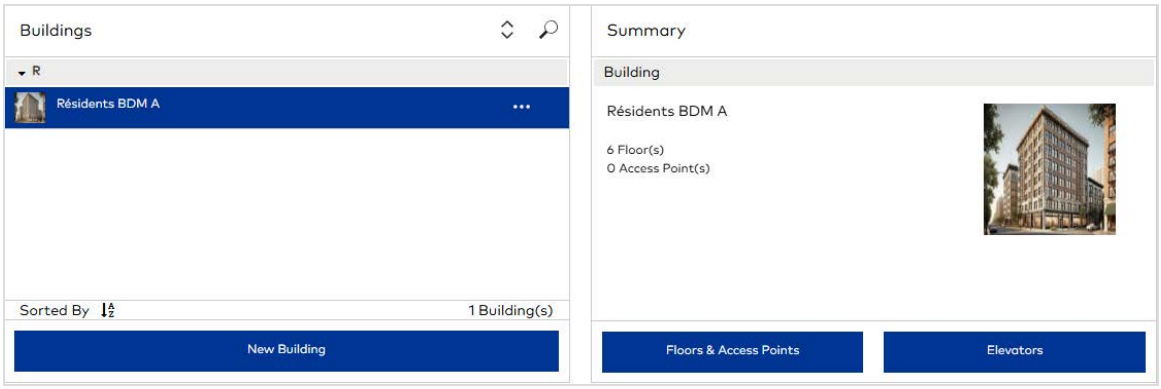
Add elevators

The process for configuring elevator access involves adding at least one elevator bank, adding the elevators for each bank, then mapping elevator panel relays to floors for each elevator bank. To learn more about elevators, see "Elevators" in *Learning about Property Builder*.

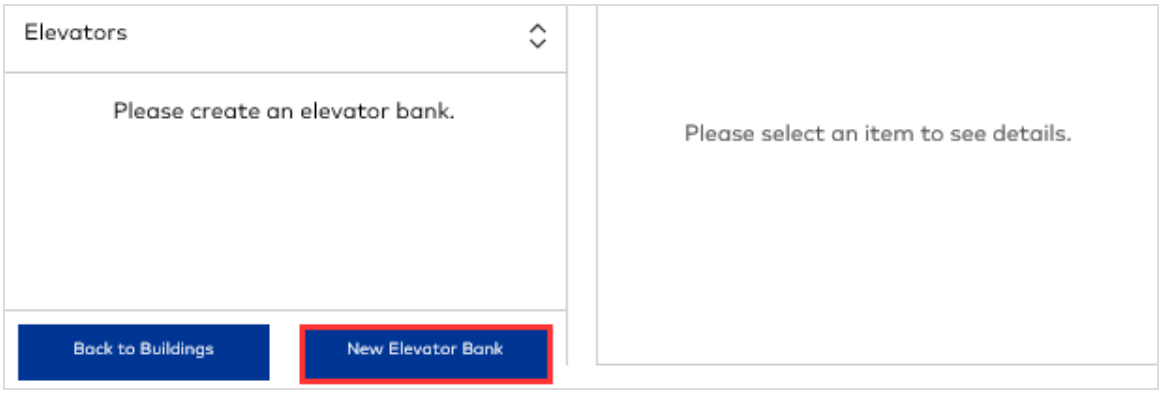
Add elevator banks

To add an elevator bank:

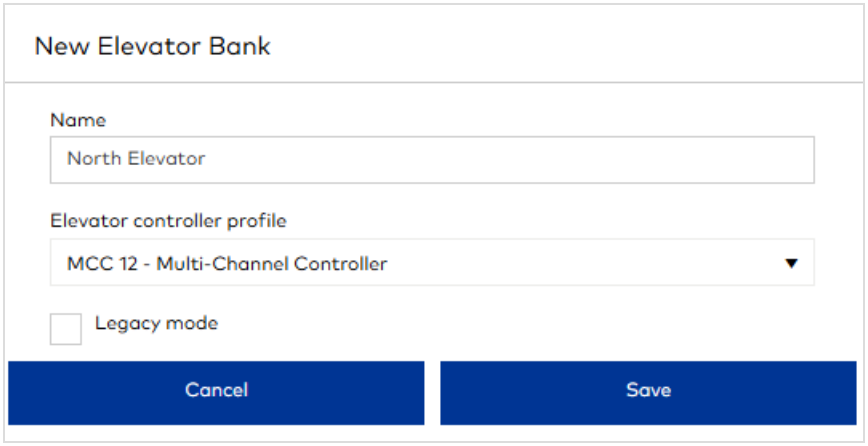
1. Go to **Property Builder**.
2. Select a building.



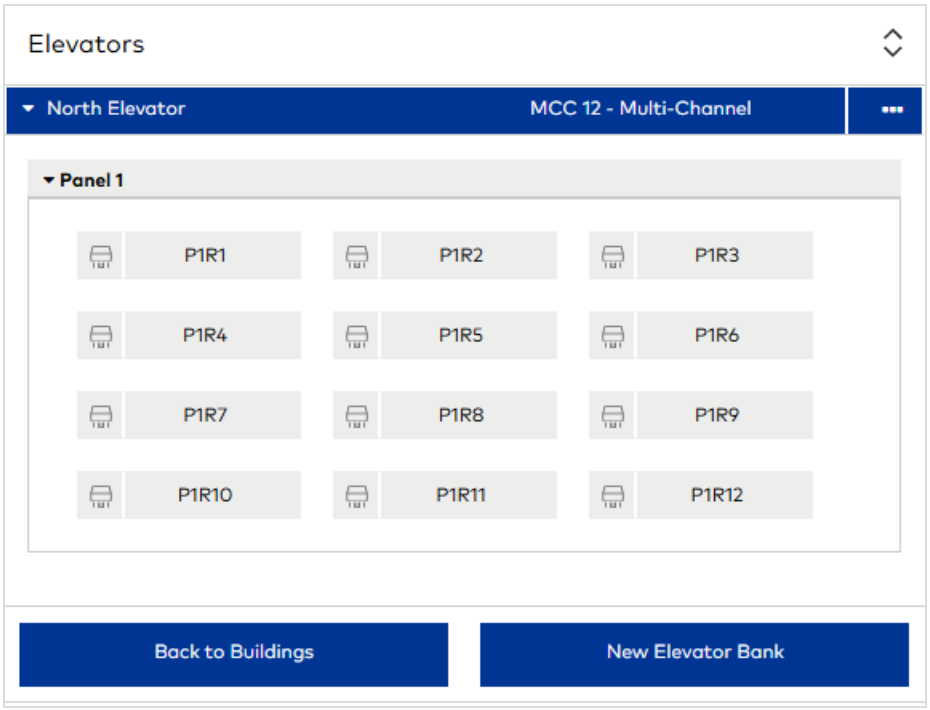
3. Click **Elevators**.



4. Click **New Elevator Bank**.



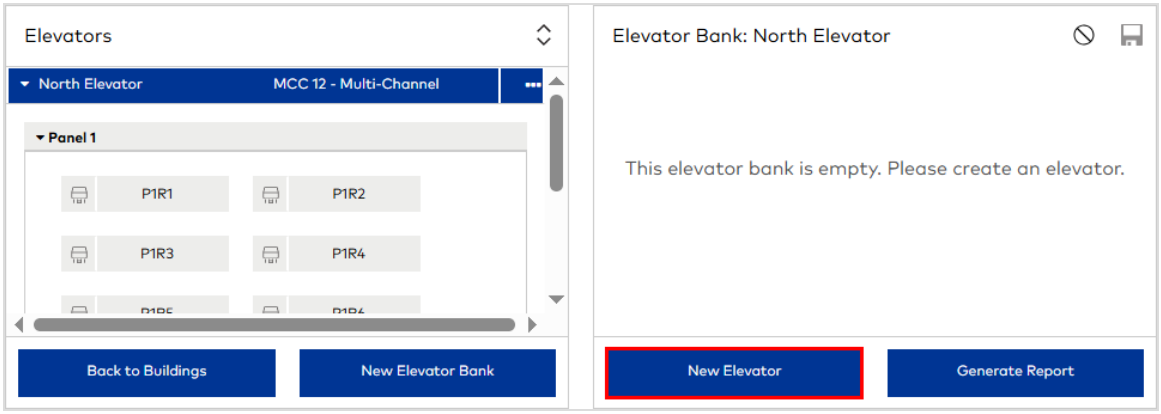
5. Specify a name for the elevator bank.
6. Select an elevator controller profile. (RAC5 must be configured in **Device Management**.)
7. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
8. Click **Save**. The elevator bank is listed in the Elevator list along with the number of Panel rows supported by the lock profile. The panel rows are where you map panel relay–to–floor access.



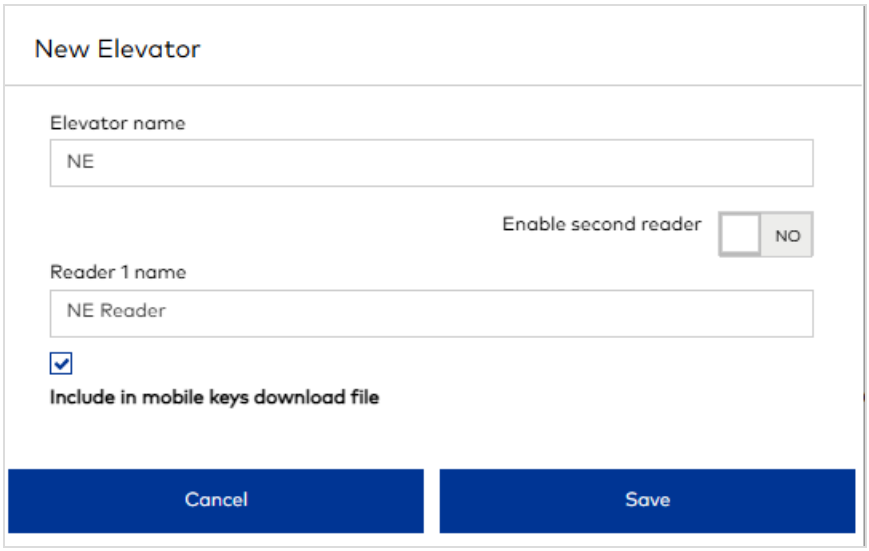
Add elevators

To add an elevator:

1. Go to **Property Builder**.
2. Select a building.
3. Click **Elevators**.



4. Select the elevator bank where you want to add the elevator.
5. Click **New Elevator**.



6. Specify a name for the elevator. For RAC 5 controllers, specify the name of the access point.
7. (*MFC controllers only*) Select whether to enable a second reader panel for the elevator.
8. (*MFC controllers only*) Specify a name for any reader.
9. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
10. Click **Save**.

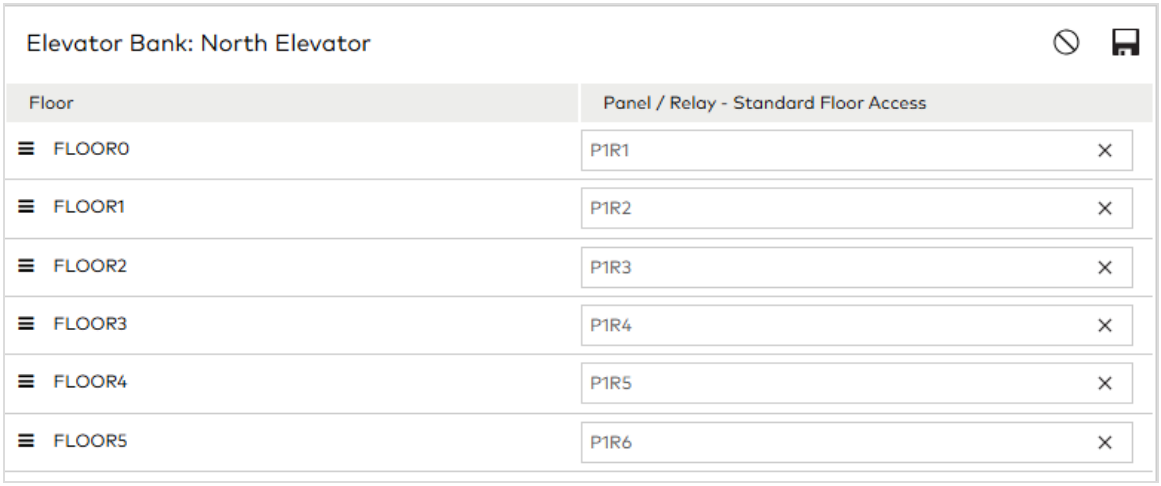
Map floor access

Relay–to–floor mapping controls elevator access to building floors. If you do not map a floor to a relay, there is no elevator access to the floor.

To map floor access:

1. Go to **Property Builder**.
2. Select a building.
3. Click **Elevators**.

4. Select the elevator bank where you want to map floor access. If the elevator bank contains at least one elevator, the list of floors in the building are displayed.
5. Select a Panel to configure.
6. Drag-and-drop panel relays (P*n*R*n*) to the Panel / Relay column for the floor that you want to map. The same relay can be mapped to multiple floors, but each floor can be mapped to only one relay.
7. Click **(Save)**.



Step 3

Configure Access

This section includes the following subjects:

Learning about Access Management 91
Add auto-unlatch schedules 95
Add access schedules 97
Add shift schedules 99
Create access point groups 101
Add Credentials 103
Assign schedules 107
Configure access profiles for limited-access common areas 108

Learning about Access Management

The **Access Management** module is where the access controls to all of the access points created in **Property Builder** are configured. While all of the configuration options work together to control access, defining credentials and configuring access to limited-access common areas are principle objectives in **Access Management**. Scheduling is an optional feature. The following figure summarizes all access configuration options.



Credentials

Credentials are essentially the access rights that are encoded on keys. During the process of adding a credential, you select the access points that you want the credential to authorize. You can add individual access points and access point groups. You can also select a shift schedule for each credential.

Structure of Credentials

All credentials in Community are organized into three hierarchical levels:

Credential Class Type > Credential Class > Credential

Credential class types are fixed definitions from which all credential classes are derived. The fixed definition consists of one or more persisting properties. For example, keys encoded with a credential based on an Emergency credential class type always include the property to override a projected deadbolt or privacy switch. Other properties determine whether access is configured in **Access Management** or at key-making time, whether toggle mode is supported, and the number of times a key can be used.

Credential classes merely serve to pass down any property defined for the class type to the credential. The default credential class for each class type bears the same name as the type. For example, the default credential class for the Emergency class type is *Emergency*.

Credentials are the level at which access is enabled. Depending on the selected class type/class, access point groups and access points are selected while defining the credential or at key-making time.

Default Credential Classes for Staff/Vendor Keys

The credential classes used for making staff/vendor keys each offer a unique combination of characteristics. The following table summarizes the credential class types and default credential classes used to make staff/vendor keys.

The Emergency credential class is only available when Emergency Keys are enabled in **System Settings > Staff/Vendor Keys**.

Credential Class Type/ Default Credential Class	Unique Property	Access	Toggle	Common Areas
Emergency	Always overrides deadbolt/ privacy switch	Predefined	Default: No. For access point types Unit/Suite, can be enabled in Property Builder.	Predefined
Limited Use	Key use is limited to a specified number of times	Predefined	No	Common Area Access Profile
Staff	None	Predefined	Default: No. For access point types Unit/Suite, can be enabled in Property Builder.	Common Area Access Profile
Staff (variable access)	None	Variable	Default: No. For access point types Unit/Suite, can be enabled in Property Builder.	Common Area Access Profile
Vendor	None	Variable	Default: No. For access point types Unit/Suite, can be enabled in Property Builder.	Common Area Access Profile

Learn more about each credential class type and the default credential class:

- **Emergency Keys**—The principal property of the Emergency class is that keys always override a projected dead bolt or active privacy switch. As such, reserve this class for emergency personnel only, such as firefighters and safety officers. All access is predefined (no access points can be selected at key-making time). By default, keys do not toggle access; however, toggle mode is supported for unit and suite access point types if the option **Enable toggle mode** is selected when creating the access point in **Property Builder**.
- **Limited Use Keys**—Except for all common areas, access is predefined. All unlimited and limited resident and staff common areas must be associated with a *Limited Use* profile in **Common Area Access** before they display at key-making time. Keys encoded with a credential in this class cannot toggle access. The special characteristic that differentiates the Limited Use class is that access is limited to a pre-defined number of times. The limit is specified in **System Settings > Staff/Vendor Keys**. For example, if the limit is six, the key opens the lock the first six consecutive times then expires.
- **Staff Keys**—The Staff class options are flexible to meet the needs of the different types of keys that you may need to make for staff:
  - **Staff**—Except for all common areas, access is predefined. All unlimited and limited resident and staff common areas are selected at key-making time; however, the common areas must first be associated with a *Staff* profile in **Common Area Access**. By default, keys do not toggle access; however, toggle mode is supported for unit and suite access point types if the option **Enable toggle mode** is selected when creating the access point in **Property Builder**.
  - **Staff (variable access)**—All access is authorized at key-making time. All unlimited and limited resident and staff common areas are selected at key-making time; however, they must be associated with a *Staff (variable access)* profile in **Common Area Access** before they display at key-making time. By default, keys do not toggle access; however, toggle mode is supported for unit and suite access point types if the option **Enable toggle mode** is selected when creating the access point in **Property Builder**.
- **Vendor Keys**—All access is authorized at key-making time. All unlimited and limited resident and staff common areas are selected at key-making time; however, they must be associated with a *Vendor* profile in Common Area Access before they display at key-making time. By default, keys do not toggle access; however, toggle mode is supported for unit and suite access point types if the option **Enable toggle mode** is selected when creating the access point in **Property Builder**.

Additional floor access is configured at key-making time for all credential classes.

Predefined and Variable Access

Predefined and variable access refers to how access points are authorized when making staff/vendor keys. For credential class types with variable access, all access is authorized at key-making time. For credential class types with predefined access, access points are authorized by a credential defined in **Access Management > Credential Management**. When

making a key with predefined access, only those access points in the selected credential are authorized. (Limited-access common areas are the exception because they can be authorized at key-making time for all but the Emergency class.)

Toggle Mode

Toggle is a feature that changes the state of a lock between *Latched* and *Unlatched* each time a valid key is presented to the lock. For example, the default state of a lock is *Latched*. The first time a key is presented, the lock changes to an *Unlatched* state. The door is open and remains accessible until the key is presented to the lock again or the interior privacy switch is engaged.

Toggle is enabled in different ways depending on lock type and credential class:

- Toggle may be a mechanical feature of the lock. For example, all Nova locks operate in toggle mode.
- For credentials based on the Emergency, Staff, Staff (variable access), and Vendor classes, toggle is enabled for unit and suite access points by selecting the option **Enable toggle mode** when creating the unit/suite access point in Property Builder. Valid for lock profiles: Saflok Quantum, Saflok Confidant, Saflock RT/RT+, RCU, Pixel and Saffire LX, RAC5 XT, RAC5 Lite.
- For credentials based on the Limited Use class, toggle mode is not supported.

Limited-Access Common Areas

With the exception of keys encoded with the Emergency credential, limited-access common areas must be configured in **Access Management > Common Area Access**. Essentially, you must create a common area access profile for the selected credential type then associate limited-access common areas to either units/suite units (for resident access) or credentials (for staff access). At key-making time, the limited-access common areas are listed with the option to include or exclude access on the key.

Default Credential Classes for System Keys

The following credential class types/default classes are used to create credentials for system keys:

- **Latch**—This class is used to create system credentials that authorize Latch Keys.
- **Unlatch**—This class is used to create system credentials that authorize Unlatch Keys.
- **Toggle Latch/Unlatch**—This class is used to create system credentials that authorize Toggle Latch/Unlatch Keys.

Credentials for Resident Keys

The credential class and credentials used to make keys for residents are implicit. In other words, you don't select a Resident credential class/credential. Instead, the access points selected during unit assignment, including any units, suite units, common areas and floors, form the credential that authorizes entry. Only in the **Reports** module is there a reference to a Residents credential class. When selecting options for the **Key/User Assignment Report**, you can select the Resident class to include a list of all access points encoded on keys assigned to residents.

Credentials Made in the Community API

Credentials that are created using the Community API are listed in **Credential Management** as long as the credential is used on at least one active key. The credentials cannot be edited or selected when making a key in the Community user interface.

Common Areas

Resident Common Areas and Staff Common Areas are two access point types that are configured for general access. However, both types can be enabled for limited access. When limited access is enabled, you must configure access in **Access Management > Common Area Access**.

Resident Access

Limited-access Resident Common Areas are associated with units/suite units. Resident access depends on the common areas associated with their assigned units/suite units.

Staff Access

Limited-access Staff Common Areas are associated with a credential. Staff access depends on the common areas associated with the credential selected when making a Staff/Vendor Key.

Common areas are not configured in **Common Area Access** for credentials made with the Emergency credential class. Instead, all access points (including limited-access common areas) that you want to authorize on the key must be selected in the credential.

Scheduling

The scheduling feature provides another layer of access control. Both of the following schedule types are programed directly in the locks:

- Auto-Unlatch Schedules establish when an access point can be accessed without a key thereby allowing unrestricted access. The access point types that support auto-unlatch schedules are restricted areas, all common areas, and elevator readers.
- Access Schedules establish when an access point can be accessed with a valid key. You can assign a different Access Schedule for each credential class in which an access point is included. For example, if the Laundry Room common area is included in a Staff (variable access) credential and a Vendor credential, you can assign different Access Schedules for each. The access point types that support access schedules are all common areas and elevator readers.

Add auto-unlatch schedules

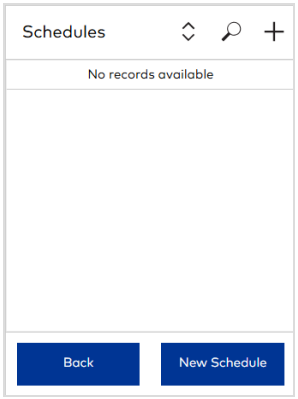
Create and configure schedules that control when the following access point types can be accessed without a key:

- common areas
- restricted areas

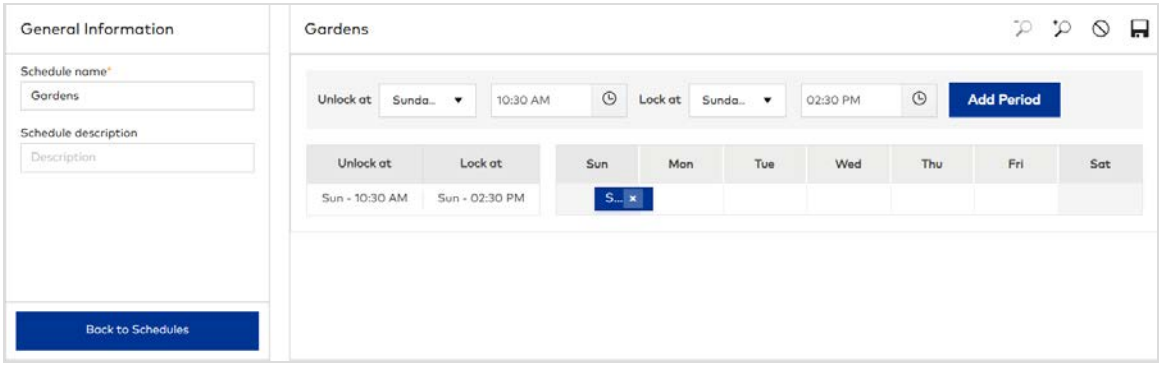
> Every time that you assign/unassign a schedule or edit a schedule, you must program (or reprogram) affected access points.

To add a schedule:

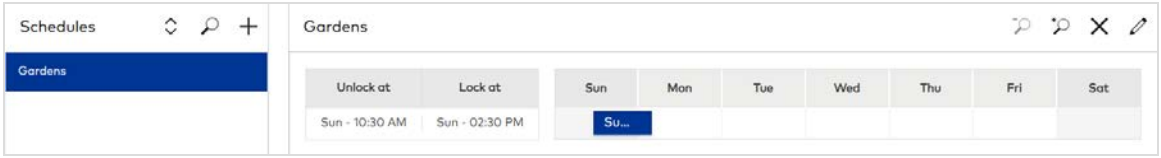
1. Go to **Access Management > Auto-Unlatch Schedules.**



2. Click **New Schedule**.



3. Specify a descriptive name for the schedule.
4. (*optional*) Specify a description for the schedule.
5. Select a day and time to enable access without a key.
6. Select a day and time to resume controlled access with a valid key.
7. Click **Add Period**. You can add multiple periods per day, but periods cannot overlap.
8. Click **(Save)** .



Edit a schedule

1. Select the schedule that you want to edit.
2. Click **(Edit)** .
3. Modify the schedule:
   - Change the name and/or description.
   - To change an existing period, select the period and click **Edit Period**.
   - To add a period, select day and time options then click **Add Period**. You can add multiple periods per day, but periods cannot overlap.
   - To delete a period, click **(Delete)** directly in the period block on the schedule.
4. Click **(Save)** .

Delete a schedule

1. Select a schedule.
2. Click **(Delete)** .
3. Click **YES** to confirm .

Add access schedules

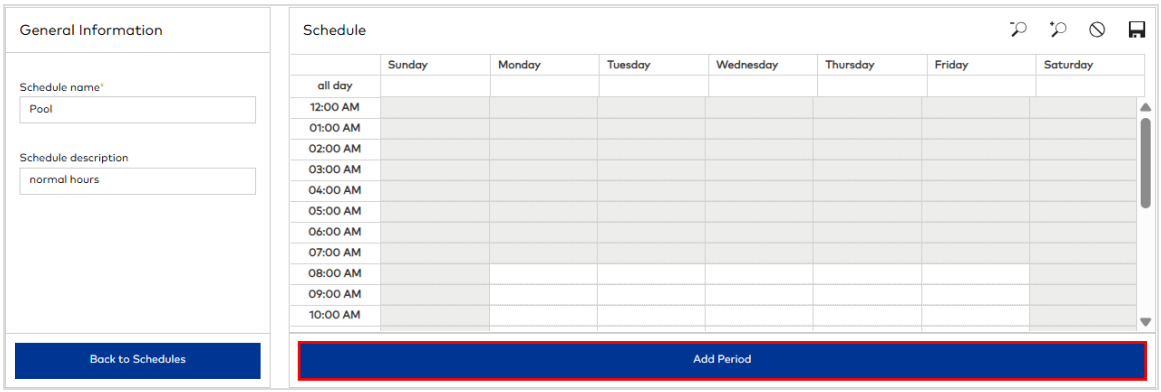
Access schedules control when the following access point types can be accessed with a key:

- common areas
- elevator readers

Every time that you assign/unassign a schedule or edit a schedule, you must program (or reprogram) affected access points.

To add a schedule:

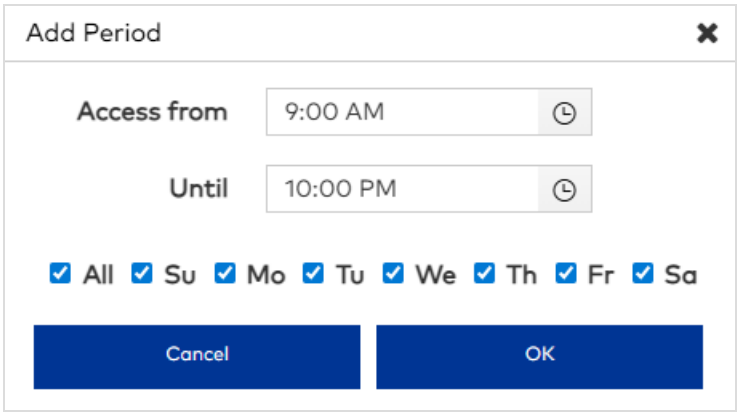
1. Go to **Access Management > Access Schedules.**
2. Click **(Add)** +.



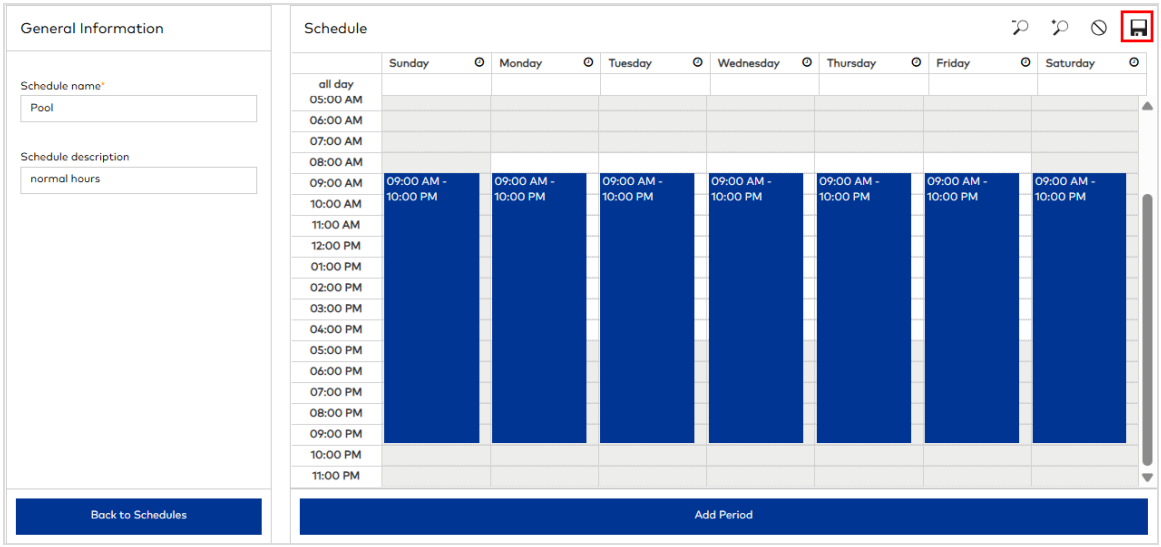
3. Specify a descriptive name for the schedule.
4. (*optional*) Specify a description for the schedule.

   Use drag-and-drop to add periods directly on the time table. To add a period that covers 24 hours, double-click the **all day** row (first row).

5. Click **Add Period**.



6. Select the time access starts.
7. Select the time access ends.
8. Select the days on which to apply the selected hours.
9. Click **Apply**. You can add one period per day.



10. Click **(Save)**.

Edit a schedule

1. Select the schedule that you want to edit.
2. Click **(Edit)** .
3. Modify the schedule:
   - Change the name and/or description.
   - To add a period, click **Add Period**, specify scheduling parameters, then click **OK**. You can add one period per day.
   - To delete a period, click **(Delete)** directly in the period block on the schedule, then click **Delete**.
4. Click **(Save)**.

Delete a schedule

1. Select a schedule.
2. Click **(Delete)**.
3. Click **YES** to confirm .

Add shift schedules

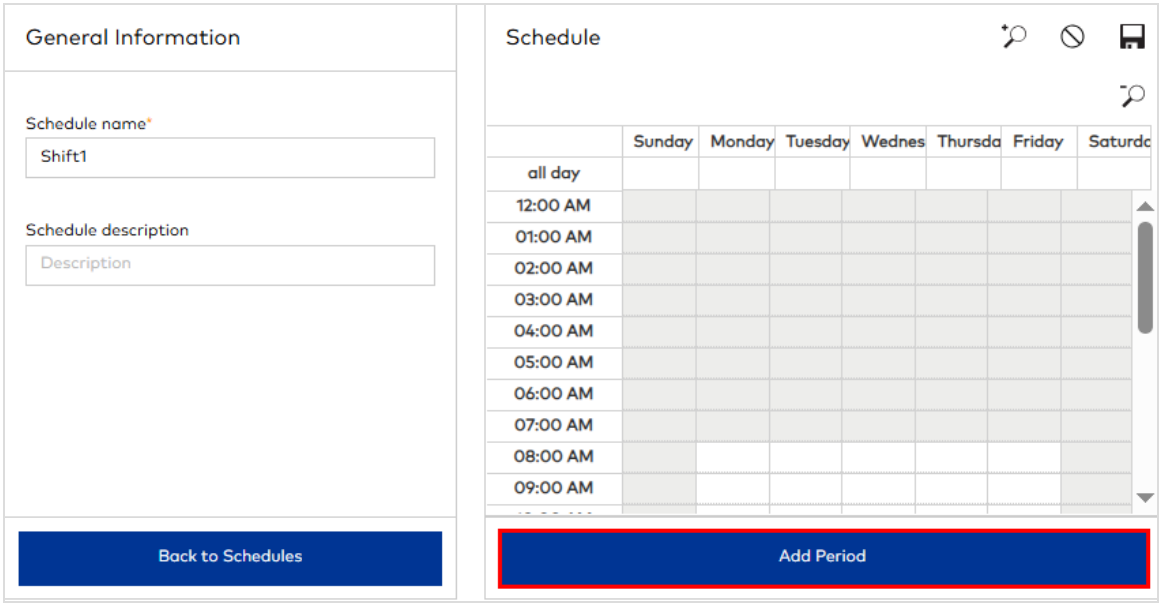
Create and configure schedules that control when staff credentials can access the following access point types:

- common areas
- restricted areas

The period configured applies to all days selected in the schedule.

To add a schedule:

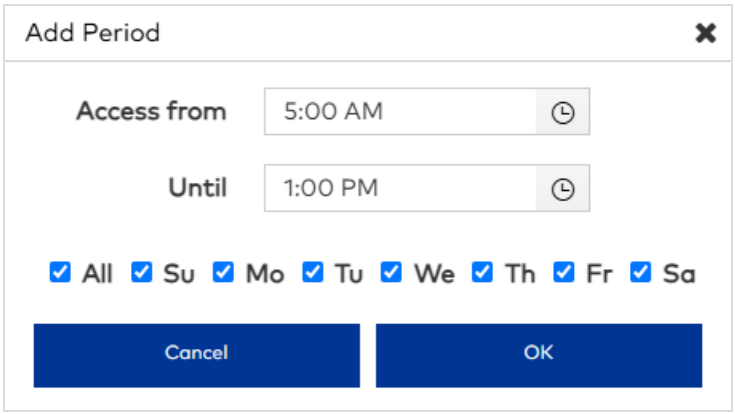
1. Go to **Access Management > Shift Schedules.**
2. Click **(Add)** +.



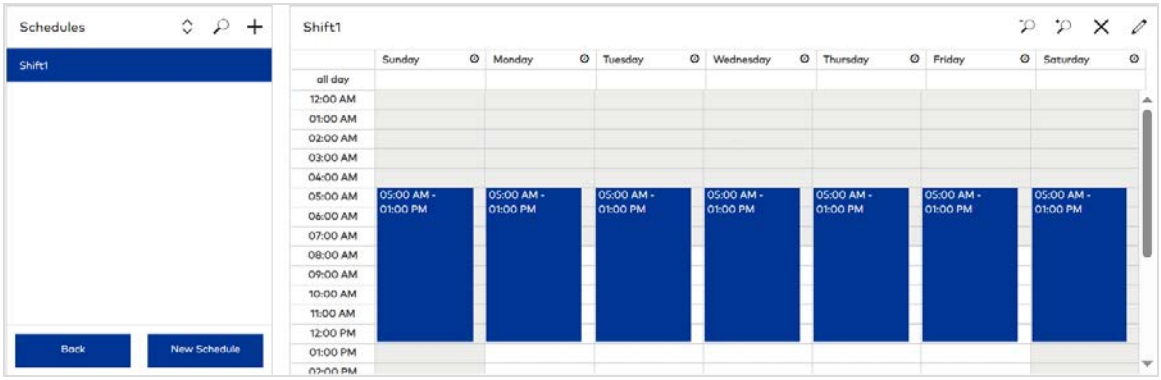
3. Specify a descriptive name for the schedule.
4. (*optional*) Specify a description for the schedule.

Use drag-and-drop to add periods directly on the time table. To add a period that covers 24 hours, double-click the **all day** row (first row).

5. Click **Add Period**.



6. Select the time access starts.
7. Select the time access ends.
8. Select the days on which to apply the selected hours.
9. Click **OK**. You can add one period per day.



10. Click **(Save)**.

Edit a schedule

1. Select the schedule that you want to edit.
2. Click **(Edit)** .
3. Modify the schedule:
   - Change the name and/or description.
   - To add a period, click **Add Period**, specify scheduling parameters, then click **OK**. You can add one period per day.
   - To delete a period, click **(Delete)** directly in the period block on the schedule, then click **Delete**.
4. Click **(Save)**.

Delete a schedule

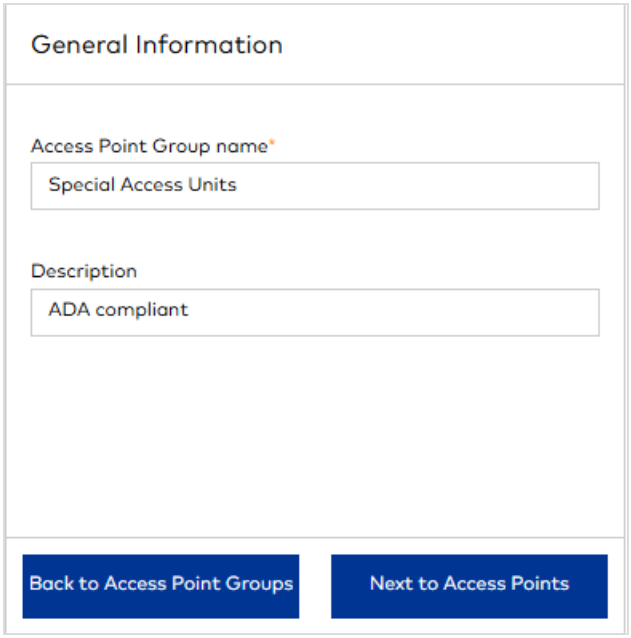
1. Select a schedule.
2. Click **(Delete)**.
3. Click **YES** to confirm .

Create access point groups

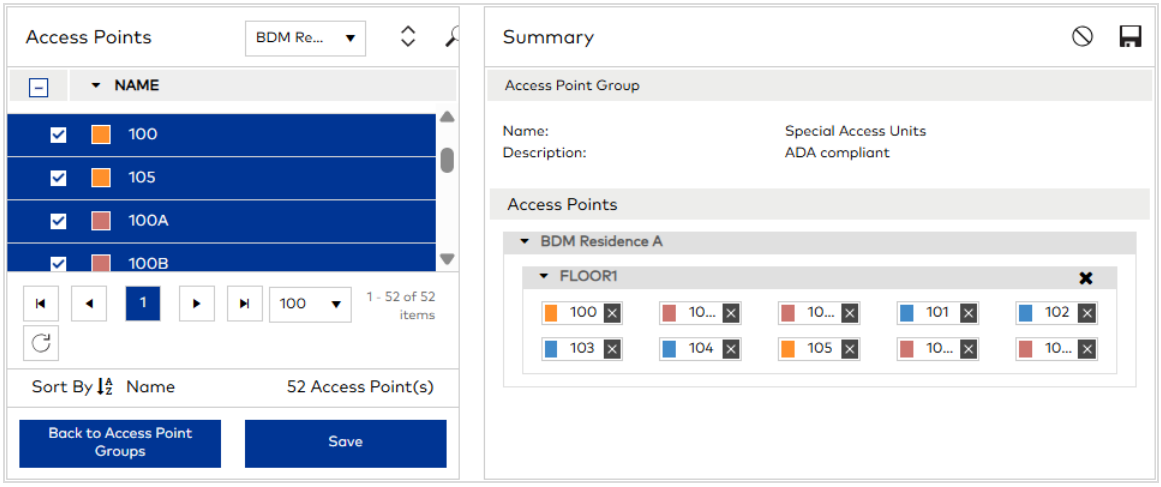
Organizing access points into logical groups based on location or intended use facilitates the assignment of credentials.

To add an access point group:

1. Go to **Access Management > Access Point Groups.**
2. Click **(Add)** +.



3. Specify a descriptive name for the group.
4. (*optional*) Specify a description for the group.
5. Click **Next to Access Points**.



6. Select the access points that you want to assign to the group. Selected access points are added to the Summary section (listed by building and floor).
   - You can select access points from different buildings.
   - You cannot add common areas to access point groups.
7. Click **Save**.

Edit access point groups

1. Select the access point group that you want to edit.

> When adding staff common areas or resident common areas with staff access enabled to a Limited Use Staff or Master credential, you must also make sure that the same common area is also associated with the credential in **Access Management > Common Area Access**.

2. Click **(Edit)** .
3. Modify the group:
   - Modify the group name and/or description.
   - To add or remove access points, click **Next to Access Points**. All access points assigned to the group are listed in the **Summary** section.
     - Select or deselect access points. Selected access points are added to group (and listed by building and floor in the **Summary** section). Deselected access points are removed from the group (and removed from the **Summary** section).
     - To remove an access point, click **(Delete)** directly in the access point block in the **Summary** section.
     - To remove all access points on a floor, click **(Delete)** in the floor row in the **Summary** section.
4. Click **(Save)**.

Delete an access point group

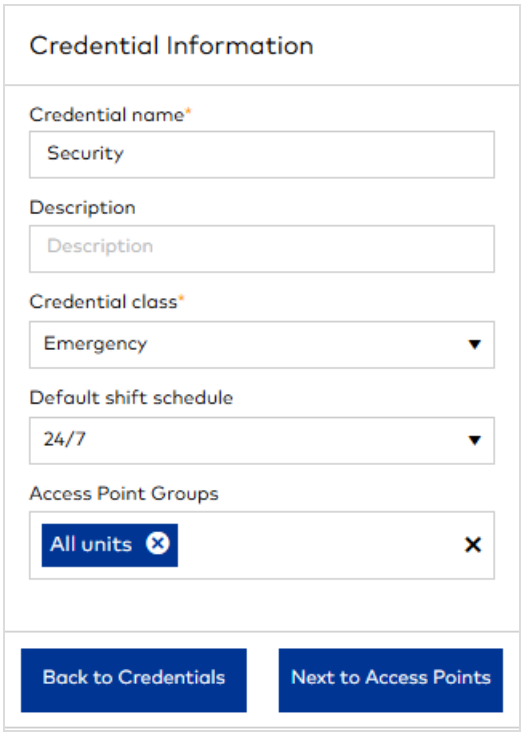
1. Select an access point group.
2. Click **(Delete)**.
3. Click **YES** to confirm.

Add Credentials

For initial site configuration, make staff/vendor credentials. it's important to make Emergency and Latch/Unlatch credentials. While it's not necessary to make Emergency and Latch/Unlatch keys, create the credentials to avoid delays during emergencies and busy daily operations.

To add a credential:

1. Go to **Access Management > Credential Management.**
2. Click **(Add)** +.



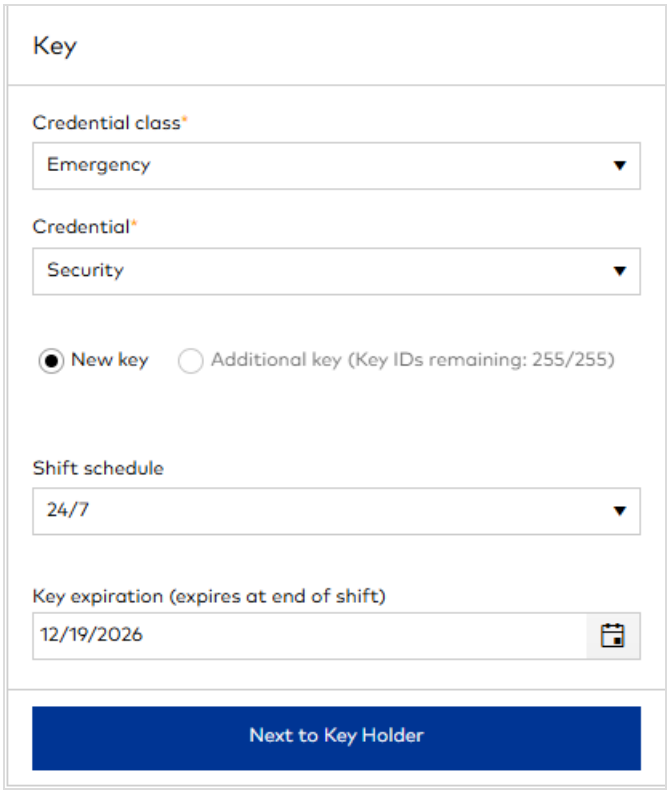
3. Specify a descriptive name for the credential.
4. (*optional*) Specify a description for the credential.
5. Select a credential class. For a description of each class, refer to "Learning about Access Management."

> You can also create a custom credential class. If you want to create a custom class, select **Edit Credential Classes** and see "Add Custom Credential Classes."

6. Select a shift schedule during which the key is valid. To enable 24/7 access, select **24/7**. To review shift schedule details, see **Access Management > Shift Schedules**. The selected shift schedule determines the days and hours that the key is valid.
7. Select the access point groups that you want to add to the credential. This option is not available for Staff (variable access) or Vendor classes or a custom class based on either class.
8. The next step depends on the selected credential class:
   - For Staff (variable access), Vendor or a custom class based on either class, click **Save**. The credential is created. All access points are selected at key-making time; however, common areas must be configured in **Access Management > Common Area Access**.
   - For Emergency, Limited Use, Staff, or a custom class based on any of these classes, click **Next to Access Points**.
9. Select the access points that you want to add to the credential. You can add access points from different buildings. Access points that are included in any selected access point groups are not listed.

- For the **Emergency** class type, all access point types are listed including elevator readers.
- For all other class types, all access point types are listed except common areas, which are selected at key-making time; however, common areas must be configured in **Common Area Access** and associated with the selected credential.

10. Click **(Save)**. The following figure shows the First Responders credential available to select when making a staff key.

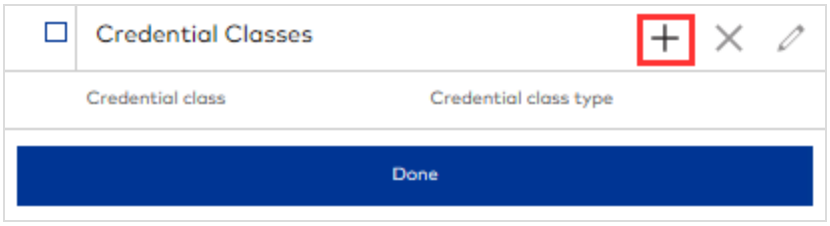


Add Custom Credential Classes

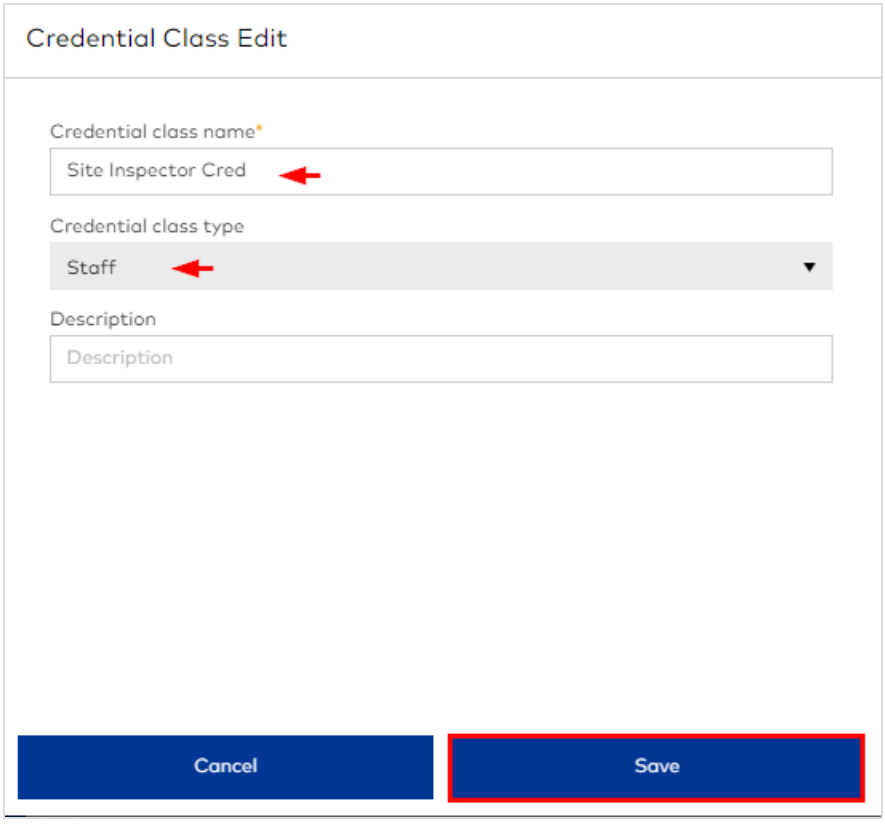
When selecting a credential class for a credential, you have the option to edit credential classes. Although you cannot edit or delete the default classes, you can add a class based on one of the default classes.

To add custom credential classes:

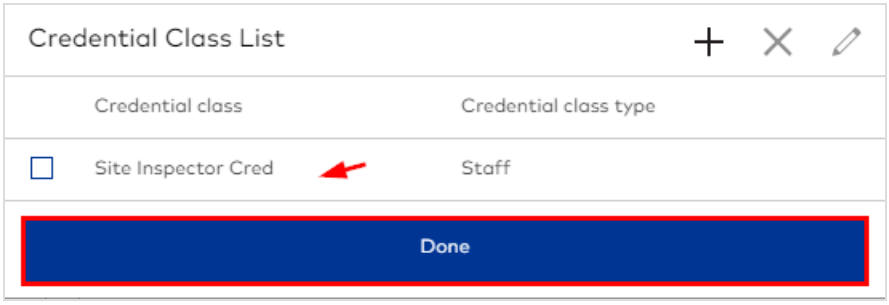
1. When selecting a credential class for a new credential, select **Edit Credential Classes**.



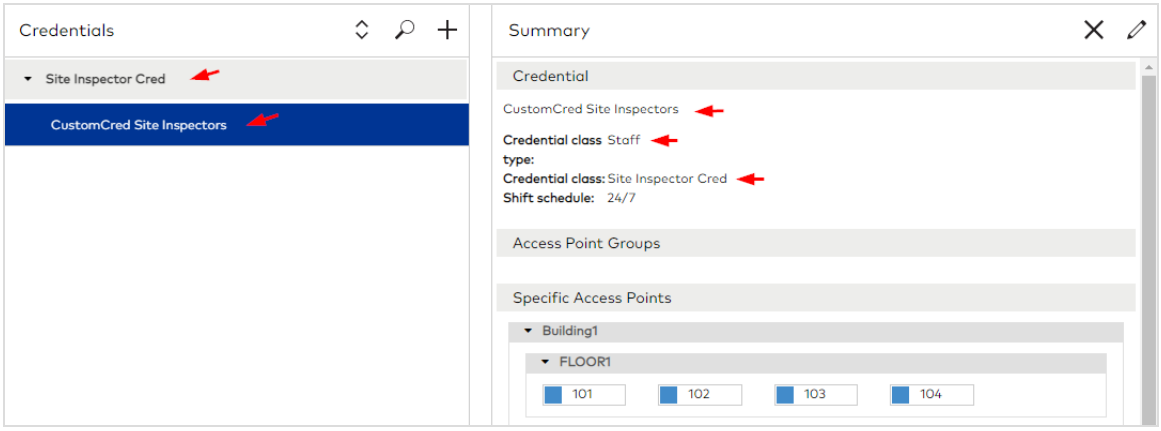
2. Click **(Add)**.



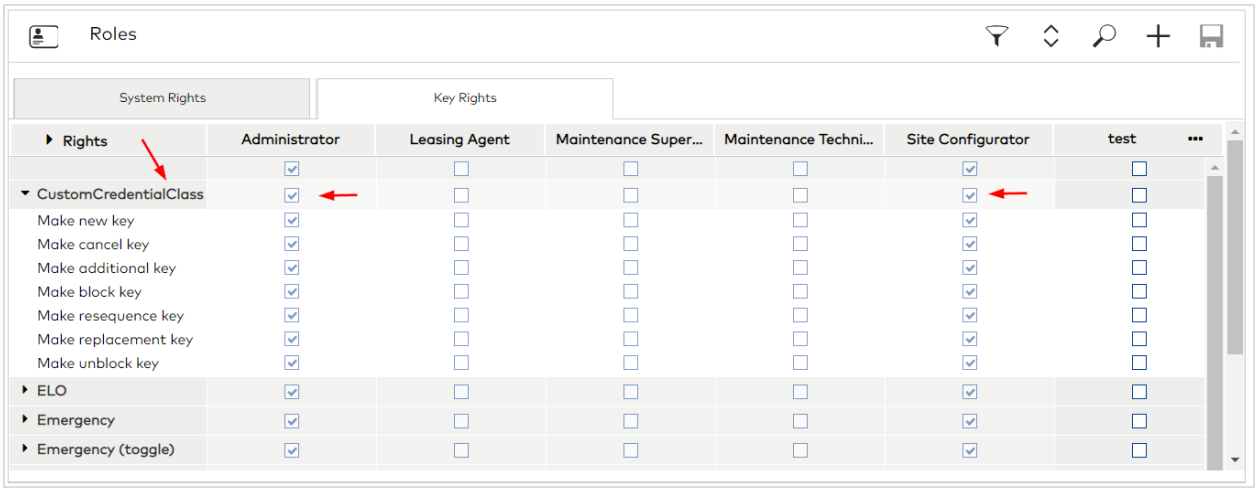
3. Specify a descriptive name for the custom class.
4. Select the credential class types on which to base the custom credential.
5. (*optional*) Specify a description for the custom class.
6. Click **Save**.



7. Click **Done**. After creating the custom class, you need to create a credential using the custom class, then the credential will be available when making a staff/vendor key.



When you create a custom credential class, all Operators who are assigned the default Administrator or Site Configurator role have the rights to make keys using the custom credential class. The following figure shows the default access in **Role Management** for a custom credential class.



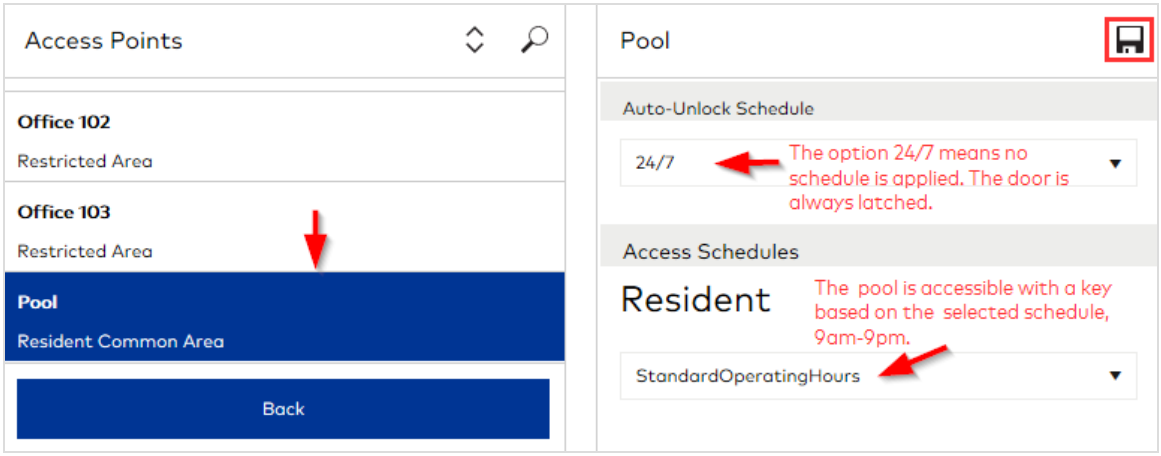
Assign schedules

Auto-Unlatch schedules can be assigned to common areas accessible by residents/staff/vendors and restricted areas.

Because access points can be included in more than one credential, you can assign different Access Schedules to the same access point for each of the following credential class types: Resident, Limited Use and Staff.

To assign schedules to an access point:

1. Go to **Access Management > Access Point Scheduling.**



2. Select an access point.
3. Select an Auto-Unlatch Schedule to apply to the access point. The default selection (24/7) means no schedule is applied.
4. Select an Access Schedule to apply to the access point. If the access point is included in more than one credential, you can select a schedule for each credential class.
5. Click **(Save)**.

Configure access profiles for limited-access common areas

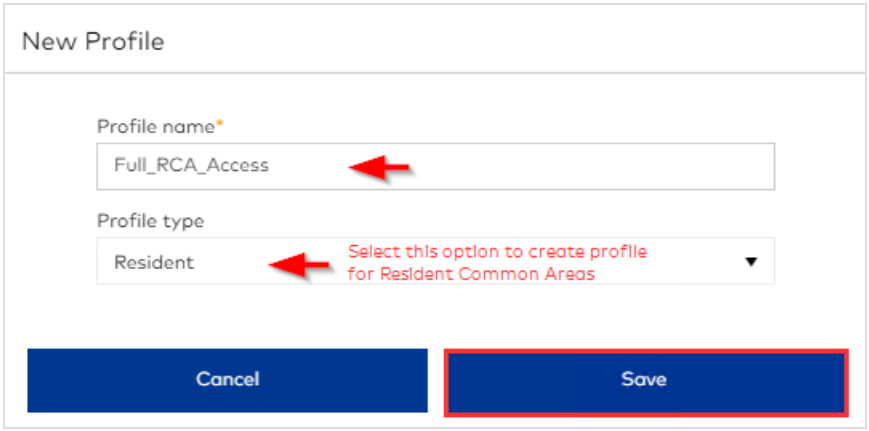
Create and configure profiles that associate units or staff/vendor credentials to limited-access common areas.

Configure resident access to limited-access common areas

Resident access to limited-access common areas can be configured as soon as all units, suite units, and limited-access common areas are created in **Property Builder**. The process involves adding a resident profile and then associating common areas to units and suite units.

Add a resident profile

1. Go to **Access Management > Common Area Access.**
2. Click **(Add)** +.

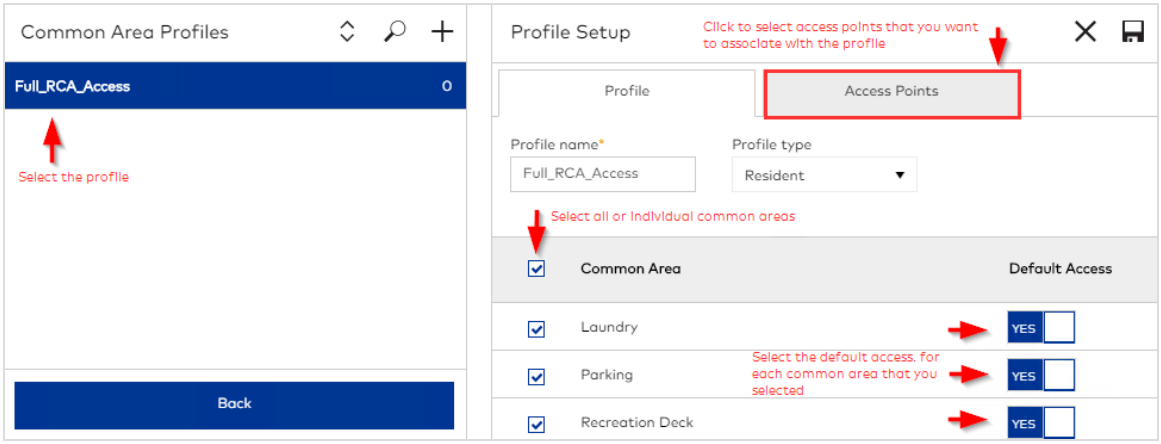


3. Specify a descriptive name for the profile.
4. Select profile type Resident.
5. Click **Save**. The profile is added to the list.

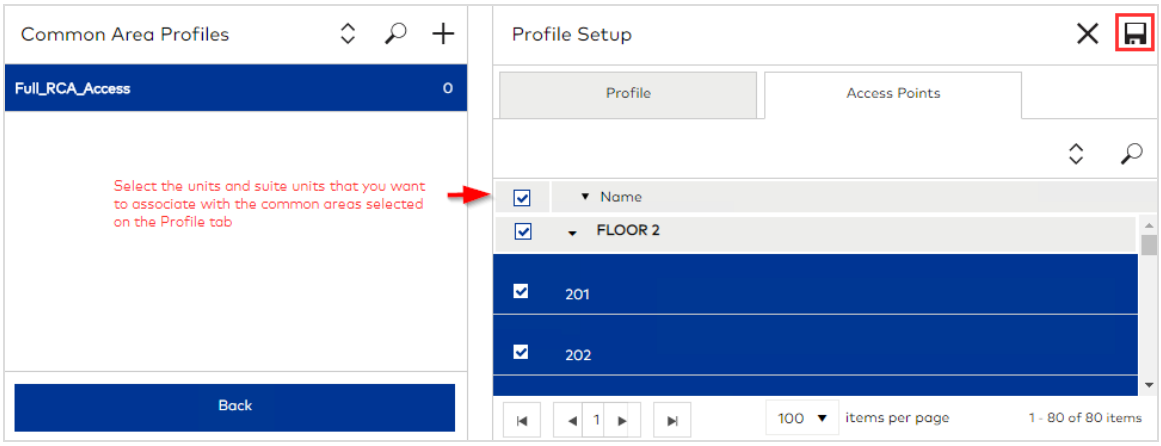
Associate common areas to units/suite units

To associate units to common areas:

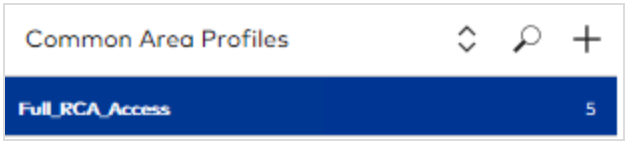
1. Go to **Access Management > Common Area Access.**



2. Select an existing common area profile or add a new profile.
3. On the **Profile** tab, select the common areas that you want to configure for access in this profile and whether to enable default access for each common area that you select. When default access is enabled, the common area is automatically added to unit assignments but can be disabled in resident profiles.



4. On the **Access Points** tab, select the access points to associate with the profile. You can add access points from different buildings.
5. Click **(Save)** .

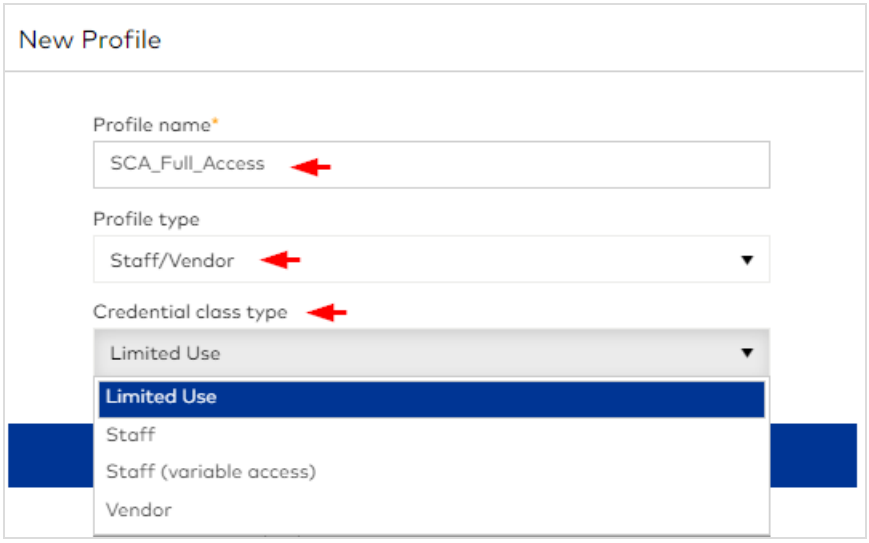


Configure staff/vendor access to limited-access common areas

Staff/vendor access to limited-access common areas can be configured after credentials are defined. The process involves adding a staff/vendor profile and then associating common areas to credentials.

Add a staff/vendor profile

1. Go to **Access Management > Common Area Access.**
2. Click **(Add)** +.

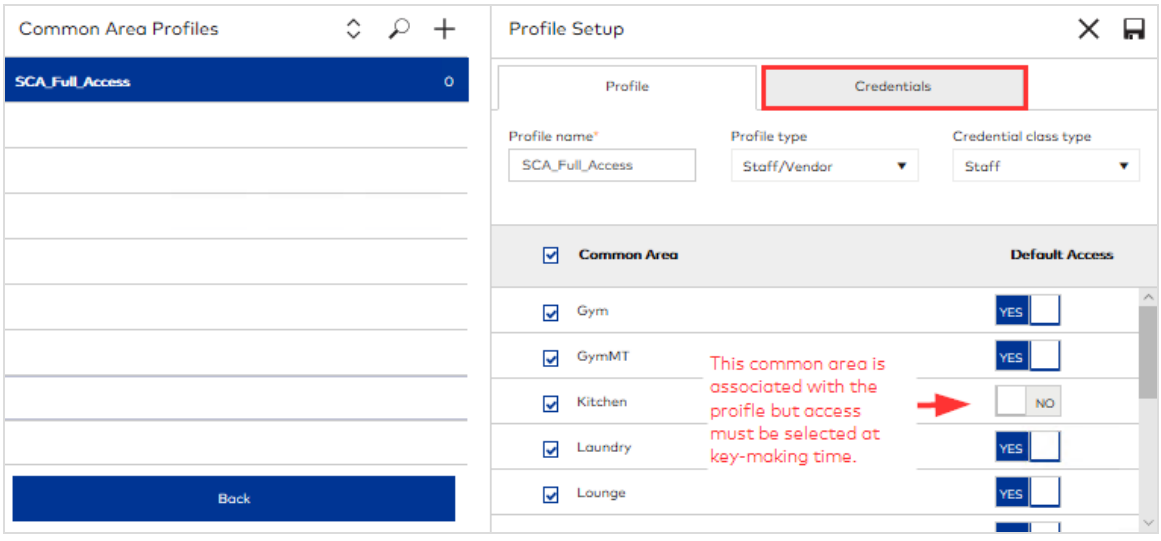


3. Specify a descriptive name for the profile.
4. Select the Staff/Vendor profile type.
5. Select a credential class type. Your selection determines the credentials that you can associate with the common areas selected on the **Profile** tab. You can only associate credentials that were made using the same class type.
6. Click **Save**. The profile is added to the list.

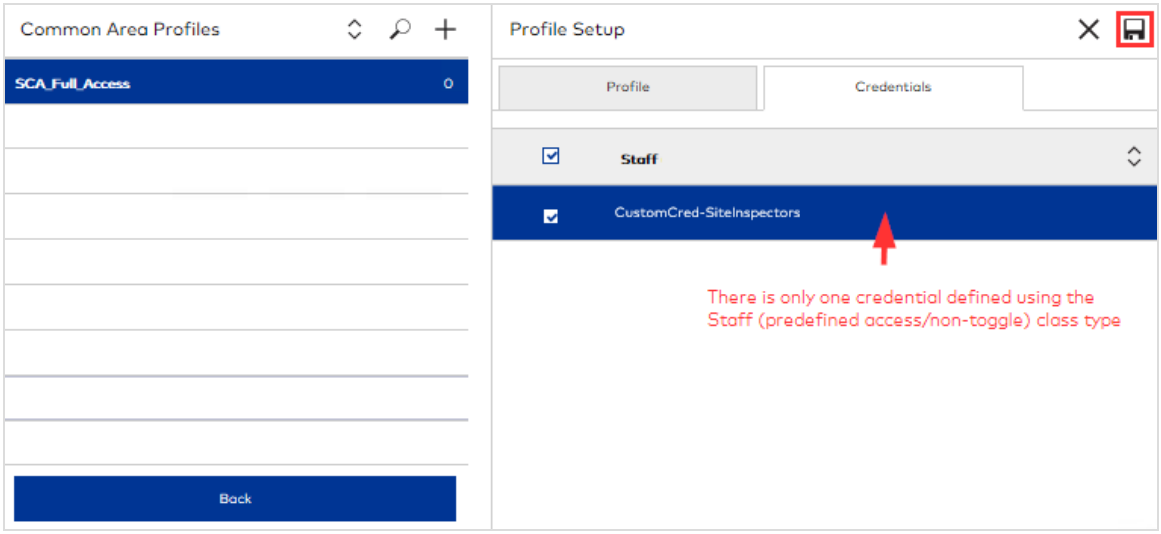
Associate common areas to credentials

To associate units to common areas:

1. Go to **Access Management > Common Area Access.**
2. Select an existing common area profile or add a new profile.



3. On the **Profile** tab, select the common areas that you want to configure for access in this profile and whether to enable default access for each common area that you select. Common area access must be enabled in **System Settings > Staff/Vendor Keys**.



4. On the **Credentials** tab, select all credentials that you want to associate with the common areas selected on the **Profile** tab. You can add access points from different buildings.
5. Click **(Save)** .



Step 4

Configure Devices

This section includes the following subjects:

Learning about Device Management 113

Add encoders 115

Learning about Device Management

Device Management is the Community module where you configure encoders.

When the licensed feature online communication is enabled, you can also configure the devices that support online communication.

Encoders

An encoder is an embedded device used to encode physical keys with configuration data from Community. Before you can encode or read a physical key, you must connect and configure at least one encoder. Encoders that have been configured in Community are listed in **Device Management > Encoders** with the current status (offline, online or Unsupported configuration), firmware type and communication mode (TCP/IP or USB).

Community supports the following:

- dormakaba RFID Encoder I—Legacy encoders. Unsupported configuration for enhanced security mode.
- dormakaba RFID Encoder II—Required for enhanced security mode. The part number 75720 displays on the underside of the encoder.

For the latest supported firmware versions, refer to the product release notes.

Prerequisites

The following prerequisites are automatically met during initial Community installation:

- The Community Client is installed on the workstation.
- The Community Client service is started.
- The Community Client configuration file is automatically configured with the correct IP address.

USB connection method

The encoder must be connected via USB cable to the workstation. You must configure an encoder for each workstation used to encode and read physical keys. Multiple workstations can share the same encoder.

TCP/IP connection method

The encoder must be connected via USB cable to the workstation for the initial configuration.

TCP/IP encoders communicate directly over the internet with the Community Server (not with workstations). You only need to configure the encoder once to use with multiple workstations. The encoder must be connected to the local network to be online.

If you change the connection method to TCP/IP after saving the initial configuration, you must reinitialize the encoder (unplug/replug).

Registered gateways and paired access points

This section displays when the licensed feature online communication is enabled.

Gateways are the network devices which are paired to access points for online communication to perform remote operations and receive access point events. After commissioning and connecting gateways to the Community Server, the devices are listed in **Device Management**. When a gateway status is **Online**, access points can be paired. Multiple gateways can be connected to Community, but an access point can be paired with only one gateway.

Maintenance Unit

The M-Unit (Maintenance Unit) is a hand-held embedded device used to transfer data between Community and the locks installed at access points. The device is used to program and audit locks.

The following M-Unitsare supported:

- M-Unit Saflok HH6 NFC–Wireless connection supported. Required for enhanced security mode.
- M-Unit Saflok HH6–Legacy device. Requires cable connection.

M-Unit authentication is enabled by default but can be disabled in **System Settings > Security**. When authentication is enabled, M-Unit credentials must be configured for at least one Operator in **Staff/Vendor Management**.

When enhanced security mode is enabled, M-Unit authentication is required, and the M-Unit security password (displayed at **System Settings > Security > Enhanced Security Mode**) is required to program access points. When Enhanced Security Mode is enabled, the M-Unit is site-specific. Using the M-Unit at a different site requires a factory reset.

The type of probe used to connect the M-Unit to locks depends on the lock model.



The M-Unit connects to the workstation using a serial connector.



For additional information about the M-Unit, refer to the documentation distributed with your device.

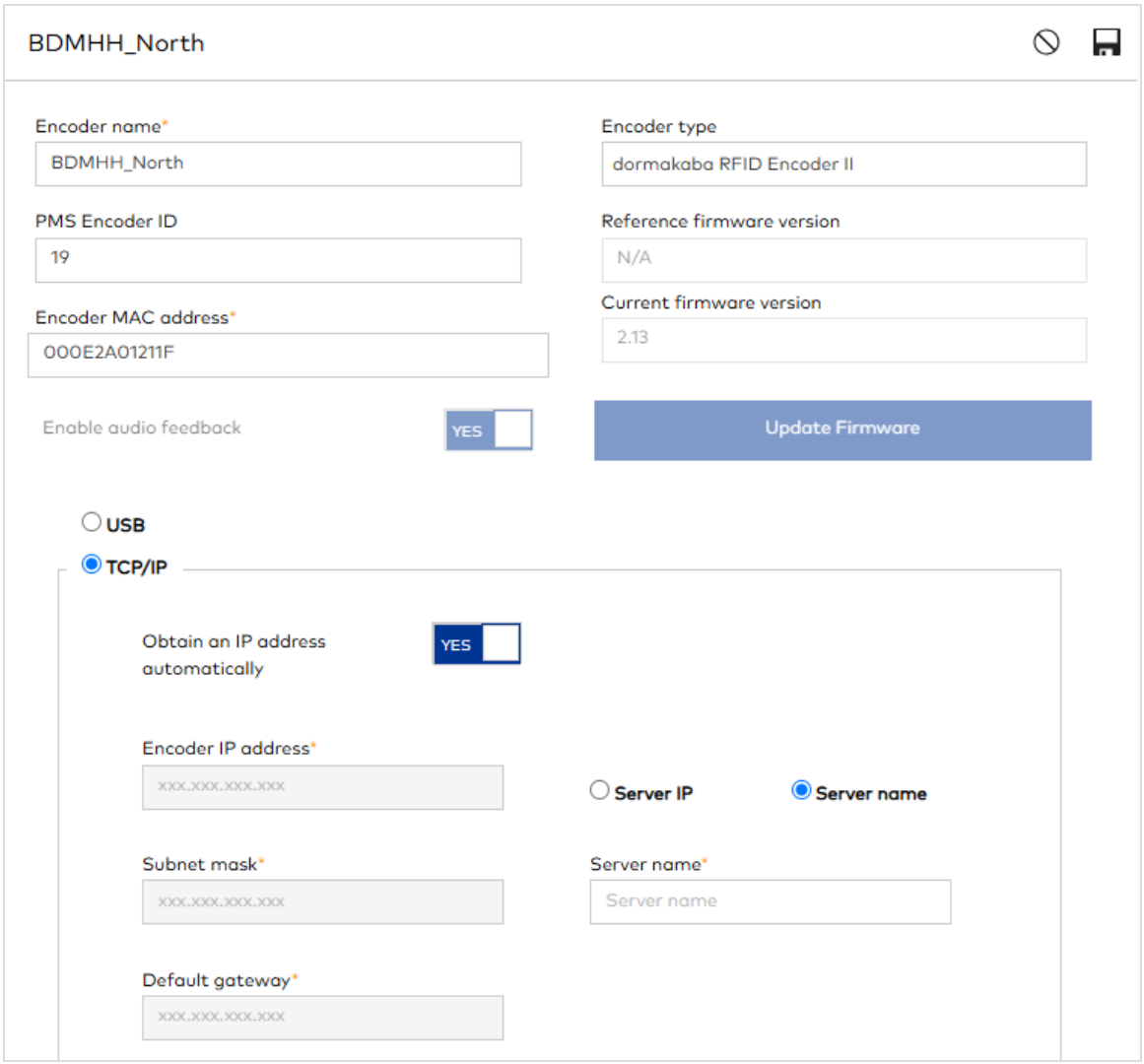
Add encoders

An encoder is required to encode keys with Community configuration data.

For fresh installations, enhanced security mode is enabled by default and cannot be disabled after any encoder (part 75720) is configured. Verify the enhanced security mode setting at **System Settings > Security > Enhanced Security Mode**.

To add encoders:

1. Connect the encoder via USB to the workstation. The initial configuration of an encoder requires that you connect the encoder to the Community workstation using a USB cable. By default, the device emits two audible beep and flashes a green light to indicate a successful connection.
2. Go to **Device Management**. (If online communication is enabled, click **Encoders**.)
3. Click **New Encoder**.



4. For **Encoder name**, specify a unique name that does not exceed 50 characters. This name displays in the list of encoders.
5. The encoder type is detected based on firmware version:
   - **dormakaba RFID Encoder I**—Legacy encoders. Unsupported configuration for enhanced security mode.
   - **dormakaba RFID Encoder II**—Required for enhanced security mode. The part number 75720 displays on the underside of the encoder. Unsupported configuration when Enhanced Security Mode is disabled.
6. (*conditional*) If integrating a third-party API, specify a number to identify the encoder. Valid values: 0-99.
7. Select the encoder MAC address. The value is automatically detected when you connect the encoder to the workstation.
8. Select whether the encoder emits audible beeps when a successful connection is made with the workstation and when making keys.
9. **TCP/IP** or **USB**—Select the method to connect the encoder with the workstation after initial configuration. If you change the connection type from TCP/IP to USB or from USB to TCP/IP you must reinitialize (unplug/replug) the encoder.
   - Specify TCP/IP settings to define the network configuration for the encoder device:
     - **Obtain an IP address automatically**—Select one of the following:
       - **Yes**—This is the default setting. A dynamic encoder IP address, subnet mask and default gateway are assigned.
       - **No**—Consult with your network administrator to obtain values for the encoder IP address, subnet mask, and default gateway.
     - Configure one of the following:
       - Server IP—IP address of the Community server.
       - Server name and local DNS IP address—Name of the Community server. If specifying server name, the encoder and server must be on the same domain. If you choose to use a static IP address and specify the server name, the IP address of the local domain name server is required.
10. Click **Save Changes**. The encoder is added to the list of encoders. If you selected the USB connection method, the encoder must remain connected to the workstation via USB. TCP/IP encoders must be connected to the network before the status changes to **Online**.

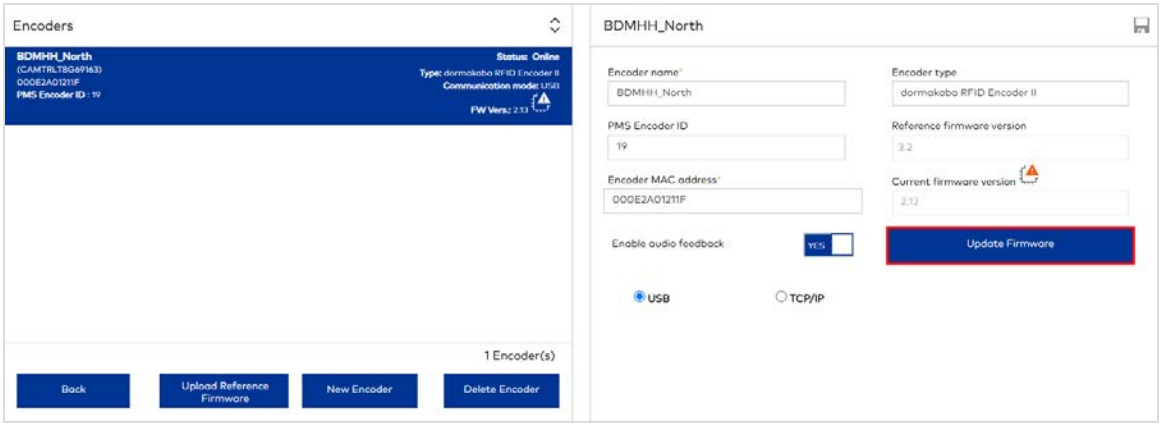


Update encoder firmware

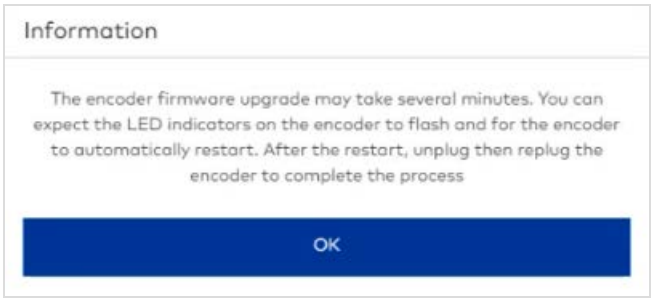
Firmware updates can be performed directly in Community for encoder type dormakaba RFID Encoder II. When the firmware version installed on the encoder is out-of-sync with the latest recommended firmware version listed in the product release notes, request the firmware update file from dormakaba Support.

Before performing the following steps, obtain the latest recommended firmware version file from dormakaba Support.

1. Go to **Device Management**. (If online communication is enabled, click **Encoders**.)
2. Click **Upload Reference Firmware**.
3. Navigate to and select the firmware file (*.enc2), then click **Open**.
4. Click **OK**. The firmware version populates in the **Reference firmware version** field. When the reference version and current version do not match, a warning symbol ( ) displays adjacent to the **Current firmware version** field.



5. Select the encoder that requires a firmware update.
6. Click **Update Firmware**.



7. Click **OK** to acknowledge the update may take several minutes. Expect the LED indicators on the encoder to flash. When the update is complete, the encoder restarts.
8. After the restart, unplug then replug the encoder.

Edit encoders

1. Go to **Device Management**. (If online communication is enabled, click **Encoders**.)
2. Select the encoder that you want to modify.
3. Modify settings.
4. Click **Save Changes**.

Delete encoders

1. Go to **Device Management**. (If online communication is enabled, click **Encoders**.)
2. Select the encoder that you want to delete.
3. Click **Delete Encoder**.
4. Click **YES** to confirm.

Step 5

Program Locks

This section includes the following subjects:

Learning about Programming & Auditing 119

Program locks 122

Learning about Programming & Auditing

Programming & Auditing is the Community module where you can perform the data transfers necessary to program and audit locks. The M-Unit (Maintenance Unit) is the hand-held device used to transfer data between the Community workstation and locks. During programming, configuration data is transferred from the Community workstation to the M-Unit to the locks. To audit locks, historical data is transferred from the locks to the M-Unit and then to the Community workstation.

When the licensed feature online communication is enabled, you can also program devices used in online environments.

Transferring data from the M-Unit to a workstation requires the Community Client. Download and install the client from the main toolbar in the **Programming & Auditing** or **Device Management** module.

Over time, locks may experience *time drift*—a small loss or gain of time—which can impact (albeit minor) time-relevant access point settings. Every time the M-Unit transfers data to a lock, the time in the lock is updated thereby correcting time drift. Ensuring that the M-Unit is connected to each lock at least once per year is a best practice.

Prior to locks being programmed for the first time, access points are accessible using the Construction (or Zone) Keys distributed with the software.

Programming locks

Each lock must be programmed with the respective access definition configured in Community. The process involves selecting the access points that you want to synchronize, transferring configuration data from the Community workstation to the M-Unit , then connecting the M-Unit to each lock for programming.

Community provides a filter feature to make it easy to identify the access points that require synchronization. Although all access points require synchronization for initial site configuration, the filter feature is useful if you program locks in batches, add access points, or make changes to the access configuration for locks.

The following color codes identify the access point types that require synchronization.

Color	Description
	Unit
	Resident Common Area
	Suite Common Door
	Suite Unit
	Restricted Area
	Staff Common Area
	Elevator readers

Access point programming required

Access points must be programmed or reprogrammed after specific tasks in the following modules:

Property Builder

- After adding or modifying the configuration of any of the following access point types:
  - Units
  - Suite Units

  - Restricted Areas
  - Resident Common Areas
  - Staff Common Areas
  - Elevator Reader
- After configuring or modifying elevator floor-to-relay mapping.

Access Management > Auto-Unlatch Schedules

- After editing an Auto-Unlatch schedule.

Access Management > Access Schedules

- After editing an Access schedule.

Access Management > Access Point Groups

- After assigning/unassigning access points from access point groups which are assigned to credentials.

Access Management > Credential Management

- After assigning/unassigning access point groups to/from credentials.
- After assigning/unassigning access points to/from credentials.

Access Management > Access Point Scheduling

- After assigning/unassigning an Auto-Unlatch schedule.
- After assigning/unassigning an Access Schedule.

System Settings > Residents

- After modifying the **Enable deadbolt/privacy switch override for resident keys** setting.

System Settings > Security

- After modifying Lock Access settings.
- After enabling Enhanced Security Mode.
- After terminating active legacy keys under Enhanced Security Mode.

System Settings > Staff/Vendor Keys

After modifying the **Maximum number of times Limited Use keys are valid** setting.

System Settings > Advanced Settings > RFID Key Types

- After modifying any of the RFID key types settings, all access points must be reprogrammed.

System Settings > Advanced Settings > Enable mobile keys

- After modifying the **Project ID** in LEGIC settings, all access points for which a mobile key is issued must be reprogrammed.

System Settings > Online Communication > Rx-Link

- After enabling or disabling this setting, all online access points must be reprogrammed.

Programming devices

This option displays when the licensed feature online communication is enabled.

The device must first be configured in **Device Management > Online Device Configuration.** A maximum of 240 devices can be programmed simultaneously. Programming devices requires a USB connection. Upon data transfer, the date/time on the M-Unit is synchronized with the server. When the USB connection is present and no devices are selected, the option to synchronize date/time on the M-Unit is available. Without a USB connection, the option to save configuration data is available for some device types.

