dormakaba Canada

Ambiance User Guide

Ambiance 2.2

dormakaba

dormakaba Canada
7301 Decarie Blvd
Montreal, Quebec H4P 2G7
Phone 877-468-3555

PK#: 3722 Rev 20190531

CONTENTS

Welcome to Ambiance

Ambiance® Access Management Software is a secure and scalable access control management system with the sophisticated back-end logic to support robust functionality and a user-friendly front-end for fast, easy and flexible deployment.

Getting Started

Whether you want to take a self-guided tour of your new software or jump straight into configuring your site, the Ambiance 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 *Ambiance User Guide* is organized to follow the recommended workflow and provides information and instructions for all Ambiance Operators.

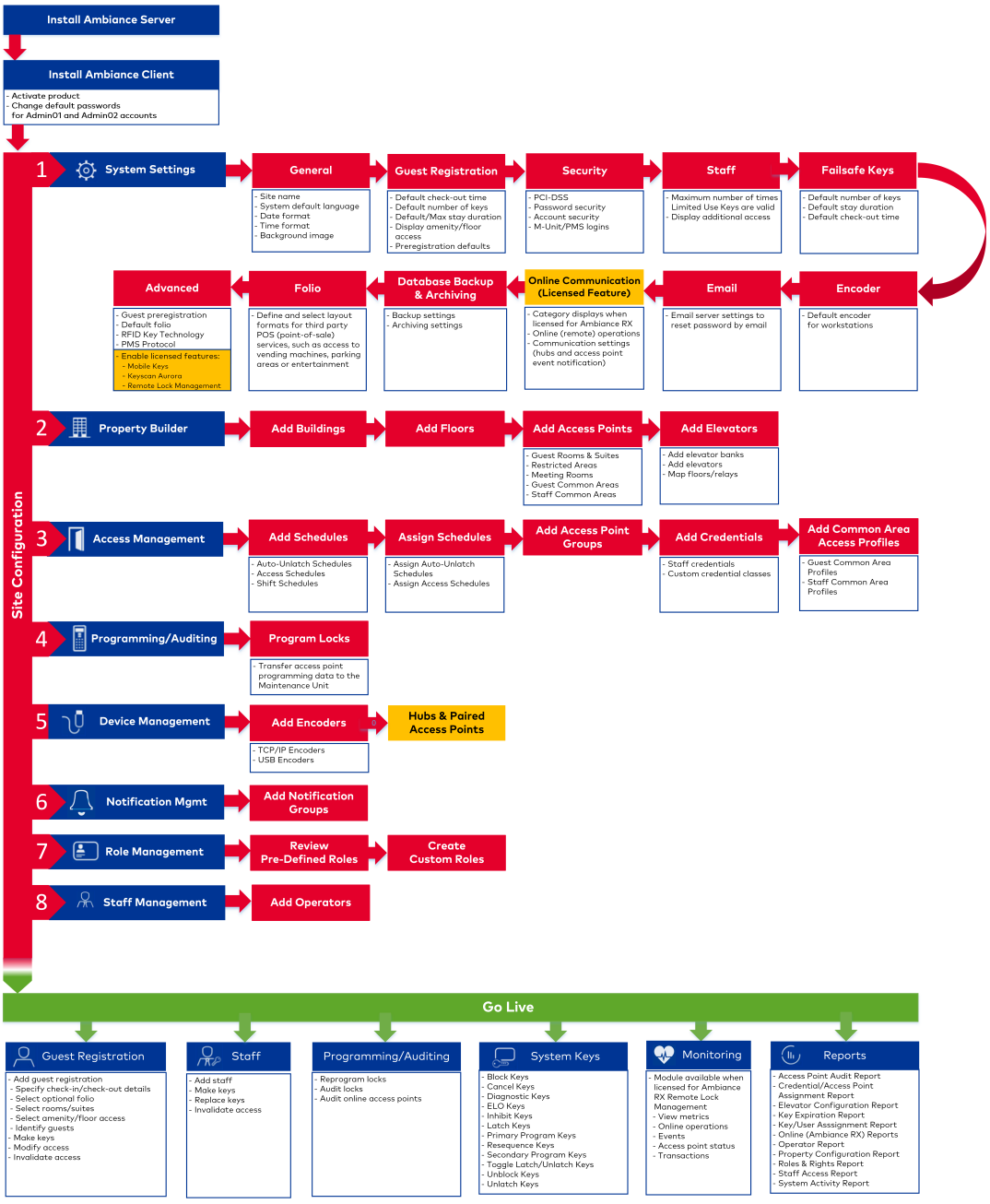
An Operator is a staff member who can log in and use Ambiance.

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 Ambiance" provides instructions for day-to-day work after Go Live and includes Working with ... topics that address some of the more complicated situations.
- "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.

Ambiance Workflow



Installation

Installing the Ambiance Server and Ambiance Client is a straightforward wizard-driven process. For detailed instructions, see the *Ambiance Installation Guide* and *Ambiance 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 Ambiance.

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 Ambiance. Add buildings, floors, access points and elevators.
- **Access Management** where you add the credentials that are available to encode on staff and system keys. You can also configure limited-access common areas and configure and assign schedules to credentials and/or individual access points.
- **Programming & Auditing** where you access the data transfer function required to program and audit locks. If remote lock management is enabled, you can also audit online access points.
- **Device Management** where you configure encoders. If licensed for remote lock management, you can also work with hubs and paired access points.
- **Notifications Management** where you create logical groupings of notifications to which Operators can subscribe. The module is only active when licensed for remote lock management.
- **Role Management** where you create and configure Operator roles and the associated rights.
- **Staff 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 guests. Use the following Ambiance modules to perform daily work:

- **Guest Registration** where you create guest registrations and make guest keys.
- **Staff Management** where you create and manage profiles for staff, replace staff keys, and cancel staff keys.
- **Staff Keys** where you make keys for staff.
- **Programming & Auditing** where you re-program and audit locks. If remote lock management 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 Ambiance. If licensed for remote lock management, 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 Ambiance Features

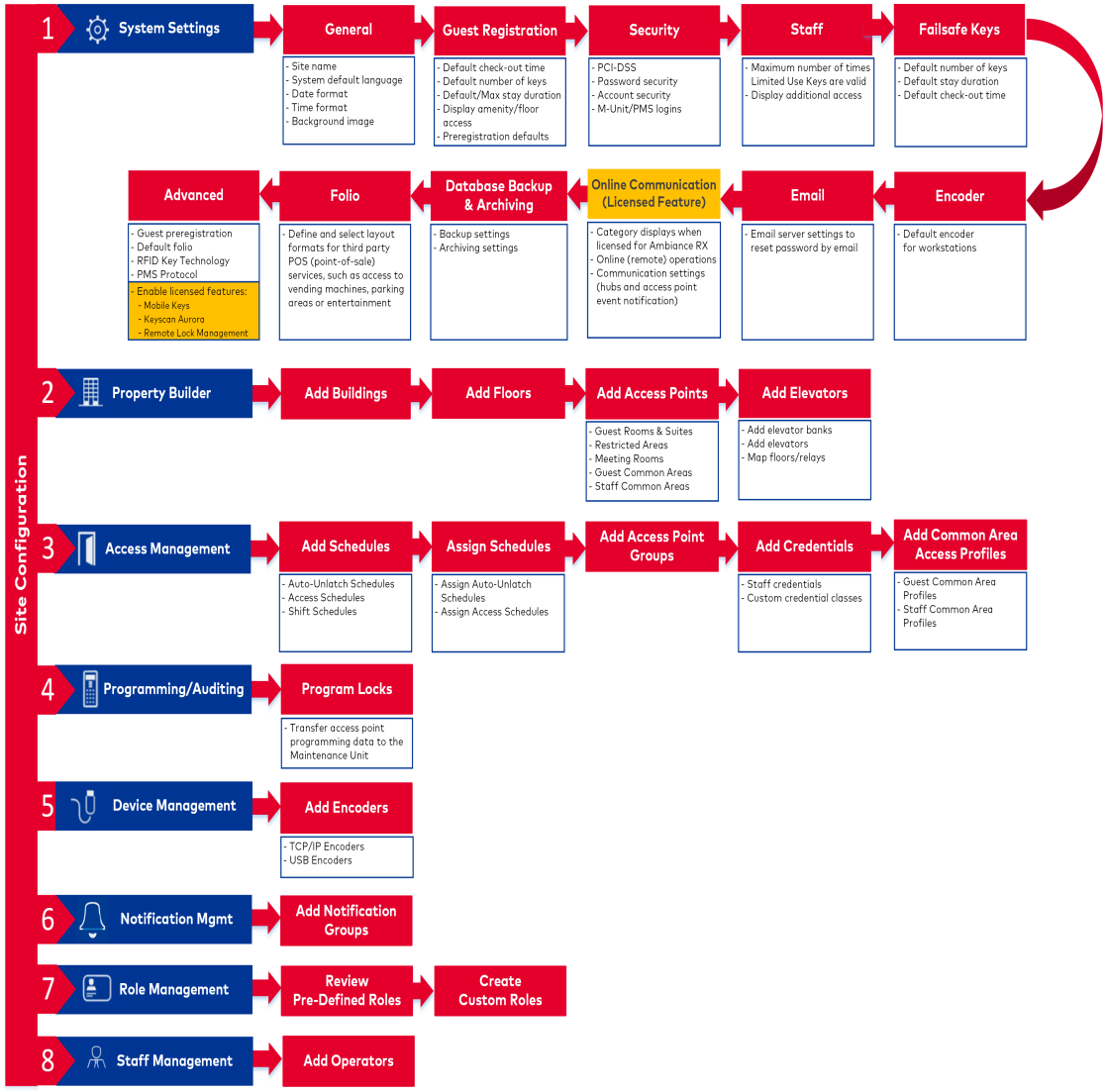
The features and options that display in Ambiance depend on the rights selected for the role assigned to the active Operator. For example, if the Operator that is currently logged in does not have rights to access the Property Builder module, the module does not display. Likewise, if the only right selected 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 chapter discusses the following.

Site Configuration Workflow

The Ambiance Site Configuration Workflow provides an overview of the recommended site configuration process. Each step corresponds to an Ambiance module. Review the process before getting started.



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

Step 1: Define Global Options

This section includes the following subjects:

Learning about System Settings

System Settings is the Ambiance module where you can define system preferences and default values for global options. In some cases, the options in System Settings control whether Ambiance 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 for a guest 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 for mobile keys, Keyscan Aurora and remote lock management. To make site configuration more efficient, Ambiance 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 the site name, default display language, time and date formats, and site image. With the exception of the site name and site image, all settings have system defaults. None of the options in this category require attention.

Guest Registration

Configure defaults for the Guest Registration module. All settings have system defaults. However, if you plan to control access to elevators or issue keys that override a projected deadbolt/privacy switch, the options **Display floor access** and **Enable deadbolt/privacy switch override for guest keys** require attention.

Security

Configure settings related to passwords and account security. All settings have system defaults. However, if you plan to disable authentication for PMS and Maintenance Unit accounts, options in this category require attention.

Staff

Configure how many times a Limited Use Key can be used by staff and select whether to display the menus to add additional access and floor access when making staff 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 three sets of two keys for each guest room and suite door.

Encoder

Select the default encoder to use when making keys on the workstation where you are currently logged in.

Email

Configure settings used to send emails to staff. No system defaults are populated. This category requires attention so that Ambiance can send automated emails regarding account access to staff and to send notifications by email.

Online Communication

This category only displays if Remote Lock Management is enabled in System Settings > Advanced.

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

Database Backup & Archiving

Configuring regularly scheduled backups is a top priority.

Perform on-demand backup of Ambiance database, enable and automate database backups, enable and schedule data retention.

Folio

Define a guest folio that integrates Ambiance with third-party POS (point-of-sale) vendors, such as access to vending machines, parking areas or entertainment venues.

Advanced

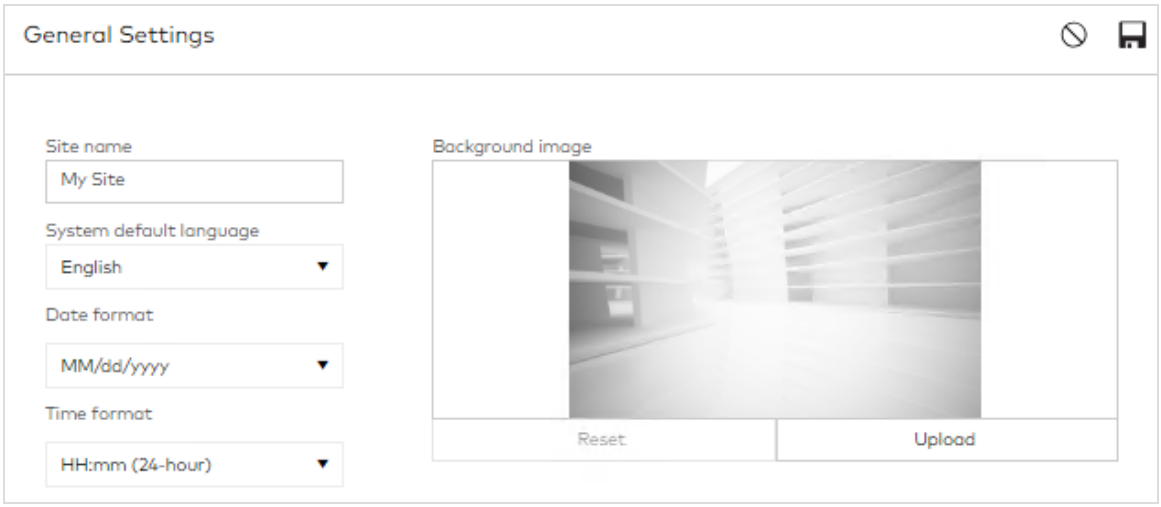
Change key technology settings, configure defaults for pre-registrations, select a PMS protocol, and enable licensed features including mobile keys. This category requires attention if you are licensed for any of the following:

- Mobile keys
- Keyscan Aurora
- Remote Lock Management

General Settings

Configure basic site settings.

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

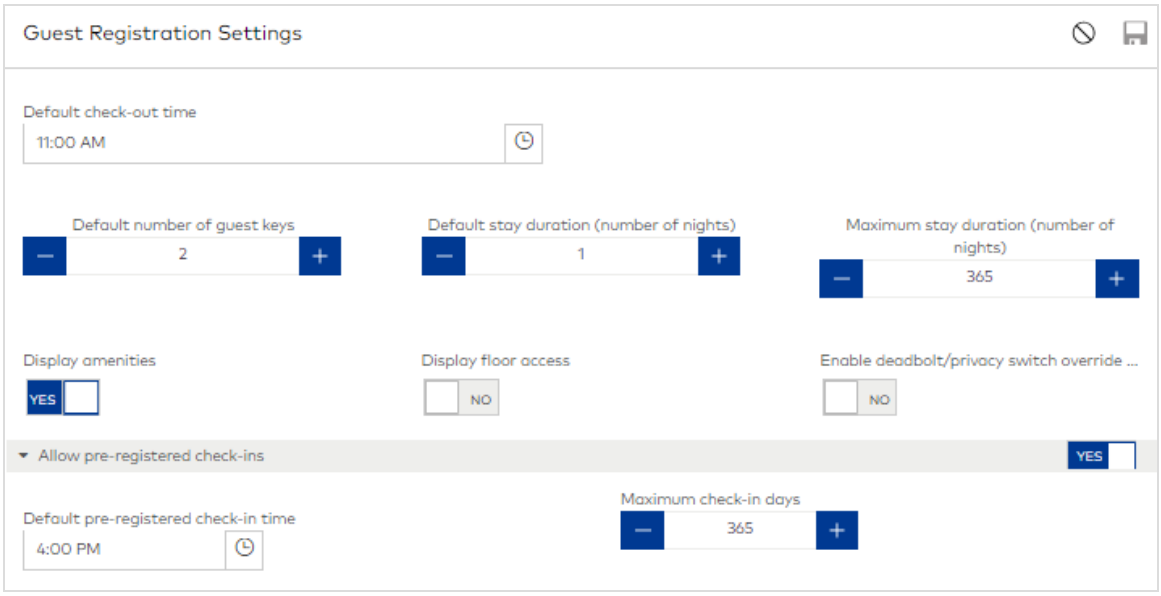


3. For **Site name**, specify the name of the property. The site name appears in reports. Default: My Site.
4. (*international versions only*) For **System default language**, select the language for the user interface. Upon saving your selection, the user interface refreshes. The **Preferred language** option in account Preferences overrides the value selected for this option. Default: English.
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. 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 Ambiance Home page.
8. Click (Save) .

Guest Registration Settings

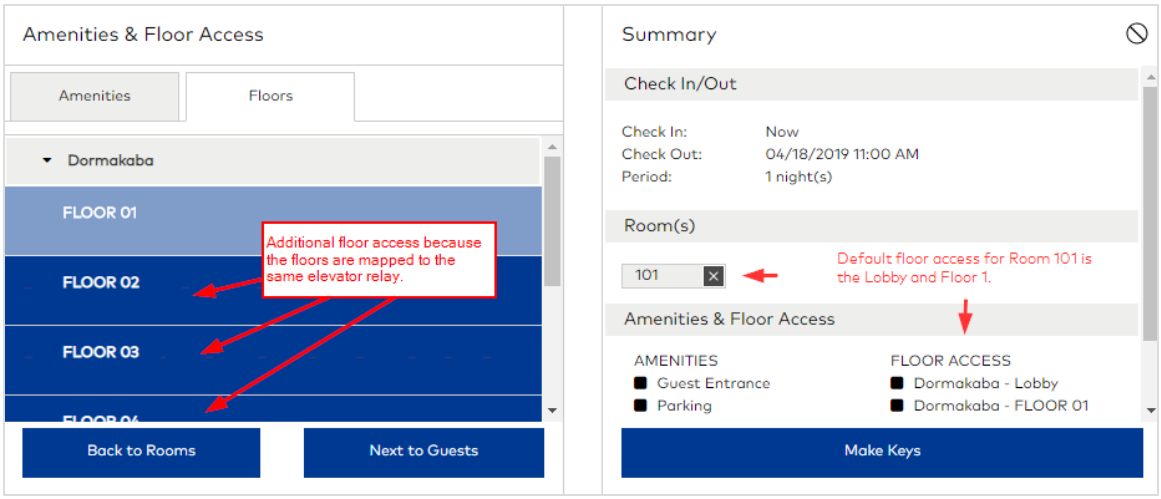
Configure system-wide defaults for the Guest Registration module.

1. Go to System Settings.
2. Click **Guest Registration**.



3. Select the default check-out time for all guest registrations. The value can be modified when registering a guest. Default: 11am.
4. Select the default number of guest keys to make for each guest in a single guest registration. The value can be modified when registering a guest. Default: 2.
5. Specify the default number of nights for a single guest registration. The value can be modified when registering a guest. Default: 1.
6. Specify the maximum number of nights for a single guest registration. Default: 365.
7. Select whether to display amenities (guest common areas) associated with a guest registration. Default: YES.
8. (*only when elevators are configured*) Select whether to display floors associated with a guest registration. Default: YES. By default, guests have elevator access to floors on which they are assigned a room. When the floors that a guest can

access are mapped to the same elevator relay as other floors, the guest has access to all floors mapped to the same relay. The following figure shows a guest registration that displays floor access.



9. Select whether Guest Keys can override the deadbolt/privacy switch for guest room and suite room doors. If you change this setting, access points may need to be reprogrammed. Default: NO.
10. Select whether to enable pre-registrations. This feature lets you create (and modify) registrations for a guest stay in the future. Default: YES.
11. Select the default check-in time for all guest registrations. The value can be modified when registering a guest. Default: 3pm.
12. Specify the maximum number of days in the future for which you can pre-register a guest stay. Default: 365.
13. Click (Save) .

Security Settings

Security settings protect account access. All settings in this category (except **PCI-DSS**) are populated with recommended or moderate values. Customize settings in the following sections or reset all settings to the initial system default values.

All sample values in the figures reflect the system defaults.

Reset to Factory Defaults

To reset all security settings to system defaults:

» Scroll to the bottom of the page and click **Reset to factory settings**.

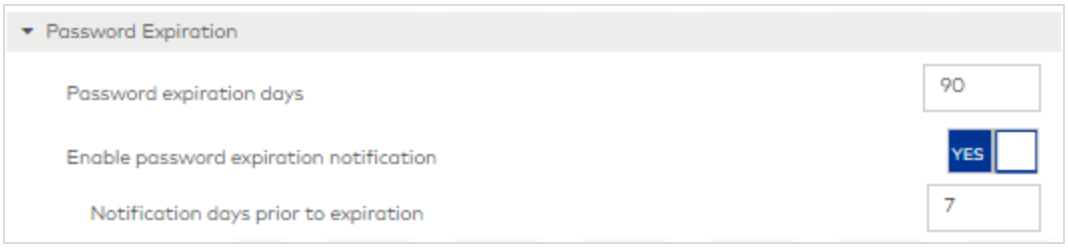
Customize Security Settings

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

Password Criteria

- **PCI-DSS**—Select whether to enable PCI-DSS (Payment Card Industry Data Security Standard), an information security standard for organizations that handle credit cards. Recommended value: YES. When you enable PCI-DSS, the **Enable security questions** option in Password Reset is set to YES and cannot be disabled.
- **Minimum password length**—Specify the minimum number of characters in Ambiance account passwords. Valid values: 7-20.
- **Minimum lowercase characters**—Specify the minimum number of lowercase characters in Ambiance account passwords. Valid values: a-z (maximum 5).
- **Minimum uppercase characters**—Specify the minimum number of uppercase characters in Ambiance account passwords. Valid values: A-Z (maximum 5).
- **Minimum numerical characters**—Specify the minimum number of numeric characters in Ambiance account passwords. Valid values: 0-9 (maximum 5).
- **Minimum special characters**—Specify the minimum number of special characters in Ambiance account passwords. Valid values: ~!@#$%^&_. (maximum 5).

Password Expiration

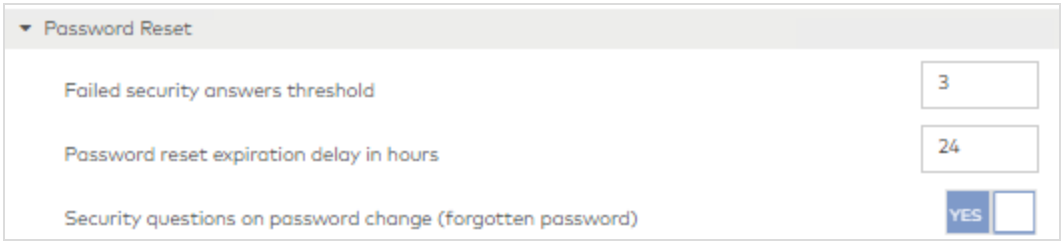


- **Password expiration days**—Specify the number of days after which the password for an Operator account expires. Valid values: 30-365.
- **Enable password expiration notification**—Specify whether to notify Operators when their password is near expiration. Recommended value: YES.
- **Notification 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

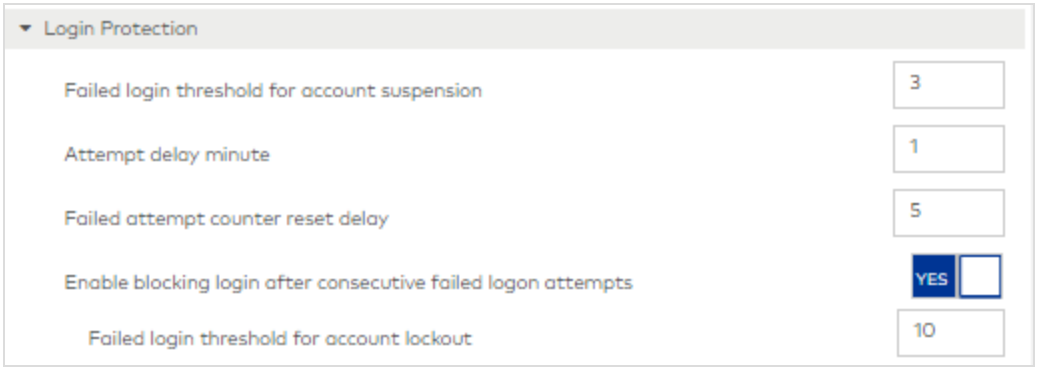
- **Number of previous passwords to check**—Specify the number of most recently used passwords to check when an Operator creates a new password. The new password cannot be the same as any previous password that is checked. Valid values: 4-30.

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: 3-10.
- **Password reset expiration delay in hours**—Specify the number of hours the link sent in response to a password reset request is valid. Default: 24. Valid values: 1-72.
- **Security questions on password change (forgotten password)**—Select whether to prompt the Operator with challenge questions when requesting a password reset. Recommended value: YES. When you enable PCI-DSS, this option is set to YES and cannot be disabled.

Login Protection



- **Failed login threshold for account suspension**—Specify the number of failed login attempts before the Ambiance account is temporarily blocked. Accounts that are suspended are blocked for the number of minutes specified in **Attempt delay**

minute. Valid values: 1-30.

- **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.
- **Enable blocking login after consecutive failed logon attempts**—Select whether to lock out an Operator when the **Failed login threshold for account lockout** is reached.
- **Failed login threshold for account lockout**—Specify the number of failed login attempts before the Ambiance account is locked out. When the threshold is reached, the Operator cannot log in without administrator support. Valid values: 6-30.

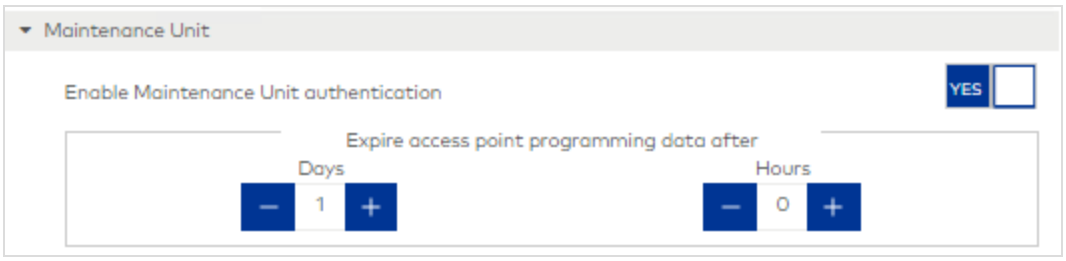
Account Inactivity

- **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: 7-365.

Session Inactivity

- **Inactivity threshold for session logout (minutes)**—Specify the number of minutes after which an active Ambiance session with no activity is locked out. When the threshold is reached, the Operator cannot log in without administrator support. Valid values: 5-360.

Maintenance Unit

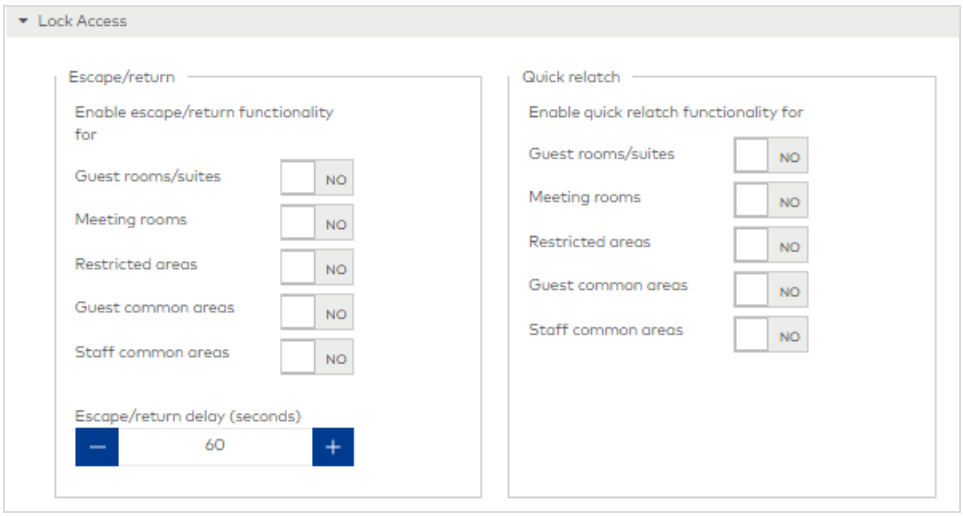


- Select whether to require M-Unit (Maintenance Unit) authentication. When authentication is enabled, M-Unit credentials are required to program and audit locks. Configure credentials for at least one Operator in Staff Management. Default: YES.
- Specify the number of days and hours after which the data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

PMS

- Select whether to require authentication for PMS requests. When authentication is enabled, PMS credentials must be configured in Staff Management for at least one Operator. Default: YES.

Lock Access



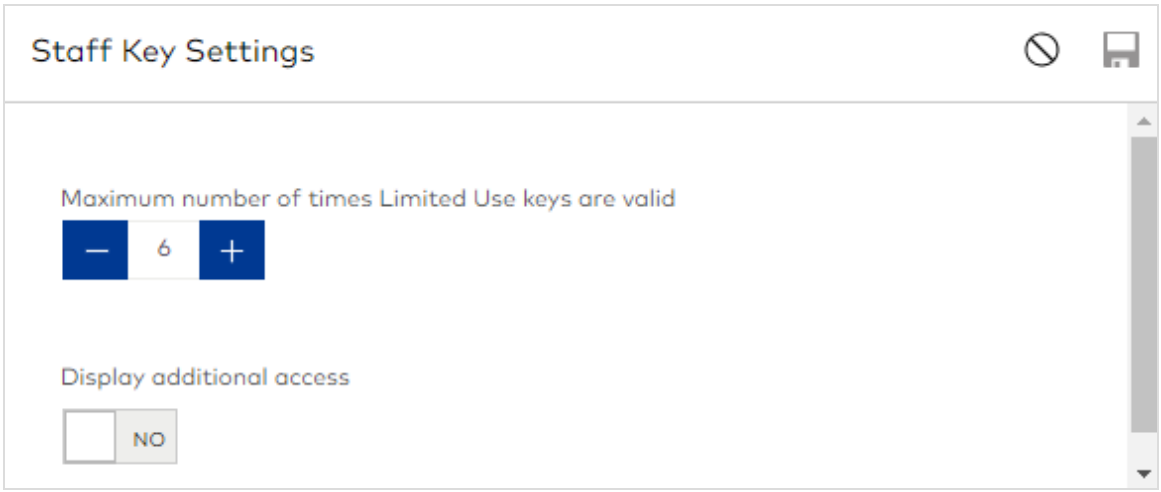
- **Escape\return**—For each access point type, select whether to allow a grace period during which a lock remains accessible without a key when the door is opened then closed from the inside. If any access point is enabled for Escape/return, specify the number of seconds the lock remains accessible. Defaults: NO / 60. Valid values: 20-300 (increments of 20). Changes to this setting may require reprogramming locks.
- **Quick relatch**—For each access point type, select whether the lock is secured immediately after the door is shut. (Default behavior allows 15 seconds before the lock is secured.) Changes to this setting may require reprogramming locks.

> Access points can be programmed for both Escape/return and Quick relatch.

Staff Key Settings

Configure system-wide defaults for Staff Keys.

1. Go to System Settings.
2. Click **Staff Keys**.

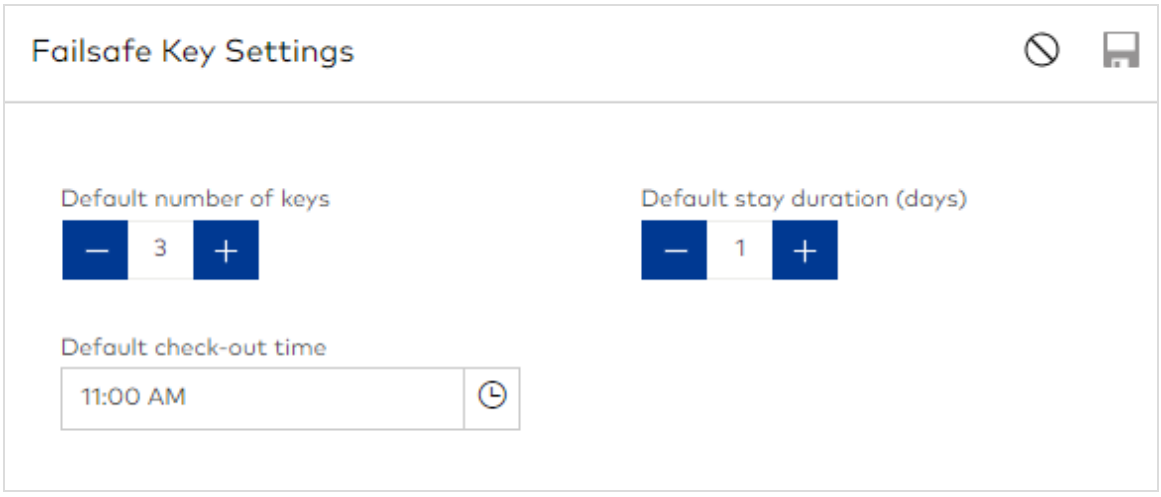


3. Specify the number of times a Limited Use Key can be utilized. Default: 6. Valid values: 1-7.
4. Select whether to include the Additional Access menu in the workflow when making staff keys. When the option is set to YES, access points that are not included in the selected credential can be added to the staff keys. Default: NO.
5. Click (Save) .

Failsafe Key Settings

Failsafe Keys are backups of individual guest room keys that are 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 three sets of two keys for each guest room and suite door.

1. Go to System Settings.
2. Click **Failsafe Keys**.

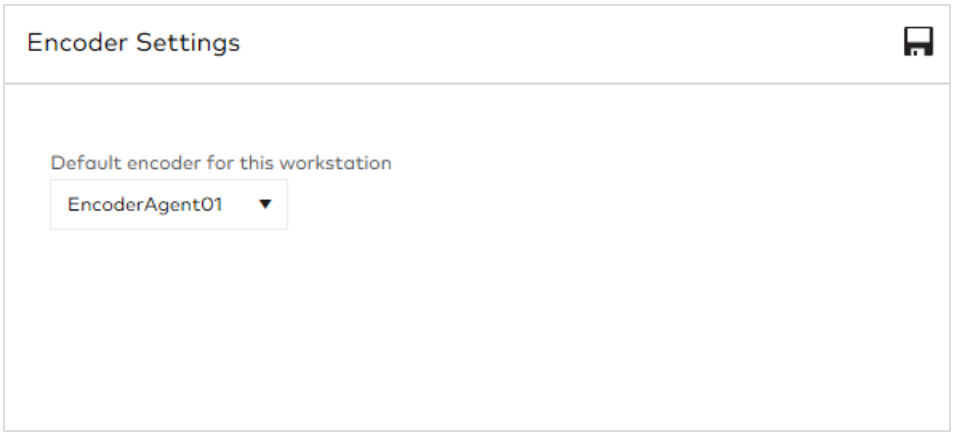


3. Specify the default number of Failsafe Keys to create for each access point. Default: 3.
4. Specify the number of days Failsafe Keys remain valid. After first use, the Failsafe Keys expire after the specified number of days. Default: 1.
5. Select the time after which Failsafe Keys are invalid on the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

Encoder Settings

The default encoder that you select in System Settings is for all workstations. Select the encoder to use as the default.

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



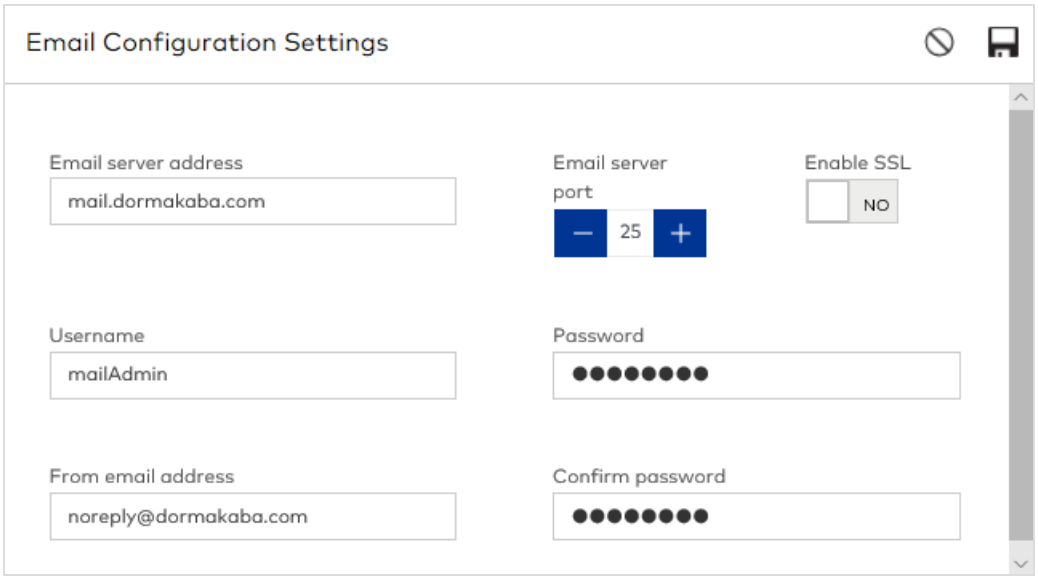
3. Select the encoder to automatically populate when making keys. If you do not select a default encoder, you can select an encoder at key-making time. Default: none.
4. Click (Save) .

The default encoder for a workstation can be selected from the main Ambiance toolbar. Navigate to the homepage for any module in which keys are made (Guest Registration, Staff Management, Staff Keys, System Keys), click (Encoder status) in the toolbar, select a default, then click **Done.**

Email Settings

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

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



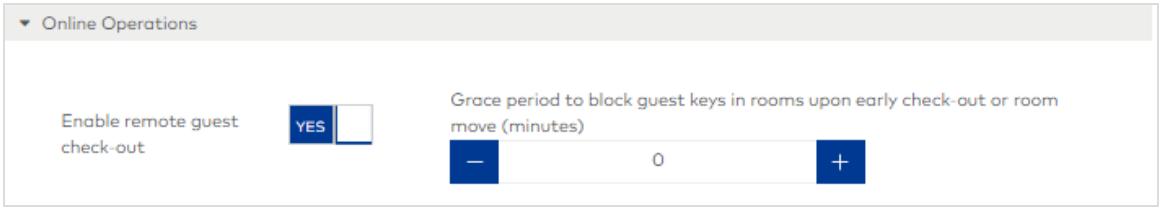
3. For **Email server address**, specify the IP address or host name of the email server.
4. Specify the communication port on the email server dedicated for automated emails.
5. Select whether to enable SSL (Secure Sockets Layer). When SSL is enabled and security certificates are valid, all email data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

Online Communication Settings

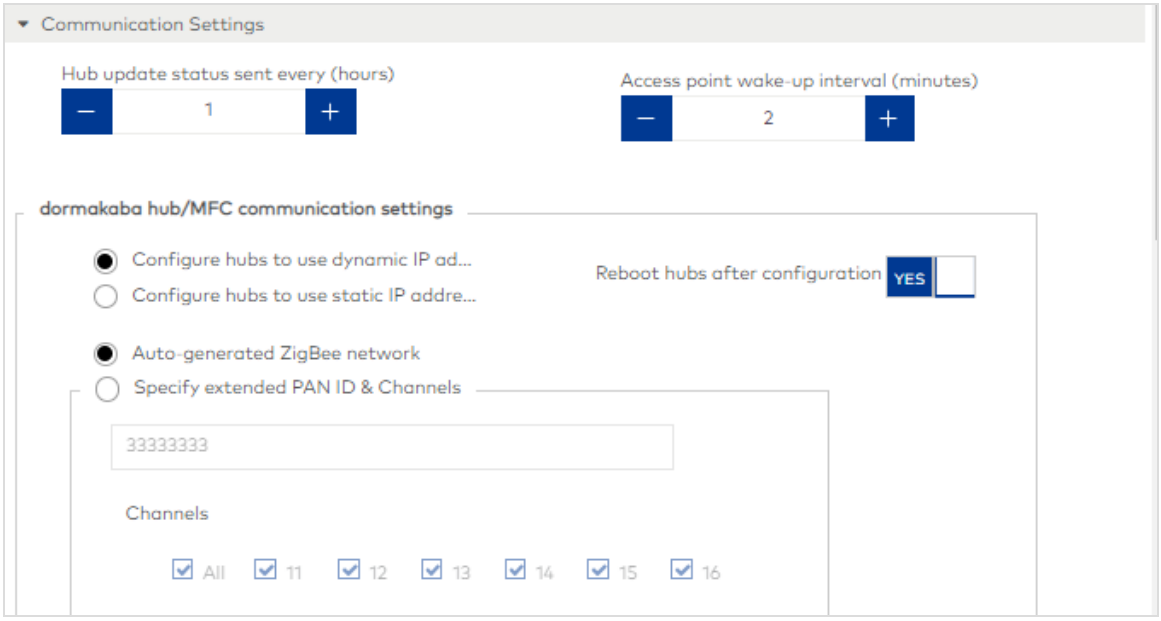
> This category only displays if Remote Lock Management is enabled in System Settings > Advanced Settings.

To configure online communication settings that support Remote Lock Management:

1. Go to System Settings.
2. Click **Online Communication**.

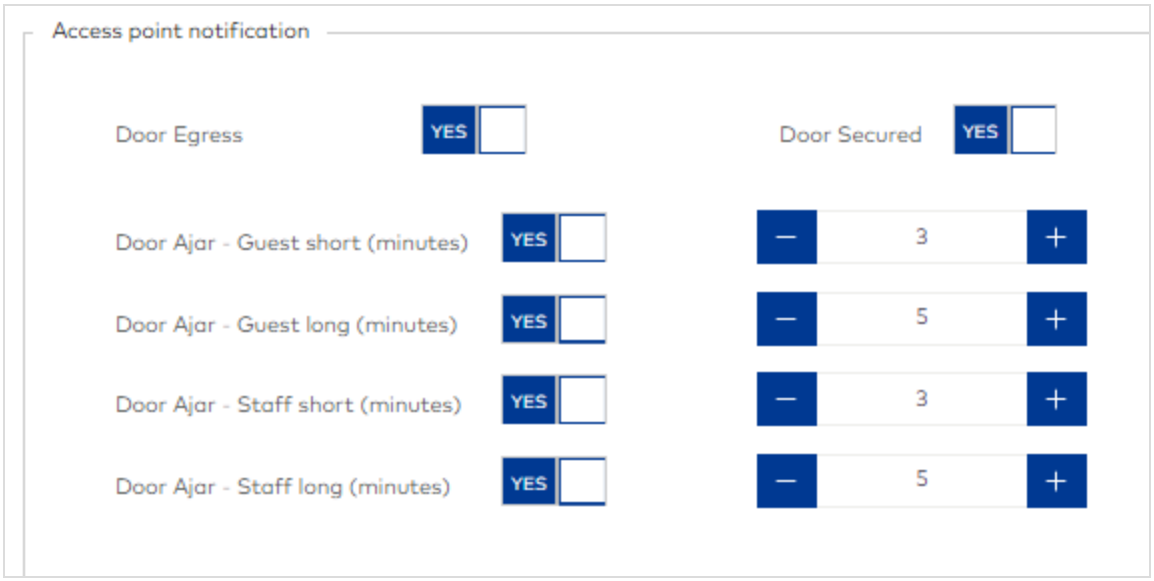


3. Select whether to enable remote guest check-out in Guest Registration. Default: YES.
4. Specify the number of minutes that guest keys remain valid after changes have been made to a guest registration and the keys are updated remotely. For example, if you change the room assignment for a guest, access to the new room begins as soon as the keys are updated remotely. Access to the original room is not canceled until the number of minutes specified as the grace period. Default: 5.



5. Configure the following communication settings:
   - Hub update status sent every—Specify the frequency to update hub status. Valid values: 1-255. Default: 1.
   - Access point wake-up interval—Specify the frequency at which access points verify if the paired hub has received remote operation requests. Default: 2.
   - Reboot Hub Immediately—Select whether a hub restarts after the **Set communication settings** command has been sent to the hub in Device Management > Hubs & Paired Access Points.
   - Configure hubs to use dynamic IP addresses (DHCP)—If enabled, hubs resolve their own IP address. A DHCP server is required for this option.
   - Configure hubs to use static IP addresses—If enabled, each hub must be configured with a unique IP address.
   - Select whether to allow hubs to automatically generate the most appropriate ZigBee communication channels or specify a unique extended PAN (Personal Area Network) ID and select the channels for hub 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.

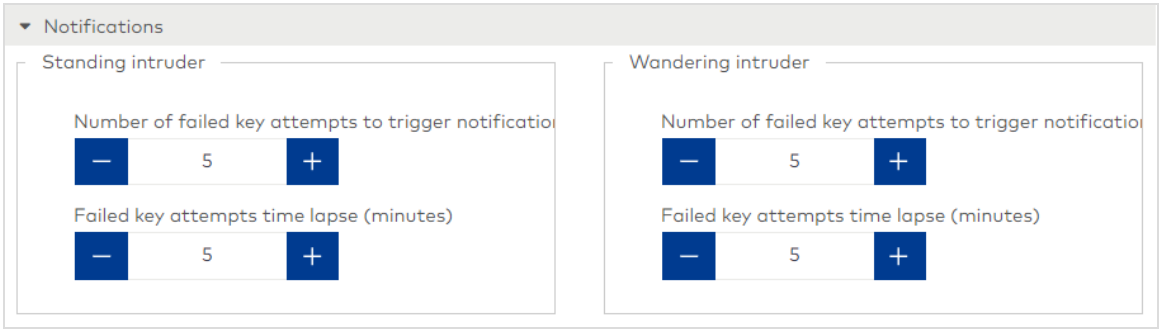
dormakaba recommends using the Auto-generated ZigBee network.



6. Select the access point notifications that you want to receive:
   - 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 - Guest short (minutes)—Select YES to send a notification that a door has been left open by a guest for a short period of time, for example the time it would take to vacate a room. Specify the number of minutes after which the notification is sent.
   - Door Ajar- Guest long (minutes)—Select YES to send a notification that a door has been left open by a guest for a longer period of time, indicating an usual state or potential intrusion. Specify the number of minutes after which the notification is sent.
   - Door Ajar - Staff short (minutes)—Select YES to send a notification that a door has been left open by a staff member for a short period of time, 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 long (minutes)—Select YES to send a notification that a door has been left open by a staff member for a longer period of time, 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.



7. Configure intruder alert notifications. 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.

8. Click (Save).

Database Backup & Archiving

Database backup and archiving are administrative utilities that enable you to protect and manage all Ambiance data. In the event of data loss or corruption, backups provide a full restore of the Ambiance database. You can run backups on demand and automate regularly scheduled backups.

> dormakaba strongly recommends backing up the Ambiance database on a regular basis and storing backups (and archival data) in a secure location off-site.

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

Backup and archival files are stored in their respective directory path locations. Backups are stored for the designated number of months. The most recent backup name and date are displayed when you select the Database Backup & Archiving category in System Settings. Archives are stored indefinitely.

Storing Backups on a Remote Server

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

- The Ambiance Server and remote server must be in the same domain.
- You must create and point to a shared folder on the remote server.
- The Ambiance Server must have full access to the shared folder.

When a remote directory path is specified for database backups, ensure the following requirements:

On the Ambiance Server:

1. Open and log in to SQL Server Management Studio.
2. Navigate to **Security** > **Logins** > **NT AUTHORITY\SYSTEM**, right-click and select **Properties**.
3. Select **Server Roles**.
4. Select **sysadmin**.
5. Click **OK**.

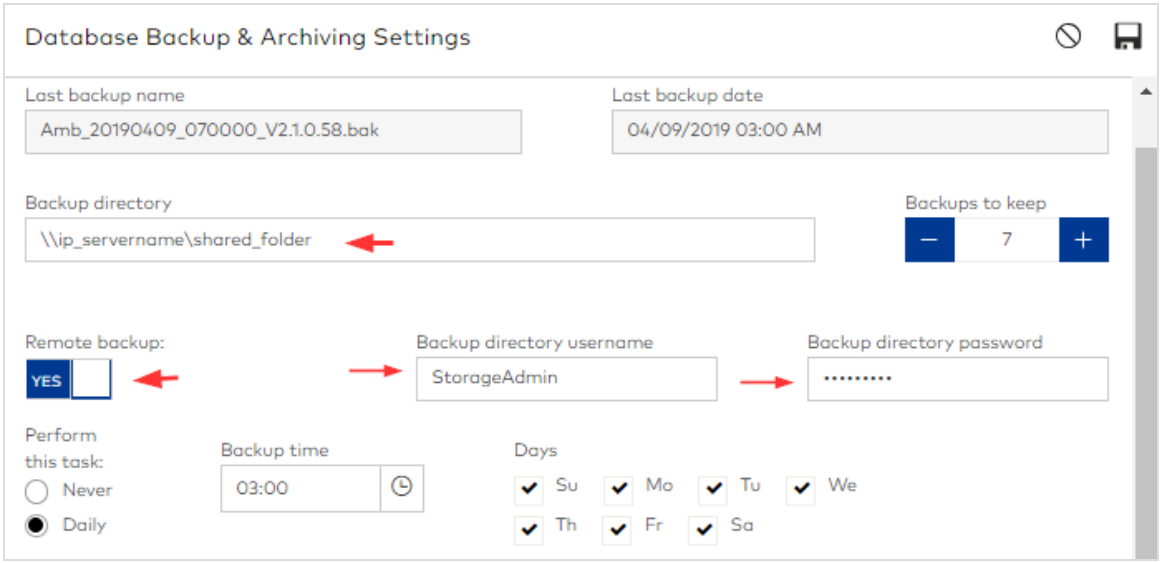
On the remote server:

Share the backup folder and add read/write access for the domain user (the same account specified in System Settings > Database Backup & Archiving).

Configure Backups

Configure scheduled database backups.

1. Go to Systems Settings.
2. Click **Database Backup & Archiving**.



3. For **Backup directory**, specify where you want to store database backups. You must specify the full path to a location accessible by the Ambiance server. You can specify a local or remote path. If you specify a path to a remote server, set the **Remote backup** switch to **YES** and provide valid credentials to the remote server.

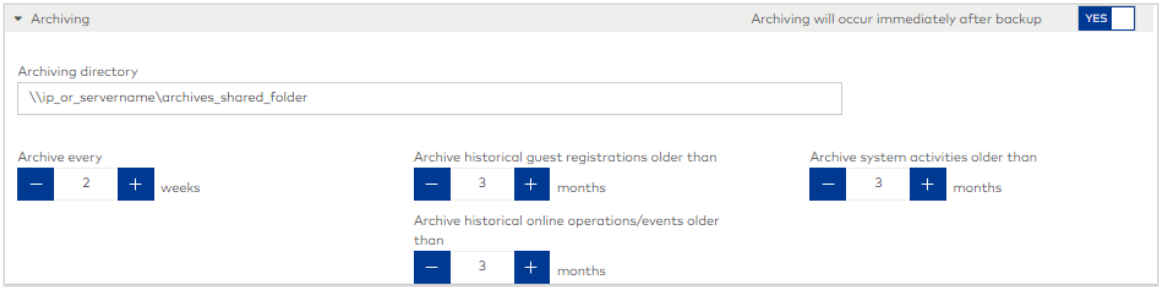
   > To verify the directory path when specifying a remote server, right-click the shared folder, select Properties, click the Sharing tab, then refer to the value for Network Path.

4. For **Backups to keep**, click -/+ to specify the number of 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.
5. For **Perform this task**, specify backup frequency and schedule. If you select **Never**, no backups are regularly scheduled and archiving cannot be enabled. You must back up the database manually or use an external process. If you select **Daily**, select the time and days on which to perform a scheduled backup. Default: Daily, 03:00 (3AM), all days.
6. Click (Save) . Upon saving settings, Ambiance validates the specified directory path.

Configure Archiving

To configure archiving:

1. Go to System Settings.
2. Click **Database Backups & Archiving**.



3. For **Enable archiving**, select whether to enable archiving. Recommended value: YES. If archiving is not enabled, the database will grow to the system limit and space will be unavailable for normal processing.
4. For **Archiving directory**, specify the full path to a location accessible by the Ambiance server. You can specify a local or remote path. Default: Ambiance root\Archives.
5. For **Archive every**, click -/+ to specify the weekly frequency for archiving historical data.
6. For **Archive historical guest registrations older than**, click -/+ to select the number of months to retain guest registration records in the Ambiance database. All guest registrations that go beyond this threshold are archived. Default: 3.
7. For **Archive 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 archived. Default: 3.
8. For **Archive system activities older than**, click -/+ to select the number of months to retain system activity records in the Ambiance database. All system activity records that go beyond this threshold are archived. Default: 3.
9. Click (Save) .

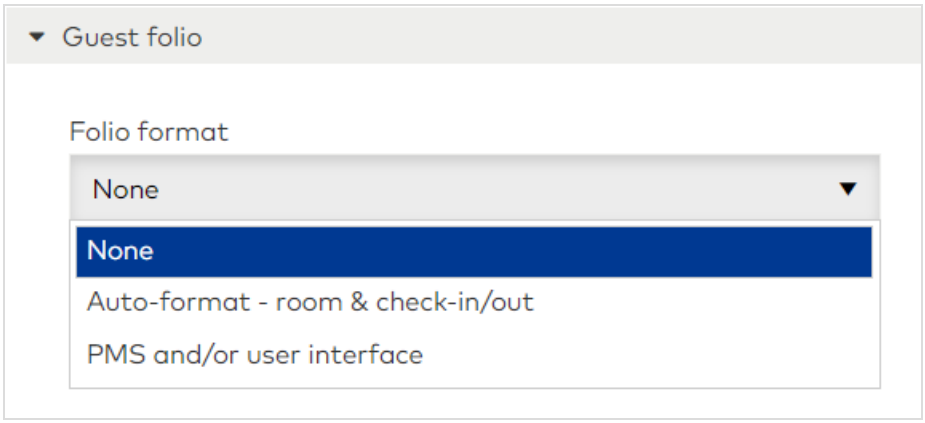
Folio Settings

The Guest Folio enables Ambiance to integrate with third-party POS (point-of-sale) services such as access to vending machines, parking areas or entertainment venues. The individual points of access, or *fields*, defined in the folio layout can be selected during guest registration. For example, a guest folio may include a parking garage, water park and arcade. If the folio is selected during guest registration, access to any or all fields can be selected to integrate onto the key.

> Before defining a guest folio, obtain requirements from your PMS (Property Management System) Administrator and third-party vendors.

To configure a guest folio:

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

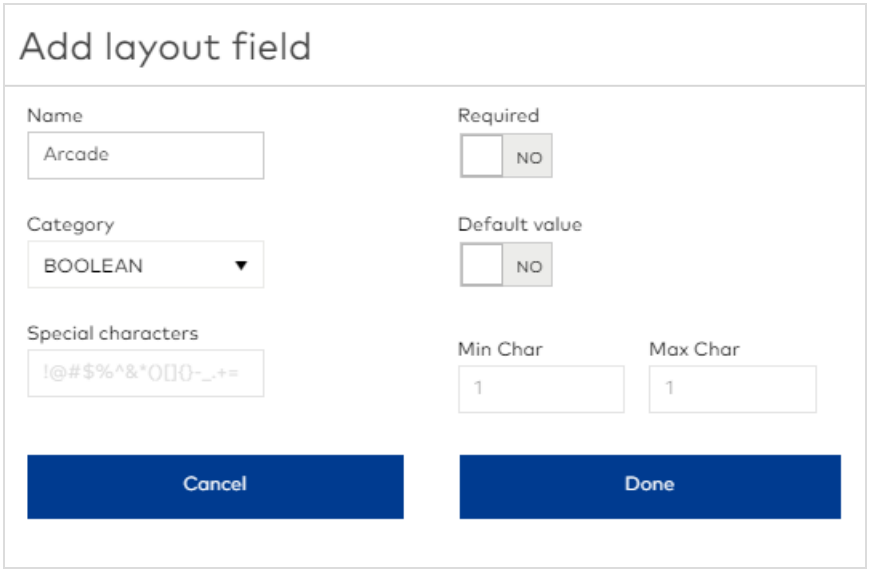


3. Select the required folio format:
   - **Auto-format - room & check-in/out**—When you select this format, the folio is automatically included in all guest registrations. Data includes the guest room number and check-out date/time. If you select this option, click (Save) . You are done.

     > When this format is selected, all access points site-wide must be numeric only.

- **PMS and/or user interface**—Select this option to use a PMS-provided folio number and/or custom folio layout which will appear in guest registration. You can create one guest folio with a maximum of 20 distinct fields. When mobile keys are enabled, you can also reserve character positions for mobile key folios.

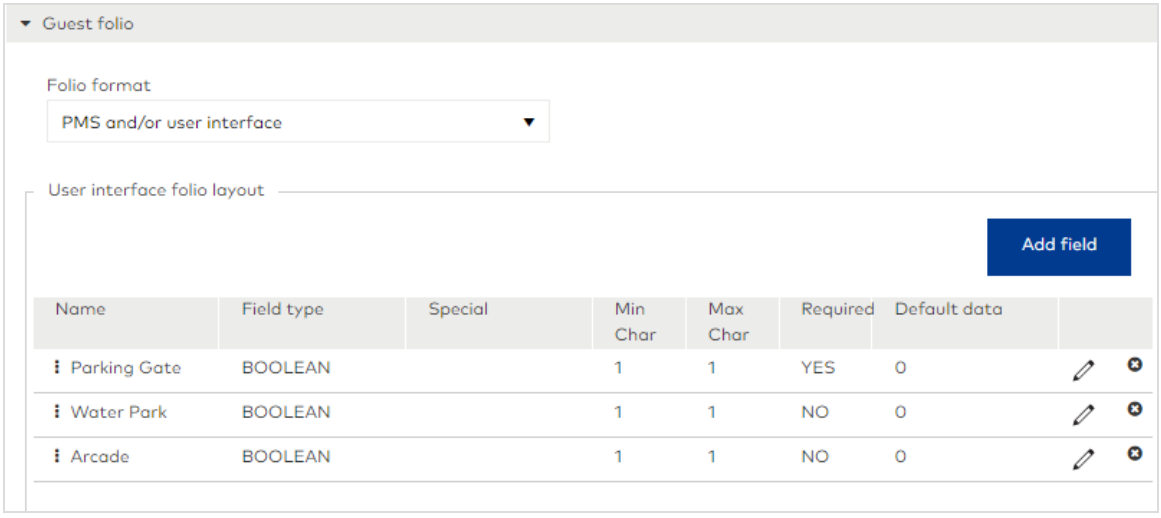
4. For each field that you want to add, click **Add field**.



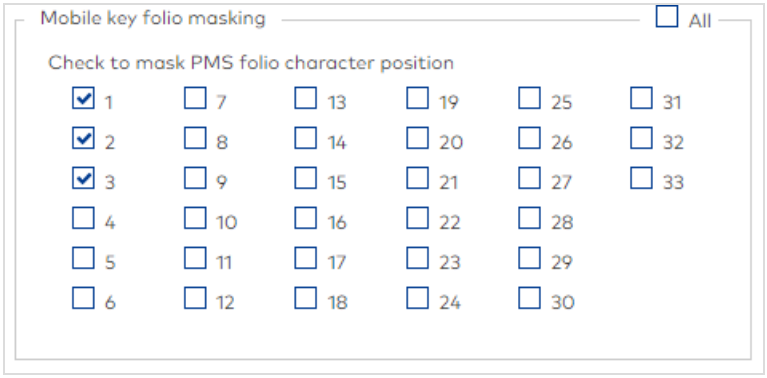
Configure the following options:

- Name—Specify a unique and descriptive name.
- Required—Toggle the soft switch Yes/No to require field entry at guest registration. Default: No.
- Category—Select the type of field:
  - Numeric—For example, 01234
  - Boolean—For example, True/False, Yes/No.
- Default value — Applies to Numeric field types only.
- Special characters—Valid values: !@#$%-+=*
- Min Char/Max Char—Valid values: 0 (zero)-48

When ready, click **Done**. Repeat this step for each field that you want to define. You can define a maximum of 20 fields.



5. (*conditional*) If mobile keys are enabled, reserve character positions for storing folio data. To reserve all positions, select **All**.



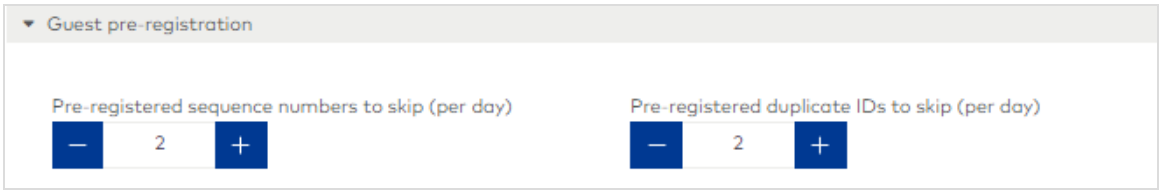
6. Click (Save).

Advanced Settings

To configure Advanced settings:

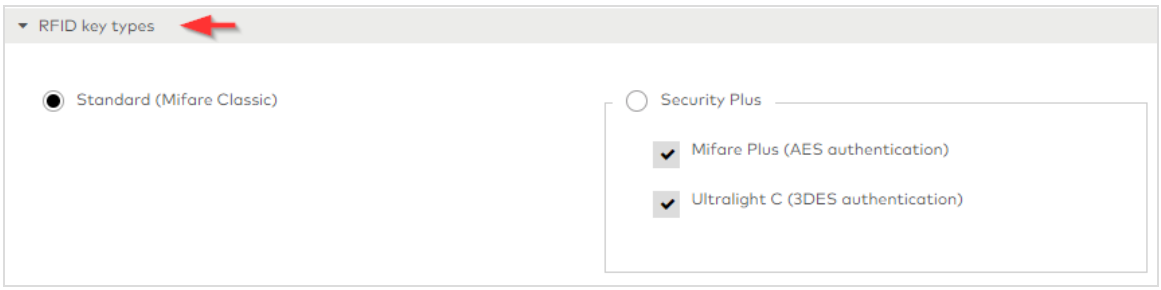
1. Go to System Settings.
2. Click **Advanced**.

Guest Pre-Registration



1. Specify the number of registrations that can be created for the same room until the actual check-in of a pre-registration. For example, if the value is 2 and a pre-registered stay with a check-in date/time starts in 3 days, 6 registrations can be created prior to the start of the pre-registration (2 sequence numbers x 3 days).
2. Specify the number of Additional Keys that can be encoded for the same room for a single registration until the actual date of the pre-registration.
3. Click (Save).

RFID Key Types



Changing the RFID key type is rare and requires that all locks be reprogrammed. The default selection Mifare Classic represents the typical Ambiance deployment.

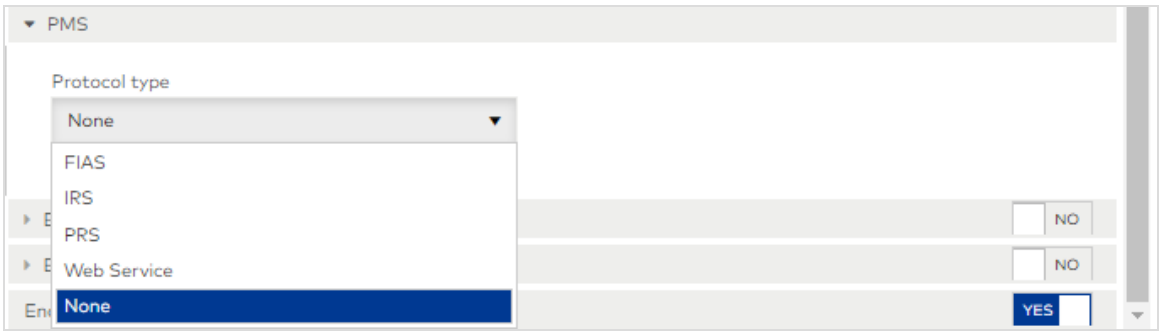
The following key types are supported:

- Mifare Classic
- Mifare Plus (AES authentication)
- Ultralight C (3DES authentication)

> dormakaba recommends upgrading to Mifare Plus for increased security.

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

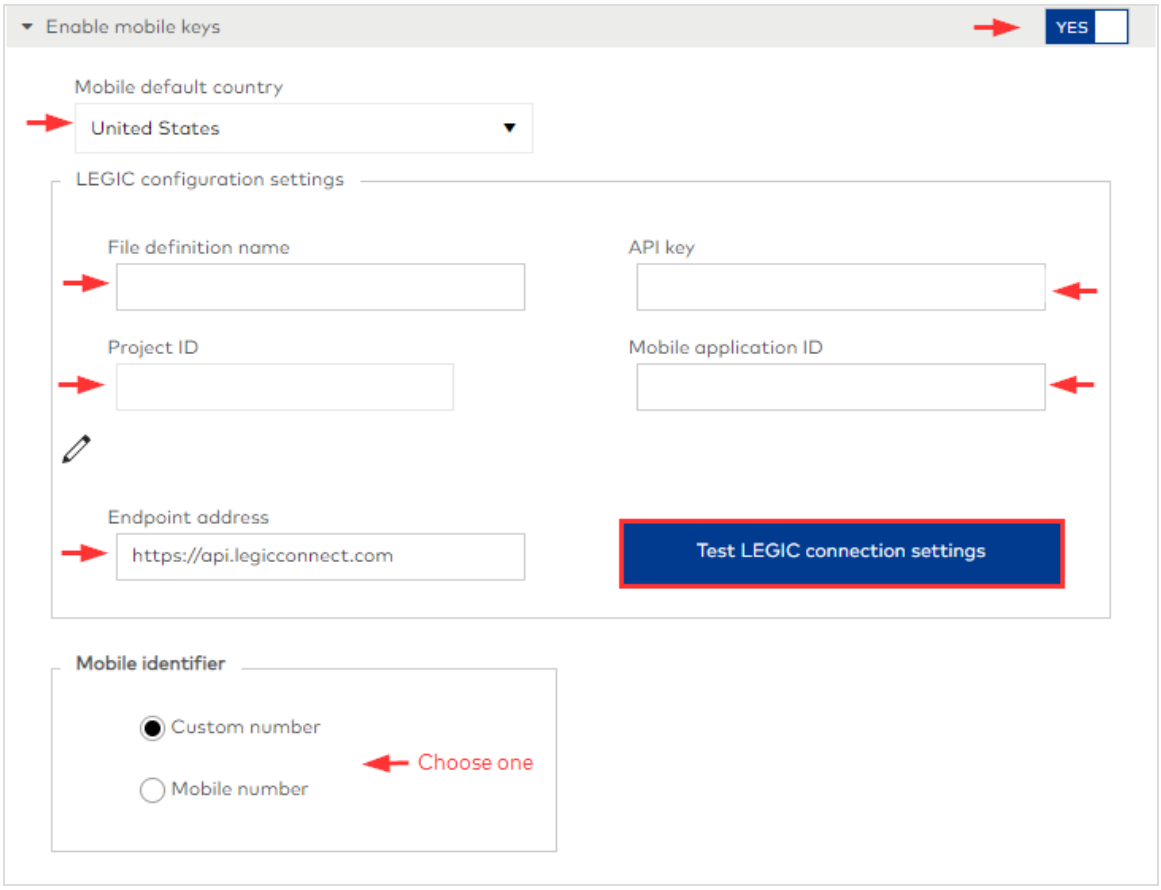
PMS



If using a PMS (Property Management System), select the protocol to use site-wide. When you change the selection, the corresponding service restarts automatically. If you are licensed for remote lock management, the corresponding service restarts automatically when online features are activated or disabled.

- For IP-based connections, select IRS or FIAS.
- For serial port connections, select PRS. (PRS and IRS are the same protocol but use different connection methods.)
- For Web Service connections that use SOAP requests, select Web Service.

Mobile keys

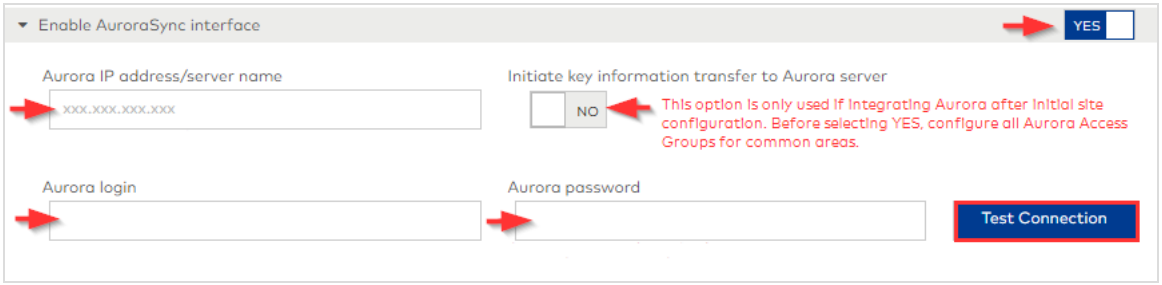


1. Set the **Enable mobile keys** switch to YES.
2. For **Mobile default country**, select the default country for mobile numbers. The corresponding country code is retrieved for the mobile number.
3. For **LEGIC configuration settings**, a dormakaba Customer Service technician provides valid values.
4. For **Mobile identifier**, select whether to use mobile 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.

When mobile keys are enabled, each access point that you create can be enabled for mobile keys. The setting is informational only but is required to include the access point in the download file of mobile-enabled access points (an option available on the *Buildings* page in Property Builder).

For full details about mobile keys, see Working with Mobile Keys.

Keyscan Aurora



To integrate Ambiance with Keyscan Aurora, you must enable Aurora in System Settings:

1. Set the **Enable Aurora Integration** switch to YES.
2. Specify the IP address or server name of the Aurora server. Dynamic and static IPs are supported. If you specify a server name, DNS must be configured.
3. Specify valid credentials to access the Aurora server. Optionally, click **Test Connection** to verify the connection
4. Click (Save) .

If Aurora is integrated with the initial deployment of Ambiance, this is all you need to do. Because data on the Ambiance and Aurora servers is automatically synchronized, you should not initiate key information transfer. If Aurora is integrated with Ambiance after the initial deployment of Ambiance, see Working with Keyscan Aurora.

Remote Lock Management

To enable remote lock management, set the switch to YES. Remote lock management is a licensed feature that supports online operations including remote lock audits and remote Guest Registration operations. For example, changes to can be sent to locks remotely instead of making/issuing new keys. After enabling remote lock management, online communication can be configured in System Settings.

Step 2: Build Your Property

This section includes the following subjects:

Learning about Property Builder

Setting up your site in Ambiance involves building a virtual representation of all access points on the property. Access points represent points of entry under control by Ambiance. 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 guest rooms, suite rooms, common areas, meeting rooms and restricted areas on each floor. You can also add elevators and configure elevator access.

Access Point Types

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

- **Guest Room**—Type of access point assigned to a guest during guest registration.
- **Suite**—A connected series of guest rooms that includes a common door and one or more inner door access points.
- **Restricted Areas**—Type of access point intended for staff only for back-of-the-house access. For example, the Electrical Room would be a restricted area.
- **Meeting Room**—Type of access point intended to accommodate special events for the public and/or registered guests. An Auto-Unlatch schedule can be assigned to a meeting room.
- **Guest Common Areas**—Type of access point where general access is configured for guests. Access may be unlimited or limited.
- **Staff Common Areas**—A type of access point where general access is configured for staff. Access may be unlimited (for staff) or limited.
- **Elevators**—An elevator is an access point type that provides access to building floors. An elevator bank is a group elevators that share the same floor mapping.

Mobile-Enabled Access Points

All access point types can be mobile-enabled. When mobile keys are enabled in System Settings, the option **Enabled for mobile keys** is available when creating and editing access points. Although the option is strictly informational, it is required to include an access point in the file download of mobile-enabled access points from the Property Builder *Buildings* menu.

Lock Models

Ambiance supports the following lock models:

- MT4
- Pixel
- RCU4
- RT, RT+
- Saffire LX
- Confidant

All lock models for Guest Room, Suite Common Door and Suite Inner Door access points support 255 distinct active guest keys. All lock models for Guest Common Areas can manage guest keys for a site deployed with up to 8,192 access points (combination of Guest Room, Suite Common Door and Suite Inner Door access points).

Floor and Access Point Names

During the process of adding floors and access points in Property Builder, the access point names that you will see in Ambiance 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. The following special characters are supported: -#%=!,.:_()?*'<>/+.

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 room number are, by default, included in the access point name. For example, if you select the range 1 to 1 when adding a guest room to Floor1, then you will add one guest room named 101 to Floor1.

> ⚠ If using Guest Folios (configured in System Settings > Folio) and Auto-Format - Room & Check-In/Out is selected, all access point names site-wide must be numeric.

Batch Access Point Creation

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

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 guest room names and/or add a prefix to the guest room 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.

Guest Common Areas

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

Unlimited Guest Common Areas

When limited access *is not enabled*, the common area (amenity) is included with all guest registrations and authorized on all Guest Keys. Unlimited Guest Common Areas are also authorized on all Staff Keys.

Limited-Access Guest Common Areas

When limited access is enabled, access must be configured in Access Management > Common Area Access. Essentially, limited Guest Common Areas are associated with

guest rooms. Guest access depends on the common areas associated with their assigned guest rooms/suite guest rooms. For more information, see Working with Limited-Access Common Areas.

When creating the limited common area, you must also select a common area ID. The ID is a numeric value 1-12 used by the system to synchronize with third-party PMS (Property Management System) settings. There are a maximum of 12 common area IDs to support 12 limited common areas.

Staff access to limited Guest 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 general access only by staff, such as break rooms, supply closets and office spaces. When you create a Staff Common Area access point, you have the option to enable limited access.

Unlimited Staff Common Areas

When limited access *is not enabled*, the Staff Common Area is authorized on every Staff Key.

Limited-Access Staff Common Areas

Access to limited Staff Common Areas is configured in Access Management > Common Area Access. Essentially, limited common areas are associated with a credential. Staff access depends on the common areas associated with the credential selected when making a Staff Key. For more information, see Working with Limited-Access Common Areas.

Common area IDs are not selected for Staff Common Areas.

Ambiance and Keyscan Aurora

Ambiance extends support for Keyscan Aurora. After enabling Aurora integration in Systems Settings > Advanced Settings, configure common areas for Aurora access groups in Property Builder. You can configure Aurora access groups for guest and staff common areas. For more information, see Working with Keyscan Aurora.

Elevators

Configuring elevators to control building floor access involves an elevator technician and Ambiance 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

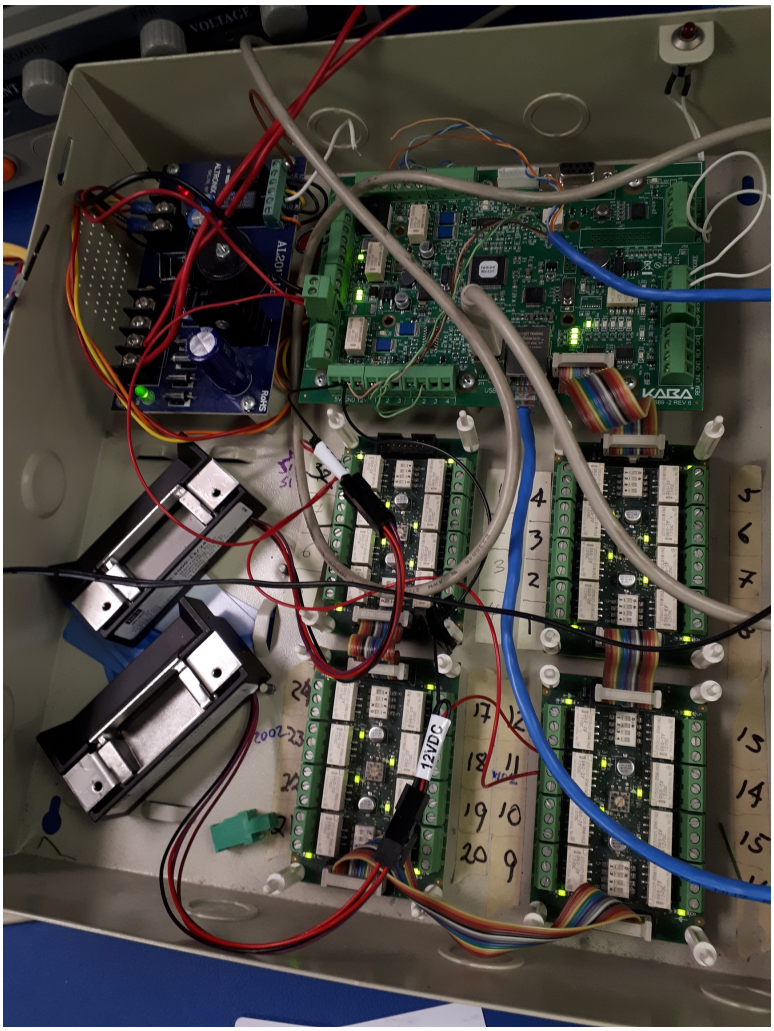
The Site Configurator maps floor access for each elevator bank. While all floor mapping works the same, the control box model selected when adding the elevator bank affects the options available. Generally, as the number of floors that need to be independently controlled increases, the size of the control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

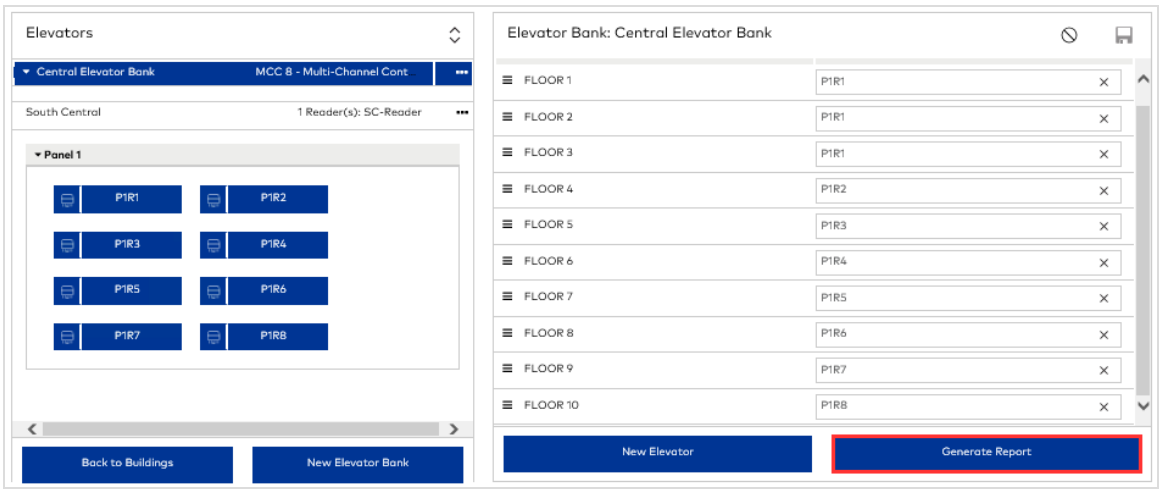
- ECU - Elevator Controller Unit—One panel with one relay.
- MFC - Multiple Floor Controller—Four panels with eight relays per panel.

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 Ambiance, relay switches are mapped to floors.

The following figure shows Ambiance 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.

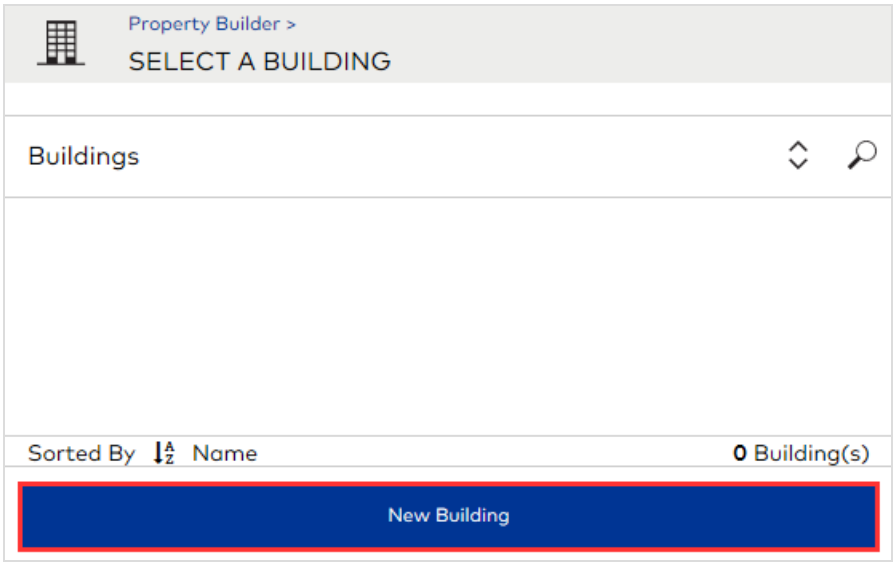
Aside from the basic rule, *a floor can be mapped to only one relay*, relay-to-floor mapping is entirely configurable. The important thing to remember is that a signal from the reader to open the relay opens access to all floors mapped to the relay. For example, if Floors1-3 are mapped to Relay1 and 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

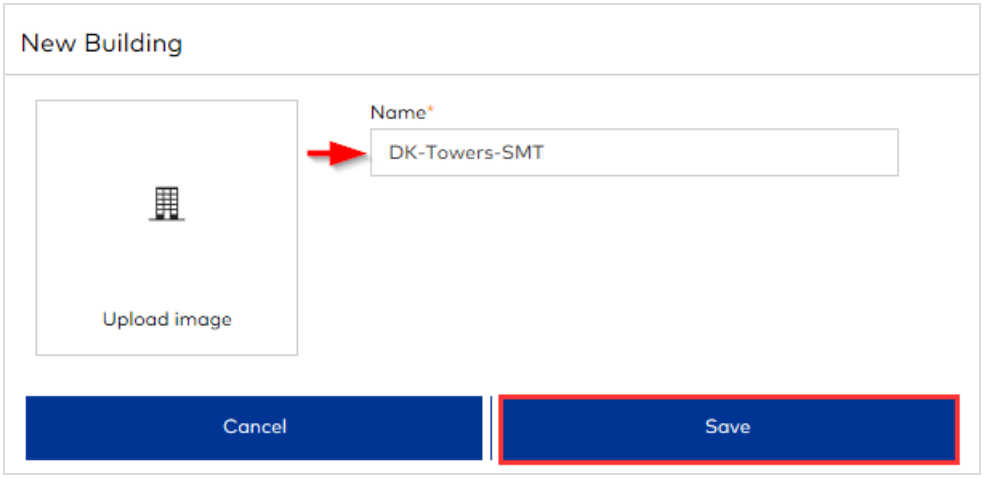
Buildings are the independent structures on your site.