Auditing locks

A lock audit retrieves detailed information about an access point. Audits retrieve access point data (such as the lock model and access point type), lock status data (such as the firmware version or time zone), and all activity for the lock. Audit data from both methods is stored in the Community database and available when generating Access Point Audit Reports.

Depending on the purpose, the following methods are available for lock audits:

- **Audit Key**—The Audit Key is a Special Function System Key that can be presented to a lock then read in Community.
- **M-Unit** —The M-Unit procedure transfers audit data to the M-Unit. Another step is required to transfer the interrogation files to Community for viewing. The M-Unit procedure is the option to choose to store and track historical data about access point activity.

Auditing online access points 

This option displays when the licensed feature online communication is enabled.

Online access points can be audited directly in Community.

Program locks

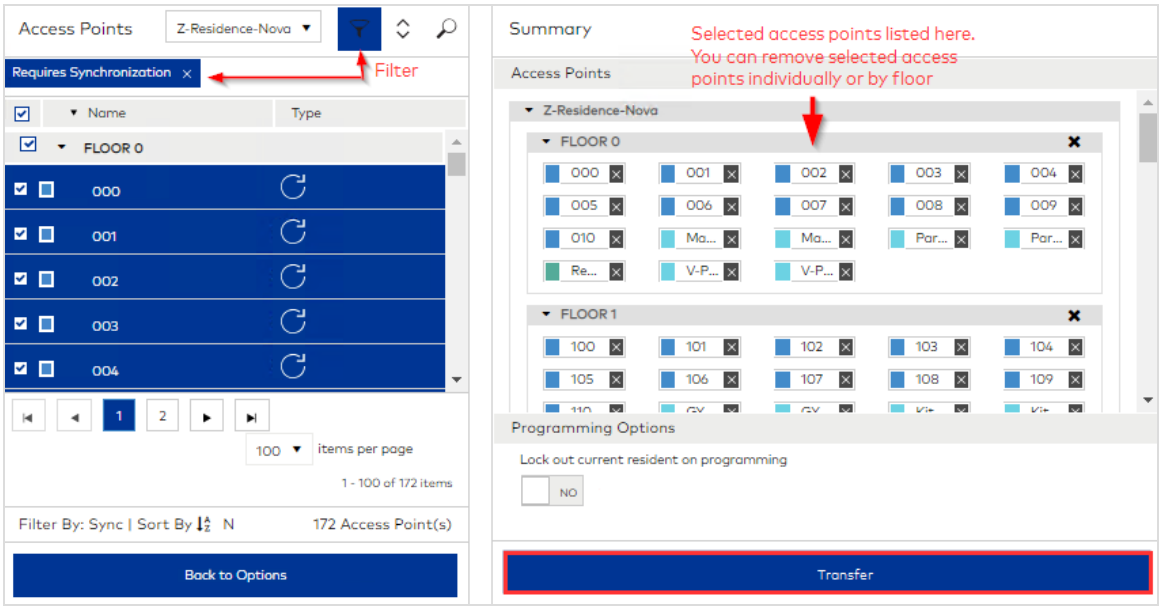
Some programming steps are performed on the M-Unit (Maintenance Unit). For official instructions, refer to the documentation distributed with your device. If M-Unit authentication is enabled in **System Settings > Security > M-Unit** credentials must be configured for at least one Operator in **Staff/Vendor Management**.

A Microsoft issue prevents the Edge browser from detecting/connecting to the Maintenance Unit. Consequently, access points cannot be programmed or audited without intervention. Open the Command prompt and issue the following command:

```
C:\windows\system32\CheckNetIsolation.exe LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
```

To program locks:

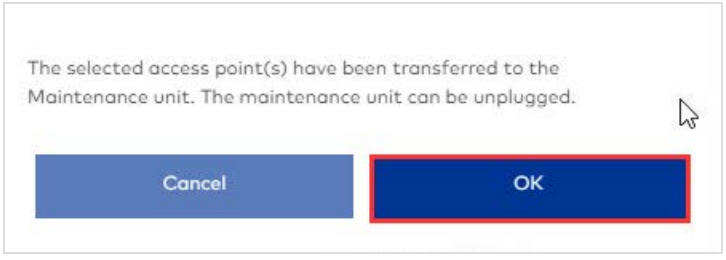
1. Go to **Programming & Auditing > Programming.**



2. Select the access points that you want to synchronize with Community configuration data. You can select access points from different buildings and filter the list to show only access points that require synchronization. The selected access points display in the **Summary** section organized by building and floor.

   The **Lock out current resident on programming** option only applies when keys have already been made and issued.

3. Connect the M-Unit to the workstation.
4. In Community , click **Transfer**. Messages on the workstation and M-Unit display that the transfer is in progress. Wait until the message on the workstation indicates transfer is complete and that you can unplug the M-Unit.



5. Click **OK**.
6. Disconnect the M-Unit from the workstation. The remaining steps are on the M-Unit.
7. If enhanced security mode is enabled, specify the M-Unit security password. The password displays at **System Settings > Security > Enhanced Security Mode**. (In some cases, the M-Unit displays a message prior to the password prompt indicating that the unit is not personalized; simply select OK.)
8. If M-Unit authentication is enabled, specify the M-Unit login credentials.
9. On the M-Unit menu, select **LOCKS**.
10. Use the UP / DOWN arrow keys to highlight **1- Program**, then press **ENTER**. The access point names display in groups of five.
11. Select the access point name for the lock, then press **ENTER**. Use the **PREV**, **NEXT** and **SEARCH** options to navigate and refine the list of names.
12. Select the type of probe that you are using to connect the M-Unit to the lock.
13. When prompted, insert the probe into the lock. Programming starts immediately. If the lock has already been programmed, the M-Unit issues a message requesting confirmation to overwrite the existing programming.
14. When prompted that programming is complete, click **OK**.

Testing locks with valid keys after programming is a best practice.

If issues arise when programming locks, create and present an LED Diagnostics Key in **System Keys** and see "Troubleshooting locks."

Step 6

Review & Customize Roles

This section includes the following subjects:

Learning about Role Management 125

Review pre-defined roles 127

Configure custom roles 128

Learning about Role Management

Role Management is the Community module where the roles that are assigned to Operators are configured. A role is a grouping of rights that authorizes access to Community features and functions. By assigning a role to an Operator, you are granting access to all of the rights selected for the role. Operators can only see and use the features and functions that are authorized by their assigned role. Role Management is only accessible to operators assigned the Administrator or Site Configurator role.

Predefined and custom roles

When assigning roles to Operators, you can use the predefined roles or create custom roles. Community includes the following predefined roles based on typical organizational requirements:

- Administrator
- Site Configurator
- Leasing Agent
- Maintenance Supervisor
- Maintenance Technician

The rights selected for predefined roles cannot be modified.

Custom roles are based on one of the predefined roles and are entirely configurable. The exception is that Role Management is not accessible to any custom role. When a custom role is modified, the changes apply to all Operators who are assigned the role.



Before changing the rights associated with a custom role, generate a **Roles & Rights** report to determine any Operators who may be affected.

Rights

There are two types of rights in Community:

- **System Rights** are categorized by module so that you can authorize an entire module or discrete functions within a module. **Reports** is a category of system rights. When the **Reports** category is authorized for a role, any Operator assigned the role can generate all report types.
- **Key Rights** are categorized by key type so that you can authorize all commands for a key type or discrete commands for each key type. **Staff/Vendor Keys** is a category of key rights. When the entire **Staff/Vendor Keys** category is authorized for a role, any Operator assigned the role can perform all of the discrete functions:
- Make replacement key
- Make unblock key
- Make resequence key
- Make cancel key
- Make additional key
- Make block key
- Make new key

For both system and key rights, authorization can be enabled at the category level or individual right level. When the category is selected, access is granted to all individual rights in the category.

Roles control user interface display

The features and options that display in Community depend on the rights selected for the role assigned to the Operator. For example, if the Operator that is currently logged in does not have rights to access the **Property Builder** module, the module does not display. Likewise, if the only right selected in the ***ELO (Electronic Lockout)*** key right category is *Make Additional*

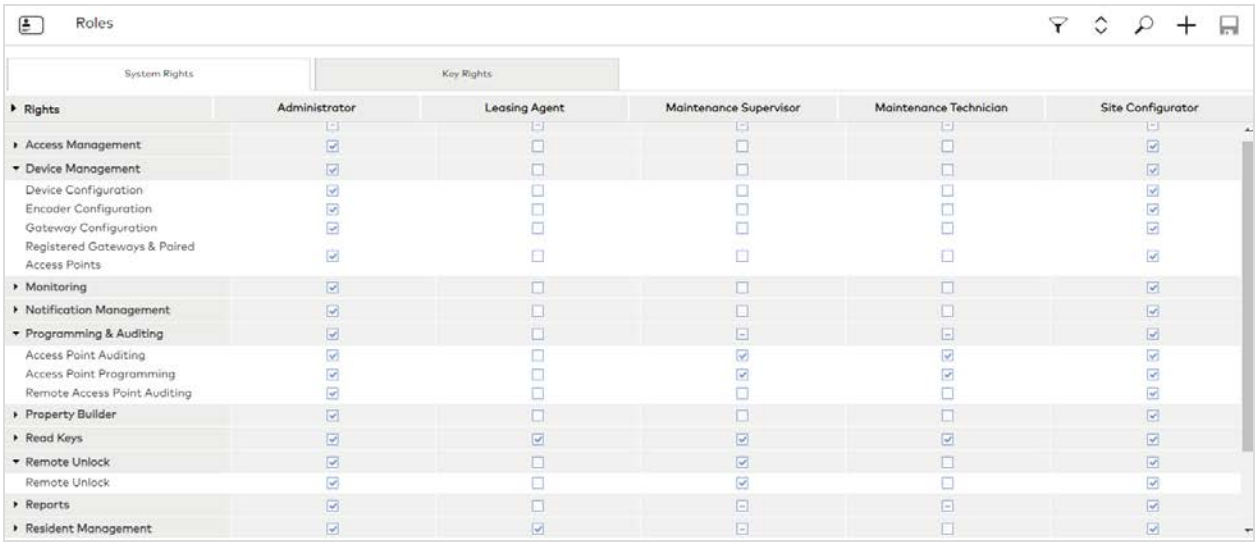
Key, the only time ***ELO*** displays as an option when selecting a credential class is when the Operator is making an additional key.

Review pre-defined roles

dormakaba recommends reviewing the rights associated with the predefined roles before assigning roles to Operators or creating custom roles.

To review roles and rights:

» Go to **Role Management**.



Roles are identified in the column headings. Rights are listed in collapsed row categories on the left. A selected checkbox adjacent to a right or category of rights indicates that Operators with the assigned role can perform the features/functions related to the right. The pre-defined roles cannot be modified, but you can create custom roles to enable a unique grouping of rights (see "Configure custom roles").

The following table lists the rights associated with each predefined role.

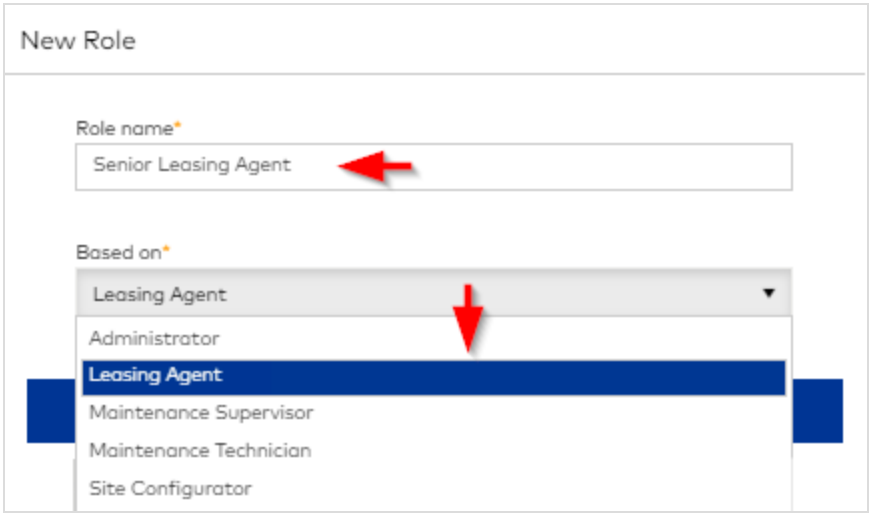
Role	System Rights	Key Rights
Administrator	All	All
Site Configurator	All	All
Leasing Agent	■ Read Keys ■ Resident Management	None
Maintenance Supervisor	■ Programming & Auditing ■ Read Keys ■ Remote Lock Management ■ Resident Management ■ Reports ■ System Keys > Diagnostic Keys	None
Maintenance Technician	■ Programming & Auditing ■ Read Keys ■ Reports ■ System Keys > Diagnostic Keys	None

Configure custom roles

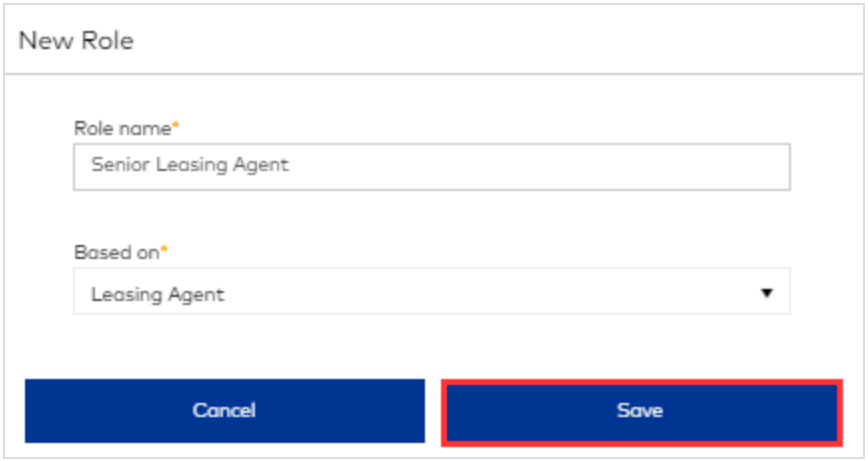
Custom roles offer the flexibility to authorize any combination of system and key rights.

To configure a custom role:

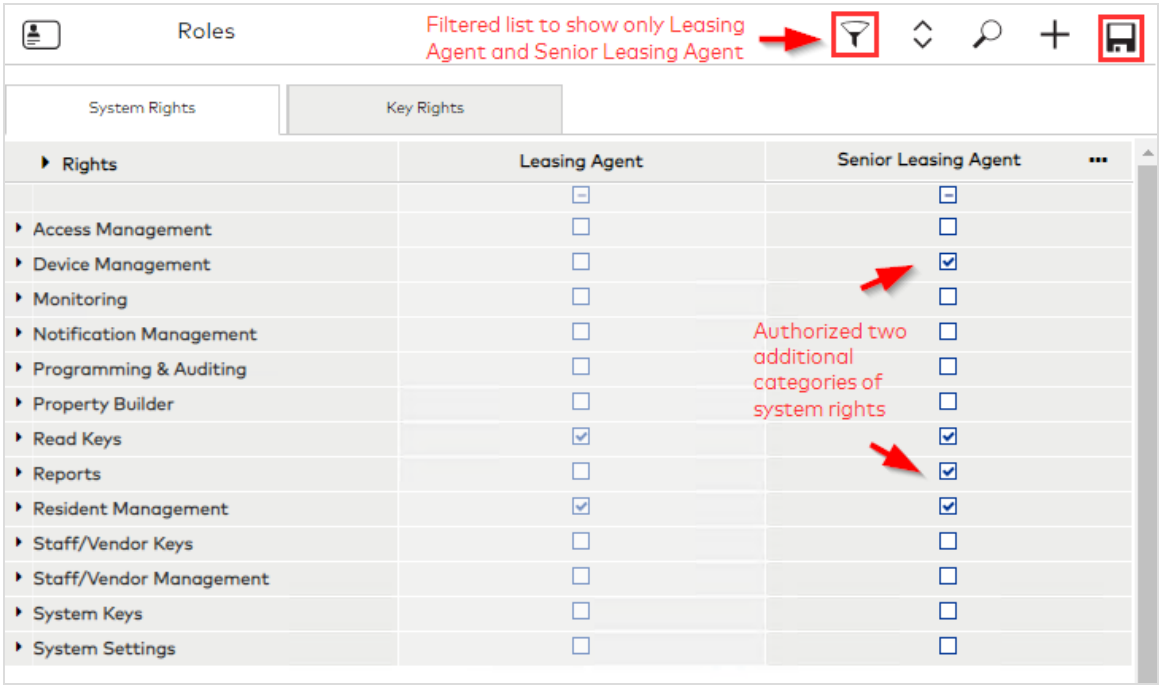
1. Go to **Role Management**.
2. Click **(Add)** +.



3. Specify a descriptive name for the role.
4. Select an existing role on which to base the new role. All rights associated with the role that you select apply to the new role but can be modified after creating the role.



5. Click **Save**.



6. Select or deselect rights for the new role on the **System Rights** and **Key Rights** tabs. If you select or deselect a category of rights, then all individual rights in the category are implicitly selected or deselected, respectively.
7. Click **(Save)** .

Step 7

Add Operators

This section includes the following subjects:

Learning about Staff/Vendor Management 131

Configure operators 133

Import staff/vendor list 138

Learning about Staff/Vendor Management

Staff and vendors are the key holders who work at or perform a service on the property. Most staff are people whose rights are limited to using the keys issued to them, for example, maintenance personnel. Some staff, however, require access to Community. The staff who have access to Community are called *Operators*.

A staff member is designated an Operator in the staff profile. The degree of access depends on the selected Operator role. For example, an Operator with the predefined *Administrator* role has access to all Community functions whereas the rights for an Operator with the predefined role *Leasing Agent* are limited to **Resident Management** and **Read Key** functions.

You can add staff/vendors manually or import a list.

Staff/vendor profiles

When a staff member or vendor is added to Community, a profile is created with the following tabs:

- **Staff/Vendor Info**—This tab is where basic identification details about staff/vendors are defined and notifications are enabled. The option to designate the staff member as an Operator is on this tab.
- **Operator Info**—This tab is where Operator access is configured. The tab is only active if the staff member is designated as an Operator.
- **Assigned Keys**—This tab lists active keys assigned to the staff member/vendor. You can cancel and/or replace keys in the list.
- **Visitor Management**—This tab is where PIN delegation can be enabled and configured for the staff member/vendor.

To view a staff member/vendor profile:

» Go to **Staff/Vendor Management** and select a staff member/vendor.

You can filter the list of profiles based on status (Active/Deactivated/Operators only).

Importing staff/vendors

If the *Import list* right is enabled in **Role Management**, you can create staff/vendor profiles by importing a CSV file that contains basic data (*firstname/lastname/ID*). Any additional information, including the option to designate Operators, must be specified manually in the staff/vendor profile. The *Import list* right is enabled by default for the Administrator and Site Configurator roles.

Visitor Management

Visitor management is a complimentary feature that works exclusively with AuroraSync and mobile keys. Visitor management to provides residents and staff the ability to extend all or part of their access to on-site visitors. Using the dormakaba BlueSky app, residents and staff can generate PIN codes to authorize perimeter and common area access. Residents also have the option to delegate mobile keys for visitors that can work on common doors and the resident's unit if desired.

A PIN is a 7-digit sequence that can be used at access points where a numeric keypad is installed. A delegated mobile key (or PIN code in mobile key format) provides access using the dormakaba BlueSky app.

When Visitor Management is enabled in System Settings for staff/vendors, PIN delegation can be enabled/disabled on the Visitor Management tab in staff/vendor profiles. When Visitor Management is enabled in System Settings for residents, PIN and mobile key delegation can be enabled/disabled on the Visitor Management tab in resident profiles.

Prerequisites include:

- AuroraSync must be enabled and configured.
- Mobile keys must be enabled and configured.
- The resident profile must include a valid mobile number.
- The dormakaba BlueSky app must be installed and registered on the mobile device used to generate PIN code/mobile key.

Staff/vendor keys

Staff/vendor keys are made and issued to people who work on the site, which may include employees, contractors and vendors. Staff/vendor keys are encoded with a credential defined in **Access Management > Credential Management** that may include access to all access point types: units, suites, common areas (resident and staff), and restricted areas.

Staff/vendor keys are made in the **Staff/Vendor Keys** module. Key instances are subsequently managed in **Staff/Vendor Management** by selecting the staff/vendor to whom the key (instance) was assigned and then the **Assigned Keys** tab in the profile.

Staff/vendor keys are valid in staff and resident common areas and elevator controllers until key expiration is reached. Note that staff/vendor keys with the status Obsolete continue to allow access to common areas and elevator controllers until key expiration. To maintain security for keys with an obsolete status, create a block key for the key sequence. See System Settings > Block Keys.

For information about invalidating staff access, see Invalidating staff access.

Configure operators

The first step to configuring operators is to add staff members. You can add staff members manually or, if the *Import staff list* right is enabled in Role Management, you can import staff members. The import is limited to creating staff profiles with basic data: *firstname*/*lastname*/*ID*.

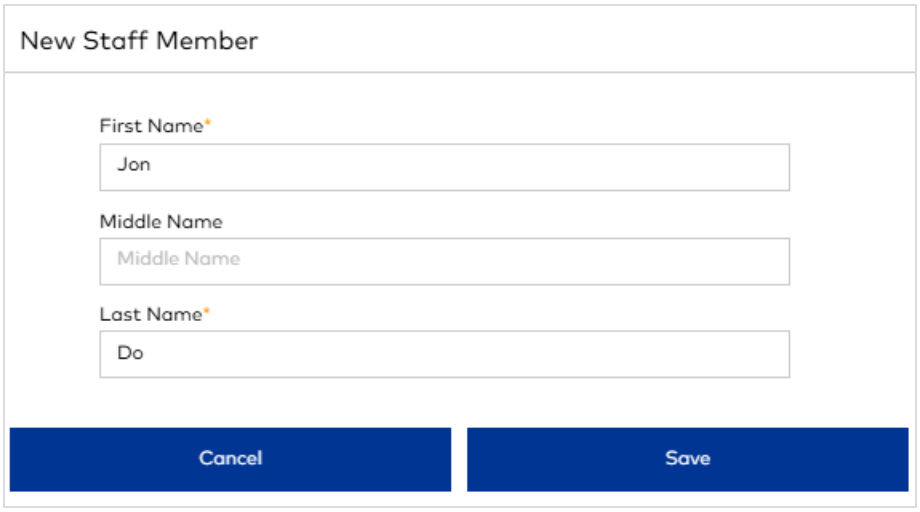
Unless otherwise indicated, creating and managing operators requires Staff Management system rights. By default, the Administrator, Site Configurator, and Staff Manager roles have default access.

- Add staff member
- Designate staff member an operator
- Select / change default software language for operator
- Assign / change operator role
- Change operator login password (SSO disabled only)
- Add / update Maintenance Unit credentials
- Add / update API login credentials

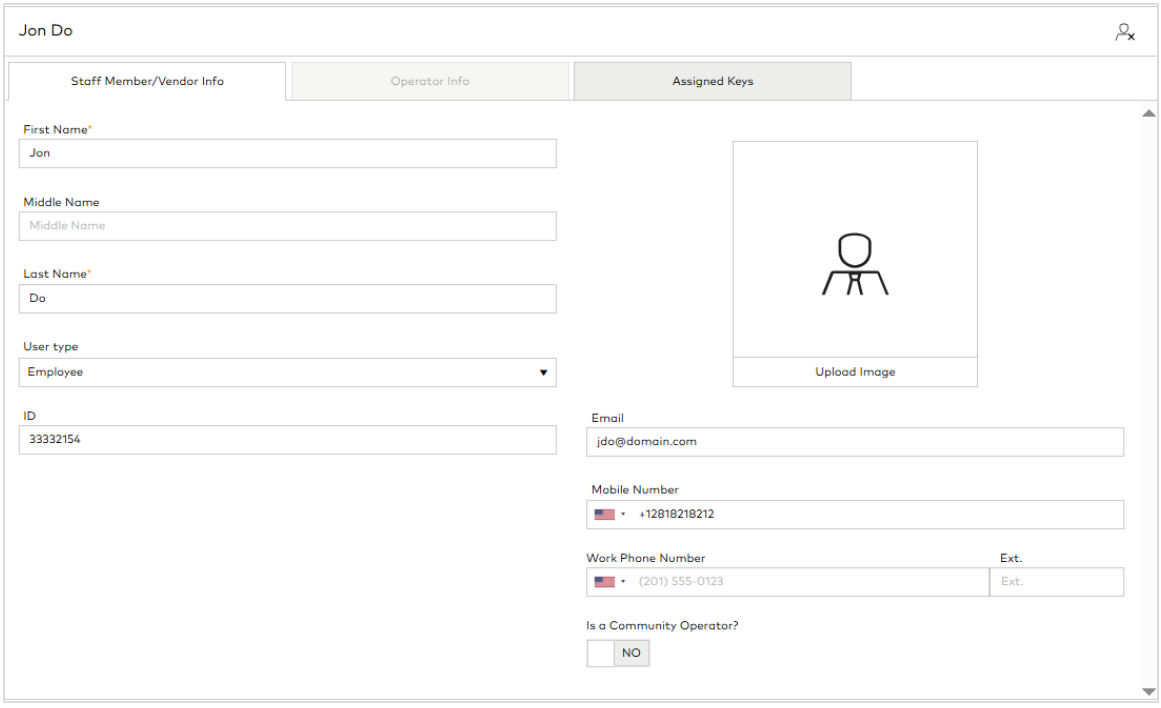
Add staff member

To add a staff member:

1. Go to **Staff/Vendor Management**.
2. Click **(Add)** .



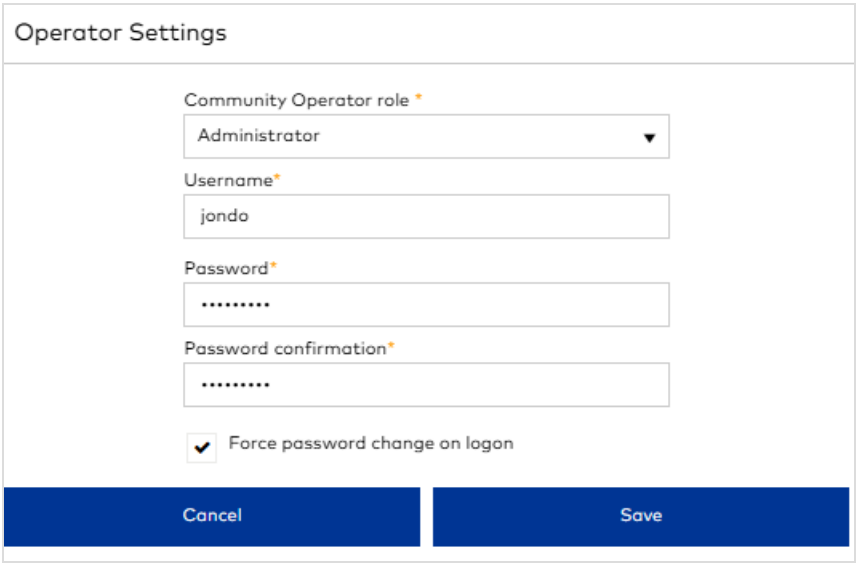
3. Specify the name of the staff member. Use the middle name to distinguish between staff with the same first and last names. Max chars per field: 25.
4. Click **Save**. Community creates a profile and displays the **Staff/Vendor Info** tab.



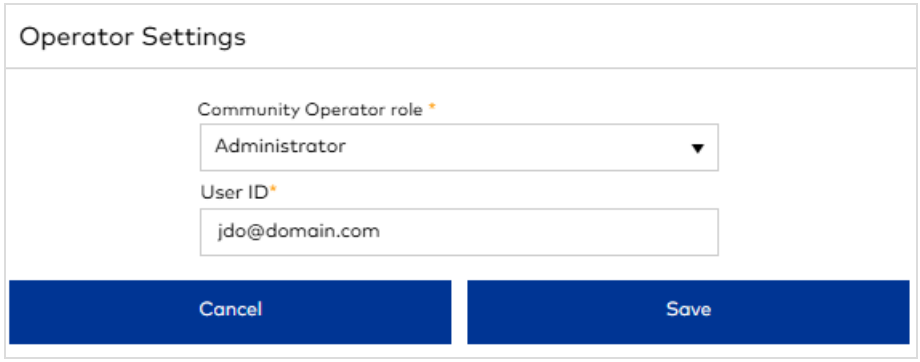
5. Specify a valid email address. An email address is required to send automated emails regarding account access. Alternatively, operators can specify or change the email address in account Preferences after logging in to Community.
6. Click **Save**.

Designate staff member as operator

1. Go to **Staff/Vendor Management** and select a staff/vendor profile.
2. On the Staff Member/Vendor Info tab, set the **Is a Community Operator** switch to **YES**.
   - SSO is disabled.

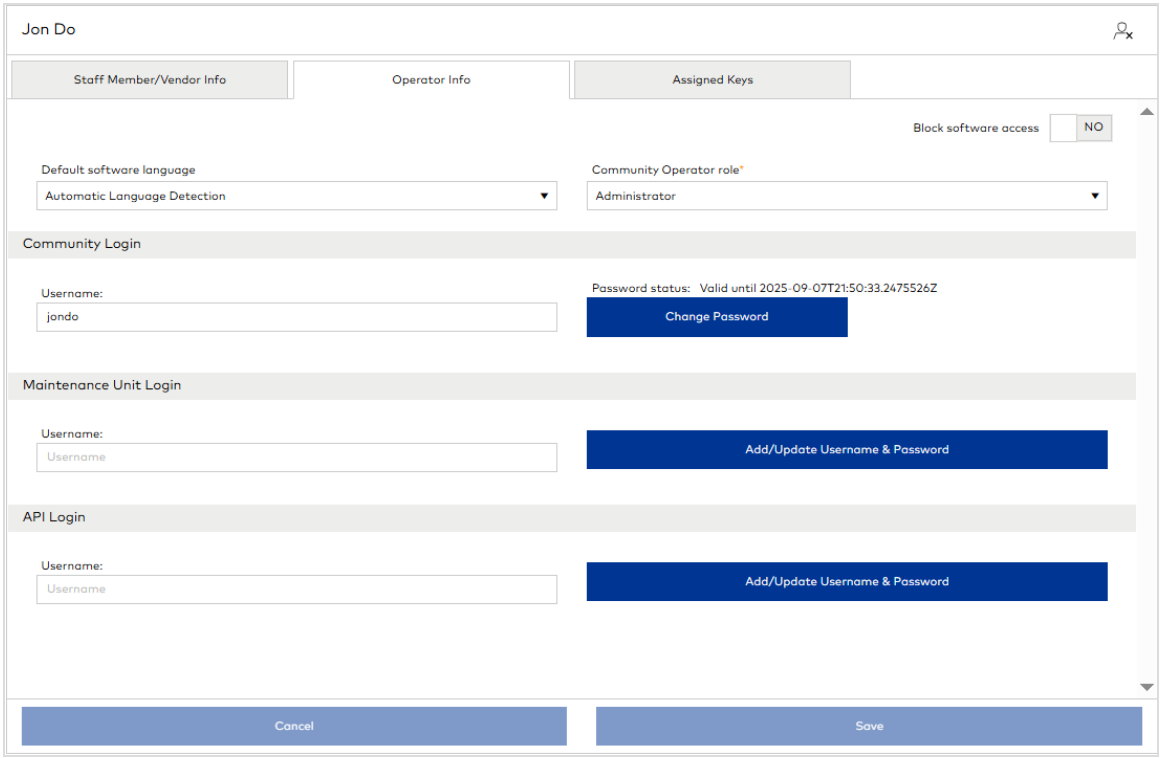


- SSO is enabled.

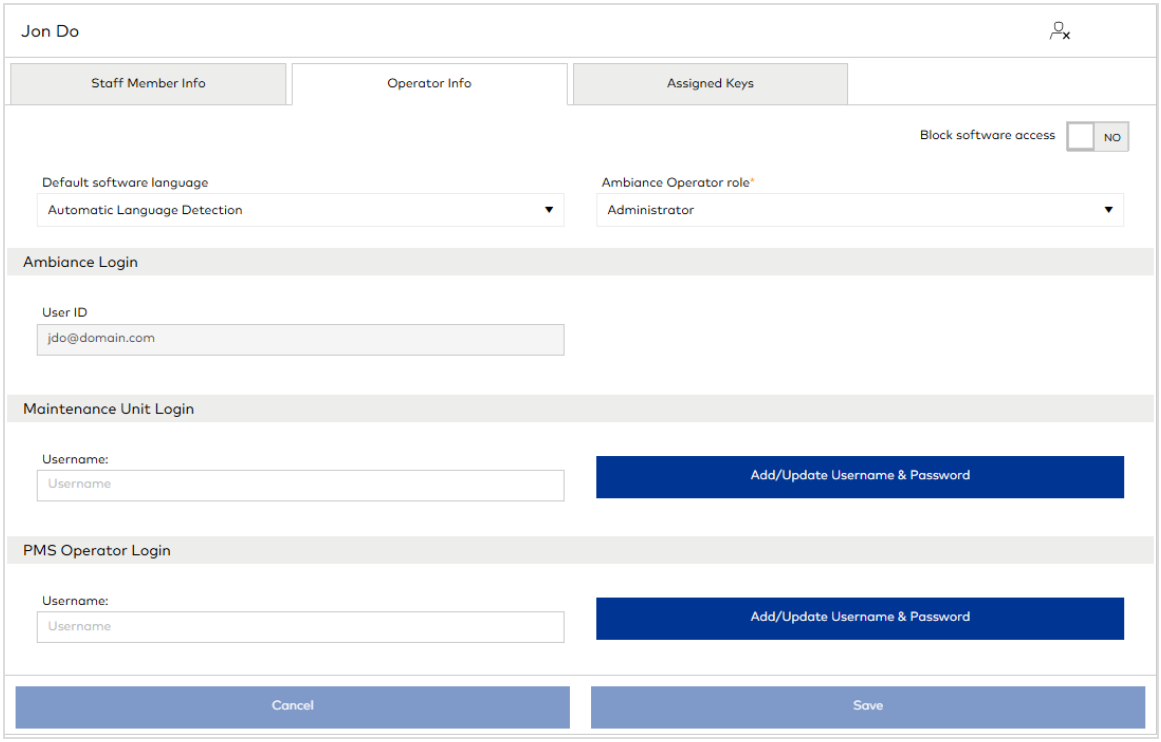


3. Select an operator role. The list of roles is populated by the roles created in the **Role Management** module.
4. Choose one of the following:
   - SSO is disabled.
     - Specify a unique username for the operator.
     - Specify and confirm a password for the operator.
     - (*recommended*) To force the operator to change the password upon initial login, select **Force password change on logon**.
   - SSO is enabled.
     - Specify a unique User ID for the operator. The value can be a valid email address or EID (Enterprise ID). Automatically populated if a value is defined for Email on the Staff Member/Vendor Info tab.
5. Click **Save**. The Operator Info tab is enabled. Refer to the following sections to configure additional options.

SSO is disabled:



SSO is enabled:



Select / change default software language

1. Go to **Staff/Vendor Management** and select a staff/vendor profile.
2. Click the **Operator Info** tab.
3. Select the default software language. The operator can change the language in account **Preferences**.
4. Click **Save**.

Assign / change operator role

1. Go to **Staff/Vendor Management** and select a staff/vendor profile.
2. Click the **Operator Info** tab.
3. Select an operator role. The list of roles is populated by the roles created in the **Role Management** module.
4. Click **Save**.

Change operator login password (SSO disabled only)

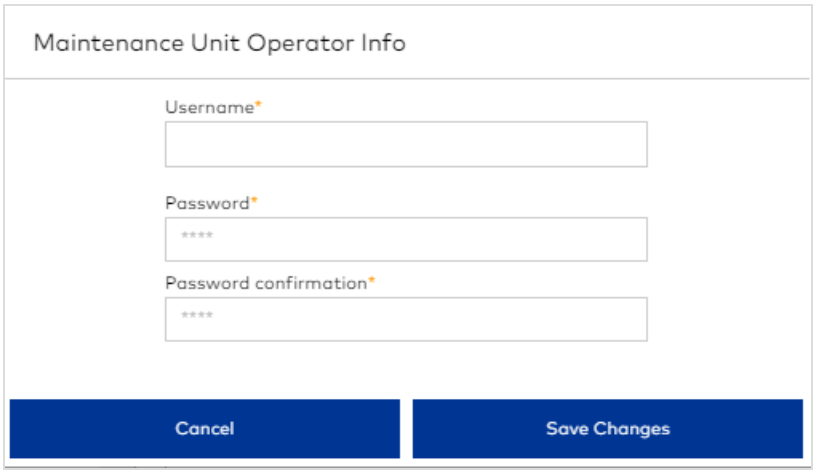
Only available when SSO is disabled.

1. Go to **Staff/Vendor Management** and select a staff/vendor profile.
2. Click the **Operator Info** tab.
3. In the Community Login section, click **Change Password**. Specify and confirm a new password, then click **Save**. You must communicate account credentials to the operator.
4. To force the operator to change the password upon initial login, select **Force password change on logon**. This setting is enforced the first time a new operator logs in.
5. Click **Save**.

Add / update Maintenane Unit login credentials

When Maintenance Unit (M-Unit) authentication is enabled, the **Maintenance Unit Login** section displays. Credentials must be configured for at least one operator. To disable M-Unit authentication, see "Maintenance Unit Authentication."

1. Go to **Staff/Vendor Management** and select a staff/vendor profile.
2. Click the **Operator Info** tab.
3. In the Maintenance Unit Login section, click **Add/Update Username & Password**.

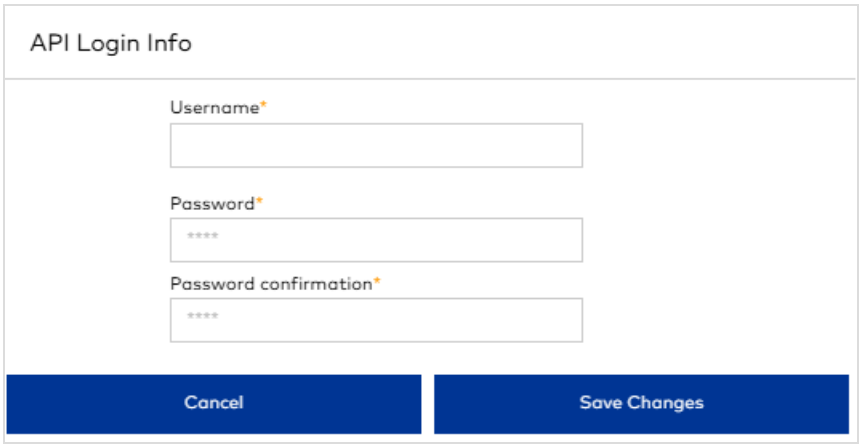


4. Specify a username.
5. Specify and confirm a password.
6. Click **Save Changes**.

Add / update API login credentials

When API login authentication is enabled, the API Login Login section displays. Credentials must be configured for at least one operator. To disable API authentication, see **System Settings > Security > API integration**.

1. Go to **Staff/Vendor Management** and select a staff/vendor profile.
2. Click the Operator Info tab.
3. In the API Login section, click **Add/Update Username & Password**.

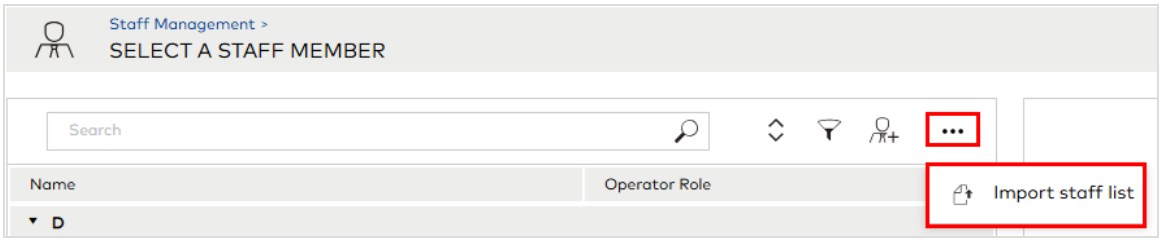


4. Specify a username.
5. Specify and confirm a password.
6. Click **Save Changes**.

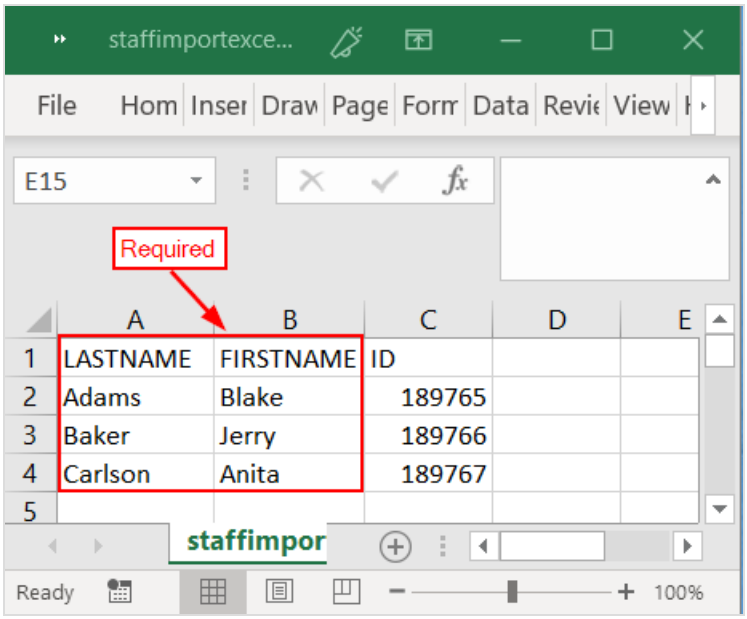
Import staff/vendor list

To import staff/vendors:

1. Go to **Staff/Vendor Management**.
2. Click **(More)** ▪▪▪ > **Import staff list**.

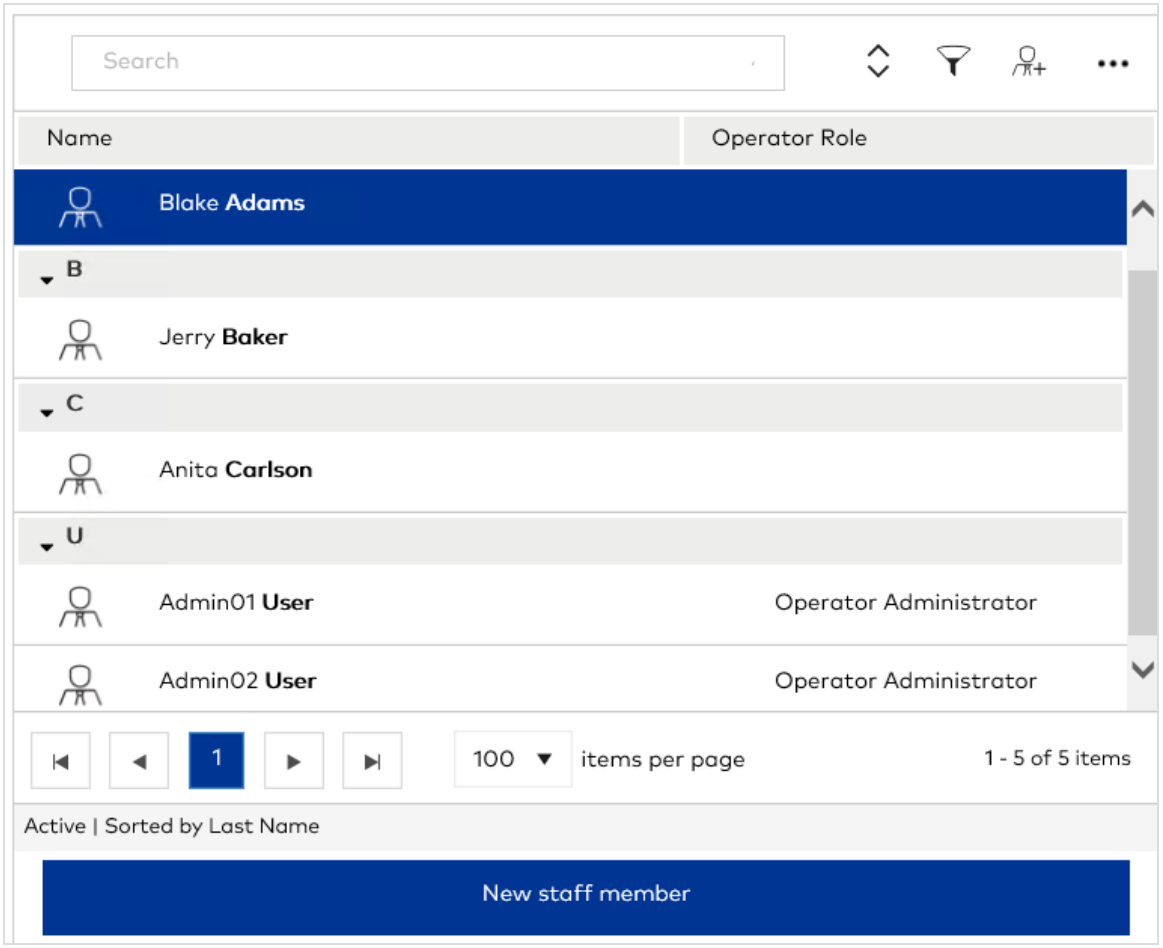


3. Navigate to and select the file that you want to import, then click **Open**. Supported files type: csv. The following figure shows a sample file and the required data format. If a required field is missing, the staff member/vendor is not added.



> If staff member profiles have already been created, you are prompted to proceed. Click **YES** to proceed.

4. When notified the import is successful, click **OK**.


Search
Name
Operator Role
Blake Adams
B
Jerry Baker
C
Anita Carlson
U
Admin01 User
Operator Administrator
Admin02 User
Operator Administrator
1
100
items per page
1 - 5 of 5 items
Active | Sorted by Last Name
New staff member

Use Community

This section includes the following subjects:

Resident Management 143
- Learning about Resident Management 144
- Add residents 151
- Import resident list 153
- Assign units 155
- Make Resident Keys 162
- Modify Resident Access 165
- Invalidate resident access 171
- Make keys for common area access only 178
- Make mobile keys for multiple residents 180
- Configure Visitor Management for residents 182

Staff and Vendor Management 184
- Learning about Staff/Vendor Management and Staff/Vendor Keys 185
- Add staff members/vendors 187
- Import staff/vendor list 189
- Make Emergency keys 191
- Make Staff key (predefined access) 194
- Make Staff Keys (variable access) 198
- Make Vendor keys 202
- Make Limited Use keys 206
- Replace Staff/Vendor Keys 210
- Invalidate staff/vendor access 212
- Configure Visitor Management for staff/vendors 217

Programming/Auditing 218
- Reprogram locks 219
- Audit locks 221

Audit online access points 222
System Keys 223
Learning about System Keys 224
Block and unblock keys 227
Cancel keys 231
Diagnostic keys 233
Electronic lockout keys 235
Failsafe keys 237
Inhibit keys 238
Latch and unlatch keys 240
Primary and secondary program keys 242
Resequence keys 245
Special function keys 247
Monitoring 248
Learning about Monitoring 249
Monitor keys 250
Monitor digital key usage 251
Reports 253
Access Point Audit Report 254
Credential/Access Point Assignment Report 256
Elevator Configuration Report 257
Key Expiration Report 258
Key/User Assignment Report 259
Operator Report 260
Property Configuration Report 261
Roles and Rights Report 262
Staff/Vendor Access Report 263
System Activity Report 264
Visitor Management Report 267
Toolbar Basics 268
Navigate Community 269
Set operator preferences 271
Install / update Community Client 273
Select default encoder 274
Remote unlock/lock 275

Read key/erase key/access tracking report 277
View notifications 281
Physical keys 283
Digital keys 285

Residents

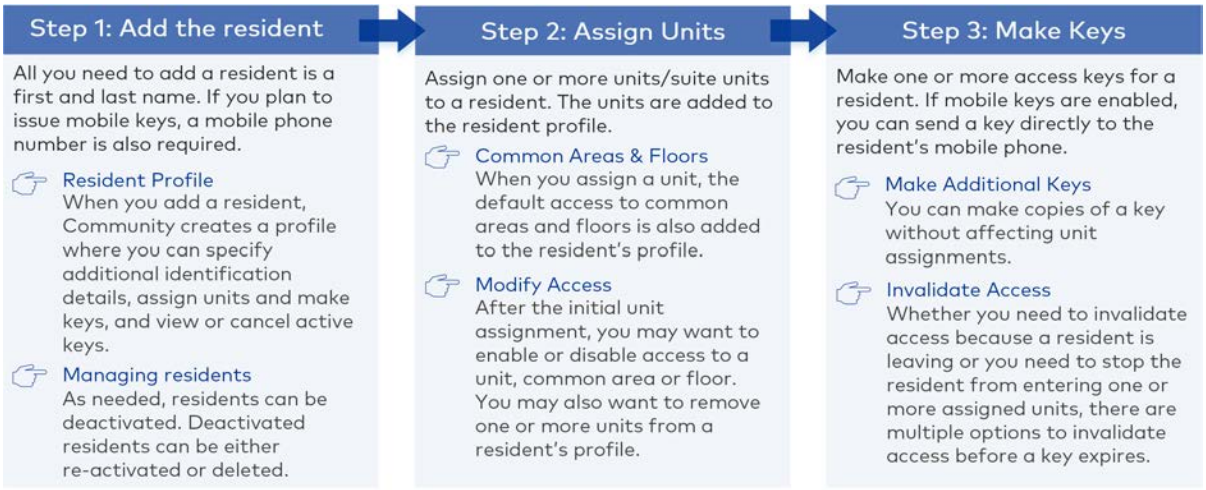
Resident Management

This section includes the following subjects:

Learning about Resident Management 144
Add residents 151
Import resident list 153
Assign units 155
Make Resident Keys 162
Modify Resident Access 165
Invalidate resident access 171
Make keys for common area access only 178
Make mobile keys for multiple residents 180
Configure Visitor Management for residents 182

Learning about Resident Management

The Resident Management module is where you add residents to Community, configure and manage resident access, and make or cancel resident keys. The following figure summarizes the steps.

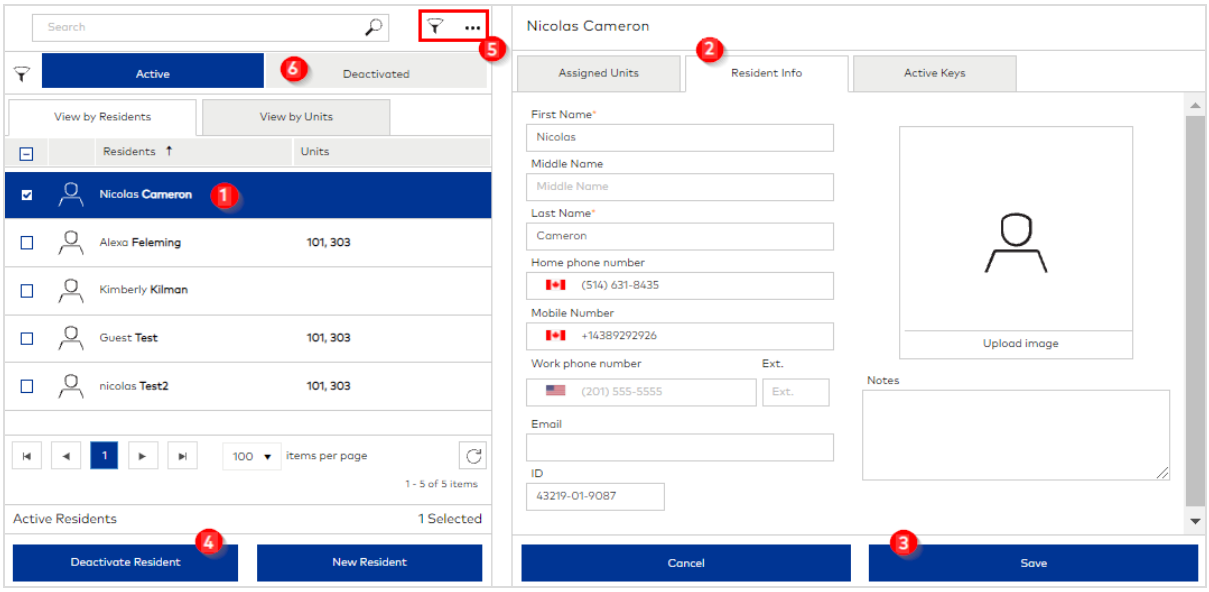


If Visitor Management is enabled for residents, you can also configure PIN and/or mobile key delegation settings for the resident.

If Aurora is enabled, the Perimeter FOB tab displays. For more information, refer to *Community-Aurora-Integration*, PK3769.

Adding residents

Residents can be added individually or by batch import. After adding residents, optional identification details can be specified on the **Resident Info** tab.



Refer to the figure above and the following reference list to learn more about adding a resident and the actions that you can take after adding a resident.

1: A new resident is added to the list of active residents.

2: The profile opens on the **Resident Info** tab.

3: After adding more details, such as an ID, click **Save**.

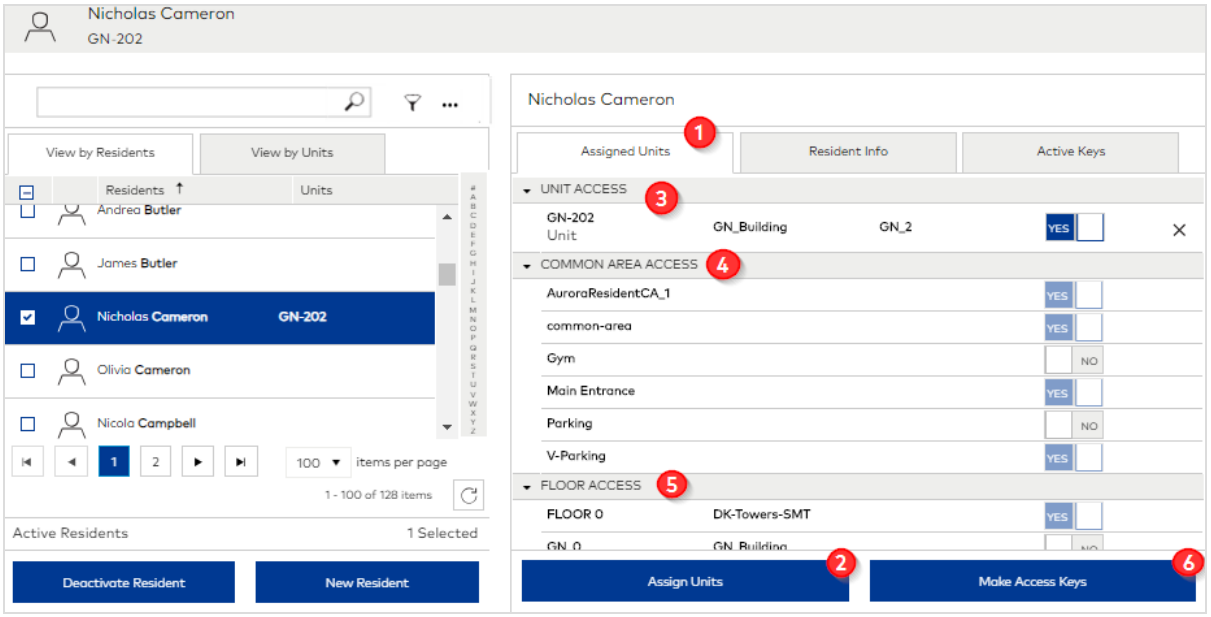
4: Click **Deactivate** to deactivate selected residents.

5: Click the (Filter) to show the **Active** and **Deactivated** tabs. Click **(More) ...** to import a resident list.

6: Deactivated residents are listed here; you can either reactivate or delete deactivated residents.

Assigning units and making keys

Configuring access for a resident involves assigning units and enabling or disabling associated access points, such as common areas and floors. The resulting configuration creates the credential to encode on access keys.



1: Resident access can be configured and managed on the **Assigned Units** tab in the resident's profile. You can assign units, modify access and make access keys. You can also configure access to commons areas without assigning a unit.

2: When you click **Assign Units**, you can add a unit to the resident's profile. Filtering options show where the unit is located and whether it is occupied or vacant. You can assign an occupied unit to another resident, but sharing policies apply. For more information about built-in sharing policies, see Shared resident access.

When units are shared among two or more residents, modifying access for one resident may also modify access for the residents who share access. When changes to access for one resident affect other residents, the Community messaging system lists all residents affected by the change.

3: The **UNIT ACCESS** section lists assigned units. Access is enabled by default. At any time, you can enable or disable access to any unit in the profile.

4: The **COMMON AREA ACCESS** section lists all unlimited and limited common areas. Access to unlimited common areas is set to **YES** and cannot be disabled. Access to limited common areas can be enabled and disabled. The default access depends on whether a unit is assigned and, if so, the Common Area Access profile associated with the assigned units. If no units are assigned, the default access for limited common areas is set to **NO**. When at least one unit is assigned, limited common areas that are enabled by default in the Resident Common Area Access profile associated with assigned units are enabled. Any limited common areas that were previously enabled (prior to assigning a unit) remain enabled after assigning a unit.

5: The **FLOOR ACCESS** section lists all floors for the buildings in which the resident is assigned a unit. By default, access is enabled for floors on which resident access to units is enabled, but access to any floors in the list can be enabled or disabled.

The FLOOR ACCESS section displays only if the **Floor access** option is enabled (**System Settings > Residents**).

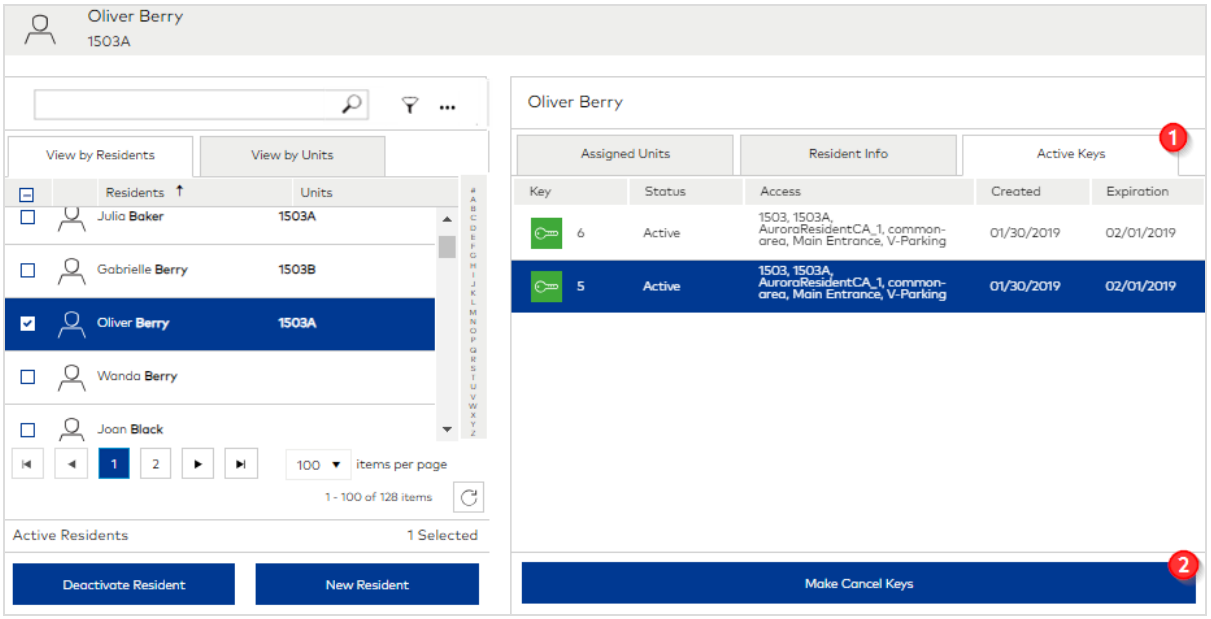
6: When you click **Make Access Keys**, you can make physical keys and/or mobile keys. Using mobile keys is a licensed feature that must be enabled in **System Settings**.

- Resident keys are valid in resident common areas until key expiration or until a New key for the same unit/s is presented to the respecrive lock/s.
- Resident keys are valid in elevator controllers until key expiration.

If necessary, the Block Key can be used to invalidate access to all access point types; however, after the Block Key is presented to the respective locks, the Unblock Key will not restore access to common areas.

Active keys

The active keys assigned to a resident are listed on the **Active Keys** tab in the resident's profile. At any time, you can check the status of a key or cancel a key.

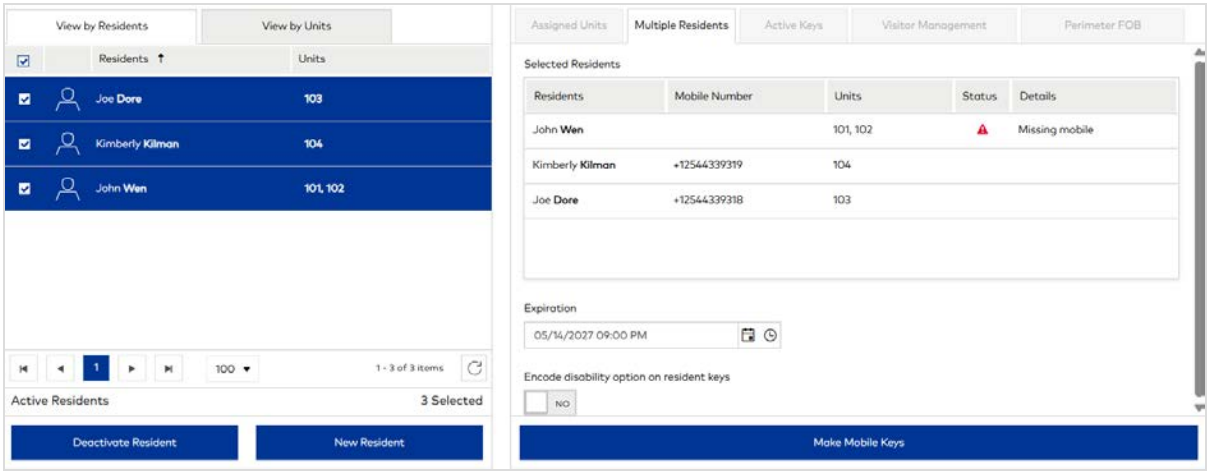


1: The **Active Keys** tab lists all active keys for the selected resident.

2: Any physical Cancel Keys that you make for an active key instance must be presented to the lock installed at each access point (units and common areas) before access is canceled. If canceling mobiles keys is enabled in **System Settings**, you can send the Cancel Key directly to the resident's mobile phone.

Multiple Residents

When two or more residents are selected on the **View by Residents** tab, the **Multiple Residents** tab displays. Make mobile keys for multiple residents at the same time. Each resident must have a valid mobile phone number and at least one unit assignment.

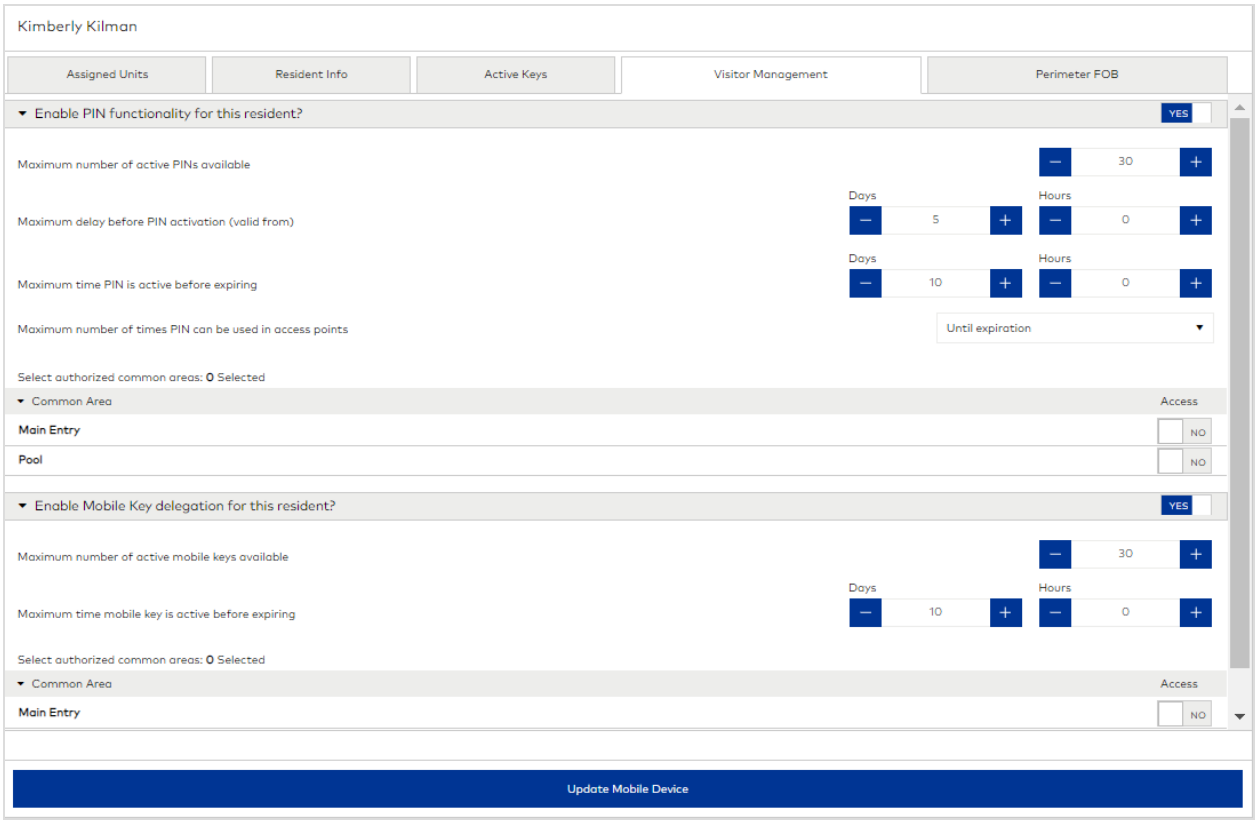


Visitor management

Visitor management is a complimentary feature that works exclusively with AuroraSync and mobile keys to provide residents with the ability to extend all or part of their access to on-site visitors. Using the dormakaba BlueSky app, residents can generate PIN codes and mobile keys to authorize perimeter and common area access.

- A PIN is a 7-digit sequence that can be used at access points where a numeric keypad is installed.
- A delegated mobile key (or PIN code in mobile key format) provides access using the dormakaba BlueSky app.

When Visitor Management is enabled for residents in **System Settings**, PIN and mobile key delegation can be enabled/disabled on the **Visitor Management** tab in resident profile.

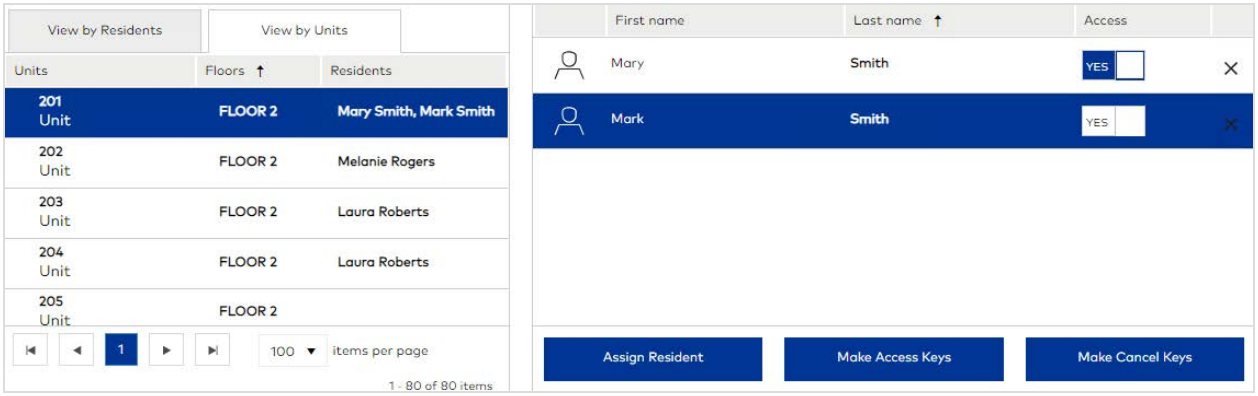


Prerequisites include:

- AuroraSync must be enabled and configured.
- Mobile keys must be enabled and configured.
- The resident profile must include a valid mobile number.
- The dormakaba BlueSky app must be installed and registered on the mobile device used to generate PIN code/mobile key.

Units view

An alternative to managing resident access in the resident profile is to view a list of all units on the **View by Units** tab. When you select a unit in the list, all residents assigned to the unit are listed. You can assign a new or existing resident to the unit, enable or disable resident access to the unit, unassign the resident from the unit, and make access and cancel keys for the selected resident.



Shared resident access

Community sharing is based on how units are grouped. Unit groups are created and operate in the background. When a vacant unit is assigned to a resident who has no other assigned units, a group is created. When a second vacant unit is assigned to a different resident who has no other assigned units, a second group is created.

John is a new resident. Vacant Unit 100 is assigned to John. This action creates a group (GroupA) with one unit (100). Lisa is also a new resident. Vacant Unit 101 is assigned to Lisa. This action creates a second group (GroupB).

Because the typical scenario is one unit per resident, most groups contain only one unit. However, when multiple residents share more than one unit, changes to access for one resident may affect all other residents who share access.

There are three policies that control sharing:

- A unit can only be in one group.
- A resident can only be assigned units from one group.
- Each resident who is assigned at least one unit in a group is assigned all units in the group; however, access to each unit in the group can be enabled or disabled in the individual resident profiles.

Community filters the selection lists of residents and units to enforce the sharing policies.

With Unit 100 (GroupA) assigned to John and Unit 101 (GroupB) assigned to Lisa, Community excludes Unit 101 in the selection list of units when assigning units to John. Likewise, Community excludes Unit 100 in the selection list of units when assigning units to Lisa. The units are in two different groups.

Let's look at what is allowable and how the sharing polices apply.

Assigning units to a resident

You can assign a unit to a resident when:

- The unit is vacant and the resident has no other units assigned.

Vacant Unit 100 is assigned to John. Unit group GroupA is created.

- The unit is occupied and the resident has no other assigned units.

Unit 100 is assigned to Mark. John and Mark share Unit 100. Both residents are assigned a unit in GroupA.

- The unit is vacant and the resident shares access to other units. In this case, each resident who is assigned at least one unit in a group is assigned all units in the group.

Unit 102 is assigned to Mark. Because Mark shares access with John, Community messaging informs that Unit 102 will also be assigned to John. If you proceed, Unit 102 is added to the resident profiles for John and Mark with access enabled.

Removing resident access

There are three ways to remove resident access to assigned units:

- Delete the unit from the resident profile
- Delete the resident from the unit profile
- Disable access to the unit in the resident profile

The appropriate method to choose depends on whether you want to temporarily suspend or permanently remove access; and, whether the unit is one of at least two units shared by multiple residents.

- If you are temporarily suspending access, it makes sense to disable access to the unit in the resident profile.
- If you want to permanently remove access, then delete the unit from the resident profile (or delete the resident from the unit profile).

To help you decide whether to delete or disable, understand that when a unit is one of at least two units shared by multiple residents, deleting a unit from a resident profile (or deleting a resident from the unit profile) removes the unit for all residents who share access.

John and Mark share Units 100, 101, 102. Removing Unit 101 from John's profile removes Unit 101 from Mark's profile.

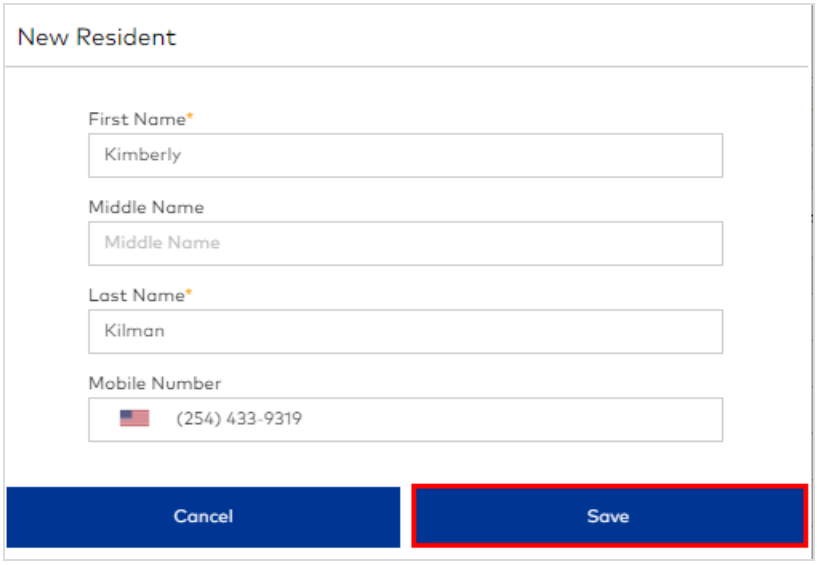
Add residents

Adding a new resident to Community requires only a first and last name. If the deployment plan includes issuing mobile keys, specifying a mobile phone number is required. For each resident that you add, Community generates a resident profile. All data about the resident, including identification details, unit assignments and active keys, are configured and managed in the resident profile. Upon defining a new resident, the profile opens to the **Resident Info** tab where optional details about the resident can be specified.

To import resident information, see Import resident list.

To add residents:

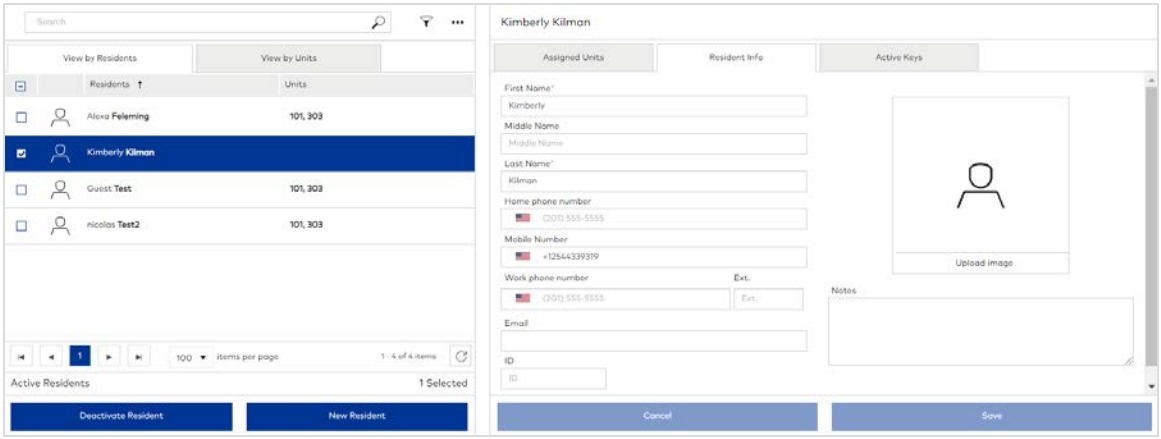
1. Go to **Resident Management**.
2. Click **New Resident**.



3. Specify the first and last names. Although the middle name is not required, use the field to distinguish people with the same first and last names. Max chars per field: 25.
4. (*conditional*) If you plan to issue mobile keys, specify the complete mobile phone number including country and area codes. The mobile number is required to issue mobile keys.
5. (*optional*) Specify additional phone numbers, a unique identification code (max chars: 100), notes (max chars; 2,000) and upload an image.

If phone/mobile number validation override is enabled in **System Settings**, Operators can permit use of unknown numbers.

6. Specify a valid email address for the resident.
7. Click **Save**.

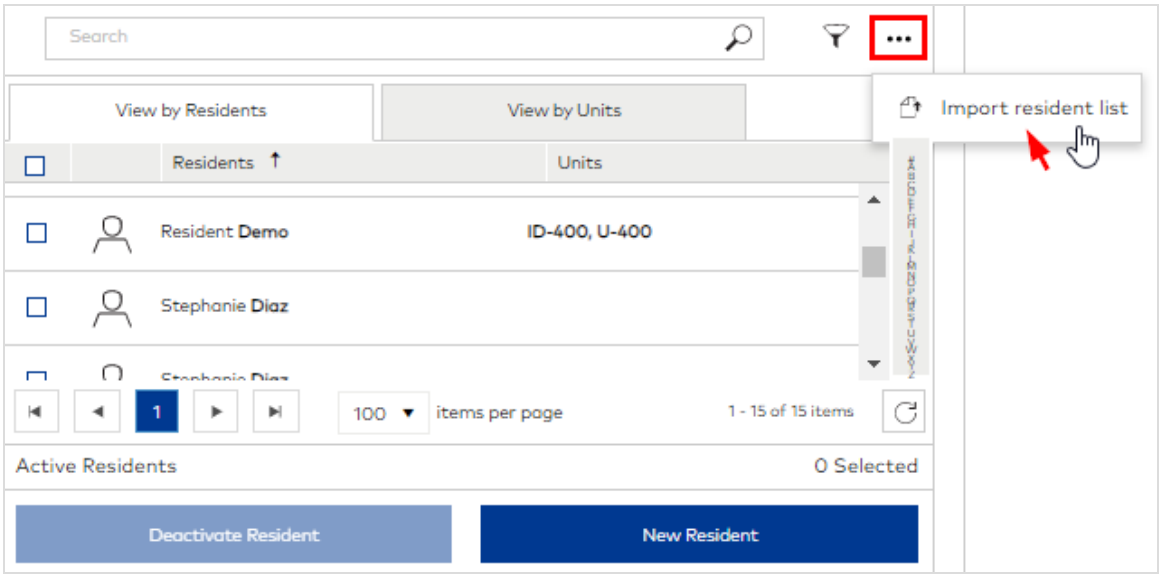

Search
View by Residents
View by Units
Residents
Units
Alexa Feleming
101, 303
Kimberly Kilman
Guest Test
101, 303
nicolas Test2
101, 303
items per page
Active Residents
1 Selected
Deactivate Resident
New Resident
Kimberly Kilman
Assigned Units
Resident Info
Active Keys
First Name*
Kimberly
Middle Name
Last Name*
Kilman
Home phone number
Mobile Number
+12544339319
Work phone number
Ext.
Email
ID
Upload image
Notes
Cancel
Save

Import resident list

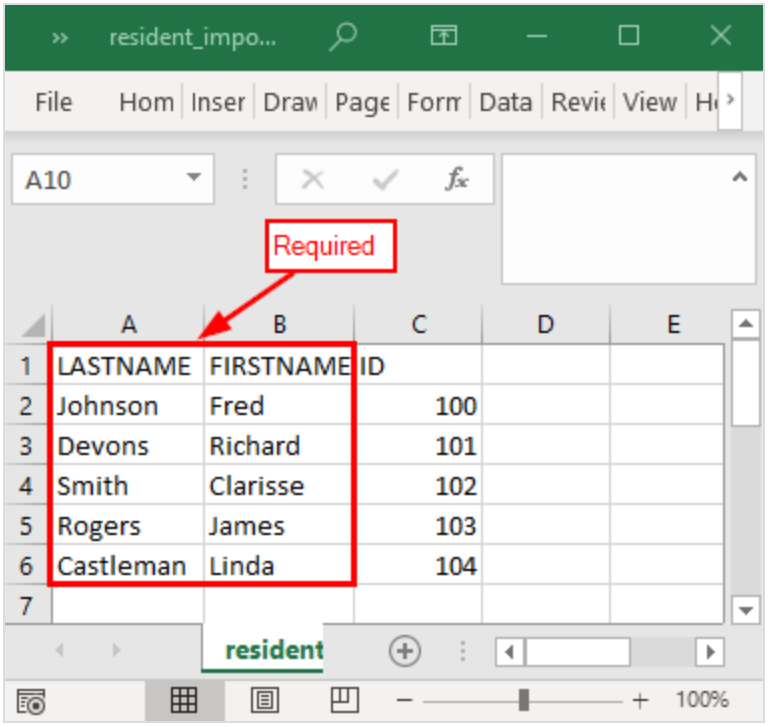
Use the provided import template to ensure format requirements. Download the template from the Context Help / Resident Management home page.

To import residents:

1. Prepare the import file.
2. Go to **Resident Management**.
3. Click **(More)** ▪▪▪ > **Import resident list**.

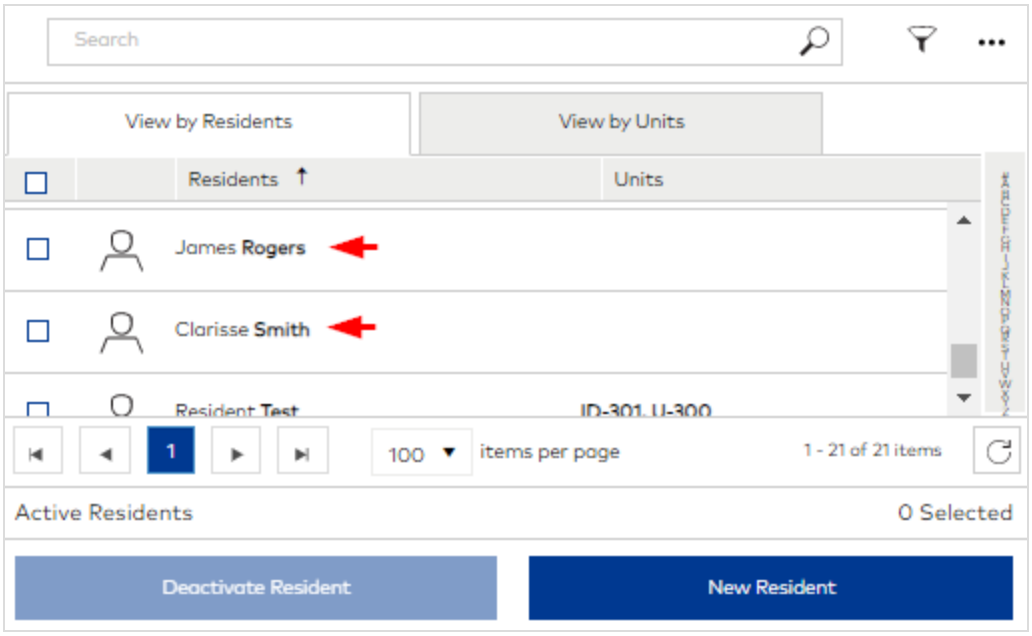


4. Navigate to and select the file that you want to import, then click **Open**. Supported files type: csv (.csv UTF-8 for non-English languages). The following figure shows a sample file and the required data format. If a required field is missing, the resident is not added.



If the LASTNAME/FIRSTNAME pair in existing resident profiles match data in the import file, duplicate profiles are created.

5. When notified the import is successful, click **OK**.

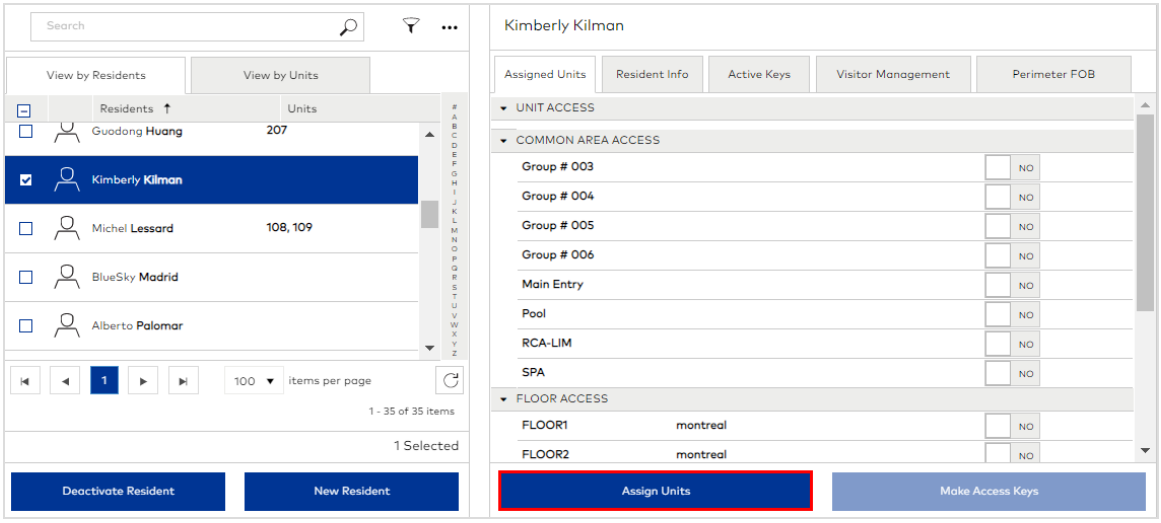


Assign units

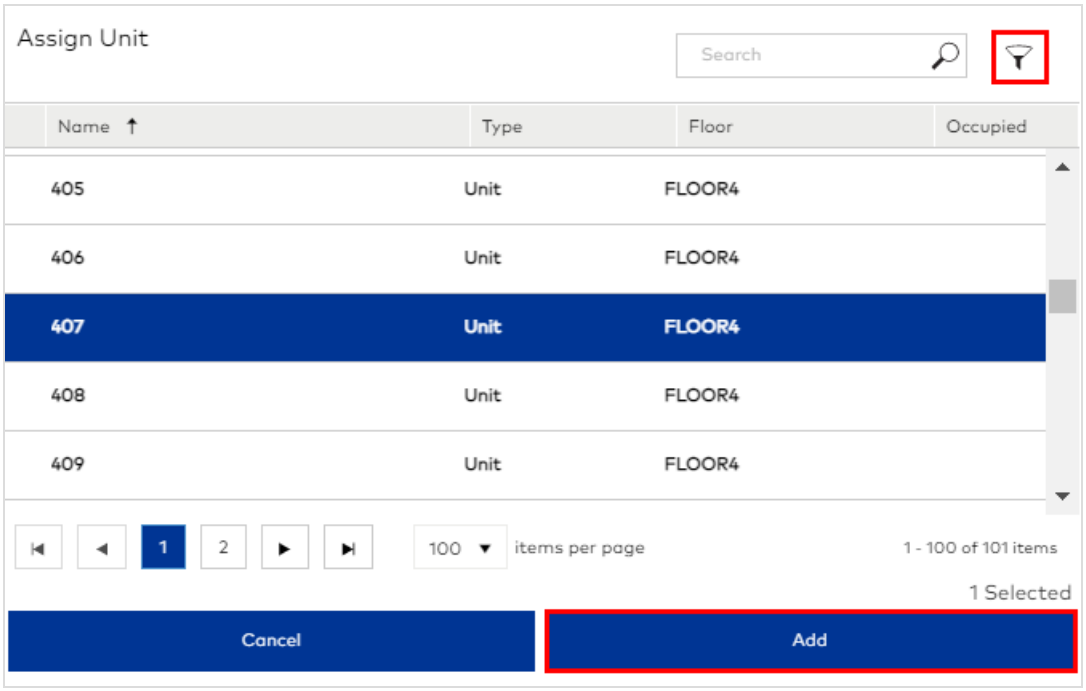
You can assign units to residents from the **View by Residents** tab and you can assign residents to units on the **View by Units** tab. The simplest and most common scenario is that each resident is assigned a single and unique unit. However, Community supports shared access so that one or multiple residents can be assigned to one or multiple units.

View by residents

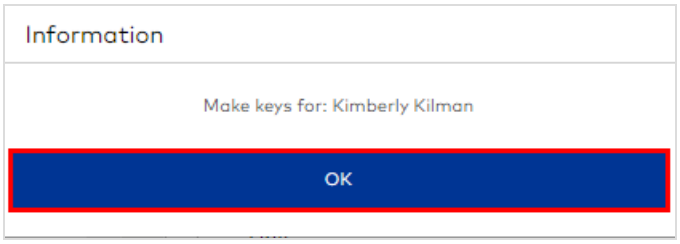
1. Go to **Resident Management**.
2. Select a resident.
3. Click the **Assigned Units** tab.



4. Click **Assign Units**.



5. Select a unit.
   - You can select units from different buildings.
   - You can filter the list by room type, floor and occupancy.
6. Click **Add**.

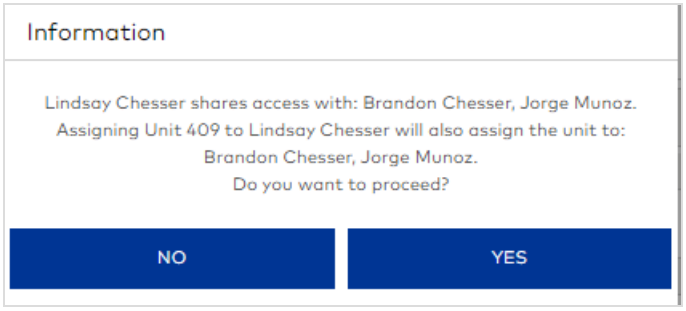


7. When notified about the keys that you need to make, click **OK**.

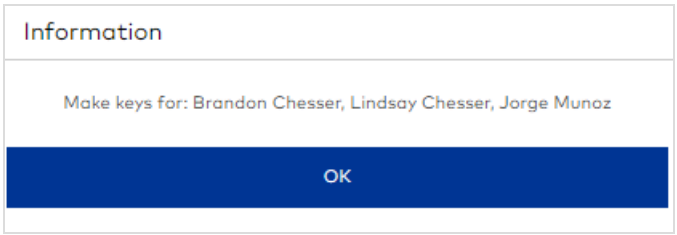
> Every time a change to access is made, Community issues a message that lists the names of residents for whom keys need to be made. If these messages do not display, change the option **Display key warning messages** in **System Settings > Resident** to **YES**.

Assigning units when residents share access

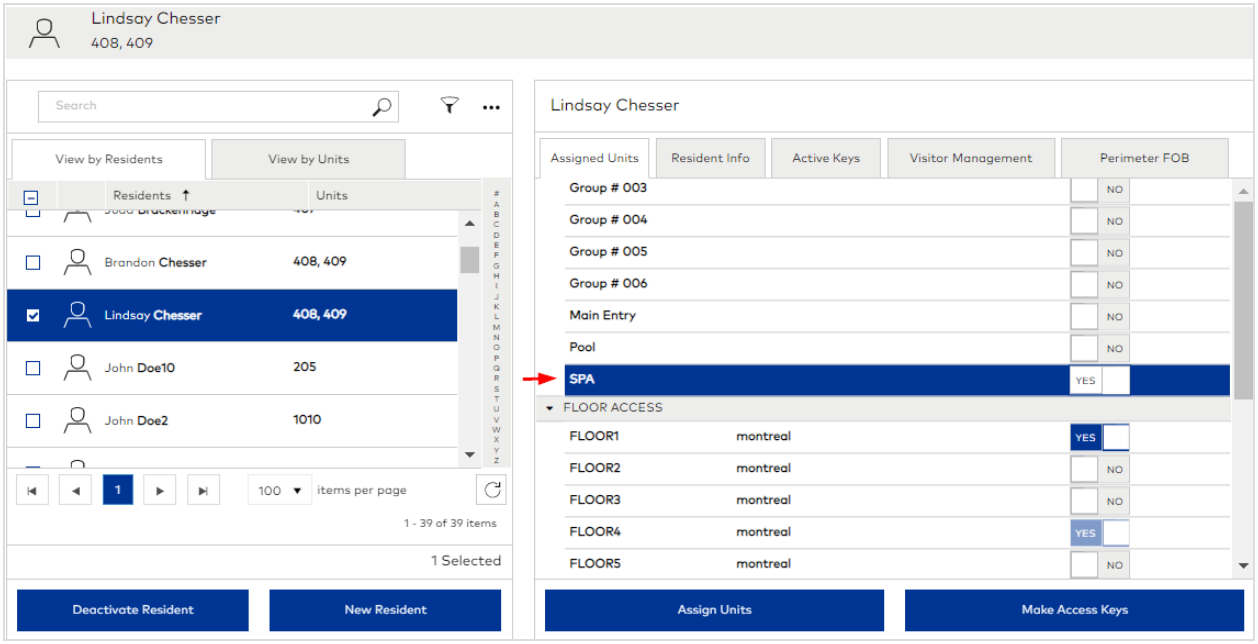
When you assign a unit to a resident who shares access, you must extend access to all residents who share access.



When you select **YES**, Community adds the unit (with access enabled) to the resident profiles for all residents who share access. Community also notifies you about the keys that you need to make.



If you want all affected residents to have access to the unit, click **OK** and make keys for each resident. However, you can make additional changes, such as adding/removing access to common areas, in individual resident profiles before making keys.



Assigning Occupied Units

You can only assign occupied units to residents who have no other unit assignments.

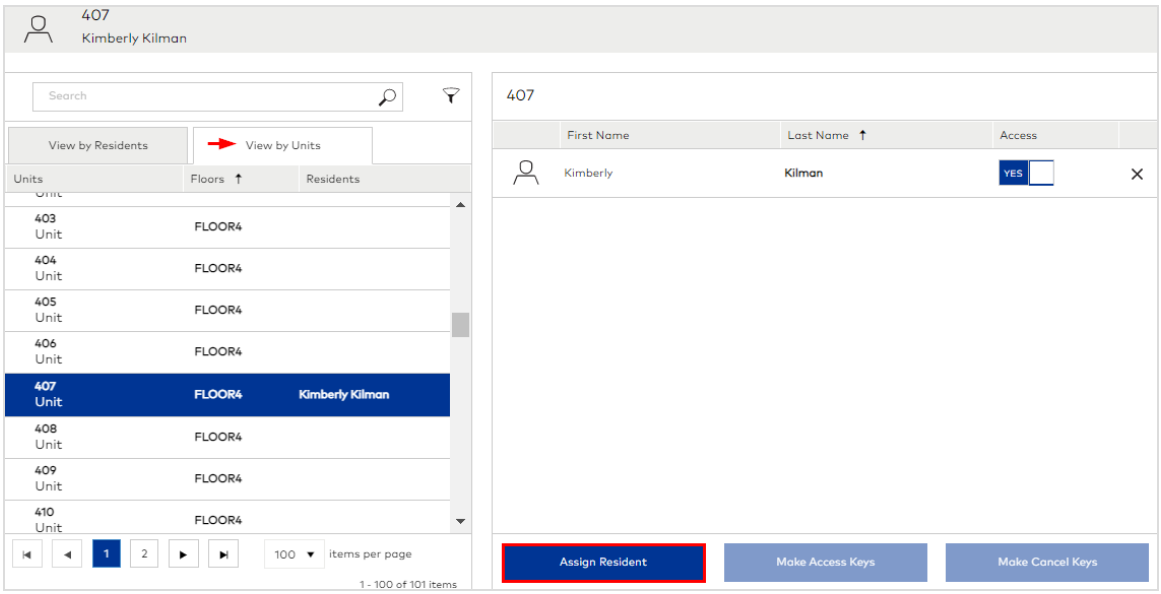
View by units

In Units View, you can add an existing or new resident to a unit.

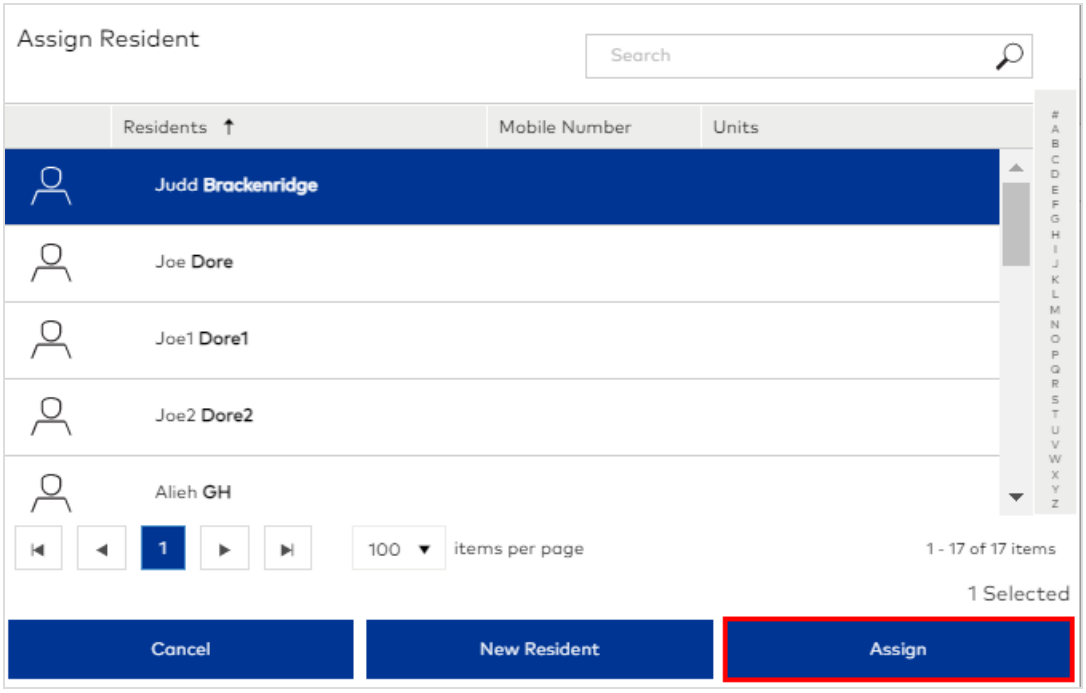
Assign existing resident to unit

To add an existing resident to a unit:

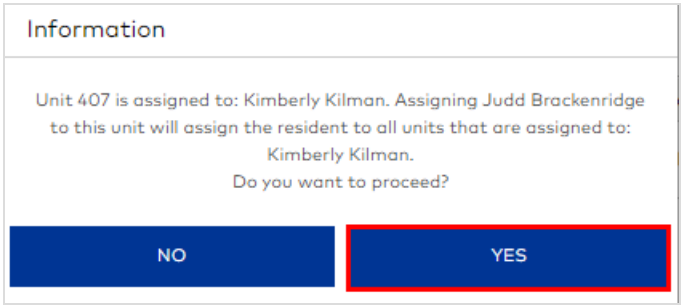
1. Go to **Resident Management**.
2. Click the **View by Units** tab.

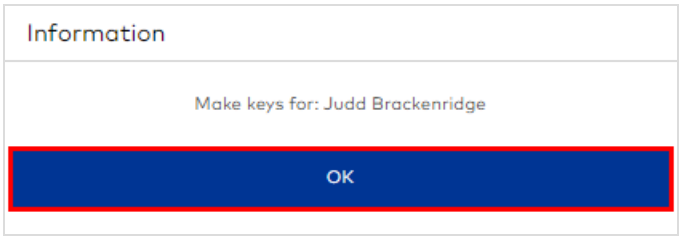


3. Select a unit.
4. Click **Assign Resident**.

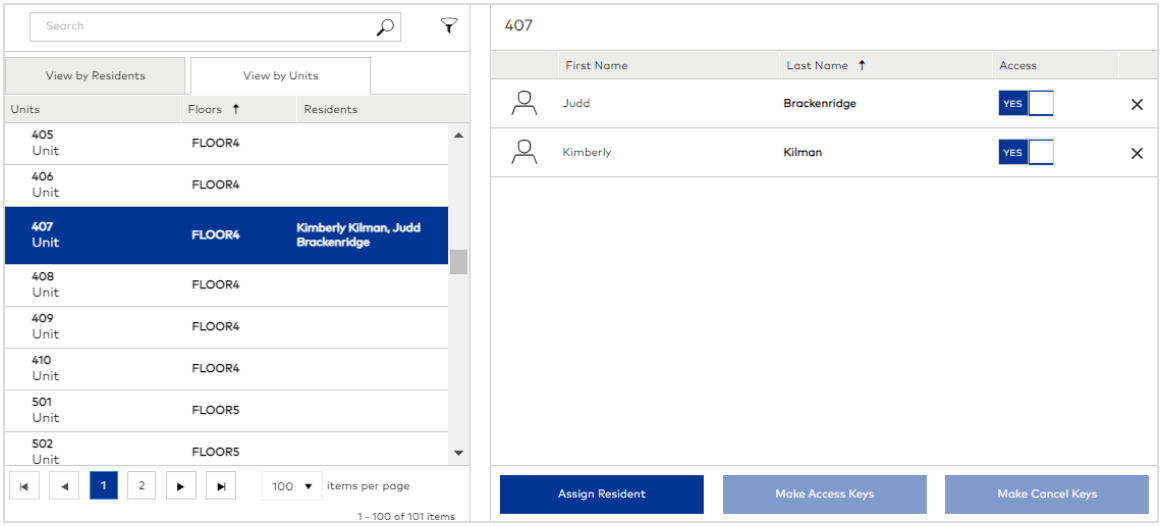


5. Select a resident.
6. Click **Assign**. Because the unit we assigned is occupied, Community requests for you to confirm the unit assignment.



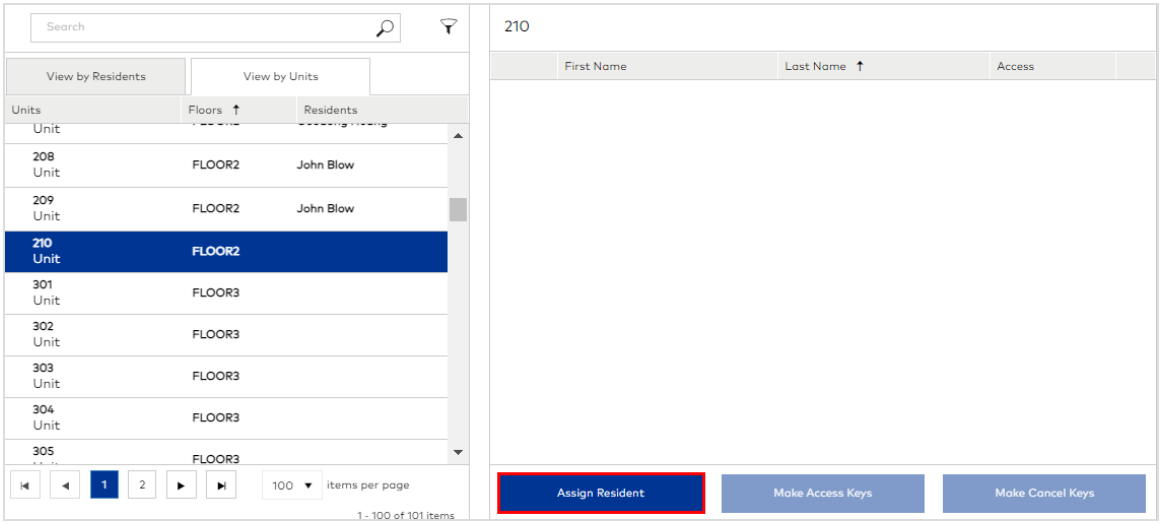


7. When notified about the keys that you need to make, click **OK**.

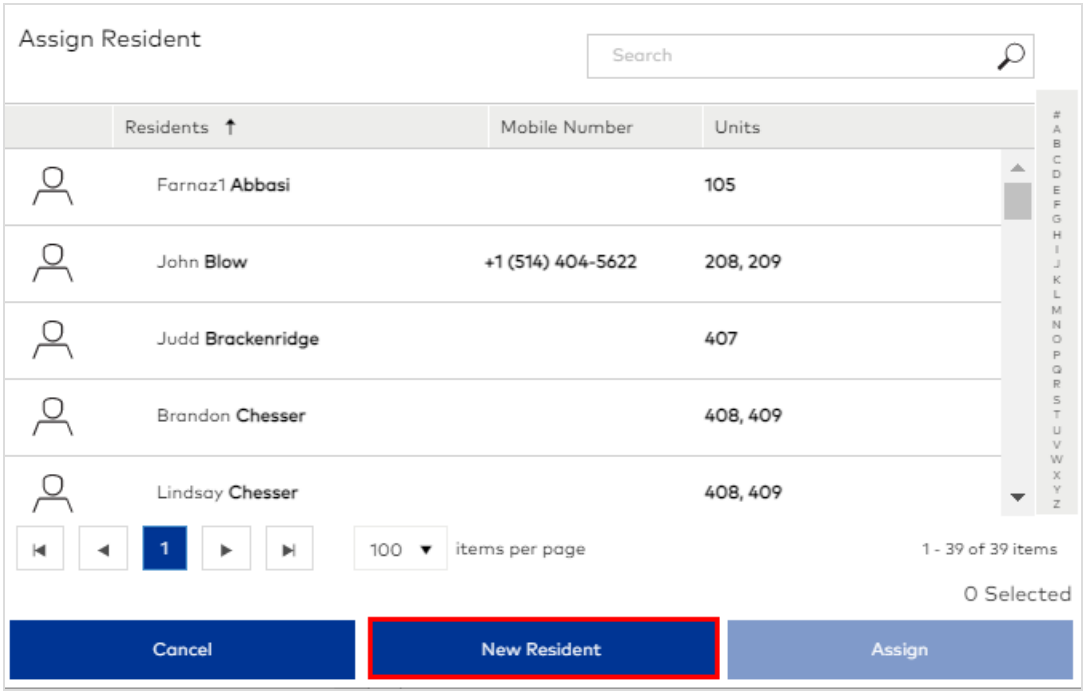


Assign New Resident to a Unit

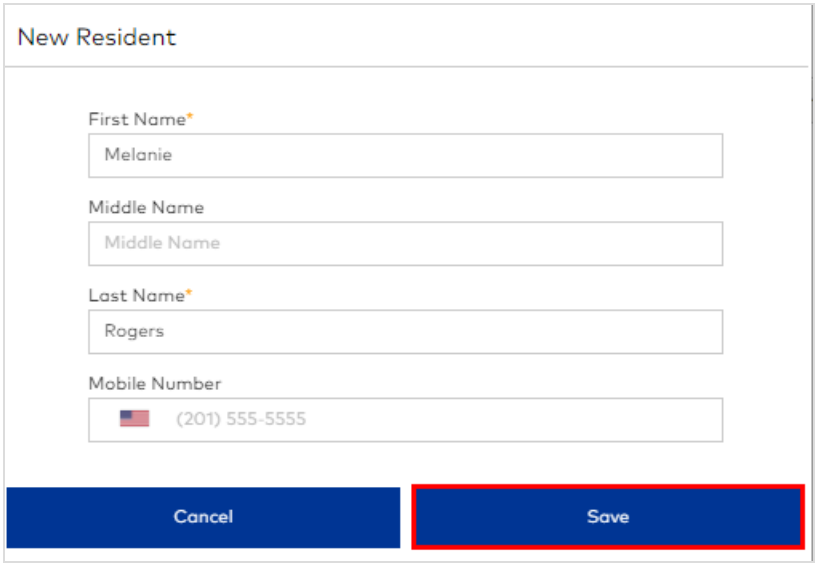
1. Go to **Resident Management**.
2. Click the **View by Units** tab.



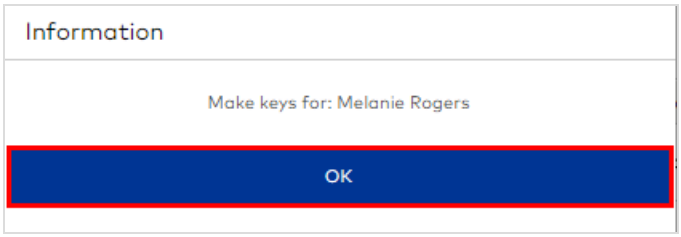
3. Select a unit.
4. Click **Assign Resident**.



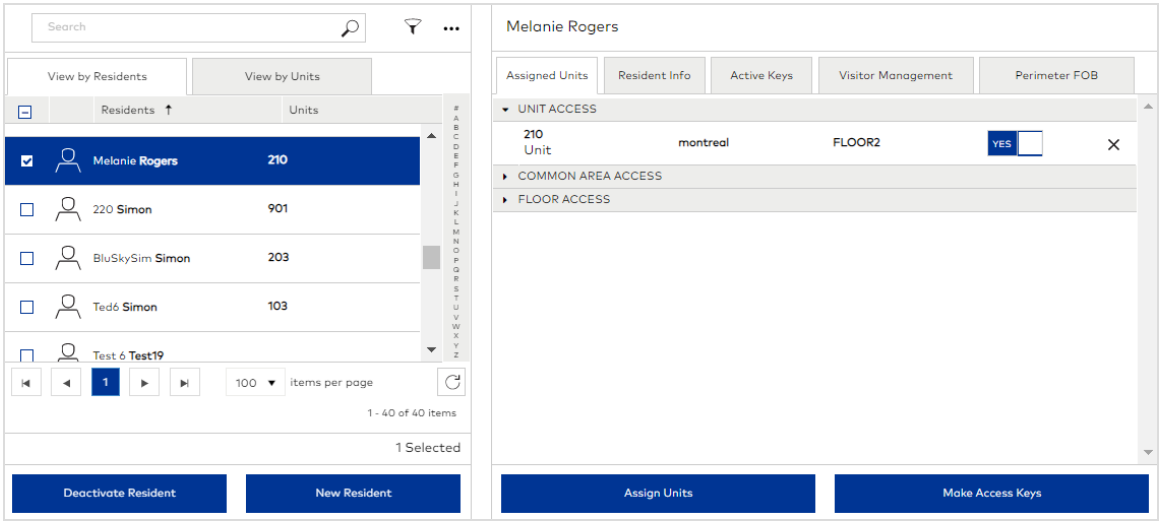
5. Click **New Resident**.



6. Specify the first and last names of the resident and, if issuing a mobile key, the complete mobile phone number including country and region codes.
7. Click **Save**.



8. When notified about the keys that you need to make, click **OK**. You can open the new resident's profile to verify the unit was assigned or to modify access in the profile.



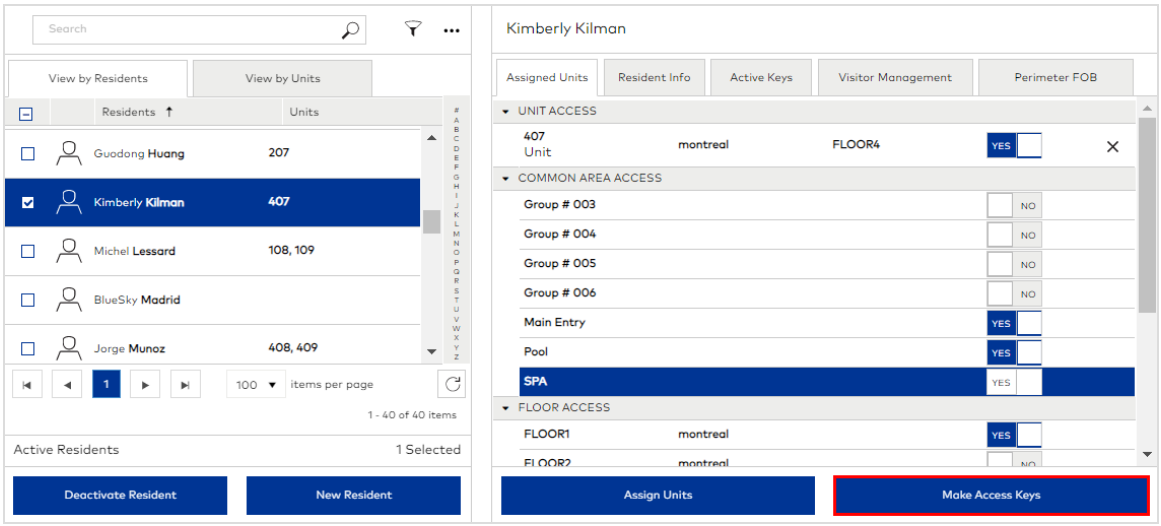
Make Resident Keys

Resident Keys are made and issued to residents to enable access to assigned units and resident common areas. If at least one unit is assigned, you can make resident keys from the **View by Residents** tab and the **View by Units** tab. If you are making a key for common areas only, you must use the **View by Residents** tab.

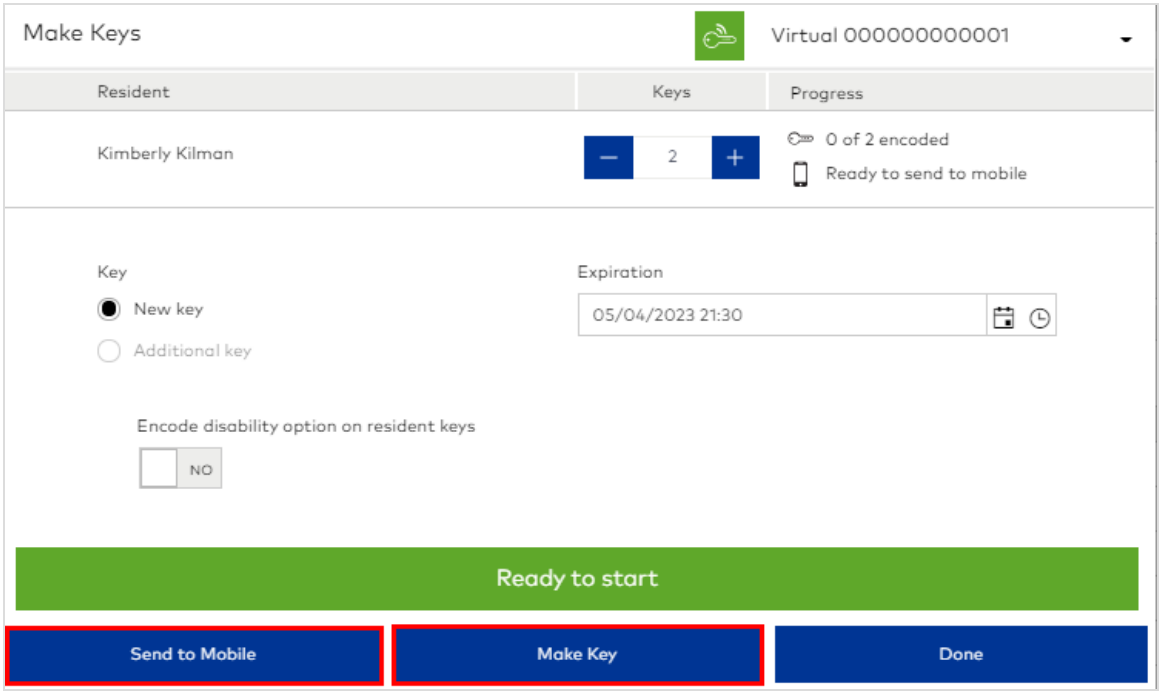
View by Residents

To make Resident Keys:

1. Go to **Resident Management**.
2. Select a resident.



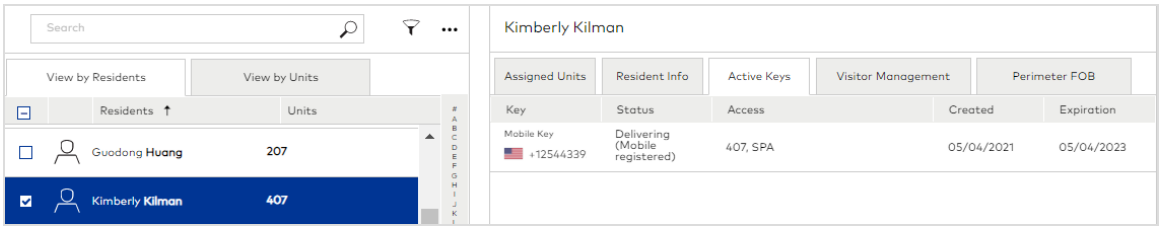
3. Click **Make Access Keys**.



4. Specify how many keys to make. If you are making a mobile key, select **1**.
5. Select a key mode. If there is no active key for the selected unit/s, **New Key** is required. if an active key exists, making a New key invalidates the selected credential on all active keys. Making Additional keys (copies) has no effect on existing active keys.
6. (*optional*) Specify a date and time after which the key is invalid.
7. Select whether to encode the disability option on resident keys. This option is only available when enabled in **System Settings > Security > Lock Access > RAC5 Options**.
8. Select an encoder that is online, click **Make Key**, then present keys to the encoder (as prompted).

To make a mobile key, click **Send to mobile**.

9. When notified that the key request is complete, click **Done**.

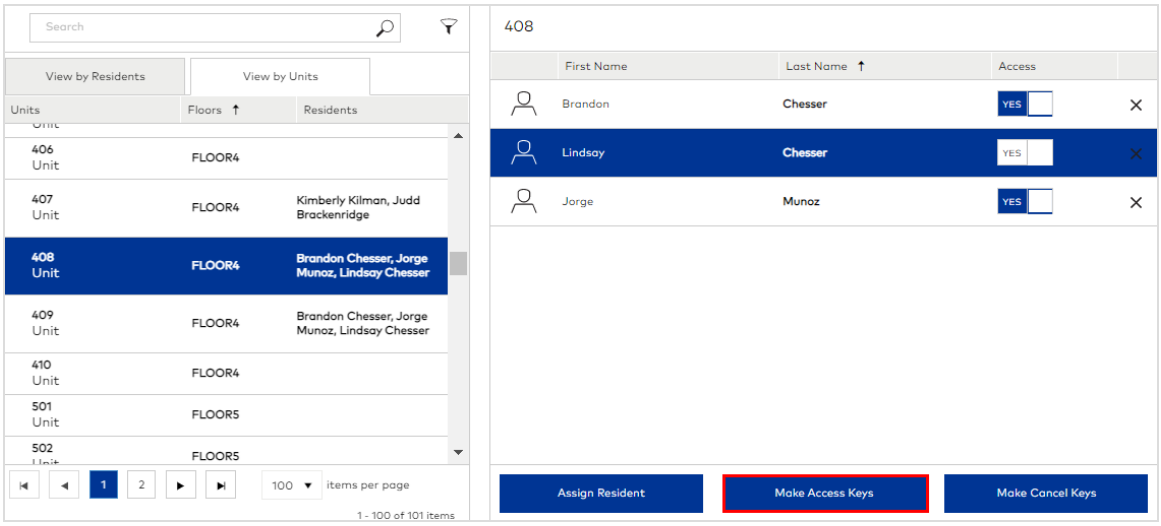


For mobile keys, you can click the **Active Keys** tab in the resident profile to verify the key was delivered.

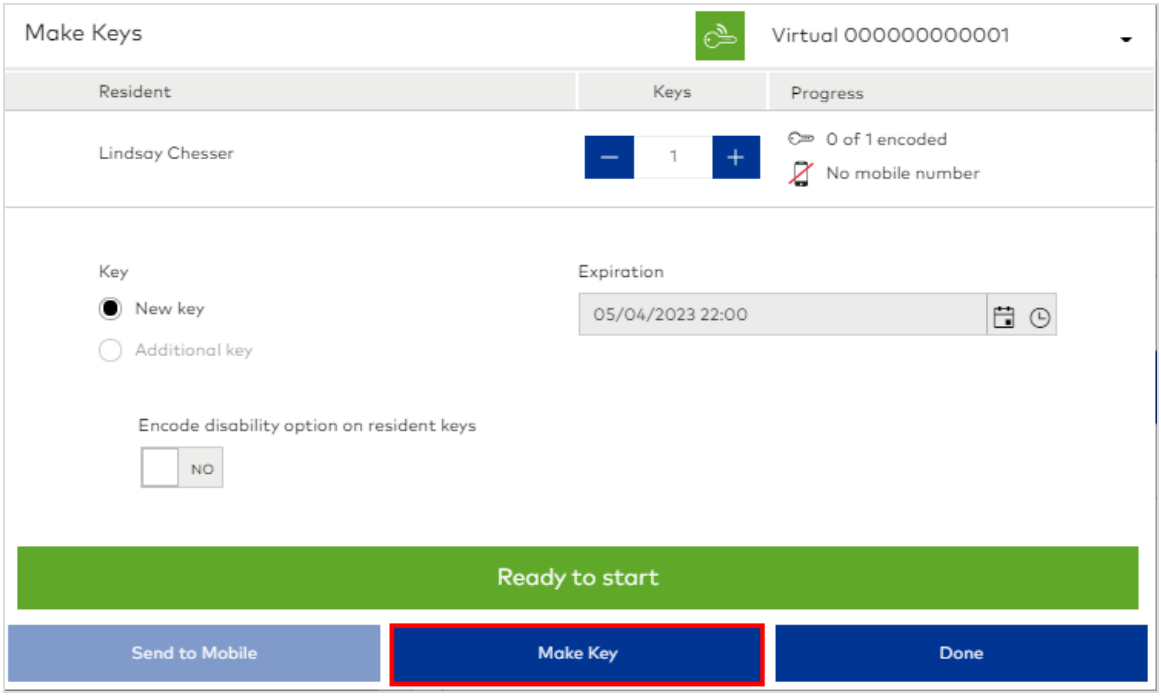
View by Units

To make Resident Keys

1. Go to **Resident Management**.



2. Click the **View by Units** tab.
3. Select a unit.
4. Select a resident.
5. Click **Make Access Keys**.



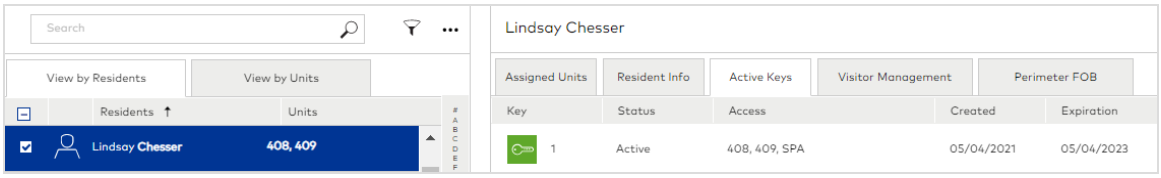
6. Specify how many keys to make.

> For mobile keys, select 1.

7. Select a key mode. If there is no active key for the selected unit/s, **New Key** is required. if an active key exists, making a New key invalidates the selected credential on all active keys. Making Additional keys (copies) has no effect on existing active keys.
8. (*optional*) Specify a date and time after which the key is invalid.
9. Select whether to encode the disability option on resident keys. This option is only available when enabled in **System Settings > Security > Lock Access > RAC5 Options**.
10. Select an encoder that is online, click **Make Key**, then present keys to the encoder (as prompted).

> To make a mobile key, click **Send to mobile**.

11. When notified that the key request is complete, click **Done**.



> For mobile keys, you can click the **Active Keys** tab in the resident profile to verify the key was delivered.

Modify Resident Access

Resident access can be modified by enabling or disabling access to assigned units, common areas, and floors or by removing access to assigned units.

Enabling/Disabling Access to Assigned Units

You can enable and disable resident access from the **View by Residents** tab and the **View by Units** tab.

Every time a change to access is made, Community issues a message that lists the names of residents for whom keys need to be made. If these messages do not display, change the option **Display key warning messages** in **System Settings > Resident** to **YES**.

View by Residents

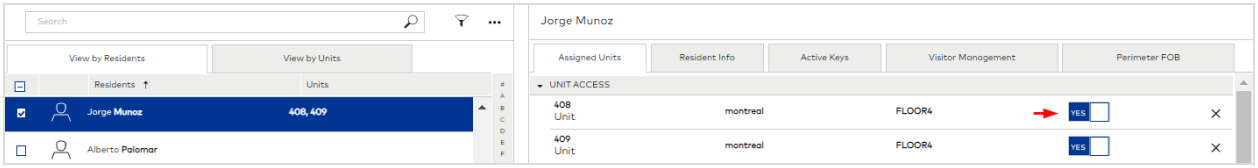
The **Assigned Units** tab in the resident profile lists all units assigned to the resident, all common areas, and all floors (for elevator access) in each of the buildings where the resident has access to a unit or common area.

Access to the individual units, common areas and floors can be enabled or disabled in the respective section of the profile (**UNIT ACCESS**, **COMMON AREA ACCESS**, **FLOOR ACCESS**).

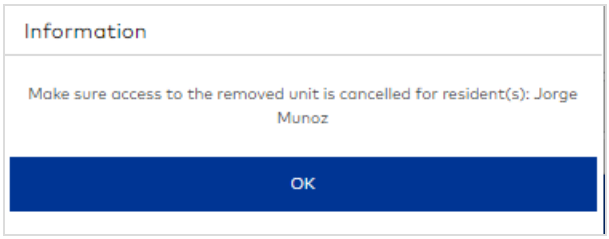
1. Go to **Resident Management**.
2. Select a resident.
3. On the **Assigned Units** tab:
   - To enable access, slide the Access switch to **YES**.
   - To disable access, slide the Access switch to **NO**.

UNIT ACCESS Section

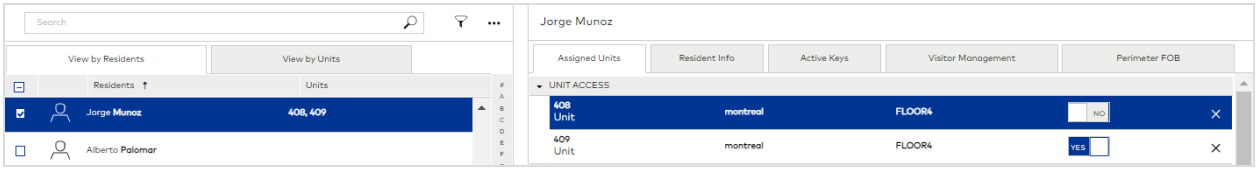
When you enable access to a unit, access to the floor where the unit is located is enabled. In addition, limited common areas that are enabled by default in the Resident Common Area Access profile associated with the unit are enabled.



When you disable access to a unit, access to the floor where the unit is located is disabled (if the resident does not have access to any other units or common areas on the same floor). Access to limited common areas that are uniquely associated with the unit in the Resident Common Area Access profile is disabled. Community notifies you about any keys that you need to make for affected residents.

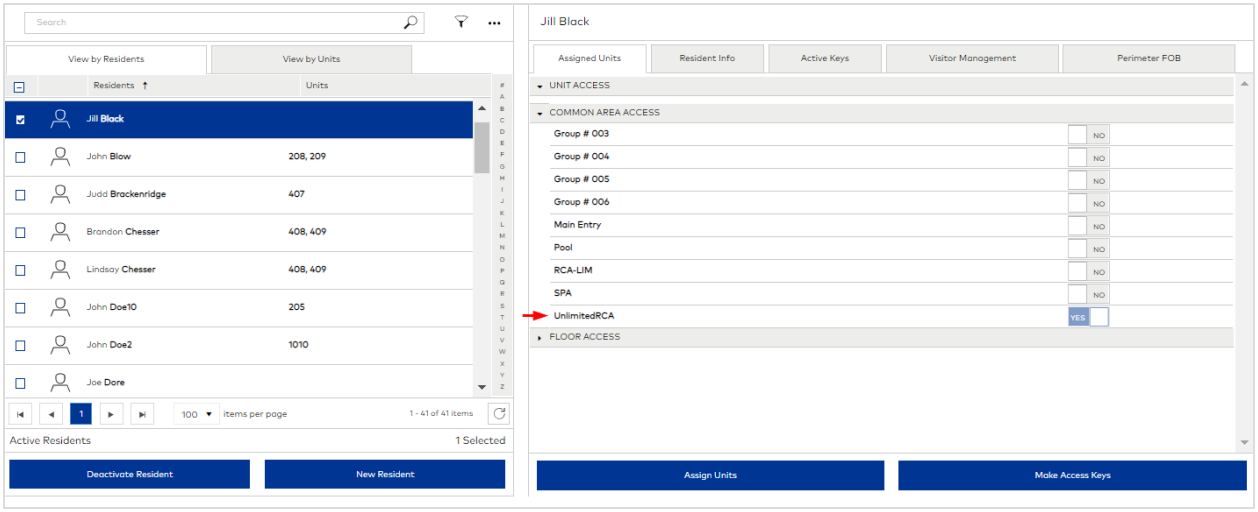


After disabling access, the Access switch is set to **NO**.



COMMON AREA ACCESS Section

When no unit is assigned to a resident, all common areas are listed. Unlimited common areas are enabled and cannot be disabled. Limited common areas are disabled by default but can be enabled.

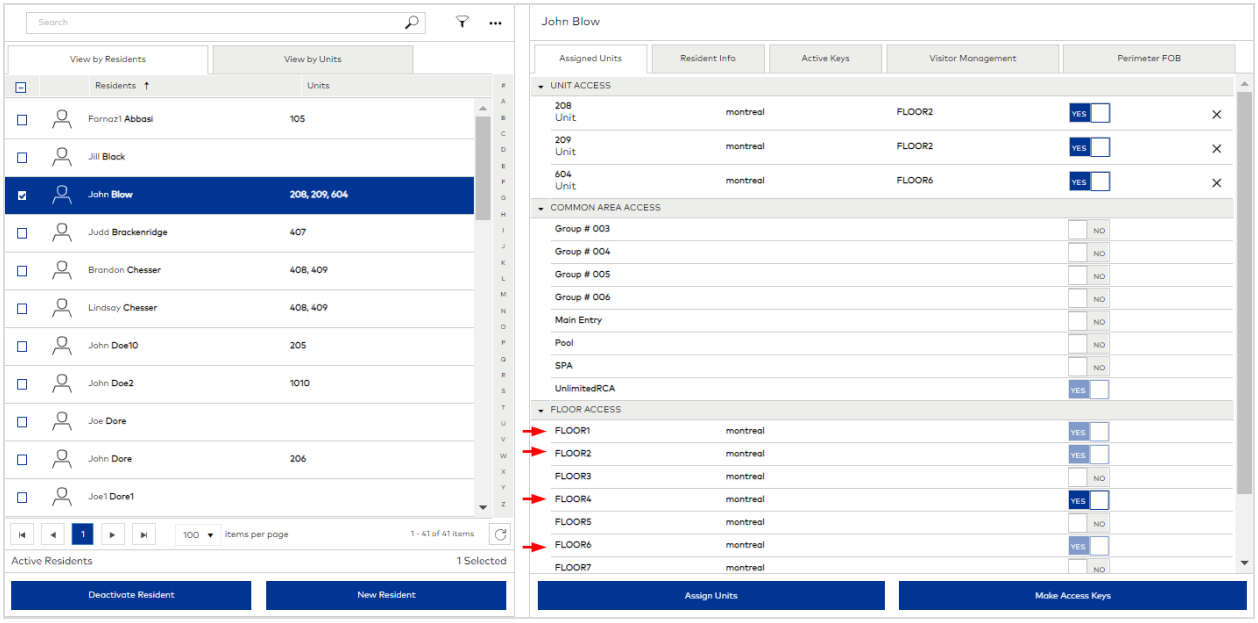


When at least one unit is assigned to a resident, all unlimited common areas remain enabled. The limited common areas that are enabled include those with default access in the Resident Common Area Access profile and any common areas previously selected before assigning a unit.

FLOOR ACCESS Section

This section is only displayed when the option **Display floor access** is set to **YES** in **System Settings > Resident**.

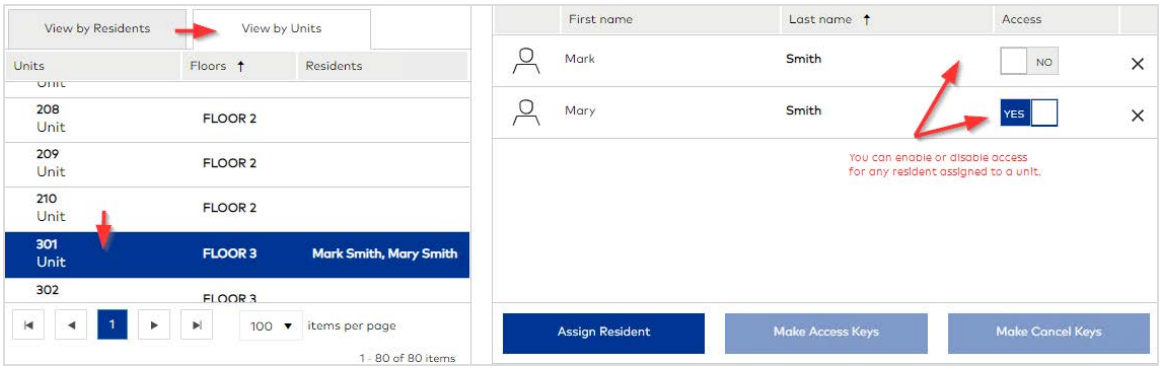
All floors for the buildings in which a resident has access to a unit or common area are listed under **FLOOR ACCESS**. By default, floor access is enabled for floors on which the resident can access a unit or common area. For all other floors, access is disabled by default.



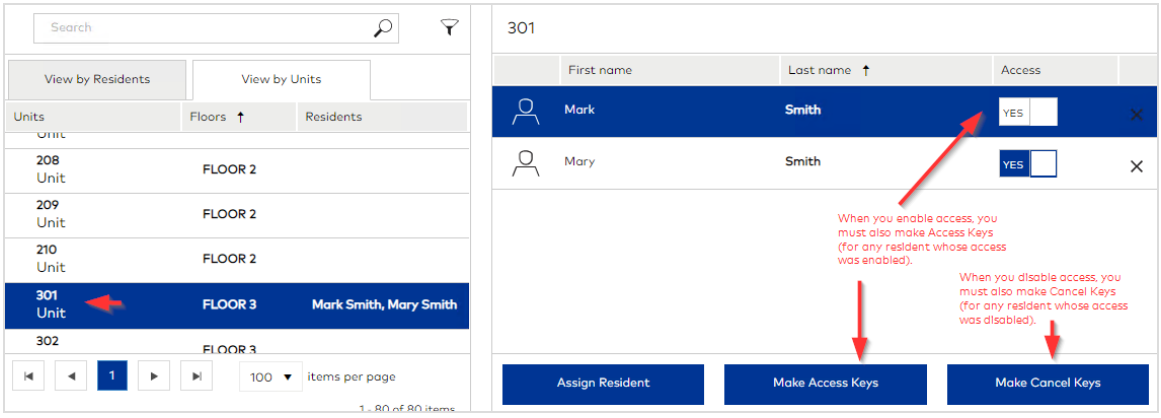
View by Units

When an occupied unit is selected, you can enable and disable resident access to the unit.

1. Go to **Resident Management**.



2. Click the **View by Units** tab.
3. Select a unit.
4. For the resident/s whose access you want to modify:
   - To enable access, slide the Access switch to **YES**. The unit and all common areas uniquely associated with the unit are authorized. You must make Access Keys for any resident whose access was enabled.
   - To disable access, slide the Access switch to **NO**. The unit remains in the profile but access to the unit and uniquely associated common areas are denied. You must make Access Keys for any resident whose access was disabled.



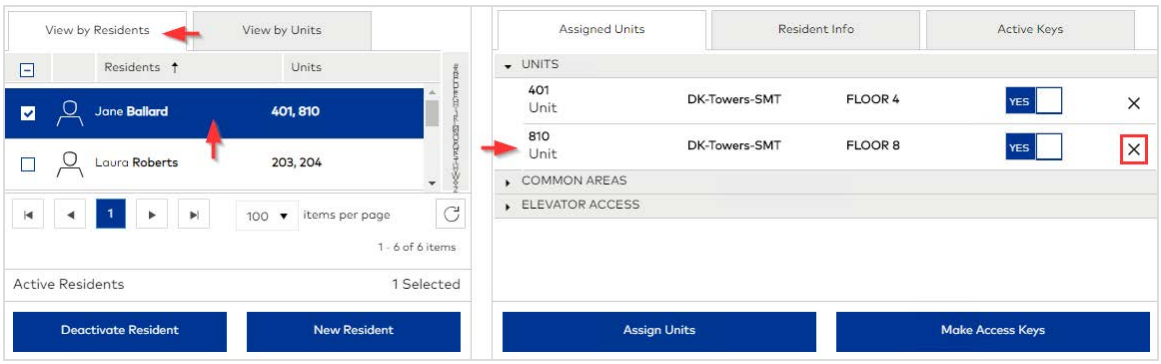
Unassigning Units

Removing a unit from a resident's profile removes access to the unit and all common areas uniquely associated with the unit. If the unit is shared with other residents, then the unit is also removed from their profiles. An alternative to removing a unit from a resident profile is to disable access to the unit.

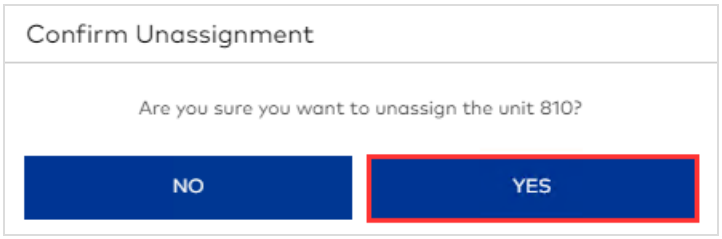
You can remove resident access from the **View by Residents** tab and the **View by Units** tab.

View by Residents

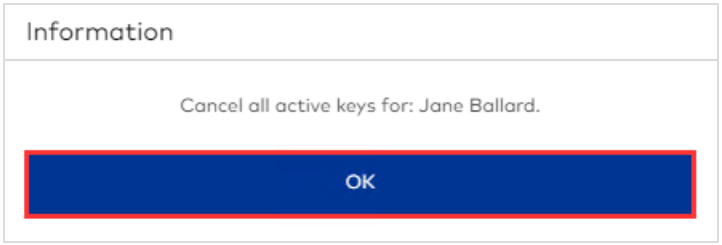
1. Go to **Resident Management**.



2. Select a resident.
3. In the **UNIT ACCESS** section, click **(Delete)** ✕ in the **Unit** row.



4. Click **YES** to confirm.

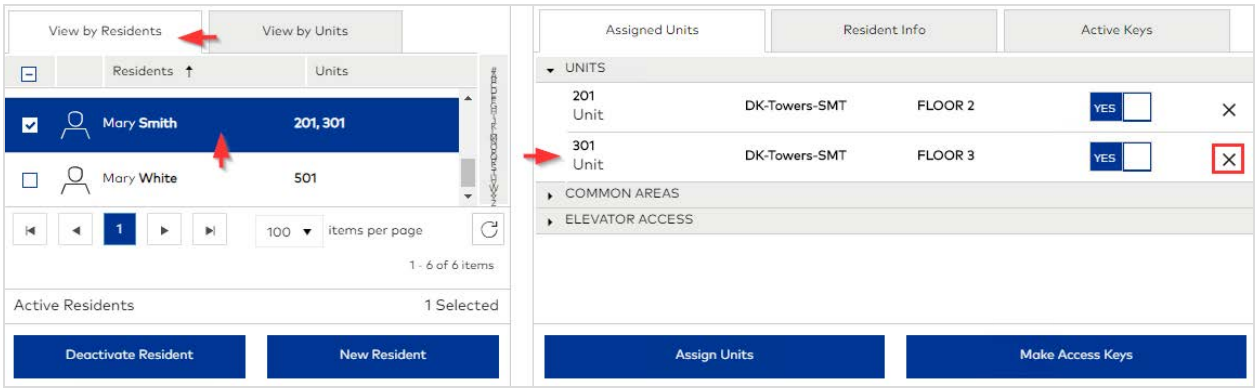


5. When prompted to make Cancel Keys, click **OK**.

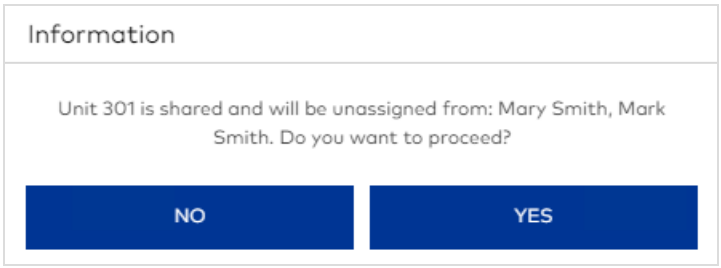
Removing Access When Residents Share Access

When access to a unit is removed from a resident who shares access, the unit is also removed for all residents who share access.

The following figure shows Unit 301 will be removed from Mary's resident profile.

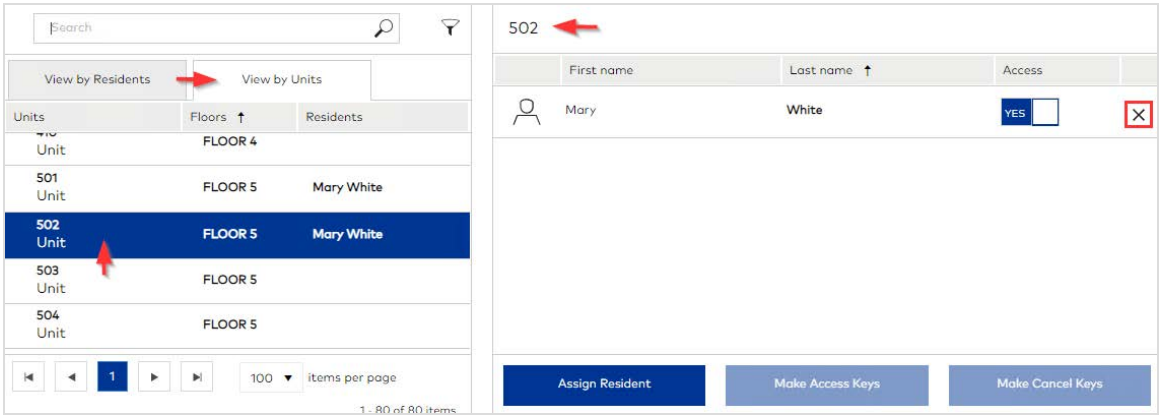


When you select to remove Unit 301 from Mary's profile, Community notifies you about affected residents.

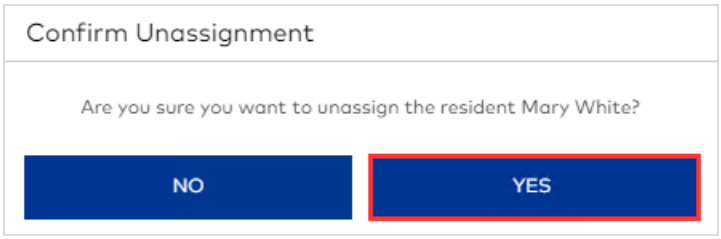


View by Units

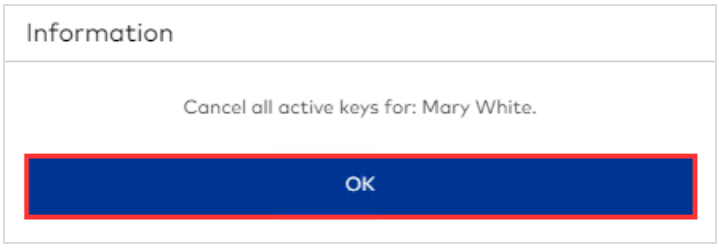
1. Go to **Resident Management**.



2. Click the **View by Units** tab.
3. Select a unit.
4. For the resident whose access you want to remove, click **(Delete)** ✕ .



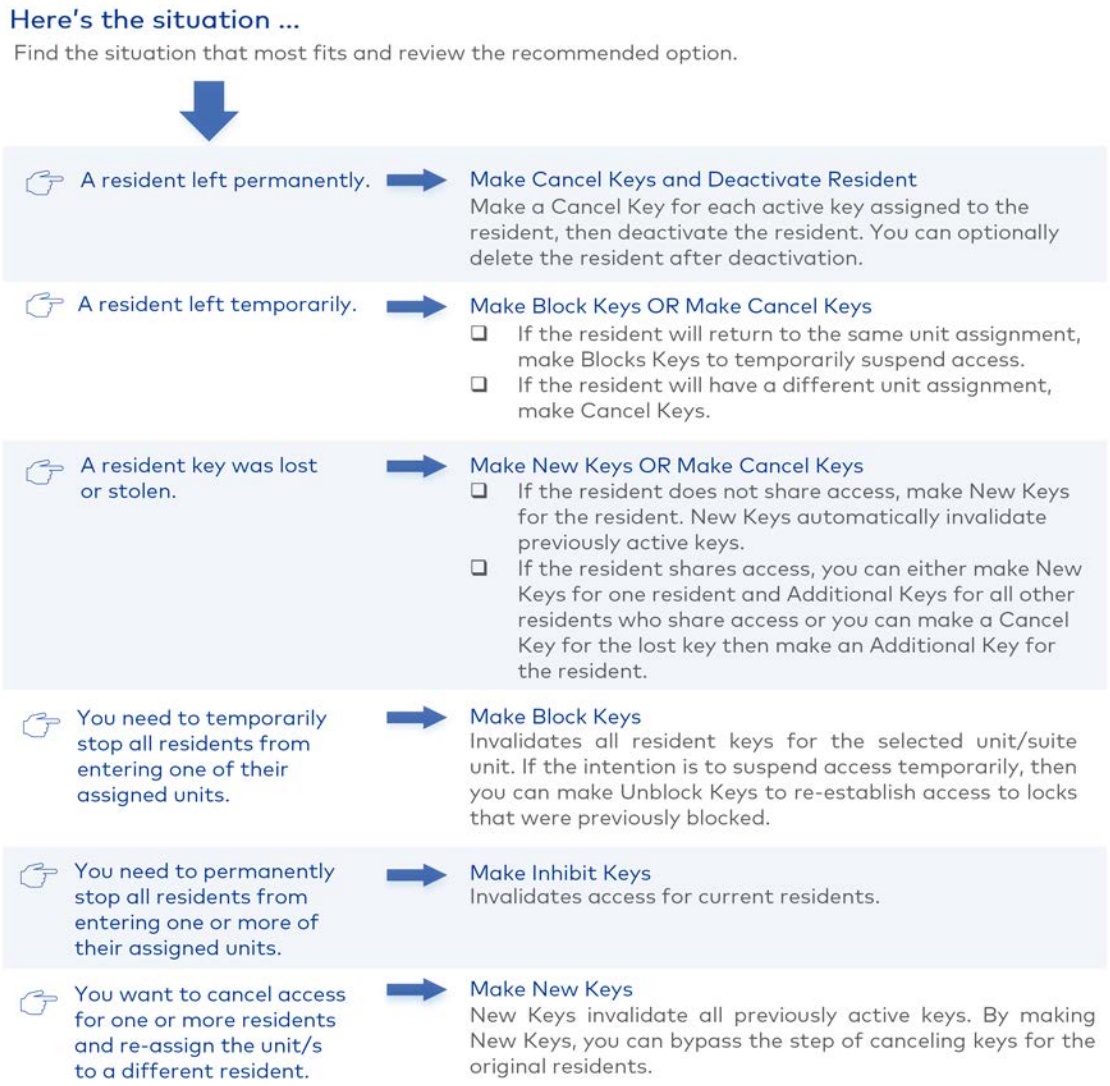
5. Click **YES** to confirm.



6. When prompted to make Cancel Keys, click **OK**.

Invalidate resident access

There are multiple options when you need to invalidate resident access before the key/s expire. The best method depends on the Community modules authorized for your Operator account and the reason you want to invalidate access.



Don't forget that access remains valid until the Cancel/Block/Inhibit/New keys are presented to locks.

In addition to invalidating resident access to units, there are special cases to consider.

Canceling Resident Access to Common Areas

invalidate access to resident commons areas without canceling the resident's access to assigned units.



You want to cancel a resident's access to a resident common area.

→ Make Cancel Keys or New Keys

- ❑ Make a Cancel Key for each active key assigned to the resident, then present the Cancel Key to any resident common area where you want to invalidate access.
- ❑ Make a New Key for the same unit assignment, then present the key to any resident common area where you want to invalidate access.

Invalidating Mobile Key Access

Invalidating access when a resident uses a mobile key is similar to the process for physical keys.



You want to invalidate access for a resident who has a mobile key

→ Make Cancel Keys

Make a Cancel Key for each active mobile key assigned to the resident.

- ❑ If **Enable resident mobile key cancellation** is set to YES in System Settings > Advanced, click **Send to mobile** when prompted. Community sends the command to remove the key from the dormakaba BlueSky app.
- ❑ In all other cases, present the Cancel Key to all access points that the key authorized.

Invalidating Access for Keyscan Aurora

There are multiple options to invalidate access when Keyscan Aurora is enabled



Keyscan Aurora is enabled and you want to invalidate access for a resident

→ Make Cancel/Block/Inhibit/New Keys or Deactivate Resident

All you need to do is encode any of these key types or deactivate the resident. You do not need to present a key to a Community lock. The Aurora Server communicates with the Keyscan reader to invalidate access. Deactivating a resident also invalidates access automatically.

Invalidating Access – Online Communication

Invalidating resident access when Online Communication is enabled does not require physical keys.



You want to invalidate access for a resident who leaves before their key/s expire

→ Deactivate Resident

In Resident Management, select the resident and click Deactivate Resident.

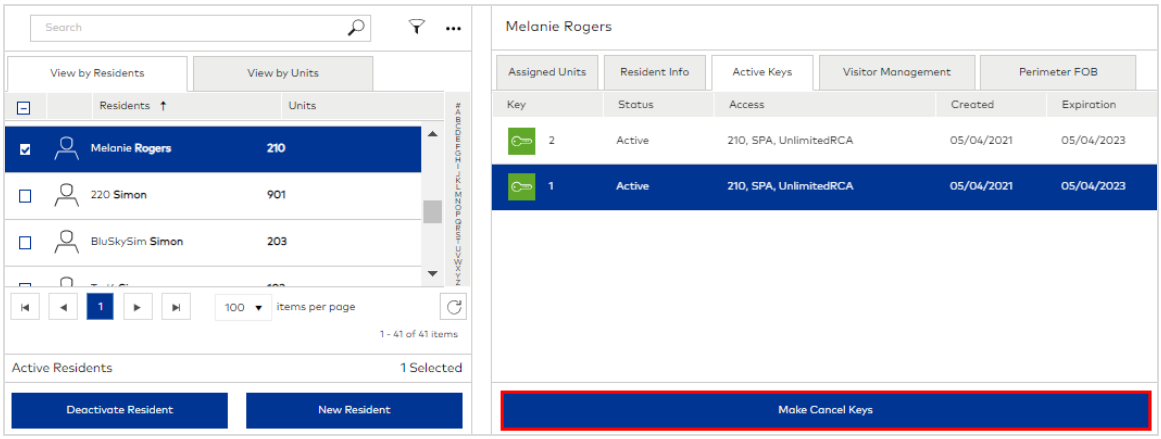
- ❑ All assigned units and common areas are removed from the profile and all active keys are canceled. You can optionally delete the deactivated resident.
- ❑ Access is also removed from all residents who share access with the deactivated resident.

Make Cancel Keys

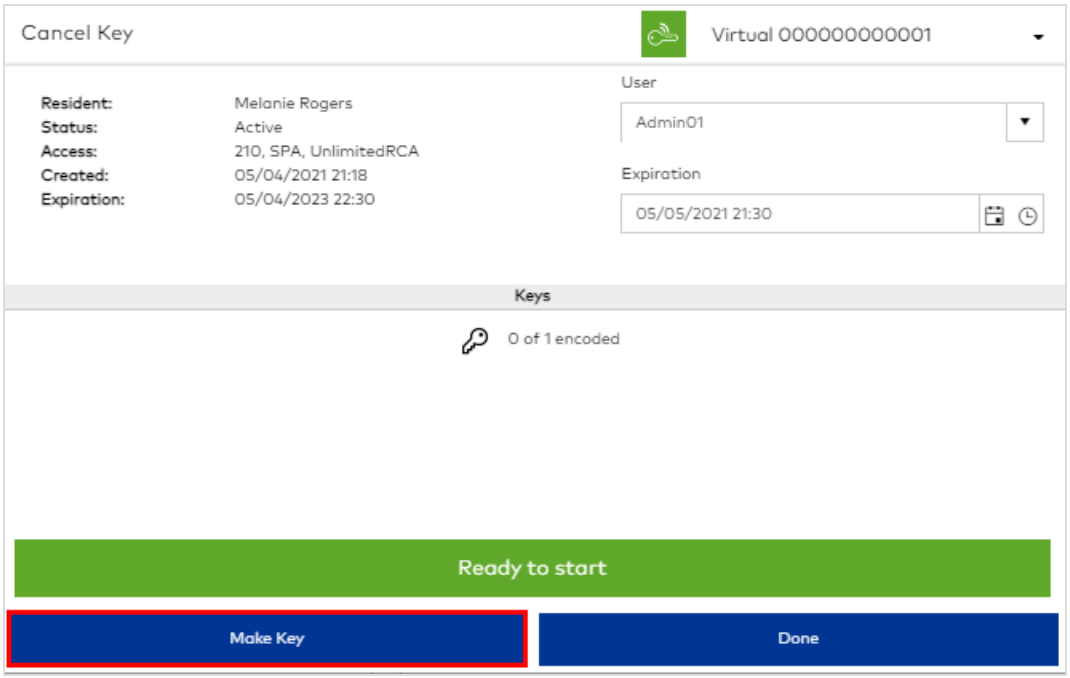
Cancel Keys permanently invalidate a single and specific key instance. To cancel physical keys, make a physical Cancel Key and present the Cancel Key to every access point authorized on the access key. To cancel mobile keys, you have the option to cancel the mobile key remotely and/or make a physical Cancel Key.

Canceling resident mobile keys remotely is a licensed feature and must be enabled in **System Settings > Advanced > Enable mobile keys > Enable resident mobile key cancellation**.

1. Go to **Resident Management**.
2. Select a resident.
3. Click the **Active Keys** tab.



4. Select the key that you want to cancel.
5. Click **Make Cancel Keys**.

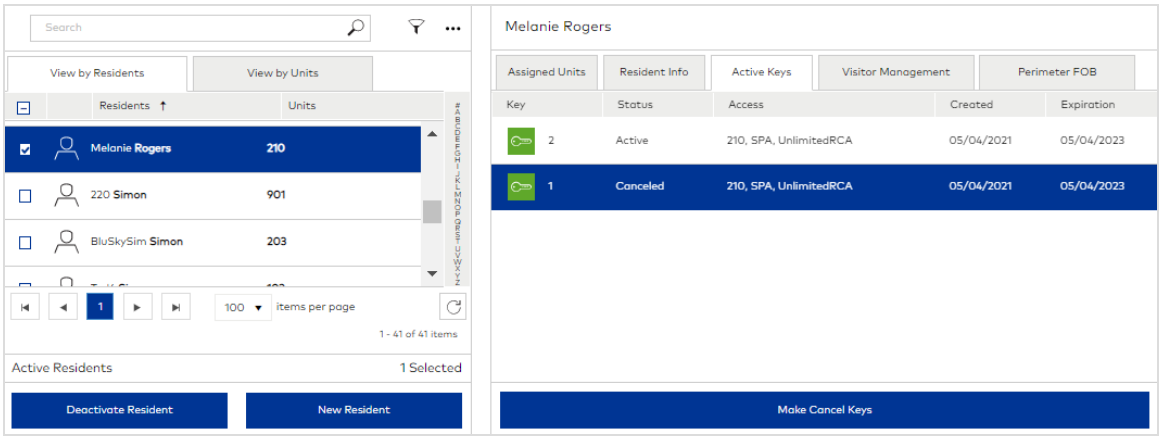


6. (*optional*) Select the staff/vendor to whom you want to assign the Cancel Key.
7. (*optional*) Specify a date after which the Cancel Key is invalid.

8. Select an encoder that is online, click **Make Key**, then present a key to the encoder.

If you are canceling a mobile key, click **Make Key** to make a physical Cancel Key and/or click **Cancel Mobile Key** to cancel the mobile key remotely. Physical Cancel Keys must be presented to access points to invalidate a mobile key.

9. When notified that the key request is complete, click **Done**. You must present the Cancel Key to the affected access points before access is canceled.



Although you can make a Cancel Key to cancel a Resident Key in the **Resident Management** module, you cannot make a Cancel Key to cancel a Resident Key in the **System Keys** module.

Deactivate residents

Deactivating a resident works differently in offline and online environments.

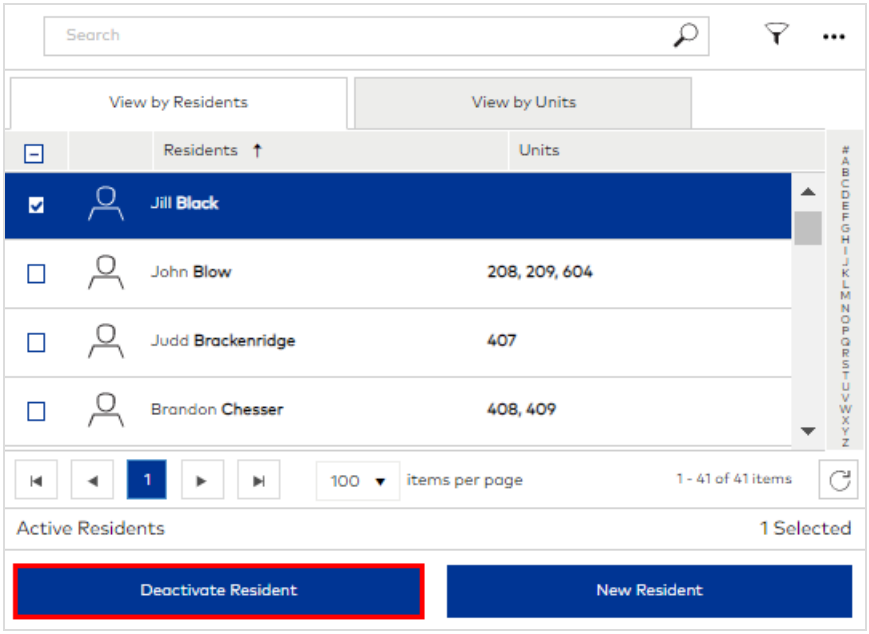
- In offline environments, you must first unassign all units from the resident, make and present Cancel Keys to relevant locks, then deactivate the resident.
- In online environments, Cancel Keys are automatically made and sent to relevant locks, all unit assignments and active keys assigned to the resident are removed from the resident profile and the resident is no longer listed on the View by **Residents** tab.

  If Visitor Management is enabled, all active delegated PINs and mobile keys are permanently canceled.

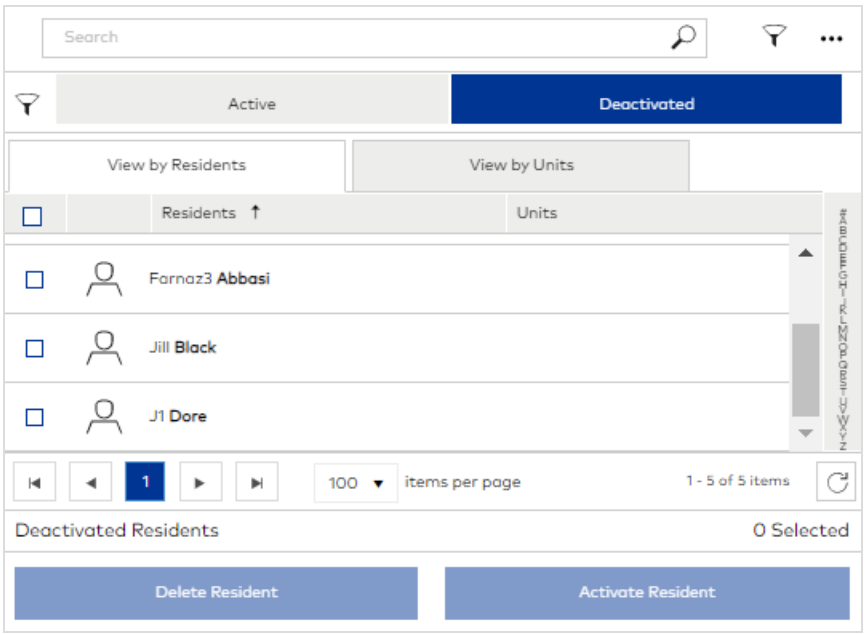
  You can delete or (re)-activate a resident who has been deactivated.

When online communication is enabled, access is also removed from all residents who share access with the deactivated resident.

1. Go to **Resident Management**.



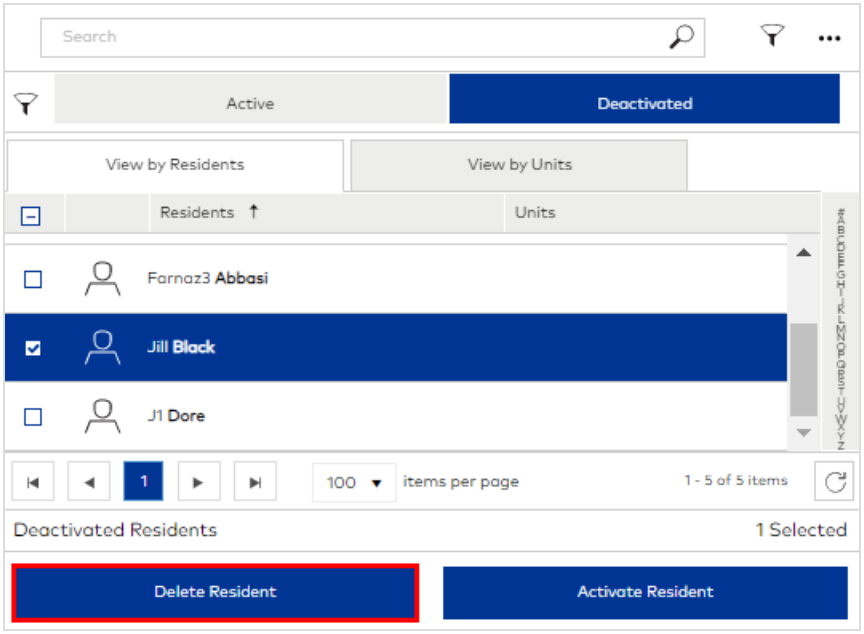
2. Select one or more residents.
3. Click **Deactivate Resident**.
4. Click **YES** to confirm. You can verify the resident was deactivated by clicking **(Filter)** and selecting the **Deactivated** tab. The resident name is listed and the profile shows that the unit assignment and active keys have been removed.



Delete residents

You can only delete residents who have been deactivated.

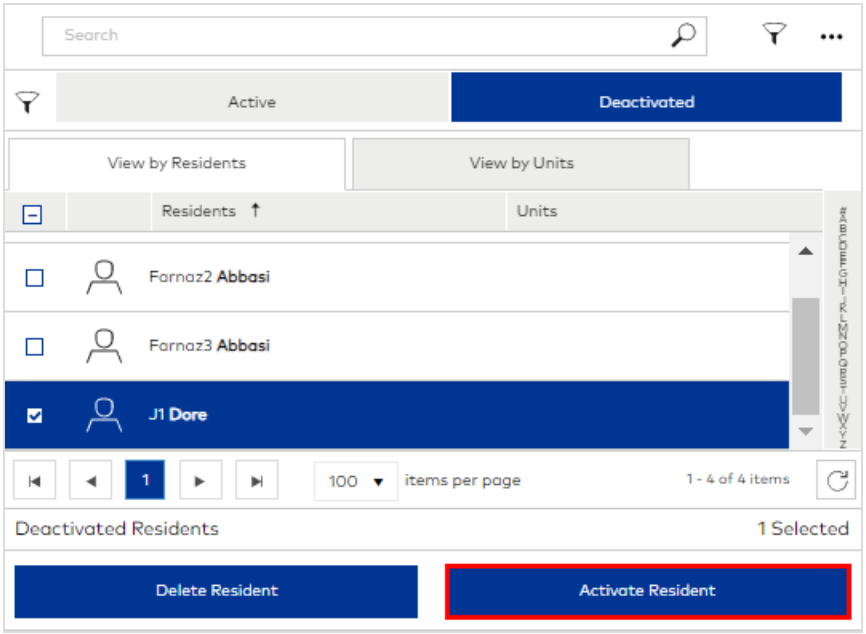
1. Go to **Resident Management**.



2. With the (Filter) options displayed, click the **Deactivated** tab.
3. Select one or more residents.
4. Click **Delete Resident**.
5. Click **YES** to confirm.

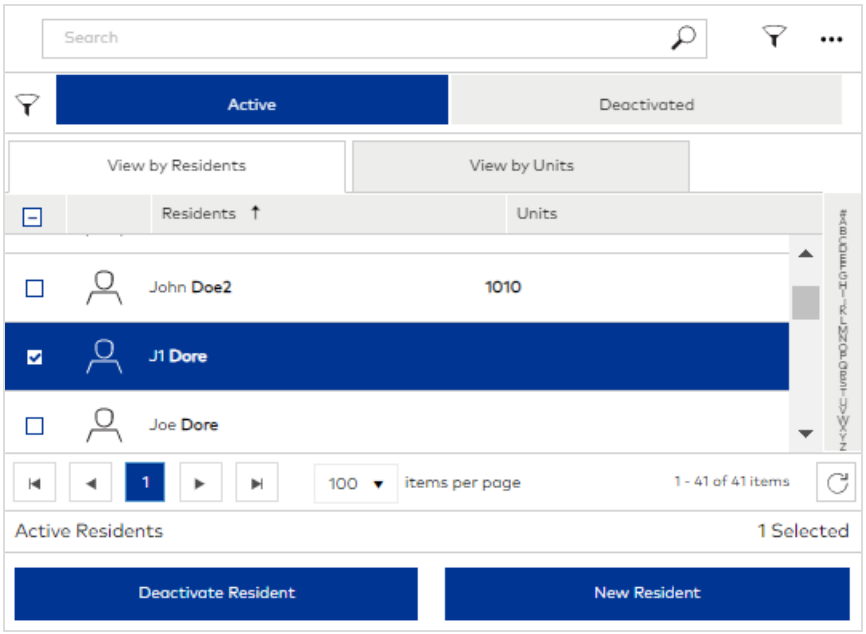
Activate residents

1. Go to **Resident Management**.



2. With the (Filter) options displayed, click the **Deactivated** tab.
3. Select one or more residents.
4. Click **Activate Resident**.

5. Click **YES** to confirm. You can verify the resident/s are activated by clicking the **Activated** tab or closing the filter options and searching for the resident/s on the **View by Residents** tab. After activating residents, you an assign units and make resident keys.



Make New Keys

Making a New Key automatically invalidates access to the selected credential on all previously active keys. For example, NewKey1 for units 100 and 101 expires at 13:00 tomorrow. If you make NewKey2 for unit 100, NewKey1 becomes invalid for unit 100 as soon as you present NewKey2 to the lock installed for unit 100. NewKey1 remains valid only for unit 101. For instructions, see Make Resident Keys.

Make Block Keys

Block Keys invalidate all instances of a specific credential. While you can use the Block Key to permanently invalidate access, the Block Key is paired with the Unblock Key to suspend then restore access. For example, make a Block Key for Unit 100 to suspend all access; then, make an Unblock Key for Unit 100 to restore access for all active keys.

When making a Block Key to invalidate resident access, the credential class that you select is *Resident*. The credential that you select is the unit/suite unit that you want to block.

After blocking access, the Unblock Key does not unblock access to common areas when access is based on a common area access profile.

For instructions, see Block/Unblock Keys.

Make Inhibit Keys

Inhibit Keys are used to permanently cancel current resident access. Most often, Inhibit Keys are used by staff after a resident vacates before their key expires. Inhibit Keys invalidate all resident keys encoded with access to the unit even if the dead bolt or privacy switch is active.

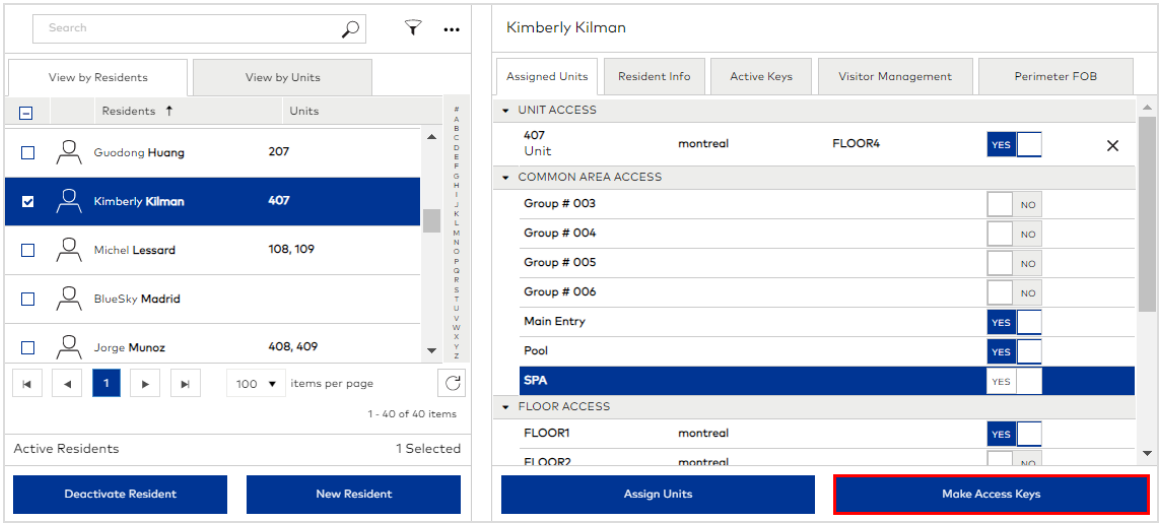
Inhibit Keys do not invalidate access to common areas and elevator readers.

For instructions, see Inhibit Keys.