To add buildings:

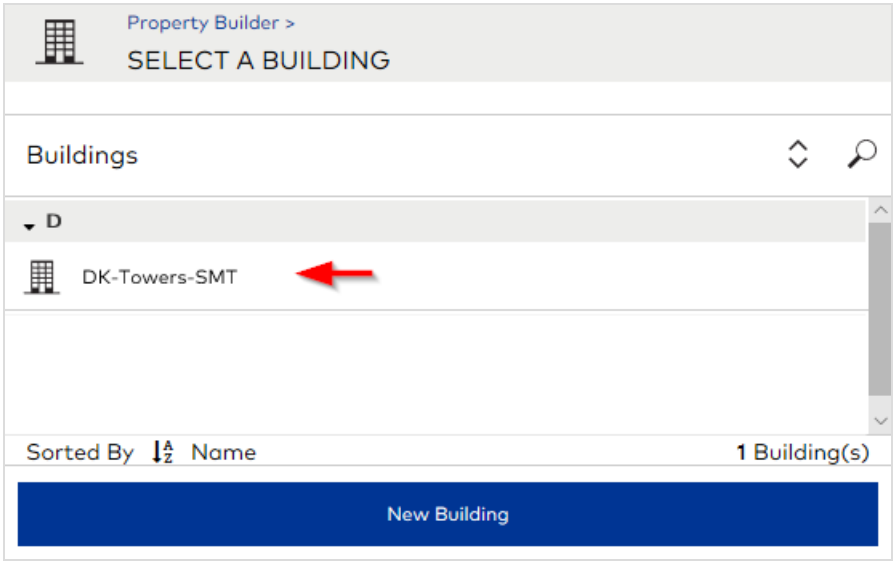
1. Go to Property Builder.



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.

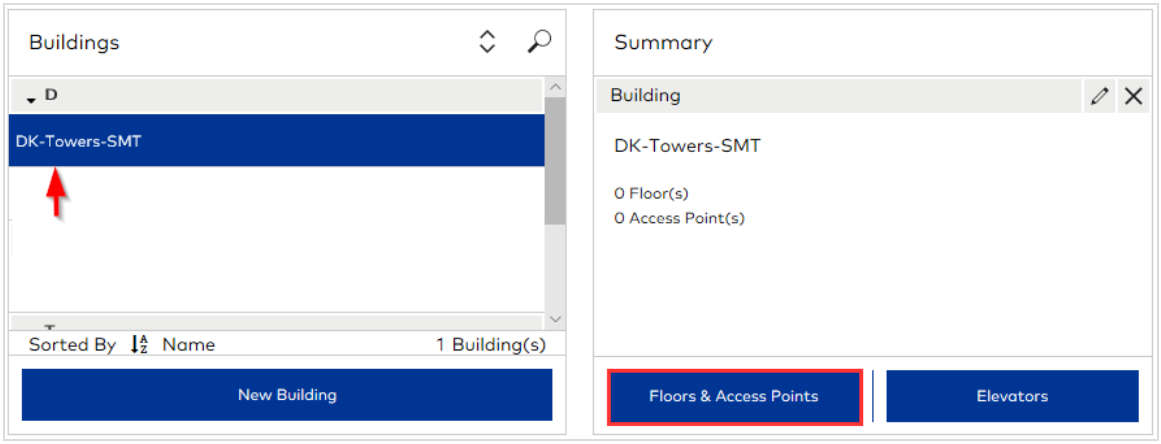


Add Floors

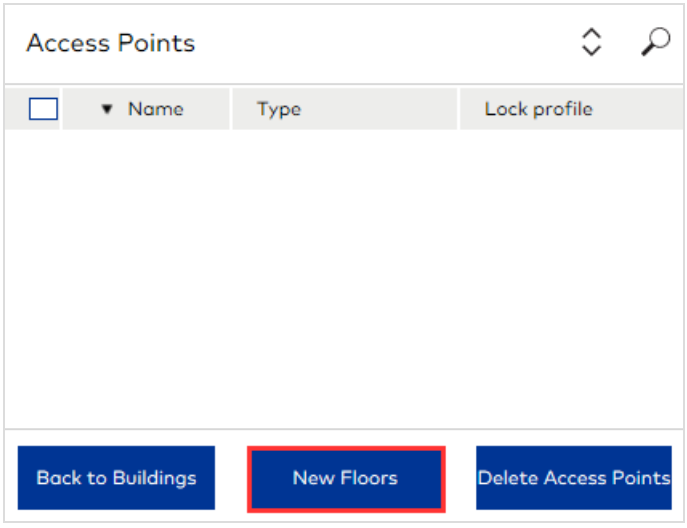
Floors are the levels in a building. You must add floors before adding access points.

To add floors:

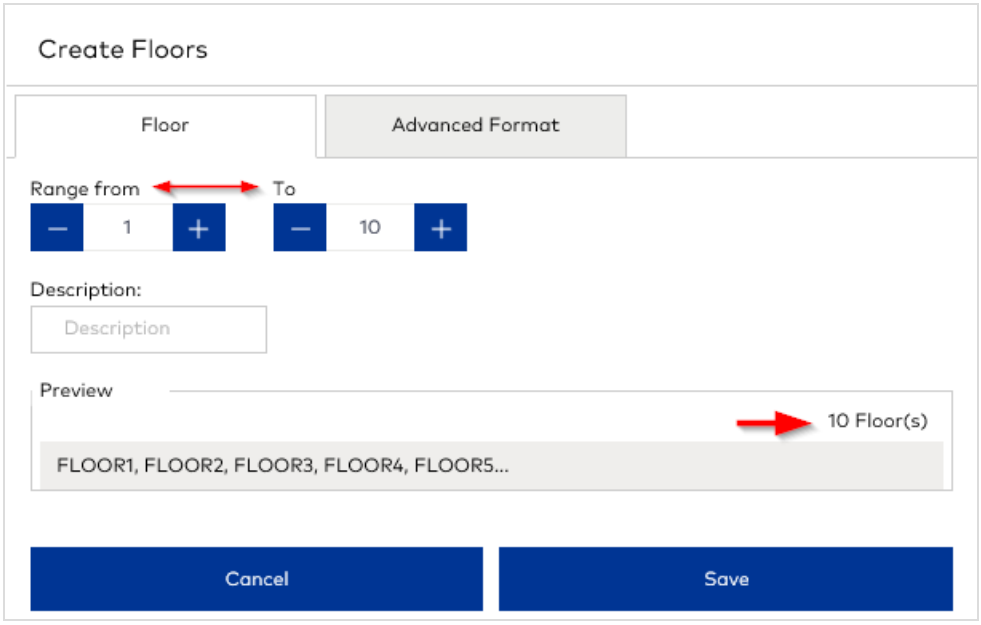
1. Go to Property Builder.
2. Select a building.



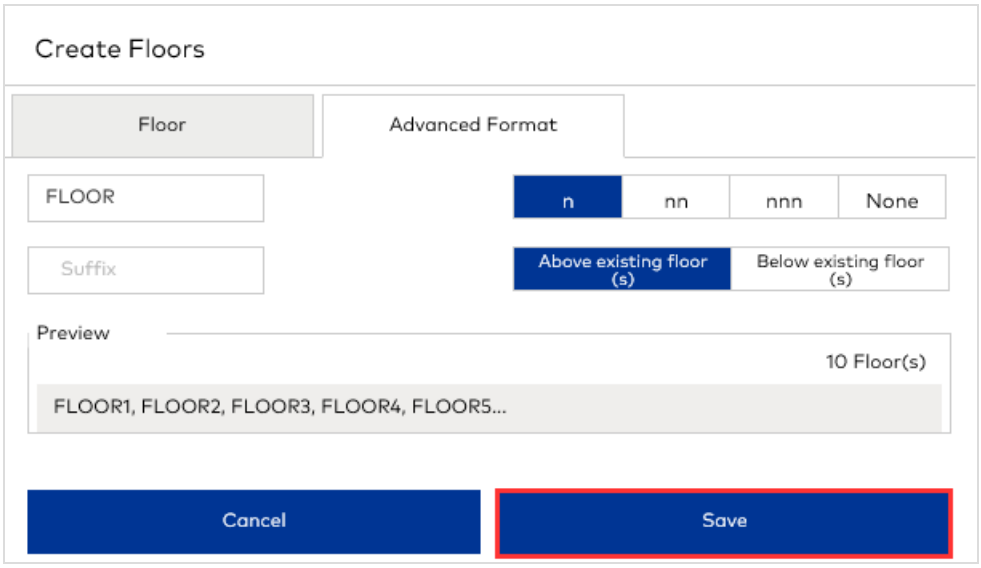
3. Click **Floors & Access Points**.



4. Click **New Floors**.

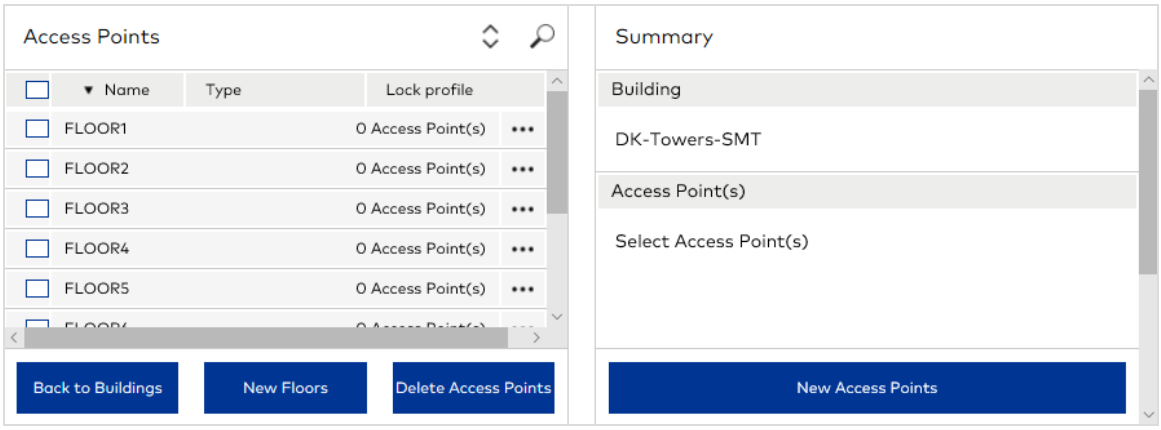


5. Specify the range of floors to add. Because floor names must be unique, you can only select numbers that have been used previously if you also specify a unique prefix or suffix.
6. (*optional*) Add a description for the floor or range of floors.
7. (*optional*) Specify any of the following options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

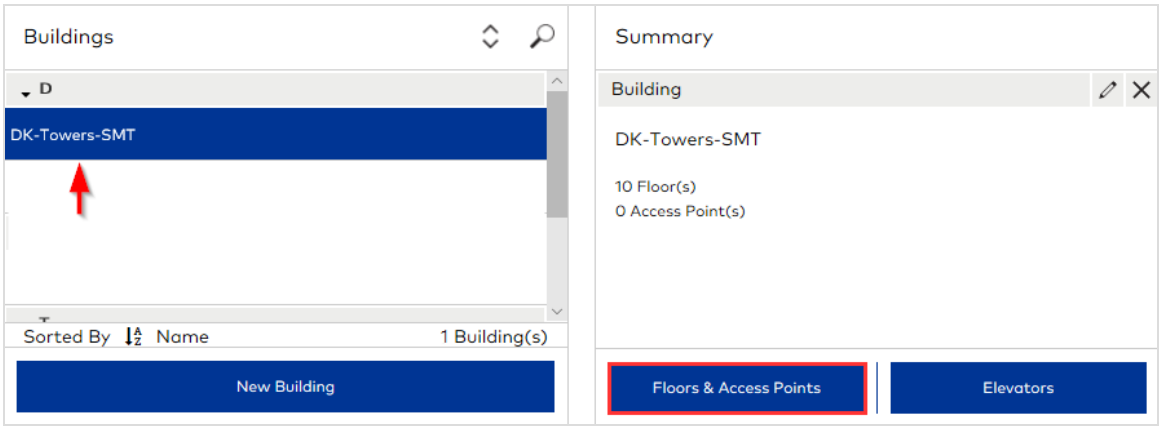


Add Guest Rooms

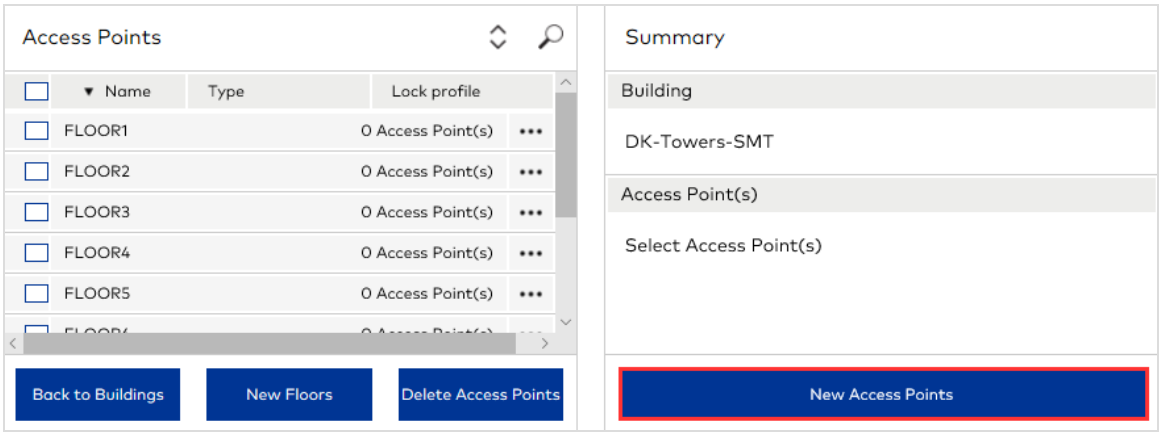
Guest Rooms are the type of access points assigned to guests during guest registration.

To add guest rooms:

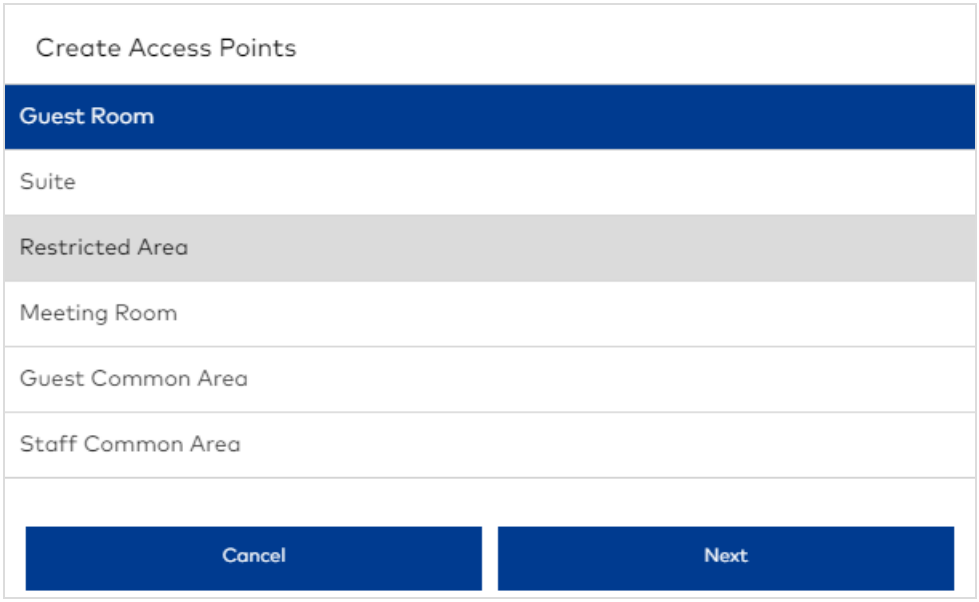
1. Go to Property Builder.



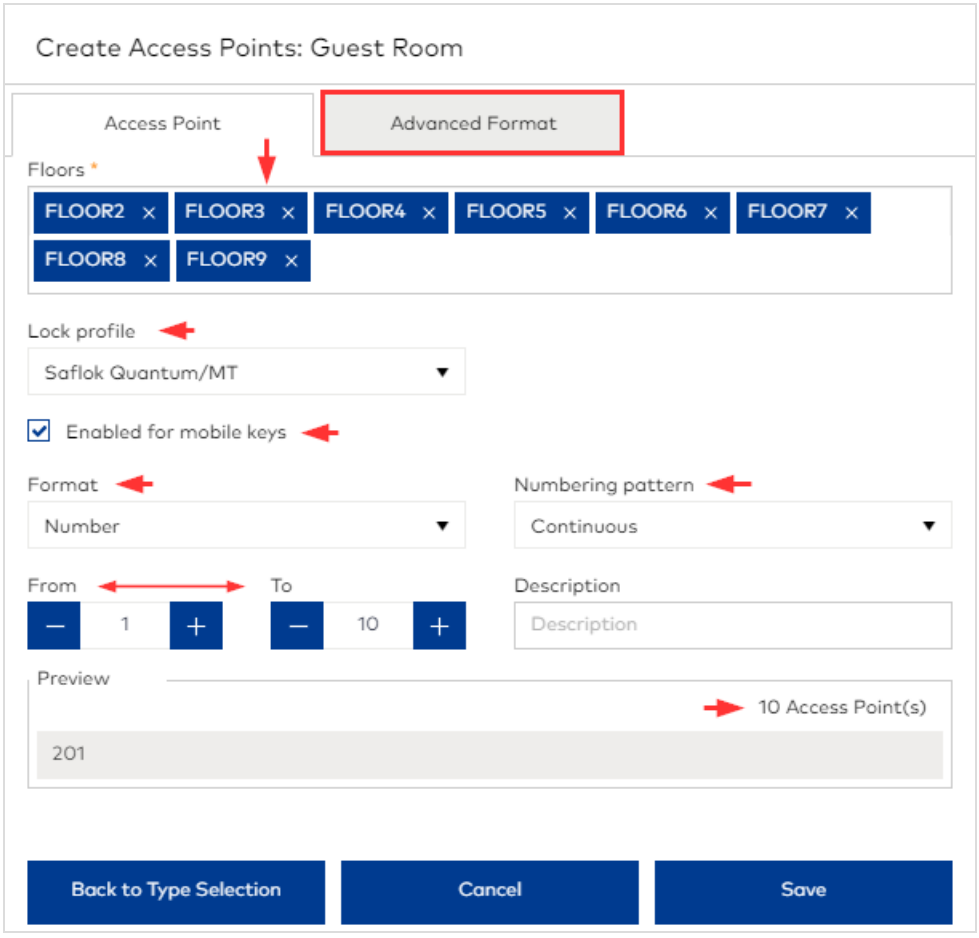
2. Select a building.
3. Click **Floors & Access Points**.



4. Click **New Access Points**.

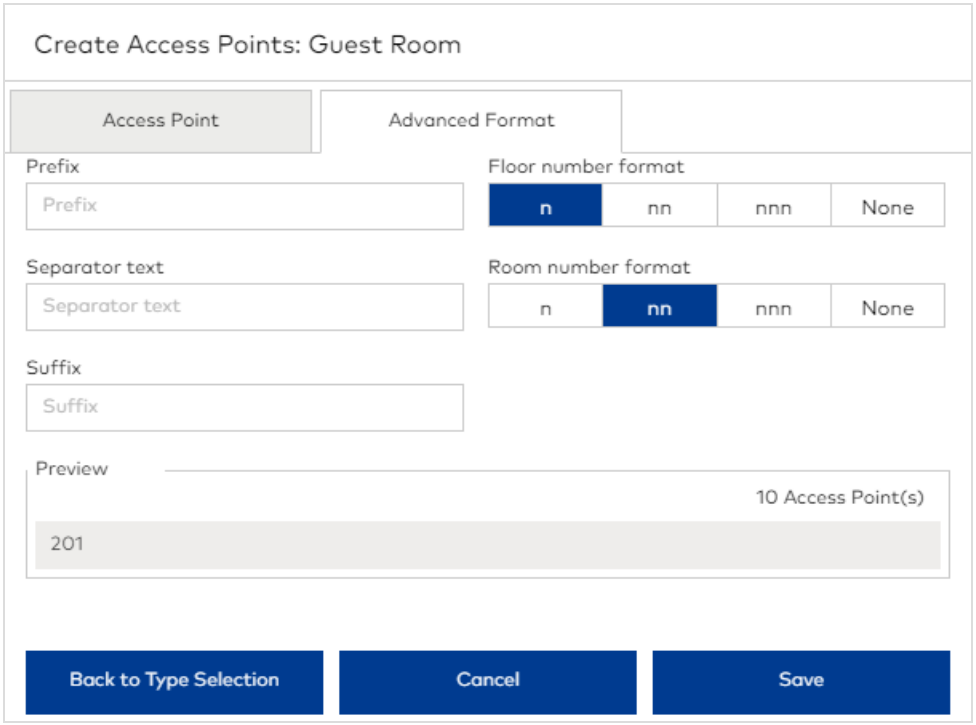


5. Select **Guest Room**, then click **Next**.



6. For **Floors**, select one or more floors where you want to add the access points.
7. For **Lock profile**, select the lock model.
8. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
9. 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.
10. (*optional*) Add a description for the access point or range of access points.

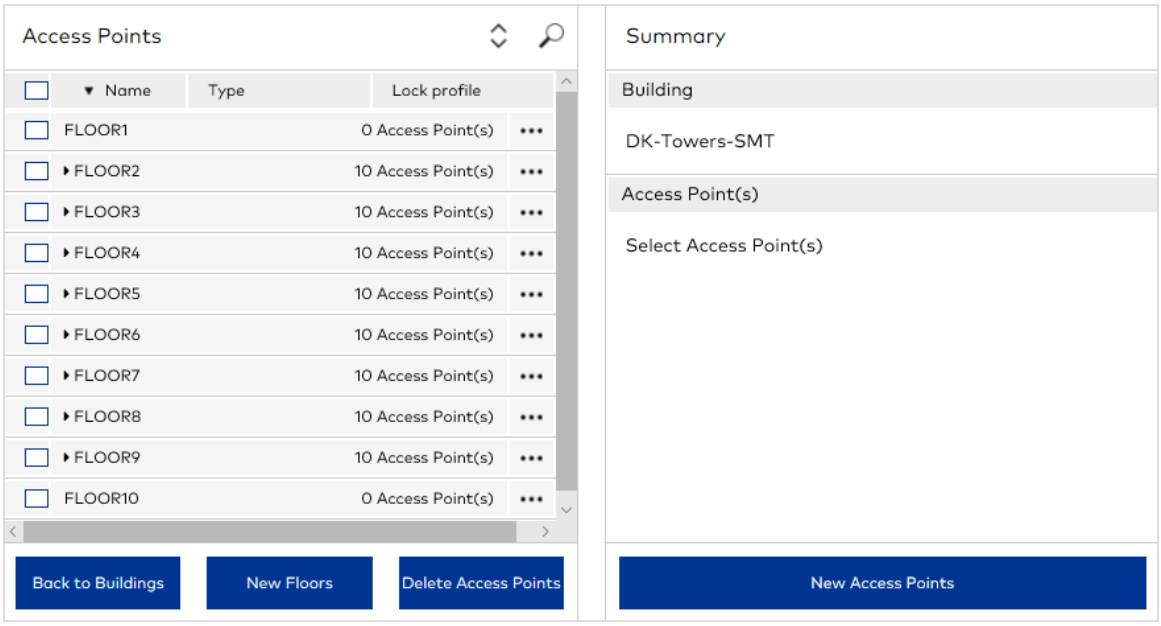
11. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the **Advanced Format** tab:



- **Prefix**—Specify the text to display before the main number. Include spaces where appropriate. Default: none.
- **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.
- **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.
- **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. 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**. Default: n.
- **Room number format**—Select how many digit positions to display for room 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 room number in the access point name, select **None**.

12. Click **Save**.

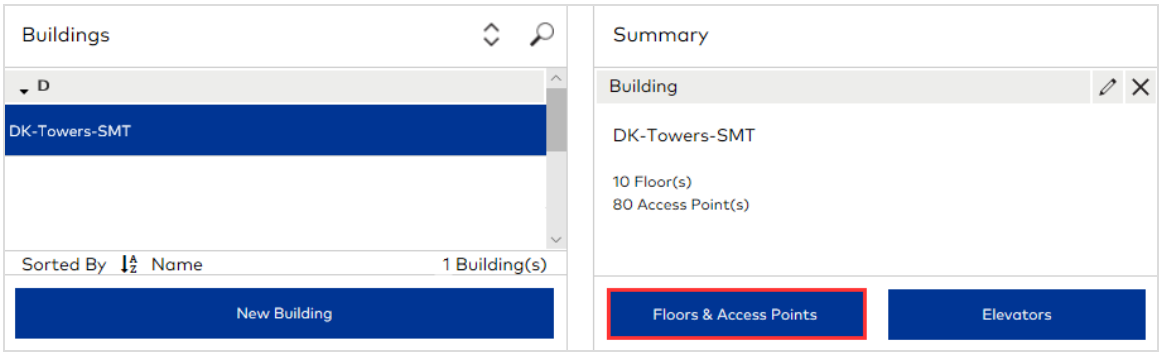


Add Suites

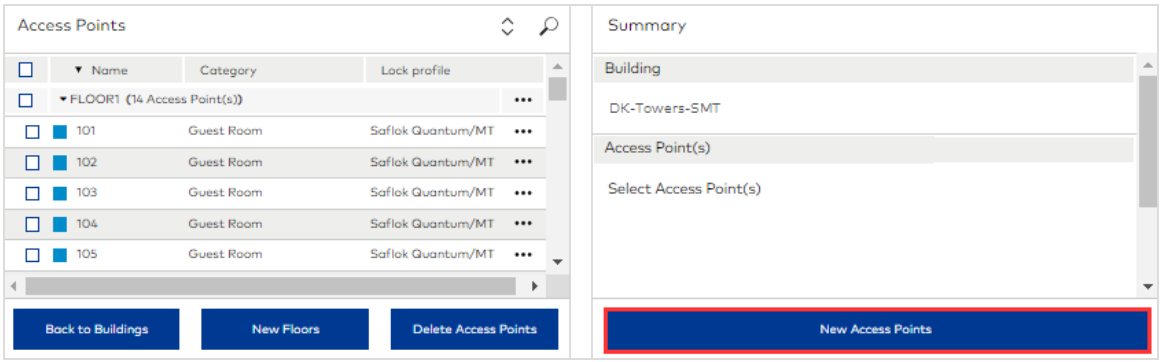
A suite is a connected series of guest rooms that includes a common door and one or more inner doors.

To add suites:

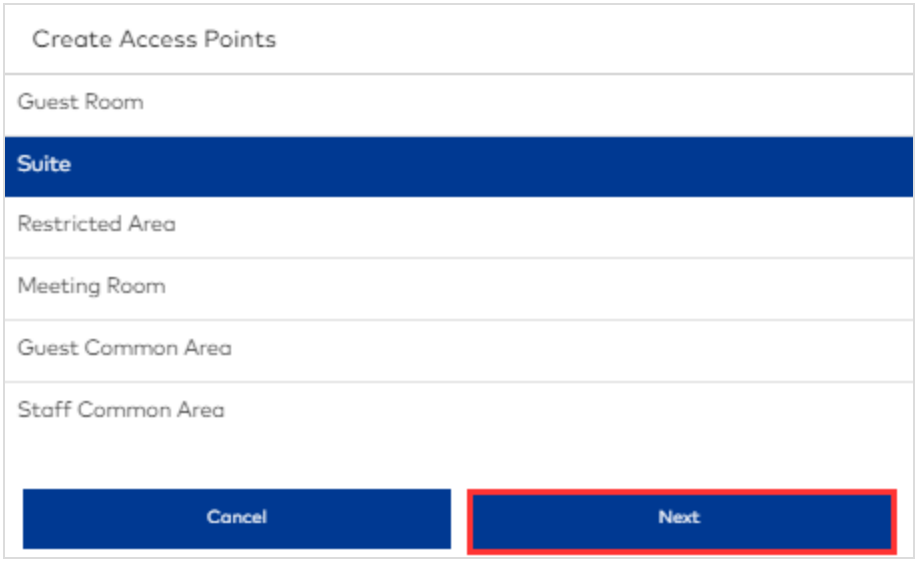
1. Go to Property Builder.



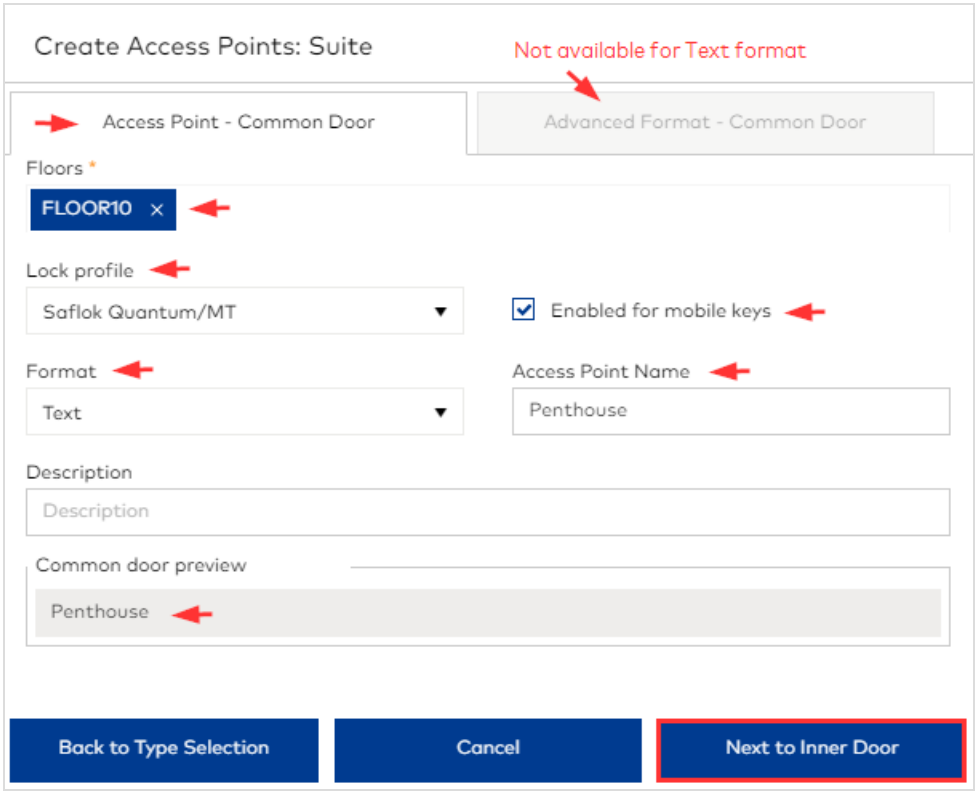
2. Select a building.
3. Click **Floors & Access Points**.



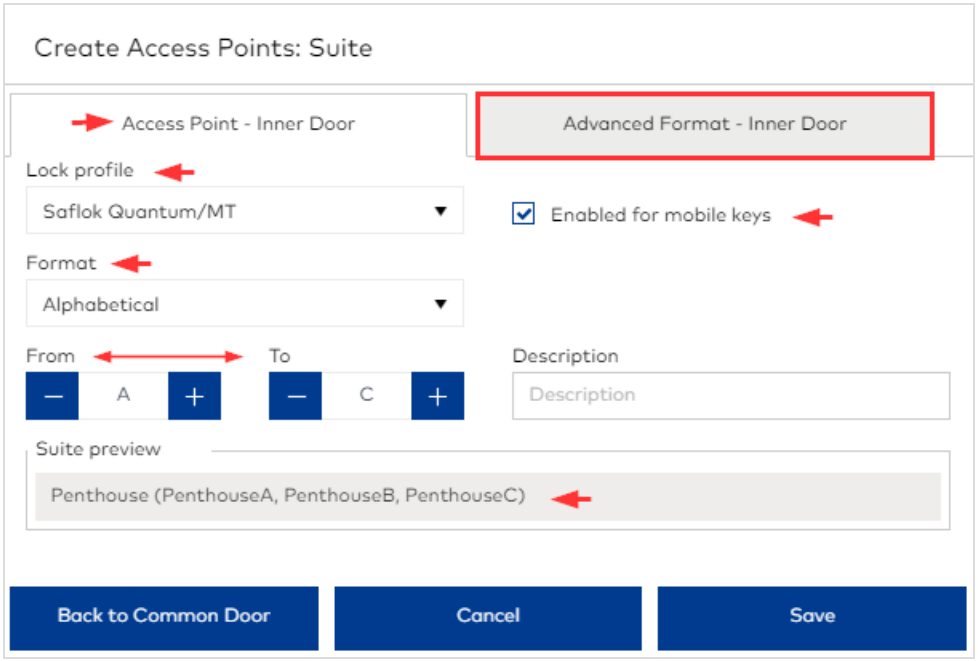
4. Click **New Access Points**.



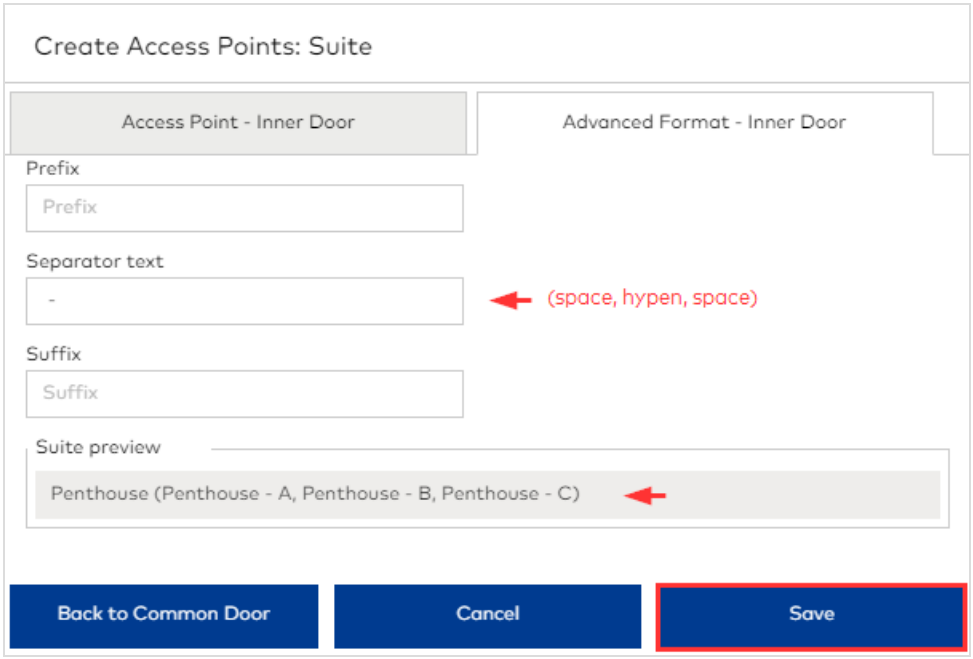
5. Select **Suite**, then click **Next**. The first options that you define are for the Common Door.



6. For **Floors**, select the floor where you want to add the access points.
7. For **Lock profile**, select the lock model.
8. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
9. 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.
10. (*optional*) Add a description for the access point or range of access points.
11. (*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. Default: none.
    - **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.
    - **Suffix**—Specify the text to display after the main number. Include spaces where appropriate. Default: none.
    - **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. 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**. Default: n.
    - **Room number format**—Select how many digit positions to display for room 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 room number in the access point name, select **None**.
12. Click **Next to Inner Door**.

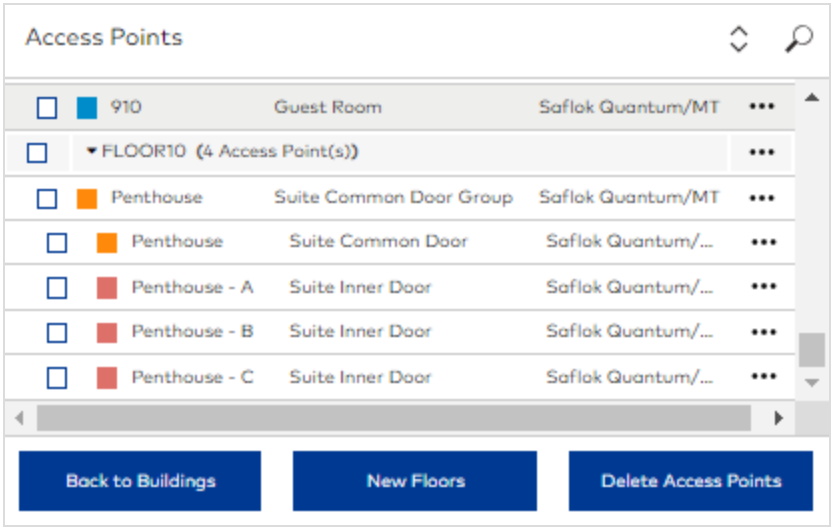


13. For **Lock profile**, select the lock model.
14. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
15. For **Format**, select whether 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.
16. (*optional*) Add a description for the access point or range of access points.
17. (*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. Default: none.
- **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.
- **Suffix**—Specify the text to display after the main number. Include spaces where appropriate. Default: none.
- **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. 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**. Default: n.
- **Room number format**—Select how many digit positions to display for room 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 room number in the access point name, select **None**.

18. Click **Save**.


Access Points
910 Guest Room Saflok Quantum/MT
FLOOR10 (4 Access Point(s))
Penthouse Suite Common Door Group Saflok Quantum/MT
Penthouse Suite Common Door Saflok Quantum/...
Penthouse - A Suite Inner Door Saflok Quantum/...
Penthouse - B Suite Inner Door Saflok Quantum/...
Penthouse - C Suite Inner Door Saflok Quantum/...
Back to Buildings
New Floors
Delete Access Points

Add Guest Common Areas

Guest Common Areas are spaces on your property that are configured for general access by guests and staff, such as lobbies, parking and recreational facilities. In the hospitality industry, these common areas are typically referred to as amenities. 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 Unlimited and Limited-Access Guest Common Areas.

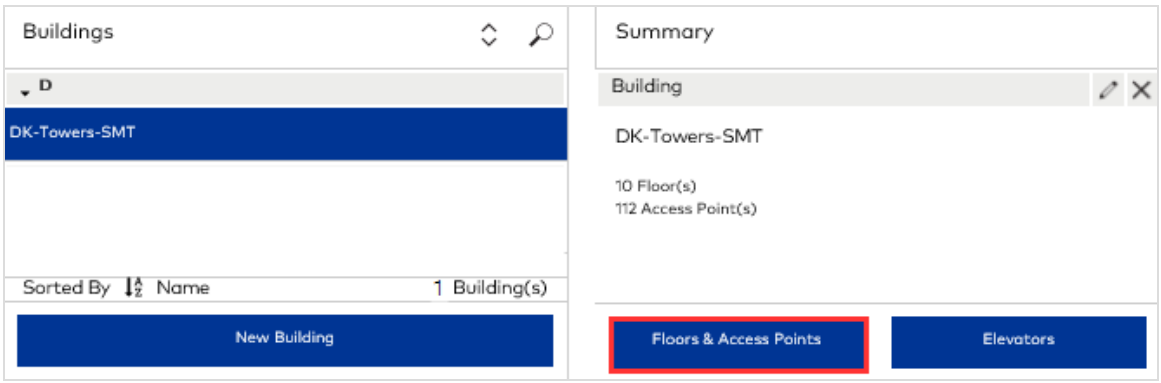
> ⚠ If you are integrating Keyscan Aurora, you must enable Aurora integration before proceeding. Go to System Settings > Advanced > Enable Aurora Integration. For instructions, see Working with Keyscan Aurora.

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

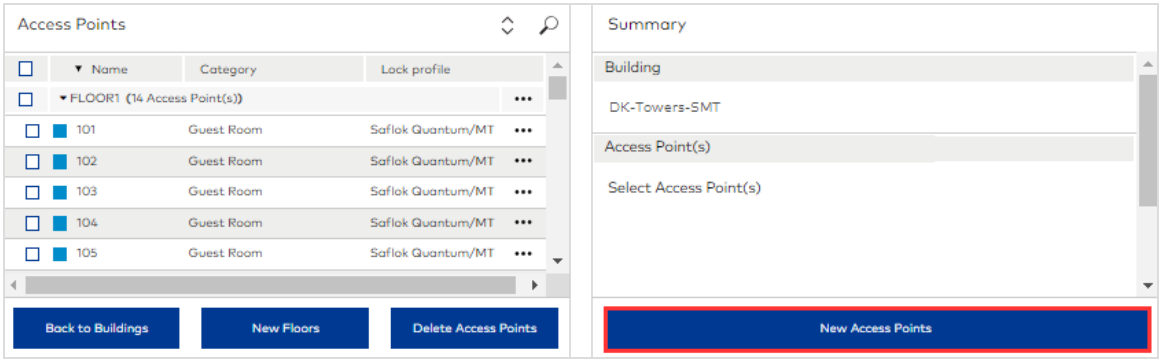
- Adding Unlimited Guest Common Areas
- Adding Limited-Access Guest Common Areas
- Adding Common Areas to Common Area Groups

Adding Unlimited Guest Common Areas

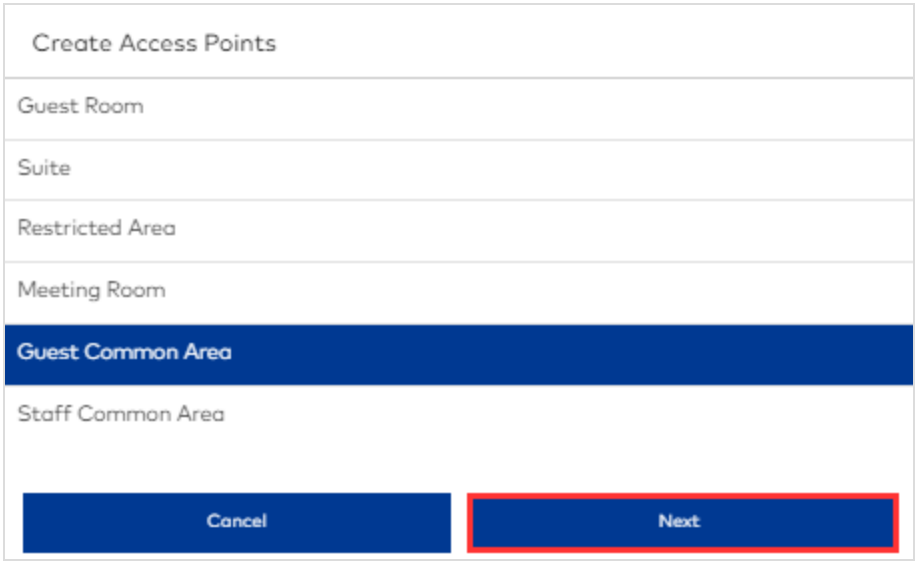
1. Go to Property Builder.



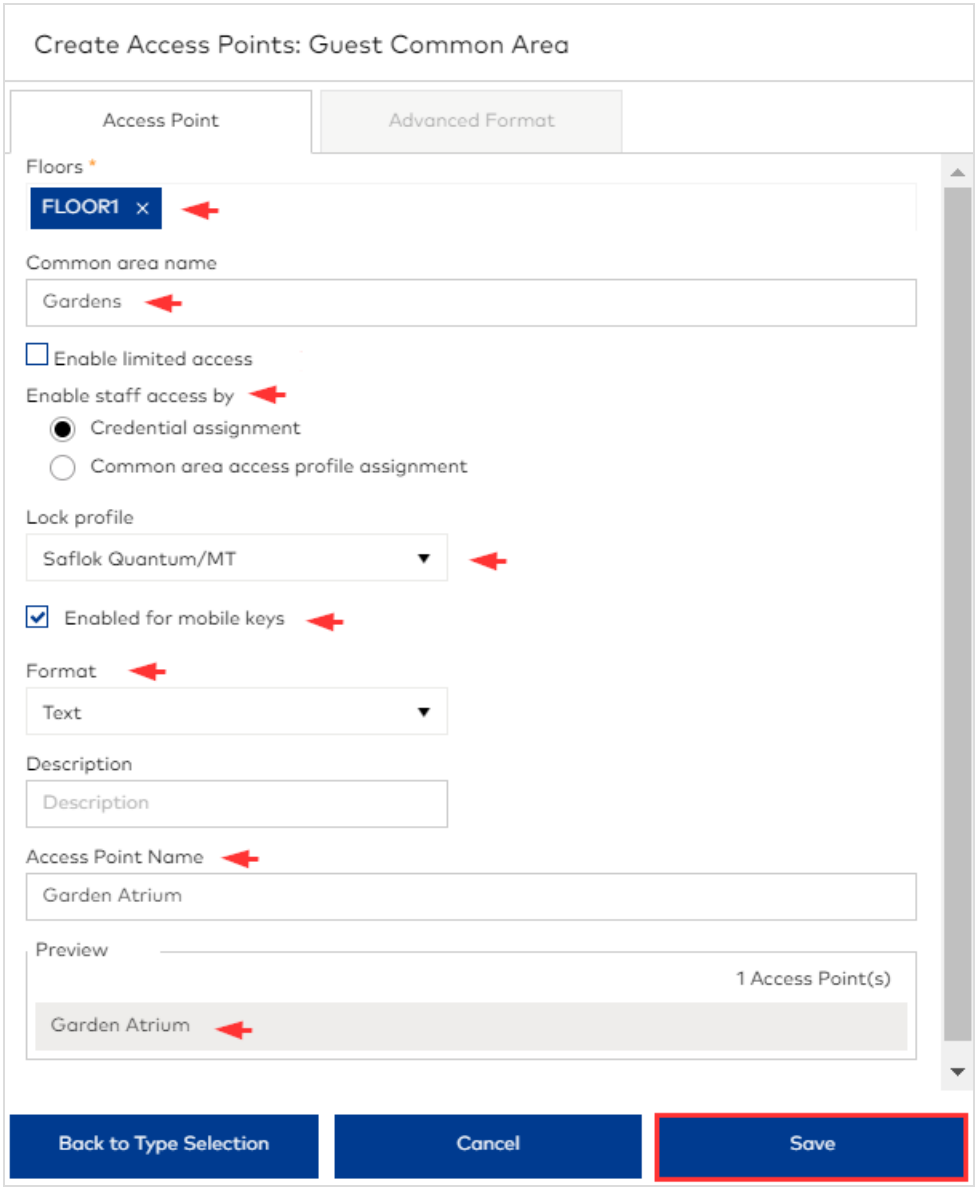
2. Select a building.
3. Click **Floors & Access Points**.



4. Click **New Access Points**.



5. Select **Guest 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.

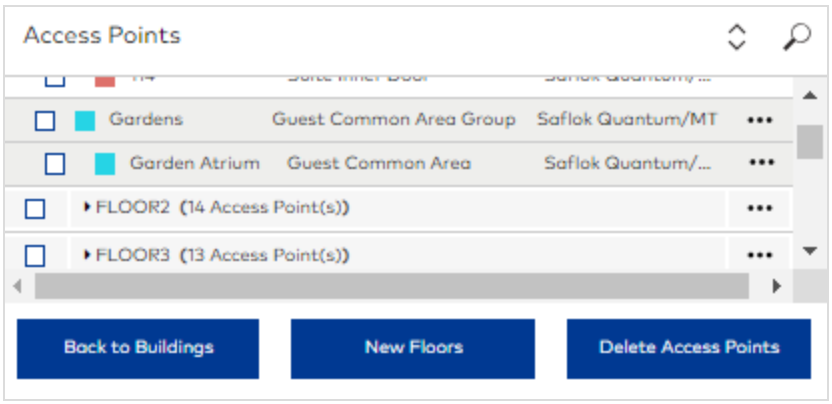
When limited access is not enabled, this guest common area and

related access points an be implicitly access by all guest keys.

8. Select whether to enable staff access by credential assignment or common area access profile.
   - Credential assignment—If you select this option, the common area must be included in the credential that you select when making the staff key.
   - Common area access profile assignment—If you select this option and the common area is unlimited, access is enabled by default (there is no need to create a common area access profile). If the common area is limited, staff access depends on the credential class type selected when making the staff key:
     - For Emergency and Grand Master class types, the common area must be included in the credential that you select when making the staff key.
     - For Master and Limited Use Staff class types, the credential selected when making a key must be associated with a common area access profile that includes the common area.
9. For **Lock profile**, select the lock model.
10. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
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. Default: none.
    - **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.

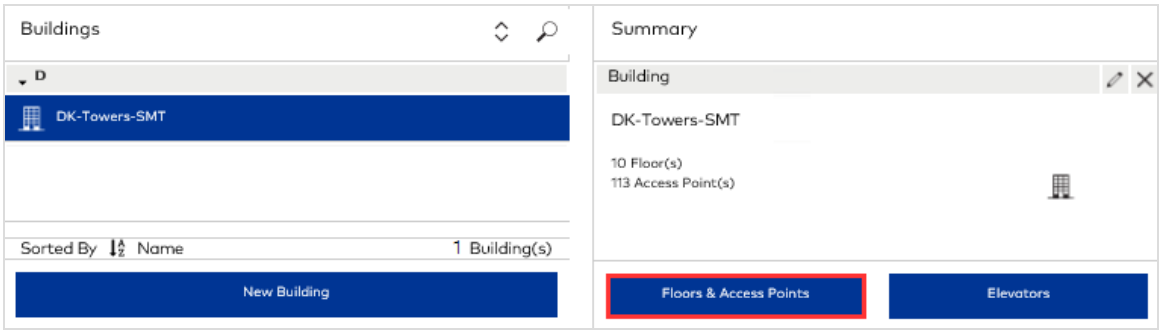
- **Suffix**—Specify the text to display after the main number. Include spaces where appropriate. Default: none.
- **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. Leading zeros occur before the first non-zero digit. For example, select **n** for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

14. Click **Save**.

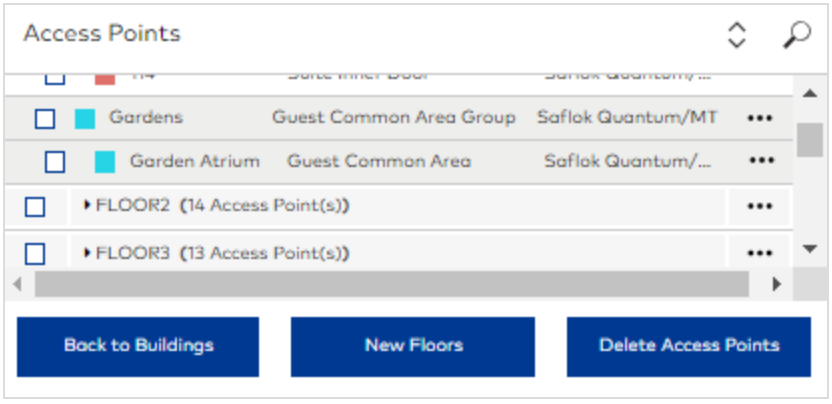


Adding Limited-Access Guest Common Areas

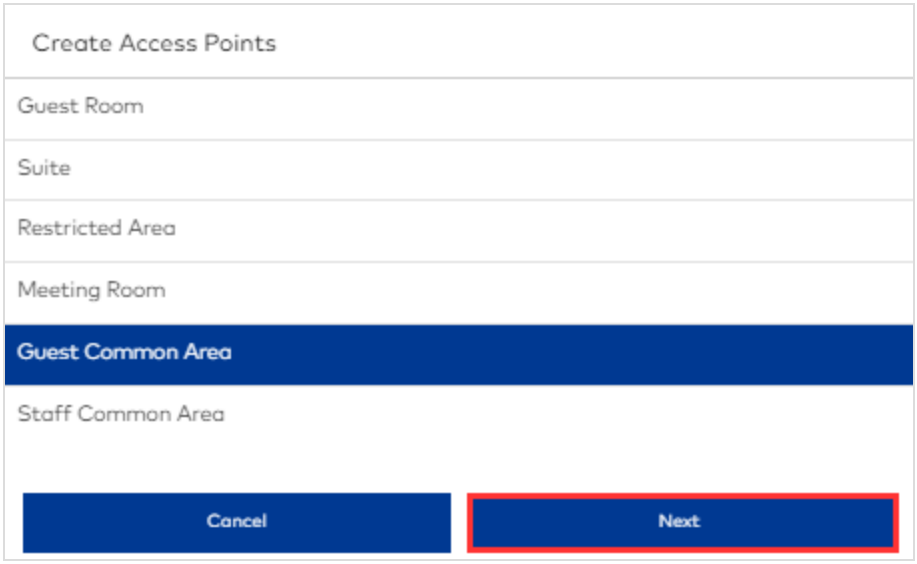
1. Go to Property Builder.



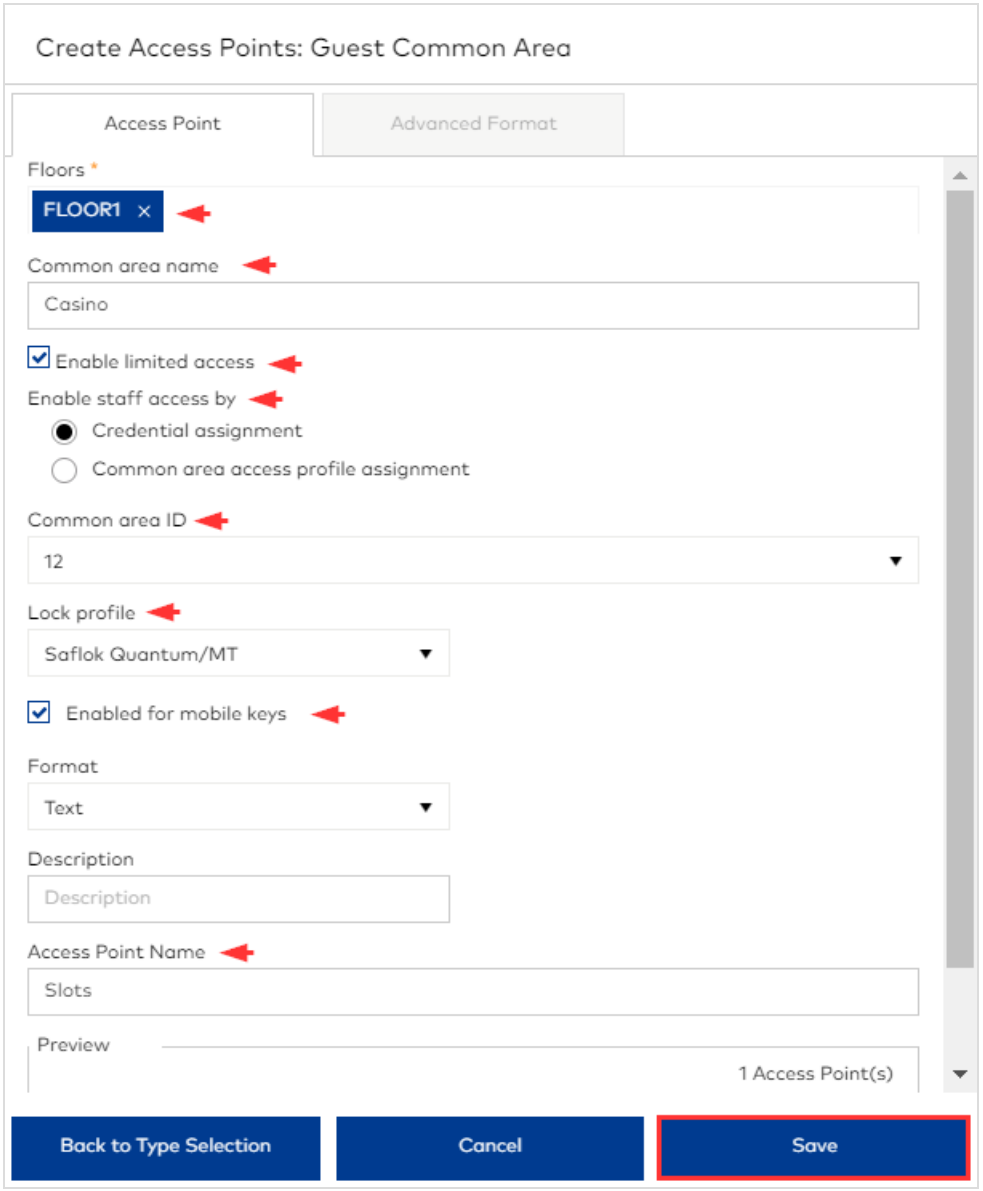
2. Select a building.
3. Click **Floors & Access Points**.



4. Click **New Access Points**.



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

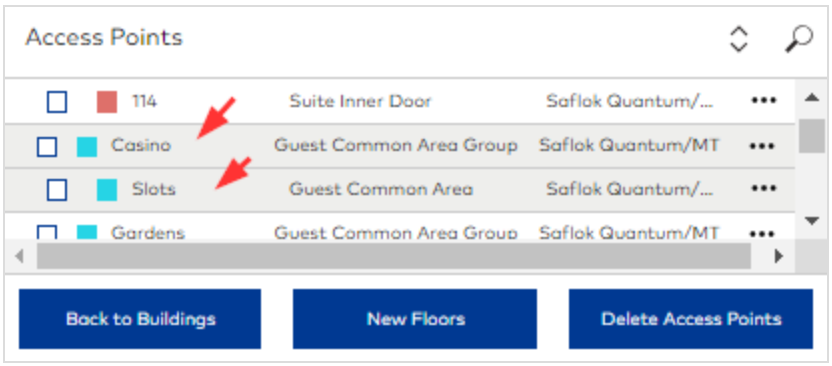


6. For **Floors**, select the floor where you want to add the access point.
7. For **Common area name**, specify a unique name that does not exceed 20 characters. This is the name of the common area group. You can add additional common areas to the group.
8. Select the **Enable limited access** option.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

9. Select whether to enable staff access by credential assignment or common area access profile.
   - Credential assignment—In Access Management > Credential Management, you must add the Guest Common Area to any credential that requires access.
   - Common area access profile assignment—For Staff/Master and Staff/Limited Use credentials that require access, you must configure a staff common area access profile in Access Management > Common Area Access and associate the Guest Common Area with the credentials. For Staff/Emergency and Staff/Grand Master credentials, you must add the Guest Common Area directly to the credential in Access Management > Credential Management.
10. All staff emergency and grand master credentials which need to have access to this guest common area will need be assigned to this guest common area's access points in Access Management/Credential Management.
11. For **Common area ID**, accept the value that the system automatically populates.
12. For **Lock profile**, select the lock model.
13. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
14. 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.
15. (*optional*) Add a description for the access point or range of access points.
16. (*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. Default: none.
    - **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.
    - **Suffix**—Specify the text to display after the main number. Include spaces where appropriate. Default: none.

- **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. 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**. Default: n.
- **Room number format**—Select how many digit positions to display for room 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 room number in the access point name, select **None**.

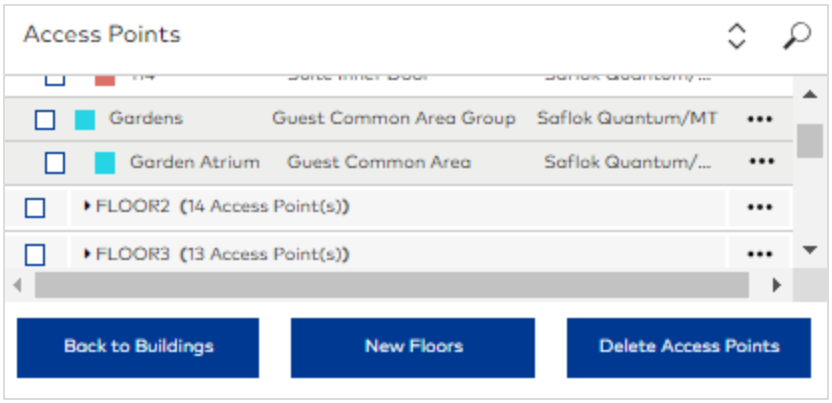
17. Click **Save**.



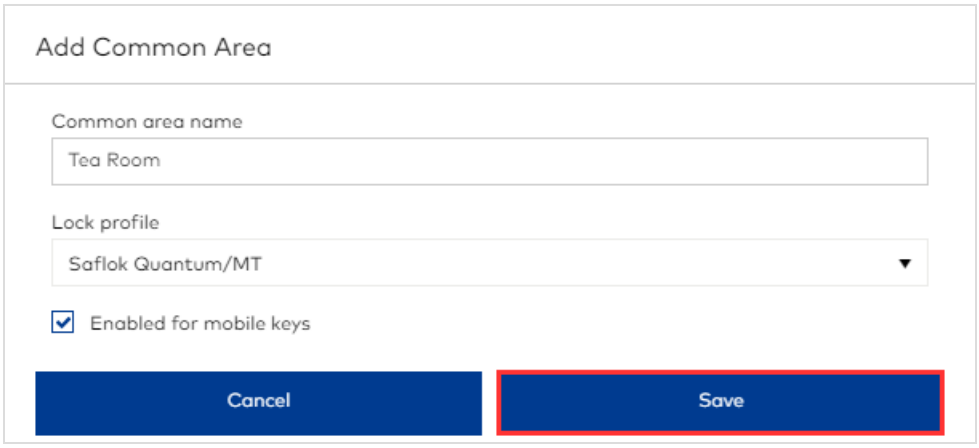
Adding Common Areas to Common Area Groups

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:

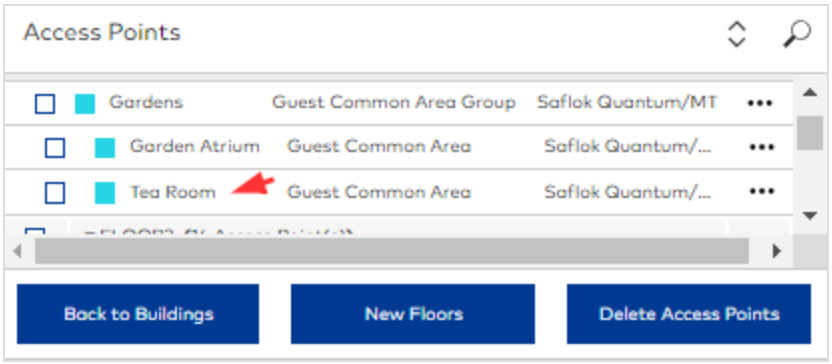
1. Go to Property Builder.
2. Select the common area group where you want to add the common area.



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



4. Specify a unique name for the common area.
5. For **Lock profile**, select the lock model.
6. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
7. 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.

> ⚠ If you are integrating Keyscan Aurora, you must enable Aurora integration before proceeding. Go to System Settings > Advanced > Enable Aurora Integration. For instructions, see Working with Keyscan Aurora.

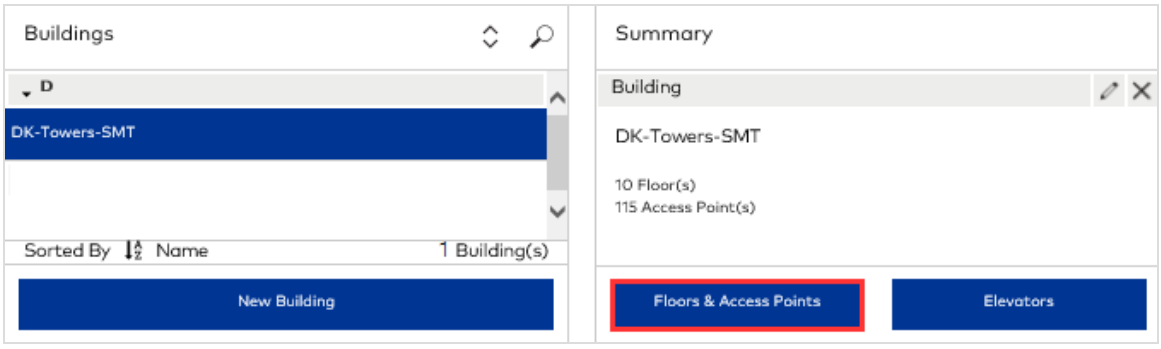
This topic provides instructions for adding the following types of common area access points:

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

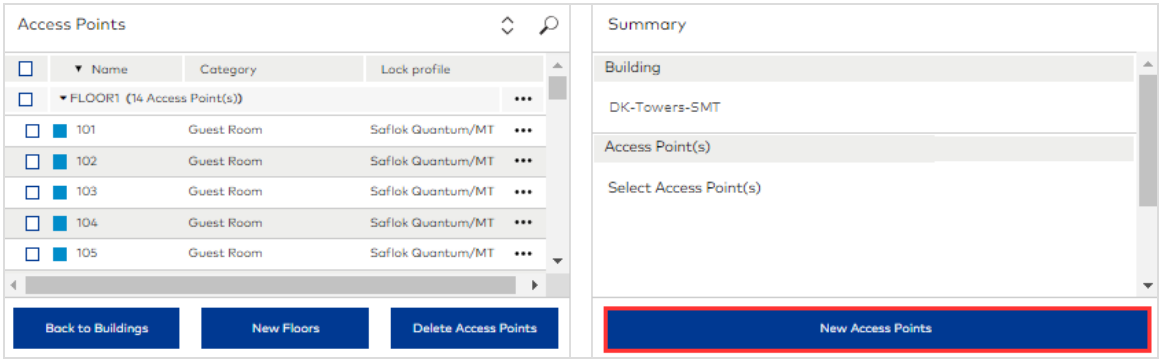
Adding Unlimited Staff Common Areas

Unlimited staff common areas are added to every staff key.

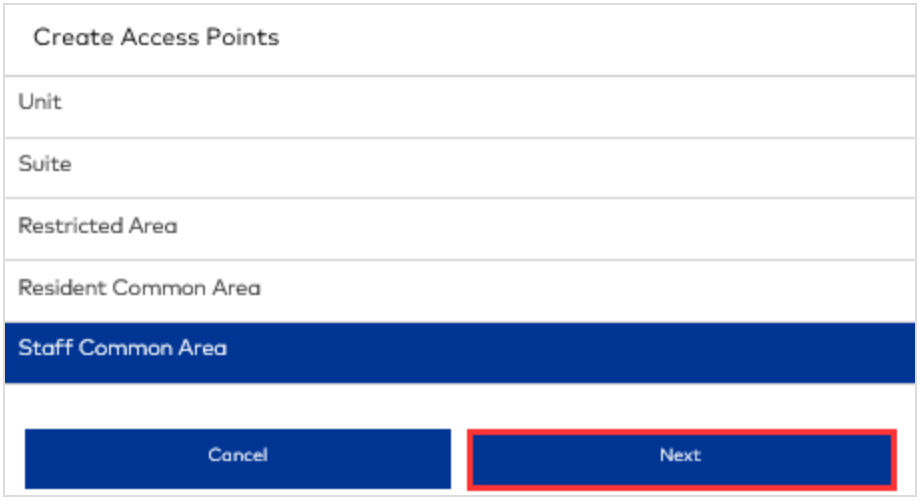
1. Go to Property Builder.

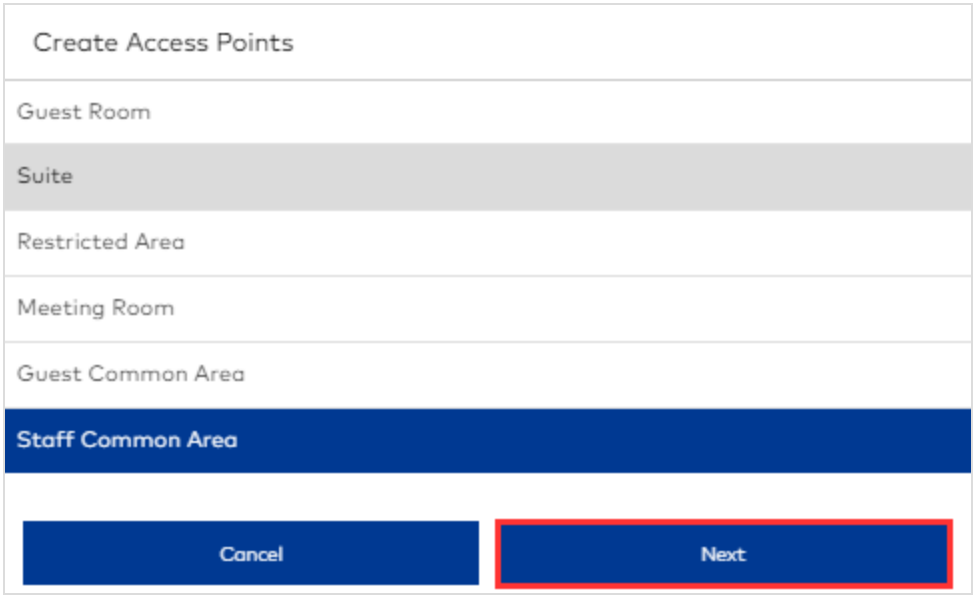


2. Select a building.
3. Click **Floors & Access Points**.

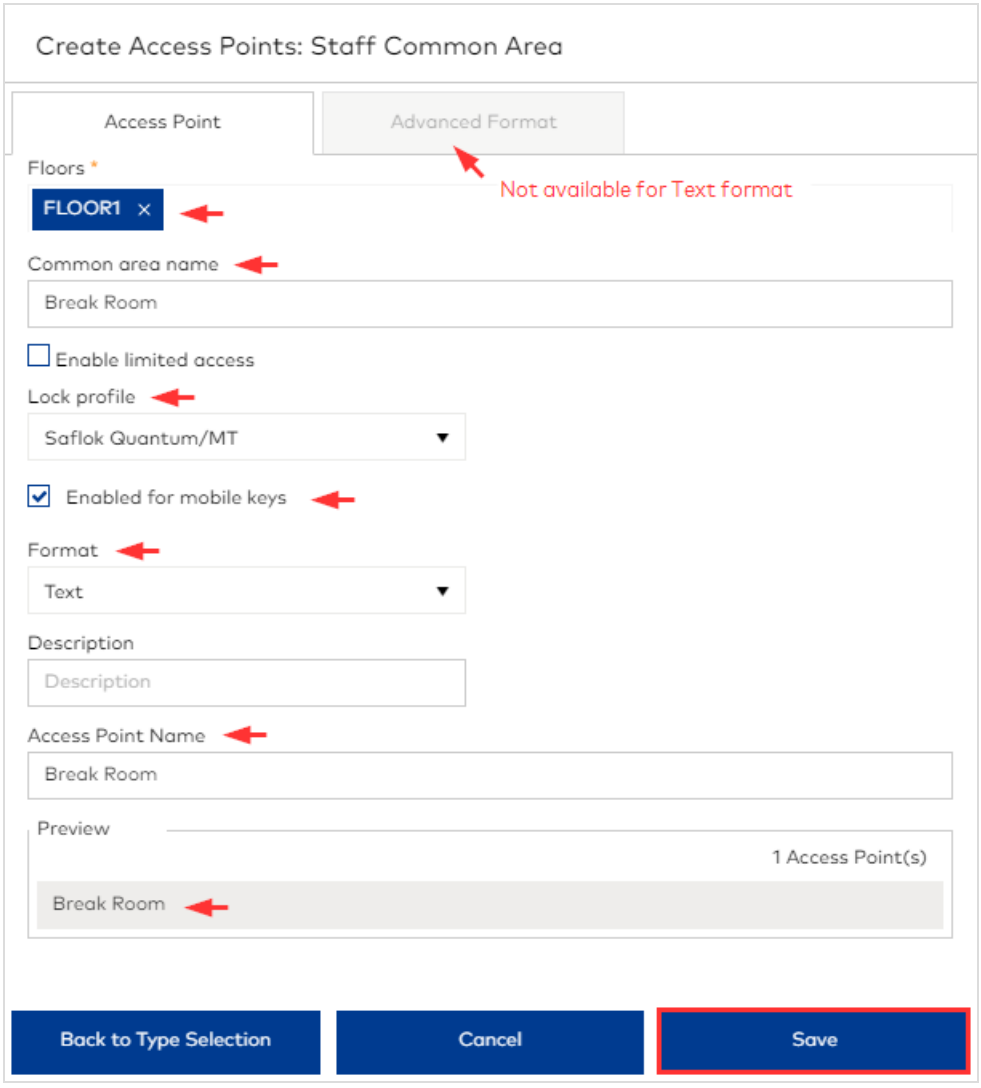


4. Click **New Access Points**.





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

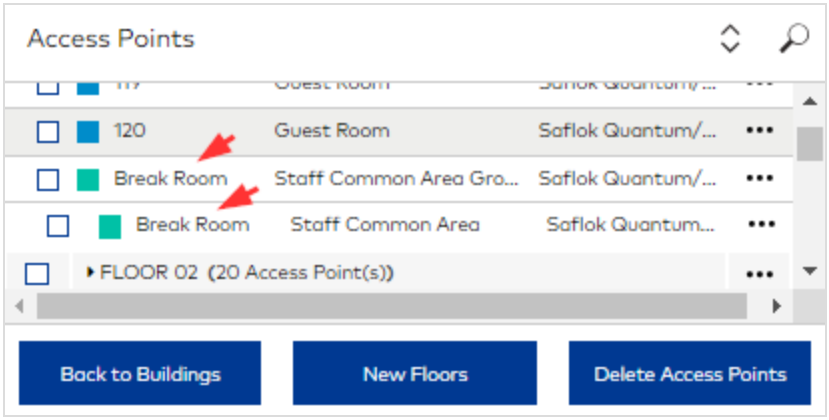


6. For **Floors**, select the floor where you want to add the access point.
7. For **Common area name**, specify a unique name that does not exceed 20 characters. This is the name of the common area group. You can add additional common areas to the group.

> When limited access is disabled, Staff/Master and Staff/Limited Use credentials have implicit access to this Staff Common Area and associated access points. For all Staff/Emergency and

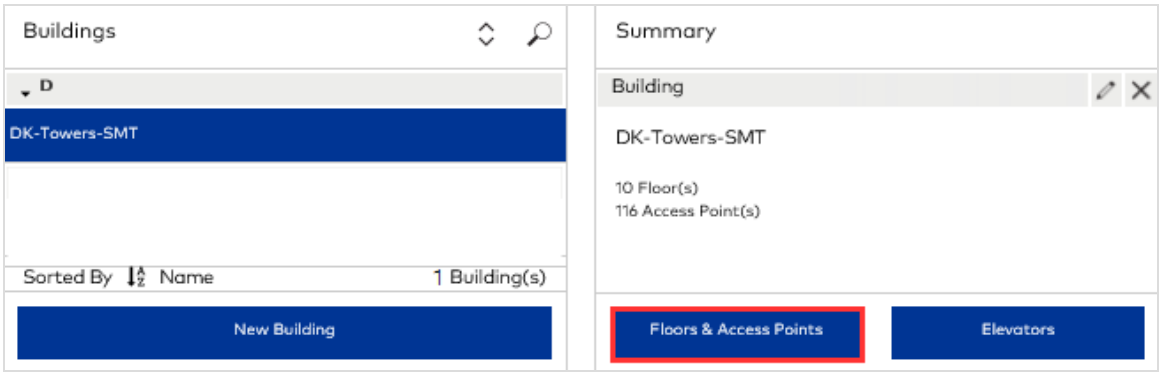
> Staff/Grand Master credentials, you must add the Staff Common Area directly to the credential in Access Management > Credential Management.

8. For **Lock profile**, select the lock model.
9. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
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. Default: none.
    - **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.
    - **Suffix**—Specify the text to display after the main number. Include spaces where appropriate. Default: none.
    - **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. 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**. Default: n.
    - **Room number format**—Select how many digit positions to display for room 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 room number in the access point name, select **None**.
13. Click **Save**.

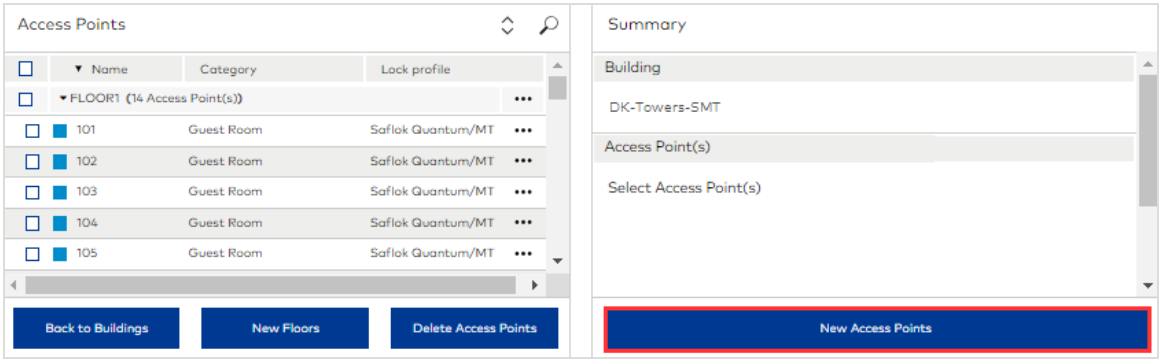


Adding Limited-Access Staff Common Areas

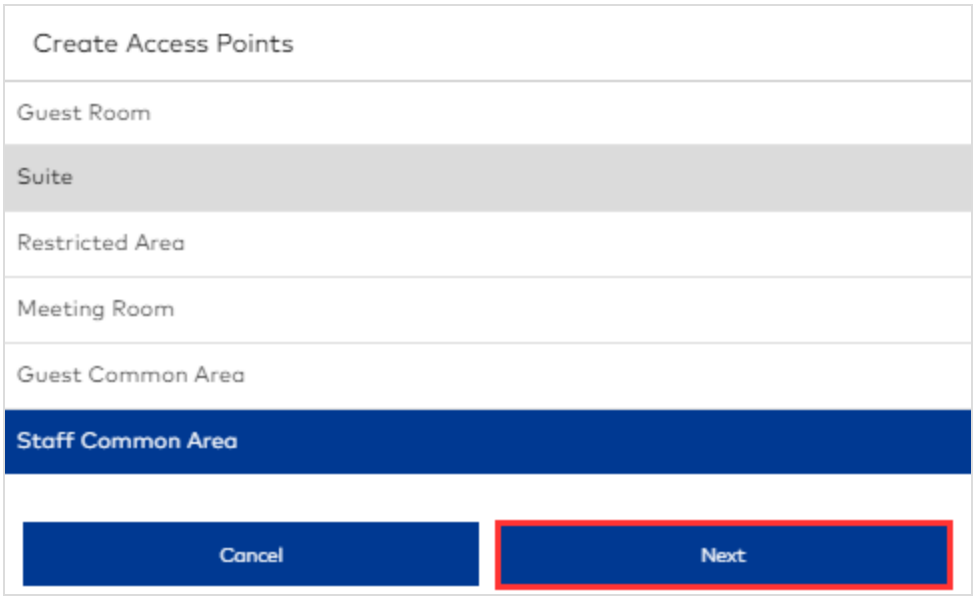
1. Go to Property Builder.



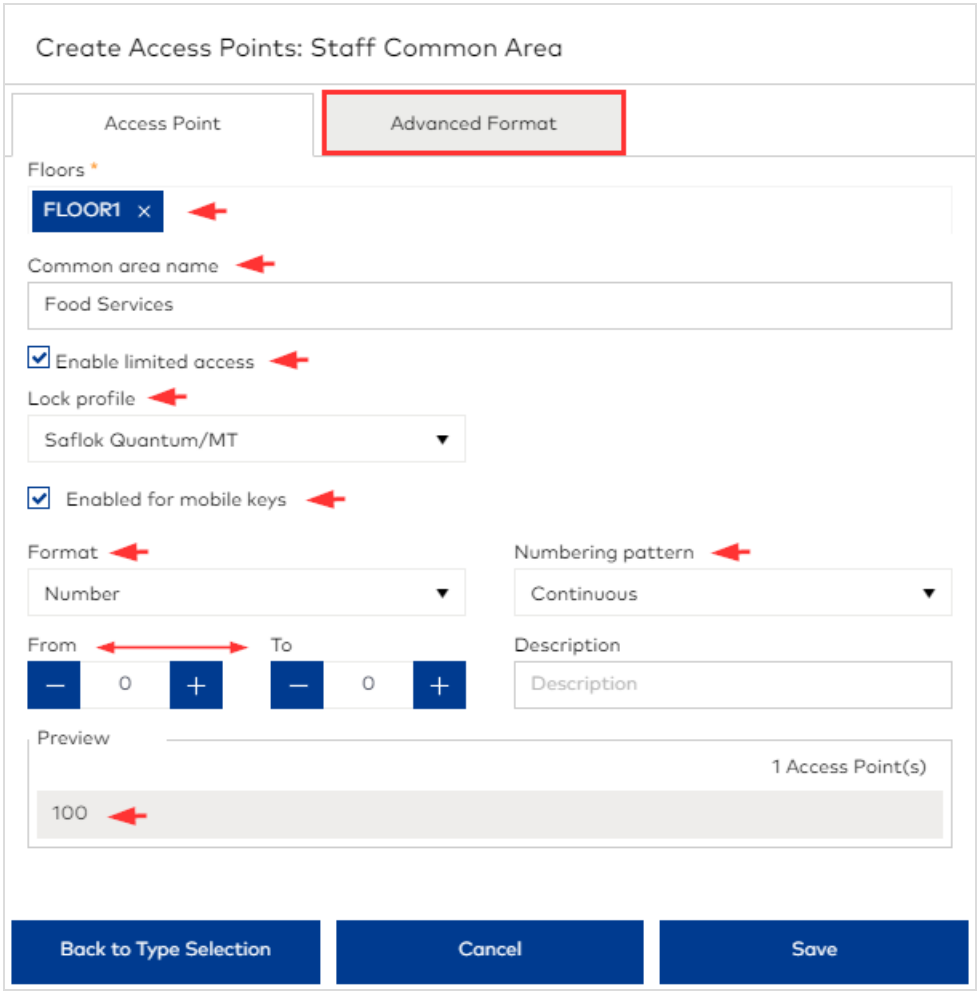
2. Select a building.
3. Click **Floors & Access Points**.