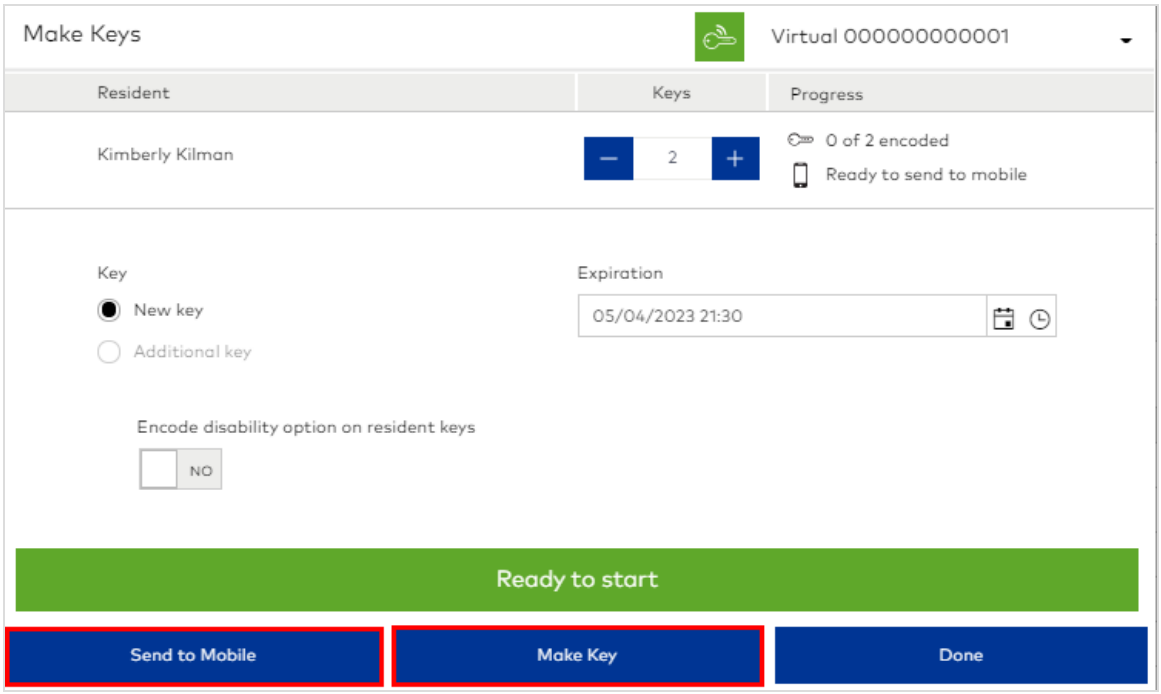
Make keys for common area access only

The Community feature to make access keys for common areas only allows properties to authorize special access to limited common areas, such as a fitness center, to people who do not lodge on the property. Although the keys are issued to non-residents, you must still add a resident profile for each key holder.

1. Go to **Resident Management**.
2. Select (or add) a resident. To add a resident, click **New Resident**, specify first and last names, then click **Save**.



3. In the **COMMON AREA ACCESS** section, select the limited common areas that you want to enable. (All unlimited common areas are enabled by default and cannot be disabled).
4. Click **Make Access Keys**.



5. Specify how many keys to make. If you are making a mobile key, select **1**.
6. Select a key mode. If there is no active key for the selected unit/s, **New Key** is required. if an active key exists, making a New key invalidates the selected credential on all active keys. Making Additional keys (copies) has no effect on existing active keys.
7. (*optional*) Specify a date and time after which the key is invalid.
8. Select whether to encode the disability option on resident keys. This option is only available when enabled in **System Settings > Resident Management**.
9. Select an encoder that is online, click **Make Key**, then present keys to the encoder (as prompted).



To make a mobile key, click **Send to mobile**.

10. When notified that the key request is complete, click **Done**.



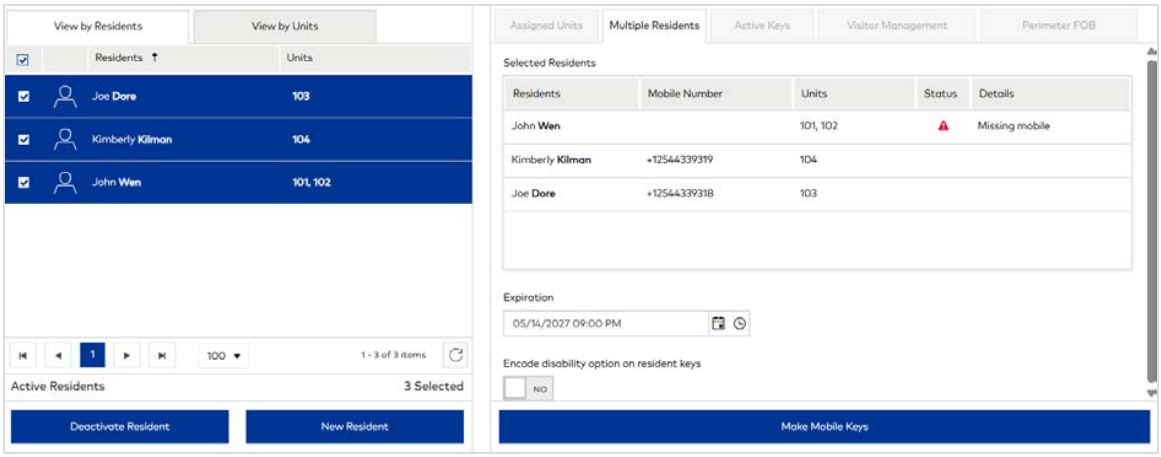
For mobile keys, you can click the **Active Keys** tab in the resident profile to verify the key was delivered.

Make mobile keys for multiple residents

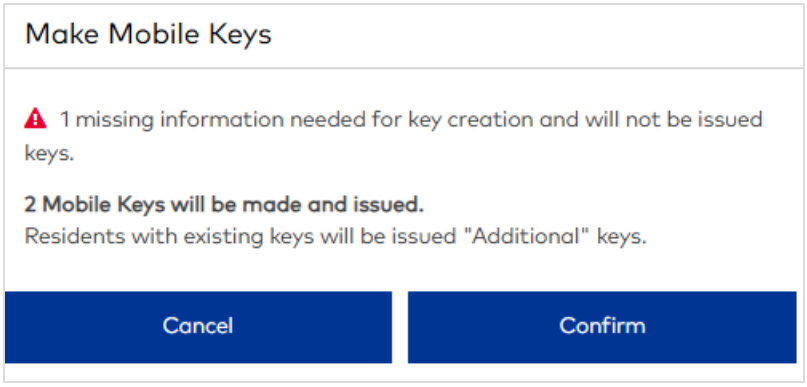
Make mobile keys for selected residents. Requirements include:

- A mobile number must be specified in the resident profile.
- At least one unit must be assigned to the resident.

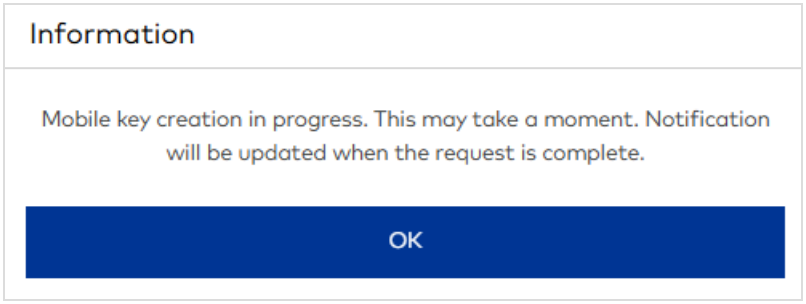
1. Go to **Resident Management**.
2. Select two or more residents. Warnings display for any selected resident that is missing a mobile number or assigned unit.



3. Select an expiration date for all mobile keys.
4. Select whether to include the disability option. The disability option (configured in System Settings/Security) extends the amount of time a door remains unlatched after presenting a valid key.
5. Click **Make Mobile Keys**.



6. Review information in the confirmation dialog, then click **Confirm**. The confirmation dialog reports the total number of keys that will be made and the number of key request warnings.



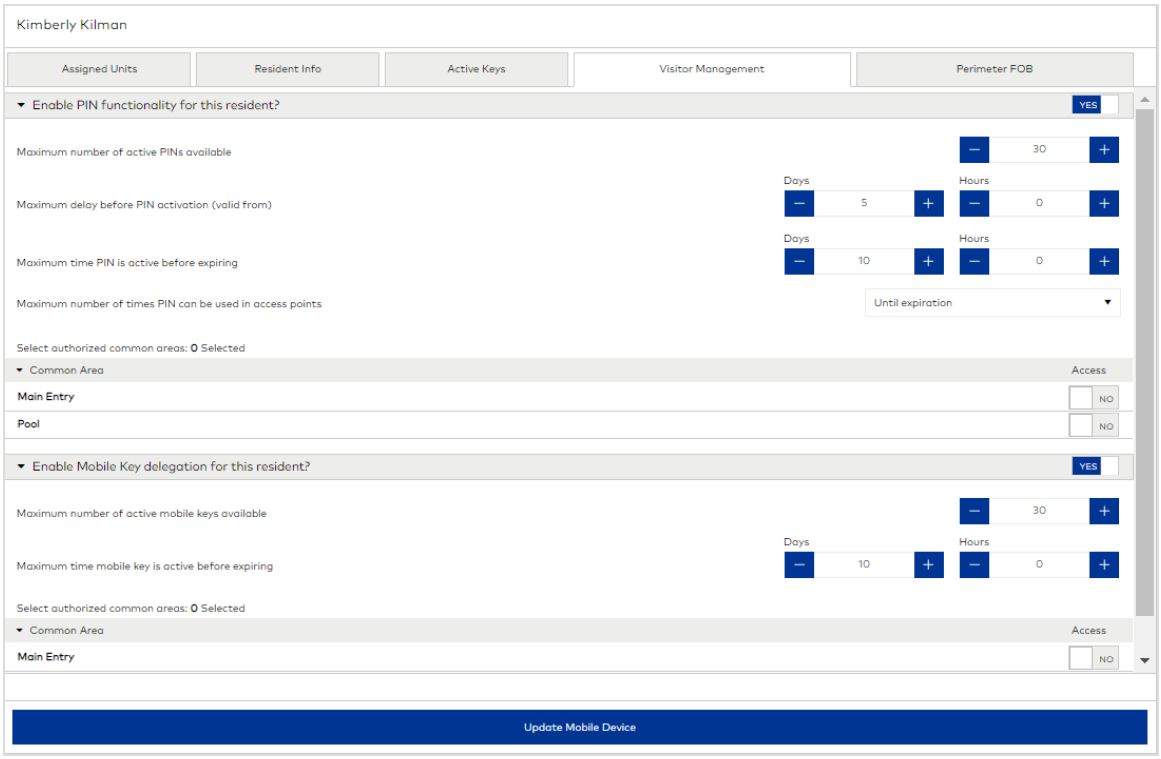
7. Click **OK** when notified the mobile key creation is in progress. The number of keys requested and potential issues with resident mobile phones impacts processing time.

Configure Visitor Management for residents

This tab displays when the licensed feature visitor management is enabled.

To configure PIN / mobiile key delegation for a resident:

1. Go to **Resident Management**.
2. Select a resident.
3. Click the **Visitor Management** tab.



4. Configure PIN delegation options:
   - **Enable PIN functionality for this resident**—When the feature is enabled, the PIN section displays, PIN settings can be customized, and PIN settings can be updated on mobile devices.
   - **Maximum number of active PINs available**—Specify the maximum number of PINs that can be active. Valid values: 1-50.
   - **Maximum delay before PIN activation (valid from)**—Specify the maximum number of days/hours that the resident can create a PIN before access authorized by the PIN starts. Range: 0-15 days/0-23 hours.
   - **Maximum time PIN is active before expiring**—Specify the maximum number of days/hours that a PIN can be active. Range: 0-15 days/0-23 hours.
   - **Maximum number of times PIN can be used in access points**—Specify the maximum number of times a PIN can be used in access points. Valid values: Until expiration, 1-5.
   - **Authorized common areas**—Select the common areas to authorize on the PIN. At least one common area must be authorized.
5. Configure mobile key delegation options:
   - **Enable Mobile Key delegation for this resident**—When the feature is enabled, the mobile key delegation section displays, settings can be customized, and settings can be updated on mobile devices.

- **Maximum number of active mobile keys available**—Specify the maximum number of delegated mobile keys that can be active for the resident. Valid values: 1-50.
- **Maximum time mobile key is active before expiring**—Specify the maximum number of days/hours that a delegated mobile key can be active. Range: 0-15 days/0-23 hours.
- **Authorized common areas**—Select the common areas to authorize on the delegated mobile key. At least one common area must be authorized.

6. To update settings on the resident's mobile device, click **Update mobile device**.

Staff & Vendors

Staff and Vendor Management

This section includes the following subjects:

Learning about Staff/Vendor Management and Staff/Vendor Keys 185
Add staff members/vendors 187
Import staff/vendor list 189
Make Emergency keys 191
Make Staff key (predefined access) 194
Make Staff Keys (variable access) 198
Make Vendor keys 202
Make Limited Use keys 206
Replace Staff/Vendor Keys 210
Invalidate staff/vendor access 212
Configure Visitor Management for staff/vendors 217

Learning about Staff/Vendor Management and Staff/Vendor Keys

Staff and vendors are the key holders who work at or perform a service on the property. Most staff are people whose rights are limited to using the keys issued to them, for example, maintenance personnel. Some staff, however, require access to Community. The staff who have access to Community are called *Operators*.

A staff member is designated an Operator in the staff profile. The degree of access depends on the selected Operator role. For example, an Operator with the predefined *Administrator* role has access to all Community functions whereas the rights for an Operator with the predefined role *Leasing Agent* are limited to **Resident Management** and **Read Key** functions.

You can add staff/vendors manually or import a list.

Staff/vendor profiles

When a staff member or vendor is added to Community, a profile is created with the following tabs:

- **Staff/Vendor Info**—This tab is where basic identification details about staff/vendors are defined and notifications are enabled. The option to designate the staff member as an Operator is on this tab.
- **Operator Info**—This tab is where Operator access is configured. The tab is only active if the staff member is designated as an Operator.
- **Assigned Keys**—This tab lists active keys assigned to the staff member/vendor. You can cancel and/or replace keys in the list.
- **Visitor Management**—This tab is where PIN delegation can be enabled and configured for the staff member/vendor.

To view a staff member/vendor profile:

» Go to **Staff/Vendor Management** and select a staff member/vendor.

You can filter the list of profiles based on status (Active/Deactivated/Operators only).

Importing staff/vendors

If the *Import list* right is enabled in **Role Management**, you can create staff/vendor profiles by importing a CSV file that contains basic data (*firstname/lastname/ID*). Any additional information, including the option to designate Operators, must be specified manually in the staff/vendor profile. The *Import list* right is enabled by default for the Administrator and Site Configurator roles.

Visitor Management

Visitor management is a complimentary feature that works exclusively with AuroraSync and mobile keys. Visitor management to provides residents and staff the ability to extend all or part of their access to on-site visitors. Using the dormakaba BlueSky app, residents and staff can generate PIN codes to authorize perimeter and common area access. Residents also have the option to delegate mobile keys for visitors that can work on common doors and the resident's unit if desired.

A PIN is a 7-digit sequence that can be used at access points where a numeric keypad is installed. A delegated mobile key (or PIN code in mobile key format) provides access using the dormakaba BlueSky app.

When Visitor Management is enabled in System Settings for staff/vendors, PIN delegation can be enabled/disabled on the Visitor Management tab in staff/vendor profiles. When Visitor Management is enabled in System Settings for residents, PIN and mobile key delegation can be enabled/disabled on the Visitor Management tab in resident profiles.

Prerequisites include:

- AuroraSync must be enabled and configured.
- Mobile keys must be enabled and configured.
- The resident profile must include a valid mobile number.
- The dormakaba BlueSky app must be installed and registered on the mobile device used to generate PIN code/mobile key.

Staff/vendor keys

Staff/vendor keys are made and issued to people who work on the site, which may include employees, contractors and vendors. Staff/vendor keys are encoded with a credential defined in **Access Management > Credential Management** that may include access to all access point types: units, suites, common areas (resident and staff), and restricted areas.

Staff/vendor keys are made in the **Staff/Vendor Keys** module. Key instances are subsequently managed in **Staff/Vendor Management** by selecting the staff/vendor to whom the key (instance) was assigned and then the **Assigned Keys** tab in the profile.

Staff/vendor keys are valid in staff and resident common areas and elevator controllers until key expiration is reached. Note that staff/vendor keys with the status Obsolete continue to allow access to common areas and elevator controllers until key expiration. To maintain security for keys with an obsolete status, create a block key for the key sequence. See System Settings > Block Keys.

For information about invalidating staff access, see Invalidating staff access.

Add staff members/vendors

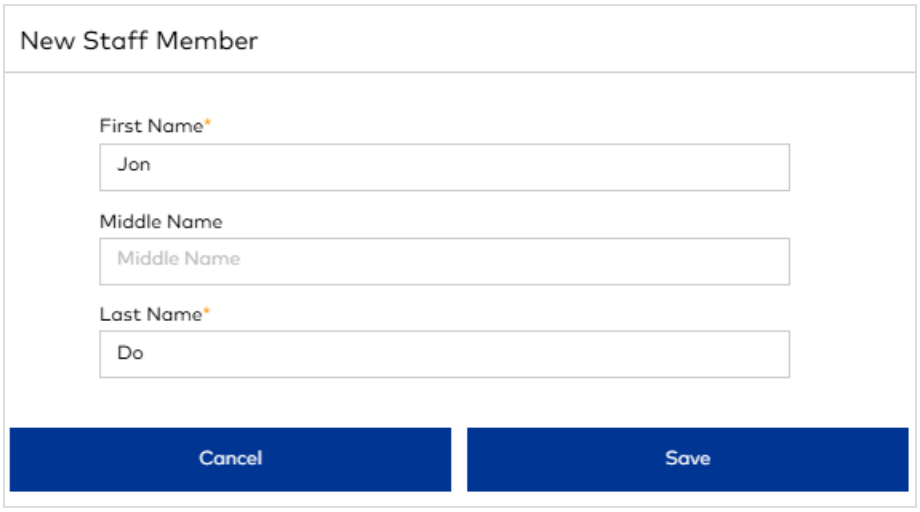
Staff members are the key holders in your organization. Vendors are key holders outside of your organization whose access is restricted to the spaces where they need to perform work. You must add all staff and vendors who will be issued a key.

You can add staff members manually or, if the *Import staff list* right is enabled in **Role Management**, you can import staff members. The import is limited to creating staff profiles with basic data: *firstname*/*lastname*/*ID*. After the import, any additional information about a staff member must be added manually in their respective staff profile.

If you are adding a staff member who you want to designate as an Operator, see "Configure Operators" in *Site Configuration*.

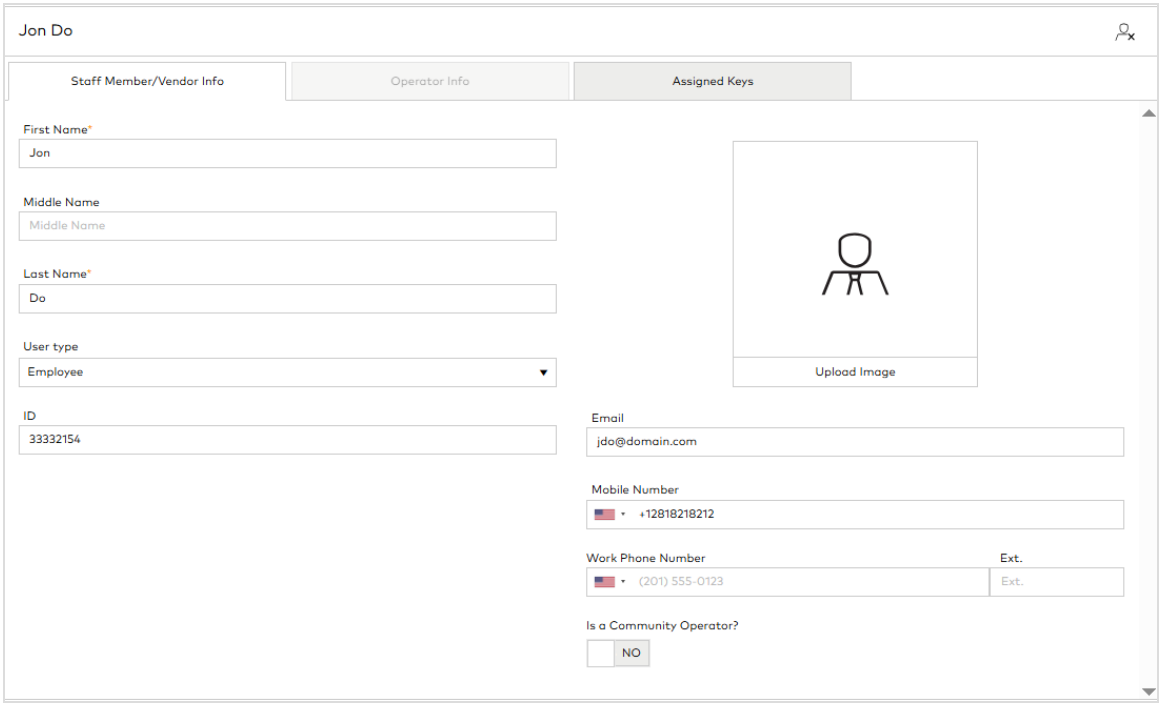
To add a staff member or vendor:

1. Go to **Staff/Vendor Management**.
2. Click **(Add)** .



3. Specify the name of the staff member/vendor. Use the middle name to distinguish between staff with the same first and last names. Max chars per field: 25.
4. Click **Save**. Community creates a staff/vendor profile and displays the **Staff/Vendor** tab. No other options are required unless you want to send automated emails to the staff member/vendor, enable notifications for the staff member/vendor or designate the staff member as an Operator.

If phone/mobile number validation override is enabled in **System Settings**, Operators can permit use of unknown numbers.

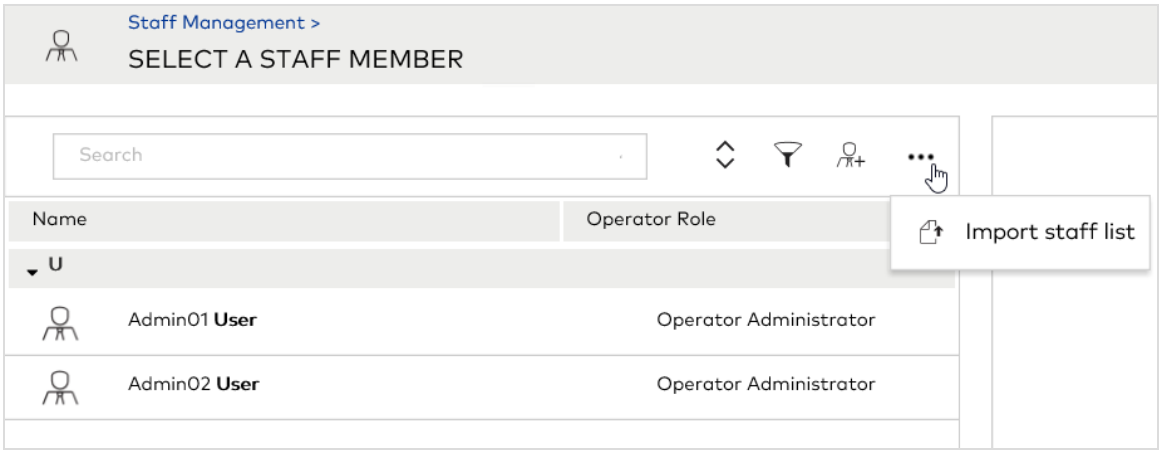


5. (*recommended*) For **Email**, specify a valid email address for the staff member/vendor. An email address is required to send automated emails regarding account access and to send notifications via email. (For Operators, the email address can be changed in account **Preferences**.)
6. Select whether to enable notifications and, if enabled, select the notification groups to subscribe for the staff member/vendor.
7. Click **(Save)** .

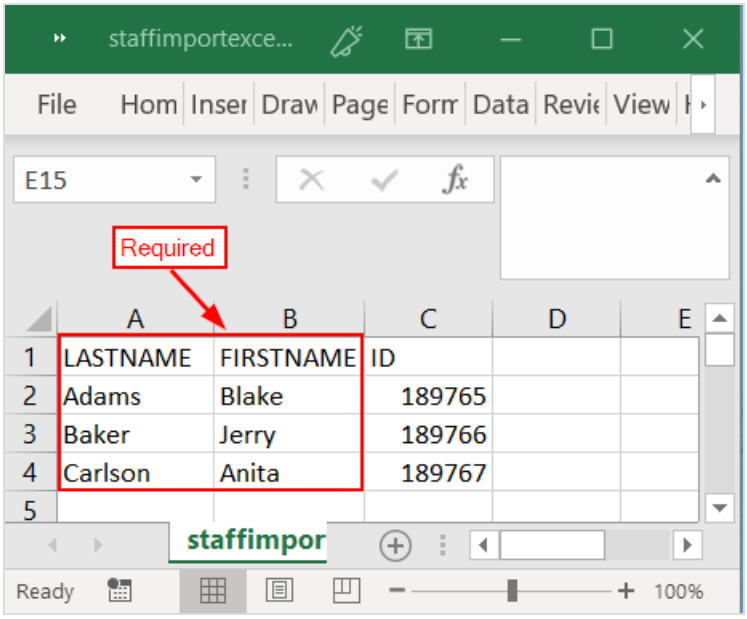
Import staff/vendor list

To import staff/vendor:

1. Go to **Staff/Vendor Management**.
2. Click **(More)** ▪▪▪ > **Import staff list**.

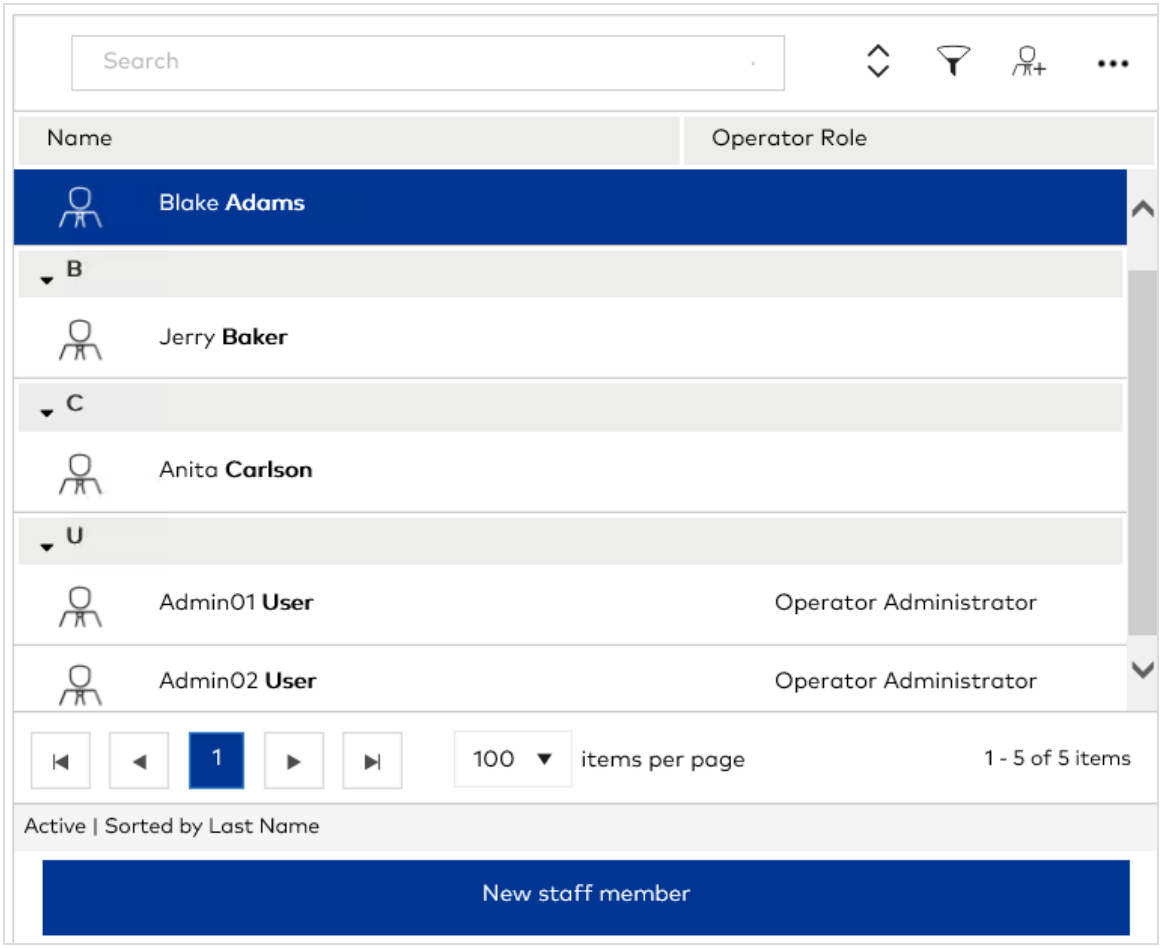


3. Navigate to and select the file that you want to import, then click **Open**. Supported files type: csv. The following figure shows a sample file and the required data format. If a required field is missing, the staff member/vendor is not added.



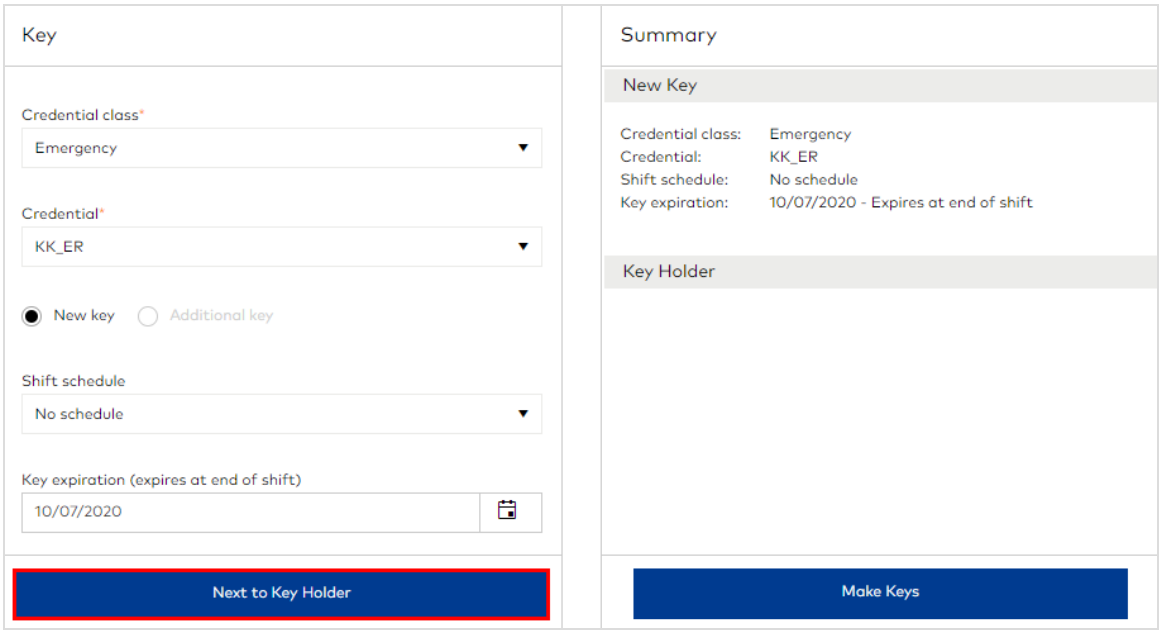
> If staff member profiles have already been created, you are prompted to proceed. Click **YES** to proceed.

4. When notified the import is successful, click **OK**.

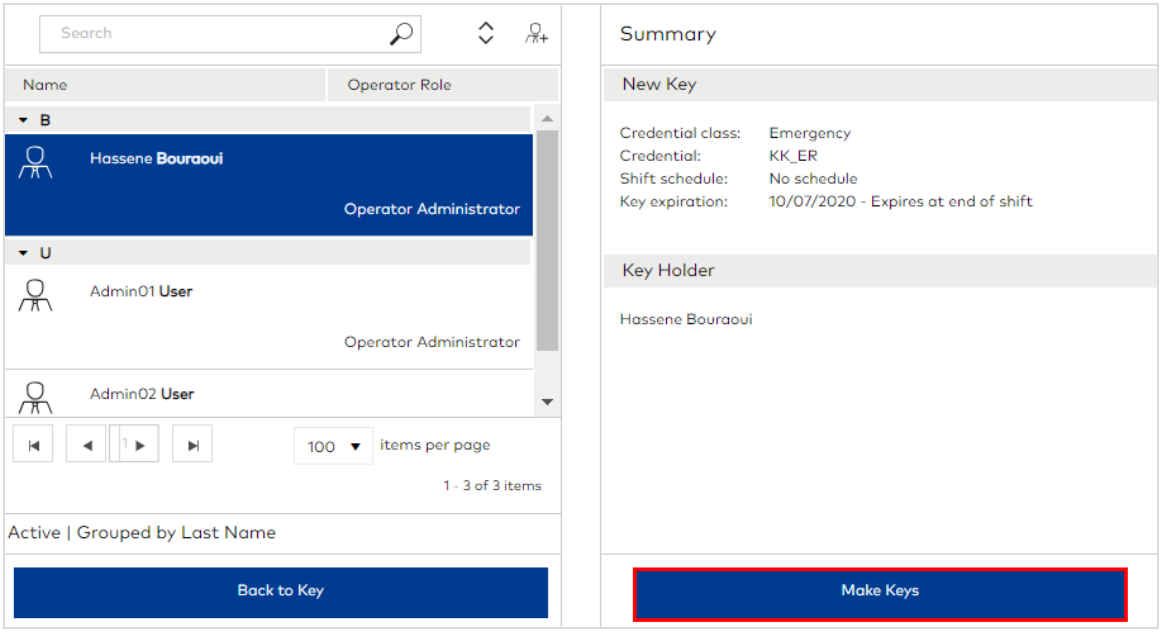

Search
Name
Operator Role
Blake Adams
B
Jerry Baker
C
Anita Carlson
U
Admin01 User
Operator Administrator
Admin02 User
Operator Administrator
1
100
items per page
1 - 5 of 5 items
Active | Sorted by Last Name
New staff member

Make Emergency keys

1. Go to **Staff/Vendor Keys**.



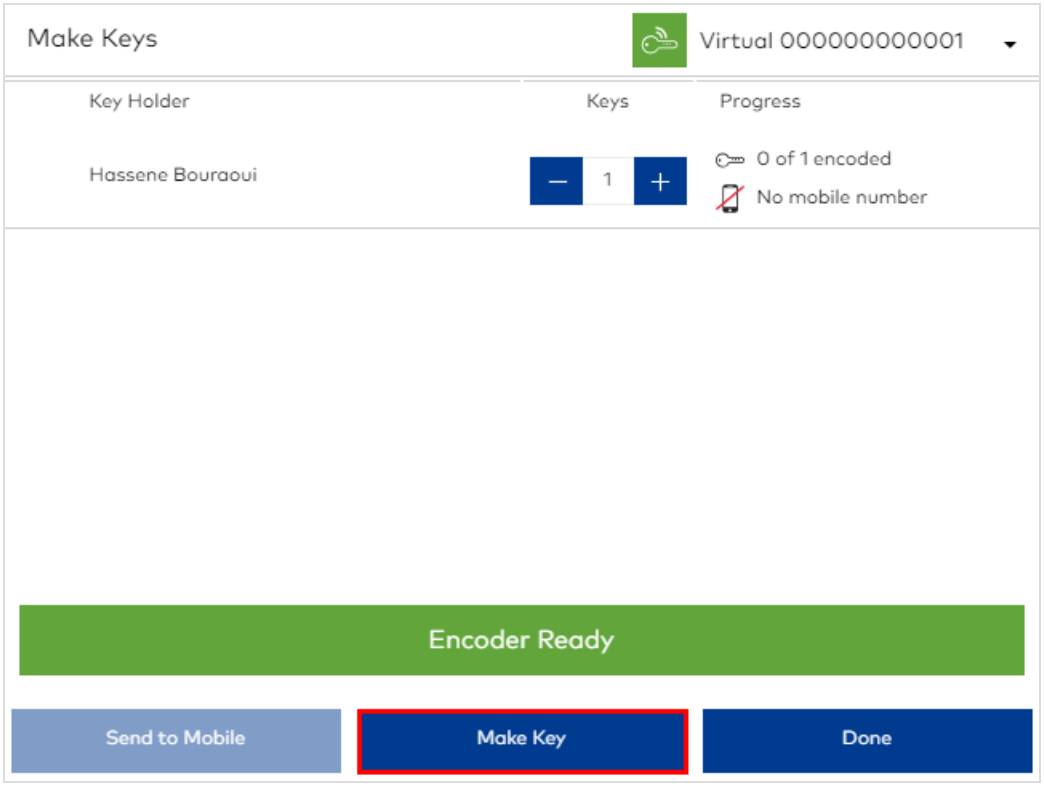
2. Select the **Emergency** credential class or a custom class based on the Emergency class type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.
4. Select whether to make a **New** or **Additional** key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Click **Next to Key Holder**, then select the staff member/vendor to whom you want to assign the key. To add a staff member/vendor, click **(Add)** , specify first and last names, then click **Save**.



8. Click **Make Keys**.

> To make a mobile key, click **Send to Mobile**.

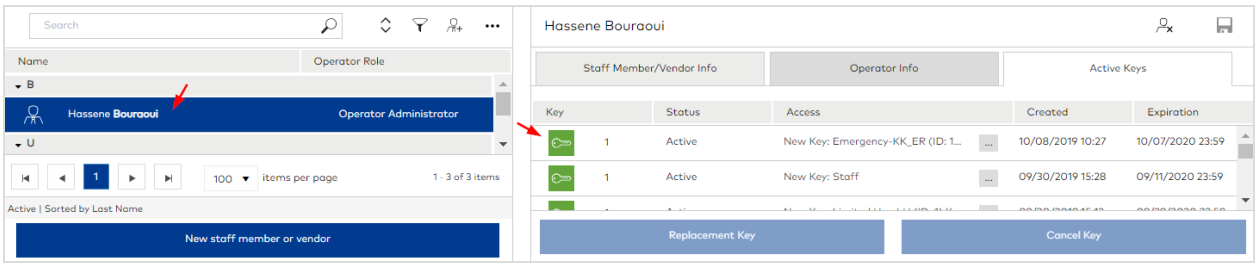
9. Specify the number of keys to make.
10. Select an encoder that is online.
11. Click **Make Key**.
12. Present keys to the encoder (as prompted).



If all Key IDs for the selected credential are assigned to active keys, a warning notifies that to continue, an existing Key ID must be selected. To reuse a Key ID, click **Continue**, then select the Key ID to reuse. Only one key can be made. Reusing Key IDs results in having multiple key holders assigned to the same key and results in less traceability in audits. Key holders using the same Key ID become possible not absolute key holders.

13. When notified that the key request is complete, click **Done**.

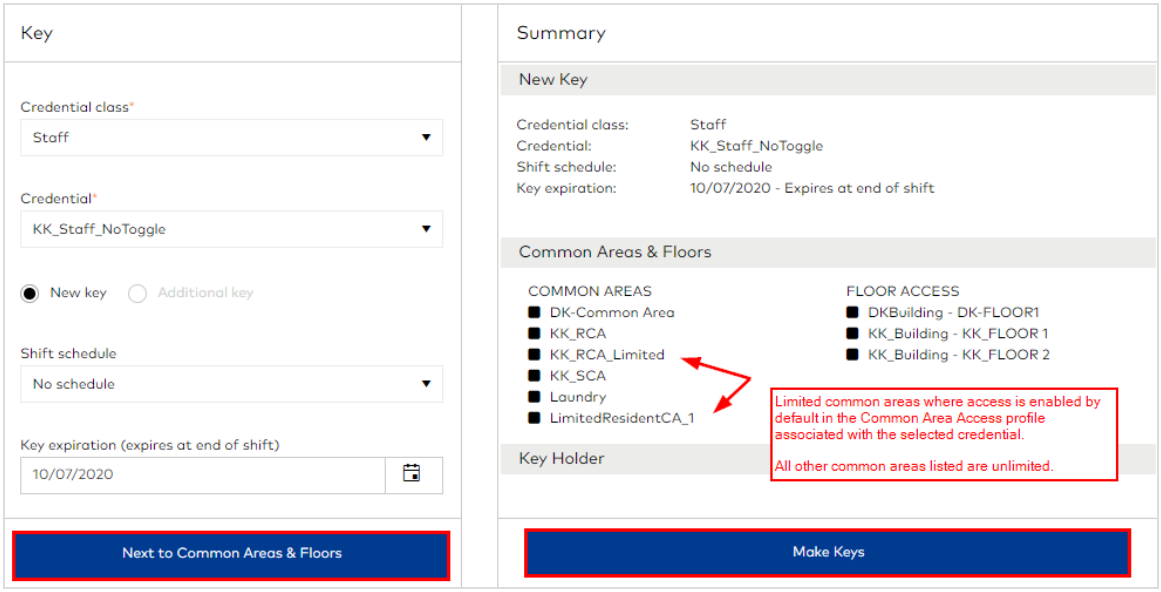
The key is listed on the **Assigned Keys** tab in the staff member/vendor profile.



You can verify that a mobile key was delivered in **Staff/Vendor Management**.

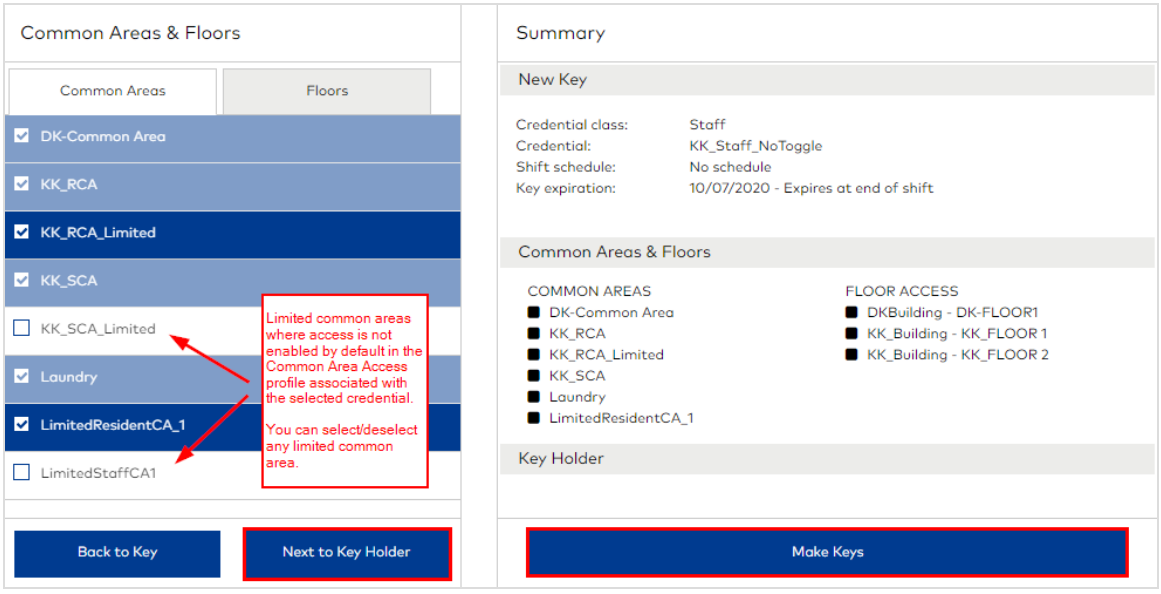
Make Staff key (predefined access)

1. Go to **Staff/Vendor Keys**.
2. Select the **Staff** credential class or a custom class based on the same type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.



When you select a credential, the unlimited common areas and limited common areas where access is enabled in the Common Area Access profile associated with the credential are listed. Floor access is dynamically selected based on the location of access points to be authorized on the key.

4. Select whether to make a **New** or **Additional** key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Take one of the following actions:
   - Click **Next to Common Areas**, **Next to Floors**, or **Next to Common Areas & Floors** and proceed to the next step.
   - Click **Next to Key Holder** and proceed to step 10.
8. Select the common areas and/or floor access to add on the key.

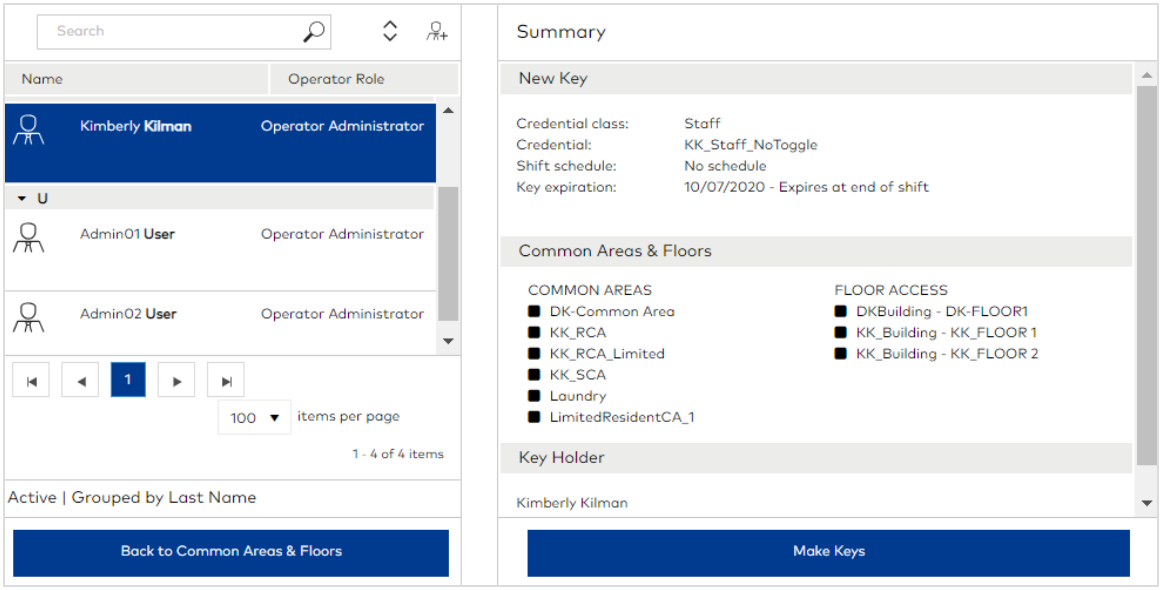


- When the **Common Areas** tab is listed, any unlimited common areas (staff and resident) are selected by default and cannot be deselected. Limited-access common areas (staff and resident) are listed if they are selected in a Common Area Access profile associated with the selected credential.
- When the **Floor Access** tab is listed, all floors where elevator access is configured are listed. By default, floor access is dynamically selected based on the location of access points to be authorized on the key.

Take caution to not remove default floor access.

When ready, click **Next to Key Holder** and proceed to the next step.

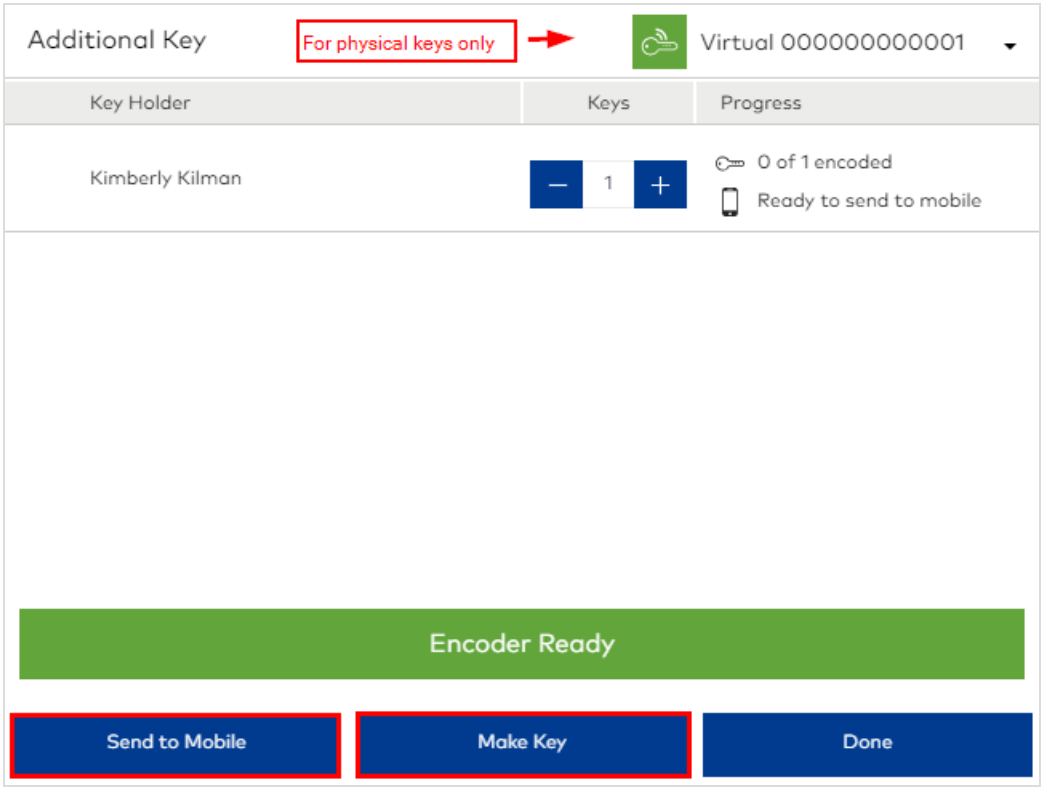
9. Select the staff member/vendor to whom you want to assign the key. To add a staff member/vendor, click (Add) , specify first and last names, then click **Save**.



10. Click **Make Keys**.

To make a mobile key, click **Send to mobile**.

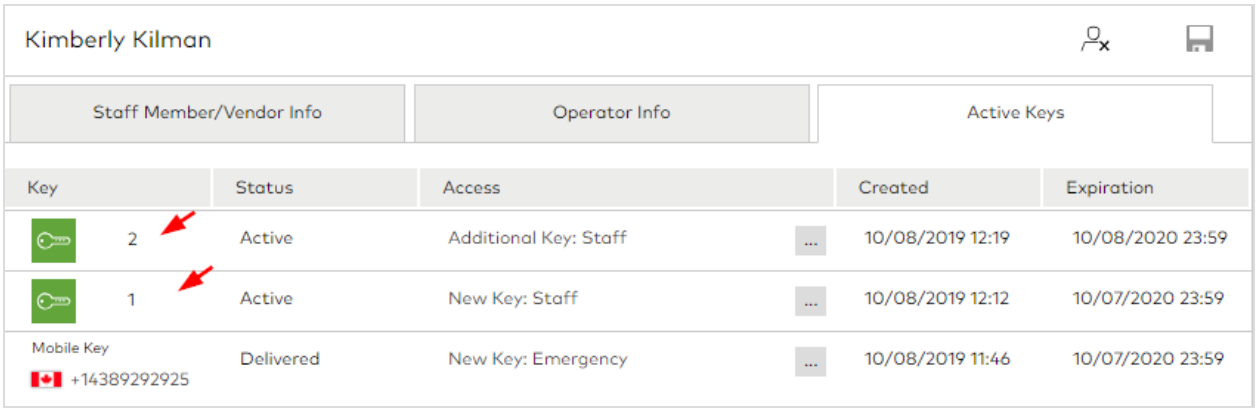
11. Specify the number of keys to make.
12. Select an encoder that is online.
13. Click **Make Key**.
14. Present keys to the encoder (as prompted).



If all Key IDs for the selected credential are assigned to active keys, a warning notifies that to continue, an existing Key ID must be selected. To reuse a Key ID, click **Continue**, then select the Key ID to reuse. Only one key can be made. Reusing Key IDs results in having multiple key holders assigned to the same key and results in less traceability in audits. Key holders using the same Key ID become possible not absolute key holders.

15. When notified that the key request is complete, click **Done**.

The key is listed on the **Assigned Keys** tab in the staff member/vendor profile.

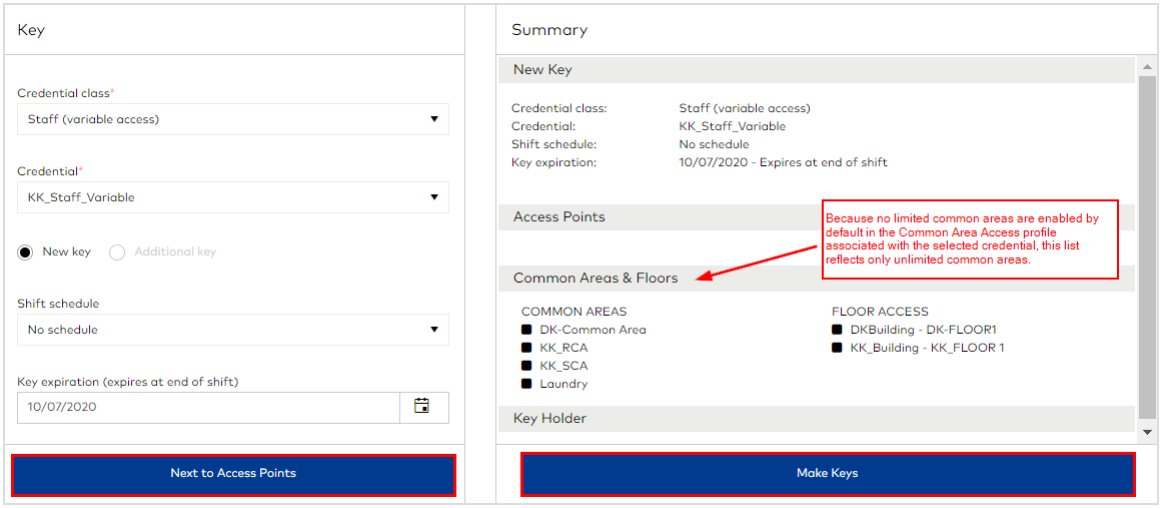




You can verify that a mobile key was delivered in **Staff/Vendor Management**.

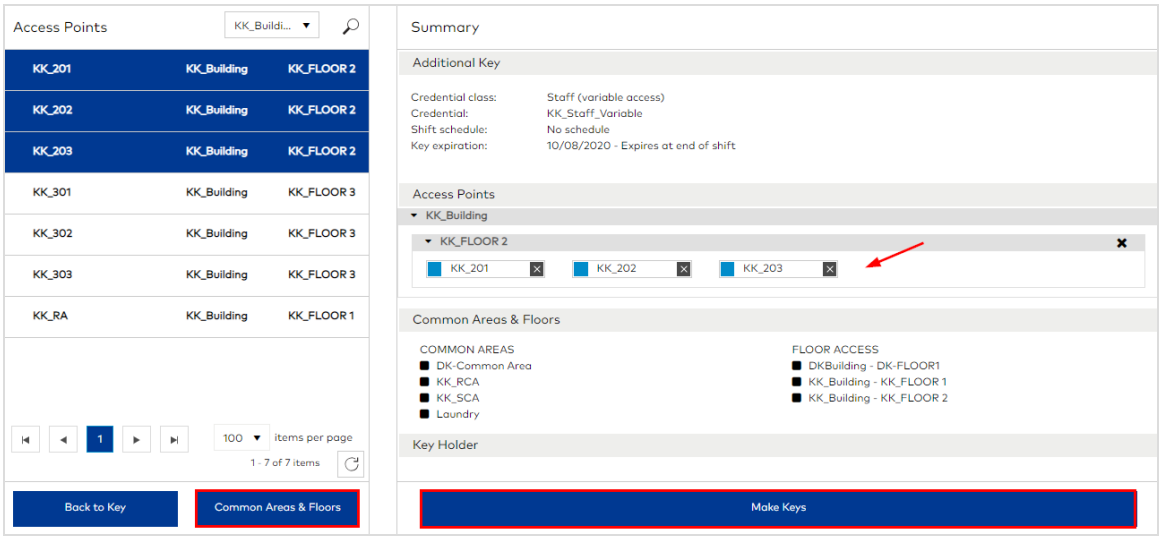
Make Staff Keys (variable access)

1. Go to **Staff/Vendor Keys**.
2. Select the **Staff (variable access)** credential class or a custom class based on the same type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.



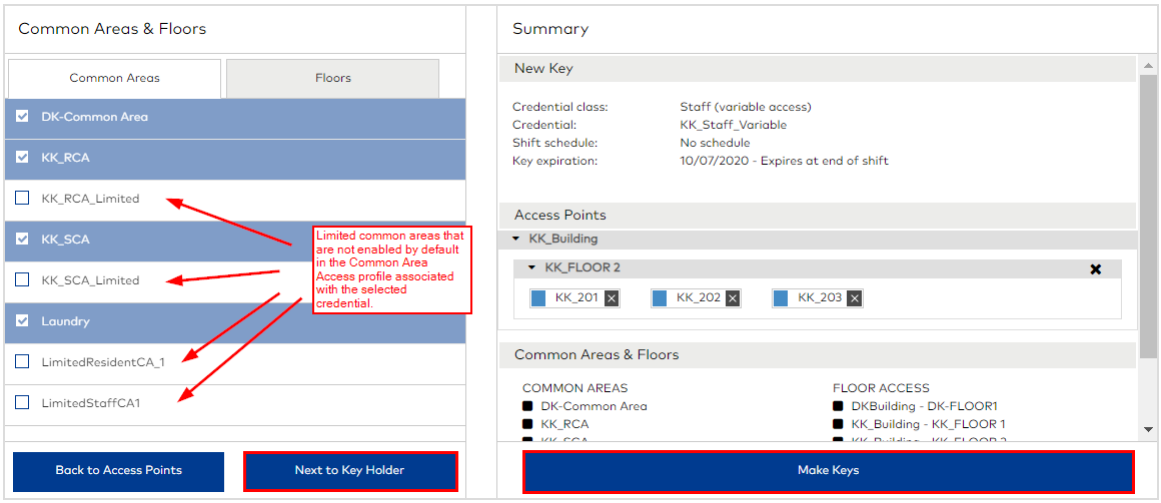
When you select a credential, the unlimited common areas and limited common areas where access is enabled in the Common Area Access profile associated with the credential are listed. Floor access is dynamically selected based on the location of access points to be authorized on the key.

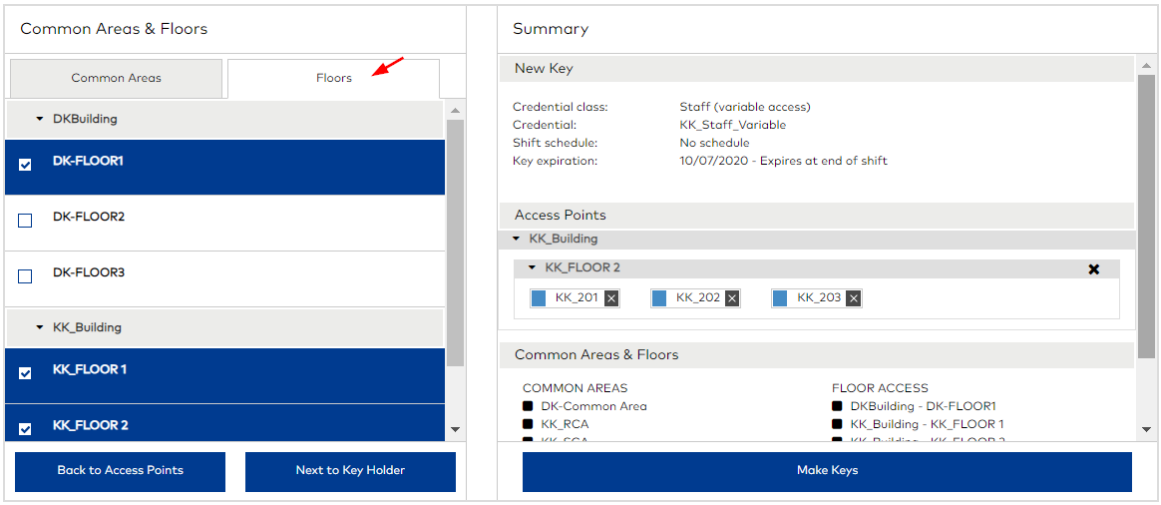
4. Select whether to make a **New** or **Additional** key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Click **Next to Access Points**.



8. Select the access points to add on the key. Access point types listed: Units/Suite Units and Restricted Areas. You can select access points from different buildings. The maximum access points that you can select are: 542 (4k keys), 94 (1k keys), 25 (mobile keys). Selected access points are added to the **Summary** section (listed by building and floor).

9. Take one of the following actions:
   - Click **Common Areas & Floors**, **Common Areas**, or **Floor Access** and proceed to the next step.
   - Click **Next to Key Holder** and proceed to step 12.
10. Select the common areas and/or floor access to add on the key.



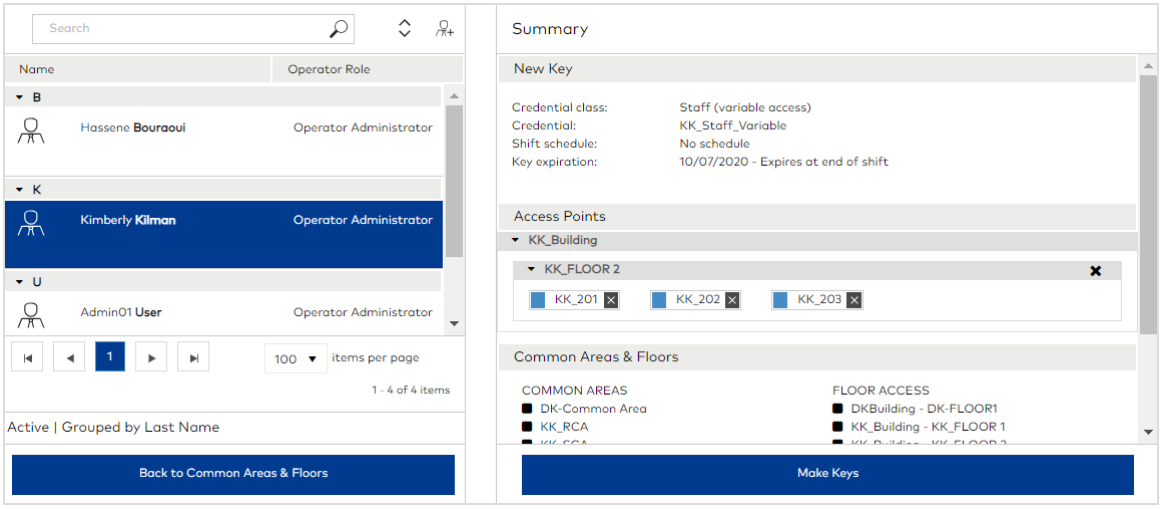


- When the **Common Areas** tab is listed, any unlimited common areas (staff and resident) are selected by default and cannot be deselected. Limited-access common areas (staff and resident) are listed if they are selected in a Common Area Access profile associated with the selected credential.
- When the **Floor Access** tab is listed, all floors where elevator access is configured are listed. By default, floor access is dynamically selected based on the location of access points to be authorized on the key.

Take caution to not remove default floor access.

When ready, click **Next to Key Holder** and proceed to the next step.

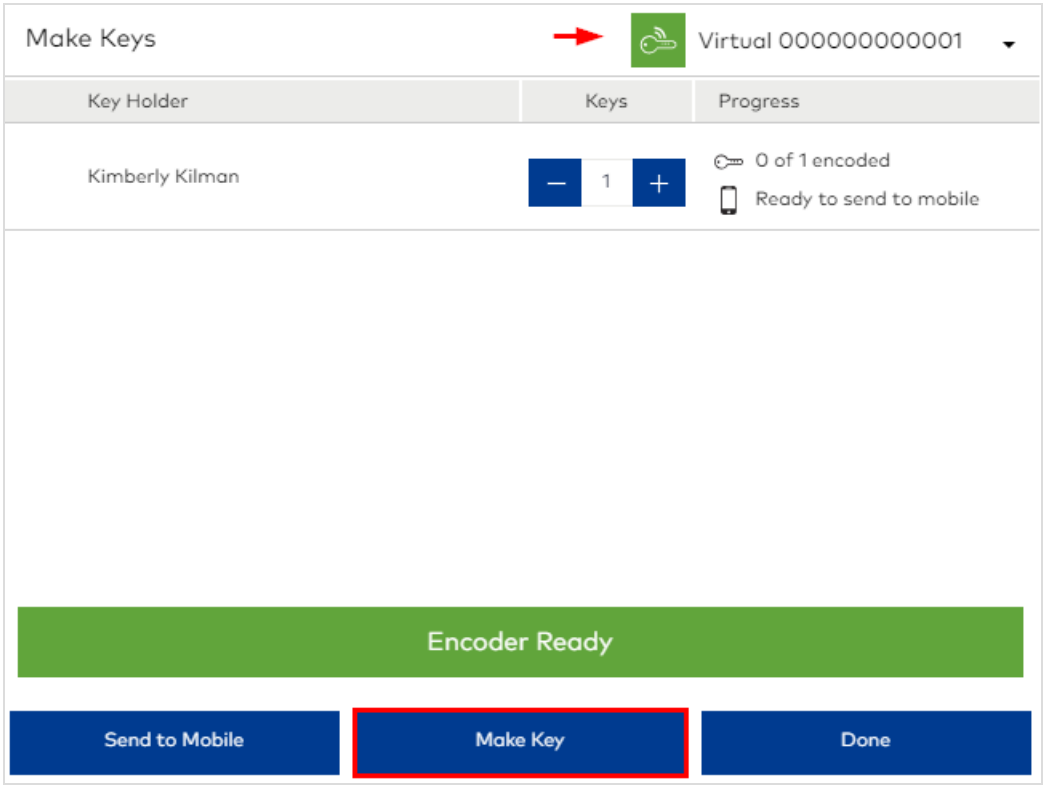
11. Select the staff member/vendor to whom you want to assign the key. To add a staff member/vendor, click (Add) , specify first and last names, then click **Save**.



12. Click **Make Keys**.

> To make a mobile key, click **Send to mobile**.

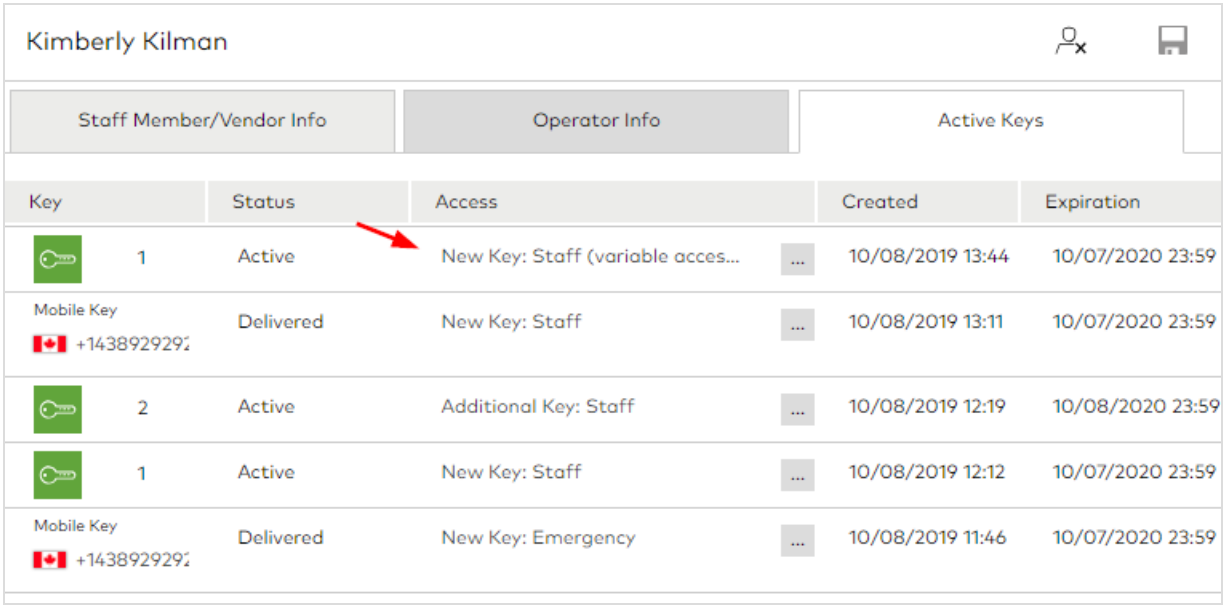
13. Specify the number of keys to make.
14. Select an encoder that is online.
15. Click **Make Key**.
16. Present keys to the encoder (as prompted).



If all Key IDs for the selected credential are assigned to active keys, a warning notifies that to continue, an existing Key ID must be selected. To reuse a Key ID, click **Continue**, then select the Key ID to reuse. Only one key can be made. Reusing Key IDs results in having multiple key holders assigned to the same key and results in less traceability in audits. Key holders using the same Key ID become possible not absolute key holders.

17. When notified that the key request is complete, click **Done**.

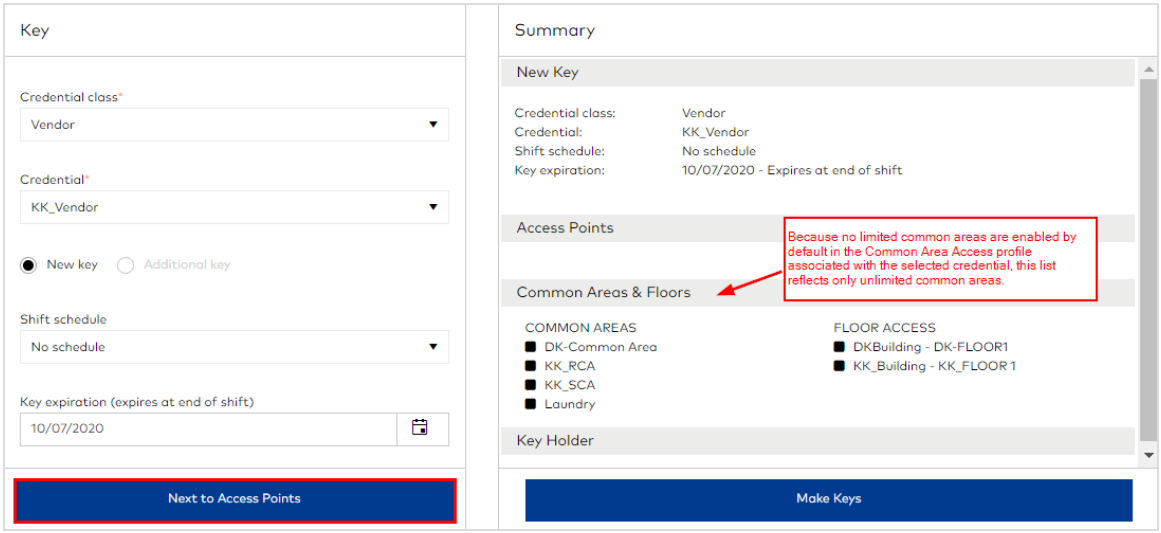
The key is listed on the **Assigned Keys** tab in the staff member/vendor profile.



You can verify that a mobile key was delivered in Staff/Vendor Management.

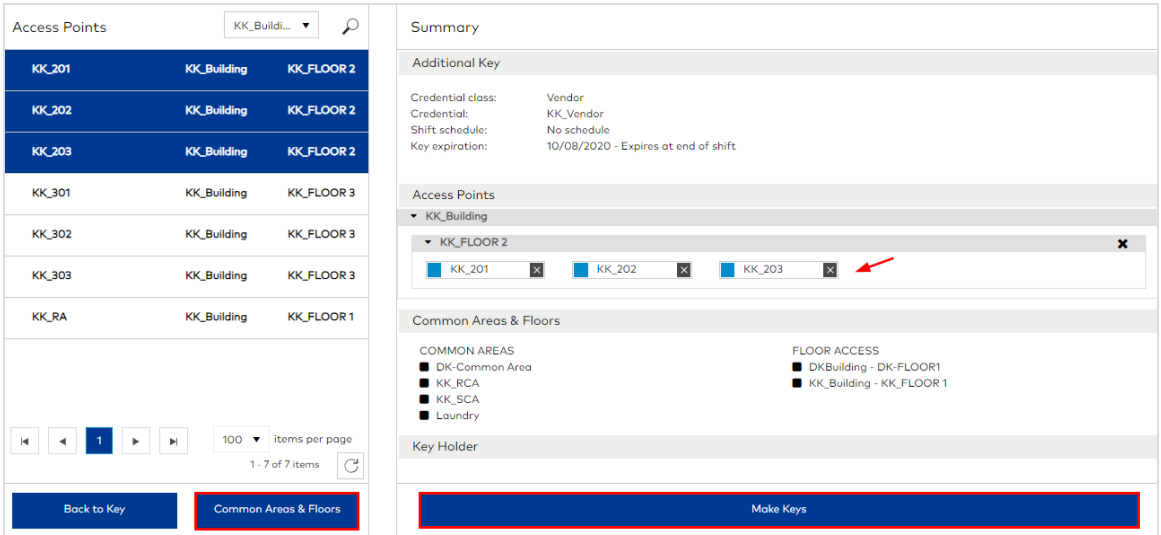
Make Vendor keys

1. Go to **Staff/Vendor Keys**.
2. Select the **Vendor** credential class or a custom class based on the same type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.



When you select a credential, the unlimited common areas and limited common areas where access is enabled in the Common Area Access profile associated with the credential are listed. Floor access is dynamically selected based on the location of access points to be authorized on the key.

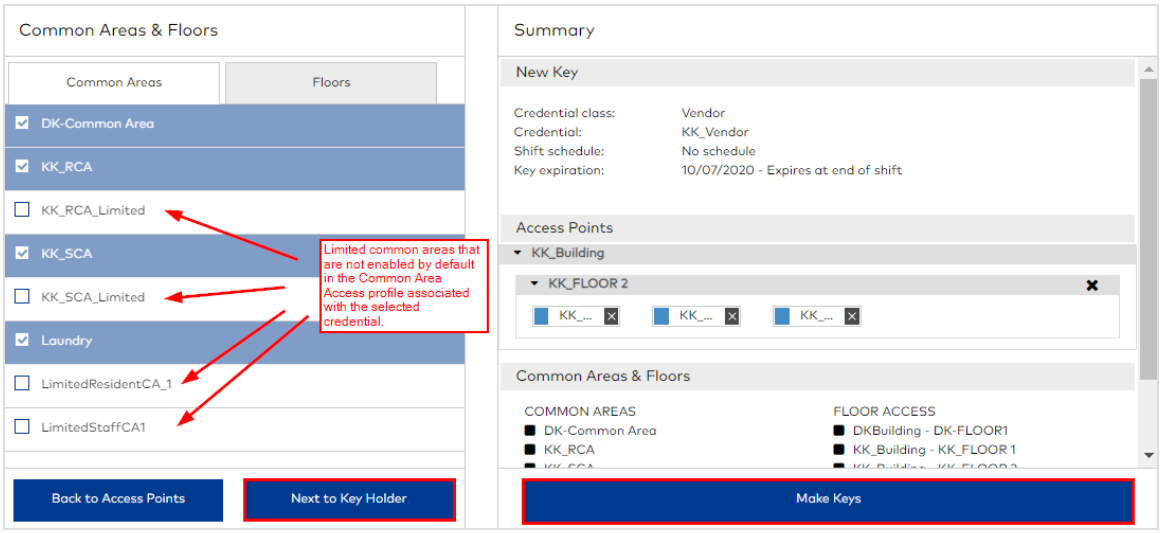
4. Select whether to make a **New** or **Additional** key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Click **Next to Access Points**.

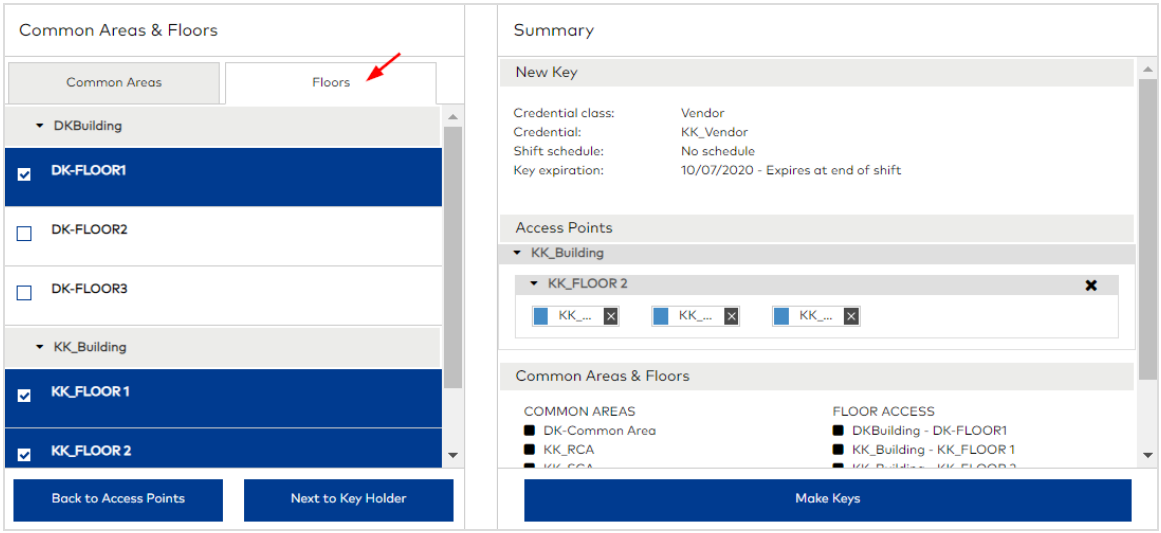


8. Select the access points to add on the key. Access point types listed: Units/Suite Units and Restricted Areas. You can select access points from different buildings. The maximum access points that you can select are: 542 (4k keys), 94 (1k

keys), 25 (mobile keys). Selected access points are added to the **Summary** section (listed by building and floor).

9. Take one of the following actions:
   - Click **Common Areas & Floors**, **Common Areas**, or **Floor Access** and proceed to the next step.
   - Click **Next to Key Holder** and proceed to step 12.
10. Select the common areas and/or floor access to add on the key.



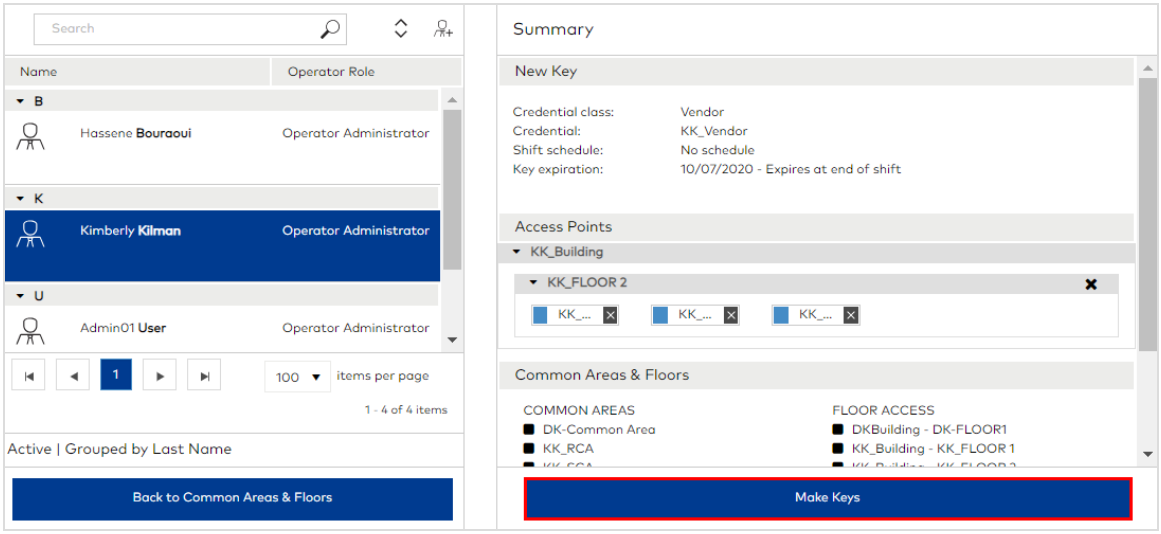


- When the **Common Areas** tab is listed, any unlimited common areas (staff and resident) are selected by default and cannot be deselected. Limited-access common areas (staff and resident) are listed if they are selected in a Common Area Access profile associated with the selected credential.
- When the **Floor Access** tab is listed, all floors where elevator access is configured are listed. By default, floor access is dynamically selected based on the location of access points to be authorized on the key.

Take caution to not remove default floor access.

When ready, click **Next to Key Holder** and proceed to the next step.

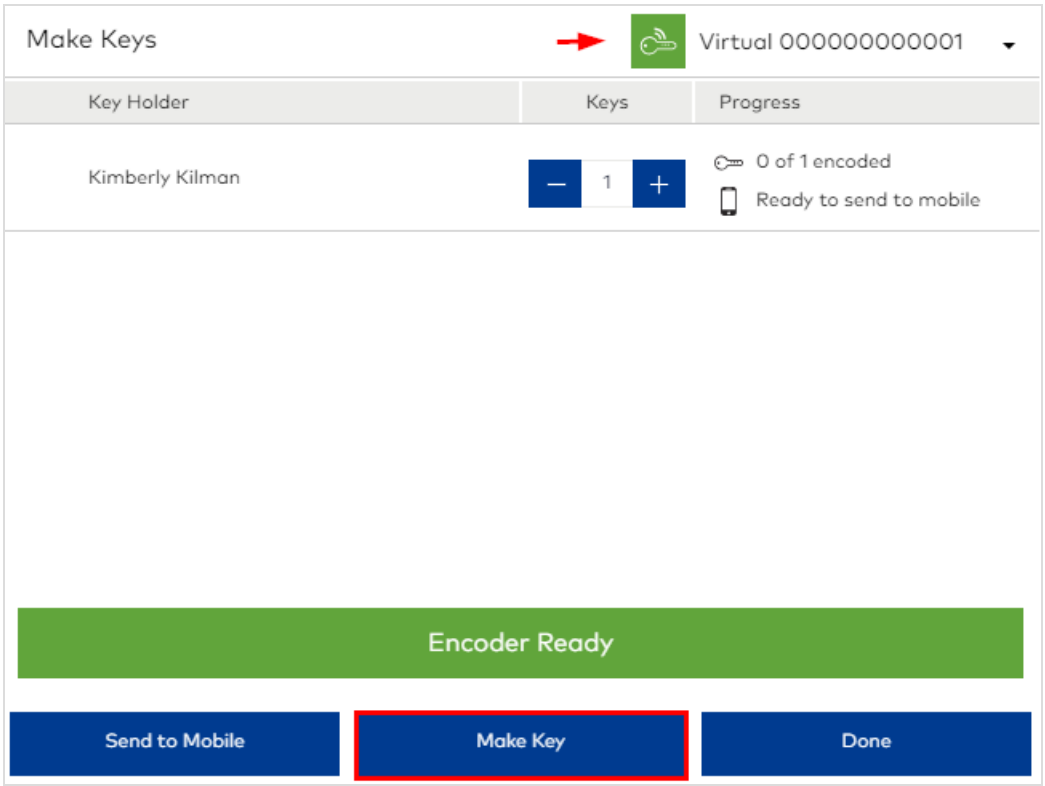
11. Select the staff member/vendor to whom you want to assign the key. To add a staff member/vendor, click (Add) , specify first and last names, then click **Save**.



12. Click **Make Keys**.

> To make a mobile key, click **Send to mobile**.

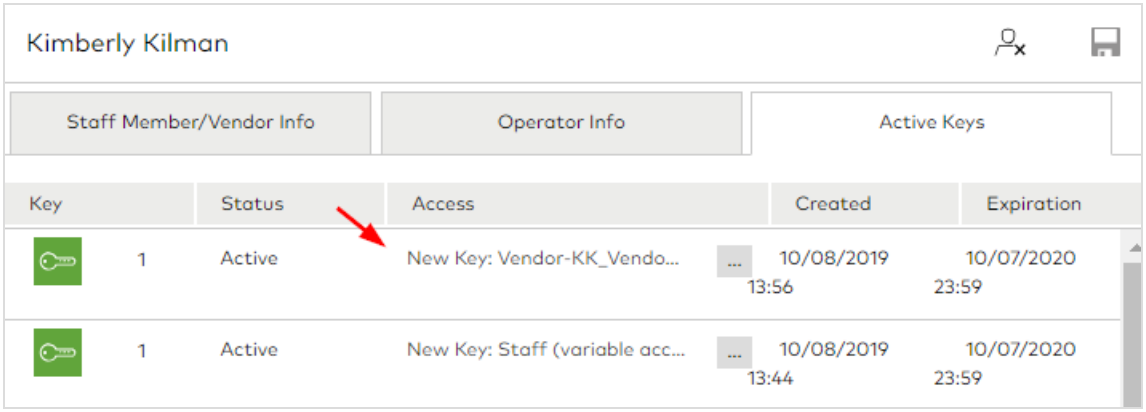
13. Specify the number of keys to make.
14. Select an encoder that is online.
15. Click **Make Key**.
16. Present keys to the encoder (as prompted).



If all Key IDs for the selected credential are assigned to active keys, a warning notifies that to continue, an existing Key ID must be selected. To reuse a Key ID, click **Continue**, then select the Key ID to reuse. Only one key can be made. Reusing Key IDs results in having multiple key holders assigned to the same key and results in less traceability in audits. Key holders using the same Key ID become possible not absolute key holders.

17. When notified that the key request is complete, click **Done**.

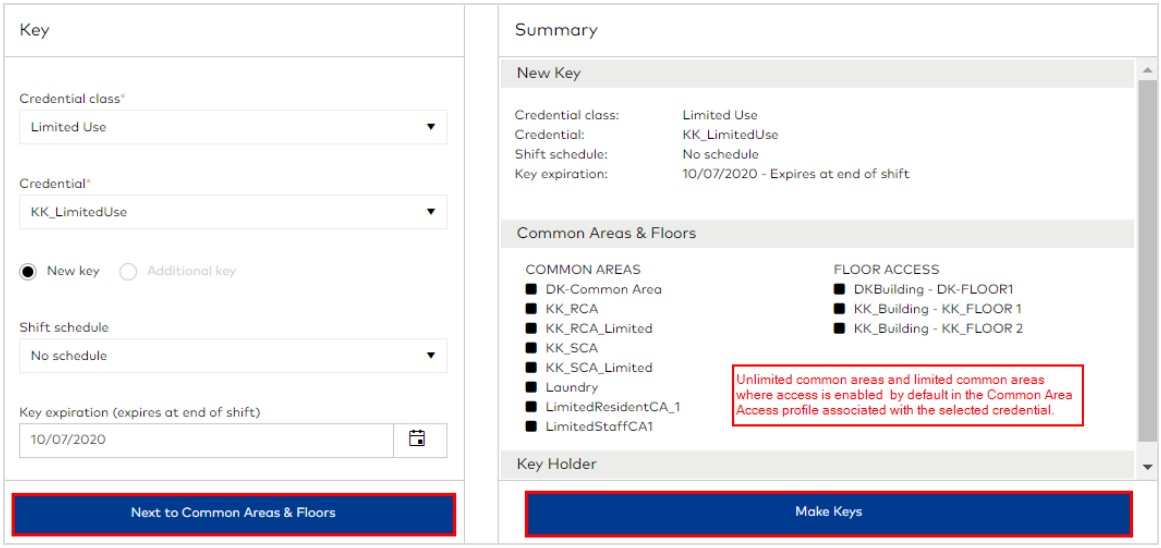
The key is listed on the **Assigned Keys** tab in the staff member/vendor profile.



You can verify that a mobile key was delivered in Staff/Vendor Management.

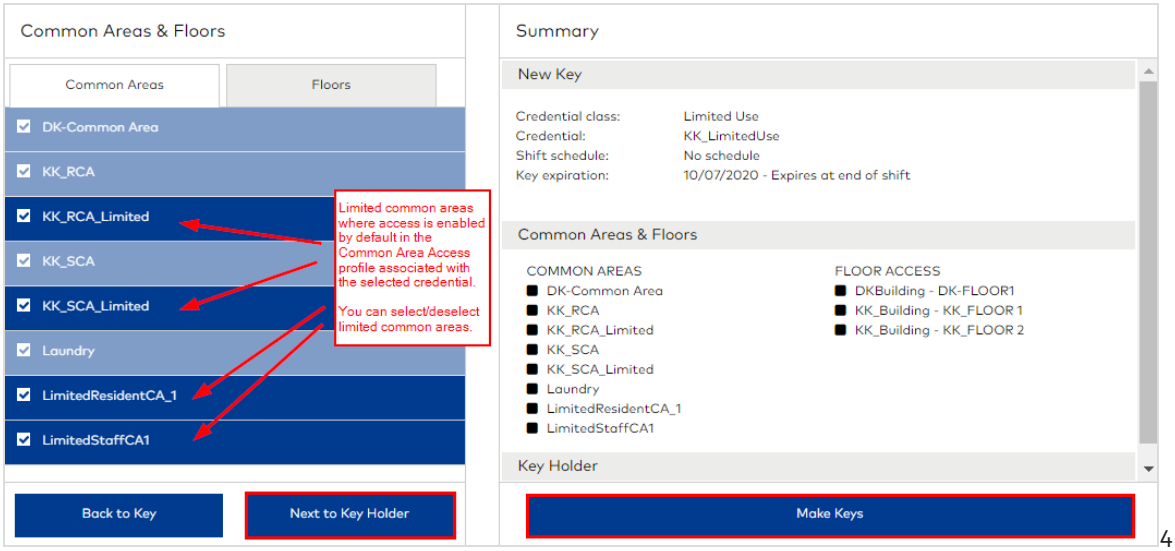
Make Limited Use keys

1. Go to **Staff/Vendor Keys**.
2. Select the **Limited Use** credential class or a custom class based on the Limited Use class type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.

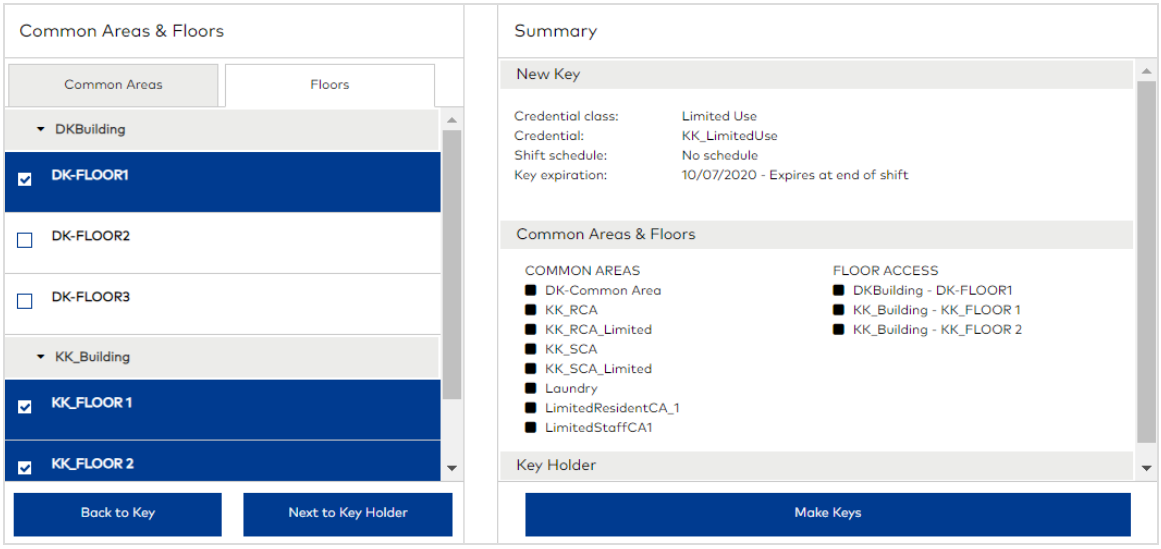


When you select a credential, the unlimited common areas and limited common areas where access is enabled in the Common Area Access profile associated with the credential are listed. Floor access is dynamically selected based on the location of access points to be authorized on the key.

4. Select whether to make a **New** or **Additional** key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Take one of the following actions:
   - Click **Common Areas & Floors**, **Common Areas**, or **Floor Access** and proceed to the next step.
   - Click **Next to Key Holder** and proceed to step 10.
8. Select the common areas and/or floor access to add on the key.



4

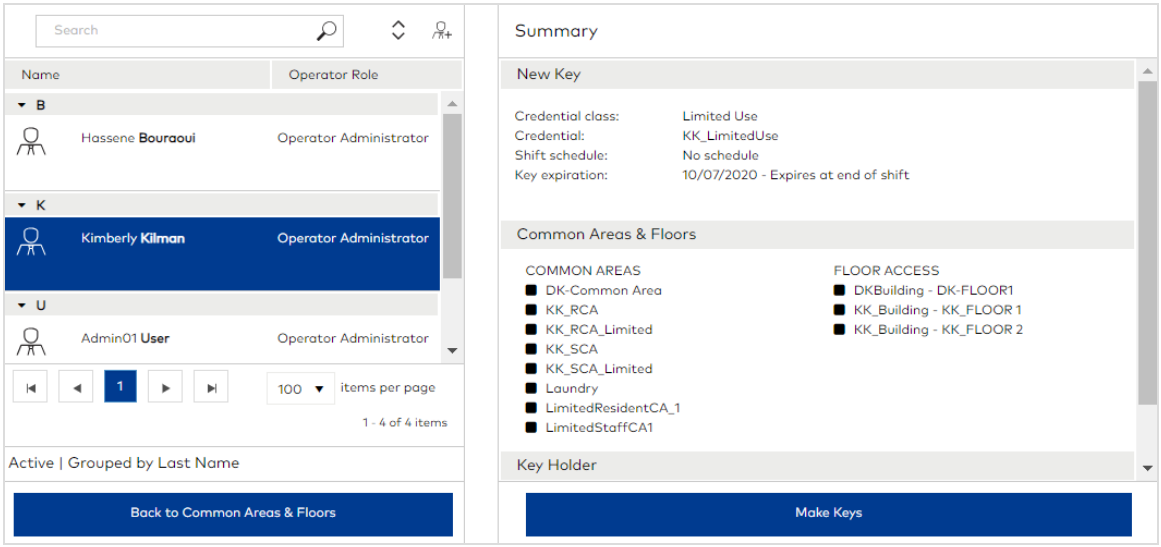


- When the **Common Areas** tab is listed, any unlimited common areas (staff and resident) are selected by default and cannot be deselected. Limited-access common areas (staff and resident) are listed if they are selected in a Common Area Access profile associated with the selected credential.
- When the **Floor Access** tab is listed, all floors where elevator access is configured are listed. By default, floor access is dynamically selected based on the location of access points to be authorized on the key.

Take caution to not remove default floor access.

When ready, click **Next to Key Holder** and proceed to the next step.

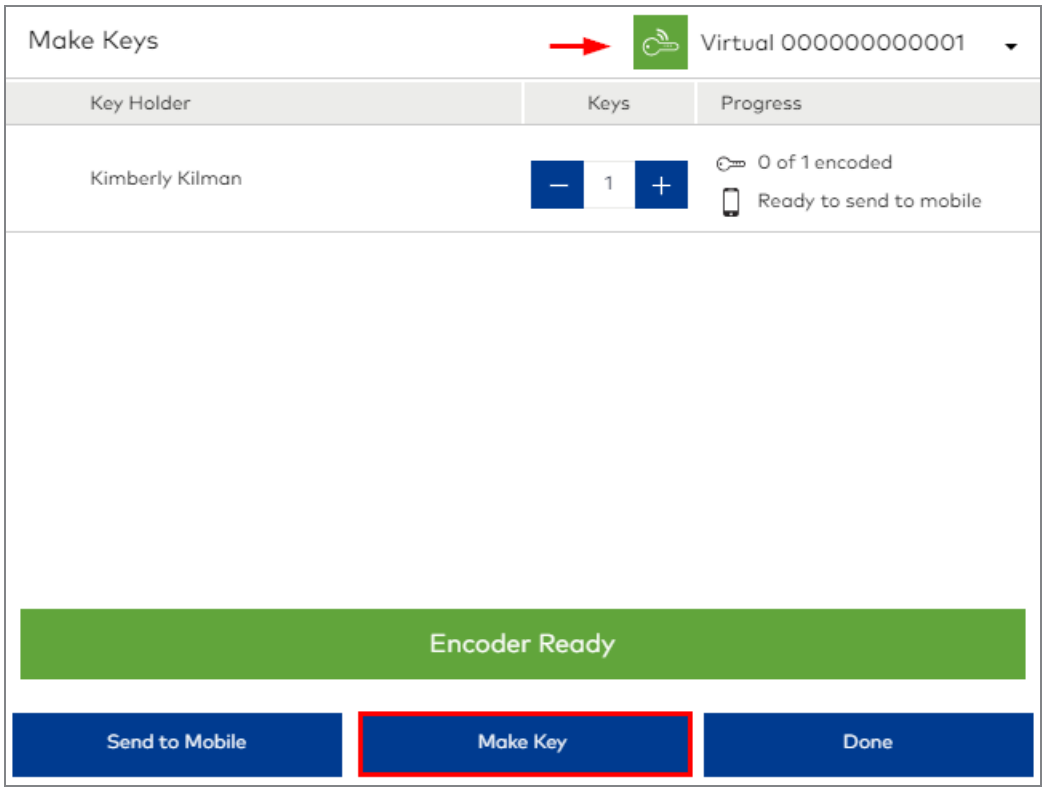
9. Select the staff member/vendor to whom you want to assign the key. To add a staff member/vendor, click **(Add)** , specify first and last names, then click **Save**.



10. Click **Make Keys**.

> To make a mobile key, click **Send to mobile**.

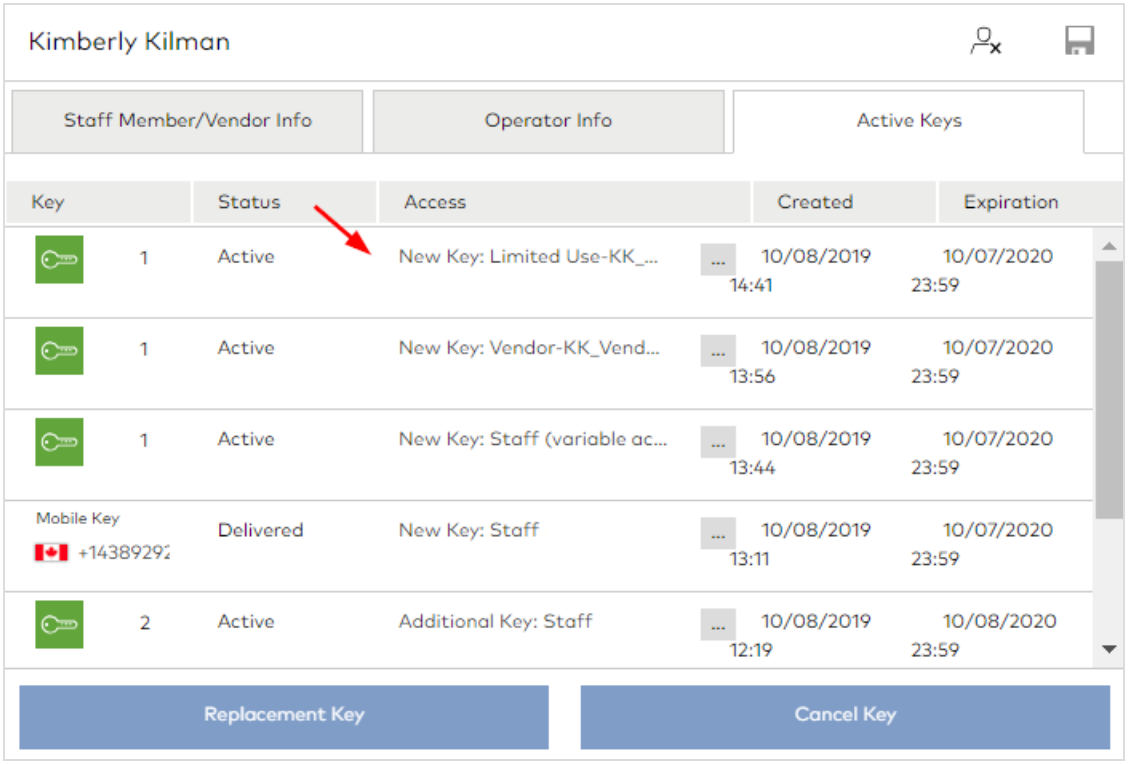
11. Specify the number of keys to make.
12. Select an encoder that is online.
13. Click **Make Key**.
14. Present keys to the encoder (as prompted).



If all Key IDs for the selected credential are assigned to active keys, a warning notifies that to continue, an existing Key ID must be selected. To reuse a Key ID, click **Continue**, then select the Key ID to reuse. Only one key can be made. Reusing Key IDs results in having multiple key holders assigned to the same key and results in less traceability in audits. Key holders using the same Key ID become possible not absolute key holders.

15. When notified that the key request is complete, click **Done**.

The key is listed on the **Assigned Keys** tab in the staff member/vendor profile.

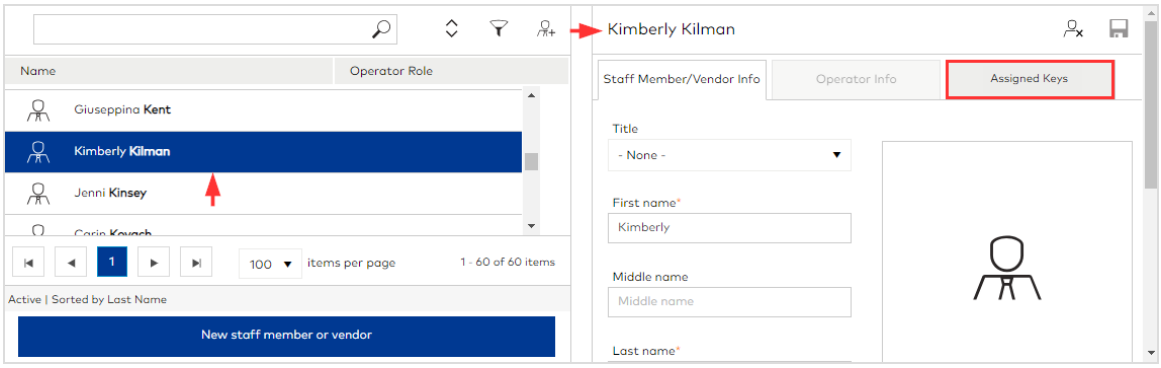


You can verify that a mobile key was delivered in **Staff/Vendor Management**.

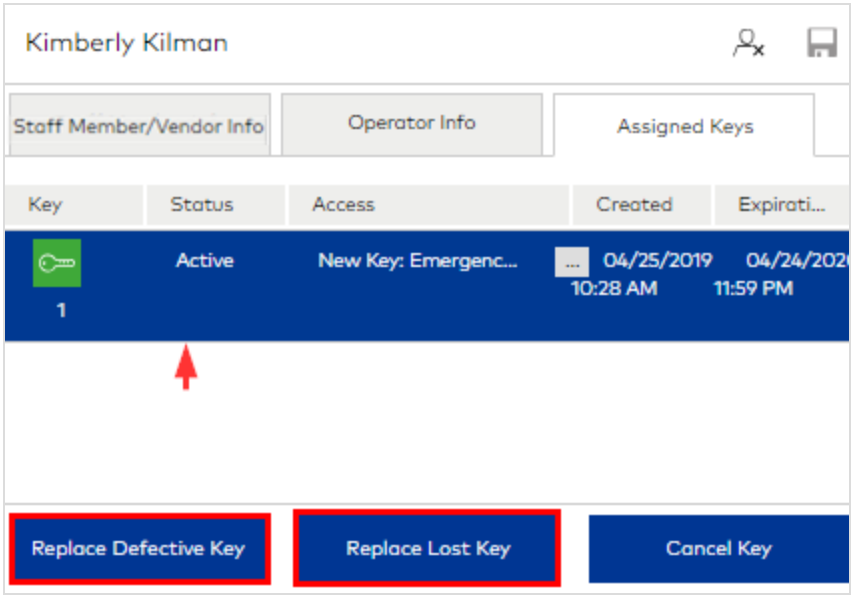
Replace Staff/Vendor Keys

Staff/Vendor Keys that are defective or lost can be replaced.

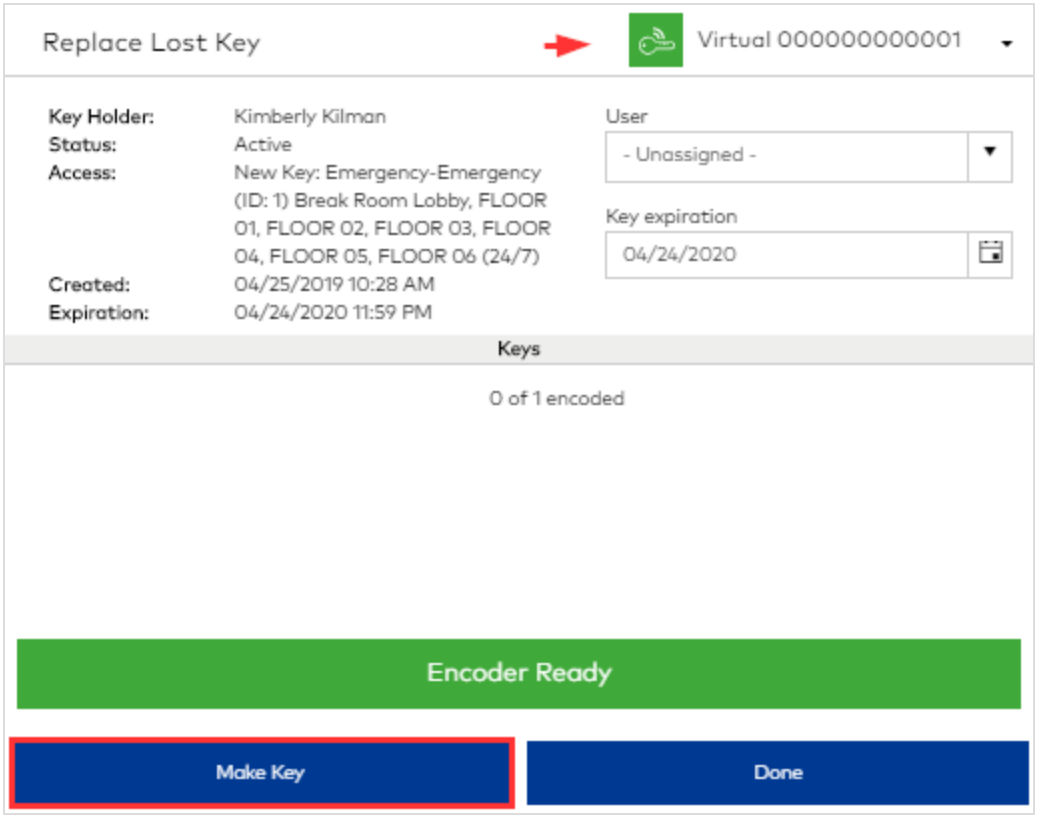
1. Go to **Staff/Vendor Management**.



2. Select the staff member whose key you want to replace.
3. Click the **Assigned Keys** tab.



4. Select the key that you want to replace.
5. Click **Replace Defective Key** or **Replace Lost Key**.



6. (lost keys only) Click **OK** to confirm the operation and to acknowledge the requirement to make and present a Cancel key.
7. Select an encoder  that is online and available to the workstation.
8. Click **Make Key**.
9. Present a key to the encoder.
10. When notified that the key request is complete, click **Done**.

If you replaced a lost key, then you must also make a Cancel Key for the lost key instance and present it to the related access points.

Invalidate staff/vendor access

There are multiple options when you need to invalidate staff/vendor access. The best method depends on the Community modules authorized for your Operator account and the reason that you want to invalidate access.



Don't forget that when invalidating access using a physical key, access remains valid until the physical Cancel/Block/ELO/New key is presented to relevant locks.

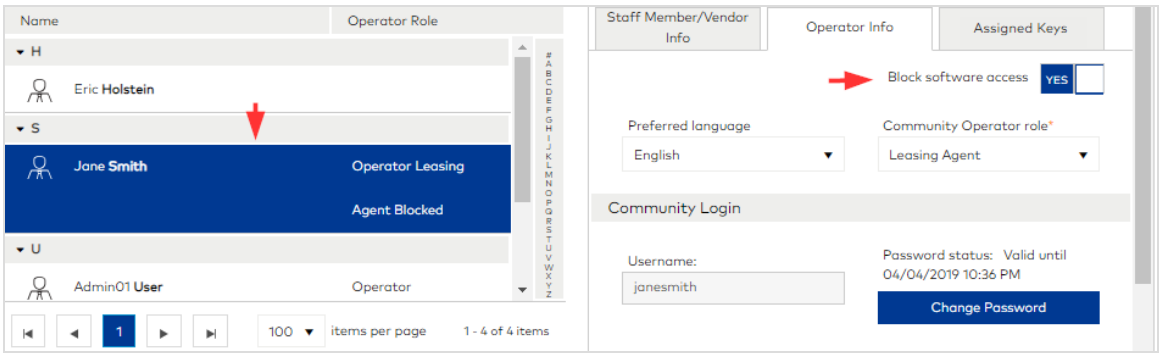
Block/Unblock Operator Access

Blocking an Operator prevents the Operator from logging in to Community. Operators may be blocked automatically due to security controls such as exceeding the failed login threshold or failing to renew an expired password. If an Operator is

automatically blocked, you must unblock access manually.

To manually block or unblock Operator access:

1. Go to **Staff/Vendor Management**.
2. Select an Operator profile.
3. Click the **Operator Info** tab.



4. For **Block software access**:
   - To block access, slide the switch to **YES**.
   - To unblock access, slide the switch to **NO**.
5. Click **(Save)**.
6. Click **YES** to confirm the action.

Demote operator

To permanently remove operator access from a staff member/vendor:

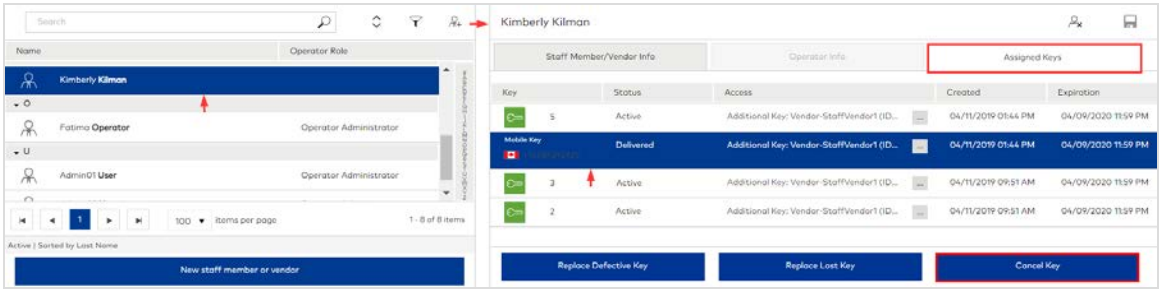
1. Go to **Staff/Vendor Management**.
2. Select the operator profile.
3. On the **Staff Member/Vendor Info** tab, change the **Is a Community Operator?** switch to **NO**.
4. Click **(Save)**. The **Operator Info** tab and access to Community is disabled.

Make Cancel Keys

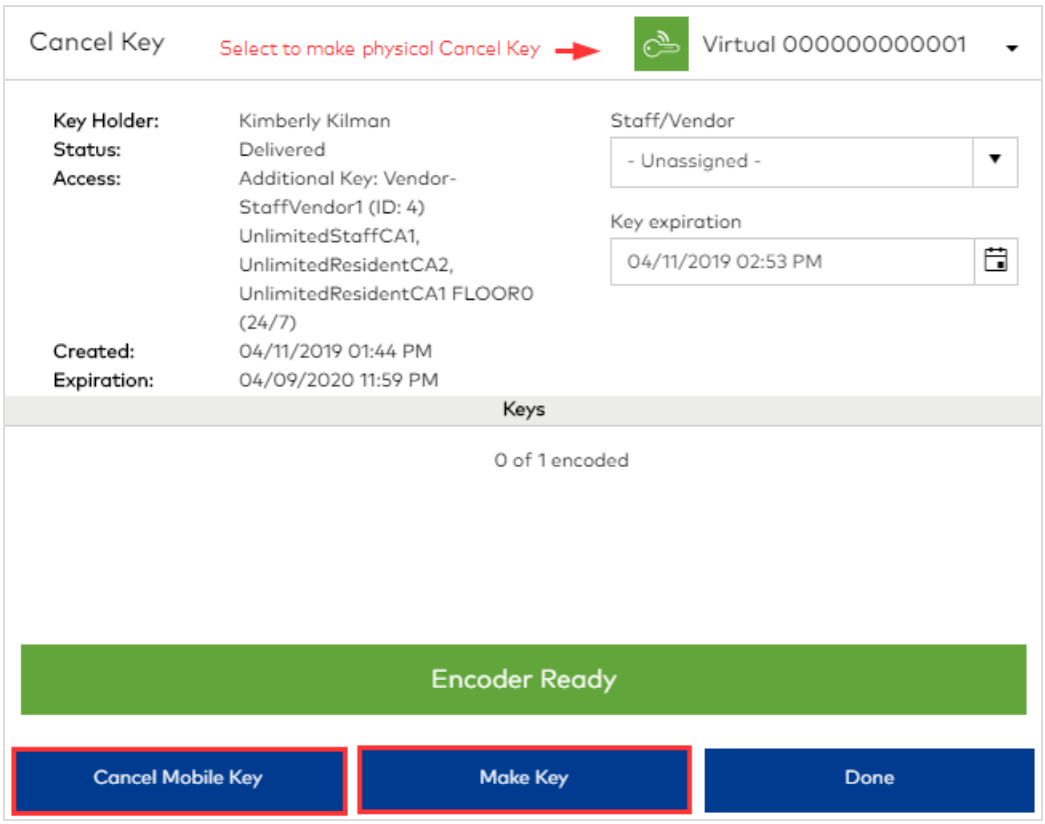
Cancel Keys permanently invalidate a single and specific key instance and must be presented to all access points for which the original key authorizes entry. Cancel Keys can be made to cancel staff/vendor keys in the **Staff/Vendor Management** module (see below) and in the **System Keys** module.

When making a Cancel Key to invalidate staff/vendor access, you must select the same credential class/credential that is encoded on the key that you want to cancel.

1. Go to **Staff/Vendor Management**.
2. Select a staff member or vendor.
3. Click the **Assigned Keys** tab.
4. Select the key that you want to cancel.



5. Click **Cancel Key**.



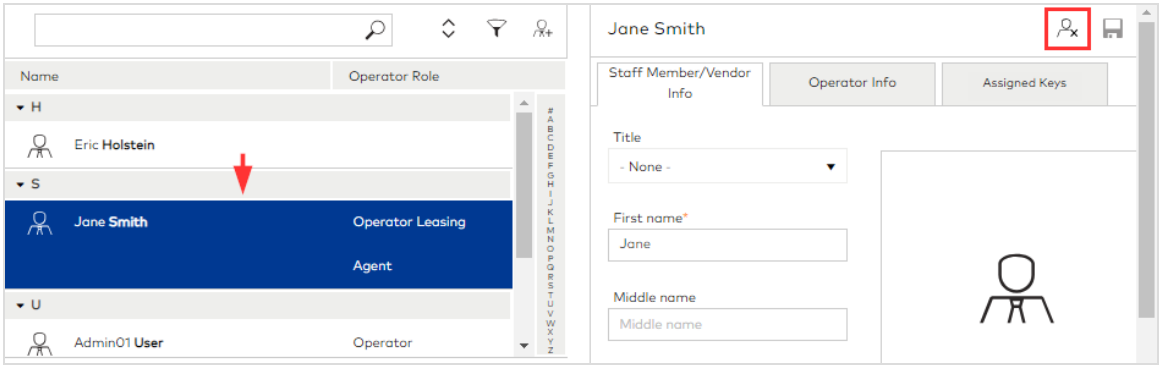
6. (*optional/physical keys only*) Select the staff/vendor to whom you want to assign the key.
7. (*optional/physical keys only*) Specify a date after which the Cancel Key is invalid.
8. Perform one of the following:
   - If you are canceling a physical key, select an encoder that is online, click **Make Key**, then present a key to the encoder.
   - If you are canceling a mobile key, click **Make Key** to make a physical Cancel Key and/or click **Cancel Mobile Key** to cancel the mobile key remotely. Physical Cancel Keys must be presented to access points to invalidate a mobile key.
9. When prompted that the key was made successfully, click **Done**. You can verify mobile keys are canceled on the **Assigned Keys** tab in the staff member/vendor profile.

Deactivate Staff/Vendors

Deactivating staff/vendors cancels all access for the staff member/vendor, and if Visitor Management is enabled, all active delegated PINs are permanently canceled. Additionally, staff who have been promoted to Operator are prevented from

logging in to Community. Staff may be automatically deactivated due to security controls such as failing to renew an expired password. If a staff member is automatically deactivated, you must (re)activate the staff member manually.

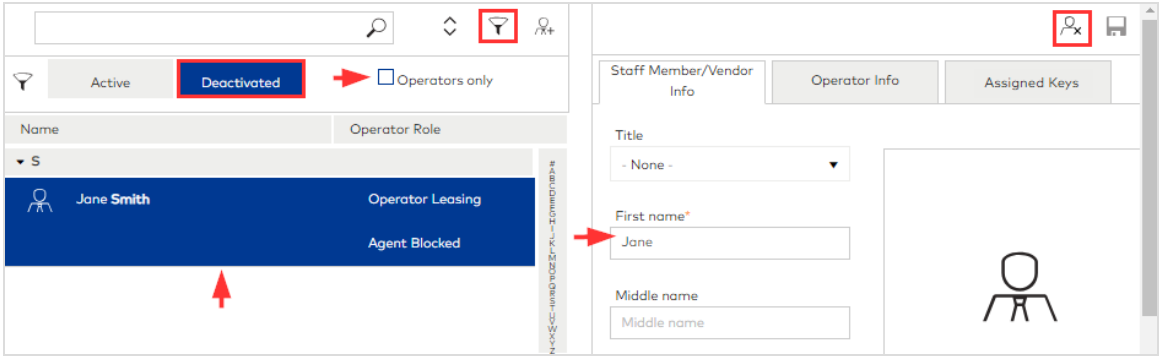
1. Go to **Staff/Vendor Management**.



2. Select a profile.
3. Click **(Deactivate user)** .
4. Click **YES** to confirm.

Activate Staff/Vendor

1. Go to **Staff/Vendor Management**.



2. Click **(Filter)** .
3. Select the **Deactivated** tab and optionally filter for Operators only.
4. Select a profile.
5. Click **(Activate user)** .
6. Click **YES** to confirm.

If you are activating an Operator, you may need to also Unblock the Operator to allow Community login.

Make New Keys

Making a New Key automatically invalidates access to the selected credential excluding common areas on all previously active keys. For example, NewKey1 for units 100 and 101 expires at 13:00 tomorrow. If you make NewKey2 for unit 100, NewKey1 becomes invalid for unit 100 as soon as you present NewKey2 to the lock installed at unit 100. NewKey1 remains valid only for unit 101.

New keys do not invalidate access to common areas on existing keys. Common area access is valid until key expiration. If the credential includes access to common areas, make Cancel keys to invalidate access (instead of New keys).

Make Block/Unblock Keys

Block Keys invalidate all instances of a specific credential. While you can use the Block Key to permanently invalidate access, the Block Key is paired with the Unblock Key to suspend then restore access. For example, make a Block Key for *credentialA* to suspend access to all access points included in credentialA; then, make an Unblock Key for *credentialA* to restore access for all active keys.

When making a Block Key to invalidate staff/vendor access, you must select the same credential class/credential that is encoded on the key that you want to block.

After blocking access, the Unblock Key does not unblock access to common areas when access is based on a common area access profile.

For instructions, see Block/Unblock Keys.

Make ELO Keys

ELO (Electronic Lockout) Keys temporarily invalidate all non-emergency keys by double locking the door from the outside (activating the privacy switch or deadbolt). When an electronic lockout is active, only a key with the Emergency credential can open the lock. When the electronic lockout is removed, normal key access resumes.

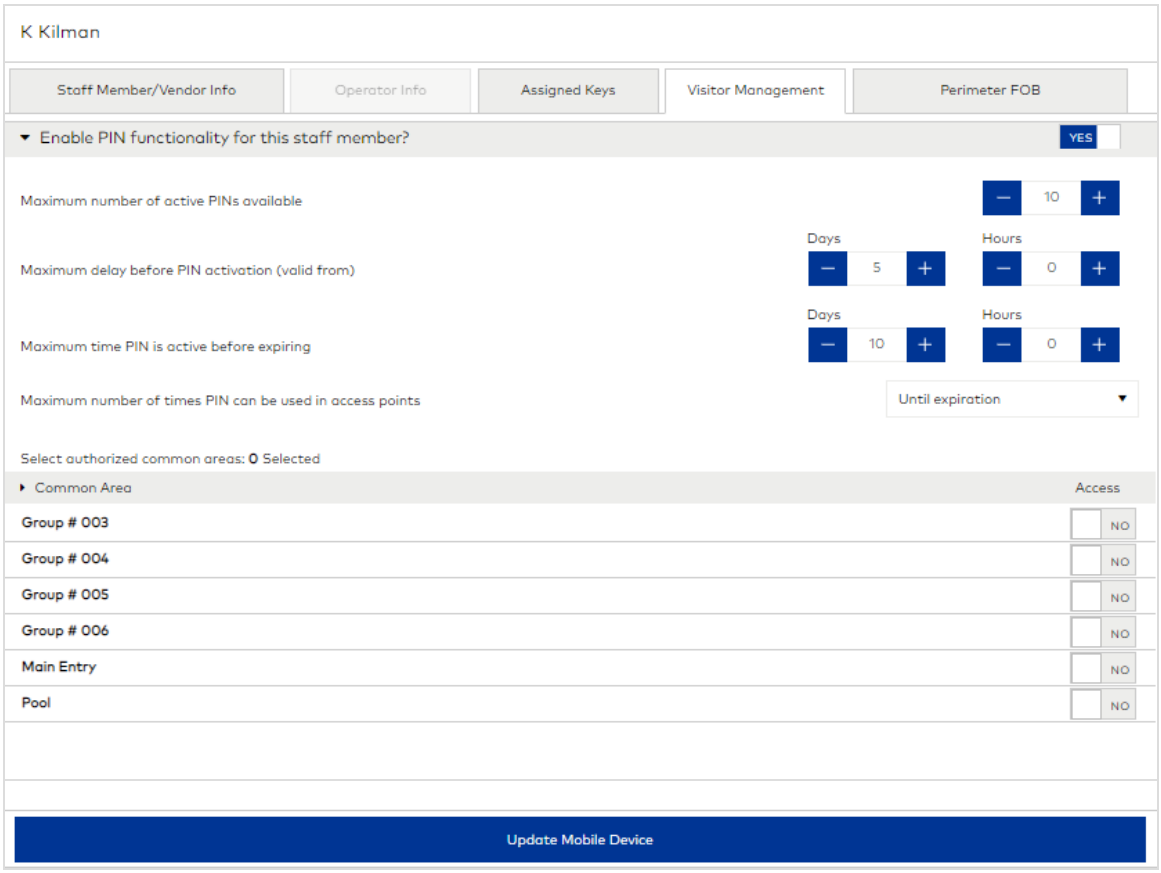
For instructions, see Electronic Lockout Keys.

Configure Visitor Management for staff/vendors

This tab displays when the licensed feature visitor management is enabled.

To configure PIN functionality for a staff member or vendor:

1. Go to **Staff/Vendor Management**.
2. Select a staff member/vendor profile.
3. Click the **Visitor Management** tab.



4. Configure PIN delegation options:
   - **Enable PIN functionality for this staff member**—When the feature is enabled, the PIN section displays, PIN settings can be customized, and PIN settings can be updated on mobile devices.
   - **Maximum number of active PINs available**—Specify the maximum number of PINs that can be active. Valid values: 1-50.
   - **Maximum delay before mobile key activation (valid from)**—Specify the maximum number of days/hours that the staff member can create a PIN before access enabled by the PIN starts. Range: 0-30 days/0-23 hours.
   - **Maximum time PIN is active before expiring**—Specify the maximum number of days/hours that a PIN can be active. Range: 0-30 days/0-23 hours.
   - **Maximum number of times PIN can be used in access points**—Specify the maximum number of times a PIN can be used in access points. Valid values: Until expiration, 1-5.
   - **Authorized common areas**—Select the common areas where access is enabled by the PIN. At least one common area must be selected.
5. Click **Save**.
6. To update settings on the staff member/vendor's mobile device, click **Update mobile device**.

Programming/Auditing

This section includes the following subjects:

Reprogram locks 219
Audit locks 221
Audit online access points 222

To learn more, see "Learning about Programming & Auditing" in **Site Configuration**.

Reprogram locks

Locks must be reprogrammed any time configuration data affecting the access point is modified in Community. For a list of when access points (locks) must be reprogrammed, see "Access Point Programming Required."

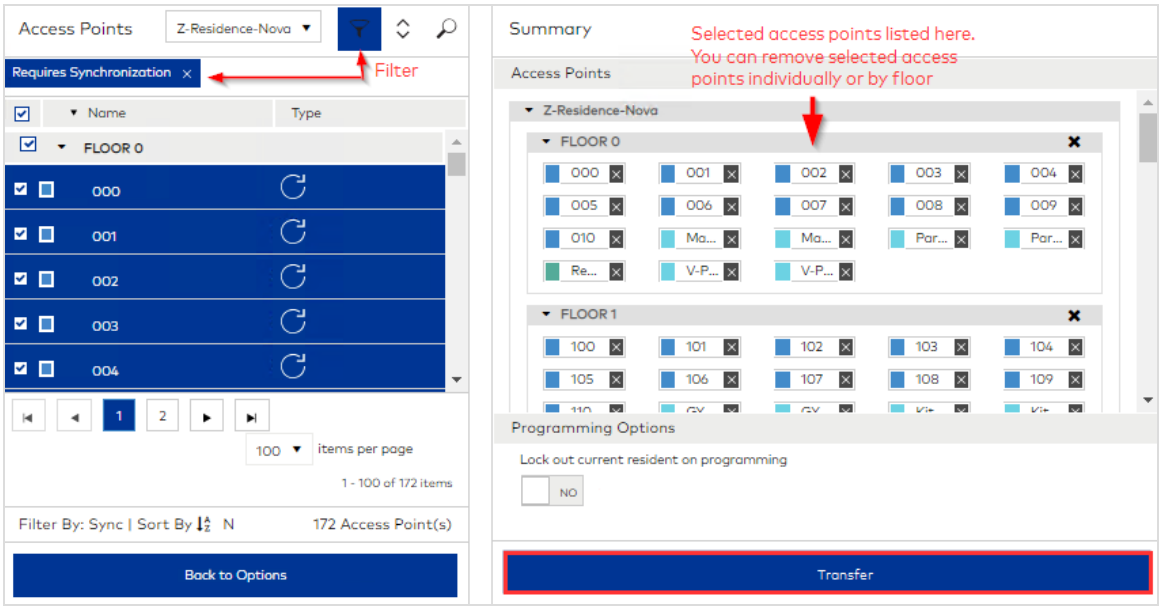
Some programming steps are performed on the M-Unit (Maintenance Unit). For official instructions, refer to the documentation distributed with your device. If M-Unit authentication is enabled in **System Settings > Security > M-Unit** credentials must be configured for at least one Operator in **Staff/Vendor Management**.

A Microsoft issue prevents the Edge browser from detecting/connecting to the Maintenance Unit. Consequently, access points cannot be programmed or audited without intervention. Open the Command prompt and issue the following command:

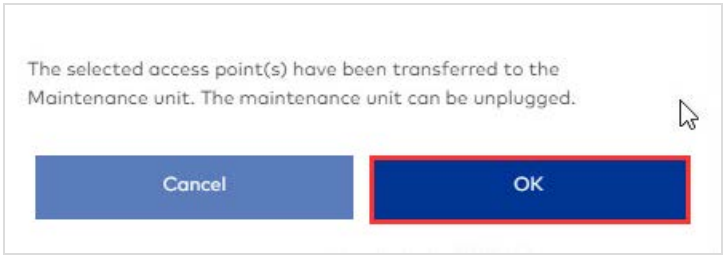
```
C:\windows\system32\CheckNetIsolation.exe LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
```

To reprogram locks:

1. Go to **Programming & Auditing > Programming**.



2. Select the access points that you want to synchronize with Community configuration data. You can select access points from different buildings and filter the list to show only access points that require synchronization. The selected access points display in the **Summary** section organized by building and floor.
3. For **Lock out current resident on programming**, select whether to invalidate all active keys issued to residents after programming the lock. If you select **Yes**, New (Resident) Keys must be made and issued after the locks are programmed.
4. Connect the M-Unit to the workstation.
5. In Community , click **Transfer**. Messages on the workstation and M-Unit display that the transfer is in progress. Wait until the message on the workstation indicates transfer is complete and that you can unplug the M-Unit.



6. Click **OK**.
7. Disconnect the M-Unit from the workstation. The remaining steps are on the M-Unit.
8. If enhanced security mode is enabled, specify the M-Unit security password. The password displays at **System Settings > Security > Enhanced Security Mode**. (In some cases, the M-Unit displays a message prior to the password prompt indicating that the unit is not personalized; simply select OK.)
9. If M-Unit authentication is enabled, specify the M-Unit login credentials.
10. On the M-Unit menu, select **LOCKS**.
11. Use the UP / DOWN arrow keys to highlight **1- Program**, then press **ENTER**. The access point names display in groups of five.
12. Select the access point name for the lock, then press **ENTER**. Use the **PREV**, **NEXT** and **SEARCH** options to navigate and refine the list of names.
13. Select the type of probe that you are using to connect the M-Unit to the lock.
14. When prompted, insert the probe into the lock. Programming starts immediately. If the lock has already been programmed, the M-Unit issues a message requesting confirmation to overwrite the existing programming.
15. When prompted that programming is complete, click **OK**.

Testing locks with valid keys after programming is a best practice.

Audit locks

This procedure documents how to audit locks using the M-Unit procedure. If fewer than five locks are being audited for troubleshooting purposes, using an Audit Key is an alternative to the M-Unit procedure. Refer to "Special Function Keys" in **System Keys**.

Some steps are performed on the M-Unit (Maintenance Unit). For official instructions, refer to the documentation distributed with your device. If M-Unit authentication is enabled in **System Settings > Security > M-Unit** credentials must be configured in **Staff/Vendor Managemen**t for at least one Operator.

A Microsoft issue prevents the Edge browser from detecting/connecting to the Maintenance Unit. Consequently, access points cannot be programmed or audited without intervention. Open the Command prompt and issue the following command:

```
C:\windows\system32\CheckNetIsolation.exe LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
```

To audit locks:

1. Connect the M-Unit to the lock that you want to audit.
2. From the M-Unit menu, select **LOCKS**.
3. Use the UP / DOWN arrow keys to highlight **Select 3-Interrogate**, then press **ENTER**. The M-Unit issues a message indicating the maximum number of interrogation records.
4. Press **ENTER** to proceed with the audit.
5. Select the type of probe that you are using to connect the M-Unit to the lock.
6. When prompted, insert the probe into the lock. The audit begins immediately. If an interrogation file for the lock already exists, the M-Unit issues a message requesting confirmation to overwrite the existing file. The M-Unit issues a message prompting for additional audits.
7. When all audits are complete, select **NO**.
8. Connect the M-Unit to the Community workstation.
9. In Community, go to **Programming & Auditing**.
10. Click **Auditing**. All access point interrogation files stored on the M-Unit are listed.
11. Select the interrogation files that you want to transfer.
12. Select whether to delete the lock audit from the M-Unit after transfer. Interrogation files on the M-Unit can be stored indefinitely or permanently deleted after the file is transferred to Community.
13. Click **Transfer**.
14. When prompted that the transfer is complete, click **OK**. All interrogation files are stored on the Community server and are accessible from the **Access Point Audit Report**.

Audit online access points

This option displays when the licensed feature online communication is enabled.

When online communication is enabled in **System Settings**, online access points can be audited directly in Community. All access points that are online are listed with the following information:

- **Access Point**—The name of the access point.
- **Category**—The type of access point: Unit, Suite, Restricted Area, Common Area.
- **Status**—The connectivity status of the access point, Online/Offline.
- **Date**—The date of the most recent audit.

To audit an online access point:

1. Go to **Programming & Auditing > Online Access Points**.
2. Select an access point.
3. Click **Audit Access Points**.

When the audit is complete, the file is accessible from the **Summary** section.

System Keys

This section includes the following subjects:

Learning about System Keys 224
Block and unblock keys 227
Cancel keys 231
Diagnostic keys 233
Electronic lockout keys 235
Failsafe keys 237
Inhibit keys 238
Latch and unlatch keys 240
Primary and secondary program keys 242
Resequence keys 245
Special function keys 247

Learning about System Keys

The **System Keys** module is used to encode keys for immediate intervention and to perform advanced operational programming.

System keys and supported access point types

All access point types are supported for all system keys with the following exceptions:

- Diagnostic keys are not compatible with NFC lock models: RT+, Saffire, MT6, and Confidant NFC.
- Failsafe keys do not support staff/vendor common areas and restricted areas.
- Inhibit keys do not support staff/vendor common areas and restricted areas.
- Unblock keys do not support common areas.

Block and unblock keys

Make a Block Key to invalidate all instances of a specific credential. For example, make a Block Key to invalidate all active keys for Unit 100. When making a Block Key, you must select the credential class and credential encoded on the key that you want to block. If the intent is to temporarily block access, you can use an Unblock Key to unblock a key that was previously blocked by a Block Key.

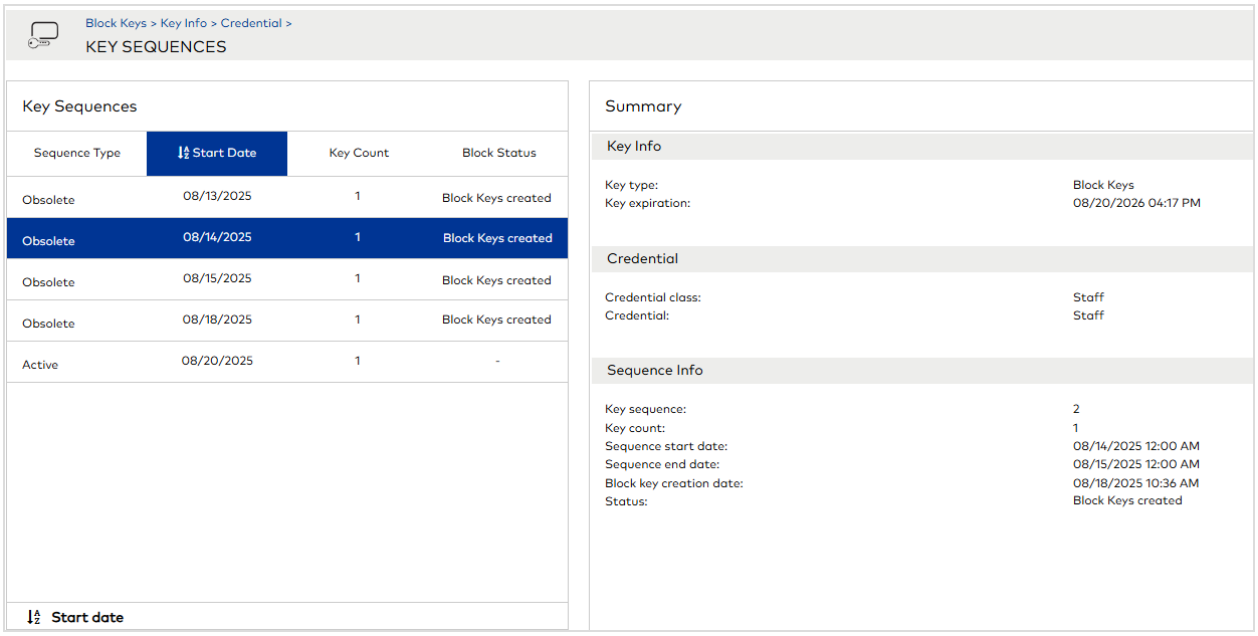
When the licensed feature online communication is enabled, remote operation is supported.

Remember that the block key must be presented at access points before access is blocked.

Blocking obsolete key sequences

Block keys can now be used to block entire sequences of obsolete keys. The option is available for keys encoded with a credential based on the Staff, Staff (variable access), Vendor, or Limited Use credential class.

Keys may be obsolete when a New key with the same credential was made and/or access was removed prior to expiration. Obsolete keys continue to allow access to common areas and elevator controllers until key expiration. dormakaba recommends to block obsolete keys.



Upon selecting a credential, the key sequences are displayed. A key sequence represents each time a new (not additional) key was created. Every time a new key (new key sequence) is created, the prior sequence becomes obsolete. Blocking a key sequence blocks all the keys in that sequence, as well as all the keys in key sequences with a prior start date.

The Key Sequences page includes the following details:

Key Sequences:

- **Sequence Type**—The current state of the key sequence: Obsolete or Active.
- **Start Date**—The date that the key sequence was created. This is also the date that the key sequence was encoded on the first (new) key.
- **Key Count**—The number of keys made using the key sequence. "1" indicates only the first or new key was made. All values greater than 1 indicate the number of additional keys (total - 1).
- **Block Status**—The current status of the keys encoded with the selected key sequence. The status indicates the method of blocking:
  - **Block keys created**—A physical block key was made for the selected or a more recent key sequence.
  - **Blocked**—When online communication is enabled and the Block Keys Remotely command is issued for the selected or a more recent key sequence.

  The value reflects the most recent action to block the selected or a more recent key sequence. For example, were the Active key sequence in the figure above blocked remotely, the status for all rows changes to "Blocked".

Summary:

- **Key Info**
  - **Key type**—Block Keys.
  - **Key expiration**—The date and time selected for the block key to expire.
- **Credential**
  - **Credential class**—The name of the credential class.
  - **Credential**—The name of the credential.
- **Sequence Info**—Only displays when credential class is Staff, Staff (variable access), or Vendor, Limited Use.
  - **Key sequence**—The order in which the key sequence was created. For example, Key sequence 2 was created prior to Key sequence 3.
  - **Key count**—The total number of keys made using the key sequence. "1" indicates only the first, or new, key was made. All values greater than 1 indicate the sum of the first new key plus all additional keys made.
  - **Sequence start date**—The date that the key sequence was created. This is also the date that the key sequence was encoded on the first (new) key.
  - **Sequence end date**—The date that keys made using the key sequence became obsolete. This is also the start date of the next key sequence.
  - **Block key creation date**—The date that the most recent block action was taken on the key sequence.
  - **Status**—The current status of the keys encoded with this key sequence. The status indicates the method of blocking: Block keys created or Blocked. The value reflects the most recent action to block this or a more recent key sequence. For example, were the Active key sequence in the figure above be blocked remotely, the status for all rows changes to "Blocked."

Cancel keys

Make a Cancel Key to permanently invalidate a specific key instance. When making a Cancel Key in System Keys, you must select the credential class and credential encoded on the key that you want to cancel. A Cancel Key must be presented to all access points for which the original key has credentials.



When the licensed feature online communication is enabled, remote operation is supported.

Diagnostic keys

Diagnostic Keys query locks to extract and report the status of various lock functions and are most often used for troubleshooting. Results of the query are communicated by an LED flash sequence.

ELO keys

ELO (Electronic Lockout) Keys temporarily invalidate all non-emergency keys by double locking the door from the outside (activating the privacy switch or deadbolt). When an electronic lockout is active, only a key with the Emergency credential can open the lock. When the electronic lockout is removed, normal key access resumes. ELO Keys are toggle keys. The behavior of the key alternates (applies lockout/removes lockout) each time it is presented to the lock.

When the licensed feature online communication is enabled, remote operation is supported.

Failsafe keys

Failsafe Keys are backups of individual unit keys that are made in advance and maintained in complete sets to be issued in the event a system or power failure. All Failsafe Keys are encoded with default floor and common area access.

The recommendation is to create and always retain three sets of two keys for each unit and suite unit. You can make as many key sets as you require; however, when a key from one set is presented to the lock, all keys from a previously used set are invalidated.

Default settings for Failsafe Keys are defined in **System Settings > Failsafe Keys**.

It is critical that Failsafe Keys are current and stored in an efficient filing system at a secure location.

Inhibit keys

Inhibit Keys are used to permanently cancel current resident access. Most often, Inhibit Keys are used by staff after a resident vacates before their key expires. Inhibit Keys invalidate all resident keys encoded with access to the unit even if the dead bolt or privacy switch is active.

When the licensed feature online communication is enabled, remote operation is supported.

Latch, unlatch and toggle latch/unlatch keys

Latch Keys disable passage mode. Access is restricted to only those people with keys encoded with the applicable credential. Unlatch Keys enable passage mode. Passage mode is a lock state during which the access controls programmed in the lock are suspended allowing unrestricted access. Toggle Latch/Unlatch Keys enable and disable passage mode, alternately.

Primary and secondary program keys

Primary Program Keys (PPKs) put the lock into programming mode and are used in conjunction with Program Information (PI) Keys and Program Status (PS) Keys to program locks and authorize special functions (see Create a Special Function Key). They are also used to reprogram the current Secondary Program Key (SPK) or remaster a different SPK. Secondary Program Keys (SPKs) reprogram or resynchronize the current Primary Program Key (PPK) into access points and remaster a different PPK into a lock. Essentially, an SPK is a backup to the PPK but does not put locks into programming mode.

Resequence keys

Resequence Keys resynchronize a specific key credential in access points. The Resequence Key is used to update the sequence number stored in the lock's memory when the number of new keys made but not used in the lock exceeds the programmed sequence range for that key.

When the licensed feature online communication is enabled, remote operation is supported.

Special function keys

Special function keys are paired with primary program keys to perform system-level operations on a lock.

Block and unblock keys

Create a Block Key to block all active key instances of a specific credential. For staff keys based on the Staff, Staff (variable access), Vendor, and Limited Use credential class, you can also block all obsolete key instances. Before making a Block Key, you must know the credential class and credential (or access point) that you want to block.

Given keys with an *Obsolete* status continue to provide access to common areas and elevator controllers until key expiration, dormakaba strongly recommends using Block Keys on locks where keys are obsolete. When making the block key, select the key sequence. Remember to present physical block keys to the necessary common areas and elevator controllers.

Before blocking a common area, note that the Unblock Key does not restore access to common areas for the key when access to the common area is based on a common area profile.

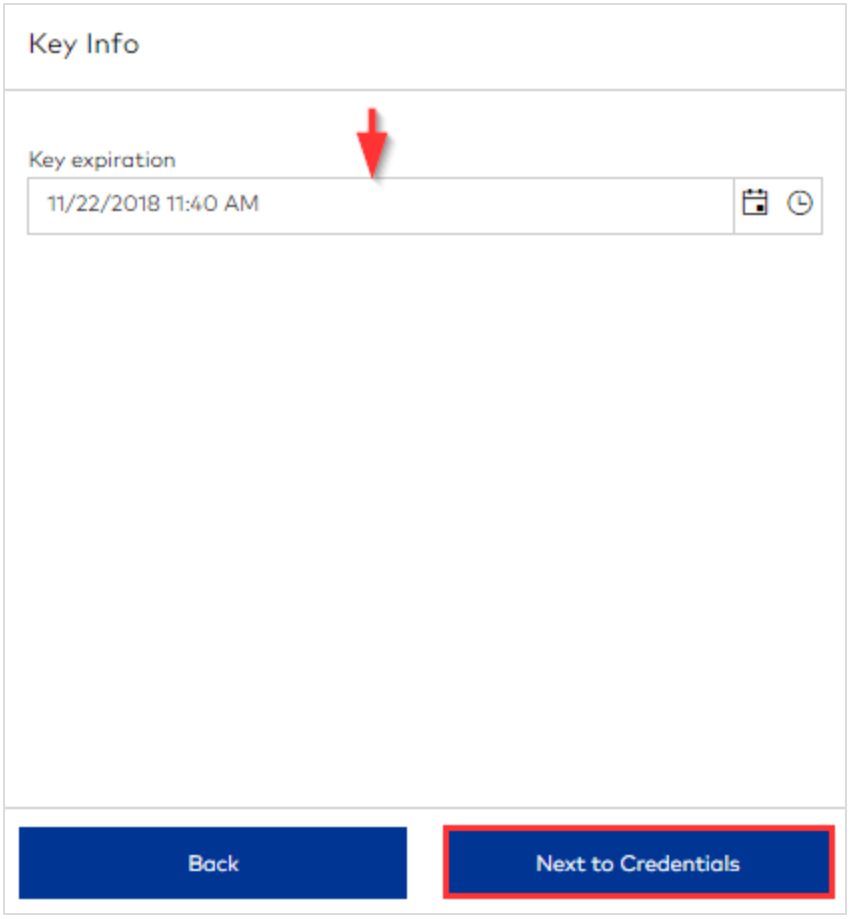
Block Keys can be used to invalidate:

- resident keys
- staff/vendor keys
- ELO keys
- Latch/Unlatch/Toggle Latch/Unlatch keys
- Inhibit keys

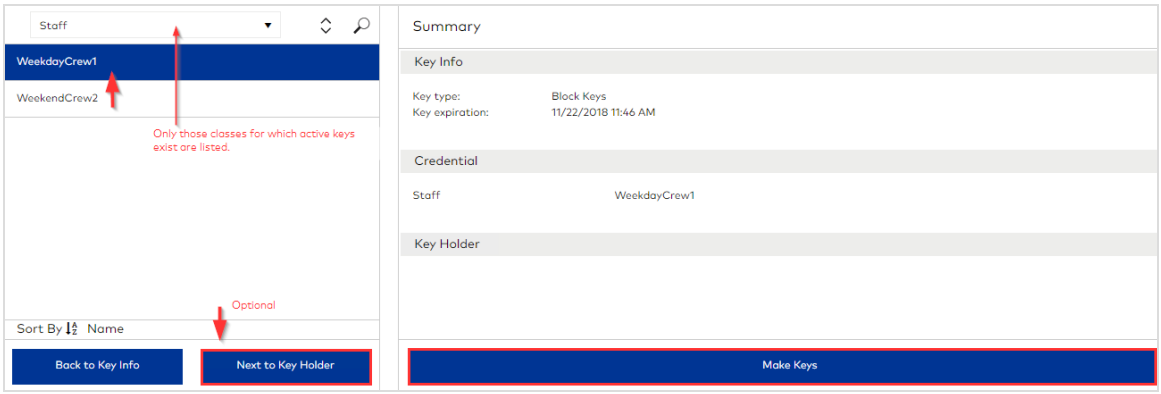
If the intent is to temporarily block access, you can use an Unblock Key to unblock a key that was previously blocked by a Block Key. Obsolete keys cannot be unblocked.

Make block keys

1. Go to **System Keys > Block Keys**.



2. Specify expiration details.
3. Click **Next to Credentials**.



4. Select the credential class under which the credential that you want to block is defined.
5. Select the credential that you want to block.
6. Take any of the available actions or proceed to the next step:
   - Click **Next to Key Sequence**. Select the key sequence that you want to block. You can block Obsolete or Active key sequences. Blocking a key sequence also blocks all key sequences with a previous start date. For more details about blocking obsolete keys, refer to Learning about System Keys.
   - Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)** +, specify first and last names, then click **Save**.

7. Click **Make Keys.**

> if online communication is enabled, you can also click **Block Keys Remotely**. This option is supported when the selected credential is based on the Emergency, Staff, or Limited Use credential class. (Keys cannot be blocked remotely for Staff [variable access] and Vendor credential classes or custom classes based on Staff (variable access) and Vendor.)

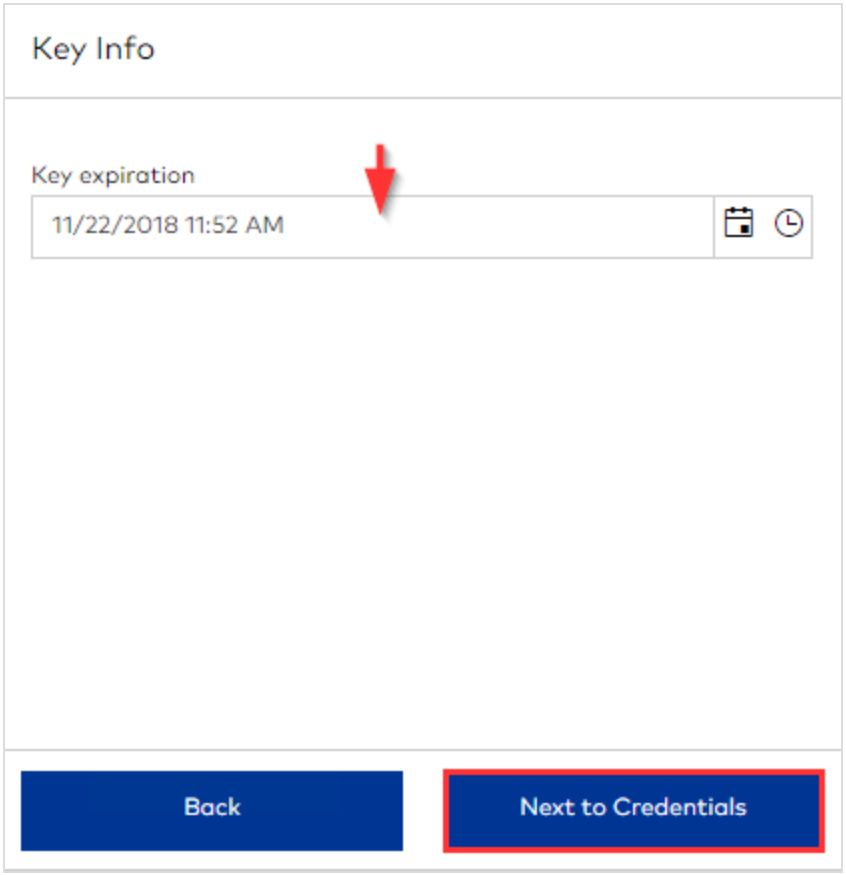
8. Select an encoder that is online.
9. Present a key to the encoder (as prompted).
10. Click **Start**.
11. When notified that the key request is complete, click **Done**.

Remember that physical keys must be presented to locks.

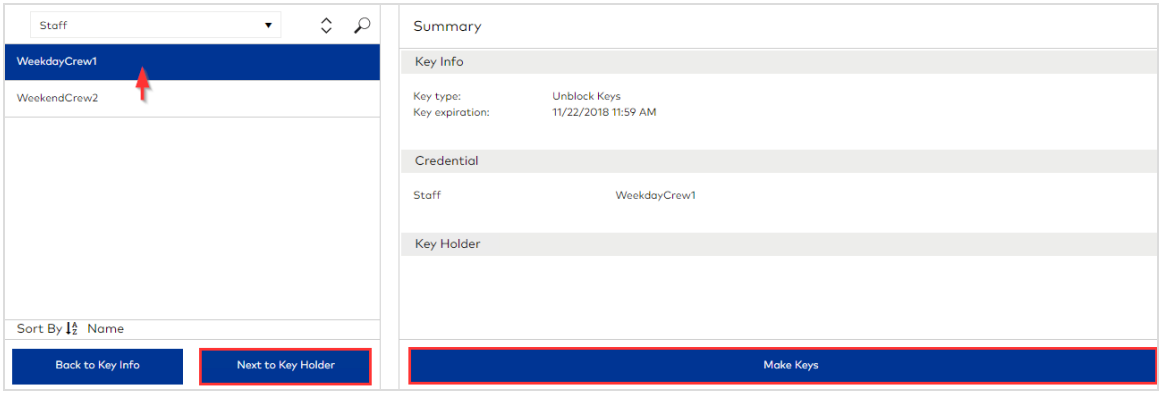
Make unblock keys

Unblock Keys unblock all instances of a specific credential in access points which have been previously blocked using the Block Key.

1. Go to **System Keys > Unblock Keys**.



2. Specify expiration details.
3. Click **Next to Credentials**.



4. Select the credential class for the credential or access point encoded on the key that you want to unblock. Only those classes for which active keys exist are listed.
5. Select the credential (or access point) encoded on the key that you want to unblock.
6. (*optional*) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)＋,** specify first and last names, then click **Save**.
7. Click **Make Keys.**

If online communication is enabled, you have the option to click **Unblock Keys Remotely**.

8. Select an encoder that is online.
9. Present a key to the encoder (as prompted).
10. Click **Start**.
11. When notified that the key request is complete, click **Done**.

Remember that physical keys must be presented to locks.

Cancel keys

Make a Cancel key to permanently invalidate a specific key instance. Before making a Cancel Key, you must know the credential class and credential that you want to cancel. A cancel key must be presented to all access points for which the original key has credentials.

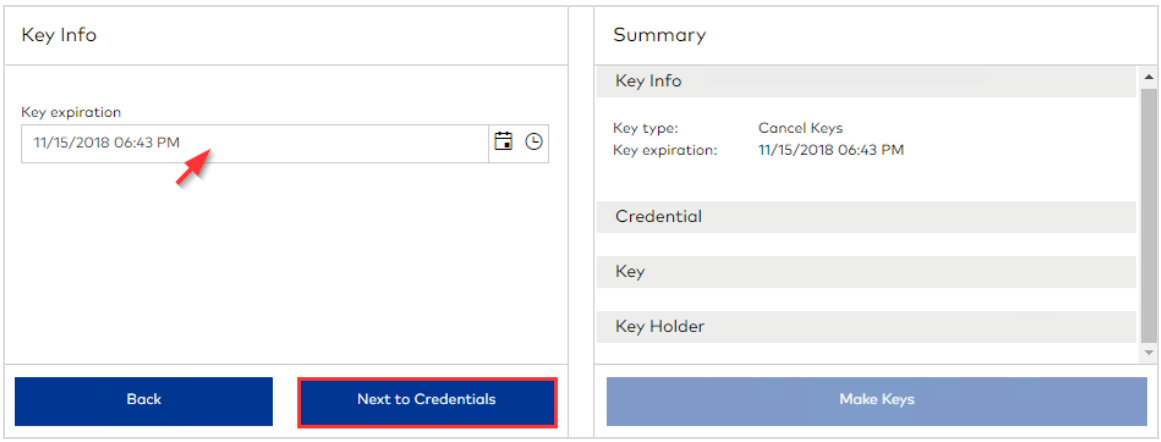
When using a Cancel key to invalidate a staff/vendor key, the status of the staff key must be Active to invalidate access to common areas. If the key status is Obsolete, access to the common areas remains valid until key expiration.

Cancel keys can be used to invalidate:

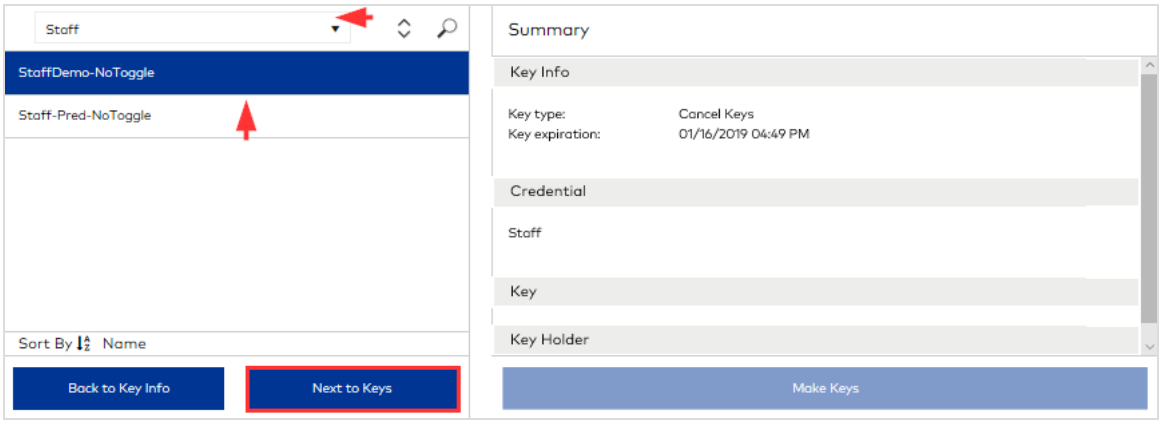
- staff/vendor keys
- ELO keys
- Latch/Unlatch/Toggle Latch/Unlatch keys
- Inhibit keys

To make cancel keys:

1. Go to **System Keys > Cancel Keys**.

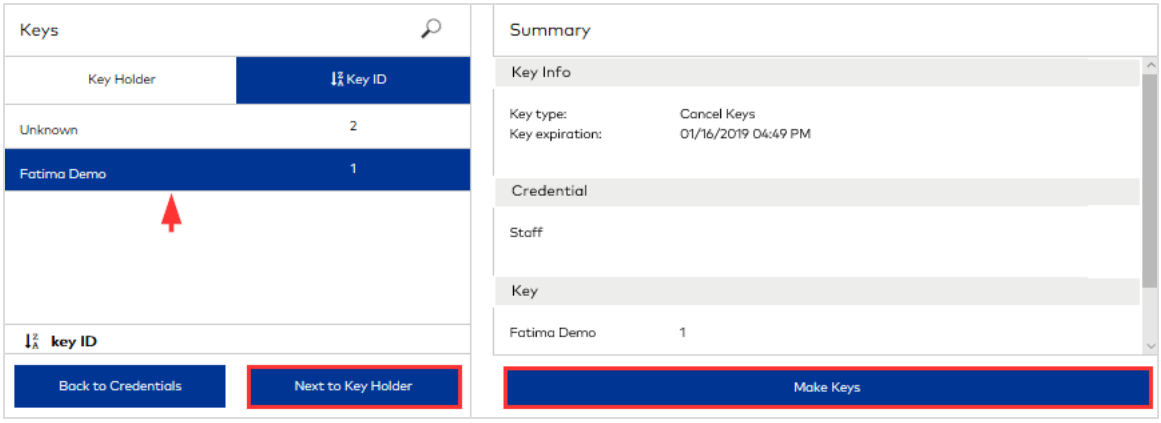


2. Specify expiration details.
3. Click **Next to Credentials**.



4. Select the credential class under which the credential you want to cancel is defined. Only those classes for which active keys exist are listed.

5. Select the credential or access point encoded on the key that you want to cancel.
6. Click **Next to Keys**.



7. Select the key that you want to cancel. You can view the list of keys by Key Holder or by Key ID.
8. (*optional*) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)** +, specify first and last names, then click **Save**.
9. Click **Make Keys**.

If online communication is enabled, you can also click **Cancel Keys Remotely**. This option is supported when the selected credential is based on the Emergency, Staff, or Limited Use credential class. (Keys cannot be cancel remotely for Staff [variable access] and Vendor credential classes or custom classes based on Staff (variable access) and Vendor.)

10. Select an encoder that is online.
11. Present a key to the encoder (as prompted).
12. Click **Start**.
13. When notified that the key request is complete, click **Done**.

Diagnostic keys

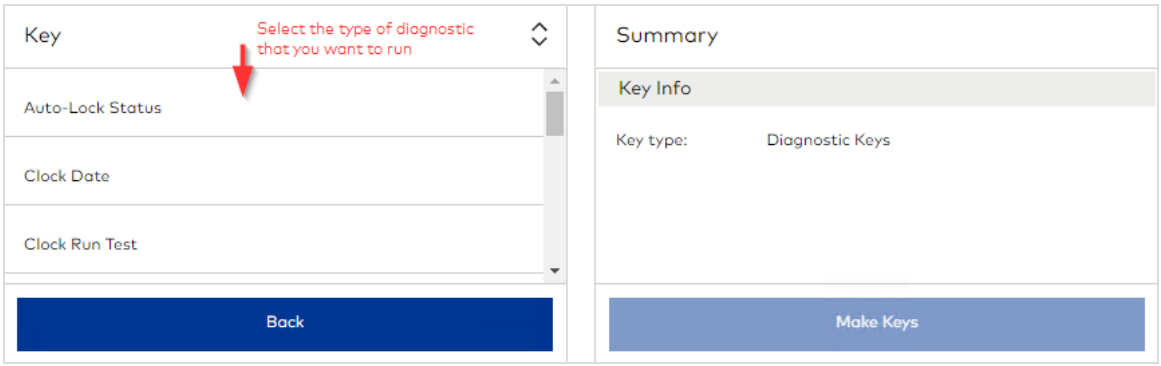
Diagnostic keys query locks to extract and report the status of various lock functions and are most often used for troubleshooting. Results of the query are communicated by an LED flash sequence.

A simpler alternative to making diagnostic keys is to use the M-Unit (Maintenance Unit) to run a diagnostic on locks. The results of the query are in readable text format instead of an LED flash sequence.

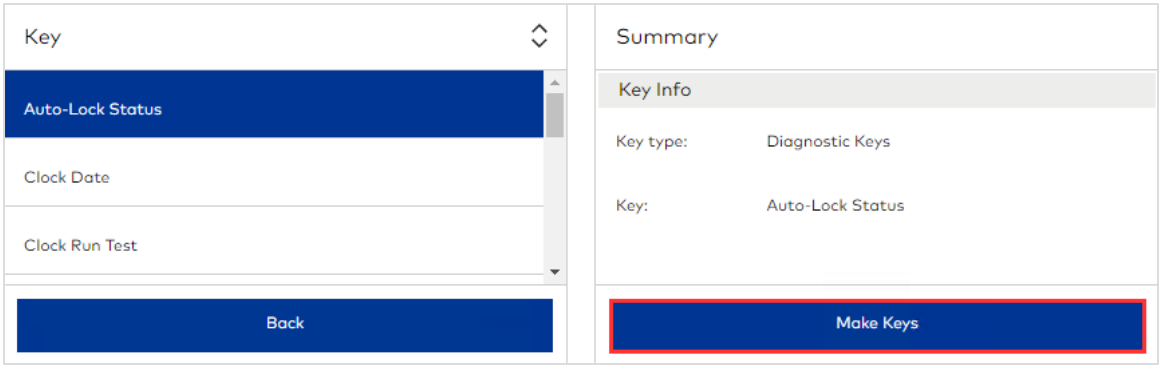
Diagnostic keys are not compatible with newer NFC lock models: RT+, Sapphire, MT6 and Confidant NFC.

Make diagnostic keys

1. Go to **System Keys > Diagnostic Keys**.



2. Select the type of diagnostic that you want to run.
   - **Auto-Lock Status**—Select this option to query the lock for Auto-Latch Schedules.
   - **Clock Date**—Select this option to query the lock for the date.
   - **Clock Run Test**—Select this option to test the lock clock function.
   - **Clock Time**—Select this option to query the lock for the time.
   - **Deadbolt Switch Status**—Select this option to query whether the lock deadbolt is projected or retracted.
   - **EPROM Version**—Select this option to retrieve the version of the micro-controller in the lock.
   - **Knob Switch Status**—Select this option to determine whether the lock is engaged or open.
   - **Last 2 LPI Records**—Select this option to query the lock for the two most recent errors.
   - **LED Lights Test**—Select this option to test the lock LED.
   - **Low Battery Status**—Select this option to learn the remaining battery charge for the lock.
   - **Motor Switch + Lock State**—Select this option to retrieve the status of the lock motor and lock state.
   - **Verify Lock Version**—Select this option to retrieve the lock firmware version.



3. Click **Make Keys**.
4. Select an encoder that is online.
5. Present a key to the encoder (as prompted).
6. Click **Start**.
7. When notified that the key request is complete, click **Done**.

Diagnostic results

For details about interpreting a flash sequence, see "Troubleshooting Locks."

LED flash sequence

Each color of light has a different base value:

- Green=100
- Yellow=10
- Red=1

To interpret a response, multiply the number of times that each color flashes by the base value. For example, if the sequence of lights is two yellow flashes followed by three red flashes, the response value is 23.

Yellow(10)X2 + Red(1)X3=23

Diagnostic elements

Each Diagnostic Key provides several pieces of information. Each piece of information is known as an element, and you must be familiar with the elements that will be displayed in order to understand the response.

For example, the Display Clock Time Key will give you information on the following elements:

- Date/Time/DST Problem (if any) (0-4)
- DST Status (0-1)
- Hours (In Military Time) (0-23)
- Minutes (0-59)

When you use the card, the response begins and ends with a delimiter that consists of all three lights flashing simultaneously. This delimiter is also used to separate the responses to each element.

Electronic lockout keys

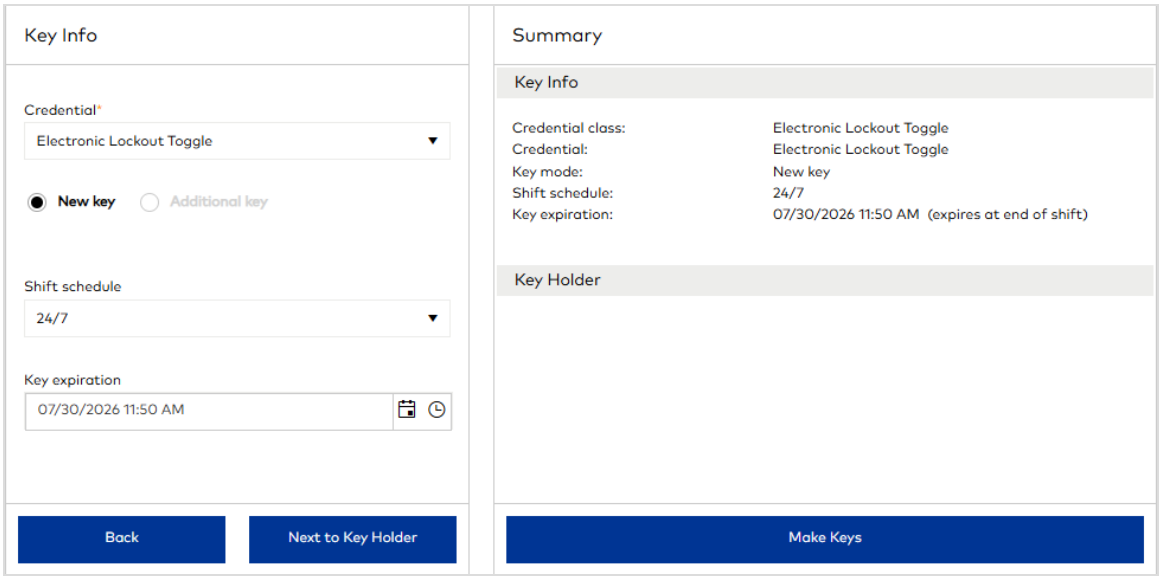
ELO (Electronic lockout) keys temporarily invalidate all non-emergency keys by double locking the door from the outside (activating the privacy switch or deadbolt). When an electronic lockout is active, only a key with the Emergency credential can open the lock. When the electronic lockout is removed, normal key access resumes.

ELO keys are toggle keys. The behavior of the key alternates (applies lockout/removes lockout) each time it is presented to the lock.

To make ELO keys:

The credential selected by default (**ELO**) or a custom credential based on the ELO credential class is required.

1. Go to **System Keys > Electronic Lockout Toggle Keys**. The default credential **ELO** is required.



2. Select whether to make a New or Additional key. if no active key exists, a New key is required. If an active key exists, **Additional key** is the selected default. Making an Additional key (copy) has no effect on existing active keys. Making a New key when an active key exists, invalidates the previously active key.
3. Select a shift schedule. To enable 24/7 access, select **24/7**. To review shift schedule details, see **Access Management > Shift Schedules**. The selected shift schedule determines the days and hours that the key is valid.
4. Specify expiration details.
5. (*optional*) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)**+, specify first and last names, then click **Save**.
6. Click **Make Keys**.

If online communication is enabled, you have the option to click **ELO Keys Remotely**.

7. Select an encoder that is online.
8. Present a key to the encoder (as prompted).
9. Click **Start**.
10. When notified that the key request is complete, click **Done**.

Electronic lockout key LED flash sequence

For details about interpreting a flash sequence, see "Troubleshooting Locks."