4. Click **New Access Points**.

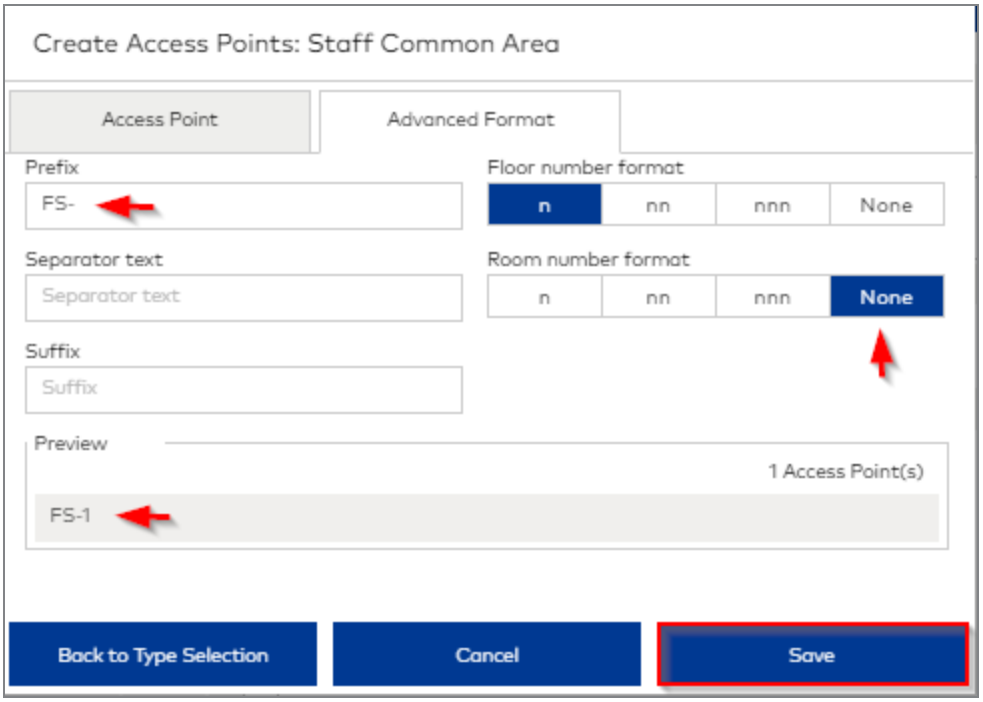


5. Select **Staff Common Area**, then click **Next**.



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. For Staff/Master and Staff/Limited Use credentials that require access to this Staff Common Area, you must configure a staff common area access profile in Access Management > Common Area Access. For Staff/Emergency and Staff/Grand Master credentials, you must add the Staff Common Area directly to the credential in Access Management > Credential Management.
9. For **Lock profile**, select the lock model.

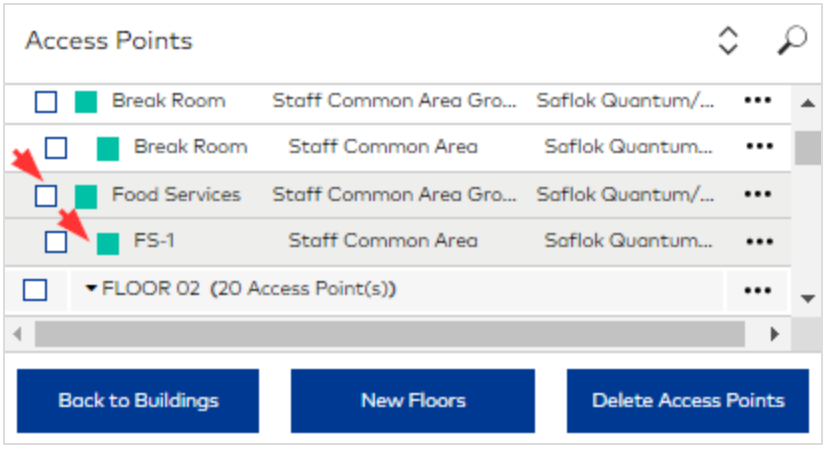
10. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
11. For **Format**, select whether to identify the access points using numbers 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. Default: none.
- **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.

- **Suffix**—Specify the text to display after the main number. Include spaces where appropriate. Default: none.
- **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. 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**. Default: n.
- **Room number format**—Select how many digit positions to display for room 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 room number in the access point name, select **None**.

14. Click **Save**.

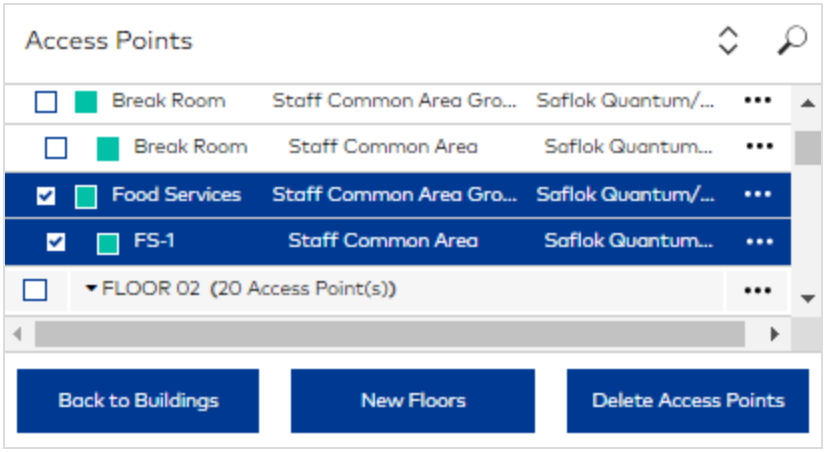


Before staff can be issued a key that authorizes access to limited-access staff common areas, you must either add the common area to the assigned staff credential or associate the common area with the assigned staff credential in Access Management > Common Area Access.

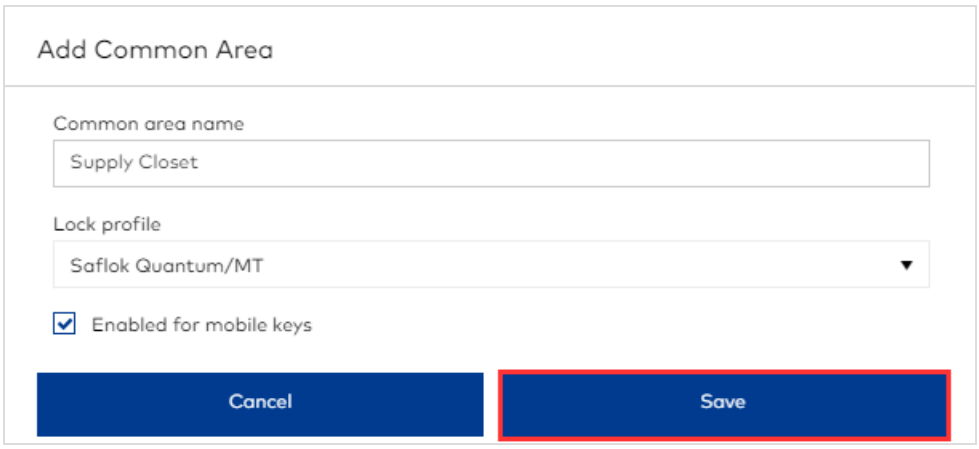
Adding Common Areas to Common Area Groups

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:

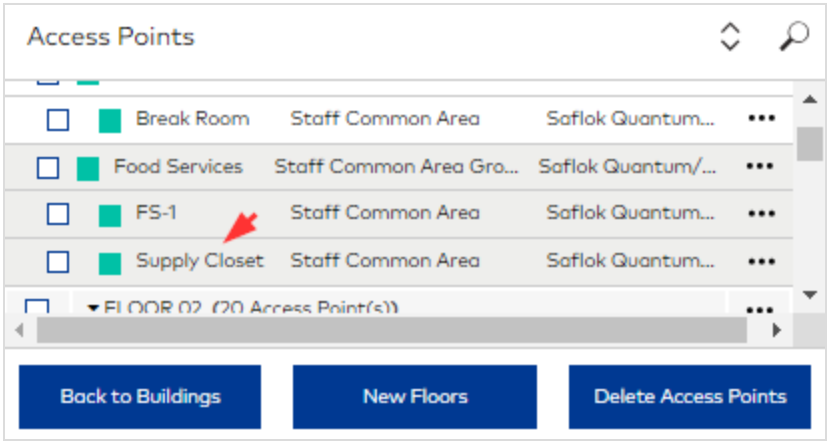
1. Go to Property Builder.
2. Select the common area group where you want to add the common area.



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



4. Specify a unique name for the common area.
5. For **Lock profile**, select the lock model.
6. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
7. Click **Save**.

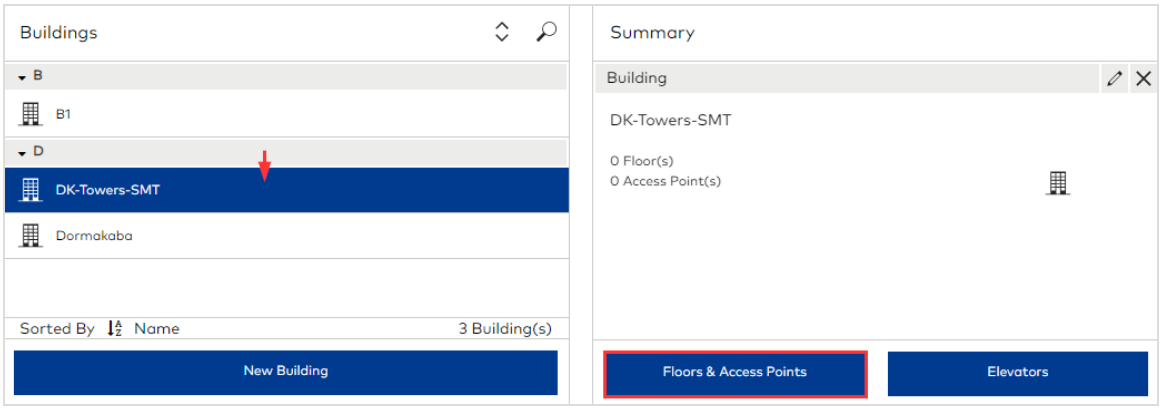

Access Points
Break Room
Staff Common Area
Saflok Quantum...
Food Services
Staff Common Area Gro...
Saflok Quantum/...
FS-1
Staff Common Area
Saflok Quantum...
Supply Closet
Staff Common Area
Saflok Quantum...
Back to Buildings
New Floors
Delete Access Points

Add Meeting Rooms

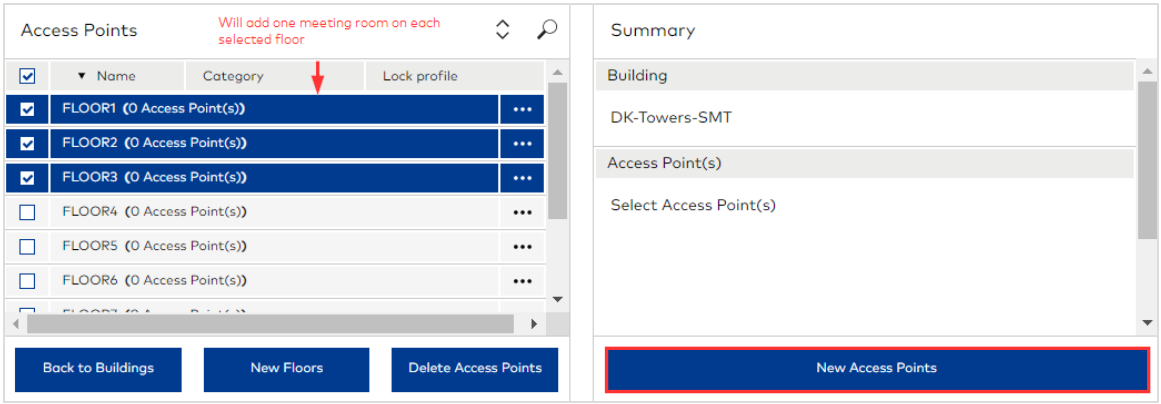
A meeting room is a type of access point intended to accommodate special events for the public and/or registered guests. An Auto-Unlatch schedule can be assigned to a meeting room.

To add a meeting room:

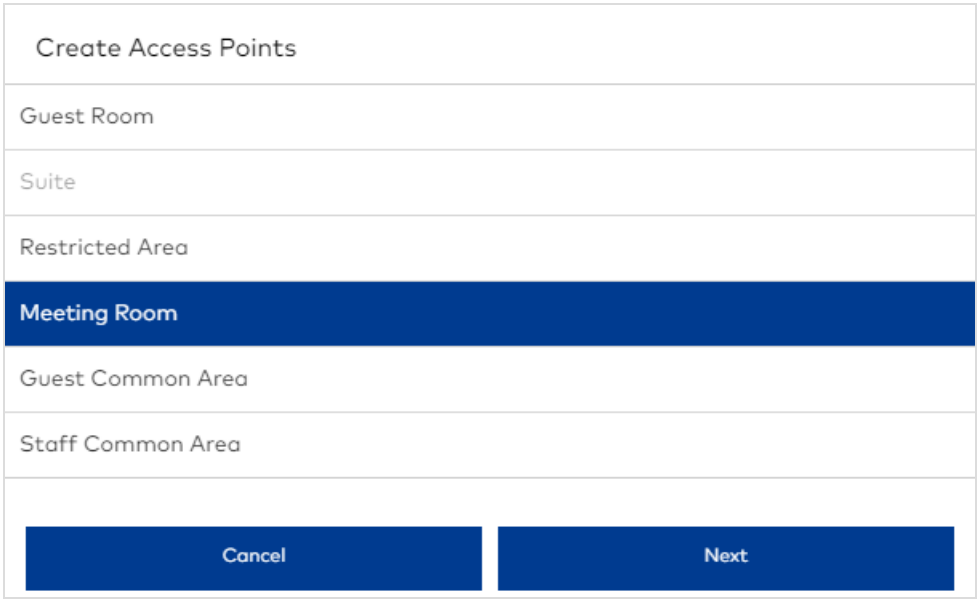
1. Go to Property Builder.



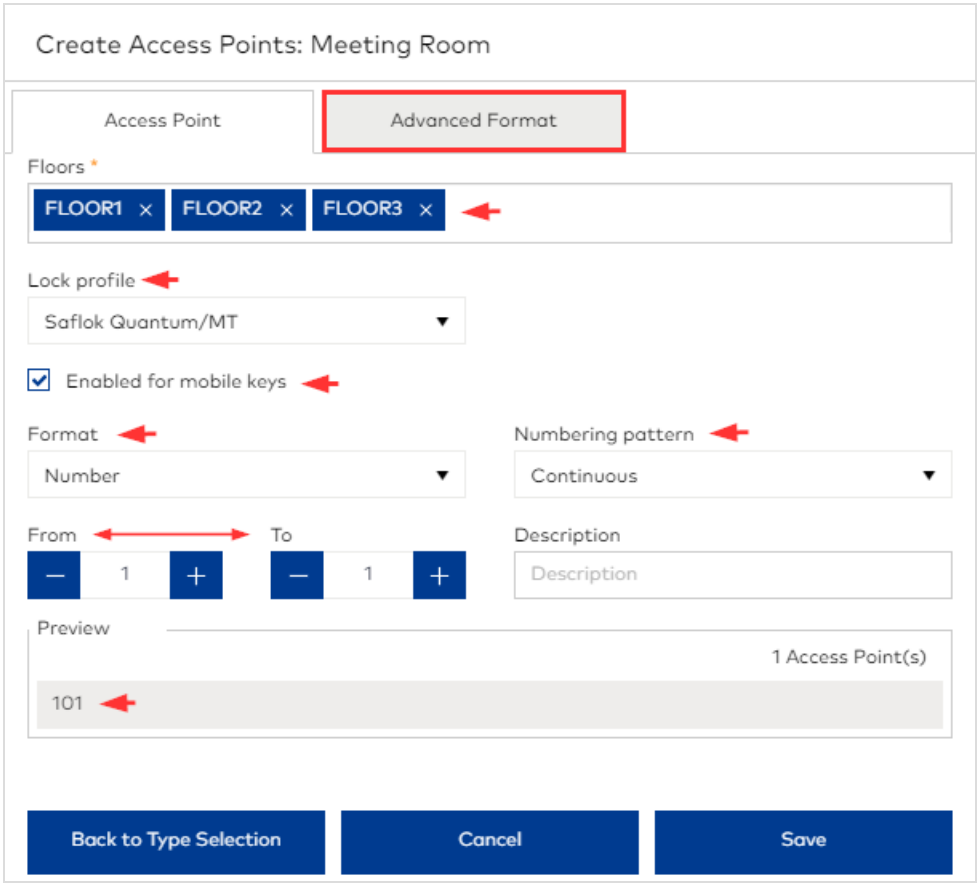
2. Select a building.
3. Click **Floors & Access Points**.



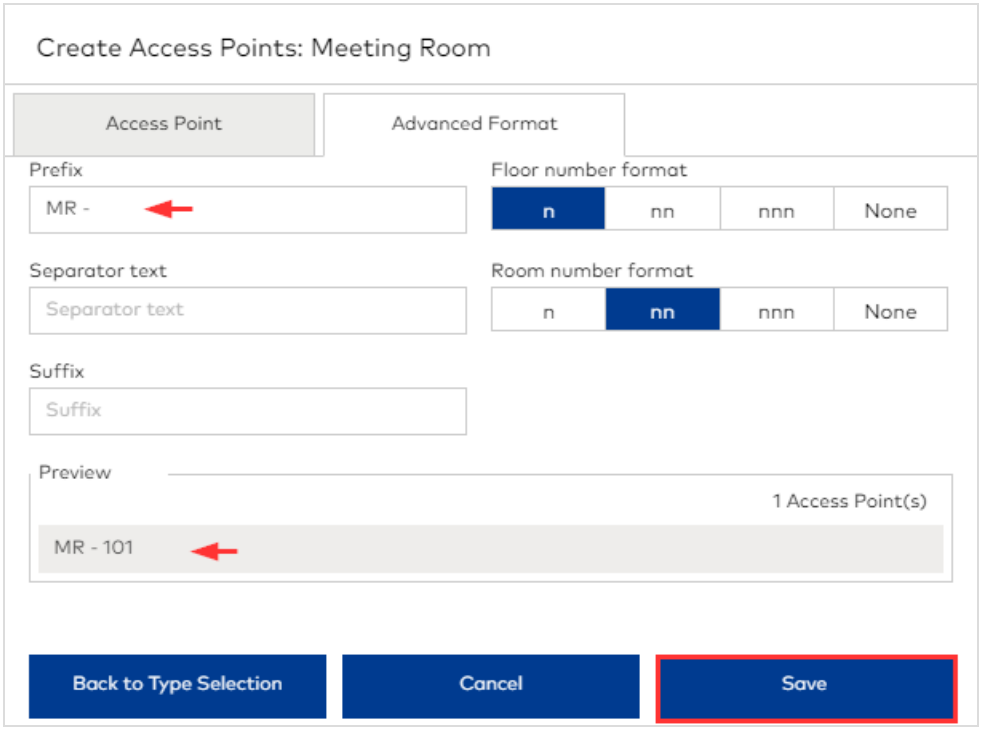
4. Select the floor where you want add the access point.
5. Click **New Access Points**.



6. Select **Meeting Room**, then click **Next**.

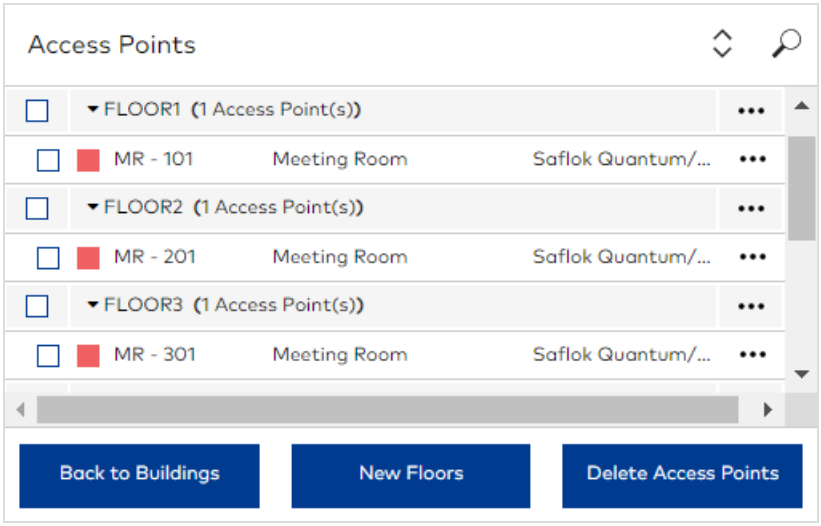


7. For **Lock profile**, select the lock model.
8. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
9. For **Format**, select whether 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 to use how to increment the numbers.
   - If you select **Text**, specify a unique access point name.
10. (*optional*) Add a description for the access point or range of access points.
11. (*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. Default: none.
- **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.
- **Suffix**—Specify the text to display after the main number. Include spaces where appropriate. Default: none.
- **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. 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**. Default: n.
- **Room number format**—Select how many digit positions to display for room 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 room number in the access point name, select **None**.

12. Click **Save**.

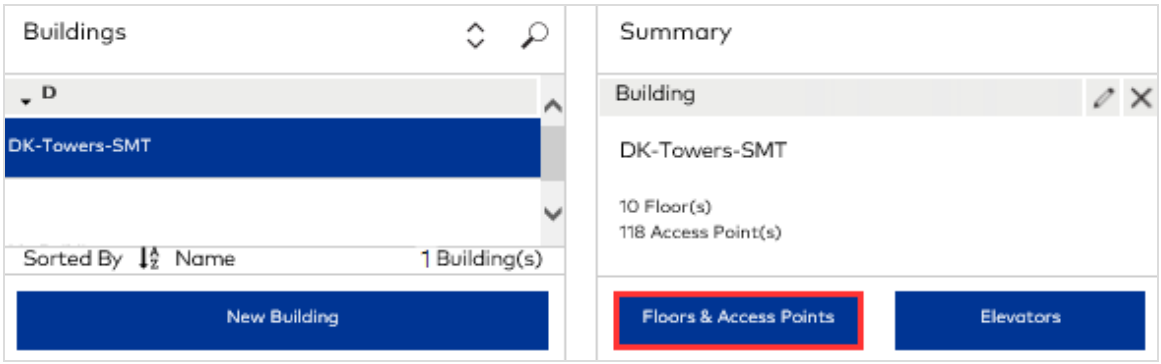

Access Points
FLOOR1 (1 Access Point(s))
MR - 101 Meeting Room Saflok Quantum/...
FLOOR2 (1 Access Point(s))
MR - 201 Meeting Room Saflok Quantum/...
FLOOR3 (1 Access Point(s))
MR - 301 Meeting Room Saflok Quantum/...
Back to Buildings
New Floors
Delete Access Points

Add Restricted Areas

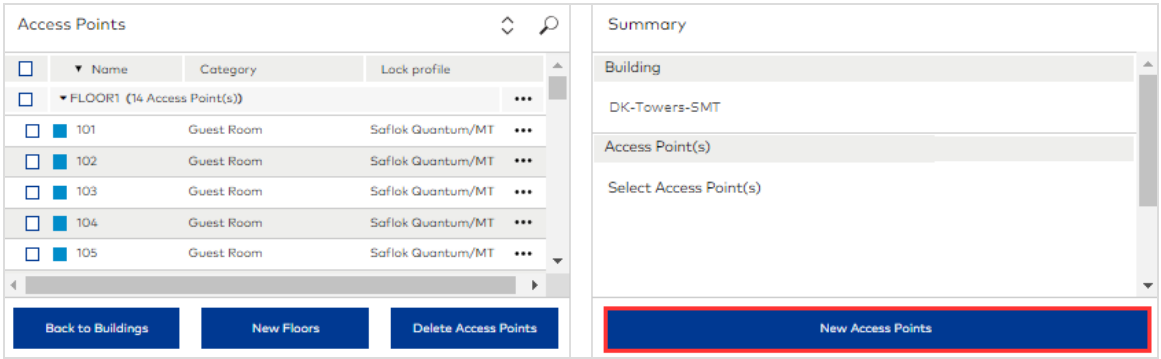
A restricted area is an access point type intended to provide back-of-the-house access for staff only.

To add restricted areas:

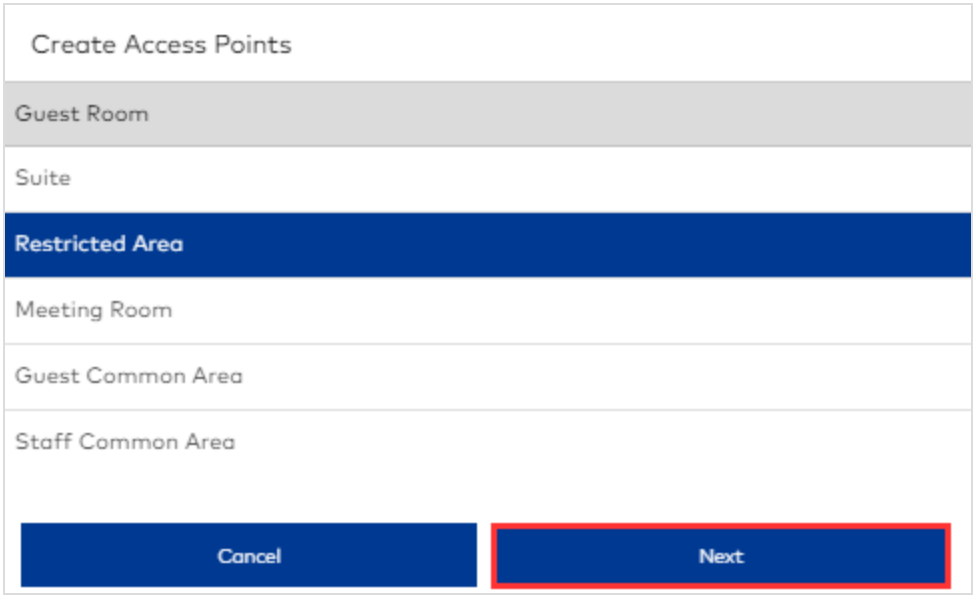
1. Go to Property Builder.



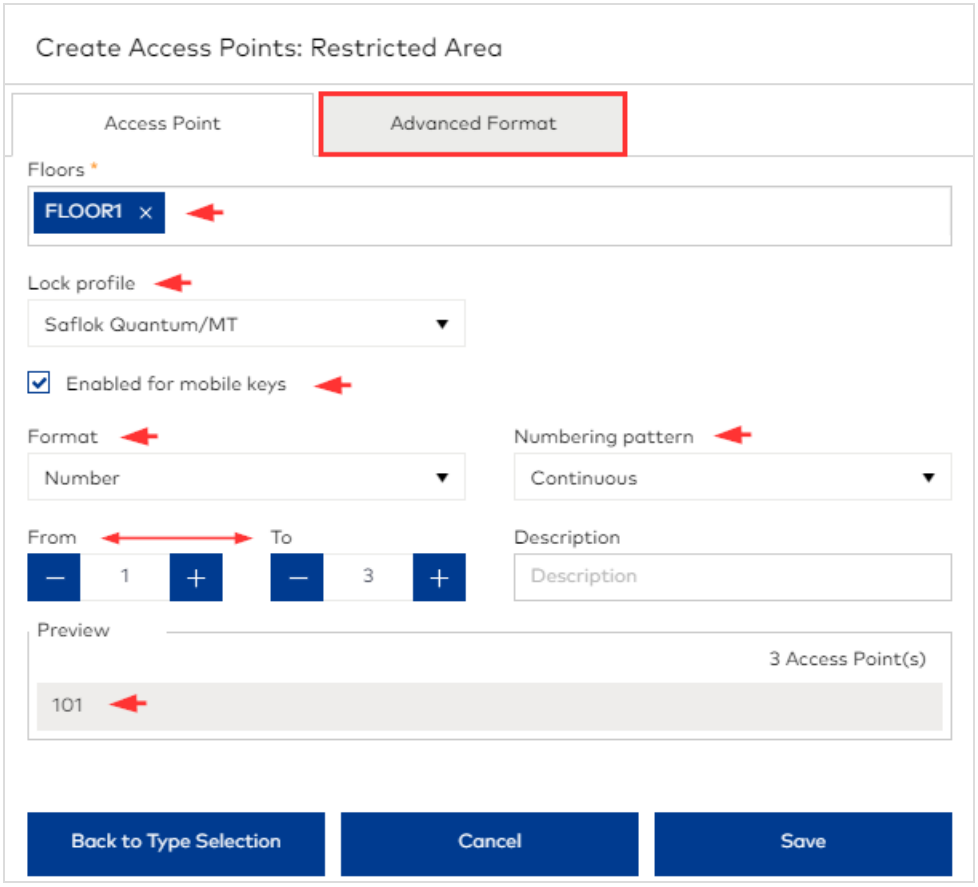
2. Select a building.
3. Click **Floors & Access Points**.



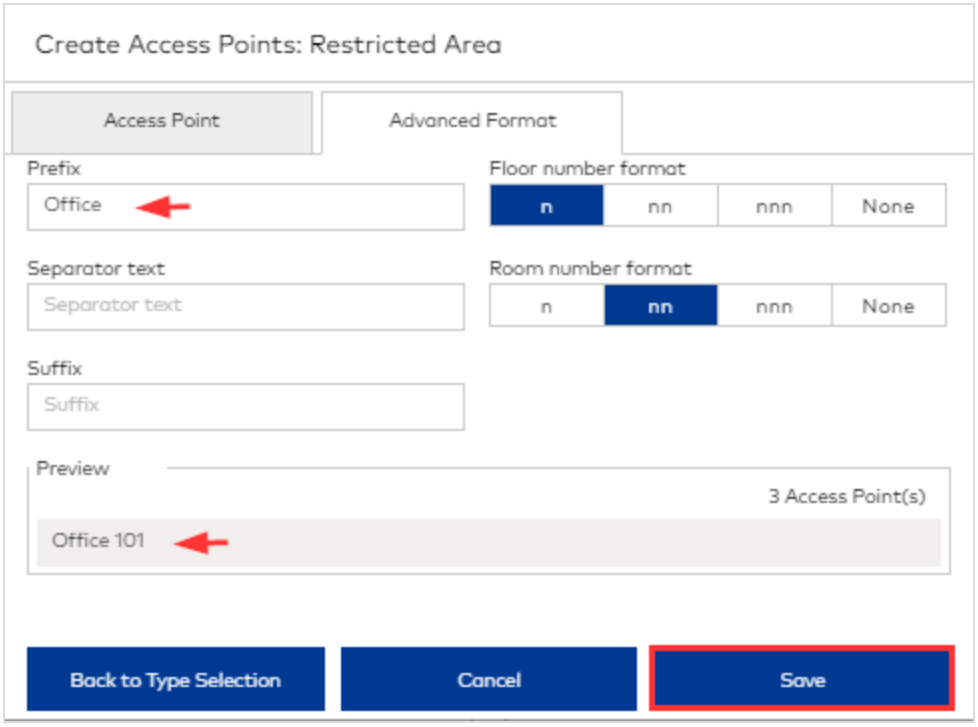
4. Click **New Access Points**.



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

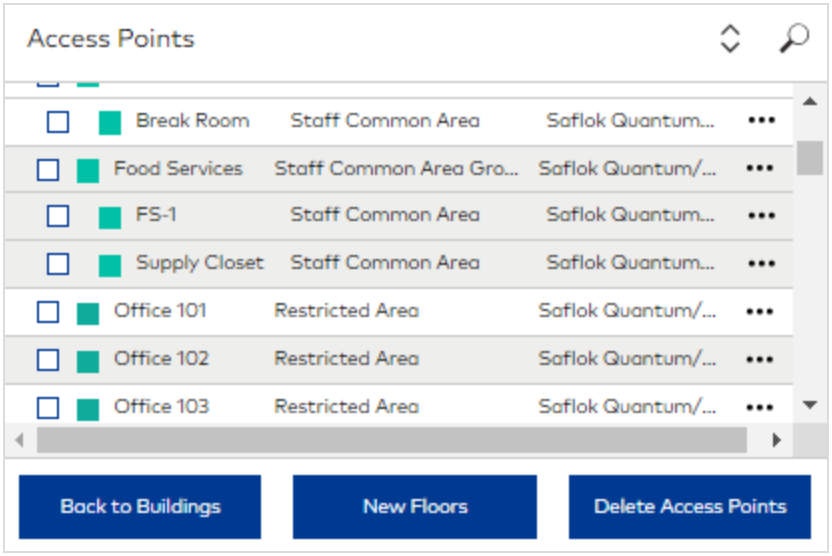


6. For **Floors**, select one or more floors where you want to add the access points.
7. For **Lock profile**, select the lock model.
8. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
9. 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 to use how to increment the numbers.
   - If you select **Text**, specify a unique access point name.
10. (*optional*) Add a description for the access point or range of access points.
11. (*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. Default: none.
- **Separator text**—Specify the text to display between the floor number and room (or restricted area/meeting room) number. Include spaces where appropriate. Default: none.
- **Suffix**—Specify the text to display after the main number. Include spaces where appropriate. Default: none.
- **Floor number format**—Select how many digit positions to display for floor numbers in the unit name. 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**. Default: n.
- **Room number format**—Select how many digit positions to display for room 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 room number in the access point name, select **None**.

12. Click **Save**.


Access Points
Break Room
Staff Common Area
Saflok Quantum...
Food Services
Staff Common Area Gro...
Saflok Quantum/...
FS-1
Staff Common Area
Saflok Quantum...
Supply Closet
Staff Common Area
Saflok Quantum...
Office 101
Restricted Area
Saflok Quantum/...
Office 102
Restricted Area
Saflok Quantum/...
Office 103
Restricted Area
Saflok Quantum/...
Back to Buildings
New Floors
Delete Access Points

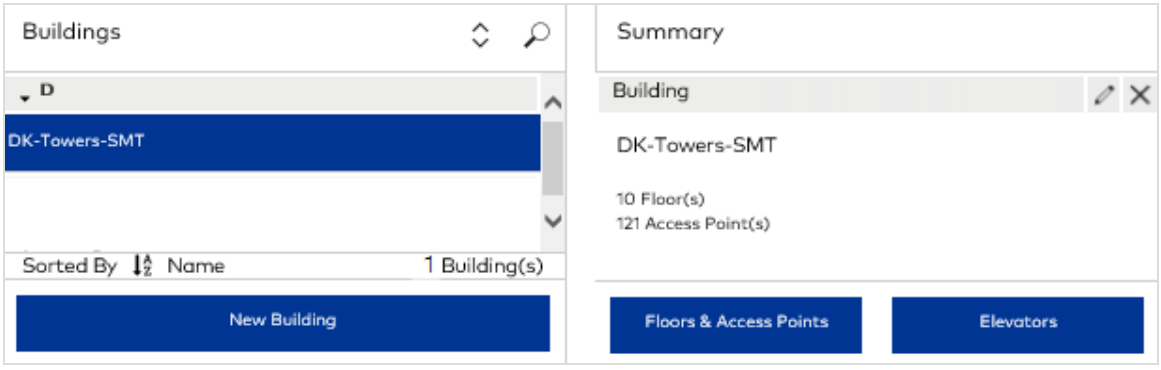
Add Elevators

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*.

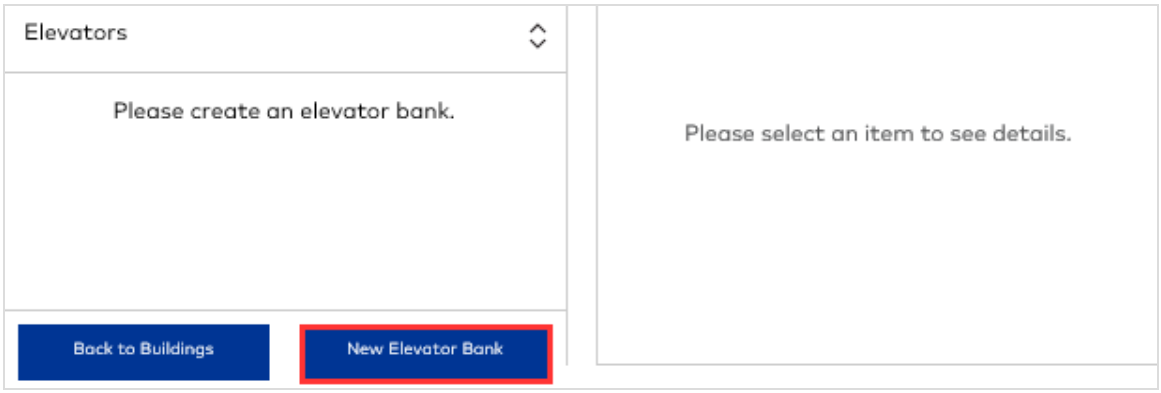
Add Elevator Banks

To add an elevator bank:

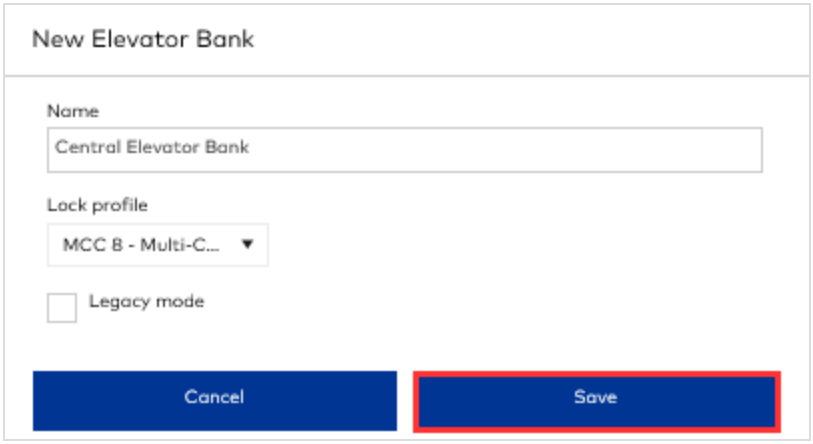
1. Go to Property Builder.



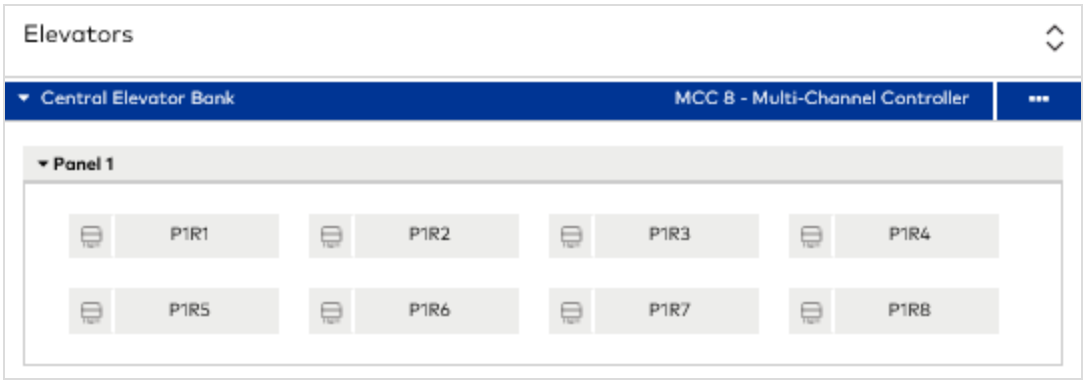
2. Select a building.
3. Click **Elevators**.



4. Click **New Elevator Bank**.



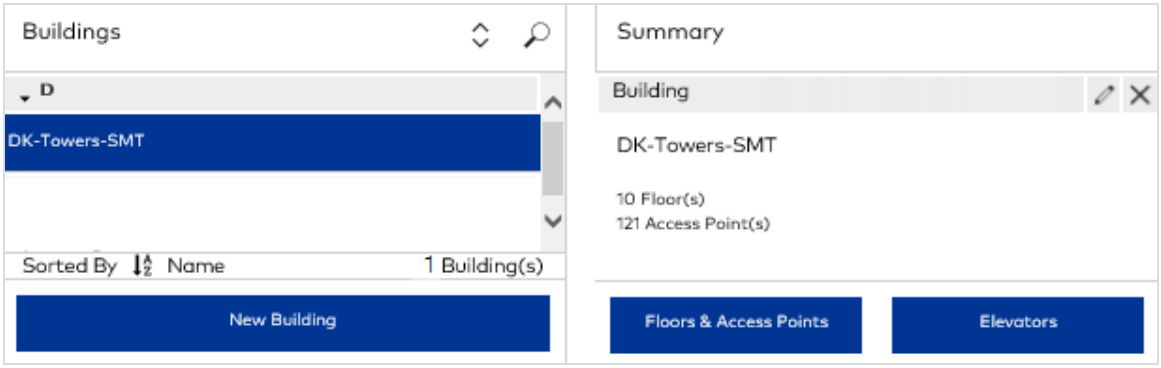
5. Specify a name for the elevator bank.
6. Select a lock profile.
7. Click **Save**. The elevator bank is listed in the Elevator list along with the number of Panel rows supported by the lock profile. The panel rows are where you map panel relay–to–floor access.



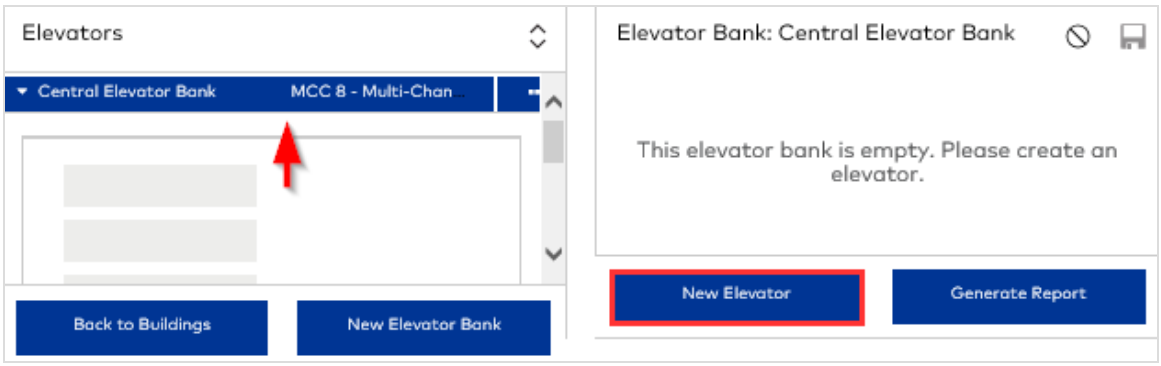
Add Elevators

To add an elevator:

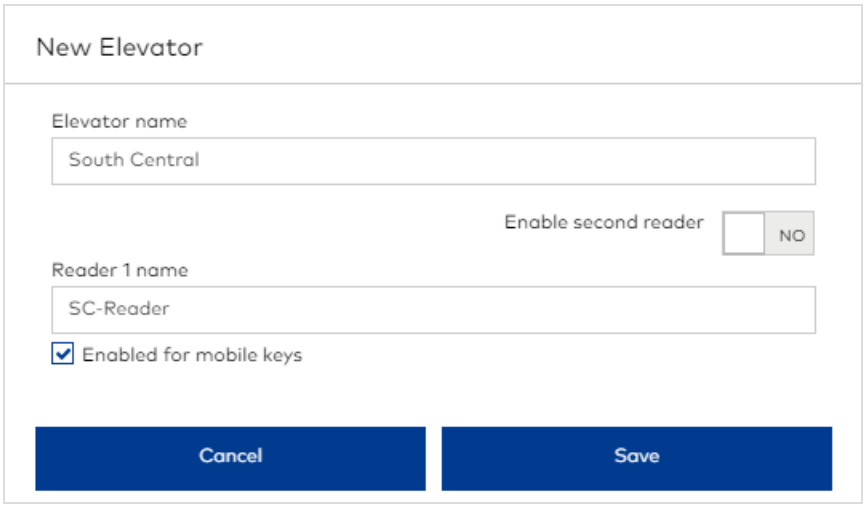
1. Go to Property Builder.



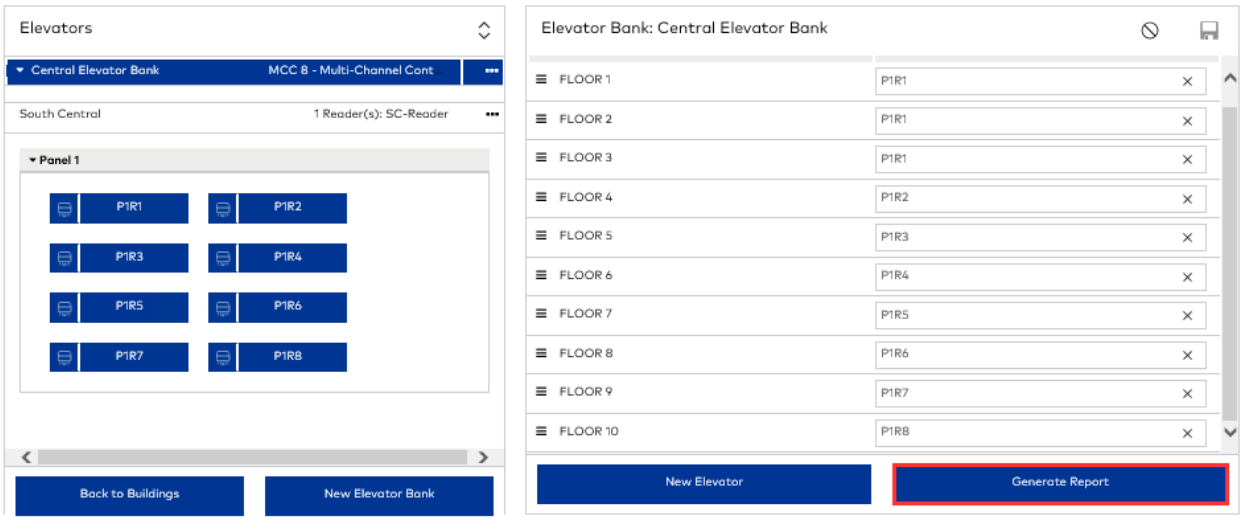
2. Select a building.
3. Click **Elevators**.



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



6. Specify a name for the elevator.
7. Select whether to enable a second reader panel for the elevator.
8. Specify a name for any reader.
9. (*optional*) Select whether the access point is enabled for mobile keys. This field is informational only and must be selected to include the access point in the CSV file download for mobile-key enabled access points.
10. Click **Save**.

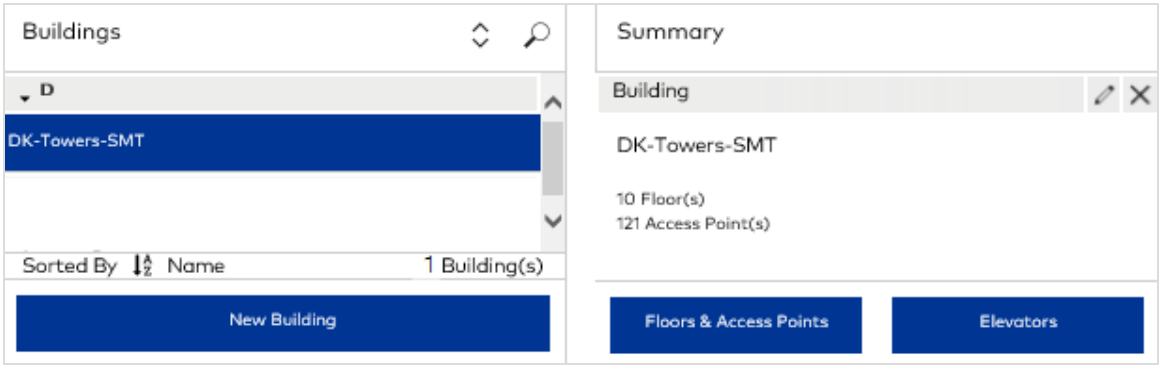


Map floor access

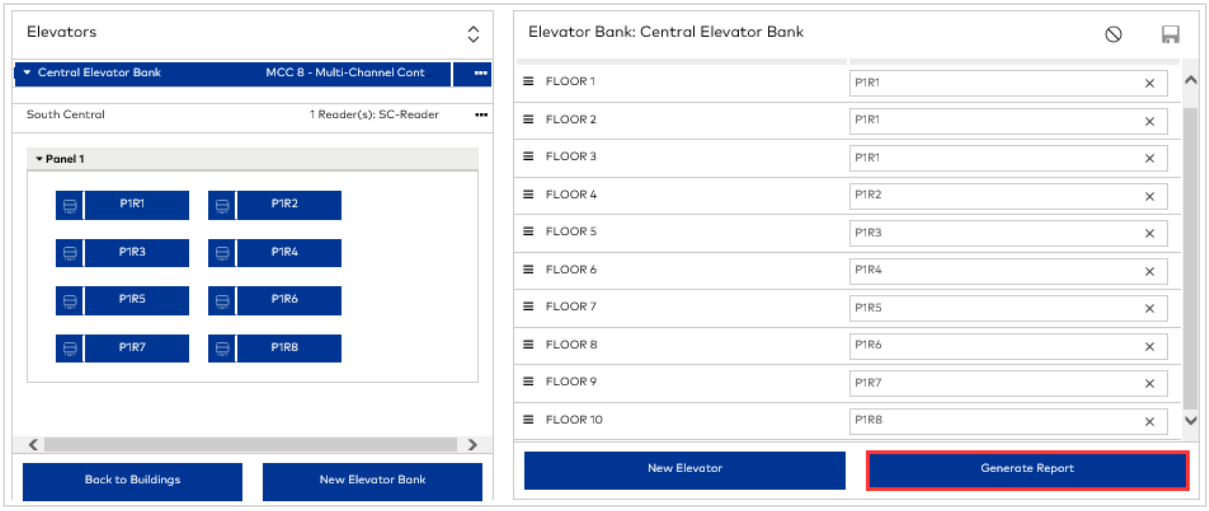
Relay–to–floor mapping controls elevator access to building floors. If you do not map a floor to a relay, there is no elevator access to the floor.

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 add the elevator. 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) .

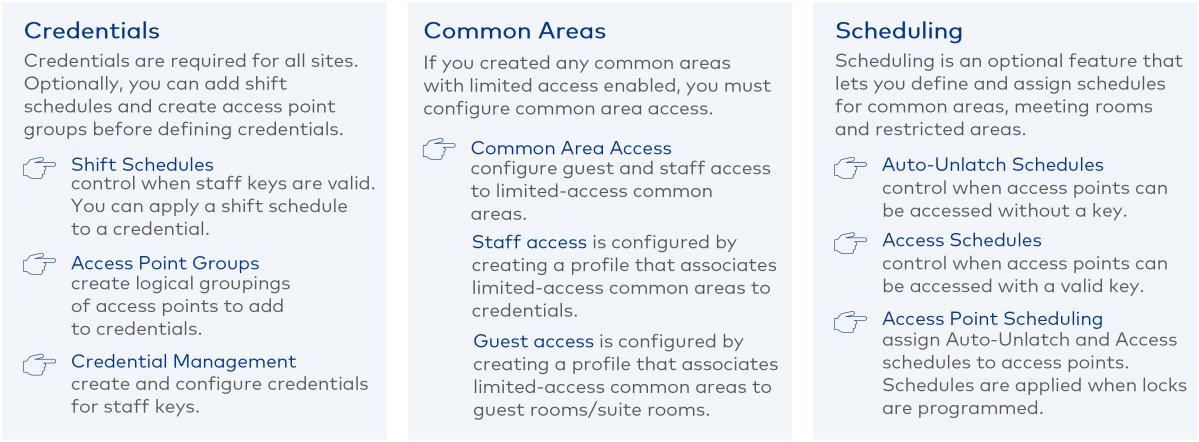


Step 3: Configure Access

This section includes the following subjects:

Learning about Access Management

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 Ambiance 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.

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 by selecting individual access points and access point groups.

Default Credential Classes for Staff Keys

Learn more about each credential class type and the default credential class used to make staff keys:

- **Emergency**—The principal property of the Emergency class type is that keys encoded with this class always override a projected dead bolt or active privacy switch. As such, reserve this class for senior management and emergency personnel.
- **Grand Master**—This is a general purpose class intended for the highest levels of access among staff. The class shares the same properties as the Emergency class except that keys never override a deadbolt or privacy switch.
- **Master**—This is a general purpose class intended for most staff keys.
- **Limited Use Staff**—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 Keys. For example, if the limit is six, the key opens the lock the first six consecutive times then expires.

For keys made using the Emergency, Grand Master and Master class type, additional access points (all access point types except common areas and elevator readers) can be added at key-making time. (Additional Access must be enabled in System Settings > Staff Keys.)

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 Guest Keys

The credential class and credentials used to make keys for guests are implicit. In other words, you don't select a Guest credential class/credential. Instead, the access points selected during guest registration, including any guest rooms, suite rooms, common areas and meeting rooms, form the credential that authorizes entry. Only in the Reports module is there a reference to a Guests credential class. When selecting options for the Key/User Assignment Report, you can select the Guest class and Limited Use Guest class to include a list of all access points encoded on keys assigned to guests.

Common Areas

Common areas are access points that are configured for general access by guests and/or staff. Guest Common Areas include spaces such as the lobby, parking areas and fitness rooms. Staff Common Areas may include administrative offices, breakrooms and supply closets.

Access to common areas depends on the credential class type selected when making a key and the options selected when the access point was created. The following policies apply to enabling staff access to common areas:

- For keys made using the **Emergency** or **Grand Master** credential class type, access to all common areas (guest and staff) is configured by credential assignment. In other words, the common area must be included in the credential selected when making the key.
- For keys made using the **Master** or **Limited Use Staff** credential class type, access to common areas depends on whether the common area is a Guest Common Area or Staff Common Area and the options selected when the access point is created. The folllowing policies apply:
  - Unlimited Guest Common Areas
    - If staff access was enabled by Credential Assignment, the common area must be included in the credential selected when making the key.
    - If staff access was enabled by Common Area Access Profile Assignment, access is enabled by default.
  - Limited Guest Common Areas
    - If staff access was enabled by Credential Assignment, the common area must be included in the credential selected when making the key.

- If staff access was enabled by Common Area Access Profile Assignment, the credential selected when making a key must be associated with a common area access profile that includes the common area.

- Unlimited Staff Common Areas—Access is enabled by default.
- Limited Staff Common Areas—Access is enabled by Common Area Access Profile Assignment. The credential selected when making a key must be associated with a common area access profile that includes the common area.

Common areas where access is enabled by default or by credential assignment are not listed in the Summary section when making a key. If access is enabled by credential assignment, you can verify which common areas are included in the selected credential in Access Management > Credential Management.

Scheduling

The scheduling feature provides another layer of access control for guest and staff common areas, meeting rooms, restricted areas and elevator readers. Both of the following schedule types are programed directly in the locks:

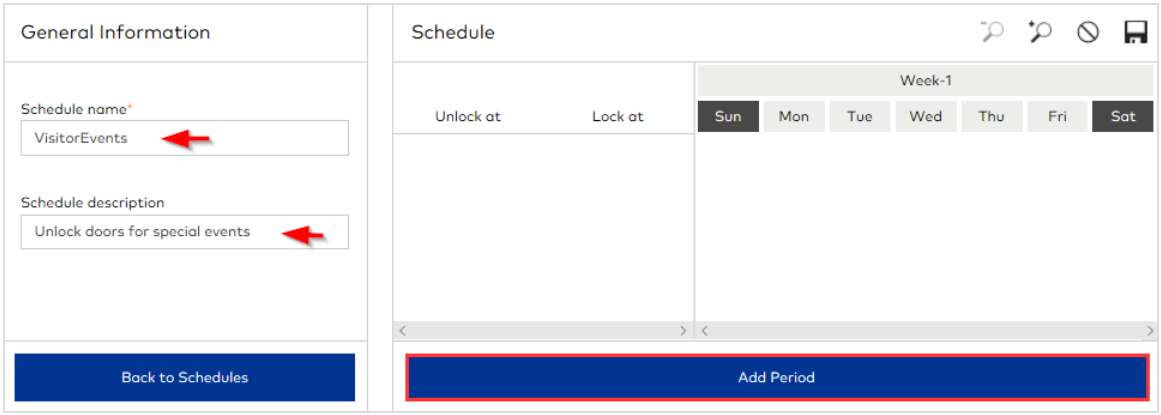
- Auto-Unlatch Schedules establish when an access point can be accessed without a key thereby allowing unrestricted access.
- Access Schedules establish when an access point can be accessed with a valid key. You can assign a different Access Schedule for each credential class in which an access point is included. For example, if the Laundry Room common area is included in a Master credential and a Grand Master credential, you can assign different Access Schedules for each.

Add Auto-Unlatch Schedules

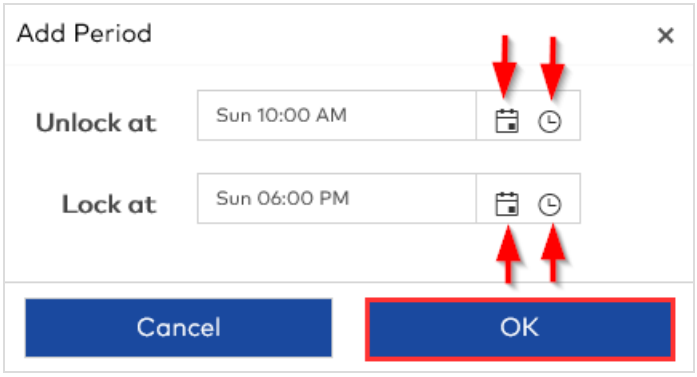
Auto-Unlatch schedules control when common areas, meeting rooms and restricted areas can be accessed without a key. For more information about schedules, see Working with schedules.

To add a schedule:

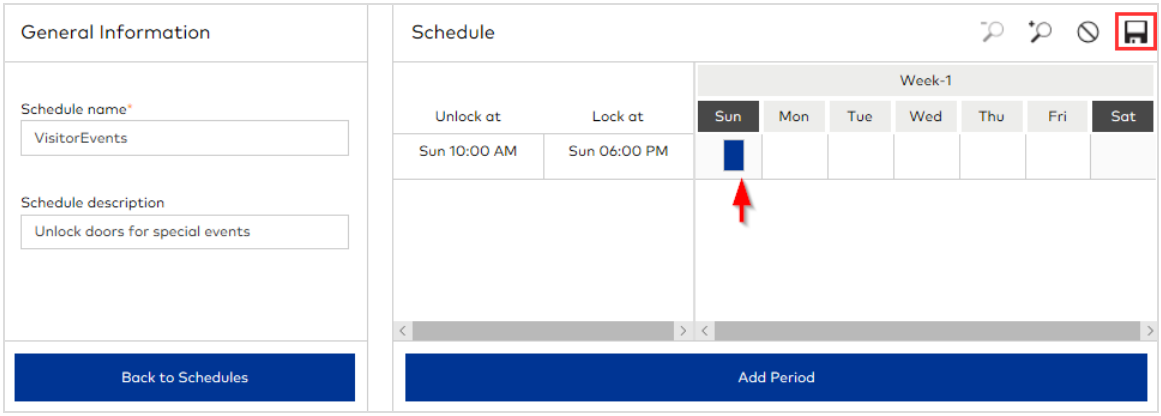
1. Go to Access Management.
2. Click **Auto-Unlatch Schedules**.
3. Click (Add) +.



4. Specify a descriptive name for the schedule.
5. (*optional*) Specify a description for the schedule.
6. Click **Add Period**.



7. Select the day and time for the access point to unlatch.
8. Select the day and time for the access point to latch.
9. Click **OK**. You can add multiple periods per day, but periods cannot overlap.



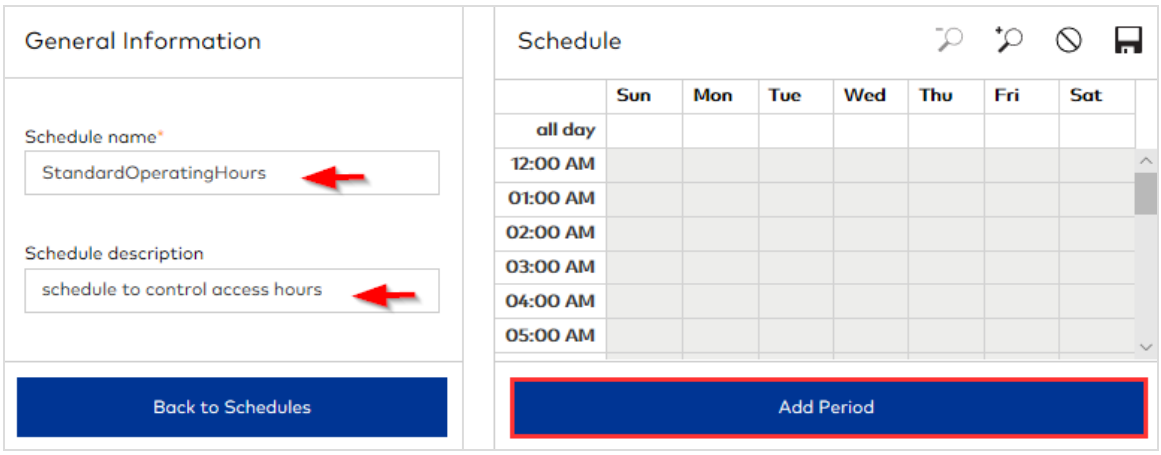
10. Click (Save) .

Add Access Schedules

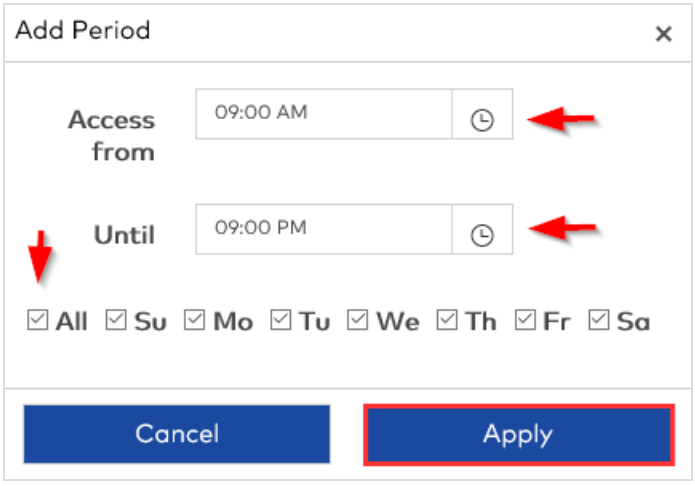
Access schedules control when common areas, meeting rooms, restricted areas and elevator readers can be accessed with a key.

To add a schedule:

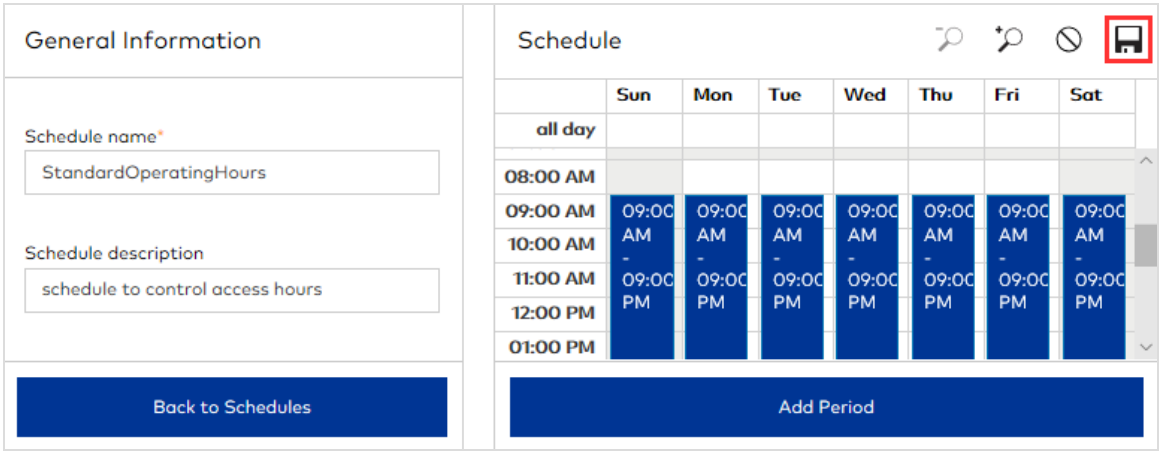
1. Go to Access Management.
2. Click **Access Schedules**.
3. Click (Add) +.



4. Specify a descriptive name for the schedule.
5. (*optional*) Specify a description for the schedule.
6. Click **Add Period**.



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



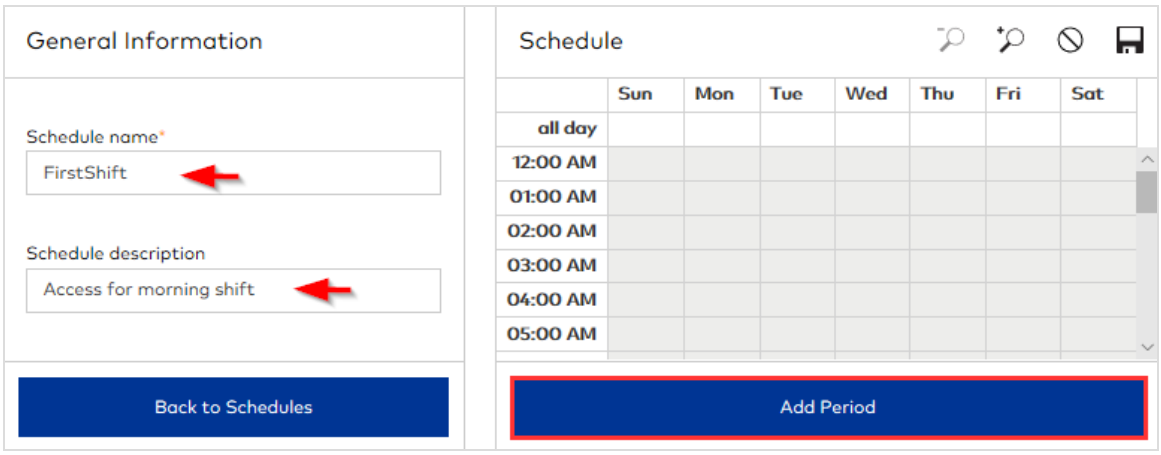
11. Click (Save) .

Add Shift Schedules

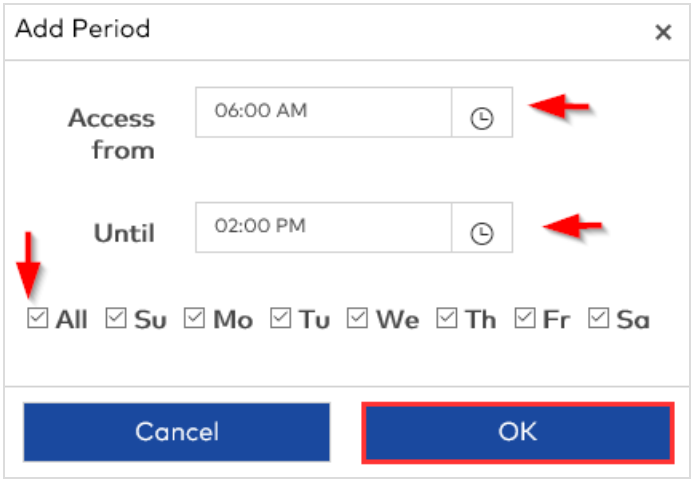
Shift schedules control when staff credentials can access common areas, meeting rooms and restricted areas.

To add a schedule:

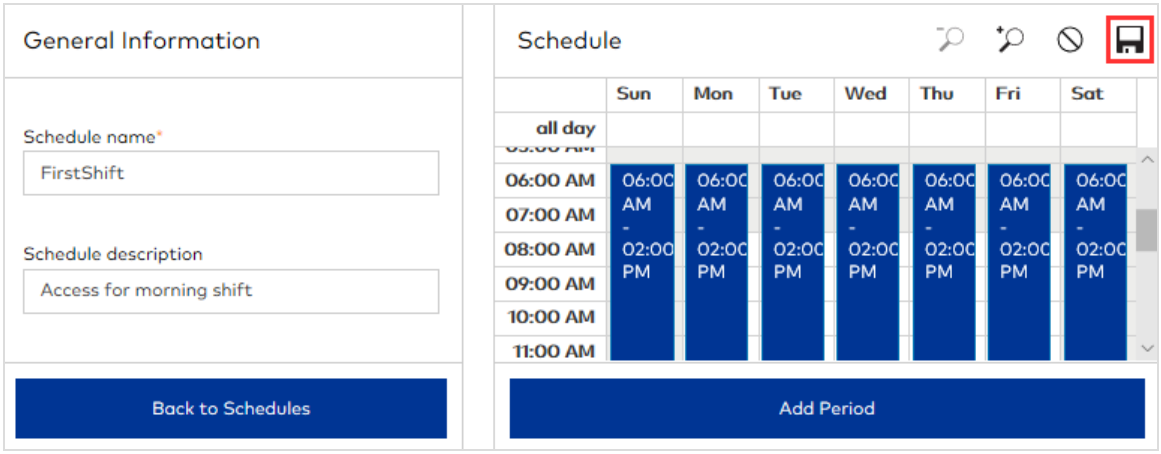
1. Go to Access Management.
2. Click **Shift Schedules**.
3. Click (Add) +.



4. Specify a descriptive name for the schedule.
5. (*optional*) Specify a description for the schedule.
6. Click **Add Period**.



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



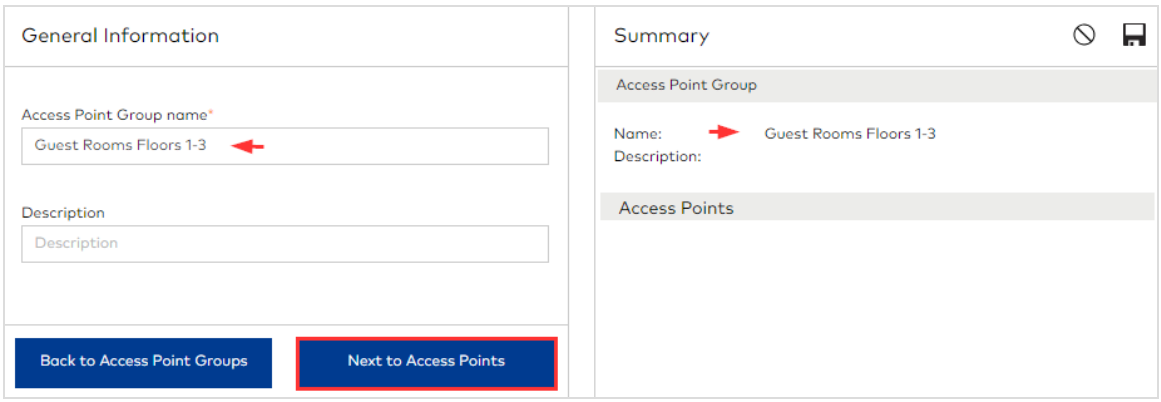
11. Click (Save) .

Create Access Point Groups

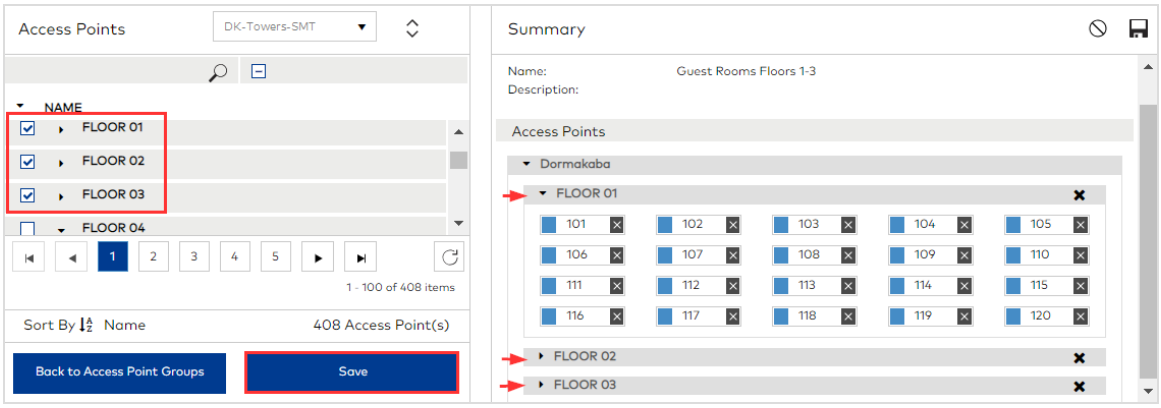
Organizing access points into logical groups based on location or intended use facilitates the assignment of credentials.

To add an access point group:

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



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



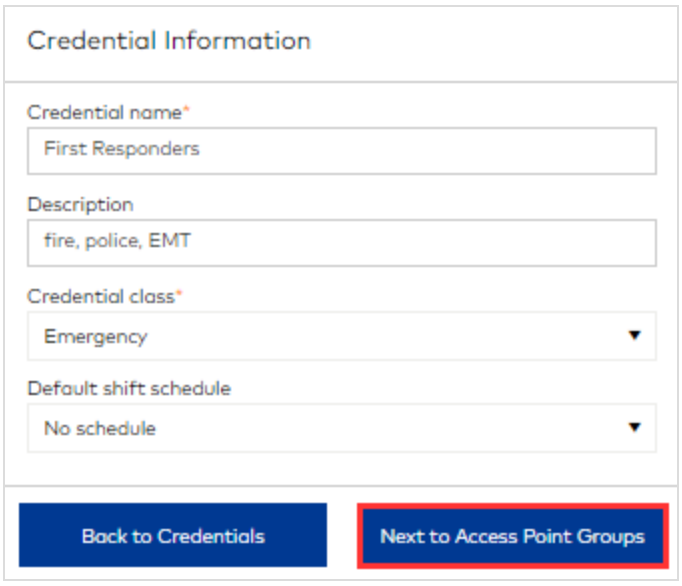
7. Select the access points that you want to assign to the group. Selected access points are added to the Summary section (listed by building and floor).
   - You can select access points from different buildings.
   - You cannot add guest or staff common areas to access point groups.
8. Click **Save**.

Add Credentials

The only credentials that you need to add during site configuration are for staff keys. To learn more about credentials, including credential classes, see Understanding Credentials.

To add a credential:

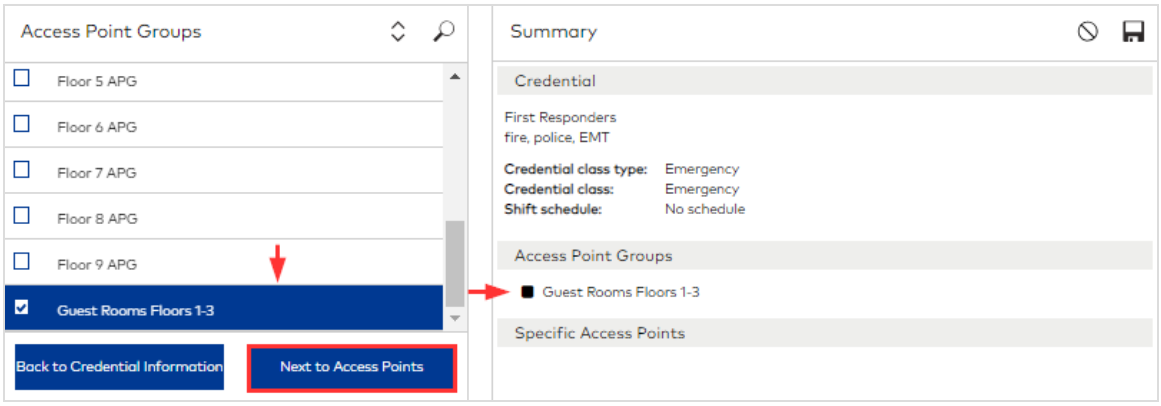
1. Go to Access Management.
2. Click **Credential Management**.
3. Click (Add) +.



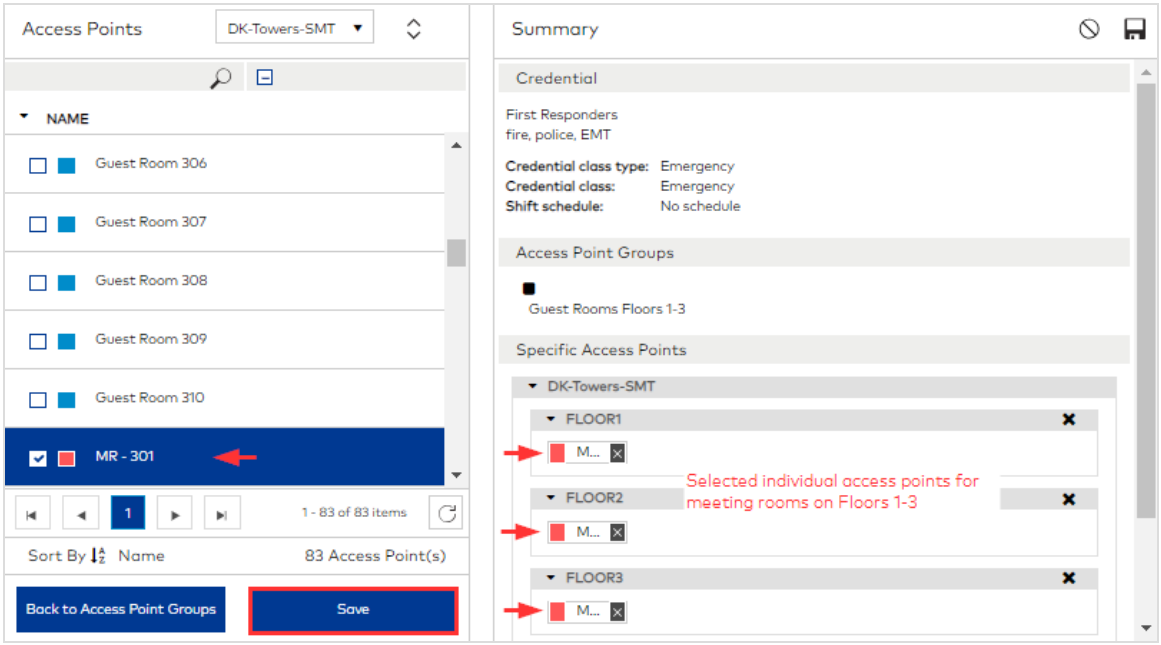
4. Specify a descriptive name for the credential.
5. (*optional*) Specify a description for the credential.
6. Select a credential class. For a description of each class, refer to Learning about Access Management.

> 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.

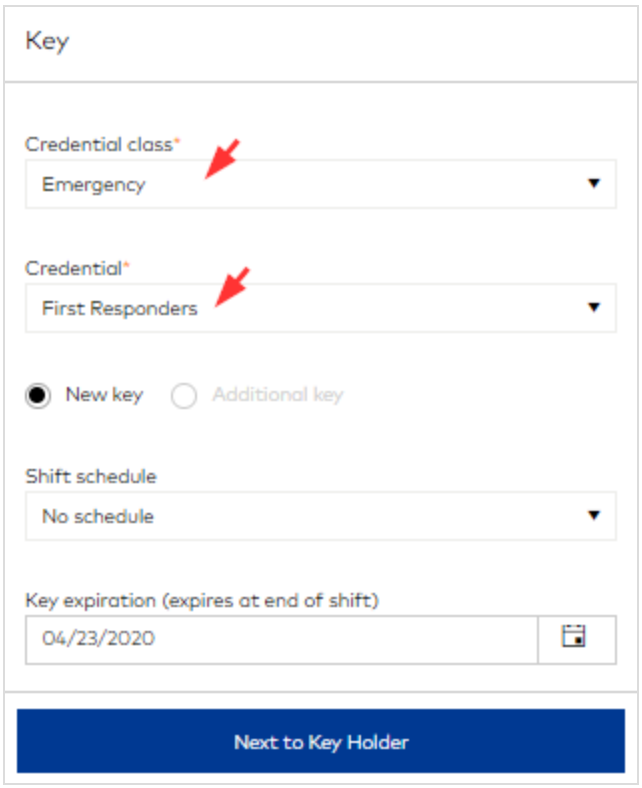
7. Select a shift schedule during which the key is valid. To enable 24/7 access, select **No Schedule**. The selected shift schedule determines the days and hours that the key is valid. To review shift schedule details, see **Access Management** > **Shift Schedules**. (A different shift schedule can be selected at key-making time.)
8. Click **Next to Access Point Groups**.



9. Select the groups that you want to add to the credential.
10. Click **Next to Access Points**.



11. 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. All access point types are listed except additional floor access, which is selected at key-making time.
12. Click (Save) . The following figure shows the First Responders credential available to select when making a staff key.

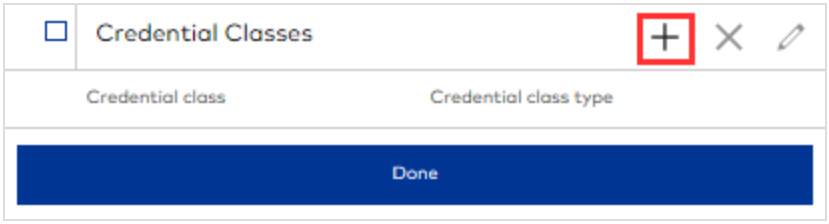


Add Custom Credential Classes

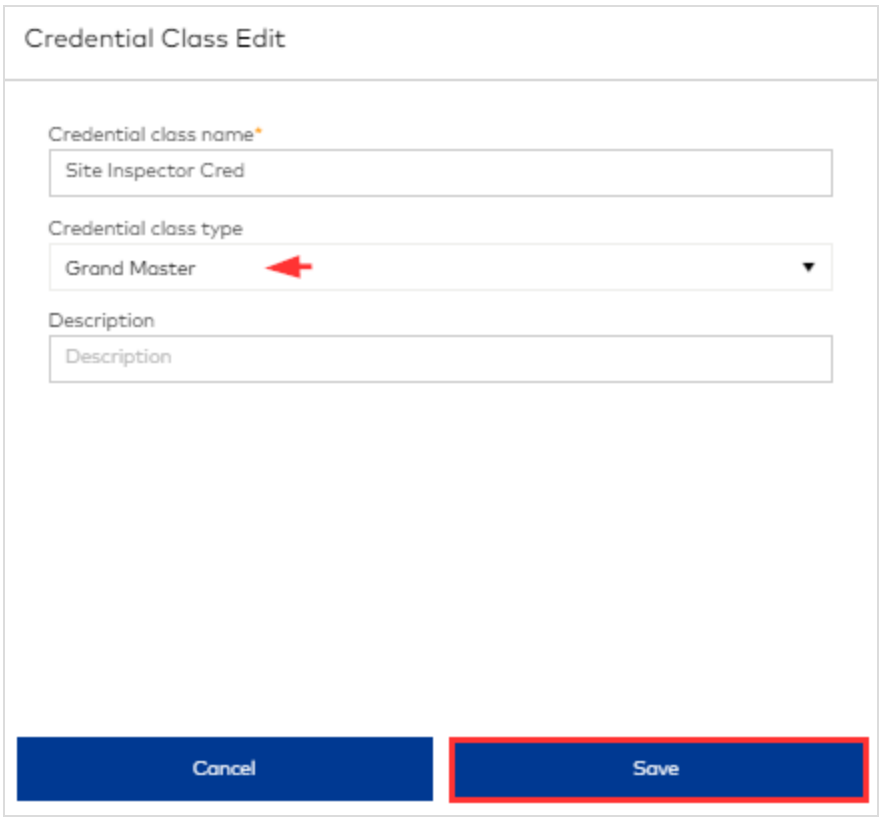
When selecting a credential class for a credential, you have the option to edit credential classes. Although you cannot edit or delete the default classes, you can add a class based on one of the default classes.