- The following LED flash sequence indicates the electronic lockout is activated:
  - Red (1) Yellow (12)
- The following LED flash sequence indicates the electronic lockout is removed:
  - Green (1) Yellow (12)

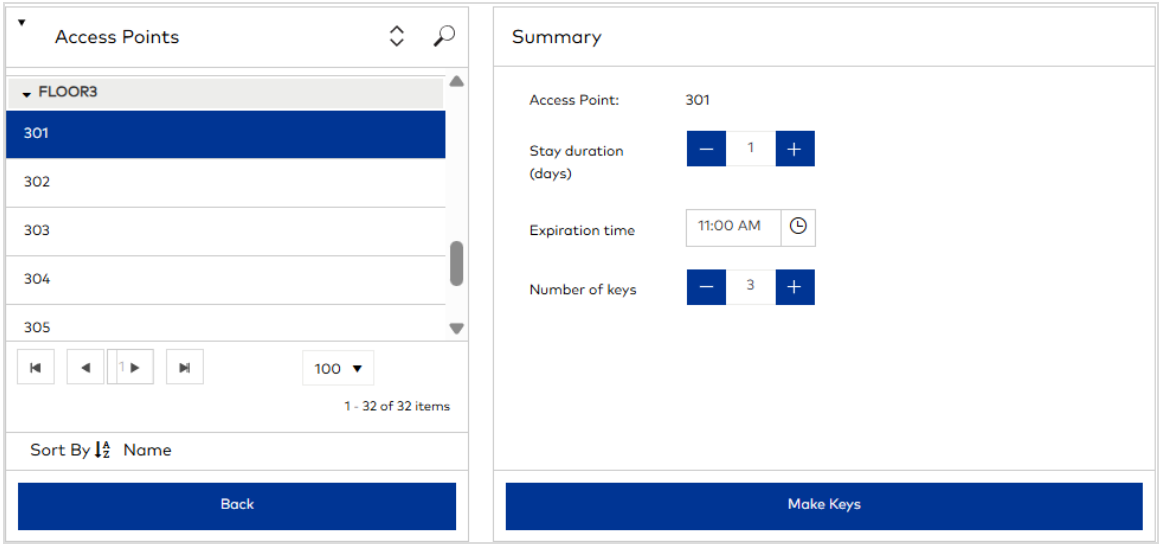
Failsafe keys

Failsafe Keys are backups of individual unit keys that are made in advance and maintained in complete sets to be issued to residents in the event of a system or power failure. The recommendation is to create and maintain two sets of three keys for each unit and suite door. After one set of Failsafe keys is issued and used, make another set of Failsafe keys to replace the used set. Locks only accept keys from the two most recent Failsafe key sets.

Using a Failsafe Key invalidates previous resident key access to units, suite common doors and suite unit doors.

To create a Failsafe key set:

1. Go to **System Keys > Failsafe Keys**.



2. Select an access point. You can select an access point from any building on site.
3. Specify the number of nights access to the Unit is enabled.
4. Specify the time after which the key expires (on the final day the key is active).
5. Specify the number of keys to make.
6. Click **Make Keys**.
7. Select an encoder that is online.
8. Specify the number of keys to make.
9. Present a key to the encoder (as prompted).
10. Click **Start**.
11. When prompted that keys were made successfully, click **Done**.

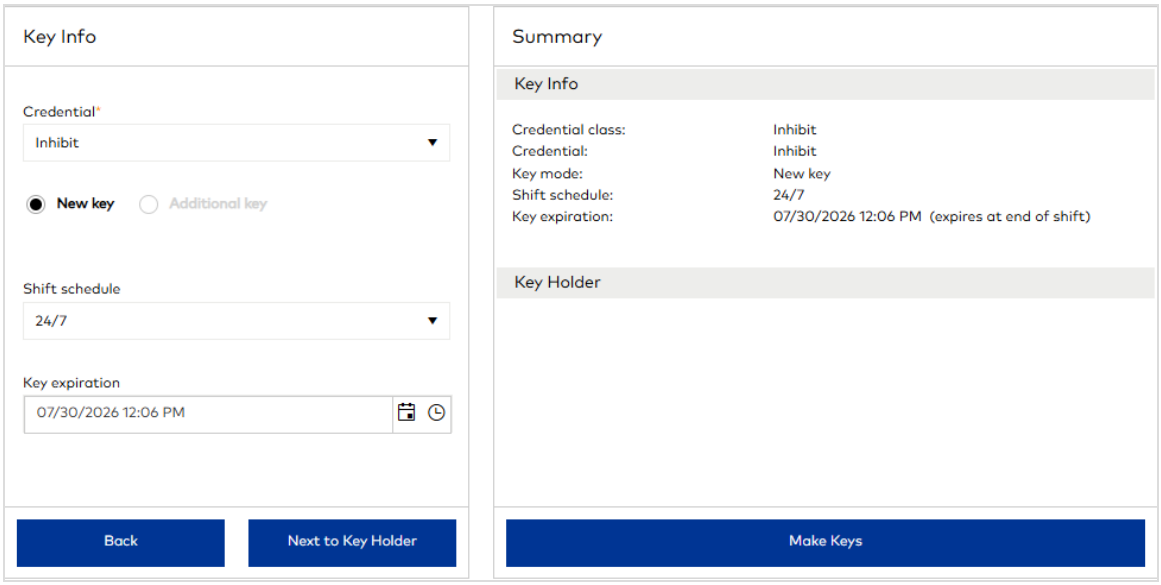
Inhibit keys

Inhibit Keys are used to permanently cancel current resident access. Most often, Inhibit Keys are used by staff after a resident vacates before their key expires. Inhibit Keys invalidate all resident keys encoded with access to the unit even if the dead bolt or privacy switch is active.

Inhibit Keys do not invalidate access to common areas and elevator readers.

Make inhibit keys

1. Go to **System Keys > Inhibit Keys**. The default credential **Inhibit** is required.



2. Select whether to make a New or Additional key. if no active key exists, a New key is required. if an active key exists, **Additional key** is the selected default. Making an Additional key (copy) has no effect on existing active keys. Making a New key when an active key exists, invalidates the previously active key.
3. Select a shift schedule during which the key is valid. To enable 24/7 access, select **24/7**. To review shift schedule details, see **Access Management > Shift Schedules**. The selected shift schedule determines the days and hours that the key is valid.
4. Specify expiration details.
5. (*optional*) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)**+, specify first and last names, then click **Save**.
6. Click **Make Keys**.
7. If online communication is enabled, you have the option to click **Inhibit Keys Remotely**. This option is supported when the selected credential is based on the Emergency, Staff, or Limited Use credential class. (Keys cannot be inhibited remotely for Staff [variable access] and Vendor credential classes or custom classes based on Staff (variable access) and Vendor.)
8. Select an encoder that is online.
9. Present a key to the encoder (as prompted).
10. Click **Start**.
11. When notified that the key request is complete, click **Done**.

Inhibit key LED flash sequence

For details about interpreting a flash sequence, see "Troubleshooting Locks."

- The following LED flash sequence displays when an Inhibit Key is first presented:
  - Red (1) Yellow (12)
- The following LED flash sequence displays when the lock has already been inhibited:
  - Yellow (12)

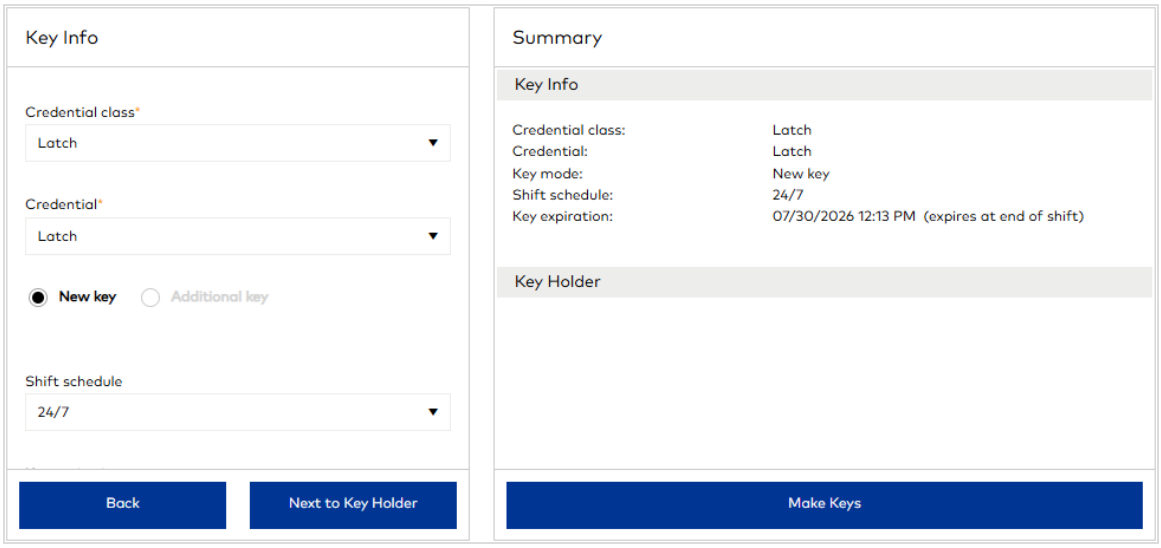
Latch and unlatch keys

The following system keys latch and unlatch locks:

- **Latch keys**—Disable passage mode. Access is restricted to only those people with keys encoded with the applicable credential.
- **Unlatch keys**—Enable passage mode. Passage mode is a lock state during which the access controls programmed in the lock are suspended allowing unrestricted access.
- **Toggle latch/unlatch keys**—Enable and disable passage mode. Passage mode is a lock state during which the access controls programmed in the lock are suspended allowing unrestricted access. A toggle key alternatives behavior each time the key is presented to the lock.

To make Latch, Unlatch, and Latch/Unlatch Keys:

1. Go to **System Keys**.
2. Select the type of key to make:
   - **Latch Keys**
   - **Unlatch Keys**
   - **Toggle Latch/Unlatch**



3. The credential class selected by default (**Latch**, **Unlatch**, **Toggle Latch/Unlatch**) or a custom credential class based on the respective type is required.
4. Select the credential that you want to latch, unlatch, or latch/unlatch.
5. Select whether to make a New or Additional key. if no active key exists, a New key is required. If an active key exists, **Additional key** is the selected default. Making an Additional key (copy) has no effect on existing active keys. Making a New key when an active key exists, invalidates the previously active key.
6. Select a shift schedule during which the key is valid. To enable 24/7 access, select **24/7**. To review shift schedule details, see **Access Management > Shift Schedules**. The selected shift schedule determines the days and hours that the key is valid.
7. Specify expiration details.
8. (*optional*) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)**+, specify first and last names, then click **Save**.
9. Click **Make Keys**.
10. Select an encoder that is online.
11. Specify the number of keys to make.
12. Present a key to the encoder.

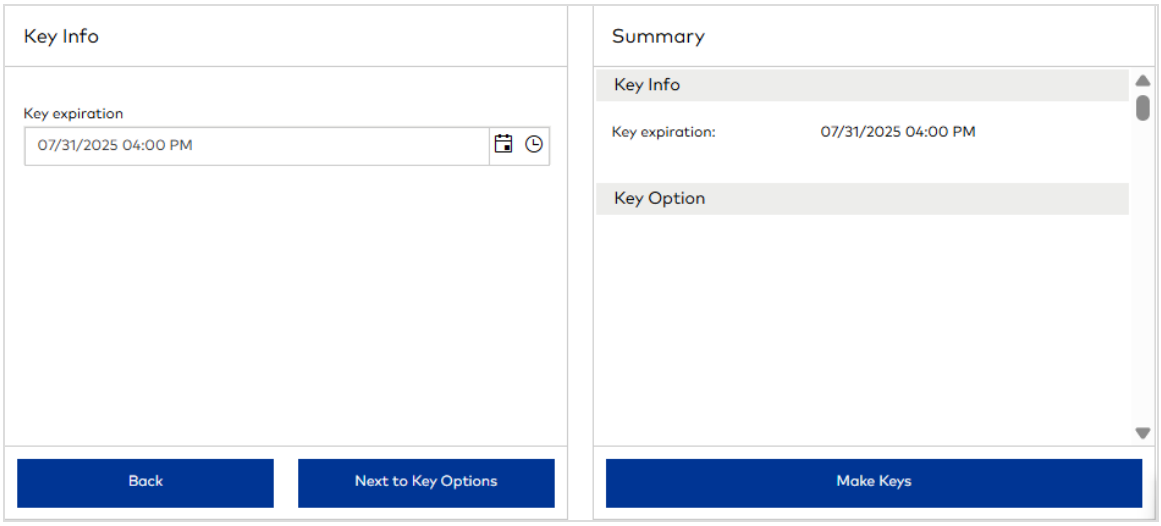
13. Click **Start**.
14. When notified that the key request is complete, click **Done**.

Primary and secondary program keys

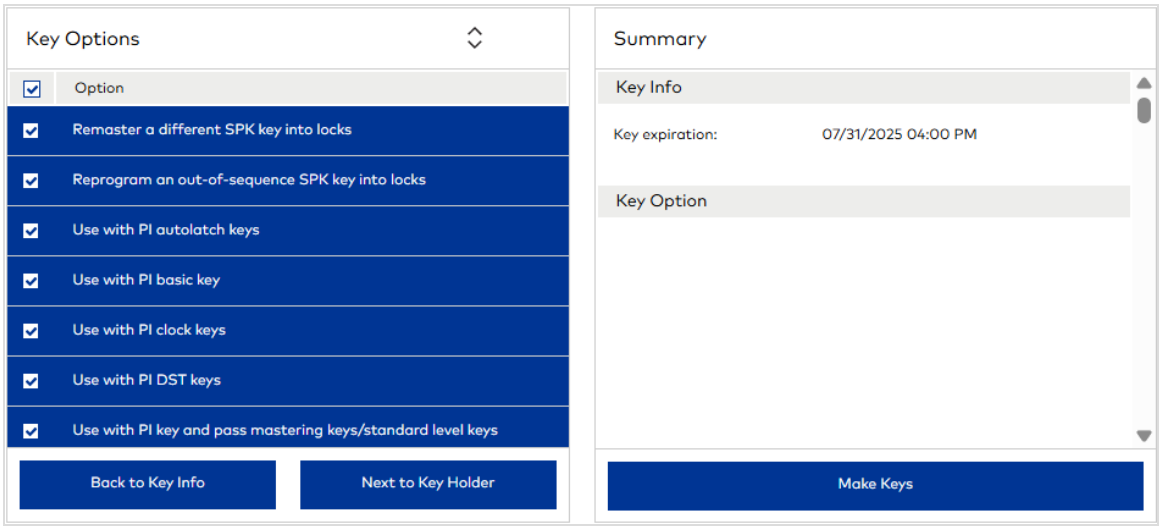
Primary program keys put the lock into programming mode and are used in conjunction with PI (Program Information) keys and PS (Program Status) keys to program locks and authorize special functions (see "Create a Special Function Key"). They are also used to reprogram the current secondary program key or remaster a different secondary program key.

Make primary program key

1. Go to **System Keys > Primary Program Keys**.



2. Specify expiration details.
3. Click **Next to Key Options**.



4. Select options to encode on the key. All options are selected by default.

> All PI options remain in the software to support legacy systems. For guidance on these options, contact dormakaba Technical Support.

- **Remaster a different SPK key into locks**—This option is only selected in rare cases when the PPK has been compromised and must be remastered. Before remastering the SPK, you must use the SPK to remaster a new PPK.

Select this option to encode a PPK that authorizes a key to reprogram a Secondary Program Key.

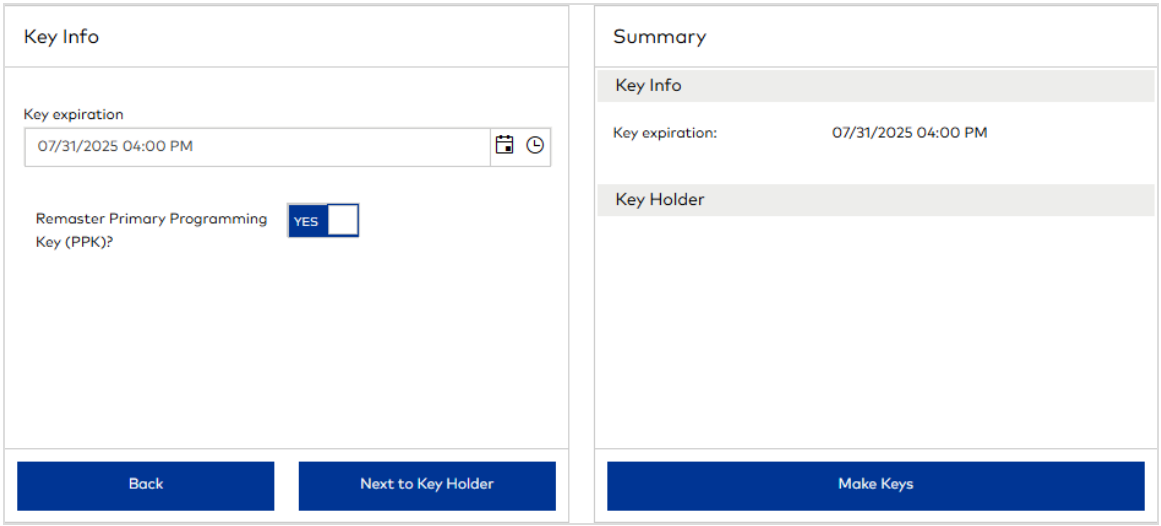
- **Reprogram an out-of-sequence SPK key into locks**—This option is only selected in rare cases. Select this option to encode a PPK that authorizes a key to reprogram a Secondary Program Key.
- **Use with PI autolatch keys**—Select this option to encode a PPK that authorizes a key to program auto-latch/unlatch schedules in the lock.
- **Use with PI basic key**
- **Use with PI clock keys**—Select this option to encode a PPK that authorizes a key to synchronize the lock clock.
- **Use with PI DST keys**—Select this option to encode a PPK that authorizes a key to update daylight savings time settings in the lock.
- **Use with PI key and pass mastering keys/standard level keys**
- **Use with PI level program keys**
- **Use with PS battery disconnect key**—Select this option to encode a PPK that authorizes a key to shut down the lock before the lock battery disconnects.

5. (*optional*) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)** +, specify first and last names, then click **Save**.
6. Click **Make Keys**.
7. Select an encoder that is online.
8. Present a key to the encoder.
9. Click **Start**.
10. When notified that the key request is complete, click **Done**.

Make secondary program key

To make a Secondary Program Key:

1. Go to **System Keys > Secondary Program Keys**.



2. Specify expiration details.
3. Select whether to remaster the PPK. Remastering a PPK is a rare occurrence and is used to reprogram the current PPK or remaster a different PPK into a lock. This remastering should only be made at the direction of dormakaba Technical Support. If you select to remaster, all keys become invalid and all locks must be reprogrammed.
4. (*optional*) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)** +, specify first and last names, then click **Save**.
5. Click **Make Keys**.
6. Select an encoder that is online.

7. Present a key to the encoder.
8. Click **Start**.
9. When notified that the key request is complete, click **Done**.

Secondary program key LED flash sequence

For details about interpreting a flash sequence, see "Troubleshooting Locks."

The following LED flash sequence displays when an SPK is first presented:

Yellow (slow flashing for 20 seconds)

Resequence keys

The Resequence Key is used to update the sequence number stored in the lock's memory when the number of new keys made but not used in the lock exceeds the programmed sequence range for that key.

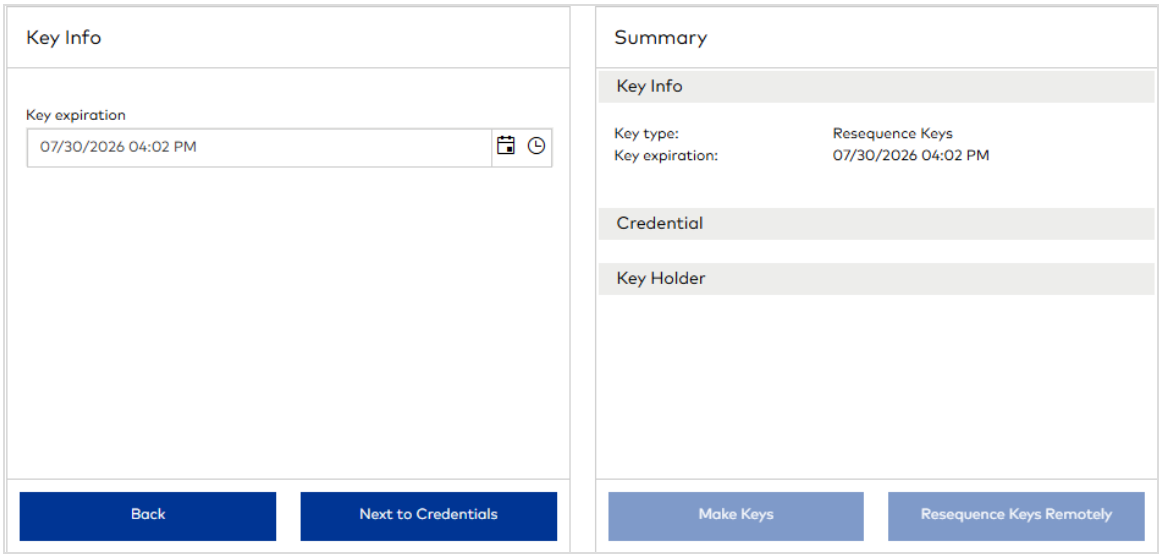
> The need to use a Resequence Key is rare. Staff can troubleshoot the lock to determine if the cause of the lock error is a corrupt sequence number.

Resequence Keys can be used to correct the sequence on:

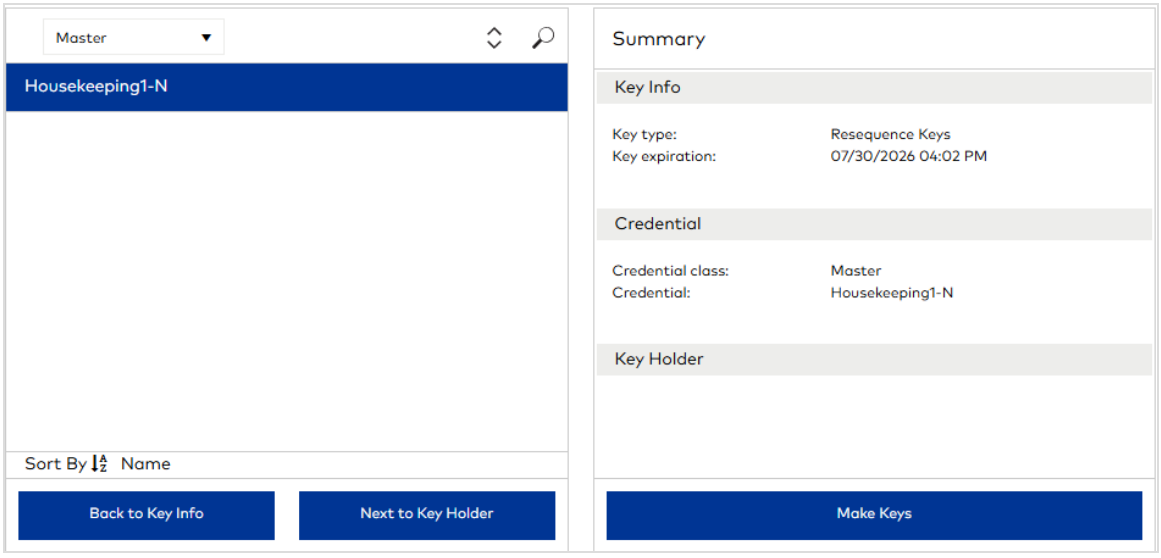
- Staff/Vendor Keys
- ELO Keys
- Latch/Unlatch/Toggle Latch/Unlatch Keys
- Inhibit Keys

Make resequence keys

1. Go to **System Keys > Resequence Keys**.



2. Specify expiration details.
3. Click **Next to Credentials**.



4. Select the credential class. Select the credential class for the credential or access point encoded on the key that you want to resequence. Only those classes for which active keys exist are listed.
5. Select the credential. Select the credential (or access point) encoded on the key that you want to resequence. You can select a credential from any building.
6. (*optional*) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add)** +, specify first and last names, then click **Save**.
7. Click **Make Keys**.

If online communication is enabled, you can also click **Resequence Keys Remotely**. This option is supported when the selected credential is based on the Emergency, Staff, or Limited Use credential class. (Keys cannot be resequenced remotely for Staff [variable access] and Vendor credential classes or custom classes based on Staff (variable access) and Vendor.)

8. Select an encoder that is online.
9. Present a key to the encoder (as prompted).
10. Click **Start**.
11. When notified that the key request is complete, click **Done**.

Resequence key LED flash sequence

For details about interpreting a flash sequence, see "Troubleshooting Locks."

- The following LED flash sequence displays when a Resequence Key is first presented:
  - Green and Yellow (6)
- The following LED flash sequence displays when a Resequence Key is presented to a lock that is not out of sequence:
  - Yellow (6)

When using a Resequence Key for resident levels, a new resident key must be made if a red flash precedes the green/yellow flashes.

Special function keys

Special function keys are paired with primary program keys to perform system-level operations on a lock.

Special function keys are supported for legacy systems. A simpler alternative to making SFKs is to use the M-Unit (Maintenance Unit) to interrogate (audit) a lock. All data that can be obtained by using an SFK is included in audit reports.

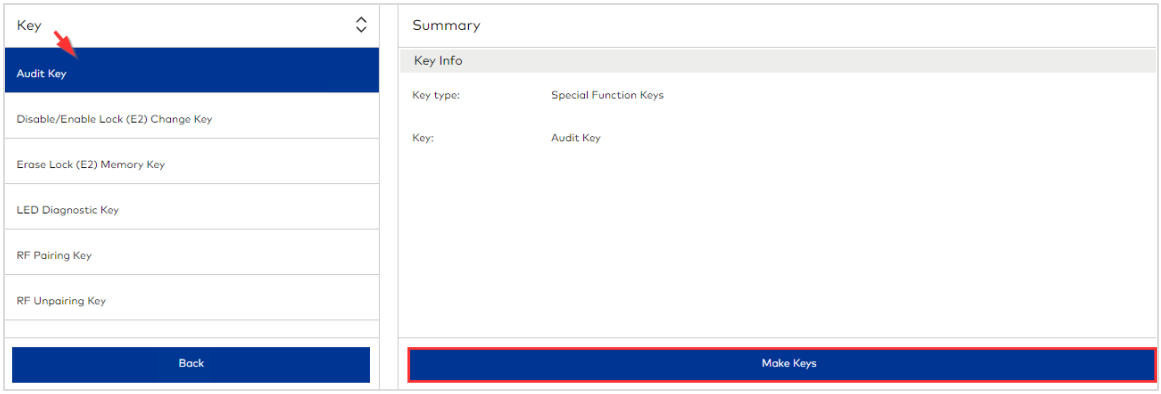
Special function key types

The following types of Special Function Keys can be made in System Keys:

- **Audit Key**—Requires 4K key. Select this option to make a key that audits a lock to obtain status and diagnostic data. A maximum of 172 records can be stored on an Audit Key. After auditing a lock with an Audit Key, present the key to the encoder and click the Read Key button in the Community toolbar. Data collected from the lock is displayed with the option to generate a report. If you generate a report from the Read Key results, the report is limited to the data collected by the Audit Key. To expand the scope of the data in the report, go to the Reports module and generate an Access Point Audit Report.
- **Disable/Enable Lock Change Key**—Select this option to make a key that disables all key and M-Unit access to the lock where the key is presented.
- **Erase Lock Memory Key**—Select this option to make a key that removes all programming stored in the lock memory.
- **LED Diagnostic Key**—Select this option to make a key that performs diagnostics on access points.
- **RF Pairing**—Select this option to make a key that connects a lock to the configured gateway. This key type only displays if online communication is enabled.
- **RF Unpairing**—Select this option to make a key that disconnects a lock from the paired gateway. This key type only displays if online communication is enabled.

Make special function keys

1. Go to **System Keys > Special Function Keys**.



2. Select the type of special function that you want to run.
3. Click **Make Keys**.
4. Select an encoder that is online.
5. Present a key to the encoder.
6. Click **Start**.
7. When notified that the key request is complete, click **Done**.

Monitor

Monitoring

This section includes the following subjects:

Learning about Monitoring 249

Monitor keys 250

Monitor digital key usage 251

Learning about Monitoring

The **Monitoring** module provides information about all keys made in Community . If you need to know the most recent time that a specific key was used and by whom, the data is readily available without generating a report.

Access to data in the **Monitoring** module is configured in **Role Management**. By default, the Administrator and Site Configurator roles have full access.



When the licensed feature mobile keys is enabled, the Digital Keys Usage tab displays to control and track the number of digital keys (mobile and wallet keys) available/consumed.

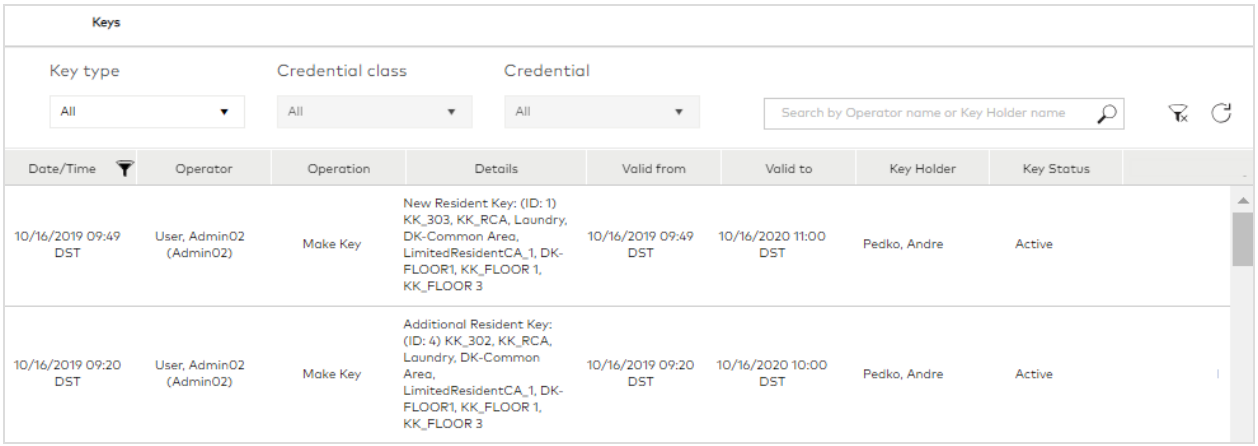


The Monitoring module includes additional features when online communication is enabled. See Monitoring (Remote Lock Management).

Monitor keys

The **Monitoring** module is where you can see the status for all resident, staff/vendor and system keys. You can filter the list based on key type, credential class and credential, and search for keys based on Operator or Key Holder name.

» Go to **Monitoring**. (If online communication is enabled, click the **Keys** tab.)



The following information is reported for each key:

- **Date/Time**—Date and time the key was encoded. You can filter the list based on date and time. A maximum of 60 transactions display.
- **Operator**—The full name of the Operator who was logged in when the key was encoded. You can search for keys that were used by a specific Operator. "API" following the name indicates the key was made using the Community API. If the key was made using the API and API authentication is disabled, only "API" is listed.
- **Operation**—The MAKE KEY command.
- **Details**—The type of key (resident/staff/vendor/system) and the access points encoded on the key (including common areas). You can search the list of keys based on details.
- **Valid from**—The date the key became valid.
- **Valid to**—The date after which the key is invalid.
- **Key Holder|Possible Key Holder**—The name of the key holder. Defaults: Resident 1 (for residents) and Unassigned (for staff/vendor or system keys). You can search for keys used by a specific key holder. In cases where a key ID is reused, the key holder may be one of multiple.
- **Key Status**—For physical keys: Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- **Aurora Status**—When Aurora is enabled, the status of the key in the Aurora system (Synchronized/Failed/Pending/Not applicable) and the date/time the status was first attained. You can filter the list of keys based on the Aurora status.

Customize the Display

- To filter data, click **(Filter)** in the column heading row, select the information that you want to display, then click **Filter**. The **(Filter Applied)** icon indicates that a filter is applied to the column.
- To clear filters for a column, click **(Filter Applied)** > **Clear**.
- To clear all filters, click **(Remove Filters)**.
- Click any column to sort the list.
- To refresh data, click **(Refresh)**.

Monitor digital key usage

When mobile keys are enabled, control and track the number of digital keys issued at the property. Digital keys include mobile and wallet keys. The following events consume a digital key:

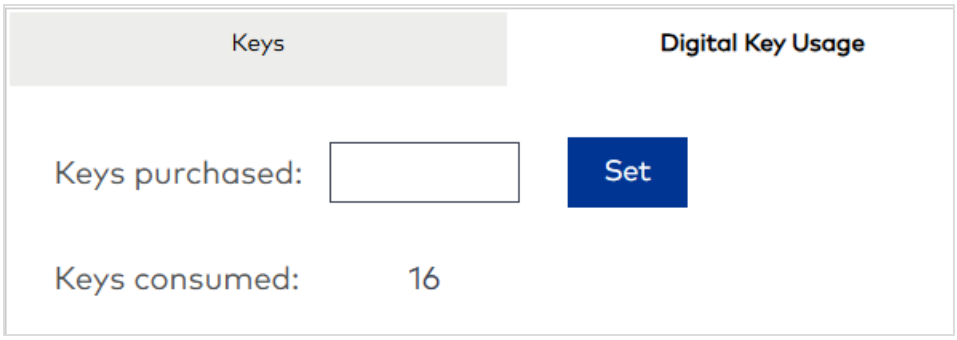
- Making a key
- Updating a key
- Canceling a key

If the number of keys purchased is not specified, then the number of consumed keys displays. If the number of keys purchased is set, then the number of keys available displays. Each time a bundle of keys is purchased (and set), a record of the purchase displays. The record lists the following information about each bundle purchase:

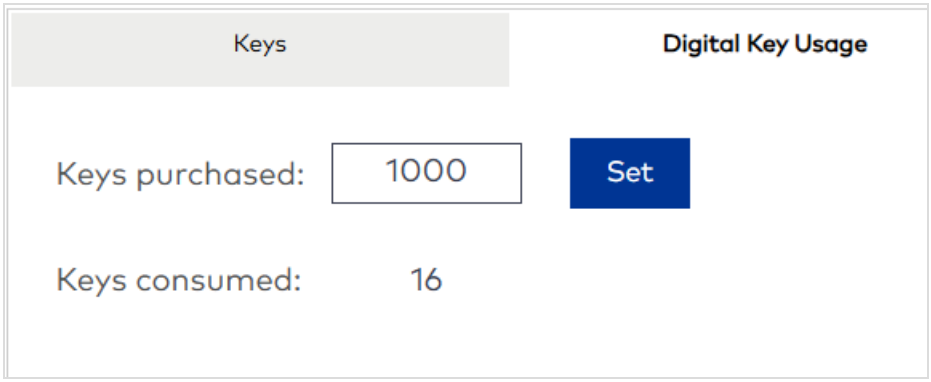
- **Date/Time**—The date and time the key bundle is added.
- **Operator**—The username / User ID of the operator who added the key bundle.
- **Operation**—For now, the only operation is Add key.
- **Total keys purchased**—The number of keys in the bundle. The number increments with each purchase.

Add key bundle

1. Go to **Monitoring**.
2. Select the tab **Digital Key Usage**.



3. Specify the number of keys purchased.



4. Click **Set**.



If another key bundle is purchased, the amount of keys increments. The following figure show the result when adding 100 keys.



Reports

Reports

This section includes the following subjects:

Access Point Audit Report 254
Credential/Access Point Assignment Report 256
Elevator Configuration Report 257
Key Expiration Report 258
Key/User Assignment Report 259
Operator Report 260
Property Configuration Report 261
Roles and Rights Report 262
Staff/Vendor Access Report 263
System Activity Report 264
Visitor Management Report 267

Access Point Audit Report

This report provides descriptive and event details about a lock. Before you can generate an access point audit report, you must first audit the lock (in **Programming & Auditing**). The audit process transfers data from the lock to Community. The resulting interrogation file can be viewed directly after transfer or from the **Reports** module. The benefit to viewing access point audits in the **Reports** module is that you can select a date range to include historical interrogation files.

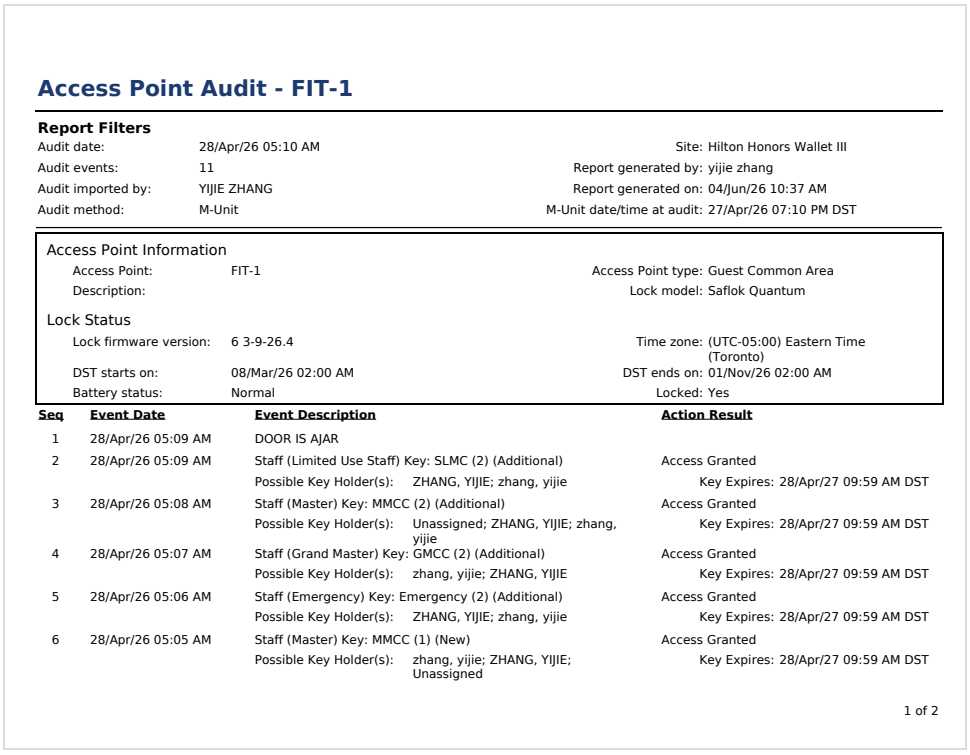
Transferring lock audit data from the M-Unit to a workstation requires the Community Client. Download and install the client from the main toolbar in the **Programming & Auditing** or **Device Management** module.

Generate report

1. Go to **Reports > Access Point Audit Report**.
2. Select the access point for which you want to transfer data to Community. Multiple files for the same access point indicate the lock has been audited multiple times. Review the date to determine the audit that you want to view.
3. Click **Next to Audit List**.
4. Select the audit for which you want to generate a report.
5. Click **Generate**.

View report details

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.



Access Point Audit - FIT-1

Report Filters

Audit date:	28/Apr/26 05:10 AM	Site:	Hilton Honors Wallet III
Audit events:	11	Report generated by:	yijie zhang
Audit imported by:	YIJIE ZHANG	Report generated on:	04/Jun/26 10:37 AM
Audit method:	M-Unit	M-Unit date/time at audit:	27/Apr/26 07:10 PM DST

Access Point Information

Access Point:	FIT-1	Access Point type:	Guest Common Area
Description:		Lock model:	Saflok Quantum

Lock Status

Lock firmware version:	6 3-9-26.4	Time zone:	(UTC-05:00) Eastern Time (Toronto)
DST starts on:	08/Mar/26 02:00 AM	DST ends on:	01/Nov/26 02:00 AM
Battery status:	Normal	Locked:	Yes

Seq	Event Date	Event Description	Action Result
1	28/Apr/26 05:09 AM	DOOR IS AJAR	
2	28/Apr/26 05:09 AM	Staff (Limited Use Staff) Key: SLMC (2) (Additional) Possible Key Holder(s): ZHANG, YIJIE; zhang, yijie	Access Granted Key Expires: 28/Apr/27 09:59 AM DST
3	28/Apr/26 05:08 AM	Staff (Master) Key: MMCC (2) (Additional) Possible Key Holder(s): Unassigned; ZHANG, YIJIE; zhang, yijie	Access Granted Key Expires: 28/Apr/27 09:59 AM DST
4	28/Apr/26 05:07 AM	Staff (Grand Master) Key: GMCC (2) (Additional) Possible Key Holder(s): zhang, yijie; ZHANG, YIJIE	Access Granted Key Expires: 28/Apr/27 09:59 AM DST
5	28/Apr/26 05:06 AM	Staff (Emergency) Key: Emergency (2) (Additional) Possible Key Holder(s): ZHANG, YIJIE; zhang, yijie	Access Granted Key Expires: 28/Apr/27 09:59 AM DST
6	28/Apr/26 05:05 AM	Staff (Master) Key: MMCC (1) (New) Possible Key Holder(s): zhang, yijie; ZHANG, YIJIE; Unassigned	Access Granted Key Expires: 28/Apr/27 09:59 AM DST

1 of 2

- Audit date
- Audit events
- Audit imported by

- Audit method
- Site
- Report generated by
- Report generated on
- M-Unit date/time at audit
- Access Point Information
  - Access Point
  - Access Point type
  - Description
  - Lock model
- Lock Status
  - Lock firmware version
  - Time zone
  - DST starts on
  - DST ends on
  - Battery status
  - Locked (YES or NO)
- Seq
- Event Date
- Event Description—Includes key holder or possible key holder. In cases where a key ID is reused, the key holder may be one of multiple.
- Action Result

Credential/Access Point Assignment Report

Generate this report to display credential/access point assignments. The lists of credential classes/credentials that you can select to include in the report include both default and custom classes/credentials. However, the list reflects only those classes/credentials for which keys have been made. If the class or credential has not yet been assigned and encoded on a key, it does not display in the list.

Generate report

1. Go to **Reports > Credential/Access Point Assignment Report**.
2. Select one of the following index options:
   - **Access Point**
   - **Credential**
3. Click **Next to Credential Classes**.
   Because all classes are selected by default, deselect any class that you want to exclude from the report.
4. Click **Generate**.

View report details (access point)

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Displayed by
  - Access Point
- Total keys
- Site
- Report generated by
- Report generated on
- Credential Class(es)
- Access Point
- Credential class
- Credential

View report details (credential)

- Displayed by
  - Credential
- Total keys
- Site
- Report generated by
- Report generated on
- Credential Class(es)
- Credential Class
- Credential
- Access Point

Elevator Configuration Report

Generate this report to view configuration information for an elevator bank. The report shows relay-to-floor mapping for each panel in the bank and lists elevator details.

Generate report

1. Go to **Reports > Elevator Configuration Report**.
2. Select an elevator bank.
3. Click **Generate**.

View report details

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Building
- Site
- Report generated on
- Report generated by
- Elevator Bank
- Elevators
- Profile
- Panel
- Relay
- Floor

Key Expiration Report

Generate this report to identify keys that are approaching expiration. The lists of credential classes/credentials that you can select to include in the report include both default and custom classes/credentials. However, the list reflects only those classes/credentials for which keys have been made. If the class or credential has not yet been assigned and encoded on a key, it does not display in the list.

Generate report

1. Go to **Reports > Key Expiration Report**.
2. Because all classes are selected by default, deselect any class that you want to exclude from the report.
3. Click **Next to Credentials**.
4. Because all credentials are selected by default, deselect any credential that you want to exclude from the report.
5. Click **Next to Date Range**.
6. Specify the time span to include in the report.
7. Click **Generate**.

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

The report shows the following details for all current and expired keys for the selected options.

- Date Range
- Total keys assigned
- Site
- Report generated by
- Report generated on
- Credentials
- Credential Class
- Credential (key ID)
- Additional Access/Common Areas
- Creation Date
- Expiration Date
- Key Holder
- Status—For physical keys: Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.

Key/User Assignment Report

Generate this report to identify the keys assigned to staff/vendors. The report includes a list of all access points encoded on each assigned key.

Generate Report

1. Go to **Reports > Key/User Assignment Report**.
2. Select whether to include active keys, inactive keys, or both in the report. (All keys with a status other than "Active" are considered inactive.)
3. Select whether to index the report by staff member/vendor name or key credential.
4. Click **Next to Credential Classes**.
5. Because all classes are selected by default, deselect any class that you want to exclude from the report.
6. Click **Generate**.

View Report Details (Staff/Vendor)

- Displayed by
- Total keys assigned
- Site
- Report generated by
- Report generated on
- Key Holder
- Credential Class
- Credential (key ID)
- Additional Access/Common Areas
- Status
- Creation Date
- Expiration Date

Operator Report

Generate this report to view a list of operators, their assigned roles, and the rights associated with each role.

Generate report

1. Go to **Reports > Operator Report**.
2. Because all operator status types are selected by default, deselect any status type that you want to exclude from the report:
   - **Active**—When selected, the report includes all active operators.
   - **Deactivated**—When selected, the report includes all operators who are deactivated.
   - **Blocked**—When selected, the report includes all operators blocked from Community software.
3. Click **Next to Operator Roles**.
   Because all roles are selected by default, deselect any role that you want to exclude from the report.
4. Click **Generate**.

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Operator status
- Operator roles
- Total operators
- Site
- Report generated by
- Report generated on
- Operator Name
- User Name
- Role
- Assign Date
- Status
  - Active
  - Deactivated
  - Blocked

Property Configuration Report

Generate this report to view the access point configuration for your site.

Generate report

1. Go to **Reports > Property Configuration Report**.
2. Select a building.
3. Click **Next to Floors**.
4. Select the floors to include in the report.
5. Click **Next to Access Point Types**.
   Because all access point types are selected by default, deselect any type that you want to exclude from the report.
6. Click **Generate**.

View report details

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Total access points
- Report generated by
- Report generated on
- Buildings
- Floors
- Sequence (Seq)
- Access Point
- Access Point Type
- Lock/Device Model
- Building Name
- Floor Name

Roles and Rights Report

Generate this report to view a list of roles defined in the **Role Management** module and the Community functions to which each role has rights.

Generate report

1. Go to **Reports > Roles & Rights Report**.
2. Select whether to generate a report that shows the roles authorized for system rights or key rights.
3. Select whether to include operators. If you select to include operators, select the operator status types to include:
   - **Active**—When selected, the report includes all active operators.
   - **Deactivated**—When selected, the report includes all operators who are deactivated.
   - **Blocked**—When selected, the report includes all operators who are blocked from Community software.
4. Click **Generate**.

View report details

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Include operators
- Total roles
- Site
- Report generated by
- Report generated on
- Roles (including list of Operators assigned the role)
- System Rights / Key Rights

Staff/Vendor Access Report

Generate this report to view historical information about staff/vendor access.

Before you can generate this report, you must obtain and read the physical key assigned to staff/vendors. The report can be viewed directly after reading the key or in the **Reports** module. The benefit to viewing access data in the **Reports** module is that you can select a date range to include historical data.

Generate report

1. Go to **Reports > Staff/Vendor Access Report**.
2. Select a name.
3. Click **Next to Key List**.
4. Select the key credentials to include in the report.
5. Click **Next to Date Range**.
6. Select start and ends dates.
7. Click **Generate**.

View report details

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Date range
- Access events
- Site
- Report generated by
- Report generated on
- Credential
- Expires in locks
- Shift schedule
- Key status—For physical keys: Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- Seq
- Event Date
- Access Point
- Access Granted
- Time Set
- Dead Bolted
- Low Battery
- Lock Prob?
- Lock Latched
- New key

System Activity Report

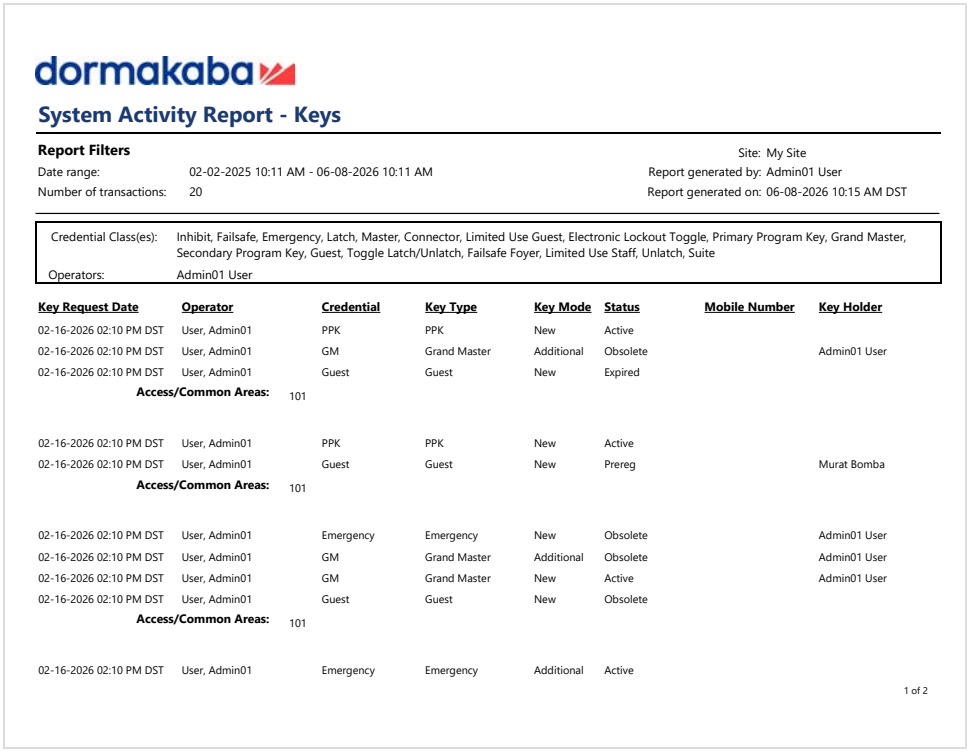
Generate this report to view the transaction history for selected operators.

Generate report

1. Select whether to generate a report that includes system activity related to key events or system events.
   - If you select **Key**, select the options to include resident (physical/mobile keys), staff/vendor (physical/mobile) and system keys, then click **Next to Credential Classes** and deselect the classes to exclude from the report.
2. Click **Next to Operators**.
3. Select the operators to include in the report.
4. Click **Next to Date Range**.
5. Specify the time span for the report.
6. Click **Generate**.

View report details (key)

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.



dormakaba

System Activity Report - Keys

Report Filters

Date range: 02-02-2025 10:11 AM - 06-08-2026 10:11 AM
Number of transactions: 20
Site: My Site
Report generated by: Admin01 User
Report generated on: 06-08-2026 10:15 AM DST

Credential Class(es): Inhibit, Failsafe, Emergency, Latch, Master, Connector, Limited Use Guest, Electronic Lockout Toggle, Primary Program Key, Grand Master, Secondary Program Key, Guest, Toggle Latch/Unlatch, Failsafe Foyer, Limited Use Staff, Unlatch, Suite
Operators: Admin01 User

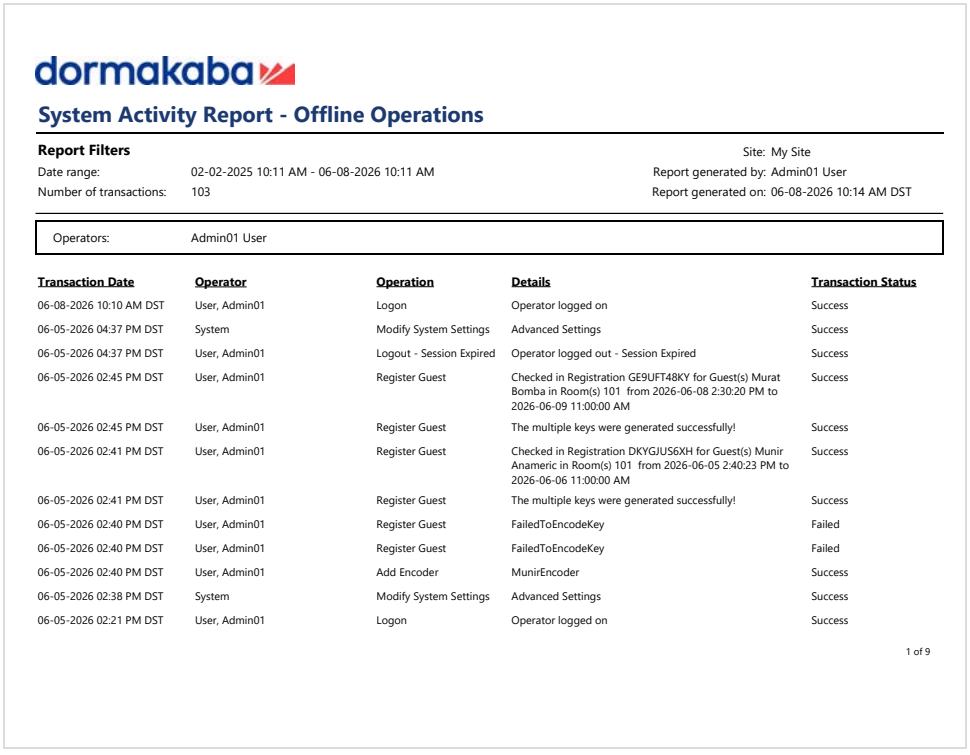
Key Request Date	Operator	Credential	Key Type	Key Mode	Status	Mobile Number	Key Holder
02-16-2026 02:10 PM DST	User, Admin01	PPK	PPK	New	Active		
02-16-2026 02:10 PM DST	User, Admin01	GM	Grand Master	Additional	Obsolete		Admin01 User
02-16-2026 02:10 PM DST	User, Admin01	Guest	Guest	New	Expired		
Access/Common Areas:	101						
02-16-2026 02:10 PM DST	User, Admin01	PPK	PPK	New	Active		
02-16-2026 02:10 PM DST	User, Admin01	Guest	Guest	New	Prereg		Murat Bomba
Access/Common Areas:	101						
02-16-2026 02:10 PM DST	User, Admin01	Emergency	Emergency	New	Obsolete		Admin01 User
02-16-2026 02:10 PM DST	User, Admin01	GM	Grand Master	Additional	Obsolete		Admin01 User
02-16-2026 02:10 PM DST	User, Admin01	GM	Grand Master	New	Active		Admin01 User
02-16-2026 02:10 PM DST	User, Admin01	Guest	Guest	New	Obsolete		
Access/Common Areas:	101						
02-16-2026 02:10 PM DST	User, Admin01	Emergency	Emergency	Additional	Active		

1 of 2

- Date range
- Number of transactions
- Site
- Report generated by
- Report generated on
- Credential Classes

- Operators—The full name of the operator who was logged in when the key was encoded. "API" following the name indicates the key was made using the Community API. If the key was made using the API and API authentication is disabled, only "API" is listed.
- Key Request Date
- Operator
- Credential
- Key Type
  - Resident (Physical)
  - Resident (Mobile)
  - Staff/Vendor (Physical)
  - Staff/Vendor (Mobile)
  - System
- Key Mode
  - Additional
  - New
- Key ID
- Status—For physical keys: Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- Mobile Number
- Key Holder or Possible Key Holder. In cases where a key ID is reused, the key holder may be one of multiple.
- Additional Access/Common Areas

View report details (system)



dormakaba

System Activity Report - Offline Operations

Report Filters

Date range: 02-02-2025 10:11 AM - 06-08-2026 10:11 AM
Number of transactions: 103
Site: My Site
Report generated by: Admin01 User
Report generated on: 06-08-2026 10:14 AM DST

Operators: Admin01 User

Transaction Date	Operator	Operation	Details	Transaction Status
06-08-2026 10:10 AM DST	User, Admin01	Logon	Operator logged on	Success
06-05-2026 04:37 PM DST	System	Modify System Settings	Advanced Settings	Success
06-05-2026 04:37 PM DST	User, Admin01	Logout - Session Expired	Operator logged out - Session Expired	Success
06-05-2026 02:45 PM DST	User, Admin01	Register Guest	Checked in Registration GE9UFT48KY for Guest(s) Murat Bomba in Room(s) 101 from 2026-06-08 2:30:20 PM to 2026-06-09 11:00:00 AM	Success
06-05-2026 02:45 PM DST	User, Admin01	Register Guest	The multiple keys were generated successfully!	Success
06-05-2026 02:41 PM DST	User, Admin01	Register Guest	Checked in Registration DKYGJUS6XH for Guest(s) Munir Anameric in Room(s) 101 from 2026-06-05 2:40:23 PM to 2026-06-06 11:00:00 AM	Success
06-05-2026 02:41 PM DST	User, Admin01	Register Guest	The multiple keys were generated successfully!	Success
06-05-2026 02:40 PM DST	User, Admin01	Register Guest	FailedToEncodeKey	Failed
06-05-2026 02:40 PM DST	User, Admin01	Register Guest	FailedToEncodeKey	Failed
06-05-2026 02:40 PM DST	User, Admin01	Add Encoder	MunirEncoder	Success
06-05-2026 02:38 PM DST	System	Modify System Settings	Advanced Settings	Success
06-05-2026 02:21 PM DST	User, Admin01	Logon	Operator logged on	Success

1 of 9

- Date range
- Number of transactions
- Site

- Report generated by
- Report generated on
- Operators
- Transaction Date
- Operator—The full name of the Operator who was logged in when the key was encoded. "API" following the name indicates the key was made using the Community API. If the key was made using the API and API authentication is disabled, only "API" is listed.
- Operation
- Details
- Transaction Status

Visitor Management Report

This report is available when licensed for visitor management.

Generate this report to view a list of delegated PINs and mobile keys. Operators who are assigned the Administrator or Site Configurator role have default access to generate this report. For all other operators, the right must be enabled for the assigned role in **Role Management**.

Generate Report

1. Go to **Reports > Visitor Management Report**.
2. Select whether to include visitor management data for residents or staff. For Staff, select the PIN status' to include in the report. (Reports for residents include all status types.)
3. Click **Next to Residents** or **Next to Staff Members**.
4. Select the residents or staff members to include in the report.
5. Click **Generate**.

View Report Details

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- User type (resident or staff member)
- Site
- Report generated by
- Report generated on
- Delegator—The resident or staff member who delegated the PIN or mobile key.
- Operation—The type of delegation, PIN or mobile key.
- Delegated—Date and time when PIN/mobile key was delegated.
- Access—For PIN: the PIN number, common areas, number of uses remaining until expiration. For mobile key: common areas.
- Valid from—The date/time when access using the PIN/mobile key starts.
- Valid to—The date/time when access using the PIN/mobile key ends.
- Key/PIN Holder—Name of visitor for whom the PIN/mobile key was issued.
- Status—Active/Revoked/Expired. Reports for residents include all status'. Reports for staff include only those status' selected.

Toolbar

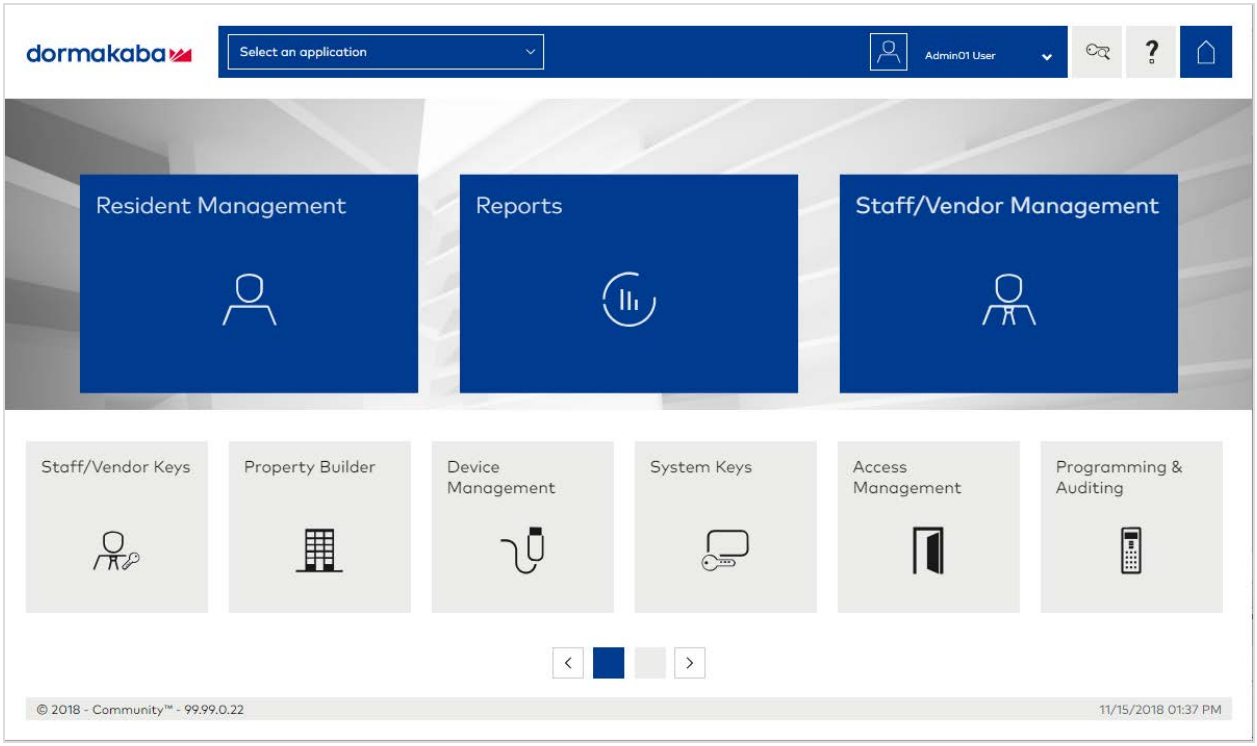
Toolbar Basics

This section includes the following subjects:

Navigate Community 269
Set operator preferences 271
Install / update Community Client 273
Select default encoder 274
Remote unlock/lock 275
Read key/erase key/access tracking report 277
View notifications 281
Physical keys 283
Digital keys 285

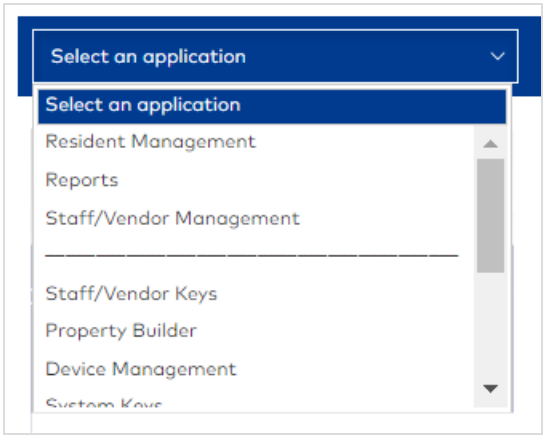
Navigate Community

Community modules are accessible no matter where you are in the product. When you first log in, the Home page uses tiles to provide access to modules. The top section is designed to show favorites (the modules that you use most often). The tiles for all other modules are in the bottom section. You may need to scroll forward to display the tile for a module. You can drag and drop tiles from the bottom section to the favorites area to customize your Home page.



Module selector

From within any module, you can quickly switch to a different module by using the module selection list in the Community toolbar. The first three items in the list show the favorites. All other modules are listed in alphabetic order.



To navigate Community modules:

- From the Home page, click a module tile. You may need to scroll forward in the bottom section to display the tile for a module.

- From all other pages, select a module from the module selection list in the Community toolbar.

Go to the Home page or log out

- To go to the Community Home page, click **(Home)** .
- To log out of Community, click ***account user name*** > **Log Out**.

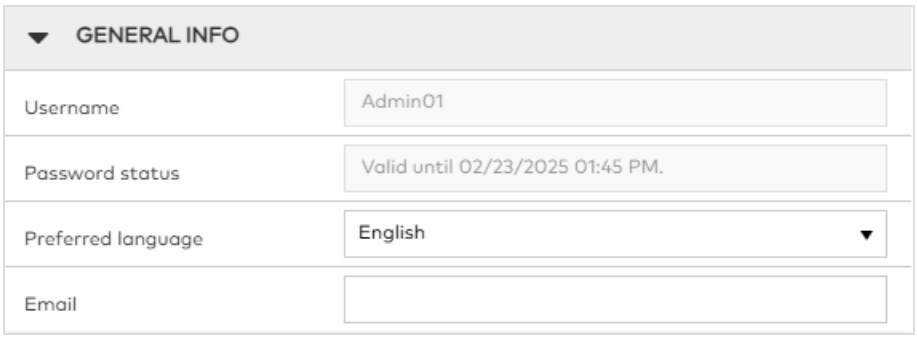
Set operator preferences

To set operator preferences:



1. On the main toolbar, click *operator user name* > **Preferences**.
2. Modify the parameters below.
3. Click **Save**. After saving the preferences, the screen refreshes in the selected language.

GENERAL section



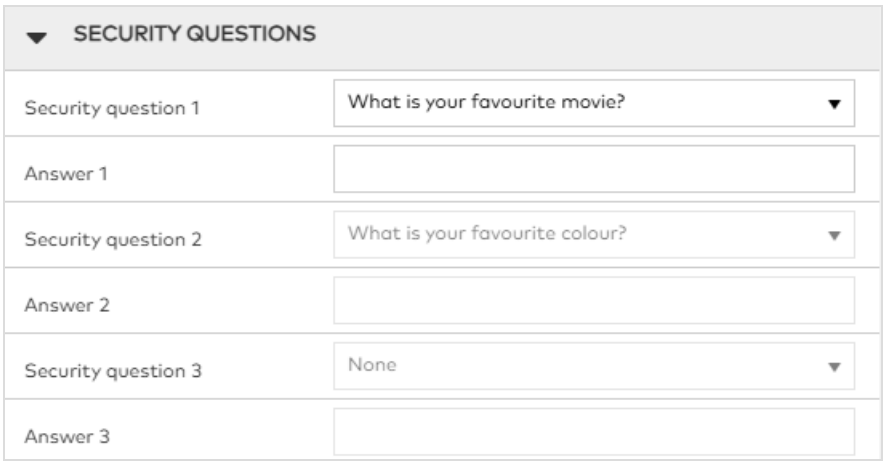
- Username is a read-only option that displays the operator user name.
- Password status is a read-only option that displays the expiration details for the Community account password.
- Select the preferred language for the account holder. The default is to detect and display the UI in the browser language. For Community to detect and display the UI in the browser language, the language setting in both **Systems Settings > General** and **Preferences** must both be Automatic Language Detection.
- For Email, specify an email address to associate with the account for notifications. Community sends automated emails regarding account status. The email address specified in the operator profile is linked with the email address in account Preferences.

PASSWORD section



Change the Community account password. To view values, click . Passwords may not contain your user ID, email address, first name or last name. Password criteria and expiration are based on settings in **System Settings > Security**.

SECURITY QUESTIONS section



Select and provide responses to the challenge questions when required to submit a request to retrieve or reset the password.

Install / update Community Client

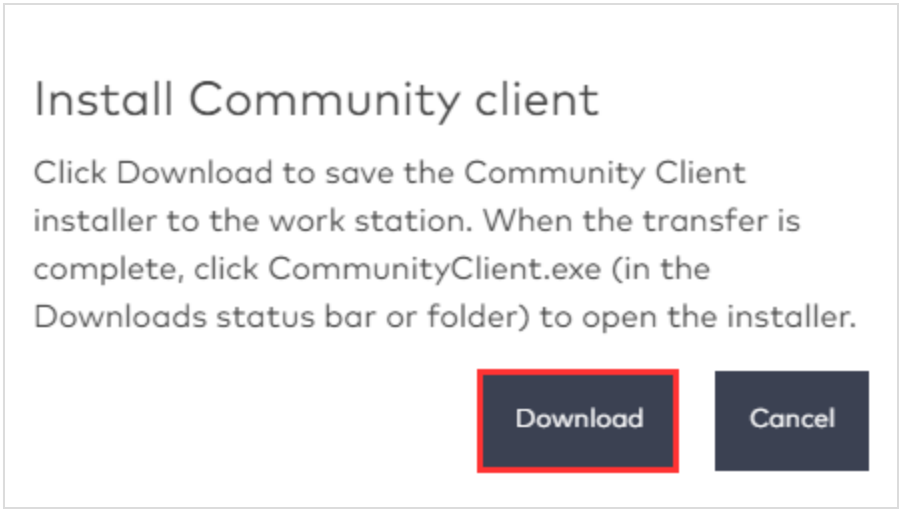
The Community Client is required to encode and read keys, and to use the M-Unit to program and audit locks and devices. The Community Client and Community Server must be the same version to ensure proper key-encoding operations. Upon login, Community detects the Client version and if it is older than the Server version, prompts you to download and install the current Client.

Perform the installation as a Local Administrator (not Network Administrator).

1. Go to **Device Management** or **Programming & Auditing**.



2. Click **(Install Community Client)** .



3. Click **Download**. A total of three files are required Community_Client.exe, serverURL.config, and token.txt. The download process can take up to one minute.
4. When the download is complete, click **CommunityClient.exe**. The installer opens. If anti-virus or firewall software is installed on the workstation, you may be prompted to allow the installer to open.
5. On the Welcome page, click **Next** (or **Repair** if the client is already installed).
   The **Setup Status** page displays while the Client is installed.
6. On the **Update Complete** page, click **Finish**.

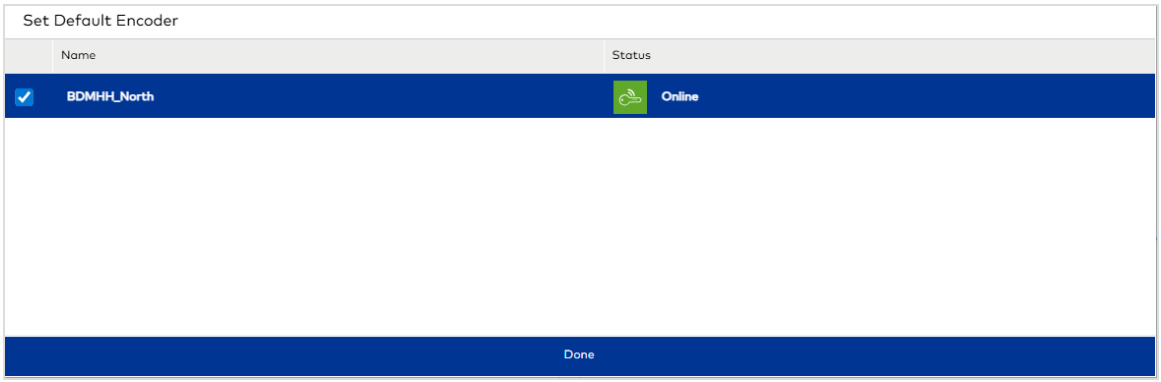
Select default encoder

You can set the default encoder from the main Community toolbar in modules where keys are made. At key-making time, you can always select any encoder that is online and available to the workstation.

1. Go to any module in which keys are made (**Resident Management**,**Staff/Vendor Management**,**Staff/Vendor Keys**, **System Keys**).



2. In the toolbar, click **(Encoder status)** .



3. Select the encoder to automatically populate when making keys.
4. Click **Done.**

Remote unlock/lock

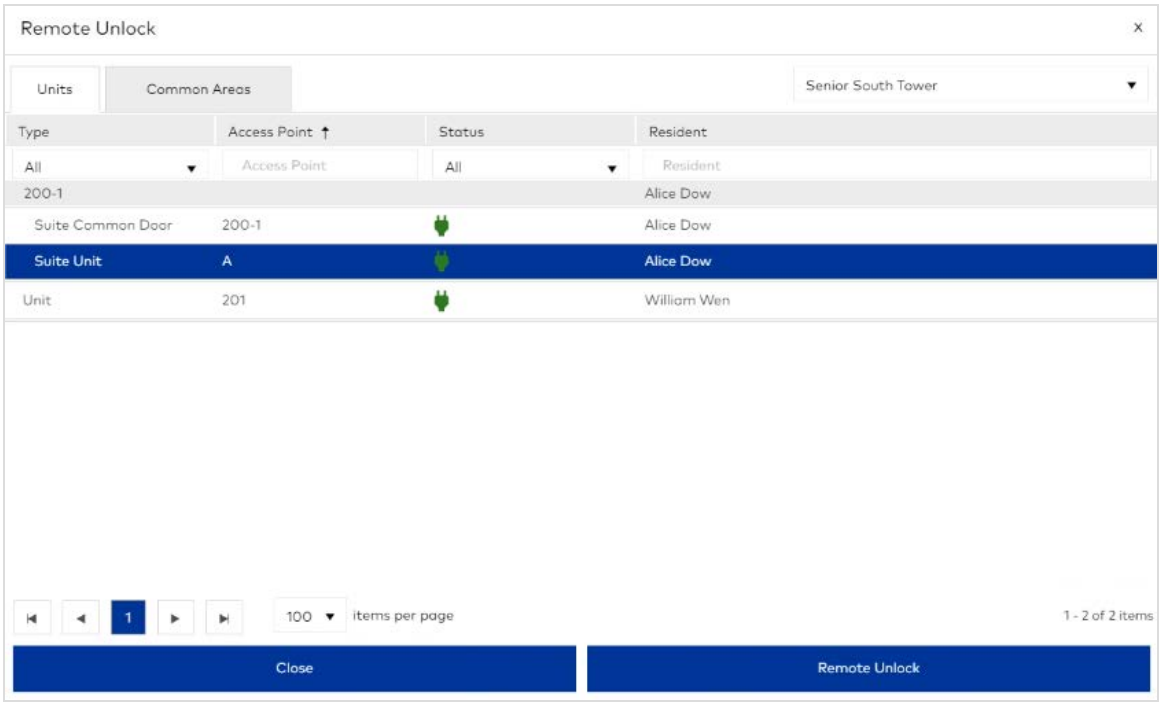
This toolbar option is available when Online Communication is enabled and configured for **Gateway II; RAC5-MFC/XT; Rx-Link**. The active Operator must also be assigned a role with the **Remote Unlock** system right enabled.

The Community toolbar includes an option to remotely lock and unlock occupied units, suites (common door and suite unit), and resident common areas. The lock must be online to issue a command.

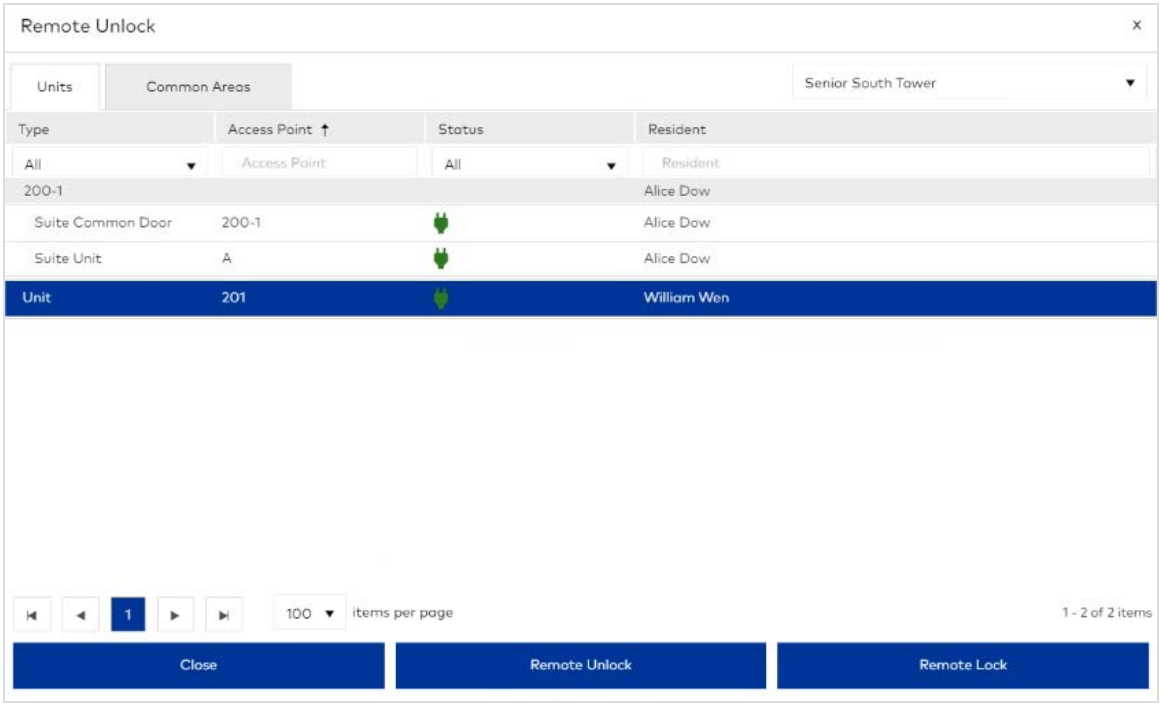


To remotely lock or unlock an access point:

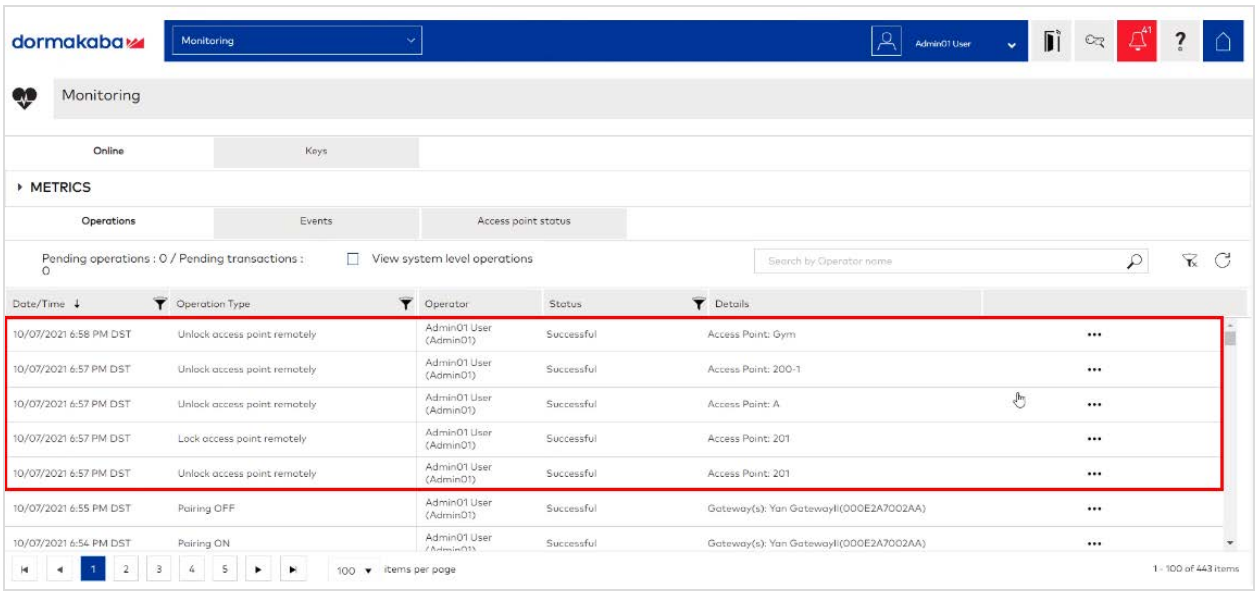
1. Click (Remote Unlock) .
2. Select the access point that you want to unlock/lock. Units and suite access points are listed on the **Units** tab. Resident common areas are listed on the **Common Areas** tab. You can filter the list by building, access point name, and status (Online/Offline). For units and suites, you can also filter by access point type and resident name.



3. Click the button for the command that you want to issue.
   - When toggle mode is not supported, the only option is to select **Remote Unlock**.
   - When toggle mode is supported, select **Remote Unlock** (or **Remote Lock**). The access point remains in the unlocked (or locked) state until a valid key or command (from the toolbar or an associated schedule) toggles the state of the lock.



View results in the **Monitoring** module.



Read key/erase key/access tracking report

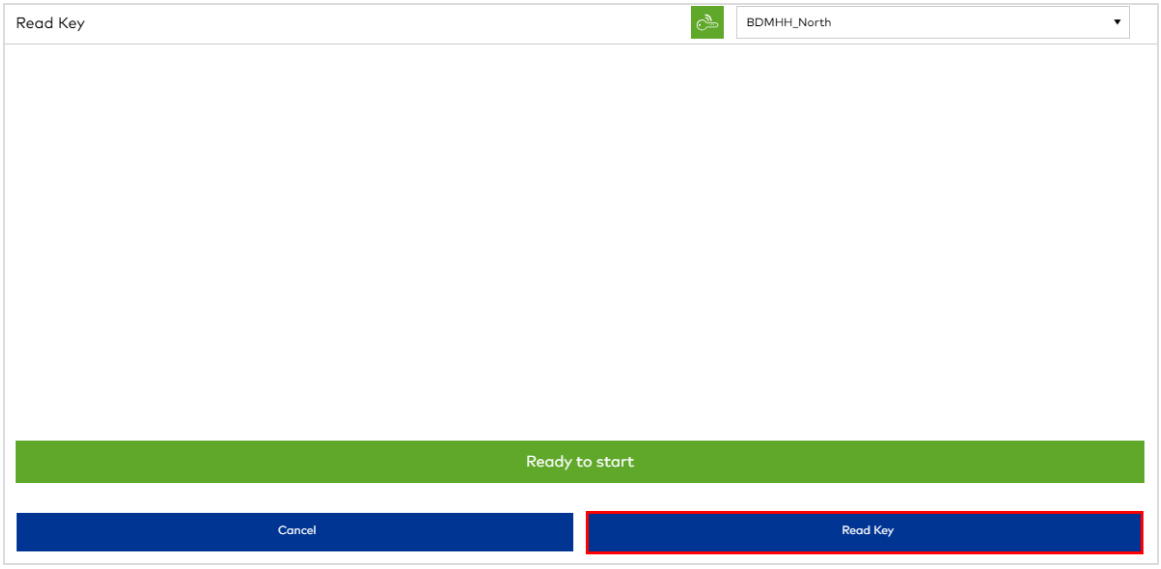
Learn the status of any key by using the Community key reader accessible from the main toolbar. After successfully reading a key, you can erase all configuration data encoded on the key and generate an access report.

Read key

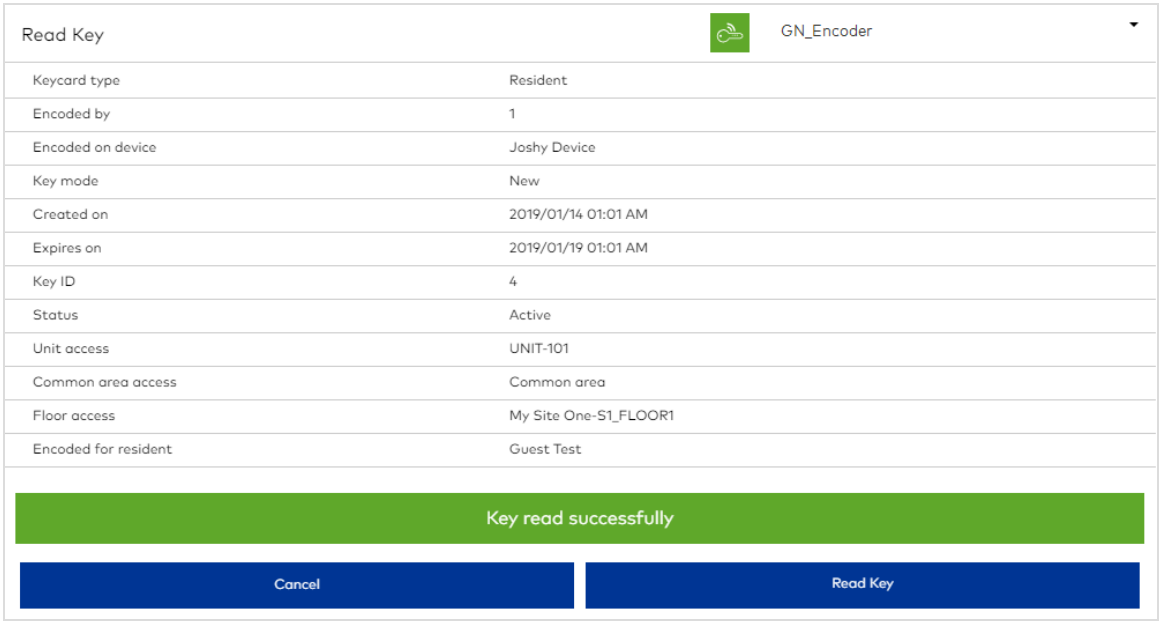
To read any key:



1. On the main toolbar, click **(Read Keys)** .



2. Select an encoder that is online and available to the workstation.
3. Present a key to the encoder.
4. Click **Read Key**.



The information displayed depends on the key type. The following details display for Resident Keys:

- Keycard type
- Encoded by
- Encoded on device
- Key mode
- Created on
- Expires on
- Key ID
- Status
- Unit access
- Common area access
- Floor access
- Encoded for resident

Additional data displays for keys which are encoded with a third-party service in sector 2.

Read key failures

When reading a key fails, an information box identifies the following problems:

- When communication between the encoder and workstation fails.
- When the encoder is offline.
- When the encoder is busy.
- When a key is not presented to the encoder within the expected delay.
- When the key is damaged, corrupt or uses unsupported technology.

Erase key

This function is not supported when Enhanced Security Mode is enabled. However, high security keys can be re-encoded at the same site using the same Community database.

You can erase any key (resident/staff/vendor/system) only directly after the key is read. Erasing a key removes all configuration data encoded on the key.

To erase a key:

1. After the key is successfully read, click **Erase Key**.
2. Click **YES** to confirm.
3. When done, click **OK**.

Keys that are erased show as "Returned" in reports and **Monitoring > Keys**.