To add custom credential classes:

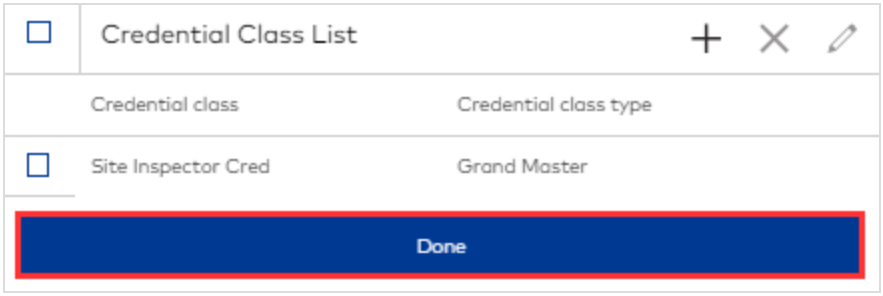
1. When selecting a credential class for a new credential, select **Edit Credential Classes**.



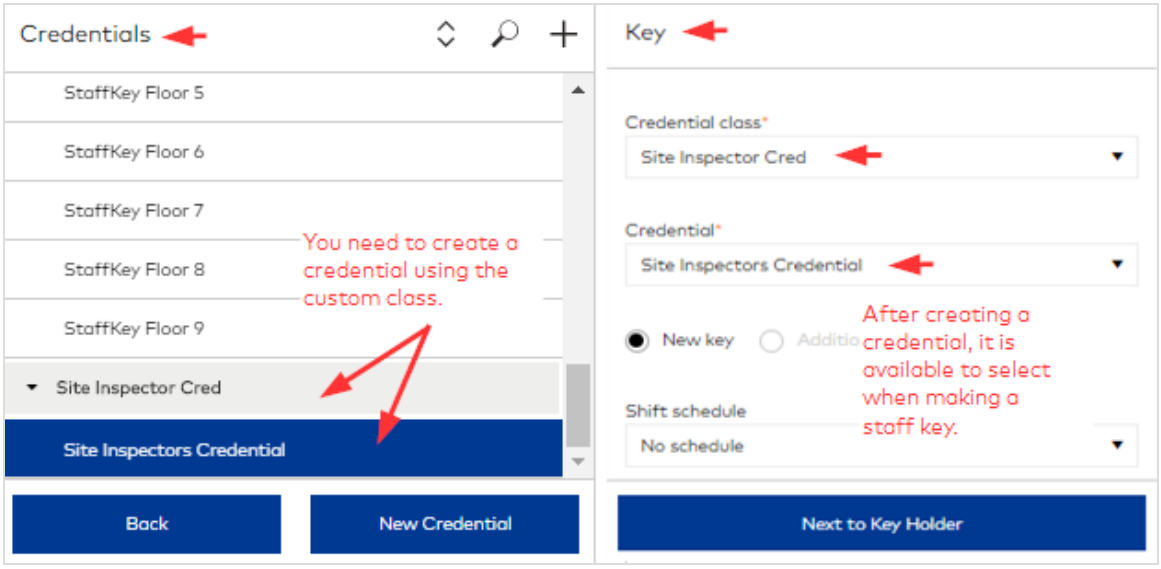
2. Click (Add) +.



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 key.



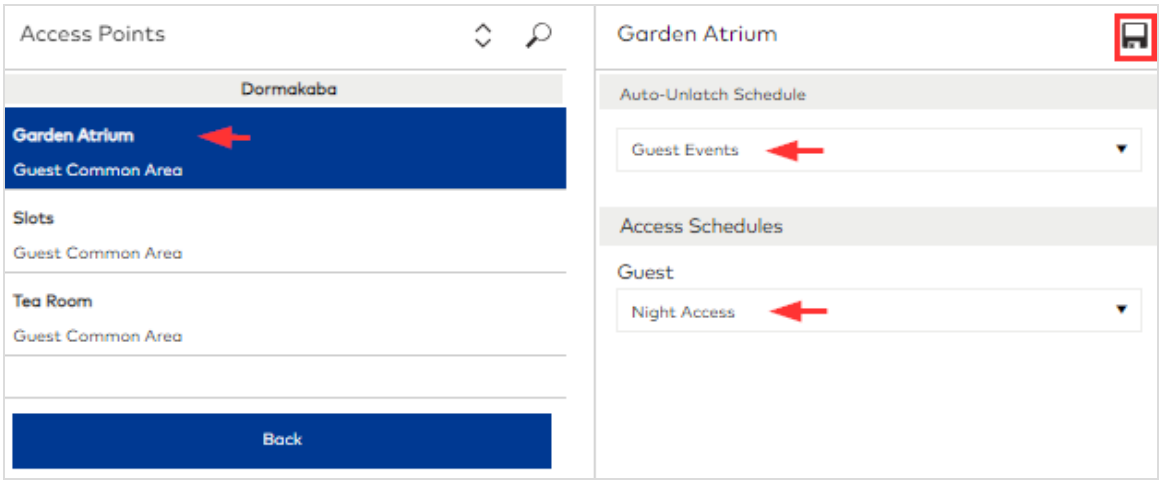
Assign Schedules

Auto-Unlatch schedules can be assigned to common areas, meeting rooms and restricted areas. Access schedules can be assigned to common areas and meeting rooms.

> 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: Guest, Staff - Limited Use Staff and Staff - Master credential classes.

To assign schedules to an access point:

1. Go to Access Management.
2. Click **Access Point Scheduling**.



3. Select an access point.
4. Select an Auto-Unlatch Schedule to apply to the access point. The default selection (24/7) means no schedule is applied.
5. 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.
6. Click (Save) .

Configure Access Profiles for Limited-Access Common Areas

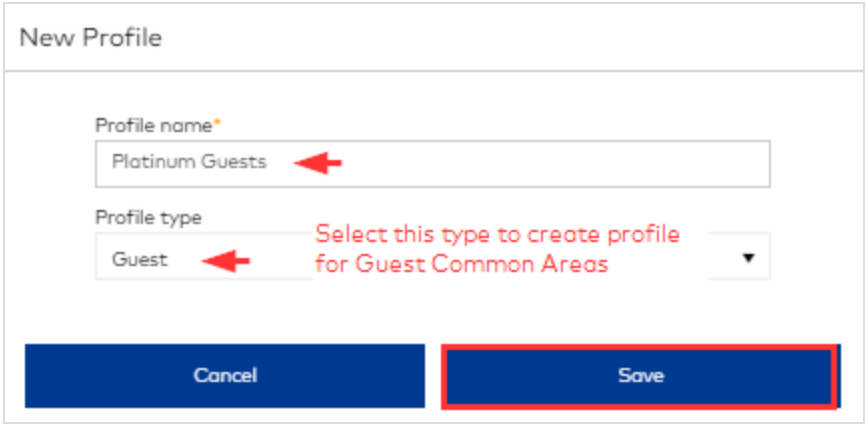
Create and configure profiles that associate guest rooms or staff credentials to limited-access common areas.

Configure Guest Access to Limited-Access Common Areas

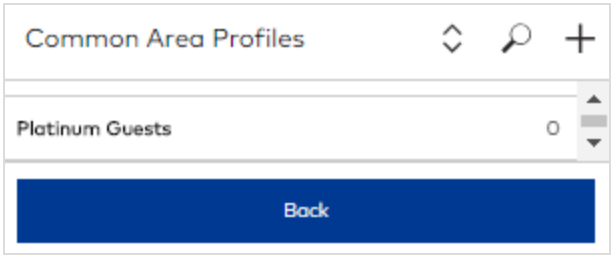
Guest access to limited-access common areas can be configured as soon as all guest rooms, suite guest rooms and limited-access common areas are created in Property Builder. The process involves adding a guest profile and then associating common areas to guest rooms and suite guest rooms.

Add a Guest Profile

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



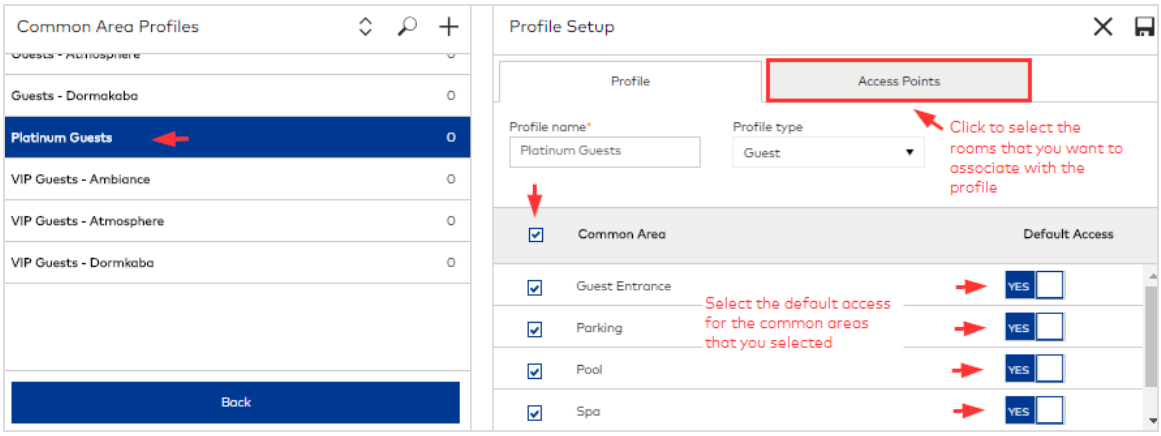
4. Specify a descriptive name for the profile.
5. Select profile type Guest.
6. Click **Save**. The profile is added to the list.



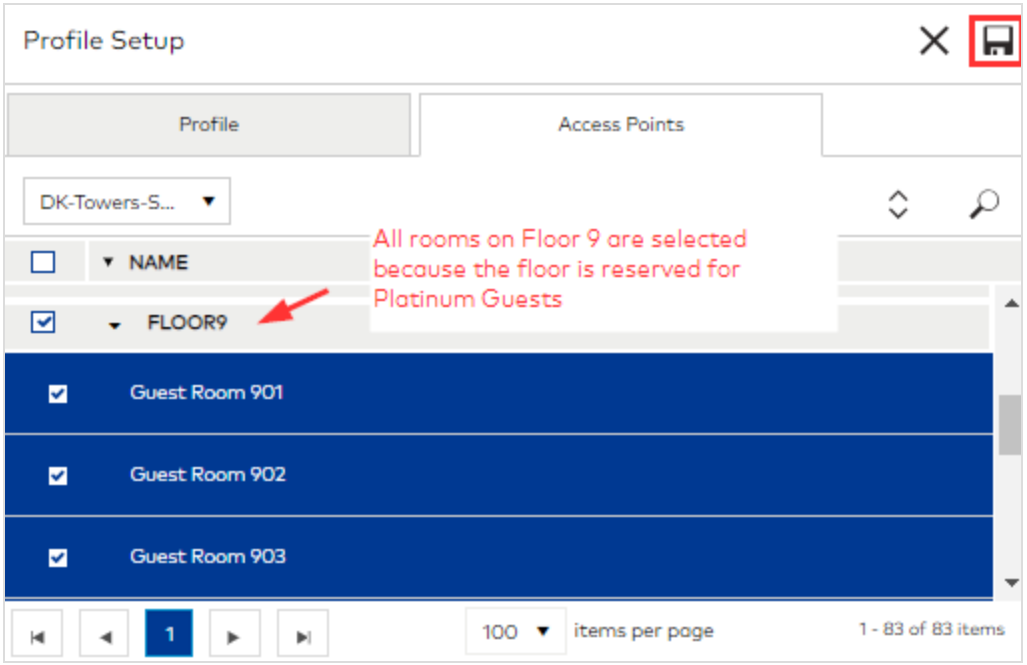
Associate Common Areas to Guest Rooms/Suite Guest Rooms/Meeting Rooms

To associate guest rooms to common areas:

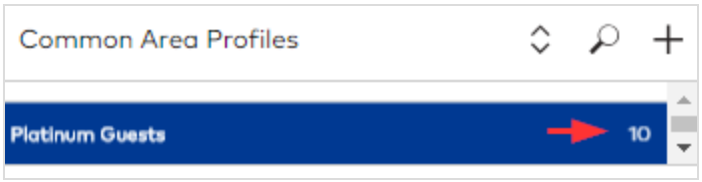
1. Go to Access Management.
2. Click **Common Area Access**.



3. Select an existing common area profile or add a new profile.
4. 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 guest registrations.



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



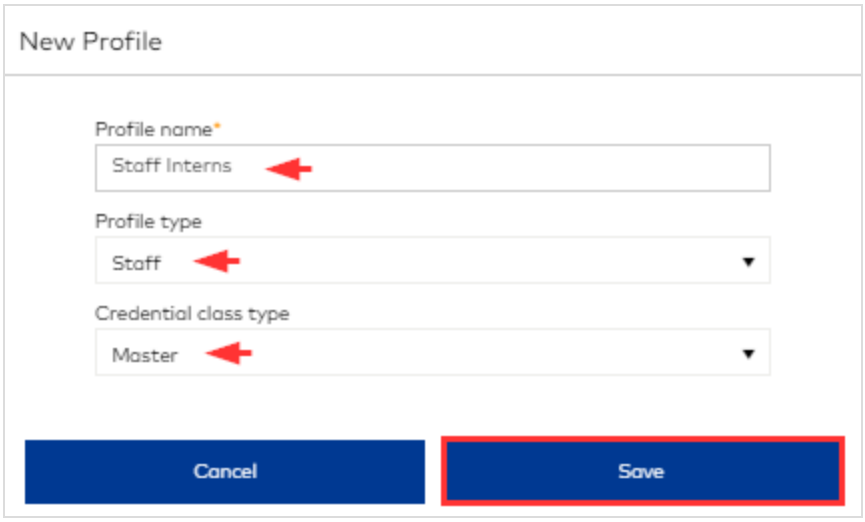
Configure Staff Access to Limited-Access Common Areas

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

Add a Staff Profile

1. Go to Access Management.
2. Click **Common Area Access**.

3. Click (Add) +.



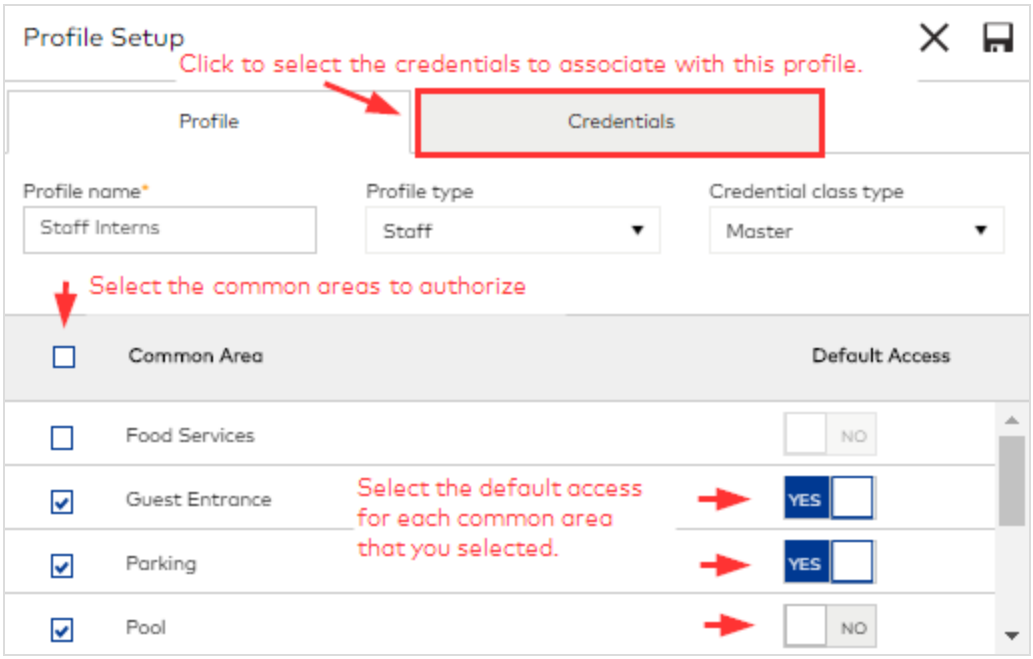
4. Specify a descriptive name for the profile.
5. Select the Staff profile type.
6. Select a credential class type. Your selection determines the credentials that you can associate with the common areas selected on the Profile tab. You can only associate credentials that were made using the same class type. For more information, see Working with Limited-Access Common Areas in *Learning about Access Management*.
7. Click **Save**. The profile is added to the list.

Associate Common Areas to Credentials

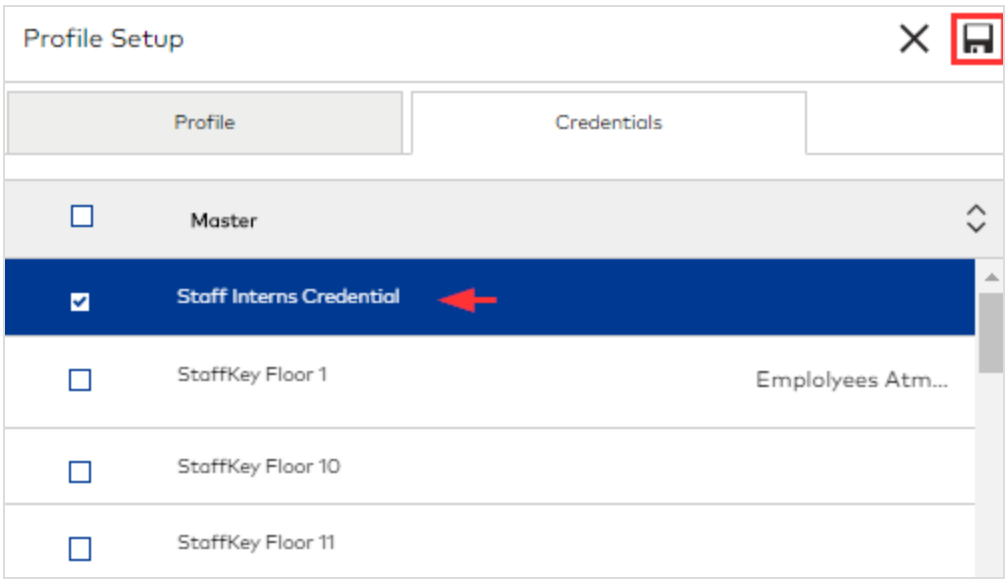
To associate units to common areas:

1. Go to Access Management.
2. Click **Common Area Access**.

3. Select an existing common area profile or add a new profile.



4. 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 Keys.



5. 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.

Step 4: Program Locks

This section includes the following subjects:

Learning about Programming/Auditing

Programming/Auditing is the Ambiance 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 Ambiance workstation and locks. To program locks, configuration data is transferred from the Ambiance 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 Ambiance workstation.

Programming Locks

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

Ambiance 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 Icon	Description
	Guest Room
	Guest Common Area
	Suite Common Door
	Suite Inner Door
	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:
  - Guest Rooms
  - Suite Common Door and Inner Doors
  - Meeting Rooms
  - Restricted Areas
  - Guest 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 > Security

- After modifying Lock Access settings.

System Settings > Staff Keys

- After modifying the **Maximum number of times Staff 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 that are enabled for mobile keys must be reprogrammed.

Auditing Locks

The Ambiance data transfer function also enables individual lock audits to track and store historical activity about access points. The data that is collected from locks and transferred to Ambiance is stored in the Ambiance database and available when generating Access Point Audit Reports.

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.

Auditing Online Access Points

When Remote Lock Management is enabled in System Settings, online access points can be audited directly in Ambiance.

Program Locks

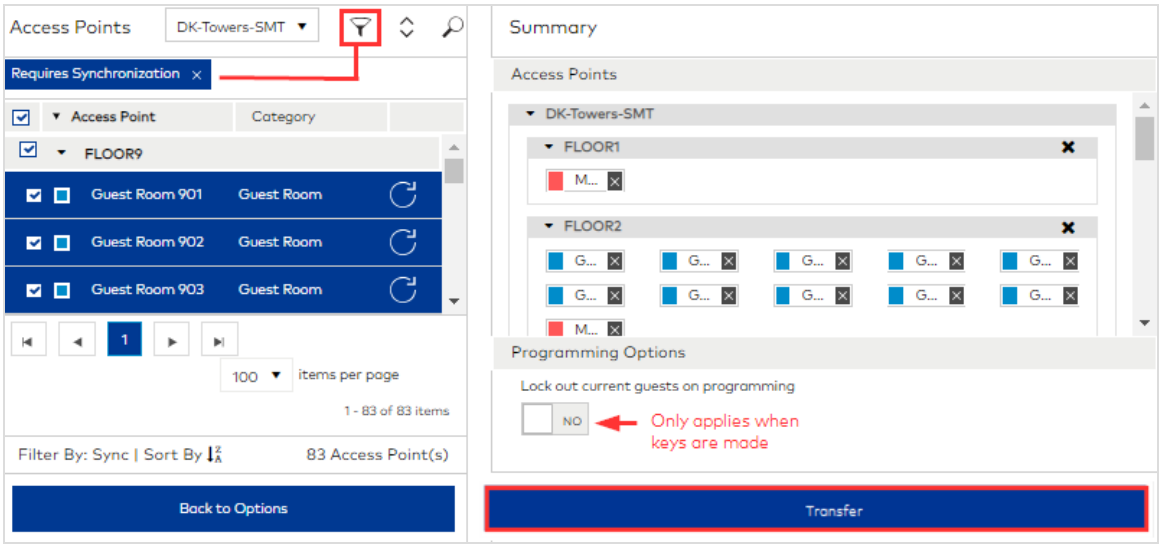
By default, M-Unit authentication is enabled. Before programming locks, you must either configure M-Unit credentials for at least one Operator or disable M -Unit authentication in System Settings > Security. If you opt to require authentication, dormakaba suggests that you add M-Unit credentials for the default Admin01 account. Go to Staff Management, select Admin01, click the Operator Info tab, specify and save credentials in the Maintenance Unit Login section.

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:

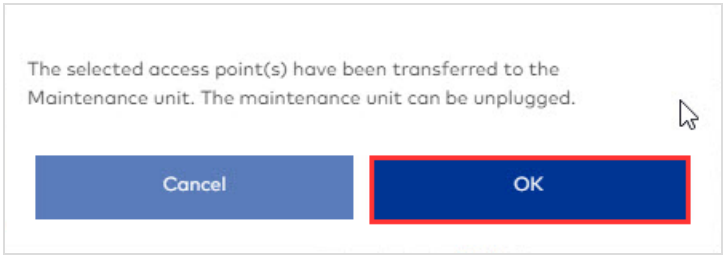
1. Go to Programming/Auditing.
2. Click **Programming**.



3. Select the access points that you want to synchronize with Ambiance 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 guest on programming** option only applies when keys have already been made and issued.

4. Connect the M-Unit to the workstation.
5. In Ambiance , 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 following steps are performed on the M-Unit. For official instructions, refer to the documentation distributed with your device.

8. On the M-Unit menu, select **LOCKS**.
9. Use the UP / DOWN arrow keys to highlight **1- Program**, then press **ENTER**. The access point names display in groups of five.
10. 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.
11. Select the type of probe that you are using to connect the M-Unit to the lock.

12. 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.
13. When prompted that programming is complete, click **OK**.

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

Step 5: Configure Devices

This section includes the following subjects:

Learning about Device Management

Device Management is the Ambiance module where you configure encoders and, when licensed for Remote Lock Management, work with the hubs that support online communication.

Encoders

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

> Only KABA RFID encoders with the minimum firmware version 1.12 (or greater) are supported.

Prerequisites

The following prerequisites are automatically met during initial Ambiance installation.

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

TCP/IP or USB Connections

When configuring encoders, you can select the TCP/IP or USB connection method. Regardless of the method that you select, the encoder must be connected via USB cable to the workstation for the initial configuration.

If you select the TCP/IP method and you have multiple workstations, you only need to configure the encoder on one workstation. If you select the USB method, you must configure an encoder on each workstation.

A TCP/IP-configured encoder connects directly to the Ambiance Server (not to workstations). A site can be deployed with several TCP/IP and/or USB encoders. Several workstations can use a shared USB or TCP/IP encoder. Not all workstations require an encoder.

⚠ If you change the connection type from TCP/IP to USB or from USB to TCP/IP after saving the initial configuration, you must restart the encoder (unplug, wait five seconds, then plug in again).

Hubs & Paired Access Points

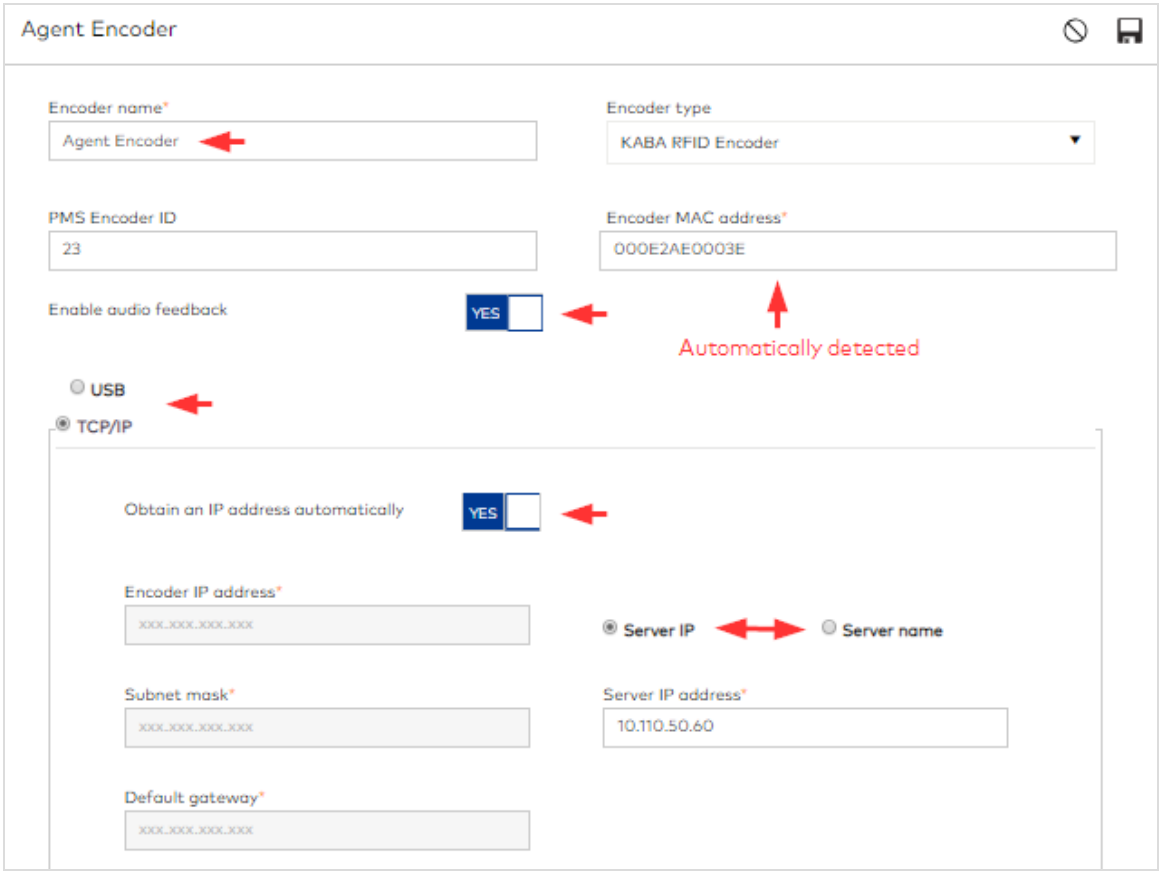
Hubs are the network devices used to communicate the configuration data in Ambiance to the locks installed at paired access points. After commissioning and connecting hubs to the Ambiance Server, hubs are listed in Device Management. When a hub status is Online, access points can be paired. Multiple hubs can be connected to Ambiance, but an access point can be paired with only one hub.

This chapter contains instructions to view the status of and issue commands to hubs and paired access points. For more information, see Working with Remote Lock Management.

Add Encoders

To add encoders:

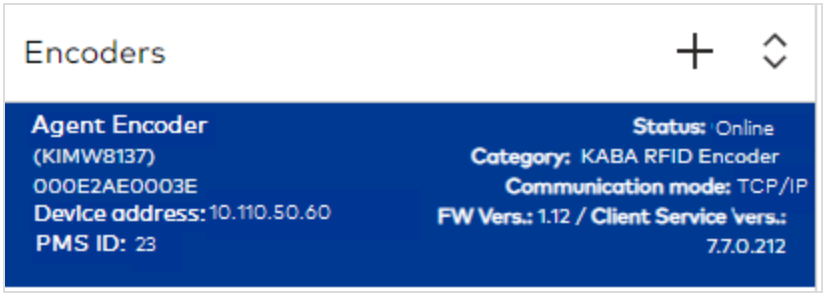
1. Connect the encoder via USB to the workstation. The initial configuration of an encoder requires that you connect the encoder to the Ambiance workstation using a USB cable. By default, the device emits two audible beep and flashes a green light to indicate a successful connection.
2. Go to Device Management.
3. Click (Add) +.



4. For **Encoder name**, specify a unique name that does not exceed 50 characters. This name displays in the list of encoders.
5. Accept the default encoder type **KABA RFID Encoder**.

6. (*conditional*) If integrating a third-party PMS, 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. (If the value is not detected, refer to Troubleshooting Encoders.)
8. Select whether the encoder emits audible beeps when a successful connection is made with the workstation and when making keys.
9. Select the method (**TCP/IP** or **USB**) to connect the encoder with the workstation after initial configuration. If you select the TCP/IP method, configure the following options:
   - Define the network configuration for the encoder device. Select whether to automatically obtain an IP address or specify values for a static IP address, subnet mask and default gateway. If specifying static information, consult your network administrator to verify the values.
   - Specify the IP address or name of the server where Ambiance is installed.

   If you choose to use a static IP address and specify the server name (instead of server IP address), you must also specify the Local DNS IP address.
10. Click (Save) . 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. If you selected the TCP/IP method, the encoder can be disconnected from the USB port but must be connected to the network before the status changes to Online.

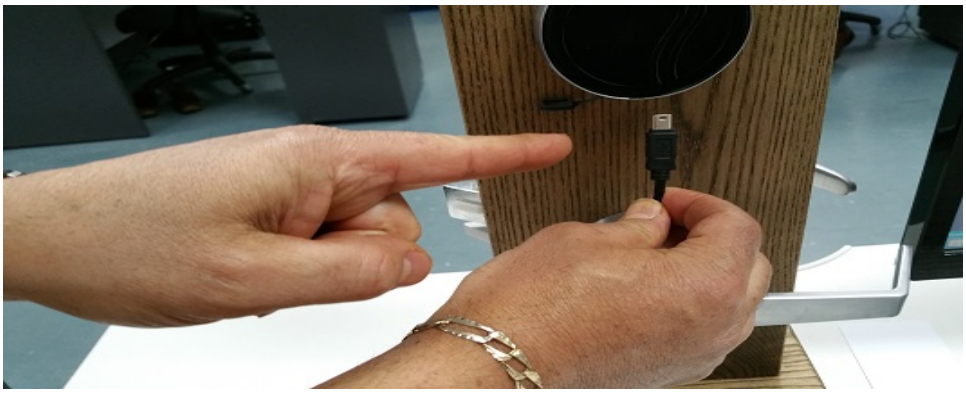


Maintenance Unit

The M-Unit (Maintenance Unit) is a hand-held embedded device used to transfer data between Ambiance and the locks installed at access points. The device is used to program and audit locks. Firmware version 1.52 or greater is required.

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 Management.

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.

Step 6: Add Notification Groups

This section includes the following subjects:

Learning about Notification Management

> Notification Management is available only when Remote Lock Management is enabled (System Settings > Advanced) and the Notification Management right is selected in the role assigned to the Operator.

Notifications 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 guest 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 profiles in Staff Management.

The following notifications are available:

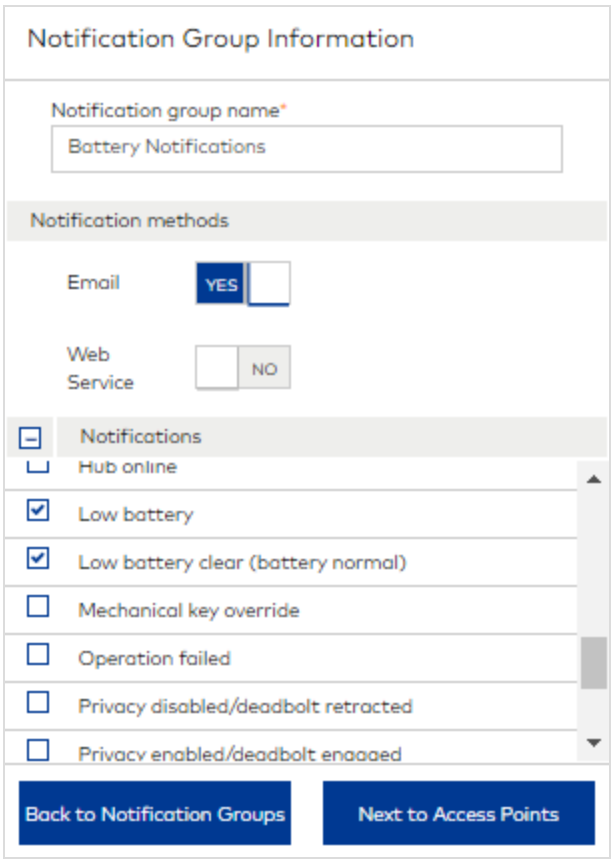
- Access point offline—Notifies that there is no communication between the lock and the hub.
- Access point online—Notifies that the lock is in communication with the hub and online.
- Access point paired—Notifies that an access point was paired to a hub.
- Door ajar clear (door secure)—Door previously ajar has now been closed and is secure.
- Door ajar generic—Notifies that a door is in an open state.
- Door ajar guest 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 guest 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 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 staff 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 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.
- Guest key used—Date and time that a guest key was used at the access point.
- Guest key used (first entry)—Notifies a guest has accessed the lock for the first time.
- Hub offline—Hub is currently not communicating with the Ambiance Server.
- Hub online—Displays all hubs 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.
- Staff key used—Notifies that a Staff key 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.

Add Notification Groups

To add notification groups:

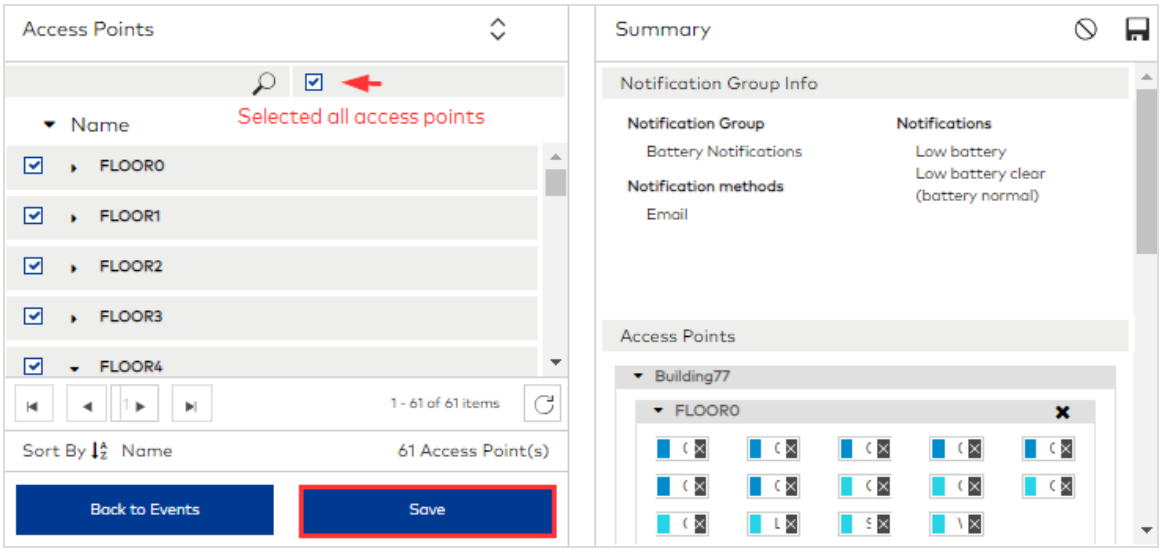
1. Go to Notification Management.



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 Ambiance.
   - Email—Send notifications by email. Recommended value: YES. Requires email configuration in System Settings > Email and an email address defined in staff profiles in Staff Management.

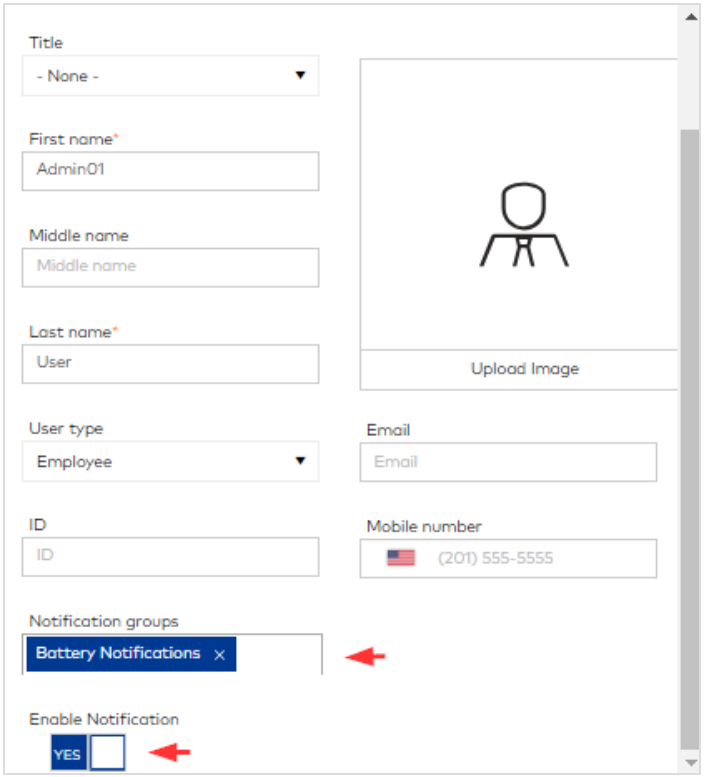
- Web Service—Send notifications through the Web Service using either the SOAP or REST protocol. You must also specify the Web Service URL.

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 profiles in Staff Management.


Title
- None -
First name*
Admin01
Middle name
Middle name
Last name*
User
Upload Image
User type
Employee
Email
Email
ID
ID
Mobile number
(201) 555-5555
Notification groups
Battery Notifications
Enable Notification
YES

Step 7: Review & Customize Operator Roles

This section includes the following subjects:

Learning about Role Management

Role Management is the Ambiance module where the roles that are assigned to Operators are configured. A role is a grouping of rights that authorizes access to Ambiance 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.

Predefined and Custom Roles

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

- Administrator
- Site Configurator
- Front Desk Agent
- Staff Manager

The rights selected for predefined roles cannot be modified, but you can add custom roles to configure a unique group of rights. Custom roles are entirely configurable and can be modified at any time. When you modify the rights authorized for a custom role, 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 Ambiance:

- **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 Keys** is a category of key rights. When the entire **Staff 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 Ambiance 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.