Read Key Access Report

After reading a key, you can generate a detailed list of the access points the key can access. This report is only available when access data is on the key, and the active operator is authorized to generate the report.

Access reports include a maximum of 72 or 408 events for 1k/4k keys respectively. MIFARE mini keys do not retain access tracking data.

To generate a report:

1. After the key is successfully read, click **View Resident Access Report**.
2. After the key is successfully read, click **View Staff/Vendor Access Report**.

Access details

- Date Range—The dates and times during which the events included in the report occurred.
- Access Events—The number of records in the report.
- Key Holder—The name of the resident.
- Access—The access points authorized for the key holder.
- Check In—The date and time access is valid.
- Check Out—The data and time access is invalid.
- Key status—The current state of the key. For physical keys: Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- Seq—The order in which an event occurred.
- Event Date—The date and time the event occurred.
- Access Point—The access point to which the key was presented.
- Access Granted—Indicates whether access was granted when the key was presented.
- Time Set—Indicates whether the lock clock is set properly. If No, then the reported Event Date may be wrong. The most common reason for the lock clock to not be set is replacing a depleted battery. For Online systems, a lock clock syncs with the online system when batteries are replaced. For offline systems, staff members can use an M-Unit to reset a lock clock.
- Dead Bolted—Indicates whether the deadbolt was engaged at the time of the event.
- Low Battery—Indicates whether the battery was low at the time of the event.
- Lock Prob?—Indicates a problem with the lock at the time of the event.
- Lock Latched—Indicates whether the lock was latched at the time of the event.
- New Key—Indicates whether the key is New. If the key is not New, it is an Additional Key.

Staff/vendor access details

- Date Range—The dates and times during which the events included in the report occurred.
- Access Events—The number of records in the report.
- Credential —The name of the credential and key mode (New or Additional).
- Shift schedule—The name of any shift schedule assigned to the key.
- Expiration—The date and time after which access on the key is invalid.
- Key status—The current state of the key. For physical keys: Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.

- Seq—The order in which an event occurred.
- Event Date—The date and time the event occurred.
- Access Point—The access point to which the key was presented.
- Access Granted—Indicates whether access was granted when the key was presented.
- Time Set—Indicates whether the lock clock is set properly. If No, then the reported Event Date may be wrong. The most common reason for the lock clock to not be set is replacing a depleted battery. For Online systems, a lock clock syncs with the online system when batteries are replaced. For offline systems, staff members can use an M-Unit to reset a lock clock.
- Dead Bolted—Indicates whether the deadbolt was engaged at the time of the event.
- Low Battery—Indicates whether the battery was low at the time of the event.
- Lock Prob?—Indicates a problem with the lock at the time of the event.
- Lock Latched—Indicates whether the lock was latched at the time of the event.
- First Key Use—Indicates whether the key has been used to access a space.

View notifications

Community offers notifications to keep operators informed about system events.

When online communication is enabled, notifications keep staff members informed about operations and events related to online communication (gateways and paired access points). For example, a notification lets you know when a key is used or a door is ajar.

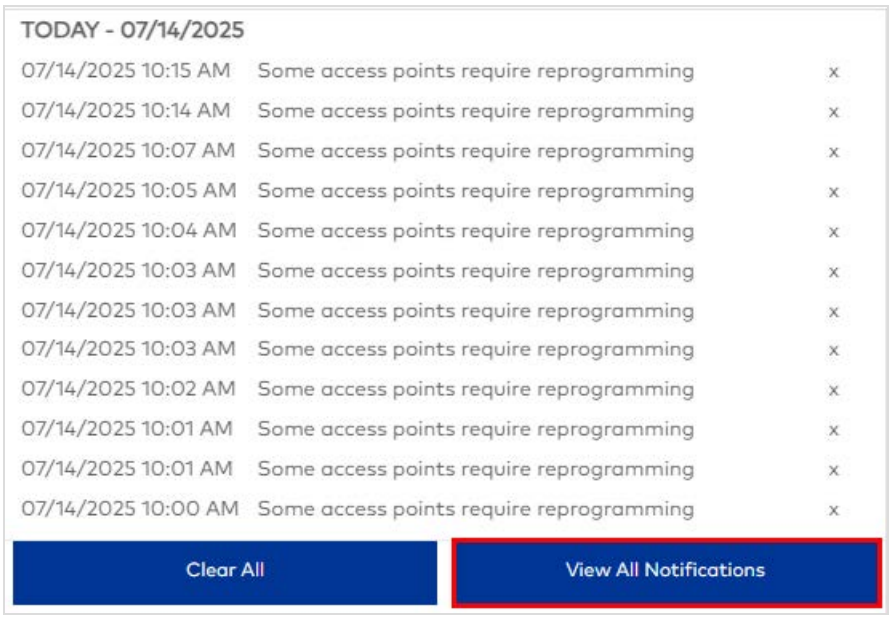


To view recent notifications:

» Click **(Notifications)** on the main toolbar. Recent notifications are listed showing the date, time and command result. To delete a recent notification, click **(Delete)** x.

To view all notifications:

» Click **(Notifications)** **> VIEW ALL NOTIFICATIONS** on the main toolbar. The list of notifications includes events selected in the notification groups to which the current Operator subscribes.



The following information is displayed for each notification:

- **Notification**—The notification text/online event.
- **Category**—The type of notification: General or Online.
- **Date/Time**—The date and time the event occurred.
- **Details**—More information about the event, such as the command sent, and if applicable, the names of paired access points.

Use the Notifications toolbar to search notifications and take any of the following actions:

- Delete notifications—Select one or more notifications, then click **(Delete)** ✕.
- Clear notifications from the Recent notifications list—Select one or more notifications, then click **(Mark as Read)** 🔔.

- Filter notifications by notification, category, and date/time—Click **(Filter)** , select **From** and **To** dates, then click **Filter**. To clear a column filter, click **(Filter Applied)** , then **Clear**. To clear all filters, click **(Reset Filters)** .
- Show/hide notification event types—Click and select the event categories to include in the list (**General** and **Online**).
- Refresh the data—Click **(Refresh)** .

General events

The basic notification feature includes only the following event:

- **Some access points require reprogramming**—Notifies when it is necessary to resynchronize Community configuration data for the access points listed in the Details column.

Online events

- **Access point offline**—Notifies that there is no communication between the lock and the gateway.
- **Access point online**—Notifies that the lock is online and in communication with the gateway.
- **Access Point Paired**—Notifies that an access point was paired to a gateway.
- **Door ajar clear (door secure)**—Door previously ajar has now been closed and is secure.
- **Door ajar generic**—Notifies that a door is in an open state.
- **Door ajar resident long**—Door ajar beyond the configured threshold. The door ajar (long) event notifies a door has been left open for a longer time interval, indicating an unusual state, a potential intrusion.
- **Door ajar resident short**—Notifies that a door ajar (short) event signaling a door has been left open for a short time interval, for example the time it would take to vacate a room.
- **Door ajar staff/vendor long** —Notifies a door ajar (long) has been left open by a staff member/vendor for a longer time interval, indicating an unusual state, a possible intrusion in progress.
- **Door ajar staff/vendor short** —The door ajar (short) notifies a door has been left open by a staff member/vendor for a short time interval.
- **Door latched**—Notifies that a door is closed with the lock engaged.
- **Door open**—The lock's anti-pick mechanism is out. This is the default state of the door.
- **Door unlatched**—Notifies that the lock motor has been disengaged and the door can be opened without a key.
- **Generic egress**—Egress is an open door event.
- **Resident key used**—Date and time that a key was used at the access point.
- **Resident key used (first entry)**—Notifies a resident has accessed the lock for the first time.
- **Gateway offline**—Gateway is currently not communicating with the Community Server.
- **Gateway online**—Displays all gateways that are online and visible in the Monitoring module.
- **Low battery**—The battery state is low and requires replacement.
- **Low battery clear (battery normal)**—The low battery notification has been cleared; the battery was replaced or the problem resolved.
- **Mechanical key override**—Notifies a lock override, accessing a lock with a mechanical key.
- **Operation failed**—The specified operation was not successful. When available, the reason is indicated.
- **Privacy disabled/deadbolt retracted**—Notifies the status of the deadbolt as disengaged.
- **Privacy enabled/deadbolt engaged**—Notifies that the deadbolt or privacy switch is engaged.
- **Access point programming required**—Lock may require resequencing or synchronization with Community configuration data.
- **Staff key used**—Notifies that a staff/vendor key has accessed the lock.
- **Standing intruder**—Alert: Possible standing intruder. Multiple keys presented at a single access point.
- **System key Used**—Notifies that a System key was presented to the lock.
- **Wandering intruder**—Alert: Possible wandering intruder. Key presented at multiple access points.

Physical keys

A key is any device on which a credential is encoded for the purpose of controlling access and/or performing system or programmatic operations. Examples include key cards and key fobs.

Selecting a Key Mode (New/Additional)

All Resident Keys have a key mode: New or Additional. When you make the first key for a credential (a unit or combination of units), the only mode that you can select is New. For all subsequent keys that you make for the same credential, the option to select New or Additional is available. If all you want to do is make copies of the same key, the mode to choose is the selected default Additional. Making Additional Keys has no effect on active keys with the same credential. Making New Keys, however, invalidates the same credential on all previously active keys with the same credential (once the New Key is presented to a unit or common area in the credential). Reasons that you may want to select the New Key mode include replacing keys that are lost, damaged or stolen.

Example

John and Mark share access to Units 100 and 101. You make a New Key with the same access for John. When John presents the key to Unit 100, Mark's key is invalid for Unit 100. When John presents the key to Unit 101, Mark's key is invalid for Unit 101.

Making keys

aking keys is the process of encoding the credential created during access configuration onto keys. You can make physical keys, mobile keys or both for a resident. To make physical keys, you need an encoder that is online and available to the workstation.

When encoding or reading a key fails, an information box identifies the following problems:

- When communication between the encoder and workstation fails.
- When the encoder is offline.
- When the encoder is busy.
- When a key is not presented to the encoder within the expected delay.
- When the key is damaged, corrupt or uses unsupported technology.

For security reasons, dormakaba imposes a maximum on the number of unused keys that can be issued for a given credential. For example, when more than 15 keys are issued but never presented to Room 100, the access point becomes "out of sequence" and denies access to all of the keys.

To restore key access, reprogram the access point using the Maintenance Unit or resequence the access point using the Resequence Key. After the access point is resequenced, the access point accepts the most recently issued key.

The maximum number of unused keys before resequencing is required depends on the key type:

- Resident Keys
  - Room and Suite=15
- Staff Keys
  - All classes=unlimited
- System Keys
  - Failsafe, Latch, Unlatch, Toggle Latch/Unlatch=15
  - ELO=3
  - Inhibit=0
  - PPK/SPK=0

Key status

The following statuses apply to resident keys, staff/vendor keys, and specific system keys (ELO, Inhibit, Latch, Unlatch, Toggle Latch/Unlatch).

Physical keys only:

- **Active**—Keys that, according to Community, are valid and available for use. This includes keys for which an Unblock key was made and keys that were unblocked remotely. Failsafe Keys always have the status Active.
- **Returned**—Keys that have been erased.

Digital keys only :

- **Delivering - Mobile registered**—Keys that are in the process of being delivered. The dormakaba server detects the mobile device is registered with the mobile application/dormakaba BlueSky.
- **Delivering - Mobile not registered**—Keys that are in the process of being delivered. cannot detect the mobile device.
- **Delivered**—Keys that are valid and available for use, and keys that are invalid because the expiration date arrived.
- **Canceling**—Keys that are in the process of being deleted from the mobile device.
- **Canceled**—Keys that have been deleted from the mobile device.
- **Failed**—Keys that were never delivered to the mobile device.

All keys:

- **Expired**—Keys that are invalid because the expiration date arrived.
- **Obsolete**—Keys may be obsolete when: a) a New key with the same credential was made, b) access was removed prior to expiration. Keys that are obsolete may include one of the following sub-statuses:
  - **Obsolete (blocked)**—Keys for which a Block key was made and keys for which a Block key was sent remotely.
  - **Obsolete (canceled)**—Keys for which a Cancel key was made and keys for which a Cancel key was sent remotely.

For staff keys, obsolete keys continue to allow access to common areas until key expiration. To maintain security, create Block Keys for key sequences with the status *Obsolete*. See System Settings > Block Keys.

Digital keys

Digital keys offer residents the convenience of using their phone to access their room and hotel amenities. dormakaba supports the following digital key types:

- mobile keys
- Apple Wallet keys (requires REST API)
- Apple Watch keys (requires REST API)
- Google Wallet keys (requires REST API)

Digital keys work in combination with hotel-specific mobile apps or the dormakaba BlueSky app for mobile keys to provide guests a fast, secure, and convenient way to access their rooms and amenities.

For wallet keys, guests can tap their device to unlock doors—even in Express Mode, which works without waking or unlocking the phone. If the phone battery runs low, the key continues to function for up to five hours. Guests can also securely share their digital room key with trusted companions.

Typically, additional cost is associated with using mobile keys. Consult LEGIC or your mobile network provider for details.

Mobile keys work with dormakaba BlueSky to offer the convenience of a virtual key. Typically, additional cost is associated with using mobile keys. Consult LEGIC or your mobile network provider for details.

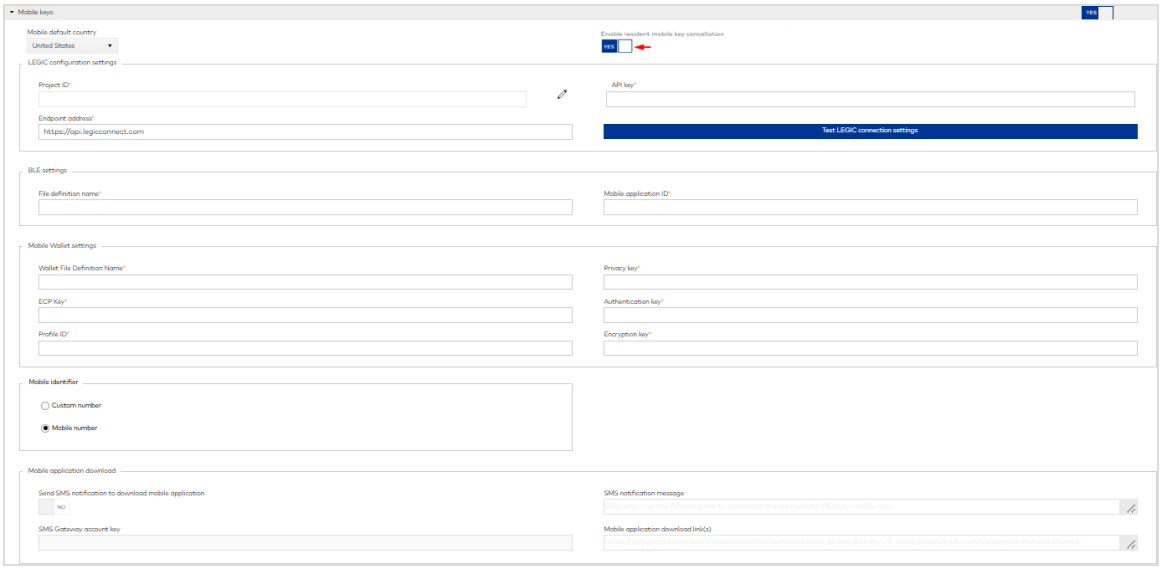
Requirements

- Mobile keys must be enabled in **System Settings > Advanced Settings**. Required for all digital keys.
- Mobile wallet settings are required to issue Apple Wallet, Apple Watch, and Google Wallet keys.
- Mobile wallet keys can only be issued using the REST API.
- The resident / staff member profile must include a valid mobile or custom number.
- Residents / staff must download, install and register their mobile number with the mobile application.

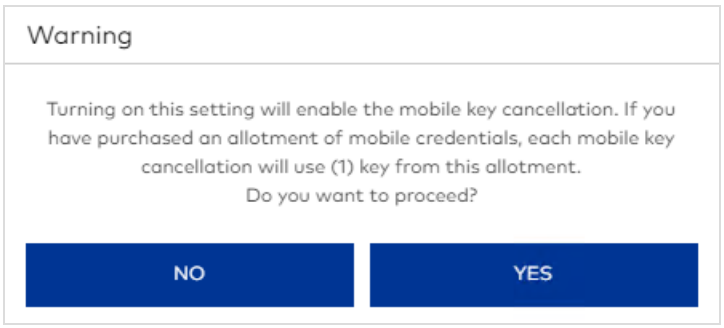
Enable Mobile Keys

To enable and configure mobile keys:

1. Go to **System Settings > Advanced**.



2. Set the **Enable mobile keys** switch to **YES**.
3. For **Mobile default country**, select the default country for mobile numbers. The corresponding country code is retrieved for the mobile number.
4. If you want the ability to cancel mobile keys, set the **Enable resident mobile key cancellation** switch to **YES**. If mobile keys are enabled and this option is not enabled, you cannot cancel a mobile key. Instead, the expiration details determine when the mobile key becomes invalid.



5. For **LEGIC configuration settings**, a dormakaba Customer Service technician provides valid values.
6. Select whether to use mobile phone numbers or custom numbers. A custom number is a unique numeric identifier that is used as an alternative to a mobile number. Key generation and cancellation work the same for mobile and custom numbers. Legic can recognize a key holder based on mobile or custom number.

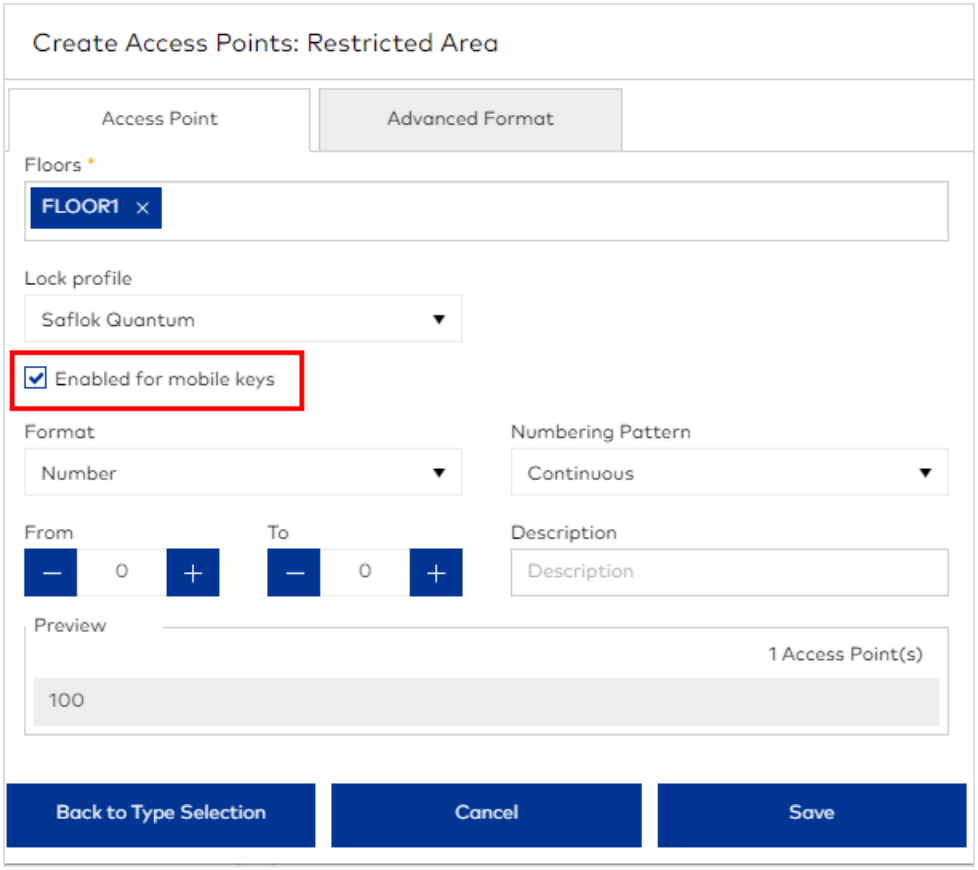
Custom numbers are only supported when mobile keys are made/issued from the API.

7. Select whether to send a text message to recipients of mobile keys to notify them that their device is not registered with dormakaba BlueSky. If you select **YES**, you must also specify the message text to send, an SMS Gateway account key (see Swift SMS Gateway), and at least one link where dormakaba BlueSky can be downloaded.

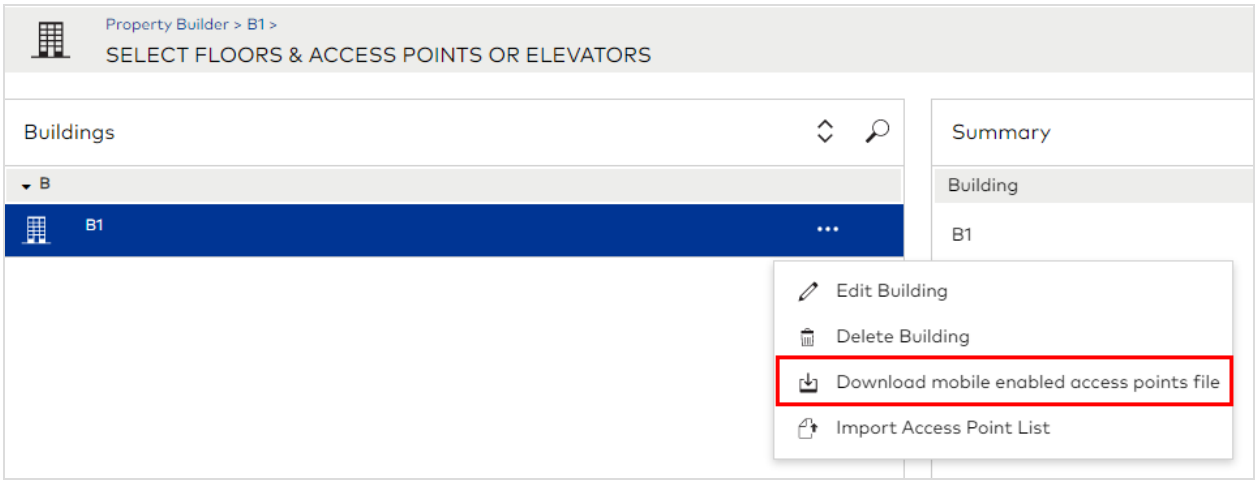
Mobile-enabled access points

From the Buildings context menu in Property Builder, you can download a file that lists all access points that were configured with the option **Include in mobile keys download file** selected. The option serves to identify the locks that are equipped to accept mobile key credentials.

The following figures shows the option to select in Property Builder.



The following figure shows where to get the download file in Property Builder.



To download the file of mobile-enabled access points:

1. Go to **Property Builder**.
2. Select a building.
3. Click **(More)** ··· **> Download mobile enabled access points file**.

When Mobile Keys Are Issued

After the mobile key is issued, Community detects the mobile provider connection and checks to make sure dormakaba BlueSky has been downloaded onto the mobile device. If no connection is detected, the failure is reported in **Monitoring** > **Keys** and **Reports** > **System Activity Report** (Keys). If a connection is detected but dormakaba BlueSky is not on the device, an SMS message can be sent to the mobile device prompting the user to download the app.

The option **Send download mobile application SMS notification** must be enabled in System Settings > Advanced Settings > Enable mobile keys.

When a connection is detected and the dormakaba BlueSky is installed on the mobile device, the status in Community indicates whether the resident has registered their mobile phone number:

- **Delivering - Mobile registered**—Keys that are in the process of being delivered. Community detects the mobile device is registered with dormakaba BlueSky.
- **Delivering - Mobile not registered**—Keys that are in the process of being delivered. Community cannot detect the mobile device.

When the status of the key is **Delivered**, mobile key recipients can use the mobile key by opening the mobile application and following the screen prompts.

Canceling a mobile key involves issuing a Cancel Key remotely or presenting a physical Cancel Key to the relevant access points. When a Cancel Key is issued remotely, the key status displays as **Canceling** or **Canceled**. If you make a physical Cancel Key to invalidate a mobile key, the status remains **Delivered** (because the key is valid until the Cancel Key is presented to the relevant access points).

The status of mobile keys that are never delivered is **Failed**. The status of mobile keys that have reached expiration is **Expired**. Mobile keys that are invalid because a new mobile key was made with the same credential show the status **Obsolete**.

When connection to a mobile phone is not detected, Community retries every 5 minutes for 24 hours.

For security reasons, dormakaba imposes a maximum on the number of unused keys that can be issued for a given credential. For example, when more than 15 keys are issued but never presented to Room 100, the access point becomes "out of sequence" and denies access to all of the keys.

To restore key access, reprogram the access point using the Maintenance Unit or resequence the access point using the Resequence Key. After the access point is resequenced, the access point accepts the most recently issued key.

The maximum number of unused keys before resequencing is required depends on the key type:

- Resident Keys
  - Room and Suite=15
- Staff Keys
  - All classes=unlimited
- System Keys
  - Failsafe, Latch, Unlatch, Toggle Latch/Unlatch=15
  - ELO=3
  - Inhibit=0
  - PPK/SPK=0

Key status

The following statuses apply to resident keys, staff/vendor keys, and specific system keys (ELO, Inhibit, Latch, Unlatch, Toggle Latch/Unlatch).

Physical keys only:

- **Active**—Keys that, according to Community, are valid and available for use. This includes keys for which an Unblock key was made and keys that were unblocked remotely. Failsafe Keys always have the status Active.
- **Returned**—Keys that have been erased.

Digital keys only :

- **Delivering - Mobile registered**—Keys that are in the process of being delivered. The dormakaba server detects the mobile device is registered with the mobile application/dormakaba BlueSky.
- **Delivering - Mobile not registered**—Keys that are in the process of being delivered. cannot detect the mobile device.
- **Delivered**—Keys that are valid and available for use, and keys that are invalid because the expiration date arrived.
- **Canceling**—Keys that are in the process of being deleted from the mobile device.
- **Canceled**—Keys that have been deleted from the mobile device.
- **Failed**—Keys that were never delivered to the mobile device.

All keys:

- **Expired**—Keys that are invalid because the expiration date arrived.
- **Obsolete**—Keys may be obsolete when: a) a New key with the same credential was made, b) access was removed prior to expiration. Keys that are obsolete may include one of the following sub-statuses:
  - **Obsolete (blocked)**—Keys for which a Block key was made and keys for which a Block key was sent remotely.
  - **Obsolete (canceled)**—Keys for which a Cancel key was made and keys for which a Cancel key was sent remotely.



For staff keys, obsolete keys continue to allow access to common areas until key expiration. To maintain security, create Block Keys for key sequences with the status *Obsolete*. See System Settings > Block Keys.

dormakaba BlueSky Installation

The BlueSky app is free and consumes 34 MB. During installation, residents may receive the following prompts:

- **Last name**—Specify the same last name that is in the resident profile. The value is not case-sensitive. A validation check is performed using the last name before a mobile key is issued to the app.
- **Allow notifications**—The selected response does not affect the operation of mobile keys.
- **Make data available to Bluetooth devices**—Residents must select **OK** because the mobile app communicates with locks using Bluetooth technology.
- **Country**—Residents must select the country associated with the mobile phone number. Upon selection, the country code is populated.
- **Mobile phone number**—Residents must specify the complete phone number including any regional or area codes.
- **Terms of Use** and **Privacy Policy**—Residents must accept the terms of use and private policy.
- **Share usage patterns**—The selected response does not affect the operation of mobile keys.



If a BlueSky registrant deletes the app, a mobile key must be sent again after the registrant re-installs the app.

Remote Lock Mgmt

This chapter is for the licensed feature online communication.

This section includes the following subjects:

- Introduction 291
- Enable and configure online communication 292

Gateways & Paired Access Points 299

- Manage online device configuration 300
- Registered gateways and paired access points 302

Program Devices 307

- Program devices 308

Notification Management 309

- Learning about Notification Management 310
- Add notification groups 312

Monitoring (RLM) 314

- Learning about Monitoring 315
- View metrics 316
- Monitor online operations 317
- Monitor online events 319
- Monitor access point status 322

Reports (RLM) 323

- Online Access Points Status Report 324
- Online Gateway Status Report 325
- Online Paired Access Point Report 326

Introduction

Deployment of online communication involves configuring gateways to work with the Community Server. Gateways are the network devices which are paired to access points for online communication (to perform remote operations and receive access point events). When a gateway is listed in **Device Management** and the connectivity status is Online, access points can be paired. Multiple gateways can be connected to Community, but an access point can be paired with only one gateway.

After configuration is complete, remote commands can be sent to gateways and paired access points. All command requests and results occur in real-time.

The **Device Management**, **Monitoring**, **Notification Management** and **Reports** modules all provide ways to stay informed about the devices and communication that support online communication.

Enable and configure online communication

To enable online communication:

» Go to **System Settings > Advanced > Enable online communication** and set the soft-switch to **YES**.



After enabling online communication, the **Online Communication** category displays.

For Control 4 devices, the only relevant option is to ensure **Using dormakaba Gateway I devices** is selected.

1. Go to **System Settings > Online Communication**
2. Configure settings in each of the following sections:
   - Online Operations
   - Communication Settings
   - Notifications
   - Rx-Link (if using)
   - INNCOM Communication (if using)
3. Click (Save).

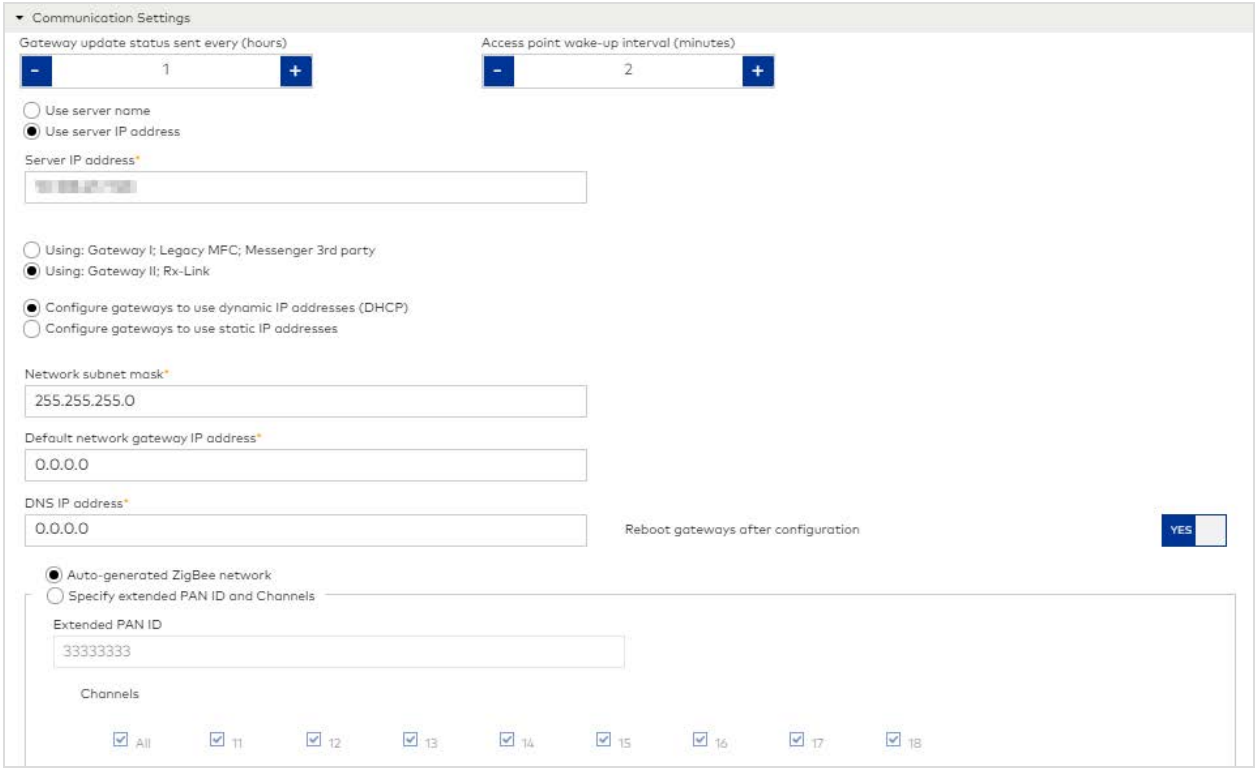
Online operations



- Set **Enable remote resident check-out** to **YES** to enable remote check-out of units, suite units, and meeting rooms in **Resident Management**. Default: YES.
- Specify the number of minutes that resident keys remain valid after changes have been made to a resident assignment and the keys are updated remotely. For example, if you changed the resident assignment for a resident, access to the new unit begins as soon as the keys are updated remotely, but access to the original unit is not canceled until the number of minutes specified as the grace period is reached. Default: 5.
- **Enable remote resident check-out in common areas and elevators**— Set to **YES** to enable remote check-out of resident common areas and elevators in Resident Management. Default: NO. When disabled, access (to common areas/elevators) remains valid until the key expiration date/time.

  Enabling remote resident check-out for resident common areas and elevators may significantly impact the network and online performance.

Communication settings



- **Gateway update status sent every**—Specify the frequency to update gateway status. Valid values: 1-255. Default: 1.
- **Access point wake-up interval**—Specify the frequency at which access points verify if the paired gateway has received remote operation requests. Default: 2.
- Select whether to use a server name or static IP address and specify details. The value that you specify overwrites any value specified for IP Server/Server Name when configuring a gateway in **Device Management**.
- Select the type of devices used in the deployment:
  - **Using: Gateway I; Legacy MFC; Messenger 3rd party**—Select this option is using any of the following:
    - Gateway I devices
    - Legacy MFC elevator controller
    - Messenger 3rd Party (INNCOM, Interel, Telkonet, Control4)
  - **Using: Gateway II; Rx-Link**—Select this option if using any of the following:
    - Gateway II devices
    - Rx-Link

    > The option Using Gateway II; Rx-Link requires using the Zigbee Generation II antenna with minimum firmware version (see the Device Requirements section in the Release Notes) and reprogramming all online access points.

    RAC5-MFC/XT are supported in both modes.

    > Gateway II and RAC5 MFC/XT devices must be configured in **Device Management**.

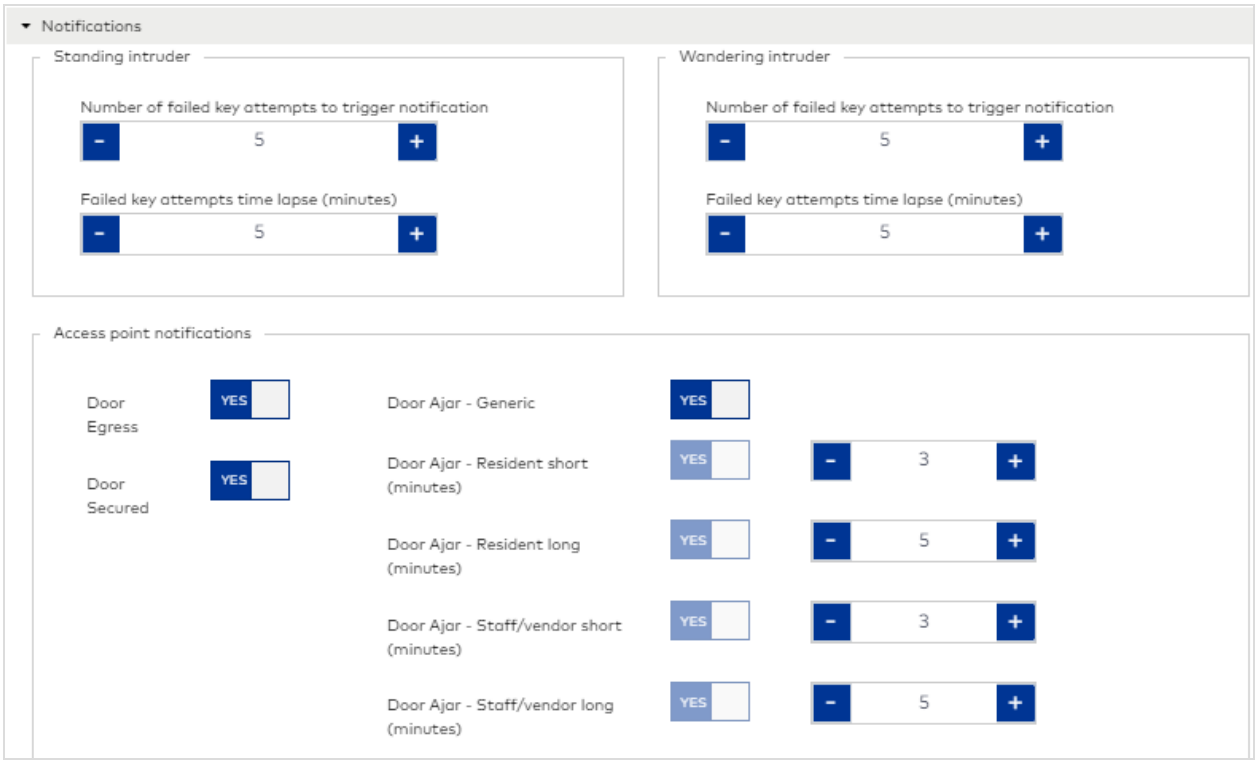
- Configure gateways to use dynamic IP addresses (DHCP) or static IP addresses. If using dynamic IP addresses, gateways resolve their own IP address. A DHCP server is required for this option. If using static IP addresses, each gateway must be configured with a unique IP address.

- Select whether a gateway restarts after the **Set communication settings** command has been sent to the gateway in *Device Management > Gateways & Paired Access Points*.
- Select whether to allow gateways to automatically generate the most appropriate ZigBee communication channels or specify a unique extended PAN (Personal Area Network) ID and select the channels for gateway and access point communication. The extended PAN ID must be eight alphanumeric characters. If the extended PAN ID is set to 0 (zero), the ZigBee network automatically generates an ID. Channels 15, 20, and 25 are recommended for minimal WiFi interference.

dormakaba recommends using the default auto-generated feature to allocate the required channels automatically.

Notifications

Set alerts for potential intruders and access point events.



Potential intruders

This section describes the alerts that you can set for potential intruders. The behavior that alerts the system about a potential intruder is the number of failed key attempts within a specified amount of time. The settings to trigger notification can be set for standing and wandering intruders. A standing intruder is when the failed key attempts occur at the same access point; for example, someone acquired several keys and presents each to the same access point. A potential wandering intruder is when the failed key attempts occur at different access points; for example, someone found a key in the parking lot and walks the hallway presenting the key to each access point.

- Standing intruder
  - **Number of failed key attempts to trigger notification**—Specify how many failed key attempts at the same access point (within the specified time lapse) trigger an intruder alert notification. Default: 5. Valid values: 3-10.
  - **Failed key attempts time lapse**—Specify the number of minutes within which the number of failed key attempts (at the same access point) must occur before a notification is triggered. Default: 5. Valid values: 1-10.
- Wandering intruder
  - **Number of failed key attempts to trigger notification**—Specify how many failed key attempts at different access points (within the specified time lapse) trigger an intruder alert notification. Default: 5. Valid values: 3-10.

- **Failed key attempts time lapse**—Specify the number of minutes within which the number of failed key attempts (at different access points) must occur before a notification is triggered. Default: 5. Valid values: 1-10.

Access point notifications

Select the access point events for which to receive notification:

- **Access Point Event Notification**—Lists access point door parameters which must be set to **YES** to enable access point status notifications.
- **Egress**—Select **YES** to send a notification about an open door event.
- **Door Secured**—Select **YES** to send a notification that a door is locked securely.
- **Door Ajar - Generic**—Select **YES** to send notifications for all Door Ajar events. If NO is selected, enable or disable each Door Ajar event.
- **Door Ajar - Resident short (minutes)**—Select **YES** to send a notification that a door has been left open by a resident for a short period of time (one minute), for example the time it would take to vacate a room. Specify the number of minutes after which the notification is sent.
- **Door Ajar - Resident long (minutes)**—Select **YES** to send a notification that a door has been left open by a resident for a longer period of time (two minutes), indicating an usual state or potential intrusion. Specify the number of minutes after which the notification is sent.
- **Door Ajar - Staff/Vendor short (minutes)**—Select **YES** to send a notification that a door has been left open by a staff member/vendor for a short period of time (one minute), for example the time it would take to vacate a room. Specify the number of minutes after which the notification is sent.
- **Door Ajar - Staff/Vendor long (minutes)**—Select **YES** to send a notification that a door has been left open by a staff member/vendor for a longer period of time (two minutes), indicating an usual state or potential intrusion. Specify the number of minutes after which the notification is sent.



Default time intervals for access point event notifications should be based on practical best practices with security considerations.

Rx-Link



For complete Rx-Link documentation, refer to *CommunityRx-Link Deployment and Support Manual* and *Community Rx-Link Partner Integration Specifications*.

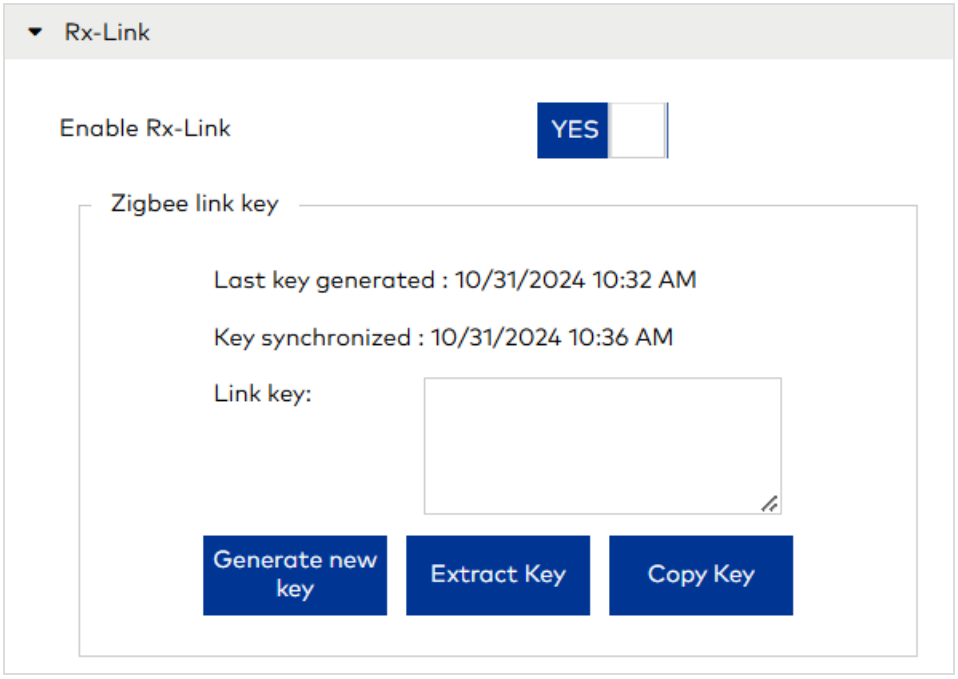
The Rx-Link section displays when the communication setting **Using: Gateway II; RAC5-MFC/XT; Rx-Link** is selected.

Select whether to enable Rx-Link. When enabled, Rx-Link Settings Management in Role Management System Rights is exposed with the default settings that authorize the Administrator and Site Configurator roles.



When you modify this setting (enable or disable) or generate a new third-party Zigbee link key, all access points must be reprogrammed.

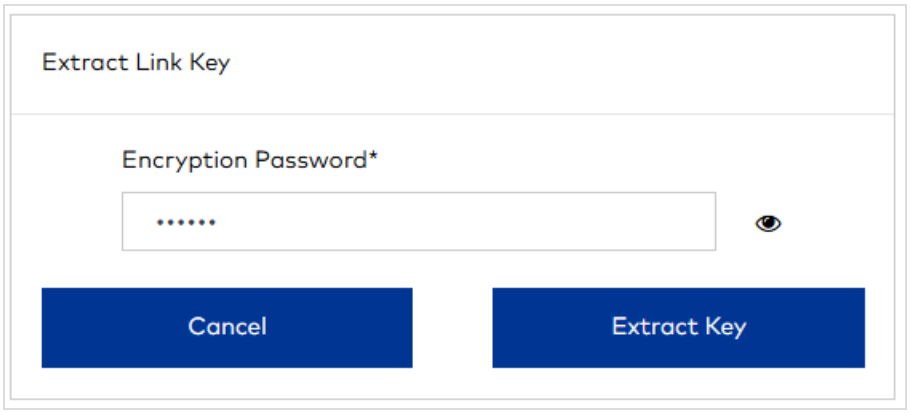
Zigbee link key



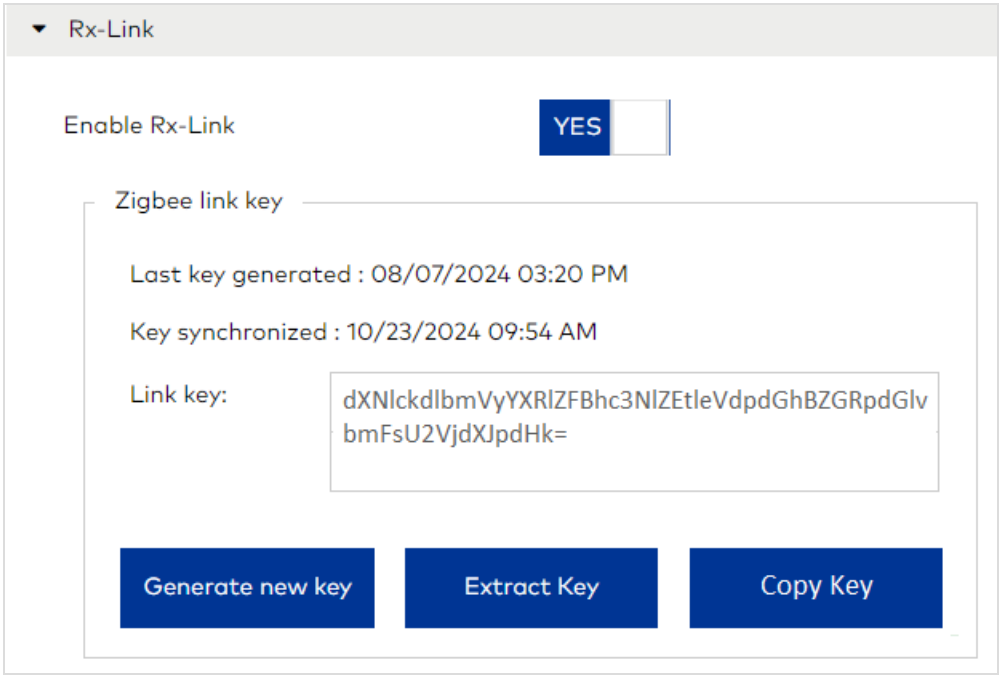
If you enable Rx-Link, Zigbee link key information is displayed (the date/time of the most recent key and when the key was synchronized). Click **Generate new key** to generate the initial or a new link key.

For third parties that require the link key be shared in a readable format, extract the link key:

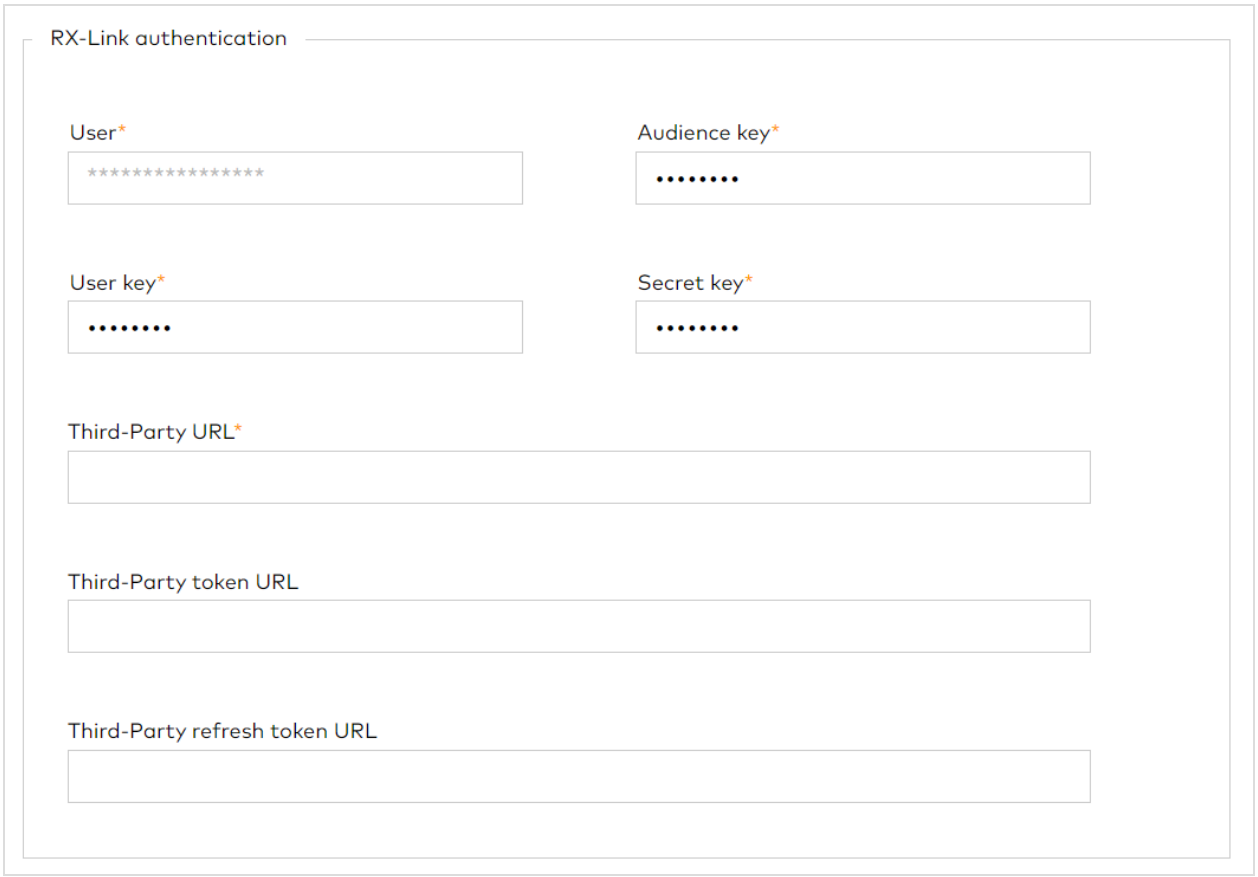
1. Click **Extract Key**.



2. Specify a password for the key. Minimum chars: 6.
3. Click **Extract Key**. The link key displays in a readable format.
4. Click **Copy Key** to copy the Link key value onto the clipboard.



Rx-Link authentication

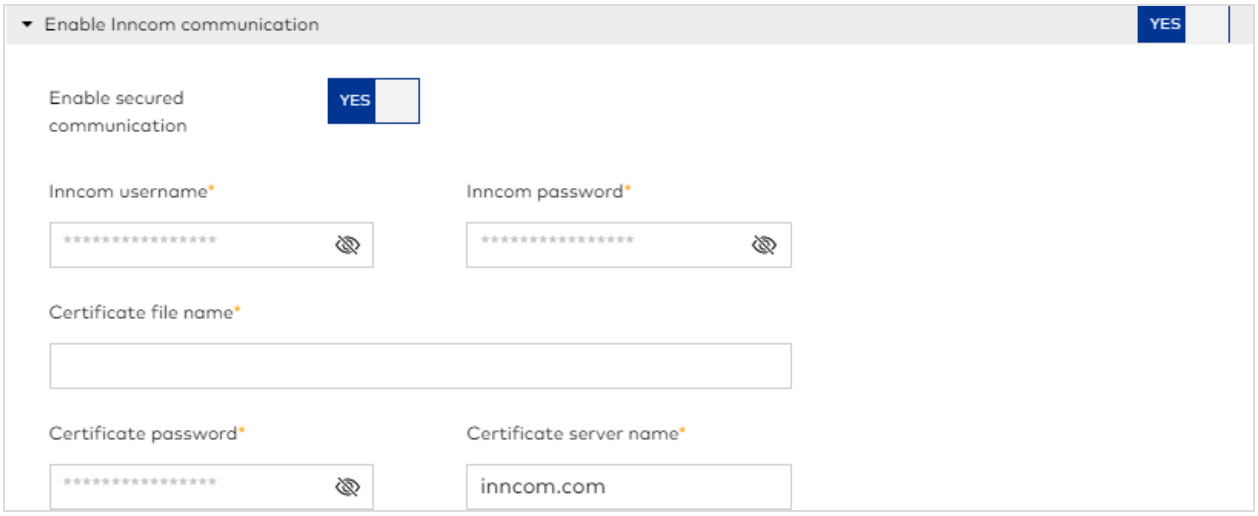


Configure authentication options:

- **User**— The unique ID provided by the third party for authentication to acquire a token. Valid length: 1-2,0 48 characters. Not required when using the WebSocket protocol.
- **User key**—The password provided by the third party that pairs with the User. Valid length: 1-2,048 characters. Not required when using the WebSocket protocol.
- **Audience key**—An API key (paired with the Secret key) that is required by a third-party to acquire an authentication token from the dormakaba server. The token eliminates the need to always submit the User/User key settings with each request. Valid value: 9b55561a54b94e2db01e15f337e902bb
- **Secret key**—A unique API key (paired with the Audience key) that is required by a third party to acquire an authentication token from the dormakaba server. The token eliminates the need to always submit the User/User key settings with each request. Valid length: 1-2,048 characters. Must be 64 bytes in length.
- **Third-Party URL**—Uri of the third-party bridging service to initiate Web requests made by dormakaba to the IoT controller. Represents the endpoint.
- **Third-Party token URL**—Third-party Uri to request a token.
  Example: https://vriot.local-mqtt.video54.local/v1/oauth/login.
- **Third-Party refresh token URL**—The third-party Uri to refresh the token. Example: https://vriot.local-mqtt.video54.local/v1/oauth/refresh.

INNCOM communication

For integrations with INNCOM, select the enable switch to **YES**.



If the option to secure communication is enabled, configure the following options:

- **INNCOM username/password**—Specify INNCOM account credentiails so that Community can connect to the INNCOM server. Value length per setting: 5-25 characters .
- **Certificate file name/password**—Specify the full path to the certificate file name (for example, c:\Program Files\dormakaba\InncomCertificate\Kaba_VHE_Client_cert.pfx) and password on the INNCOM server used to secure communication between Community and INNCOM. Value length: Unlimited (file name), 5-25 characters (password).
- **Certificate server name**—Specify the IP address of the INNCOM server. Value length: 5-25 characters.
  Default: inncom.com.

Gateways

Gateways & Paired Access Points

This section includes the following subjects:

Manage online device configuration 300

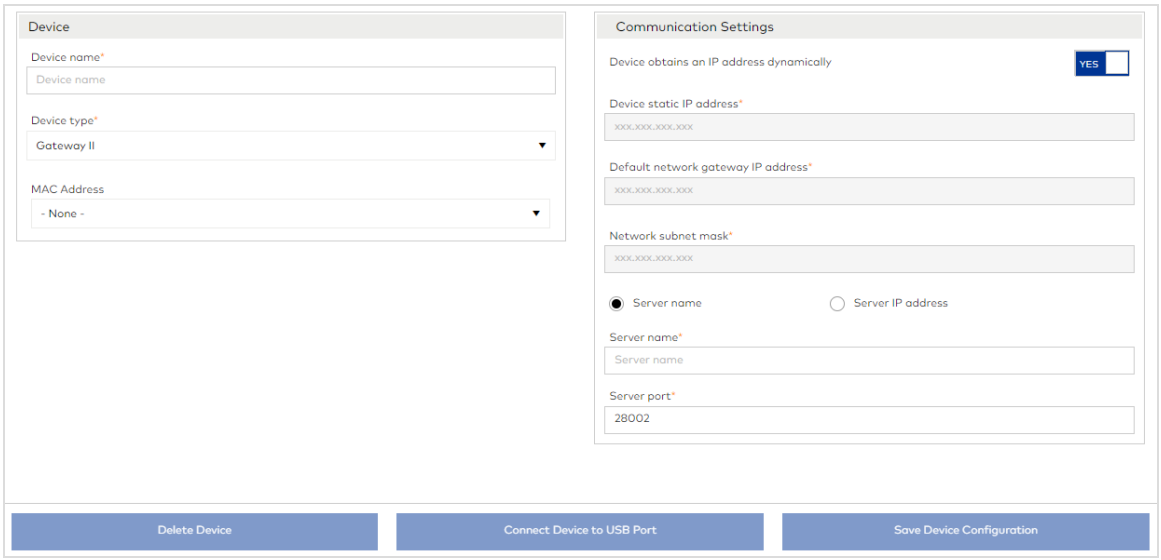
Registered gateways and paired access points 302

Manage online device configuration

You can add, configure and delete devices in the **Device Management** module. All device types can be configured in Device Management. RAC5 MFC/XT devices can also be programmed using the M-Unit (see **Programming /Auditing > Programming**.

Add online devices

1. Go to **Device Management. > Online Device Configuration**.



2. Click **New Device**.
3. Specify a unique name that does not exceed 60 characters. This name displays in the list of devices.
4. Select the device type: Gateway II, RAC5-MFC or RAC5-XT.
5. Select the MAC address of the device that you want to configure. The MAC address of the device is automatically detected when the device is connected to the workstation.
6. Select whether the gateway obtains an IP address automatically. If **NO**, specify a valid static IP address, port number, subnet mask and default network gateway IP address. (The network gateway is not the dormakaba gateway.)
7. Select whether the gateway will contact the Community Server using the IP address or server name. If using the server name, you must also specify the IP address or domain name of the local DNS Server.

The Server IP or Server Name value that you specify must refer to the same server specified in **System Settings > Online Communication** >**Communication Settings**.

8. Specify the port number for the gateway to communicate with the Community Server.
9. Take one of the following actions:
   - When the device is attached to the workstation and the MAC address is populated, click **Configure Device**. The device configuration is saved to the Community database. Wait 20 seconds or Power OFF/ON the gateway device. When the gateway is commissioned, disconnect the device from the USB cable and connect it to the Ethernet (POE or external power supply).
   - When the intent is to save device configuration settings only, click **Save Device Configuration**.

Edit device configuration

1. Select a device.
2. Modify options.
3. Click **Save Device Configuration.**

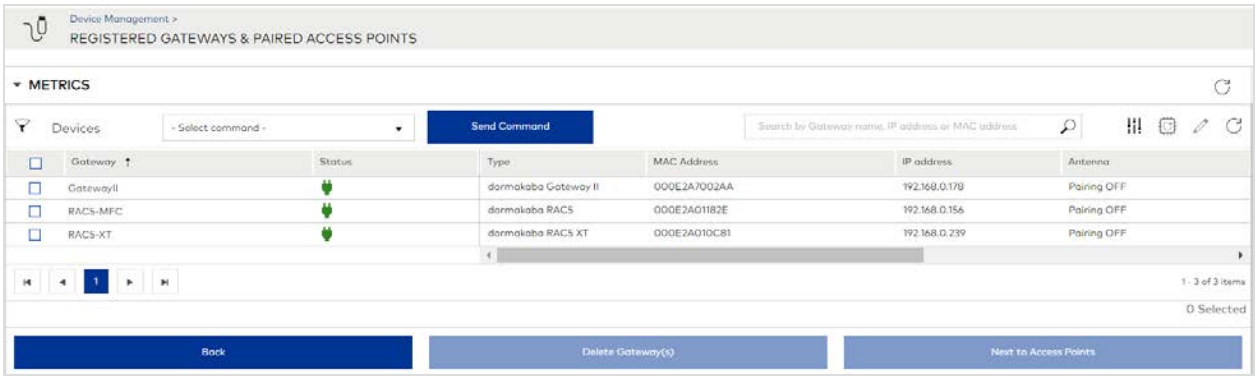
Delete a device

1. Select a device.
2. Click **Delete Device**.
3. Click **YES** to confirm.

Registered gateways and paired access points

To work with gateways (and paired access points) that are connected to the Community Server:

1. Go to **Device Management > Registered Gateways & Paired Access Points**.



Registered gateways

Gateways and their respective status' are listed by name beneath the metrics section. Color codes reflect the gateway state. Green indicates no attention is required. Yellow indicates the situation may require attention. Red indicates the gateway is offline or not working properly.

Use the Gateways toolbar to issued commands, search gateways (by name, IP and MAC address) and take the following actions:

- To filter based on connectivity status, click **(Filter)** and select the status types (Online/Offline) to list.
- To show/hide columns, click and select the information that you want to display. The following columns can be displayed:
  - **All**—Select this option to show all columns.
  - **Type**—The type of gateway.
  - **MAC Address**—Unique MAC address for each device.
  - **IP Address**—Unique Ethernet address for each device. The IP address is dynamic if a DHCP is assigned; otherwise, the IP address is static.
  - **Antenna**—Gateway antenna states (Disabled/Pairing On/Pairing Off).
  - **Last offline**—The date and time the gateway was most recently offline.
  - **Last Communication**—The date and time of the most recent and successful communication with the gateway.
  - **FW Vers. Gateway**—The current firmware version of the gateway device that runs at all times except during a firmware upgrade.
  - **FW Ver AVR**—The firmware version of the AVR (automatic voltage regulator) that runs at all times except during an upgrade of the AVR firmware.
  - **FW Vers Ember**—An electronic component on the RF board that runs at all times.
  - **FW Vers Boot**—The firmware version of the gateway that runs during an upgrade of the Main gateway firmware.
- To refresh the data, click **(Refresh)**.

Edit gateway name

1. Select a gateway.
2. Click **(Edit)**.
3. Modify the name.
4. Click **Save**.

Delete gateway/s

You can only delete gateways that are offline.

1. Select the gateway/s that you want to delete.
2. Click **Delete Gateway(s)**.
3. Click **YES** to confirm.

Issue gateway commands

1. Select one or more gateway/s.
2. Select one of the following commands:
   - **Clear gateway buffer**—Deletes buffer data on all devices connected to the gateway. The buffer is automatically cleared prior to upgrading firmware. (Not supported for C4 devices.)
   - **Deactivate Antenna**—Disables the selected gateway/s from the network and deactivates the gateway antenna. When the command result is successful, the antenna status is Deactivated (in the **Monitoring** module). (Not supported for C4 devices.)
   - **Get Access Point Status**—Requests the connectivity status (Online/Offline) for all paired access points.
   - **Get Gateway Firmware Status**—Requests the gateway firmware version installed on the gateway. (Not supported for C4 devices.)
   - **Get Gateway Status**—Requests the gateway connectivity status (Online/Offline).
   - **Pairing OFF**—Disables Pairing Mode. When the command result is successful, the antenna status is Pairing Off (in the **Monitoring** module). (Not supported for C4 devices.)
   - **Pairing ON**—Enables Pairing Mode. When the command result is successful, the antenna status is Pairing On (in the **Monitoring** module). (Not supported for C4 devices.)

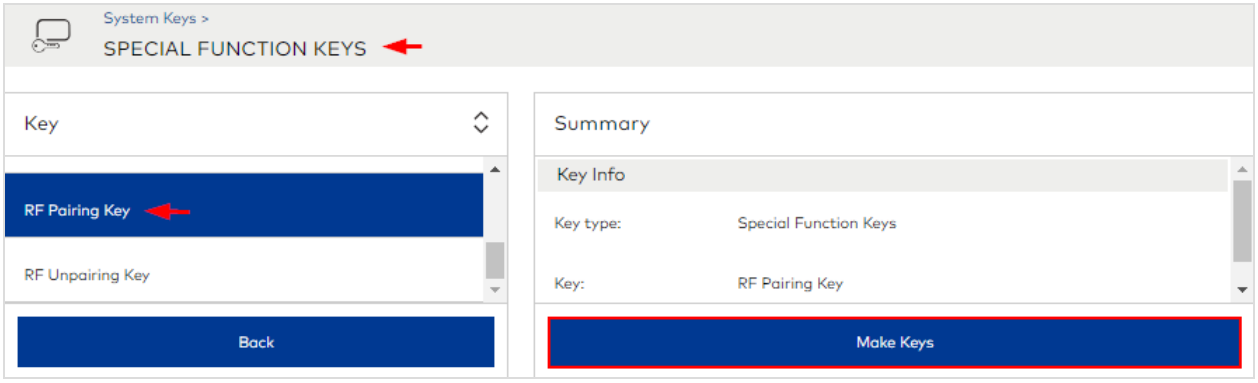
     Important! To eliminate the risk of binding access points to the wrong gateway, dormakaba strongly recommends that only one gateway be in Pairing Mode at a time. After all access points are paired to a gateway, send the Pairing OFF command to the gateway to disable Pairing Mode. As a precaution, Pairing ON mode changes to Pairing OFF after 15 minutes.

   - **Reset Gateway**—Performs a soft reset on the selected gateway/s. (Not supported for C4 devices.)
   - **Set Clock and Lock Event Mask**—Sends the server time and the access point event notification settings (defined in **System Settings > Online Communication > Notifications**).
   - **Set Communications Settings**—Sends the communication configuration settings (defined in **System Settings > Online Communication > Online Communication Settings > Gateway update status**, **Access point wake-up**, **Gateway update status**).
   - **Unpair all Access Points**—Unpairs all access points. (Not supported for C4 devices.)
   - **Upgrade firmware**—Update the system-level software installed in the gateway. Prior to the upgrade, you must obtain the required file from dormakaba Support. This command applies to Gateway II devices only. (Not supported for C4 devices.)
   - **Verify Assignment**—Requests connectivity status from paired access points.
3. Click **Send Command**.
4. When notified the command is sent, click **OK**.

Pair Access Points

Before you can pair access points, you must make an RF Pairing Key in **System Keys**.

Make RF pairing key



1. Go to **System Keys**.
2. Click **Special Function Keys**.
3. Select **RF Pairing Key**.
4. Click **Make Keys**.
5. Select an encoder that is online, present a key to the encoder, then click **Start**.
6. When prompted that the key was made successfully, click **Done**.

Pair access points

For Control 4 devices, skip directly to step 6.

1. Go to **Device Management > Registered Gateways & Paired Access Point**.
2. Select the gateway where you want to pair access points.
3. Select the command **Pairing ON** (to activate the gateway antenna and put the gateway in Pairing Mode).
4. Click **Send Command**.
5. When notified the command is sent, click **OK**.
6. Present the RF Pairing Key to every access point that you want to pair to the gateway.

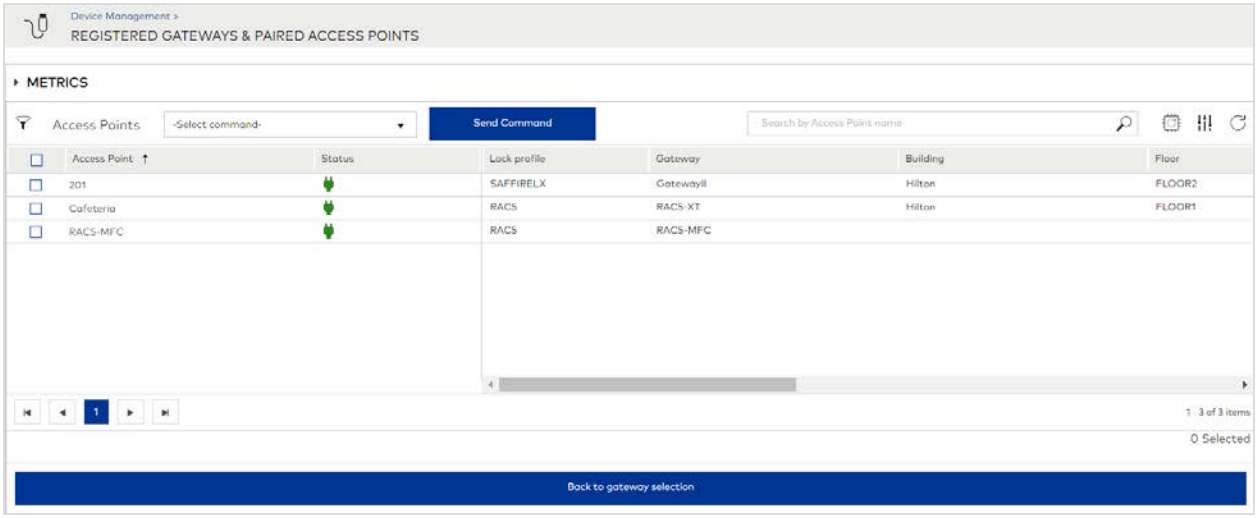
To eliminate the risk of binding access points to the wrong gateway, dormakaba strongly recommends that only one gateway be in Pairing Mode at a time. After all access points are paired to a gateway, send the **Pairing OFF** command to the gateway to disable Pairing Mode. As a precaution, **Pairing ON** is automatically changed to **Pairing OFF** after 15 minutes.

7. In Community, select the gateway that is in **Pairing On** mode.
8. Select the command **Pairing OFF** (to deactivate the antenna and disable Pairing Mode).
9. Click **Send Command**.
10. When notified the command is sent, click **OK**.

Paired access points

To view the access points that are paired to a gateway:

1. Go to **Device Management > Registered Gateways & Paired Access Points**.
2. Select the gateway where the access point/s are paired.
3. Click **Next to access points**.



The access points that are paired with the selected gateway and their respective status' are listed by name.

For RAC5 XT devices, you must trigger an event before the access point displays in the list. The simplest way to trigger an event is to present any key (valid or invalid) to the lock.

Use the Access Points toolbar to issue commands, search access points (by name) and take the following actions:

- Issue one of the following commands:
  - **Get Access Point Firmware Status**—Requests the current lock firmware version. (Not supported for Control 4 devices.)
  - **Get Access Point Status**—Gateway requests a full update to access point status.
  - **Set UTC Offset and Lock Event Mask**—Sends the server time and the access point event notification settings (defined in **System Settings > Online Communication > Notifications**).
  - **Unpair Access Point**—Unbind the access point from the gateway. This command is useful during gateway maintenance, when you need to pair an access point to a different gateway. (Not supported for Control 4 devices.)

    If you want to associate an existing access point with a new room, you need to unpair and delete (or just delete) the existing access point on the Online Access Points page. Then, the "new" access point must be reprogrammed and paired to the gateway.

  - **Upgrade firmware**—Request firmware upgrade. (Not supported for Control 4 devices.)
  - **Verify Assignment**—Requests the gateway where access points are paired and the connectivity status.
- To filter based on connectivity status, click **(Filter)** and select the connectivity status (Online/Offline) as well as the monitored states (Low Battery/Door Open/Door Ajar/PrivacyEnabled/Unlatched) to list.
- To show/hide columns, click and select the information that you want to display. The following columns can be displayed:
  - **All**—Select this option to show all columns.
  - **Lock profile**—The lock model installed at the access point.
  - **Gateway**—The gateway to which the access point is paired.
  - **Building**—The building where the access point is located.
  - **Floor**—The building level where the access point is located.
  - **Low Battery**—Indicates whether the lock battery is low (TRUE=YES/FALSE=NO). You can filter the list to show access points with a low battery.
  - **RF signal**—Indicates whether the signal between the gateway and paired access point is weak or normal.
  - **Last offline**—The date and time the gateway was most recently offline.
  - **Last communication**—The date and time of the most recent and successful communication with the gateway.

- **Door Open**—Indicates whether the door is open. You can filter the list to show access points with an open door.
- **Door Ajar**—Indicates whether the door has been open beyond a predefined threshold. You can filter the list to show access points with a door ajar.
- **Door Ajar by**—Indicates the key type that was presented to open the door that is now in Door Ajar status.
- **Door Ajar Since**—Indicates the date and time the door became considered ajar (not open).
- **Privacy Enabled**—Indicates whether the deadbolt or privacy switch is engaged at the access point. You can filter the list to show access points with privacy enabled.
- **Unlatched**—Indicates if the access point is currently in Unlatched Mode (allowing unlimited access without a key). You can filter the list to show access points that are unlatched.
- **Last Entry**—The date and time of the most recent entry to the access point.
- **Date/Time Error**—Indicates whether the date and time require synchronizing.
- **FW Vers. Lock (Main)—**The current firmware version of the lock that runs at all times except during a firmware upgrade.
- **FW Vers. Lock (Boot)—**The current firmware version of the lock that runs during a firmware upgrade.
- **FW Vers. AVR (Main)—**The firmware version of the AVR (automatic voltage regulator) that runs at all times except during an upgrade of the AVR firmware.
- **FW Vers. AVR (Boot)—**The firmware version of the AVR (automatic voltage regulator) that runs during an upgrade of the AVR firmware.
- **FW Vers. Ember—**An electronic component on the RF board that runs at all times.
- **FW Vers. Quantum**—ZigBee RF board firmware version.

- To refresh the data, click **(Refresh)** .

Program Devices

This section includes the following subjects:

Program devices 308

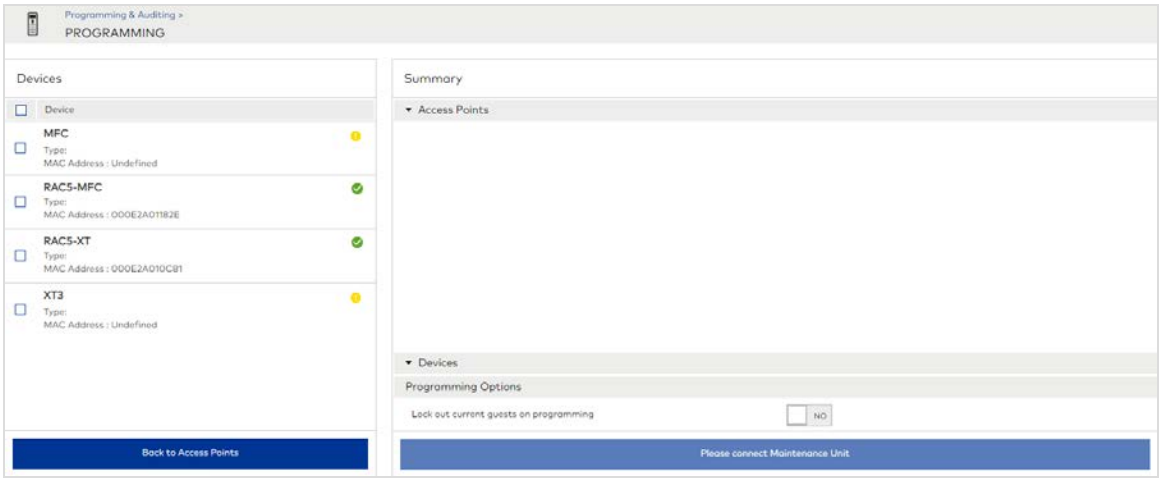
Program devices

RAC5-MFC/XT devices can be programmed using the M-Unit. Gateway II devices are configured/programmed in **Device Management > Online Device Configuration**. A device must be reprogrammed any time configuration data affecting the device is modified in Community.

Some programming steps are performed on the M-Unit (Maintenance Unit). For official instructions, refer to the documentation distributed with your device. If M-Unit authentication is enabled in **System Settings > Security > M-Unit** credentials must be configured for at least one Operator in **Staff/Vendor Management**.

To program devices:

1. Go to **Programming & Auditing > Programming** .
2. Click **Next to Devices.**



3. Select the devices that you want to synchronize with Community configuration data. The selected items display in the **Summary** section.
4. Connect the M-Unit to the workstation.
5. In Community , click **Transfer**. Messages on the workstation and M-Unit display that the transfer is in progress. Wait until the message on the workstation indicates transfer is complete and that you can unplug the M-Unit.
6. Click **OK**.
7. Disconnect the M-Unit from the workstation.
8. On the M-Unit menu, select **TOOLS / Next Page / Configure RAC5**. Device names display in groups of five. Use the **PREV**, **NEXT** and **SEARCH** options to navigate and refine the list of names. Use the UP and DOWN arrow keys to make a selection.
9. Select the device name, then press **ENTER**.
10. Select the type of cable (probe) that you are using to connect the M-Unit to the device.
11. When prompted, connect the cable to the device. Programming starts immediately. If the device has already been programmed, the M-Unit issues a message requesting confirmation to overwrite the existing programming.
12. When prompted that programming is complete, click **OK**.

Notifications

Notification Management

This section includes the following subjects:

Learning about Notification Management 310

Add notification groups 312

Learning about Notification Management

Notifications, conveniently accessible from the main Community toolbar, keep staff members informed about online operations and events as well as the status of online access points. For example, a notification lets you know when a resident key is used or a door is ajar. The **Notification Management** module is where different types of notifications can be grouped and subsequently selected for subscription in staff/vendor profiles in **Staff/Vendor Management**.

The following online notifications are available:

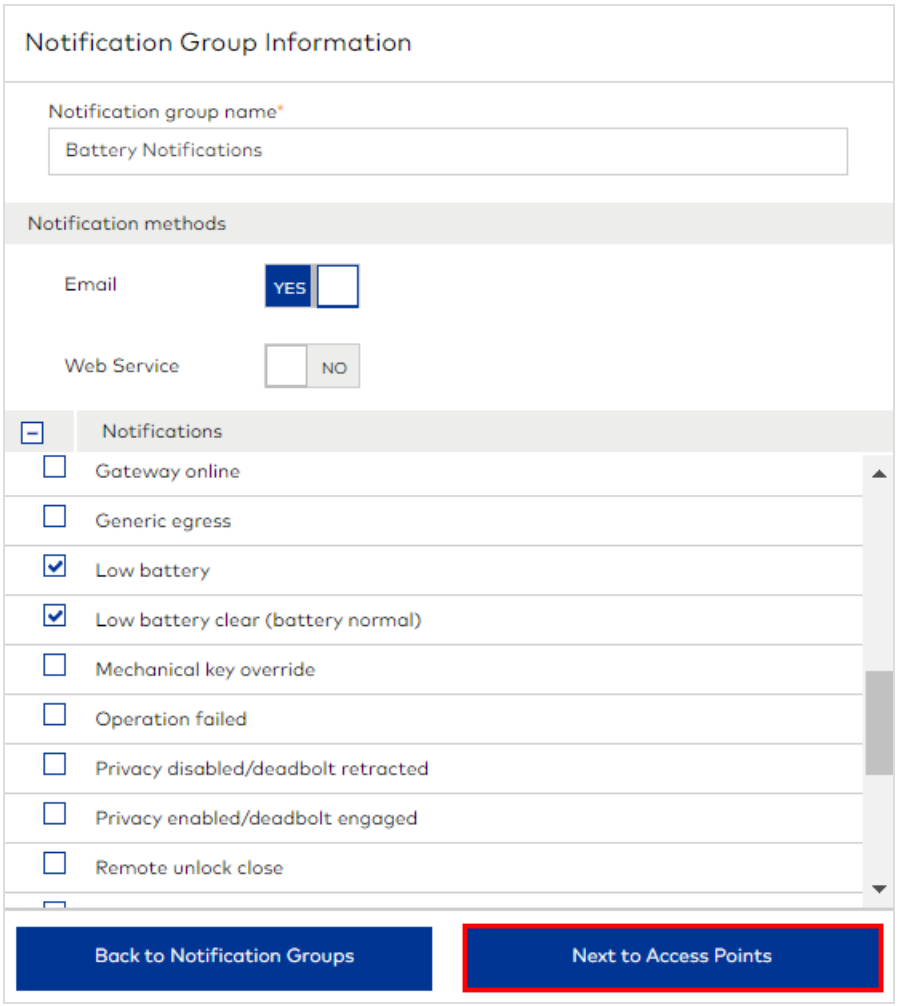
- **Access point offline**—Notifies that there is no communication between the lock and the gateway.
- **Access point online**—Notifies that the lock is in communication with the gateway and online.
- **Door ajar clear (door secure)**—Door previously ajar has now been closed and is secure.
- **Door ajar generic**—Notifies that a door is in an open state.
- **Door ajar resident long**—Door ajar beyond the configured threshold. The door ajar (long) event notifies a door has been left open for a longer time interval (two minutes), indicating an unusual state, a potential intrusion.
- **Door ajar resident short**—Notifies that a door ajar (short) event signaling a door has been left open for a short time interval (one minute), for example the time it would take to vacate a room.
- **Door ajar staff/vendor long**—Door ajar beyond the configured threshold. The door ajar (long) event notifies a door has been left open for a longer time interval (two minutes), indicating an unusual state, a potential intrusion.
- **Door ajar staff/vendor short**—Notifies that a door ajar (short) event signaling a door has been left open for a short time interval (one minute), for example the time it would take to vacate a room.
- **Door latched**—Notifies that a door is closed with the lock engaged.
- **Door open**—Notifies when the lock's anti-pick mechanism is out. This is the default state of the door.
- **Door unlatched**—Notifies that the lock motor has been disengaged and the door can be opened without a key.
- **Fire alarm activated**—RAC5 MFC/XT notification only. An event that notifies when the fire alarm for the access point is activated.
- **Fire alarm deactivated**—RAC5 MFC/XT notification only. An event that notifies when the fire alarm for the access point is deactivated.
- **Gateway error code updated**—Notifies that an error code was issued for a gateway. The update my indicate that the gateway is in a good state (error code=0) or that an error has occurred.
- **Gateway offline**—Notifies that a gateway is currently not communicating with the Community Server.
- **Gateway online**—Notifies that a gateway is communicating with the Community Server.
- **Generic egress**—Notifies that a door open event occurred.
- **Resident key used**—Notifies that a resident key was presented to a lock. Details include the date/time that the key was presented.
- **Resident key used (first entry)**—Notifies a resident key was presented to a lock for the first time.
- **Low battery**—Notifies that the battery state is low and requires replacement. Community sends a single low battery event/notification until batteries are changed. After batteries are changed, Community sends a **Low battery clear (battery normal)** event/notification.
- **Low battery clear (battery normal)**—Notifies that the low battery status is cleared. The battery was replaced or the problem resolved.
- **Mechanical key override**—Notifies a lock override, accessing a lock with a mechanical key.
- **Operation failed**—Notifies the specified operation was unsuccessful. When available, the reason is indicated.
- **Privacy disabled/deadbolt retracted**—Notifies the status of the deadbolt as disengaged.
- **Privacy enabled/deadbolt engaged**—Notifies that the deadbolt or privacy switch is engaged.
- **Remote lock**—Command was issued from the toolbar to remotely lock the selected access point.
- **Remote unlock**—Command was issued from the toolbar to remotely unlock the selected access point.
- **Staff/vendor key used**—Notifies that a Staff/Vendor key accessed a lock.
- **Standing intruder**—Alert: Possible standing intruder. Multiple keys presented at a single access point.
- **System key used**—Notifies that a System key was presented to a lock.
- **Wandering intruder**—Alert: Possible wandering intruder. Key presented at multiple access points.

Email and web service notifications are deleted from the Community database after they are successfully sent.

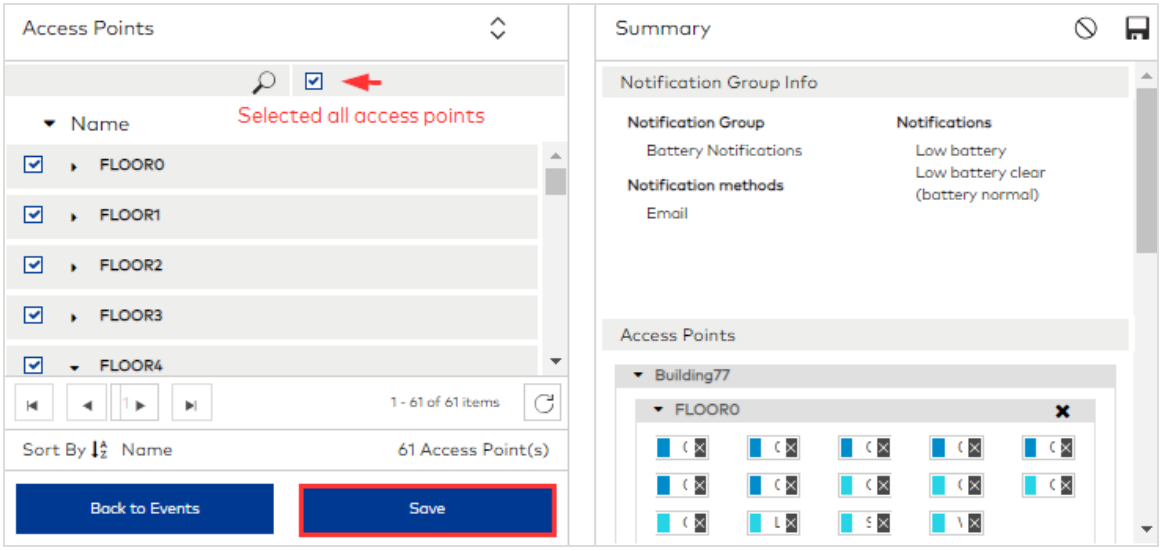
Add notification groups

To add notification groups:

1. Go to **Notification Management**.

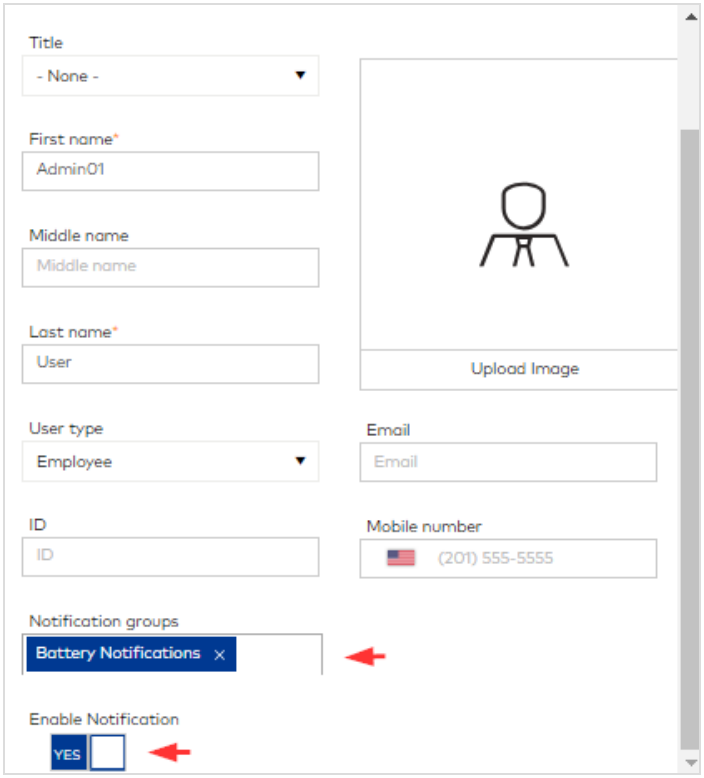


2. Click **New Notification Group**.
3. Specify a descriptive name for the group.
4. Select from available notification methods. If you do not select a method, only Operators who have the rights to view notifications will see notifications upon logging in to Community.
   - **Email**—Send notifications by email. Recommended value: YES. Requires email configuration in **System Settings > Email** and an email address defined in staff/vendor profiles in **Staff/Vendor Management**.
   - **Web Service**—Send notifications through the Web Service using either the SOAP or REST protocol. You must also specify the Web Service URL.
5. Select the events that you want to include in the notification group. You can select from the **General** and **Online** lists. To include all notifications, select the check box adjacent to **Notifications**.
6. Click **Next to Access Points**.



7. Select the access points for which you want to receive notifications.
8. Click **Save**.

Subscriptions to one or more notification groups can be selected in staff/vendor profiles in **Staff/Vendor Management**.



Monitor (RLM)

Monitoring (RLM)

This section includes the following subjects:

Learning about Monitoring 315
View metrics 316
Monitor online operations 317
Monitor online events 319
Monitor access point status 322

Learning about Monitoring

The **Monitoring** module provides information about all keys made in Community . If you need to know the most recent time that a specific key was used and by whom, the data is readily available without generating a report.

The Monitoring module is also where you can stay informed about online communication. The Metrics section provides a real-time snapshot of the gateways and access points on site. For example, you can see at a glance whether any locks have a low battery, if any doors are open, and how many access points have the deadbolt or privacy switch enabled. Beneath the metrics summary, detailed listings show remote lock operations and events and the status of all access points paired with gateways.

Access to data in the **Monitoring** module is configured in **Role Management**. By default, the Administrator and Site Configurator roles have full access.



When the licensed feature mobile keys is enabled, the Digital Keys Usage tab displays to control and track the number of digital keys (mobile and wallet keys) available/consumed.

View metrics

To view metrics:

In **Monitoring**:

» Metrics display by default.

In **Device Management**:

» Go to **Device Management > Registered Gateways & Paired Access Points**.



The **Metrics** section is expanded for view by default. Color codes reflect the state of the data. Green indicates no attention is required. Yellow indicates the situation may require attention.

- **ONLINE GATEWAYS**—Percentage and total number of gateways currently online.
- **ONLINE ACCESS POINTS**—Percentage and total number of access points currently online.
- **LOW BATTERY**—Percentage and number of access points with a low battery. Zero percent indicates no access points signal a low battery.
- **WEAK RF SIGNAL**—Indicates whether the signal between the gateway and paired access point is weak or normal.
- **AJAR DOORS**—Percentage and number of access points with an open door.
- **PRIVACY ENABLED**—Percentage and number of access points with the deadbolt or privacy switch engaged.
- **DOORS UNLATCHED**—Percentage and number of access points with doors that are closed yet there is unlimited access without a key. Zero percent indicates no doors are unlatched, which means a key is required for entry.

At any time, you can expand or collapse the section.

Color codes reflect the state of the data. Green indicates no attention is required. Yellow indicates the situation may require attention.

Monitor online operations

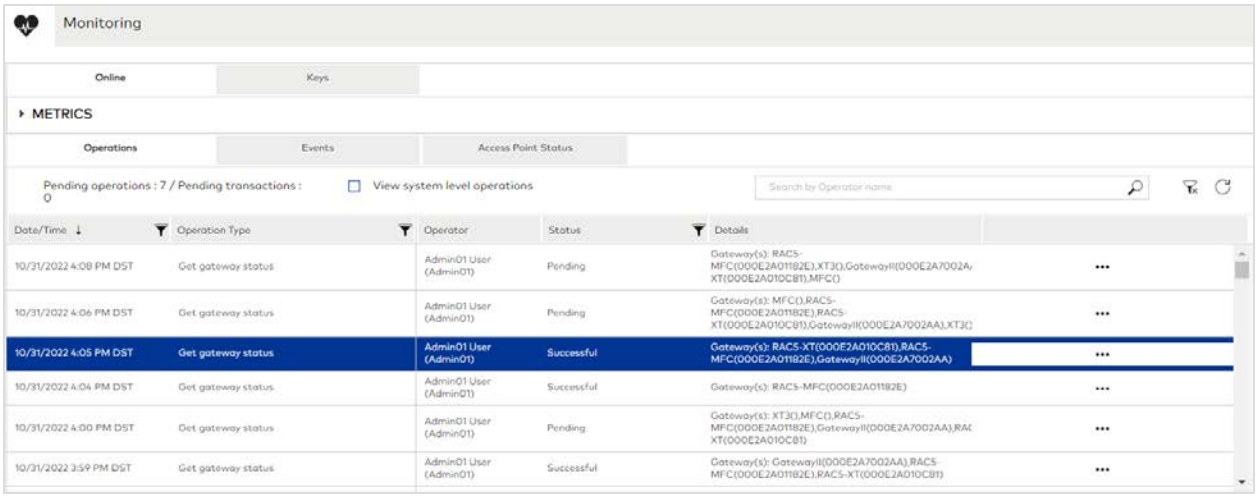
The Operations tab beneath the Metrics section lists the commands and related details sent to gateways and paired access points. Commands are issued from **Device Management > Registered Gateways & Paired Access Points**. Transaction details are reported for each operation.

View operations

To monitor online operations:

» Go to **Monitoring**. Operations are displayed beneath the **Metrics** section.

Collapse the **Metrics** section to show only the list of operations.



The following information is reported for each operation:

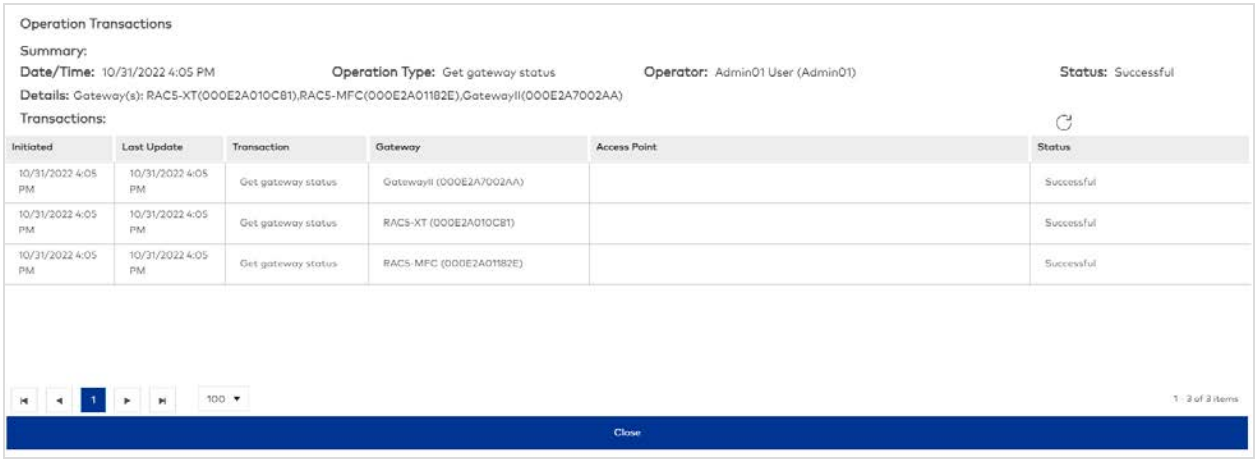
- **Date/Time**—The date and time when the operation occurred. You can filter the list based on date and time.
- **Operation Type**—Command sent to gateways and access points (for example, Pairing Off/On/Set Clock/Lock Event Mask). You can filter the list based on operation type.
- **Operator**—The full name of the Operator who was logged in when the operation occurred. You can search for commands that were sent when a specific Operator was logged in.
- **Status**—Command result (for example, Failed/Successful/Pending/Partially Successful). If the status is Failed, a reason is provided. You can filter the list based on status.
- **Details**—More information about the operation.

Customize the display

- To filter data, click **(Filter)** in the column heading row, select the information that you want to display, then click **Filter**. The **(Filter Applied)** icon indicates that a filter is applied to the column.
- To clear filters for a column, click **(Filter Applied)** > **Clear**.
- To clear all filters, click **(Remove Filters)**.
- Click any column to sort the list.
- To refresh data, click **(Refresh)**.

View Transaction Details

» Select an operation and click **(More)** ▪▪▪.



In addition to the information in the Operations list, the following transaction details are displayed:

- **Initiated**—The date and time the command was issued.
- **Last Update**—The date and time the status was updated (either a response or timeout).
- **Transaction**—The type of transaction (for example, Key update/ADD KEY/BLOCK KEY/PAIRING ON/PAIRING OFF).
- **Gateway**—The gateway name and MAC address.
- **Access Point**—If the transaction involves an access point, the access point name; otherwise, the field is blank.
- **Status**—Command result (for example, Failed/Successful/Pending/Partially Successful). If the status is Failed, a reason is provided.

Customize the Display

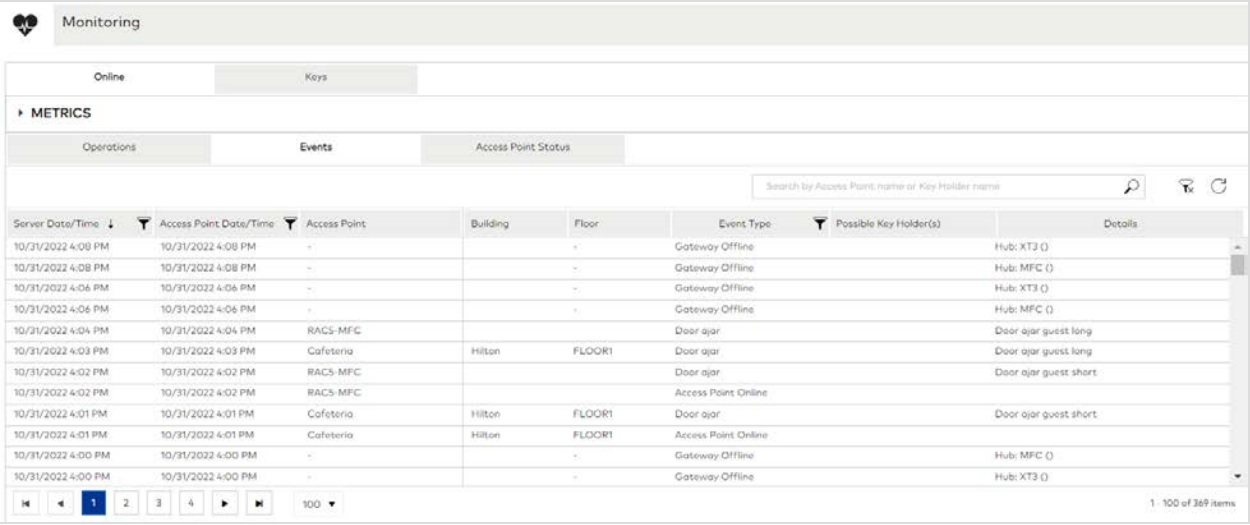
- Click any column to sort the list. When done, click **Close**.

Monitor online events

Events related to gateways and paired access points are listed. The list includes events for all key types (resident/staff/vendor/system keys) and changes to gateway/access point status.

To monitor events:

1. Go to **Monitoring**.
2. Beneath the **Metrics** section, click the **Events** tab.



The following information is reported for each event:

- **Server Date/Time**—Date and time when access point events are received by the server. You can sort and filter the list based on date and time.
- **Access Point Date/Time**—Date and time when the event occurred in the access point. You can filter the list based on date and time.
- **Access Point**—The name of the access point. You can search for events that occurred for a specific access point.
- **Building**—The building where the access point is located. This column only displays when multiple buildings are defined.
- **Floor**—The building floor on which the access point is located.
- **Event Type**—The type of event or type of key used (for example, Door Ajar or System Key Used). You can filter the list based on event type.
- **Key Holder**—The name of the key holder. Defaults: Resident1 (for residents) and Unassigned (for staff/vendor or system keys). You can search for events based on the key holder name.
- **Possible Key Holder(s)**—The name of one possible key holder. Defaults: Resident1 (for residents) and Unassigned (for staff or system keys). You can search for events based on the key holder name. In cases where a key ID is reused, the key holder may be one of multiple.
- **Details**—More information about the event (for example, Door Ajar / Short ajar - Resident). For all key types, details include the type of key, the credential class and the credential. For and keys, details include whether access was allowed or denied.

Customize the display

- To filter data, **(Filter)** in the column heading row, select the information that you want to display, then click Filter. The **(Filter Applied)** icon indicates that a filter is applied to the column.
- To clear filters for a column, click **(Filter Applied)** then **Clear**.
- To clear all filters, click **(Remove Filters)**.

- Click any column to sort the list.
- To refresh data, click **(Refresh)** .

Events

The following events are reported:

- **Access point offline**—Occurs when there is no communication between the lock and the gateway.
- **Access point online**—Occurs when the lock is in communication with the gateway and online.
- **Door ajar clear (door secure)**—Occurs when a door previously ajar is closed and secure.
- **Door ajar generic**—Occurs when a door is in an open state.
- **Door ajar resident long**—Occurs when a door ajar extends beyond the configured threshold. The door ajar (long) event occurs when a door has been left open for a longer time interval (two minutes), indicating an unusual state, a potential intrusion.
- **Door ajar resident short**—Occurs when a door has been left open for a short time interval (one minute), for example the time it would take to vacate a room.
- **Door ajar staff/vendor long**—Occurs when a door ajar extends beyond the configured threshold. The door ajar (long) event occurs when a door has been left open for a longer time interval (two minutes), indicating an unusual state, a potential intrusion.
- **Door ajar staff/vendor short**—Occurs when a door has been left open for a short time interval (one minute), for example the time it would take to vacate a room.
- **Door latched**—Occurs when a door is closed with the lock engaged.
- **Door open**—Occurs when the lock's anti-pick mechanism is out. This is the default state of the door.
- **Door unlatched**—Occurs when the lock motor has been disengaged and the door can be opened without a key.
- **Fire alarm activated**—RAC5 MFC/XT event only. Occurs when the fire alarm for the access point is activated.
- **Fire alarm deactivated**—RAC5 MFC/XT event only. Occurs when the fire alarm for the access point is deactivated.
- **Gateway Error Code Updated**—Occurs when an error code for a gateway is issued. The update my indicate that the gateway is in a good state (error code=0) or that an error has occurred.
- **Gateway offline**—Occurs when a gateway moves into the Offline state. The gateway is not communicating with the Community server.
- **Gateway online**—Occurs when a gateway moves into the Online state. The gateway is communicating with the Community server.
- **Generic egress**—Occurs when a door opens.
- **Resident key used**—Occurs when a resident key is presented to an access point. Details include the date/time that the resident key was presented to the lock.
- **Resident key used (first entry)**—Occurs when a resident has accessed the lock for the first time.
- **Low battery**—Occurs when the battery moves into the Low battery state. The battery requires replacement. Community sends a single low battery event/notification until batteries are changed. After batteries are changed, Community sends a **Low battery clear (battery normal)** event/notification.
- **Low battery clear (battery normal)**—Occurs when the Low battery state is cleared. The battery was replaced or the problem was resolved.
- **Mechanical key override**—Occurs when a lock is accessed with a mechanical key (a lock override).
- **Operation failed**—Occurs when an operation is unsuccessful. When available, the reason is indicated.
- **Privacy disabled/deadbolt retracted**—Occurs when the privacy switch or deadbolt moves into the disengaged state.
- **Privacy enabled/deadbolt engaged**—Occurs when the privacy switch or deadbolt moves into the engaged state.
- **Remote lock**—Command was issued from the toolbar to remotely lock the selected access point.
- **Remote unlock**—Command was issued from the toolbar to remotely unlock the selected access point.
- **Staff/Vendor key used**—Occurs when a Staff/Vendor key accesses a lock.
- **Standing intruder**—Alert: Possible standing intruder. Multiple keys presented at a single access point.
- **System key used**—Occurs when a System key is presented to a lock.

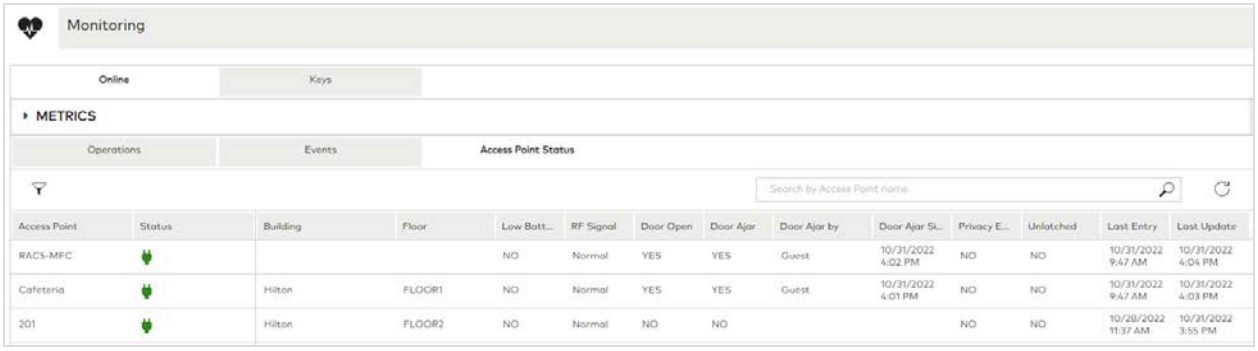
- **VIP Access**—Occurs when a VIP key is presented to a lock. Details may include: VIP access granted, VIP access denied, Access denied (unknown VIP key), or VIP token not in lock.
- **VIP First Access**—Occurs when a VIP key is first presented to a lock.
- **Wandering intruder**—Alert: Possible wandering intruder. Key presented at multiple access points.

Monitor access point status

The **Access Point Status** tab beneath the **Metrics** section lists the status of paired access points.

To view the status about paired access points:

1. Go to **Monitoring**.
2. Beneath the **Metrics** section, click the **Access Point Status** tab.



The following information is reported for each access point:

- **Access Point**—Access point name. You can search the list for a specific access point.
- **Status**—The status icon indicates the access point connectivity status (green=Online/red=Offline). You can filter the list based on connectivity status.
- **Building**—The building where the access point is located.
- **Floor**—The building floor where the access point is located.
- **Low Battery**—Indicates whether the lock battery is low (TRUE=YES/FALSE=NO). You can filter the list to show access points with a low battery. Community sends a single low battery event/notification until batteries are changed. After batteries are changed, Community sends a **Low battery clear (battery normal)** event/notification.
- **RF Signal**—Indicates whether the signal between the gateway and paired access point is weak or normal.
- **Door Open**—Indicates whether the door is open. You can filter the list to show access points with an open door.
- **Door Ajar**—Indicates whether the door has been open beyond a predefined threshold. You can filter the list to show access points with a door ajar.
- **Door Ajar by**—Displays when Door Ajar event occurs. Indicates the key type that was presented to open the door that is now in Door Ajar status.
- **Door Ajar Since**—Displays when Door Ajar event occurs. Indicates the date and time the door became considered ajar (not open).
- **Privacy Enabled**—Indicates whether the deadbolt or privacy switch is engaged at the access point. You can filter the list to show access points with privacy enabled.
- **Unlatched**—Indicates if the access point is currently in Unlatched Mode (allowing unlimited access without a key). You can filter the list to show access points that are unlatched.
- **Last Entry**—The date and time of the most recent entry to the access point.
- **Last Update**—The current lock firmware version.

Customize the display

- To filter data, click **(Filter)** and select the information that you want to display.
- Click any column to sort the list.
- To refresh data, click **(Refresh)**.

Reports (RLM)

Reports (RLM)

This section includes the following subjects:

Online Access Points Status Report 324

Online Gateway Status Report 325

Online Paired Access Point Report 326

Online Access Points Status Report

Generate this report to display Online Access Points Status.

Generate report

1. Go to **Reports > Online Access Points Status Report**.
2. Select whether to include online and/or offline gateways.
3. Select the status options to include in the report: All/Low Battery/Door Open/Door Ajar/Privacy Enabled/Unlatched.
4. Select whether to display firmware versions.
5. Click **Generate**.

View report details

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

The report shows the following details for all current online gateways and access point status.

- Access Point
- Building
- Floor
- Status
- Low Battery
- Door Open
- Door Ajar
- Privacy Enabled
- Lock Latched
- Last Entry
- Last Update
- FW Vers Locks
- FW Vers AVR
- FW Vers Ember
- FW Vers Quantum

Online Gateway Status Report

Generate this report to view gateway status information.

Generate report

1. Go to **Reports > Online Gateway Status Report**.
2. Select whether to include online and/or offline gateways.
3. Select whether to include relevant firmware versions.
4. Click **Generate**.

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Communication Status
- Display Firmware Version
- Site
- Report generated be
- Report generated on
- Gateway
- Type
- Mac Address
- Status (Online/Offline)
- Antenna
- Last Update
- FW Vers Gateway
- FW Vers AVR
- FW Vers Ember

Online Paired Access Point Report

Generate this report to display which access points are currently paired to gateways.

Generate report

1. Go to **Reports > Online Paired Access Point Report**.
2. Select whether to include offline access points.
3. Click **Generate**.

View report details

The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Gateway (Name)
- Paired Access Points
- Unpaired Access Points

Troubleshooting

This section includes the following subjects:

Services Manager 328
Troubleshooting encoders 332
Troubleshooting locks 336
Log data 342

Services Manager

The Services Manager provides convenient access to post-installation configuration options and troubleshooting. The following actions are available:

- start and stop product services
- open configuration files for product services
- install/renew SSL certificate after installation
- change server IP address
- collect Support information
- open Event Viewer
- open Windows Services

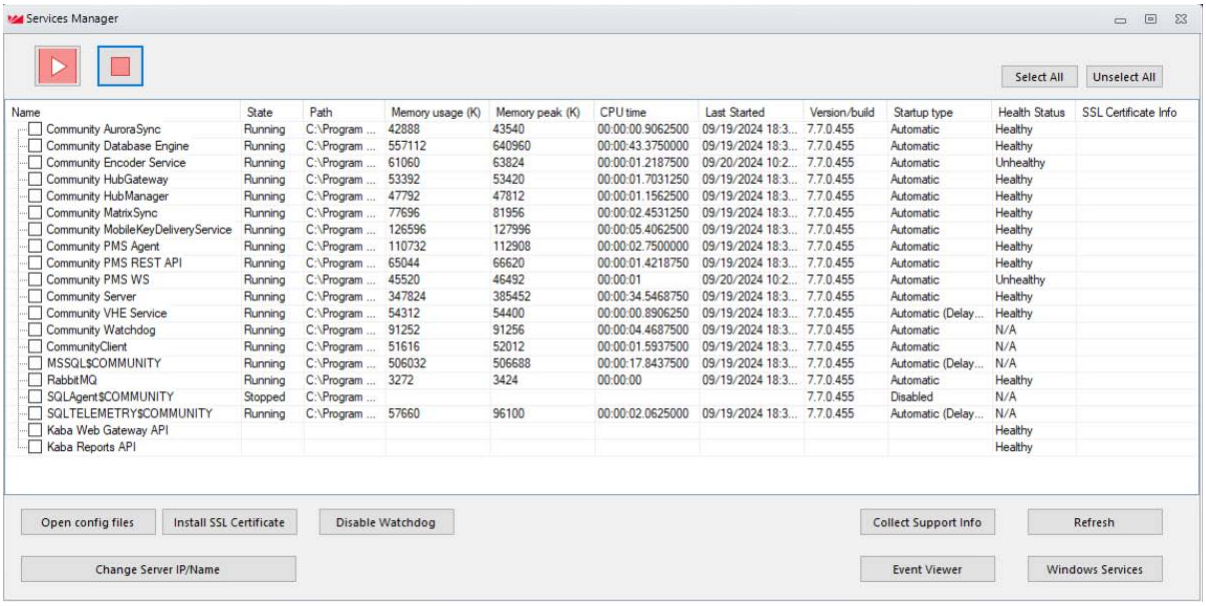
Open the Services Manager

Access the Services Manager on the server from the default location:

C:\Program Files\dormakaba\Community Server\Services\Service Manager\ServiceManager.exe

Access the Services Manager on the workstation from the default location:

C:\Program Files (x86)\dormakaba\Community Client\Services\ServiceManager\ServiceManager.exe

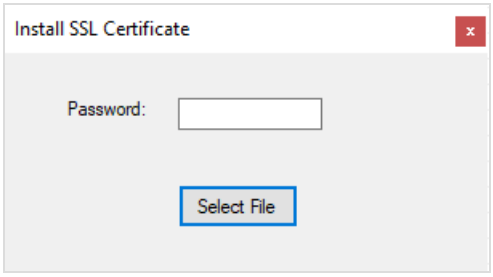


Install / renew SSL certificate after installation

Use the Services Manager to install or renew an SSL certificate on the Community server after installation. Each Community workstation must be updated to use the HTTPS protocol.

Server

1. On the Community server, open the Services Manager.
2. Click Install SSL Certificate.
3. Disregard the warning message and click Yes to proceed.



4. If applicable, specify the password for the certificate.
5. Click Select File.
6. Navigate to and select the certificate (.pfx).
7. When notified the certificate was installed successfully, click OK.

Client

The following steps must be performed on each Community workstation.

1. Open the Services Manager.
2. Select the CommunityClient service and click  to stop the service.
3. Click Open Config files.
4. Change "WebAPIUrl" and "signalrURL" values to point to **https**:

- From:
  <add key="WebAPIUrl" value="http://<Community Server IP>/WebAPI/" />
  <add key="SERVICE_URL_WITH_PORT" value="http://localhost:40100" />
- To:
  <add key="WebAPIUrl" value="https://< Community Server IP>/WebAPI/" />
  <add key="SERVICE_URL_WITH_PORT" value="https://localhost:40100" />

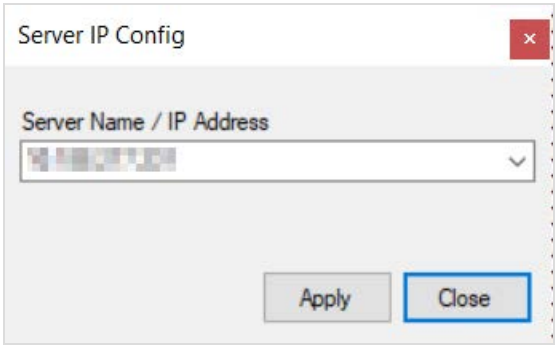
5. Save and close the configuration file.
6. Click  to restart the Community Client service.

Change server IP address / name

Use the Services Manager to change the Community server IP address after installation. Changing the IP address requires that the Community client be uninstalled and reinstalled on each workstation.

Server

1. On the Community server, open the Services Manager.
2. Click Change Server IP/Name.
3. Disregard the warning and click Yes to proceed.
4. Specify the new IP address or name, then click Apply.



5. Restart the Community Server.

Client

The following steps must be performed on each Community workstation.

1. Open the Services Manager.
2. Select the CommunityClient service and click  to stop the service.
3. Click Open config files.
4. Change "WebAPIUrl" and "signalrURL" values to point to the new IP address.

- From:
  <add key="WebAPIUrl" value="https://<Community Server IP>/WebAPI/" />
  <add key="signalrURL" value="https://< Community Server IP>/
  WebAPI/signalr/" />
- To:
  <add key="WebAPIUrl" value="https://< Community NewServer IP>/WebAPI/" />
  <add key="signalrURL" value="https://< Community NewServer IP>/
  WebAPI/signalr/"/>

5. Save and close the configuration file.
6. Click  to restart the Community Client service.

Open configuration files

To open configuration files, select the services for which you want to view the corresponding configuration files, then click **Open config files**. Each configuration file opens in a separate window.

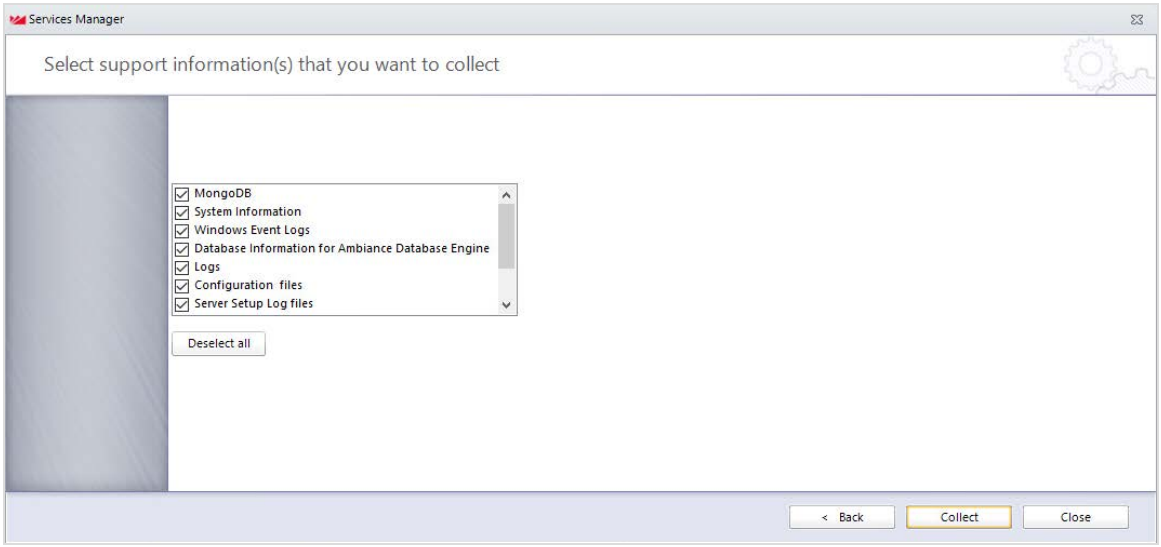
Disable/enable Watchdog

The Services Manager includes a Watchdog feature that performs regular healthchecks on the server. The Watchdog is enabled by default. To disable / enable Watchdog, open Services Manager and click the appropriate button.

Collect support information

Prior to contacting dormakaba for support, collect information about your Community system. Collect information on the server and workstation.

1. Open the Services Manager, then click **Collect Support Info**.



2. Select the type of support information that you want to collect.
3. Click **Collect**.
4. Specify a file name, then click **Save**.

Open Event Viewer

To open Windows Event Viewer app, click **Event Viewer**.

Open Windows services

To open Windows Services app, click **Windows Services**.

Troubleshooting encoders

When encoding or reading a key fails, an information box identifies the following problems:

- When communication between the encoder and workstation fails.
- When the encoder is offline.
- When the encoder is busy.
- When a key is not presented to the encoder within the expected delay.
- When the key is damaged, corrupt or uses unsupported technology.
- When communication fails at the Server level.

Is the Community Client required/installed?

You must install the Client on every workstation where a USB encoder and / or Maintenance Unit is required. From Community, download the Client. A total of three files are required:Community_Client.exe, serverURL.config, and token.txt.

Do not install the Client on the Community Server.

Follow the instructions for each of the following wizard pages.

1. On the **Welcome** page, click **Next**.
2. On the **License Agreement** page, accept the terms of the license agreement then click **Next**.
3. On the **Choose Destination Location** page, choose where to install Client files, then click **Next**. The default location is recommended.
4. When notified the installation is successful, click **Finish**.

Is the encoder connected to the workstation and configured correctly?

The initial configuration of an encoder requires that you connect the encoder to the Community workstation using a USB cable. By default, the device emits an audible beep and flashes a green light to indicate a successful connection. If you configure the encoder to connect using the USB method, the encoder must remain connected to the workstation.

Configure an encoder for USB

1. Plug the encoder into the workstation.
2. In **Device Management**, click **New Encoder**.
3. Specify a unique name that does not exceed 50 characters. This name displays in the list of encoders.
4. Specify a number to identify the encoder to the PMS (Property Management System). Valid values: 0-99.
5. Select the MAC address of the encoder. The value is automatically detected when you connect the encoder to the workstation.
6. Select **USB**.
7. Click **Save**.

Configure an encoder for TCP/IP

Before starting, verify that a port is open for inbound communication on the Community server (typically, configured during initial server installation).

1. Plug the encoder into the workstation.
2. In **Device Management**, click **New Encoder**.
3. Specify a unique name that does not exceed 50 characters. This name displays in the list of encoders.
4. Specify a number to identify the encoder to the PMS (Property Management System). Valid values: 0-99.

5. Select the MAC address of the encoder. The value is automatically detected when you connect the encoder to the workstation.
6. Select TCP/IP.
7. Select whether to obtain an IP address automatically. If using DHCP, select **YES**.
8. Select whether to use the Server name or IP address, then specify the correct information.
9. If not using DHCP, specify the IP address for the encoder including the subnet mask and default gateway.
10. Click **Save**.

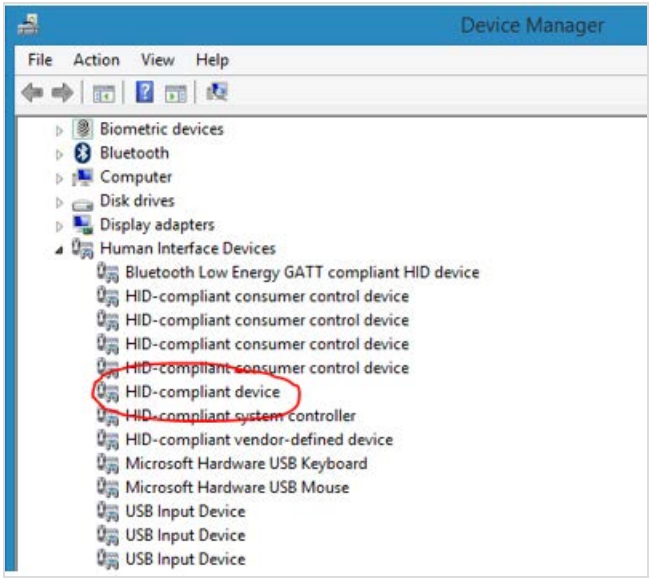
Are you still having a problem encoding or reading keys?

To prepare for troubleshooting, review the following log:

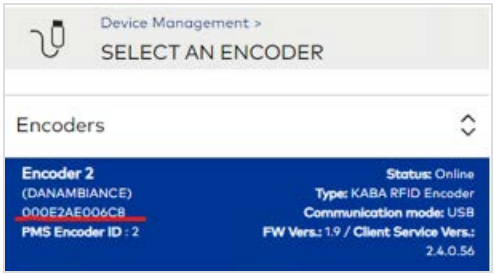
C:\ProgramData\dormaKaba\Community\logs\Services\DokaClient.exe.log

Troubleshooting steps:

1. Make sure that the Community Client Service is running on the workstation. Go to Services and check (or restart) the Community service.
2. Verify the physical connection between the encoder and the workstation. Unplug and plug in the encoder. Make sure that you hear 2 beeps and that the lights are on under the encoder.
3. Verify encoder In Device Manager:
   a. Unplug the encoder from the workstation.
   b. Open Device Manager.
   c. Plug in the encoder.
   d. Verify that a new HID-Compliant Device appears and it is not in an error state.

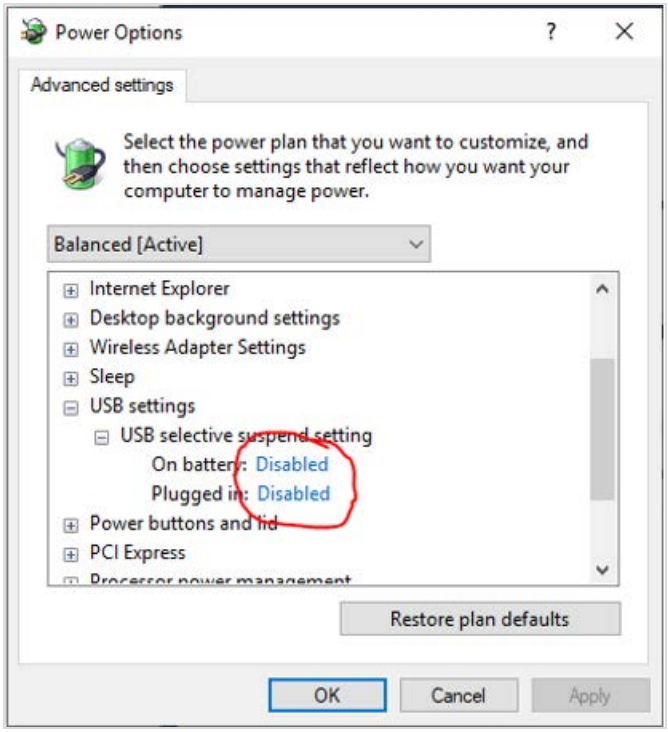


4. Verify IP address:
   a. Go to: C:\Program Files (x86)\dormaKaba\Community Client\Services\ClientServices and open the file **DokaClient.exe.Config** (in Notepad).
   b. Verify that the correct server IP address is in the following lines:
   <add key="WebAPIUrl" value="http://ip_address/WebAPI/" />
   <add key="signalrURL" value="http://ip_address/WebAPI/signalr/" />
5. In Device Management, make sure that the Encoder MAC address is not assigned to another workstation.



You may need to verify that a port is open for inbound communication on the Community Server (typically, configured during initial server installation).

6. If a USB encoder stops working follow these steps on the workstations:
   a. Go to Control Panel – Power Options.
   b. Click on Change Plan Settings.
   c. Click on Change Advanced power settings.
   d. Select USB settings.
   e. Select USB Selective suspend setting.
   f. Change both settings to Disabled.



7. Is the encoder MAC address not showing up after the Client installation?
   - The Server was set up using either the Server name or IP address.
   - Install the Client using the Server name instead of IP address.
   - Perform a hard reset on the encoder:
     a. Unplug the encoder cable.
     b. Press and hold the reset button at the back of the encoder.
     c. Insert the encoder cable to power encoder (while still pressing and holding its reset button).
     d. Keep pressing and holding the encoder reset button for 2 more second then let go of the reset button. You should hear 5 quick beeps if the encoder reset is successful.

If the problem persists after troubleshooting, contact dormakaba Support.

Troubleshooting locks

For security reasons, dormakaba imposes a maximum on the number of unused keys that can be issued for a given credential. For example, when more than 15 keys are issued but never presented to Room 100, the access point becomes "out of sequence" and denies access to all of the keys.

To restore key access, reprogram the access point using the Maintenance Unit or resequence the access point using the Resequence Key. After the access point is resequenced, the access point accepts the most recently issued key.

The maximum number of unused keys before resequencing is required depends on the key type:

- Resident Keys
  - Room and Suite=15
- Staff Keys
  - All classes=unlimited
- System Keys
  - Failsafe, Latch, Unlatch, Toggle Latch/Unlatch=15
  - ELO=3
  - Inhibit=0
  - PPK/SPK=0

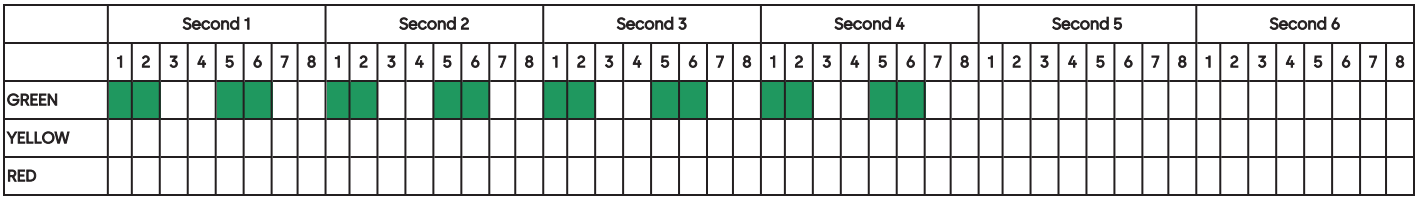
Light Indicators

The three light indicators (green, yellow and red) are located on the face of the lock. These lights provide lock status information when a key is inserted into the lock and removed. When using an RFID lock, the following LED indicators will appear when a RFID card is presented to the lock reader.

The default opening cycle is four seconds but is programmable.

Green Light

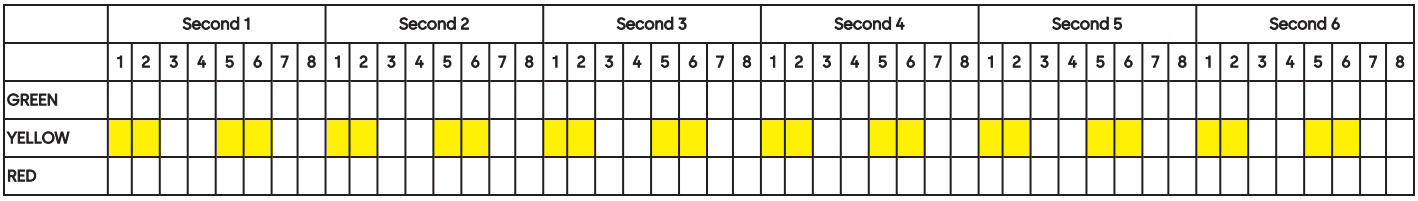
A green light will flash for approximately four seconds when a correct key is used.



This sequence indicates that the locking mechanism has been released and the door handle can be depressed to open the door. If the handle is not depressed while the green light is flashing, the locking mechanism will be secured, and the key must then be reinserted and removed from the lock to release the latch.

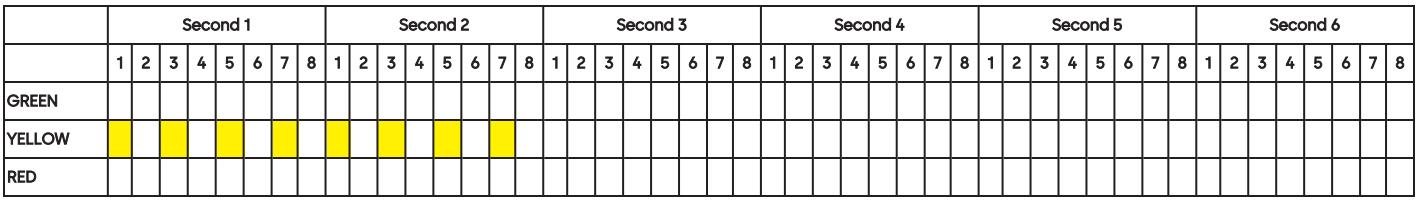
Yellow Light

Flashing Yellow Light (12 Times)



This flashing yellow light indicates that a correct key has been used in the lock, but the dead bolt or privacy button/switch has been set from inside the room.

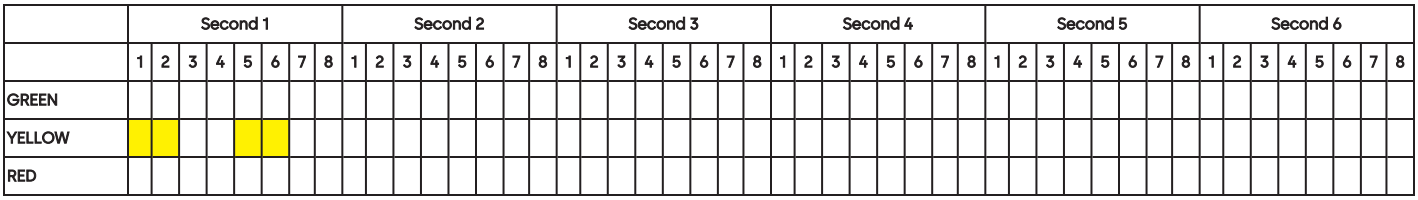
Fast Flashing Yellow Light (8 Times)



This fast flashing yellow light indicates that a correct key has been used in the lock, but entry is denied for one of the following reasons:

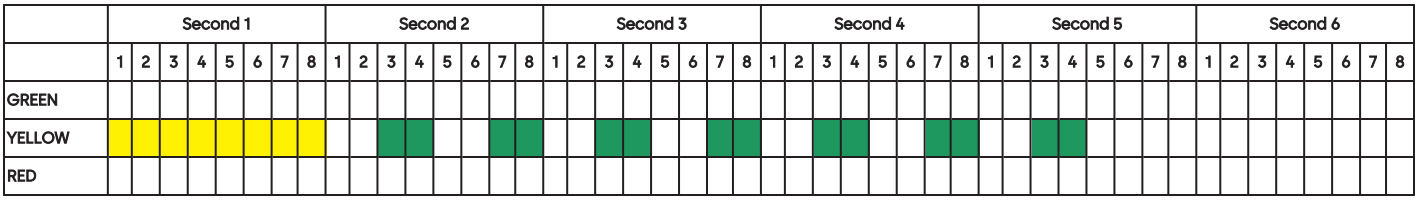
- The door has been electronically double-locked by an electronic lockout key.
- The Resident key has been automatically inhibited, or the lock has been inhibited by the inhibit key.
- The key was programmed with an expiration date and time. The light indicates that the key was used after this expiration date and time.
- The Master key was programmed to work only during certain shift hours of the day, or to work only on certain days of the week. The light indicates that the key used was not programmed for that shift or day.

Two Yellow Flashes



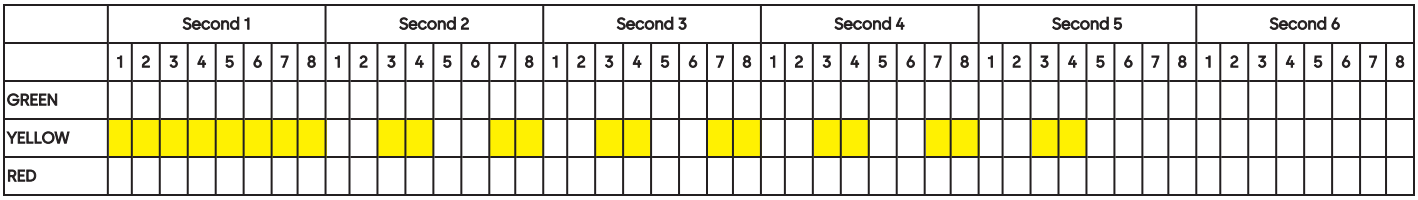
Two yellow flashes indicate that an incorrect key was used in the lock.

1 Yellow before 7 Green



This sequence indicates Master Key is about to expire but access is granted. This light will appear seven days prior to the expiration date.

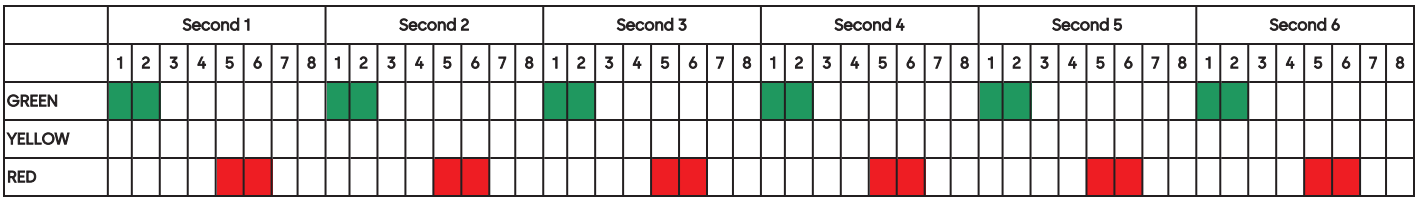
1 Yellow before 7 Yellow



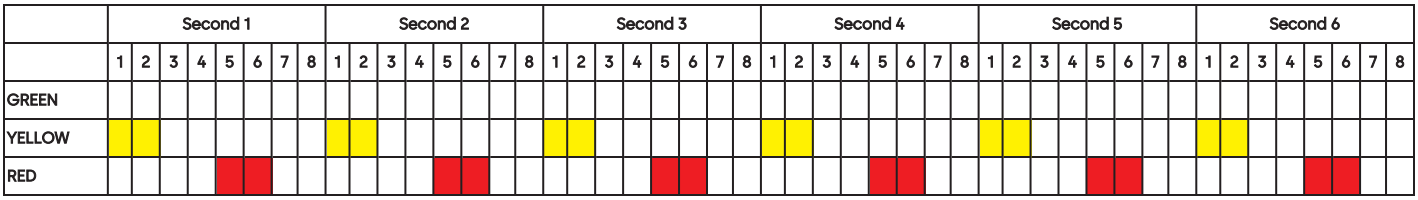
This sequence indicates Master Key is about to expire but access is denied (Privacy=ON). This light will appear seven days prior to the expiration date.

Red Light

Alternately Flashing Red Light

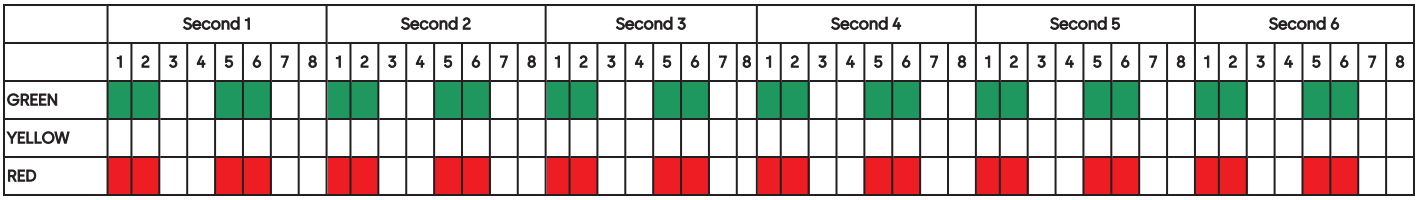


or

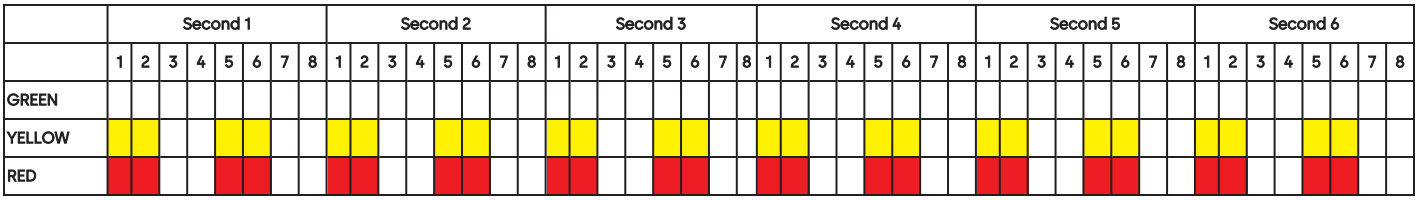


A red light will flash alternately with another light when the lock batteries are low.

Simultaneously Flashing Red Light

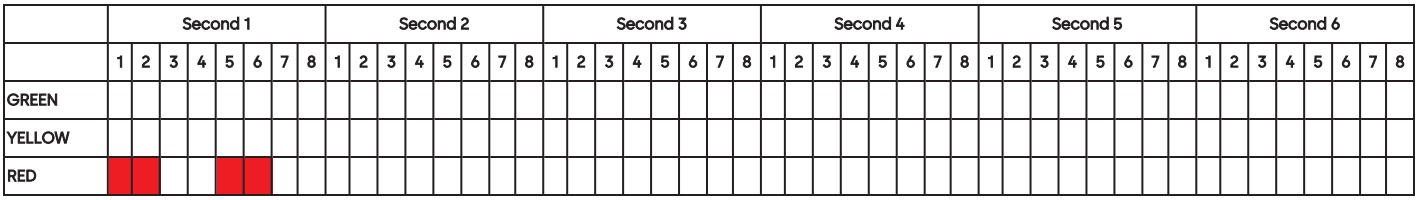


or



A red light will flash simultaneously with another light when the clock in the lock needs to be reset.

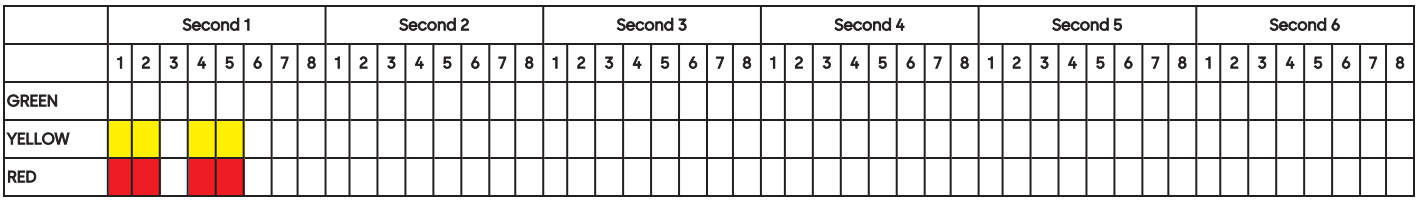
Red Flash (1 or 2 Times)



If a red light flashes one or two times when a key is used in the lock, the key was used improperly (upside down, backwards, or not removed). If a red light flashes one or two times when no key is used, the key switch is stuck.

Yellow and Red Lights

Two yellow and red flashes.



These lights indicate that the lock was unable to properly read the lock code on the key.

No Lights

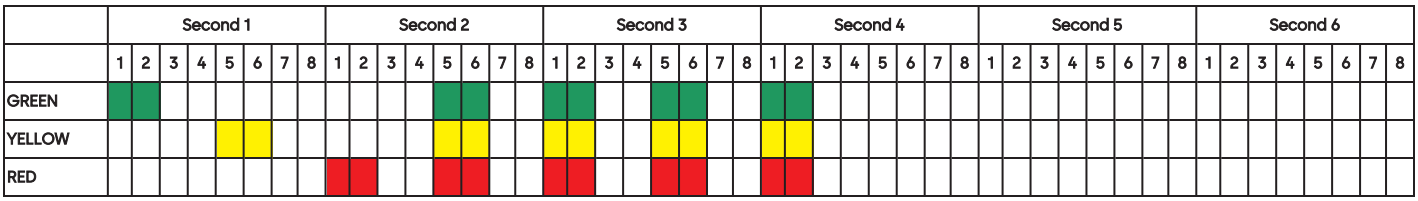
If no lights appear when a key is used:

- An invalid key shutdown is in effect.
- The key switch is broken.
- The lock batteries are dead.

Invalid Lock and Mode Indicators

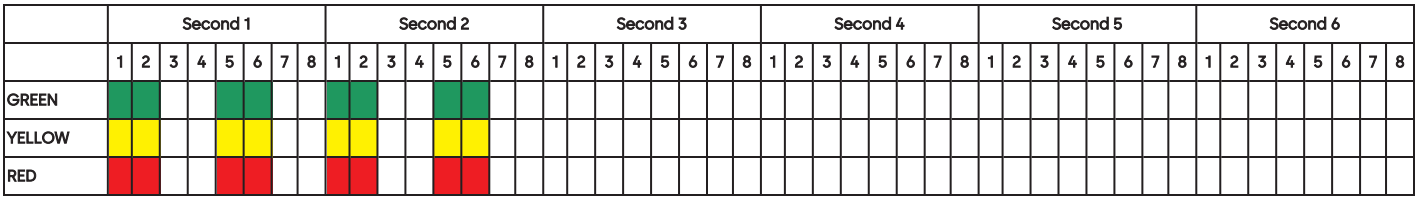
Locks are designed to operate in Mode 2 when it is programmed and properly functioning. If a lock is not operating in Mode 2, and a valid key is used, you will see one of the following patterns. These lights indicate that there is a physical problem with the lock that must be corrected before the lock will allow keys to operate normally.

1 Green, 1 Yellow, 1 Red, Then All Lights Flash (4 Times)



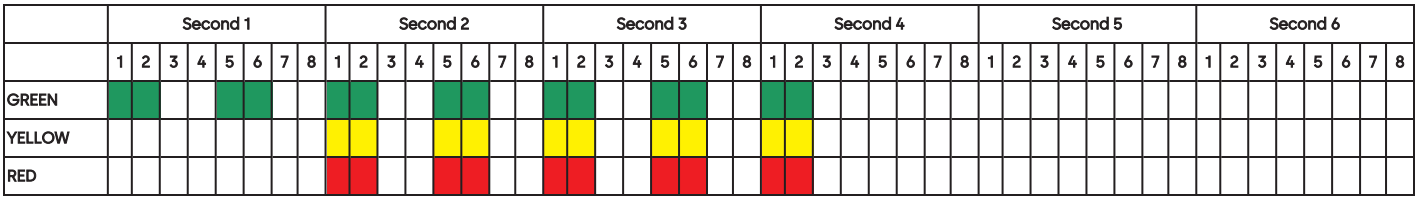
These lights that the lock is in the Test Mode, and the storage chip has failed. No key will open the lock, and the lock must be drilled to access the room.

All Lights Flash (4 Times)



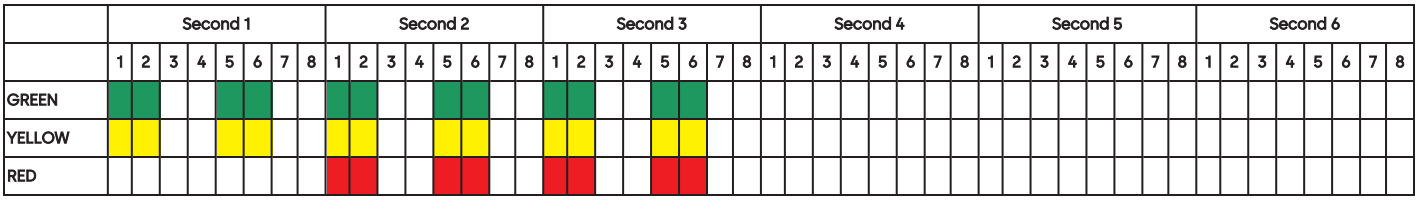
These lights indicate that the lock is in Mode 0 and that there is a problem with the circuit board. Use the erase key to change the mode to Mode 1, and program the lock using the LPI probe and terminal. Use the new key to open the door and replace the circuit board.

2 Green. Then All Lights Flash (4 Times)



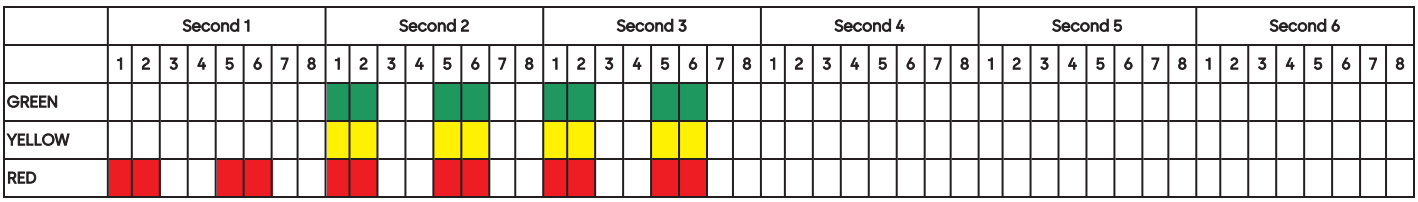
These lights indicate that the lock is in Mode 1, and is not programmed. Program the lock using the LPI probe and terminal. Use the new key to open the door and replace the circuit board.

2 Green and Yellow Flashes. Then All Lights Flash (4 Times)



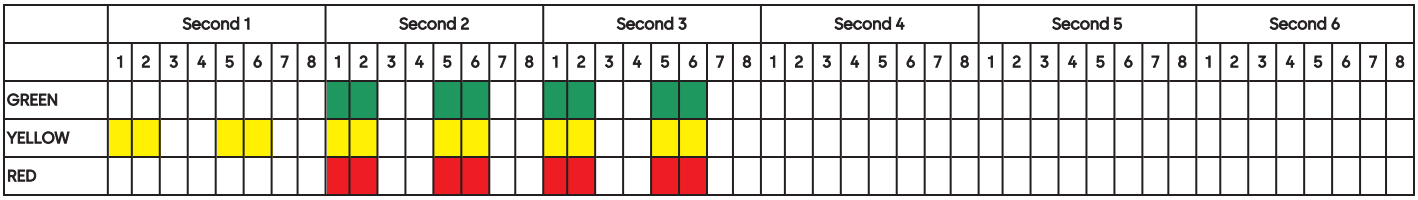
These lights indicate that the lock is in Mode 3 and that there is a programming problem with the programming chip in the lock's circuit board. Open the door using the PPK key followed by a valid Master key. Remove the lock and replace the circuit board.

2 Red Flashes. Then All Lights Flash (4 Times)



These lights indicate that the lock is in Mode 4, and that the storage chip is disabled. Use the PPK key followed by the Disable/Enable key to enable the lock.

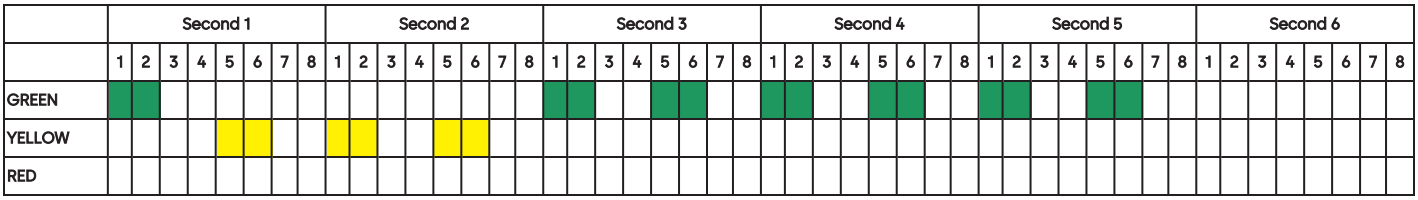
2 Yellow Flashes, Then All Lights Flash (4 Times)



These lights indicate that the lock is in Mode 5, and that there is a problem with the motor switch or the motor is jammed. Open the door using the PPK key followed by a valid Master key. Then, remove the lock and replace the lockset.

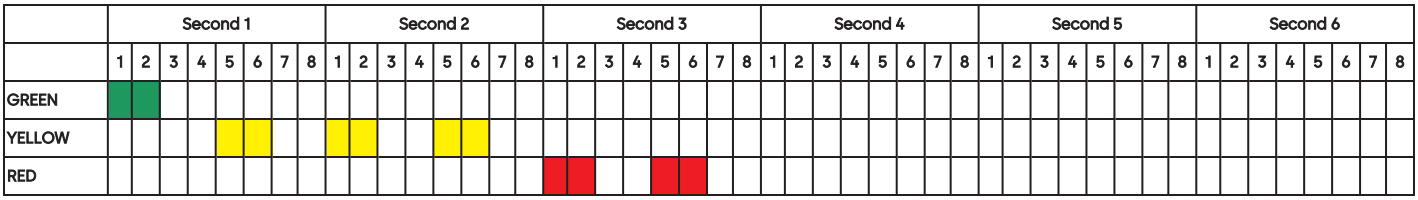
Online

1 green, few yellow, 6 green.



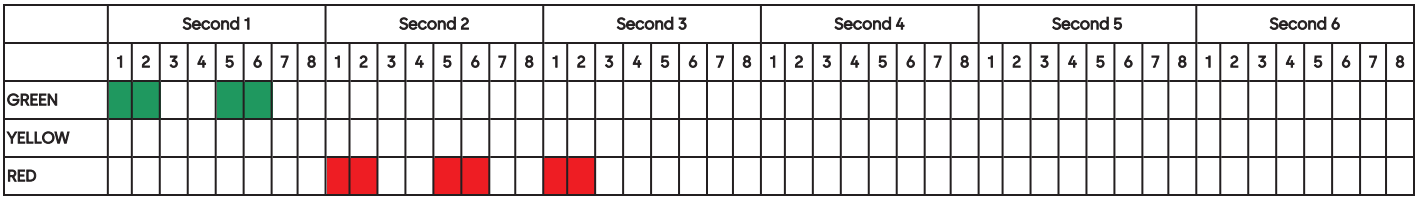
When passing an RF Pairing key and the pairing is successful.

1 green, few yellow, 2 red.



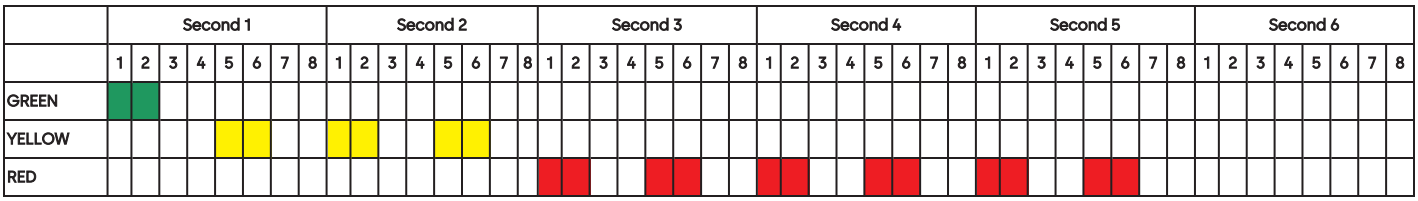
When passing an RF Pairing key and the pairing fails.

2 green, 3 red



When passing an RF Unpairing key, this sequence indicates the lock was not paired.

1 green, 3 yellow, 6 red



When passing an RF Unpairing key, this sequence indicates the lock was paired and is now unpaired.

Log data

Community logs provide detailed information about all events and system activity that occur during installation (or upgrade) and product use. For Support technicians, logs are the principal troubleshooting resource.

Installation logs

The following Installation logs are located on the server by default at: C:\Community Server:

- MongoInstall (for online communication)
- SetupServer (primary installation log)

The following Installation log is located on the workstation by default at: C:\Community Server:

- SetupClient.LOG

Product logs

Multiple logs are stored by default at: C:\ProgramData\dormaKaba\Community\logs

The logs folder organizes log files as follows:

- Services—Data related to the various Community Windows services.
- Web
  - reportapi.log.txt—Data related to the IIS component report API used to generate reports.
  - webApi.log.txt—Data related to the Community WebAPI Windows service.

Glossary

A

Access Management
The module where you define credentials for staff and system keys, configure and assign schedules, configure common area access, and create logical groupings of access points to facilitate credential assignment.

Access Point
1) Virtual representation of a physical location where passage between two spaces is controlled by a lock. 2) Reader-equipped lock encoded with access control data to allow or deny access based on credentials.

Access Point Audit Report
Detailed historical information about lock events.

Access Point Group
Logical grouping of one or more access points that facilitates the assignment of credentials to all access points in the group.

Access Point Scheduling
Submodule within Access Management where you assign auto-unlatch and access schedules to access points.

Access Point Status
Current state of the lock installed for a given access point.

Access Point Type (Community)
Functional classification of an access point. The access point types in Community include units, suites, foyer doors, resident and staff common areas, restricted areas and elevator readers.

Access Schedule
Day and time constraints that control when an access point is accessible.

Additional Key
Duplicate key. A New key must be active before the option to make an Additional key is enabled. Additional keys do not affect any existing active keys.

Audit
The process of retrieving historical information from an access point.

Auto-Unlatch Schedule
Day and time periods allowing passage without keys.

B

Block Key
System key that temporarily blocks all keys encoded with a specific credential.

Building
Component in Property Builder that represents a physical structure on the site that contains one or more floors and one or more access points.

C

Cancel Key
System key that permanently invalidates a specific key instance.

Common Area Access
Submodule in Access Management where common area profiles are defined to configure access to common areas.

Common Area Profile (Community)
Configuration that defines the common areas that are accessible for selected units and suites or for selected staff credentials, and whether access is included by default or must be manually selected.

Community API
Set of Web API methods to integrate Resident Management and Staff/Vendor Management with third-party systems.

Construction Keys
Keys that secure access points after installation yet prior to locks being programmed. Construction (or Zone) keys are obsolete after locks are programmed.

Credential
1) Configuration that consists of access point groups and/or individual access points for the purpose of authorizing staff access to a physical space or system key functionality. 2) Digital identification code stored on a key that authorizes access where the code is valid.

Credential Class
Organizational label used to group credentials based on the credential class type.

Credential Class Type
A fixed set of access properties from which all credential classes are derived.

Credential Management
Submodule in Access Management where you create and manage credentials.

Credential/Access Point Assignment Report
List of credentials and assigned access points or a list of access points and assigned credentials.

D

Device Management
The module where you add and configure encoders. If online communication is enabled, you can also configure gateways and paired access points. In cloud environments, you can also configure the cloud gateway when licensed for Cloud Gateway - PMS Bridge.

Diagnostic Key
System key that queries locks to extract and report the status of various lock functions for troubleshooting and reporting. Diagnostic results are communicated by an LED flash sequence.

E

Electronic Lockout (ELO) Key
1) Credential class for system keys. 2) System key that temporarily invalidate all non-Emergency Keys.

Elevator
A physical structure intended to provide access to building floors.

Elevator Bank
Group of elevators that share the same elevator controller configuration.

Elevator Configuration Report
Detailed information about an elevator bank including elevators and relay-to-floor mapping for each panel.

Elevator Controller Profile
The elevator bank model configuration.

Emergency Key (Community)
1) Credential class type/class that overrides deadbolt/privacy switch. 2) A type of key encoded with a credential based on the Emergency class. Toggle mode is supported for units/suite units as an opion in Property Builder.

Encoder
Embedded device used to encode keys.

F

Failsafe Key
Backup key made in advance and maintained in complete sets to be issued in the event a system or power failure prevents making keys.

Firmware
Operating software for hardware devices.

Floor
Component in Property Builder that represents a level in a building.

G

Gateway
Gateways are the network devices which are paired to access points for online communication.

I

Inhibit Key
1) Credential class for system keys. 2) System key that permanently cancels all access for a current resident.

K

Key
A transport medium on which a credential is encoded for the purpose of controlling access and/or performing system or programmatic operations. Examples include key cards and key fobs.

Key Expiration Report
Lists the expiration date of active keys.

Key Holder
A person with authorized possession of at least one key.

Key ID
Specific key among multiple keys that are encoded with the same credential.

Key Mode
Option that you select when making a key: New or Additional.

Key Status
The current state of the key.

Key/User Assignment Report
List of active keys assigned to a given key holder.

L

Latch Key
1) System key credential class. 2) System key that disables passage mode.

Limited Use Key (Staff)
1) Credential class type/class for staff keys. 2) A staff key that is encoded with temporary access to an access point for a predefined number of times or until the key expires.

Lock Profile
Lock device model.

M

Maintenance Unit (M-Unit)
Hand-held embedded device used to transfer data between Community and locks.

Mobile Key
Virtual key issued to a mobile phone.

Monitoring
The module where you view a list of all keys made by Community. When online communication is enabled, you can also view online metrics, operations, events and access point status.

N

New Key
Key made using mode New. New keys invalidate access to the selected credential on all existing keys.

Notification
Alert issued to notification subscribers.

Notification Group
Logical grouping of one or more notification events configured in the Notification Management module for the purpose of Operator subscription.

Notification Management
The module where you configure and manage the notification groups that can be assigned to staff members.

O

Online Access Point Status Report
Details about current gateways and paired access points.

Online Communication
A licensed feature that refers to wireless communication between access points and Community. Remote communication is used to perform online access point operations and to receive online access point events.

Online Gateway Status Report
Details about current gateways.

Online Paired Access Point Report
Lists the access points paired to a gateway.

Operator
Staff member who is assigned a role that is configured to authorize access to Community modules and features.

Operator Report
Lists Operators, their assigned roles, and the rights associated with each role.

Operator Status
Status of an Operator.

P

Paired Access Point
In online communication, an access point that is connected to a gateway.

Panel/Relay
Electrical component in an elevator controller box with one or more relay switches. A relay is an electrical component that is mapped to specific floors.

Passage Mode
Lock state during which the access controls programmed in the lock are suspended allowing unrestricted access.

PCI-DSS
Information security standard that provides additional login protection.

Period (Schedules)
A span of time selected for schedules in Access Management.

Predefined access
An access property associated with a credential class type that is characterized by selecting access when defining the credential.

Primary Program Key
System key that authorizes the function of another system key.

Programming & Auditing
The module where you perform the data transfers necessary to program and audit locks.

Property Builder
The module where you create a virtual representation of the site: buildings, floors and elevators per building, and access points.

Property Configuration Report
Details about the access point configuration for the site.

R

Reader
Embedded device that reads access control data stored on keys.

Replacement Key
An additional key made to replace a lost or defective key.

Reports
The module where you track, investigate and maintain current and historical records for every aspect of your site.

Resequence Key
System key that resynchronizes a specific key credential in access points.

Resident
Person added in the Resident Management module for the purpose of assigning units and/or common area access.

Resident Common Area
Type of access point where general access is configured for residents.

Resident Management
The module where you manage all resident access and keys.

Restricted Area
Type of access point intended for staff access only.

RFID
Radio Frequency Identification. Technology that supports contactless keys.

Rights (Role Management)
Discrete permissions to Community functionality.

Role
A group of rights assigned to an Operator.

Role Management
The module where you configure Operator Roles and the system and key rights associated with each role.

Roles & Rights Report
Lists the roles defined in the Role Management module and the Community functions to which each role has rights.

S

Secondary Program Key
System key that reprograms or resynchronizes the current Primary Program Key (PPK).

Shift Schedule
Day and time constraints applied to staff keys.

Site
Geographical location that consists of one or more buildings.

Special Function Key
System key that is used for advanced lock operations.

Staff
Operators and key holders in your organization.

Staff Access Report
Lists historical information about staff access.

Staff Common Area
Type of access point where general access is configured for staff.

Staff Key
Credential class type/class. Access is predefined. Toggle mode is supported for units/suite units as an option in Property Builder.

Staff Key (variable access)
Credential class type/class. Access is variable. Toggle mode is supported for units/suite units as an option in Property Builder.

Staff/Vendor Keys
1) The module where you make keys for staff/vendors. 2) Keys encoded with a staff/vendor credential.

Staff/Vendor Management
The module where you add staff/vendors, configure Operators, and manage staff/vendor keys.

Suite
A connected series of units that includes a common door and one or more suite units.

System Activity Report
Details about the system transaction history.

System Keys
1) The module where you make keys to perform lock or system-level operations. 2) Keys made in the System Keys module.

System Settings
The module where site-wide options, preferences and defaults are specified. Some settings control whether Community features are enabled and how the features operate.

T

Toggle Latch/Unlatch Key
1) System key credential class. 2) System key that is used to enable and/or disable passage mode.

Toggle mode
Feature that alternates the state of a lock to allow/deny access.

U

Unblock Key
System key that unblocks all instances of a specific credential in access points which were previously blocked using a Block Key.

Unit
Type of access point assigned to a resident.

Unlatch Key
1) System key credential class. 2) System key that enables passage mode (unrestricted access) in the lock.

User Type (Operator profile)
Option selected in staff member profiles that reflects the nature of relationship with the property.

V

Variable access
An access property associated with a credential class type that is characterized by selecting access at key-making time.

Vendor Key
Credential class type/class. Access is variable. Toggle mode is supported for units/suite units as an option in Property Builder.

Visitor Management
Complimentary feature that supports extending access to visitors by sending a PIN or delegated mobile key. Requires AuroraSync and mobile key licenses.

W

workstation
Computer used by Operators to access Community software.

Index

A

Access Management 91

access point

- groups 101
- mobile-enabled report 286
- scheduling 107
- types 52

Access Point Audit Report 254

access points

- importing 71

access report, residents/staff/vendors 279

Access schedules 97, 107

access to Community modules 10, 125

account preferences 271

activate

- residents 176

activate staff/vendors 215

activation key 50

adding

- access point groups 101
- buildings 58
- credentials 103
- custom Operator roles 128
- elevators 86
- encoders 115

floors 59
notification groups 312
operators 133
resident common areas 72
residents 144, 151
restricted areas 84
schedules 95, 97, 99
staff common areas 78
staff/vendors 187
suites 66
units 62
additional keys 283
administrator role 125, 127
API authentication 24
archiving historical data 40
assigning schedules 107
audit key 247
audit locks 121, 221
Audit Report 254
Aurora, Keyscan 47
auto-unlatch schedules 95, 107

B

backing up database 37
batch creation of access points 52
Block/Unblock Keys 227
Block/Unblock Operator access 212
BlueSky, dormakaba 289
builings 58

C

Cancel Keys 231
Cancel Keys (resident access) 173

client, Community 273, 275
color codes, access points 119
common areas, extended 45
common areas, limited access 93, 108, 178, 180
configuring
  access to common areas 108
  custom Operator roles 128
  encoders 115
  Operators 133
credential class types 91, 185, 191, 194, 198, 202, 206
credential classes 91, 185, 191, 194, 198, 202, 206
Credential/Access Point Assigment Report 256
credentials
  access point groups 101
  adding 103
  assignment report 256
  learning about 91
  resident credential class 93
  shift schedules 99
  staff/vendor classes 91
  system key classes 93
custom Operator roles 128

D

database, backing up 37
date format 19
deactivating
  residents 174
  staff/vendors 214
deadbolt override option for resident keys 21
delegating access to visitors 148
delete residents 175
Device Management 113
device programming 120, 308

Diagnostic Keys 233
disable resident access 165

E

Electronic Lockout Keys 235, 237
Elevator Configuration Report 257
elevator control system 49
elevators 55, 86, 257
ELO Keys 235, 237
Emergency (credential class types/classes) 92, 185, 191, 194, 198, 202, 206
enable resident access 165
enabling mobile keys 45, 285
encoder firmware update 116
encoders 113, 115, 274, 332
entry system, third-party 43
erase keys 278
extended common areas 45

F

Failsafe Keys 34
failures, reading and encoding keys 278
firmeware update, encoder 116
floor access in resident profiles 20
floor mapping, elevator 55
floors, adding 59

G

Grand Master (credential class types/classes) 191, 194, 198, 202, 206
grouping access points 101

H

Home page favorites 269

I

importing
- access points 71

importing resident profiles 153

importing staff members/vendors 138, 189

Inhibit Keys 238

invalidate access 227, 231, 235, 237-238
- residents 171
- staff/vendors 212

K

Key Expiration Report 258

key issuance notification 49

key issuance notification | General.C_OC_UG | [34] 18

key rights 125

key sequence 224

key, activation 50

Key/User Assignment Report 259

keys
- Block/Unblock 227
- Cancel Keys 231
- common area access only 178, 180
- deadbolt override option for residents 21
- Diagnostic 233
- Electronic Lockout 235, 237
- erasing 277-278
- expiration report 258
- Failsafe 34
- Inhibit 238
- invalidate resident access 171
- invalidate staff/vendor access 212
- key mode 283

Latch/Unlatch 240
Limited Use maximum 33
lost 171
mobile 285
physical 283
Primary/Secondary Program 242
reading 277
replacing staff/vendor key 210
Resequence 245
resident 20, 147, 162
RFID type 44
Special Function 247
staff/vendor 131
status 284, 286, 288
System 224
toggle 93
user assignment report 259
warning messages 20
keys, ID reuse 193, 196, 201, 205, 209
Keyscan Aurora 47

L

language display 19, 271
Latch/Unlatch Keys 240
Leasing Agent role 125, 127
LED flash sequence (locks) 336
LEGIC 45, 285
licensing 50
limited access common areas 93, 108, 178, 180
Limited Use (credential class types/classes) 92, 185
Limited Use Staff (credential class types/classes) 191, 194, 198, 202, 206
lock programming 122, 219
locks
audit 221

LED flash sequences 336
programming 119
troubleshooting 233, 336
logs 342
lost resident keys 171

M

Maintenance Supervisor role 125, 127
Maintenance Technician role 125, 127
Maintenance Unit 24, 122, 219, 221, 308
Master (credential class types/classes) 191, 194, 198, 202, 206
Mifare (Classic/Plus) 45
mobile app, BlueSky 289
mobile key delegation 148
mobile keys 45, 147, 285
mobile-enabled access point file download 286
monitor keys 251
monitory keys 250
multiple mobile keys 147

N

naming access points 52
navigating modules 269
New Keys 283
notification groups 310
notification, key issuance 49

O

obsolete keys 224
online communication 47, 247, 291
online reporting 325-326
Operator profile 133
Operator Report 260

Operator roles
custom 128
predefined 127
Operators
block/unblock access 212
configuring 133
roles 125

P

passage mode 95, 240
password
changing 271
security settings 22
phone/mobile number validation override 19
physical keys 283
PIN delegation 148
possible key holders 193, 196, 201, 205, 209
predefined access 92, 185
Primary Program Keys 242
profile
common area access 108
Operator 131
resident 144
staff/vendor 131
programming devices 120, 308
programming locks 119, 122, 219
Property Builder 52
reports 257, 261
Property Configuration Report 261

R

Read Key 277
remote server backups 37

removing resident access 165
replacing staff/vendor key 210
Reports
Access Point Audit 254
Credential/Access Point Assignment 256
Elevator Configuration Report 257
Key Expiration Report 258
Key/User Assignment 259
mobile-enabled access points 286
Online Gateway Status 325
Online Paired Access Point Status 326
Operator 260
Property Configuration 261
Resident/Staff/Vendor Access 279
Roles (Operator) and Rights 262
Staff/Vendor Access 263
System Activity 264
Resequence Keys 245
resident access report 279
resident access, shared 149
resident common areas 54
Resident Common Areas
adding 72
Resident Management 144
residents
activate 176
adding 144, 151
assigning units 144, 155
deactivating 174
delete 175
importing profiles 153
invalidate access 144, 171
making keys 144, 162
making mobile keys for multiple 147
modifying access 165

shared access 156
visitor management 148, 182
REST API 18, 48
restricted areas, adding 84
Return UID interface 49
Return UID interface | General.C_OC_UG | [42] 18
reusing key IDs 193, 196, 201, 205, 209
RF Pairing Key 247
RF Unpairing Key 247
RFID card UID 48
RFID key types 44
Role Management 125, 127
Roles and Rights Report 262
Roles, Operator 128

S

schedules
access 97
assigning to access points 107
auto-unlatch 95
shift (staff) 99
Secondary Program Keys 242
security settings 22
shared resident access 149
shift schedules 99
single sign-on 28
site configuration 13
Site Configurator role 125, 127
Special Function Keys 247
staff
automated email 310
making keys 191, 194, 198, 202, 206
Staff (credential class types/classes) 92, 185

staff common areas
adding 78
Staff/Vendor Access Report 263
staff/vendor access report 279
Staff/Vendor Management 131
staff/vendors
activate 215
adding profiles 187
automated email 36
deactivate 214
importing 138, 189
invalidate access 212
keys 131
replacing key 210
shift schedules 99
visitor management 131, 185, 217
status, keys 284, 288
suites, adding 66
suspend access 227
System Activity Report 264
System Keys 224
system rights 125
System Settings 15

T

time drift 119
time format 19
time zone 19
toggle mode 93
track digital keys 251
types, access point 52

U

UID 48
Ultralight C 45
unit assignments 155, 165
units
    assigning to residents 149, 155
    modifying resident access 165
Units View 149
units, adding 62, 71
update Community Client 273, 275
user preferences 271

V

validation override, phone/mobile number 19
variable access 92, 185
Vendor (credential class types/classes) 92
virtual UID 48
visitor management
    residents 148, 182
    staff 131, 185, 217

W

workflow, site configuration 13
workstation, Community 273, 275

PK3706-EN 2.6 - 08/2026
Copyright © dormakaba 2026

www.dormakaba.com

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
Canada
T: +1 877 468-3555

www.dormakaba.com