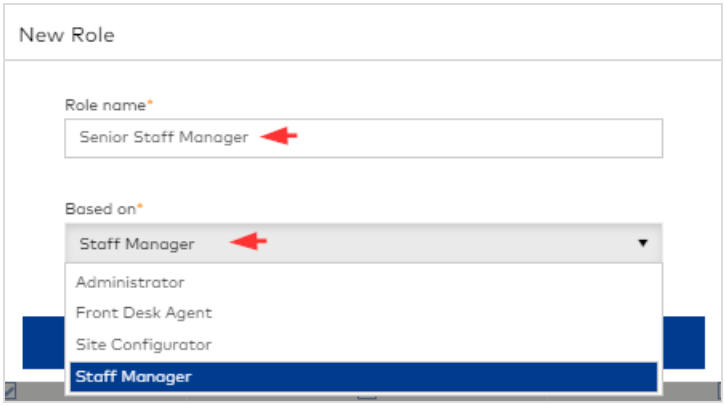
Role	System Rights	Key Rights
Administrator	All	All
Site Configurator	All	All
Staff Manager	Read and Erase Keys Guest Registration Key/User Assignment Report Staff Access Report Staff Keys Staff Management	None
Front Desk Agent	Read Keys Guest Registration	None

Configure Custom Roles

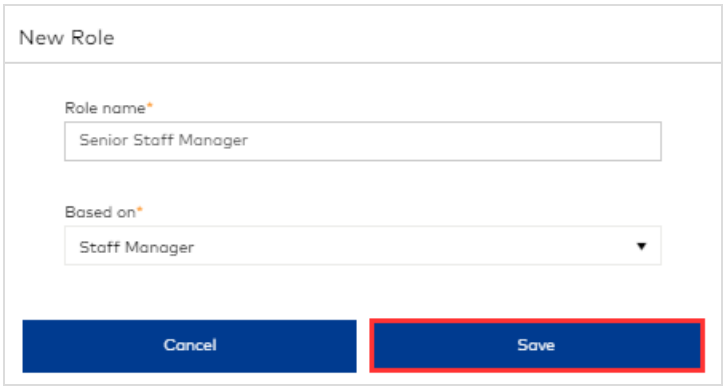
Custom roles offer the flexibility to authorize any combination of system and key rights.

To configure a custom role:

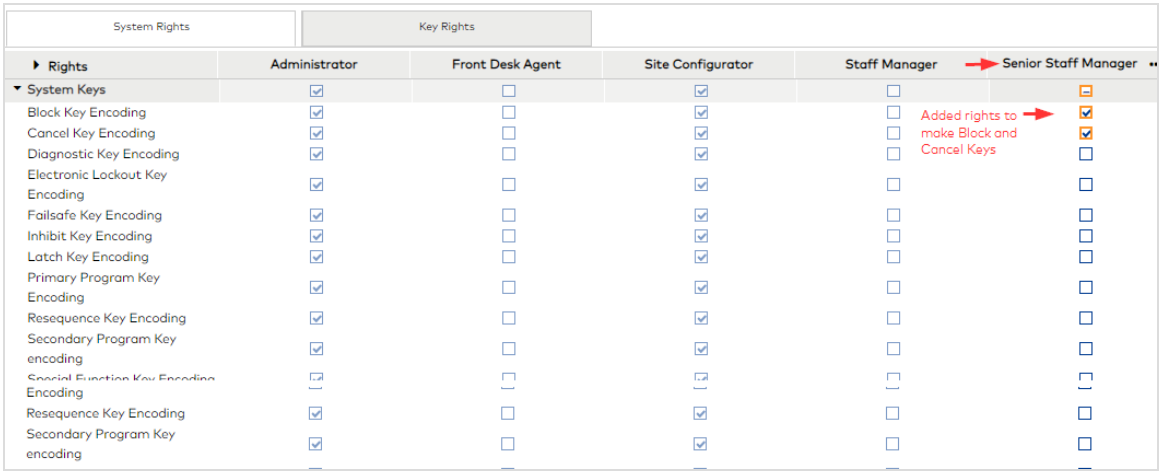
1. Go to Role Management.
2. Click (Add) +.



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 8: Add Operators

This section includes the following subjects:

Learning about Staff Management

Staff 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 Ambiance. The staff who have access to Ambiance are called *Operators*.

A staff member is designated as 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 Ambiance functions whereas the rights for an Operator with the predefined role *Front Desk Agent* are limited to Guest Registration and Read Key functions.

Staff Profiles

When a staff member is added to Ambiance, a profile is created with the following tabs:

- **Staff Member Info**—This tab is where basic identification details about staff are defined. 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.
- **Active Keys**—This tab lists active keys assigned to the staff member. You can cancel and/or replace keys in the list.

To view a staff member profile:

» Go to Staff Management and select a staff member.

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

Staff Keys

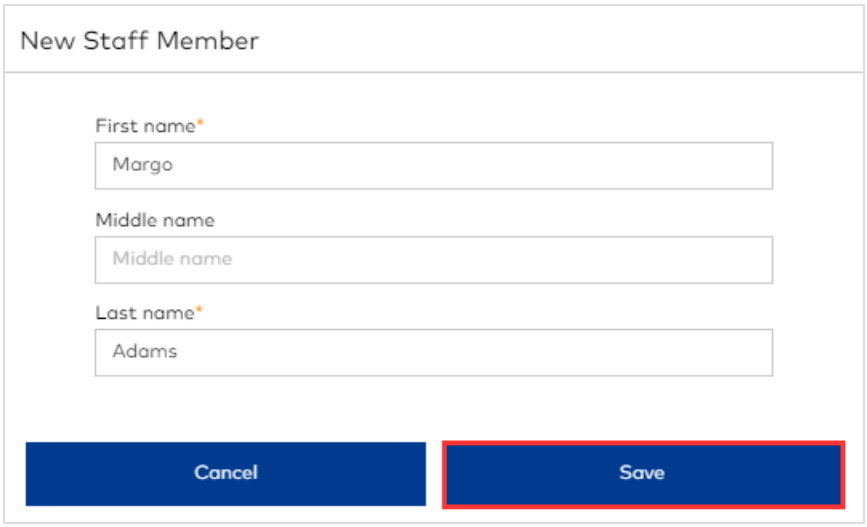
Staff keys are made and issued to people who work on the site, which may include employees, contractors and vendors. Staff keys are encoded with a credential that may include access to all access points types: guest rooms, suites, common areas (guest and staff), meeting rooms and restricted areas.

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

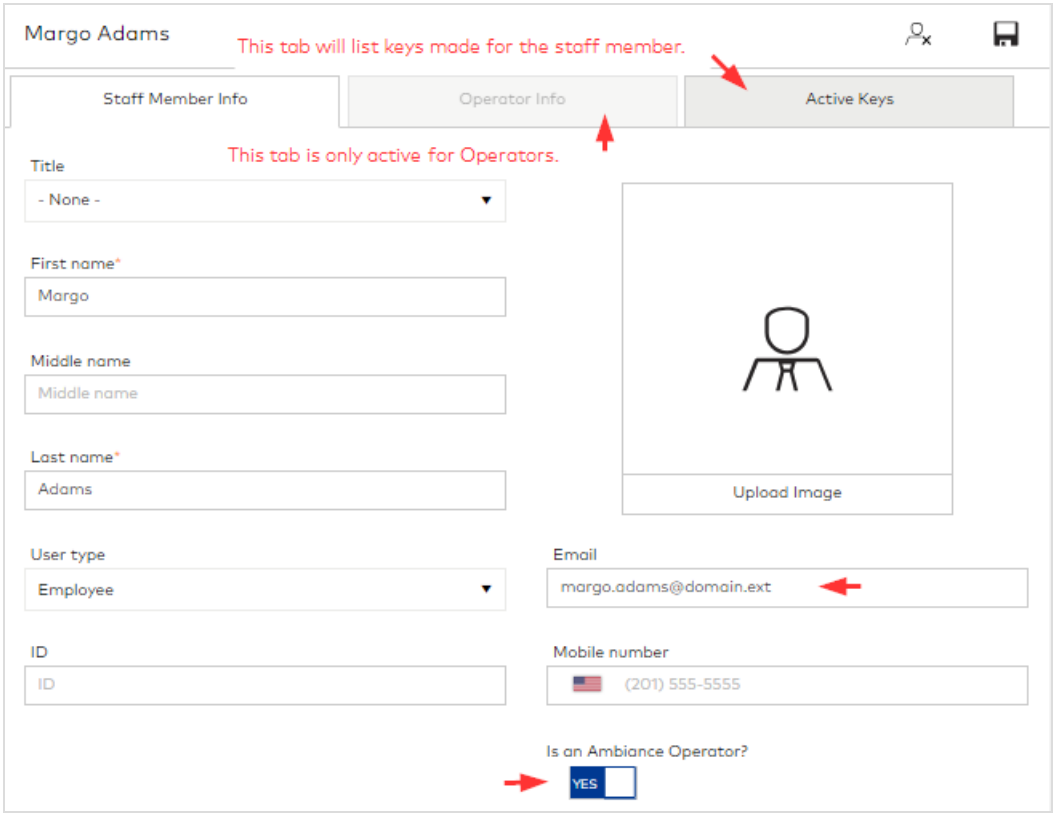
Configure Operators

To add and configure Operators:

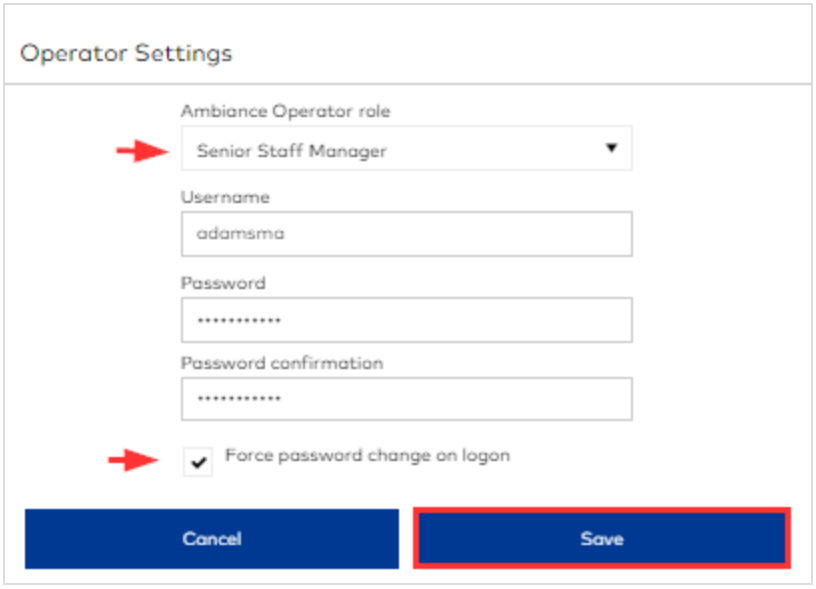
1. Go to Staff Management.
2. Click (Add) .



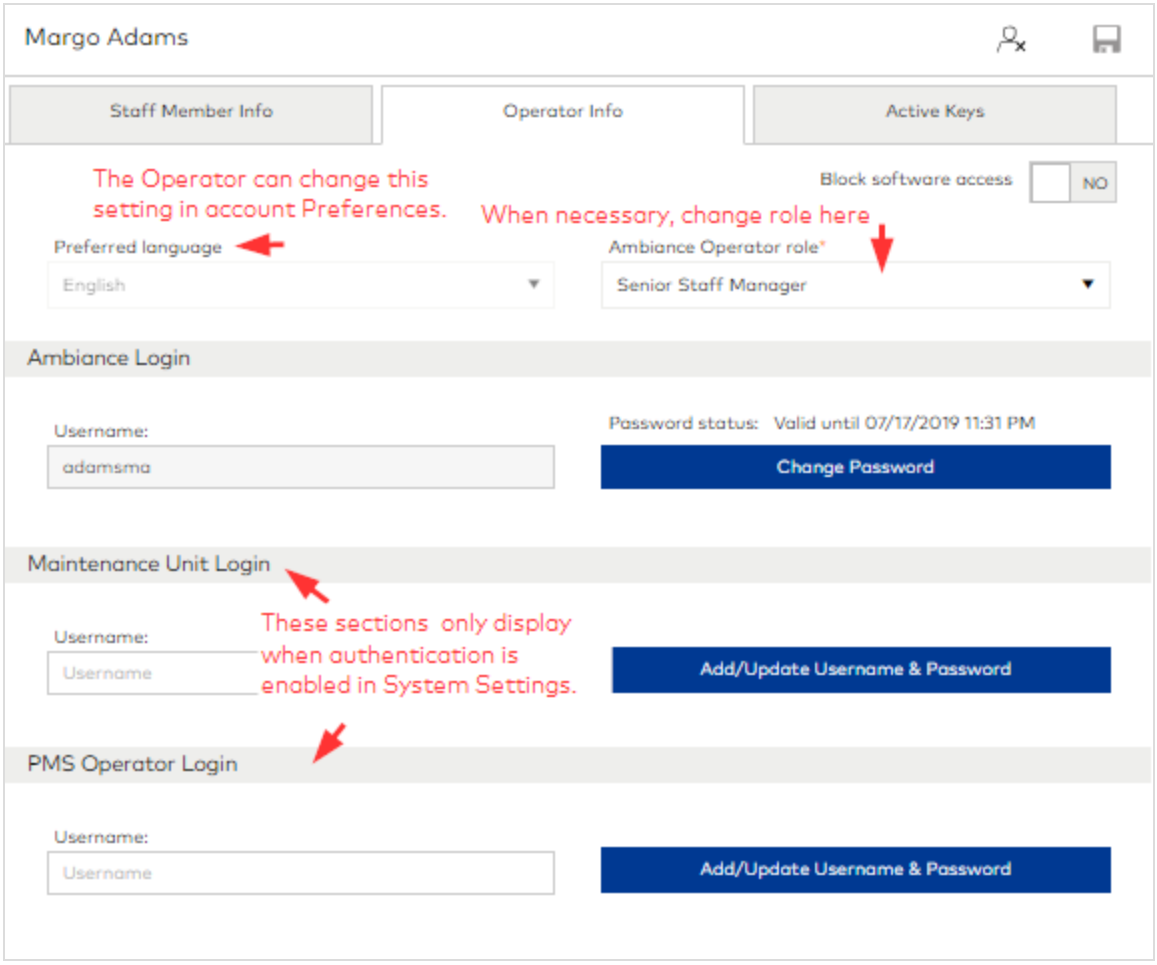
3. Specify the name of the staff member. Use the middle name to distinguish between staff with the same first and last names.
4. Click **Save**. Ambiance creates a profile and displays the **Staff Member Info** tab.



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 Ambiance.
6. Set the **Is a Ambiance Operator** switch to **YES**.



7. Select an Operator role. The list of roles is populated by the roles created in the Role Management module.
8. Specify a user name and password for the Operator. You must communicate account credentials to the Operator.
9. (*recommended*) To force the Operator to change the password upon initial login, select **Force password change on logon**.
10. Click **Save**. (If you do not need to select a preferred language for the Operator or create Maintenance Unit and/or PMS Login credentials, you can stop here. You have successfully completed configuring the Operator.)
11. Click the **Operator Info** tab.



12. Select the preferred language for the Operator. The Operator can change the language in account Preferences.
13. The role that you selected when designating the staff member as an Operator is selected. Accept or change the selection.
14. (*conditional*) When Maintenance Unit (M-Unit) authentication is enabled, the Maintenance Unit Login section displays. Credentials must be configured for at least one Operator. Click **Add/Edit Username & Password** to specify details. To disable M-Unit authentication, see Maintenance Unit Authentication.
15. (*conditional*) When PMS authentication is enabled, the PMS Operator Login section displays. Credentials must be configured for at least one Operator. Click **Add/Edit Username & Password** to specify details. To disable PMS

authentication, see **PMS Integration**.

16. Click (Save) .

USE Ambiance

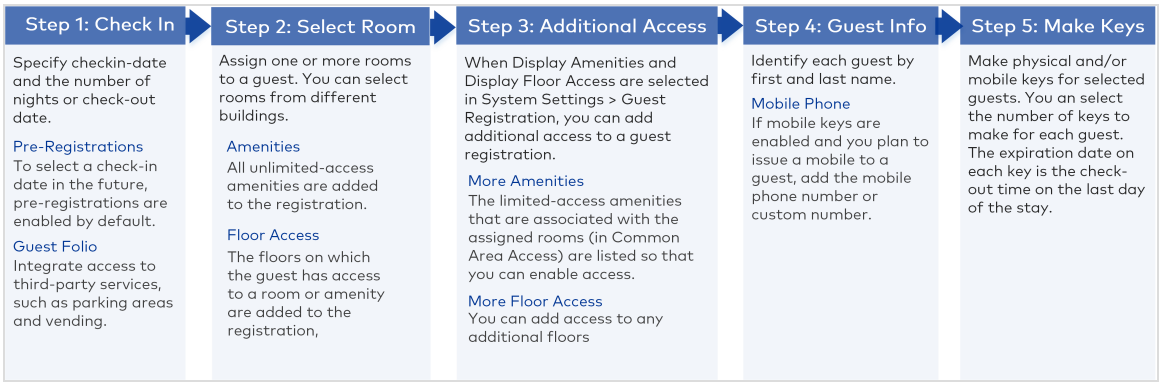
This chapter discusses the following.

Guest Registration

This section includes the following subjects:

Learning about Guest Registration

The Guest Registration module offers a guided yet flexible workflow to add and manage guest registrations.



The process starts by selecting stay details, such as the arrival date and number of nights. Next, you select a room. When you select a room, the default amenity and floor access is automatically added to the registration. You can add additional amenity and floor access depending on how your site is configured. When you reach the step for adding guest information, make sure to add a mobile phone number if you plan to issue mobile keys. As you move through the process, the options that you select are added to the Summary section. If you need to change your selections, you can use the built-in workflow or the quick access links in the Summary section.

The final step when making a guest registration is to make keys. You make any number of keys for each guest in the registration. When mobile keys are enabled and a mobile number is specified for a guest, you can make and send mobile keys remotely.

> By default, all registrations start on the current date. To make a registration for a future date, pre-registrations must be enabled in Systems Settings > Advanced and configured in System Settings > Guest Registration.

Modifying Registrations

A guest can request a check-in date change for pre-registrations or check-out date change to shorten or extend the stay. You may also need to change the room assignment, add or remove amenity access, or add mobile phone numbers for guests.

Every time a registration is modified, new keys must be made. When the new keys are presented to locks, the previously active keys are invalid.

Additional and Replacement Keys

You can make additional and replacement keys for all active registrations. Additional keys are merely copies and do not affect the original keys. You can select the number of keys that you want to make for each guest. When you make Replacement Keys, new keys are made for each guest in the registration. If only physical keys were made, all keys in the registration are replaced. If only mobile keys were made, all mobile keys in the registration are replaced. If both physical and mobile keys were made, then you can choose to replace the physical keys, the mobile keys or both. After a Replacement Key (physical or mobile) is presented at an authorized access point, all previously active keys are invalid at that access point.

Guest Check-Outs

Although guest keys expire based on the registration details, the Check-Out feature is available on the Guest Registration Home page to check out guests who leave early or before their keys expire.

Limited Use Keys

Limited Use Keys provide guest with one-time access to a room. Typically, limited use keys are issued to a guest who returns after check-out for an item left in the room. The key is valid for a single use or until expiration.

Mobile Keys

When mobile keys are enabled in System Settings and a mobile phone number is added for a guest in the registration, you can issue mobile keys directly to the guest's phone. Verify that the mobile key is delivered in the Guests row of the Summary section.

For more information, see Working with Mobile Keys.

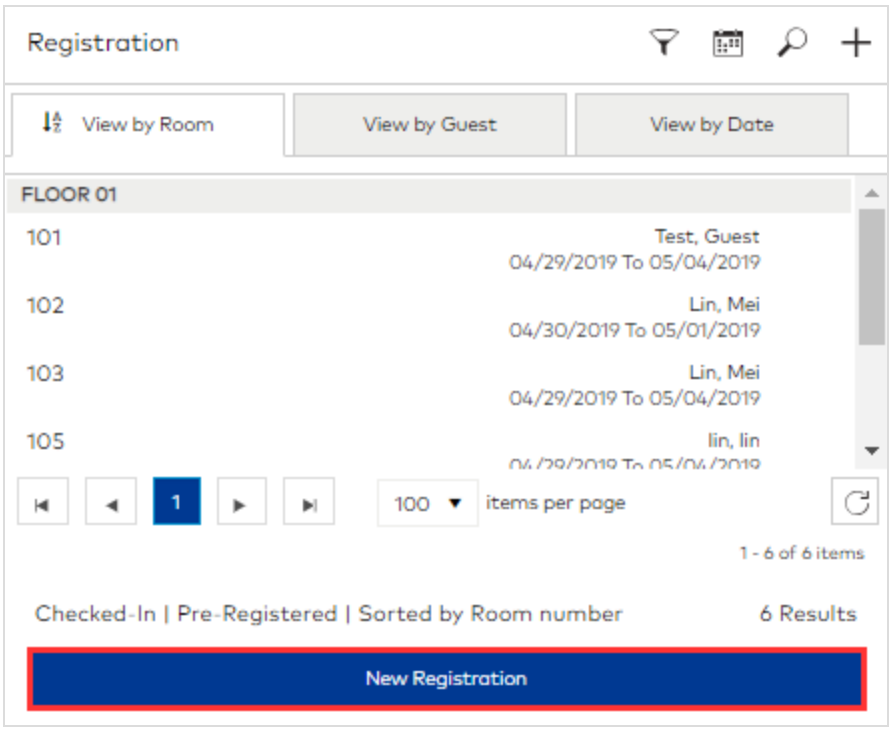
Folios

The Guest Folio enables Ambiance to integrate with third-party POS (point-of-sale) services such as access to vending machines, parking areas or entertainment venues. When a guest folio is configured for your site, you can add folio access to a registration on the Check-In/Out page.

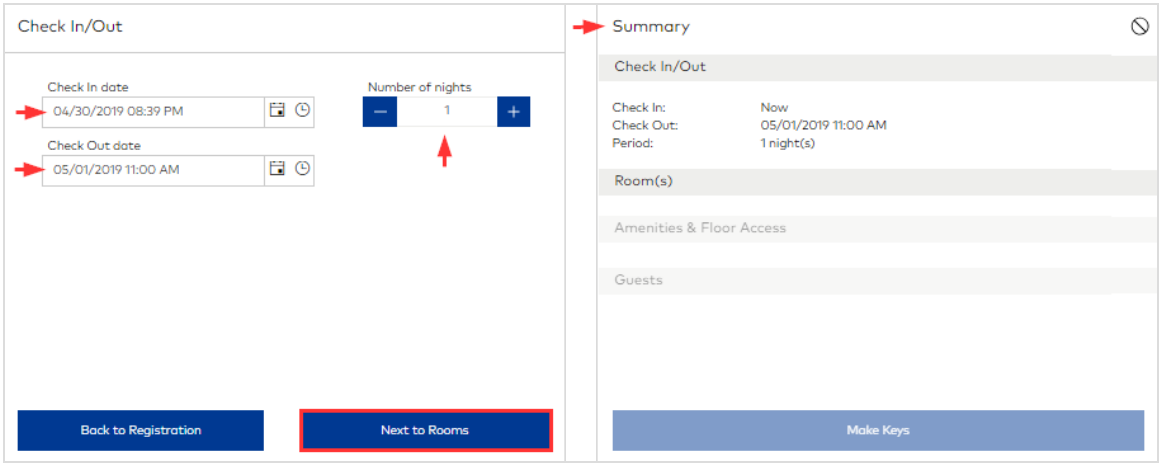
Add a Guest Registration

To add a guest registration:

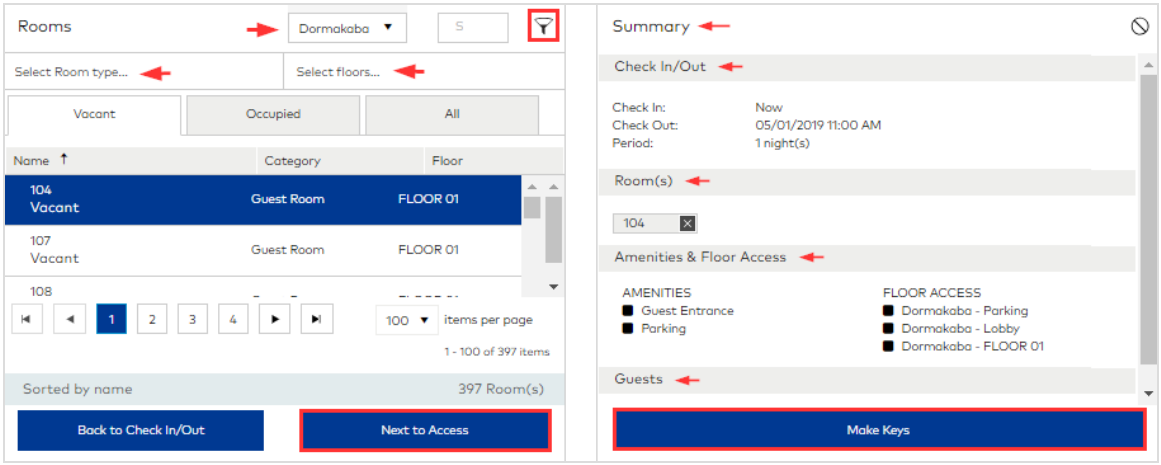
1. Go to Guest Registration.



2. Click **New Registration**.



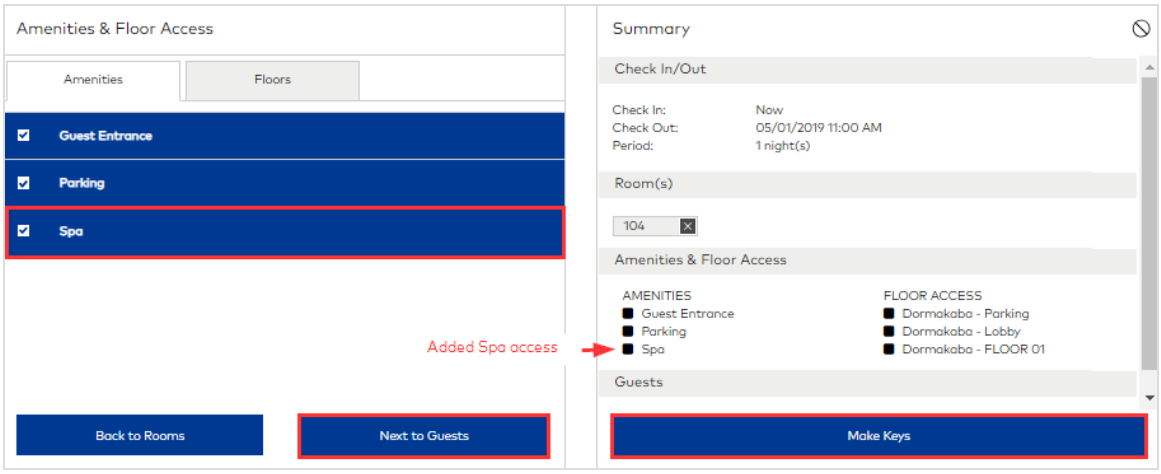
3. On the Check-In/Out page, specify stay details. To make a registration for a future date, pre-registrations must be enabled in System Settings. If a guest folio is configured for your site, select the folio access to integrate onto the guest keys (for this registration).
4. Click **Next to Rooms**.



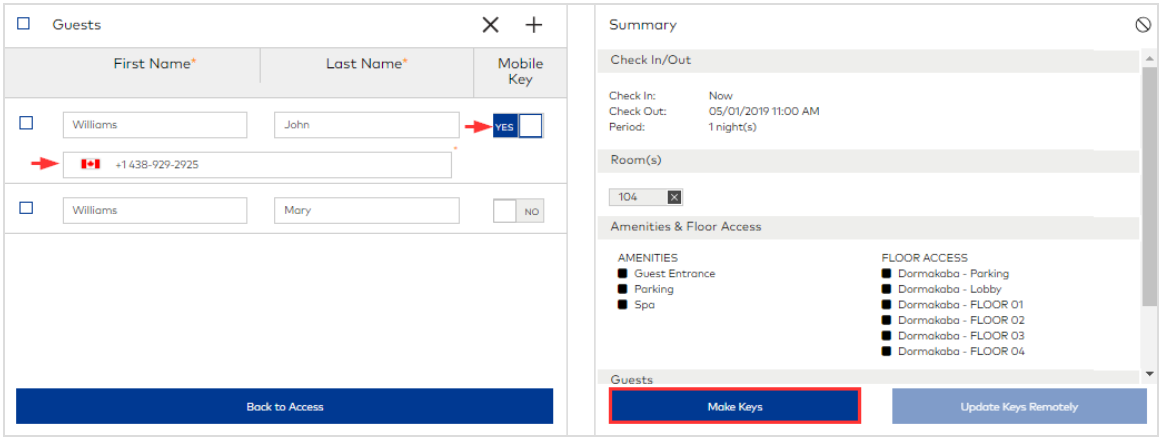
5. Select one or more rooms. You can select a different building and filter options based on room type (guest room or suite) and floor location. Use the page navigation tools to browse vacant rooms. When you select a room, the room and associated amenity and floor access is added to the Summary page.
6. Take one of the following actions:
   - If you do not need to add additional amenity or floor access, you can click the Guests row in the Summary section and proceed to step 9 or click **Make Keys**

and proceed to step 12.

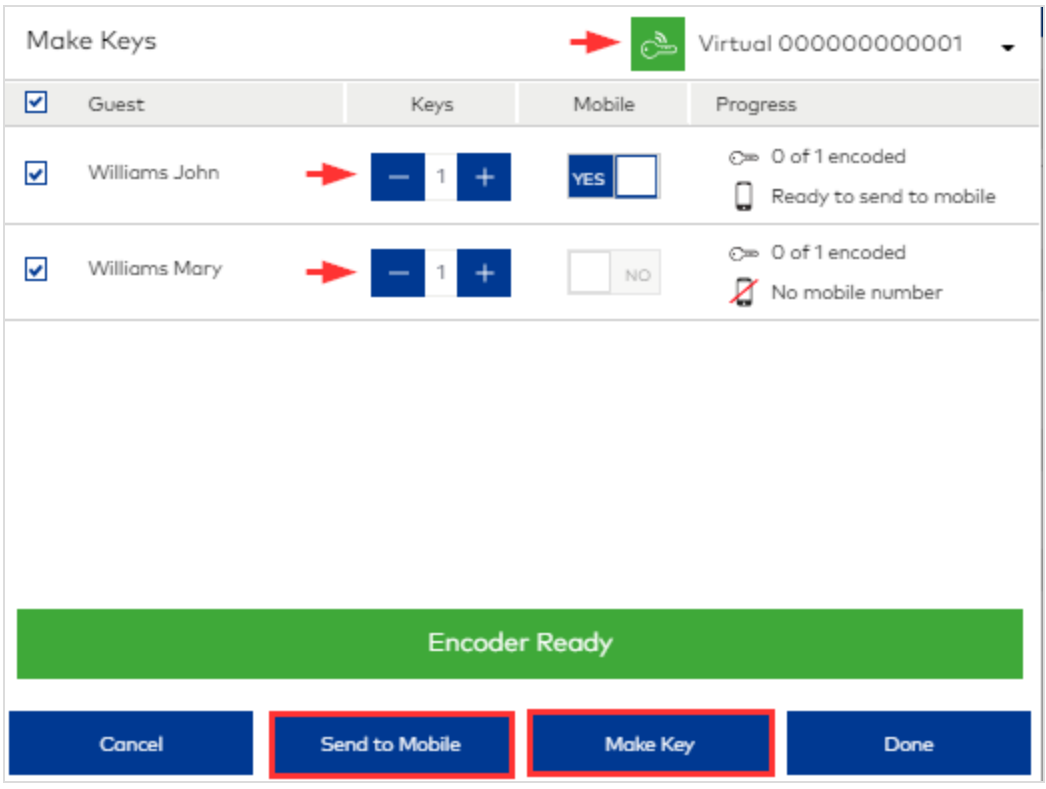
- If you need to add additional amenity or floor access, click **Next to Access**.



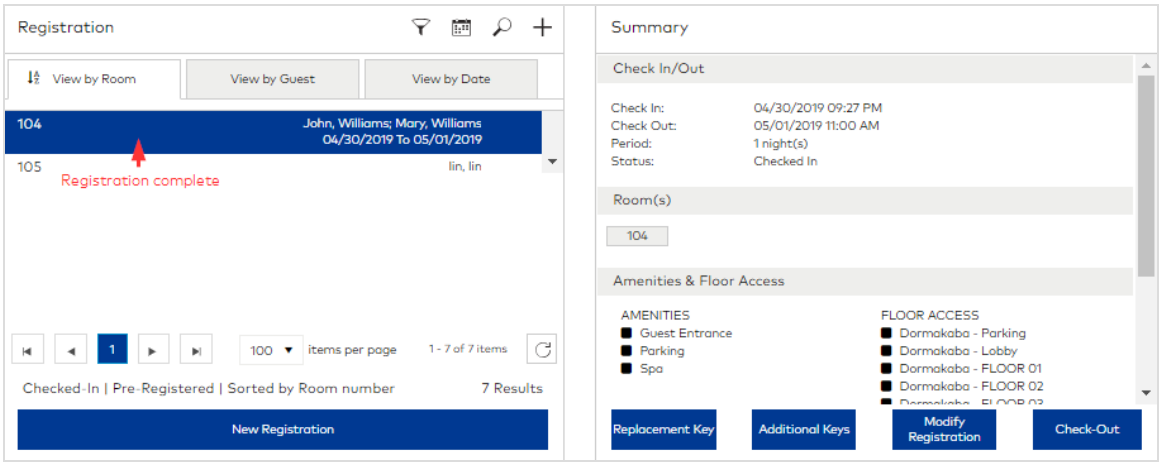
7. Configure amenity and floor access:
   - On the Amenities tab, select/deselect available amenities. Unlimited Guest Common Areas are selected by default and cannot be deselected. Limited Guest Common Areas that are associated with the selected room/s (in Access Management > Common Area Access) can be selected/deselected.
   - On the Floors tab, select the floor access to add to the registration. (This tab only displays if multiple floors are defined for the site and Display floor access is enabled in System Settings.)
8. Take one of the following actions:
   - If you don't need to specify guests, click **Make Keys** and proceed to step 12.
   - To specify a guest, click **Next to Guests**.



9. Specify the first and last names of the guest. Click (Add) + for each additional guest that you want to add. If the mobile key option is available, specify whether to enable mobile keys for each guest. A mobile phone number (or custom number) is required to issue mobile keys.
10. Click **Make Keys**.



11. (*conditional*) Select the guests for whom you want to make keys and specify the number of keys to make for each.
12. Make physical and/or mobile keys:
    - To make physical keys, select an encoder that is online and available to the workstation, then click **Make Key**. When prompted, present a key to the encoder.
    - To make mobile keys, click **Send to Mobile**.
13. When prompted that keys were made successfully or the mobile key request was submitted, click **Done**. Verify mobile key status in the Summary > Guest(s) section. The status may display Delivering, Delivered, Failed. To view the most current status, refresh the Guest Registration page.

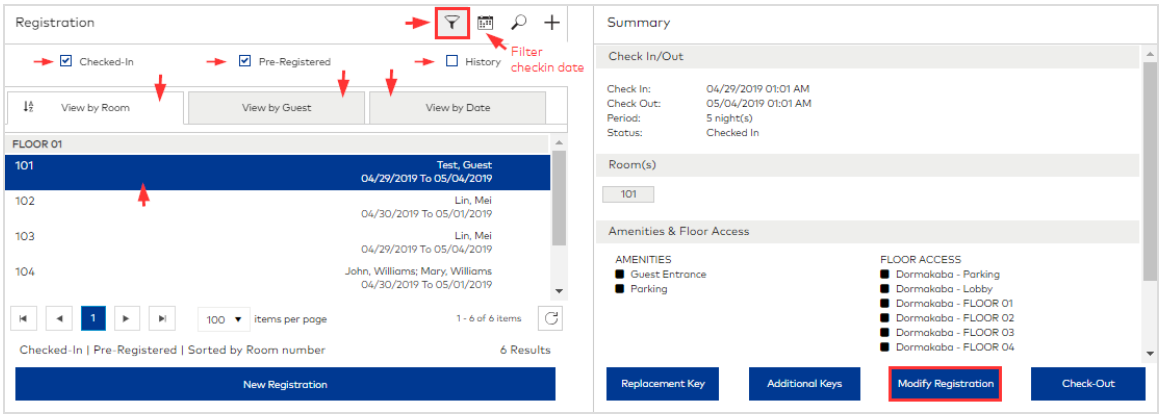


Modify a Guest Registration

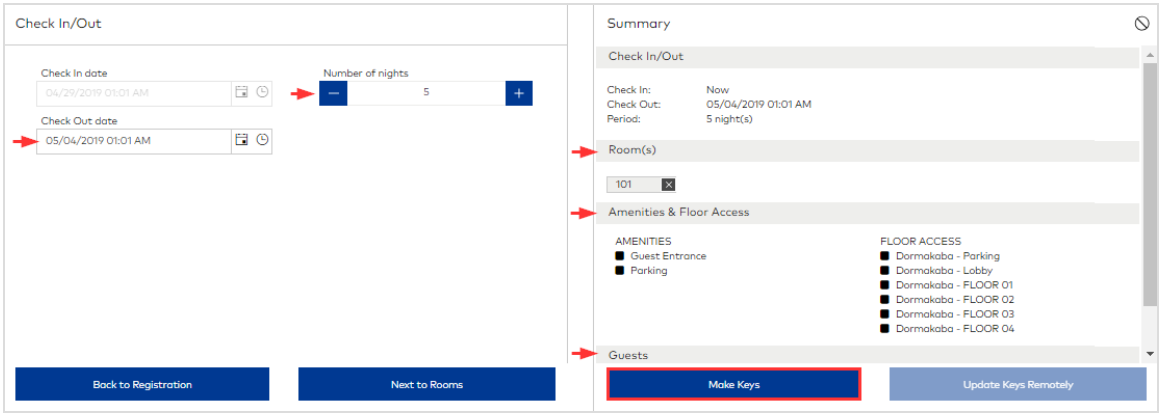
A guest can request a check-in date change for pre-registrations or check-out date change to extend the stay. You may also need to add a mobile phone number for guests. Every time a registration is modified, New keys must be made and issued. After New keys are made and presented to locks, the previous keys are invalid.

To modify a guest registration:

1. Go to Guest Registration.



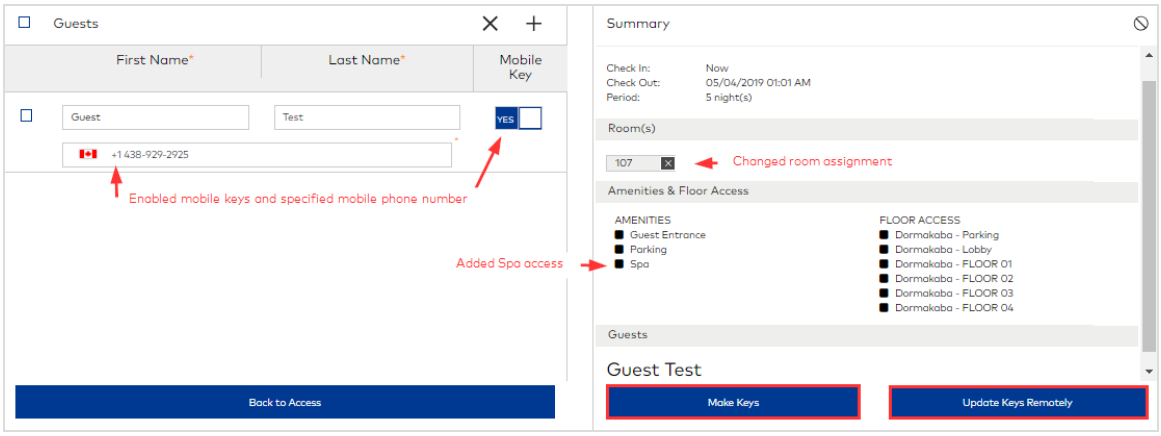
2. Select the registration that you want to modify. There are multiple options for finding a registration. You can filter the list to show only registrations that are checked in or pre-registered or both. You can constrain the list by specifying a check-in date range. You can search for a registration by room or suite number. Finally, you can use the page navigation tools and viewing options (by room, guest name or date) to browse the list of registrations.
3. Click **Modify Registration**.


Check In/Out
Check In date
04/29/2019 01:01 AM
Number of nights
5
Check Out date
05/04/2019 01:01 AM
Back to Registration
Next to Rooms
Summary
Check In/Out
Check In: Now
Check Out: 05/04/2019 01:01 AM
Period: 5 night(s)
Room(s)
101
Amenities & Floor Access
AMENITIES
Guest Entrance
Parking
FLOOR ACCESS
Dormakaba - Parking
Dormakaba - Lobby
Dormakaba - FLOOR 01
Dormakaba - FLOOR 02
Dormakaba - FLOOR 03
Dormakaba - FLOOR 04
Guests
Make Keys
Update Keys Remotely

4. Make any of the following modifications:

> To make changes to a guest registration, you can proceed through the guest registration workflow or click the relevant page/s from the Summary. After modifying a guest registration, new keys must always be made.

- On the Check-In/Out page, you can extend the stay and modify folio access for guests who are already checked in. For pre-registrations, you can modify the check-in date, number of nights, check-out date and folio access.
- On Rooms page, modify the room assignment.
- On the Amenities & Floor Access page, add or remove access to common areas or meeting rooms. (Access to unlimited common areas cannot be removed.) Add or remove floor access. (This tab only displays if multiple floors are defined for the site and Display floor access is enabled in System Settings.)
- On the Guests page, add or remove guests and add or modify mobile phone numbers for guests.

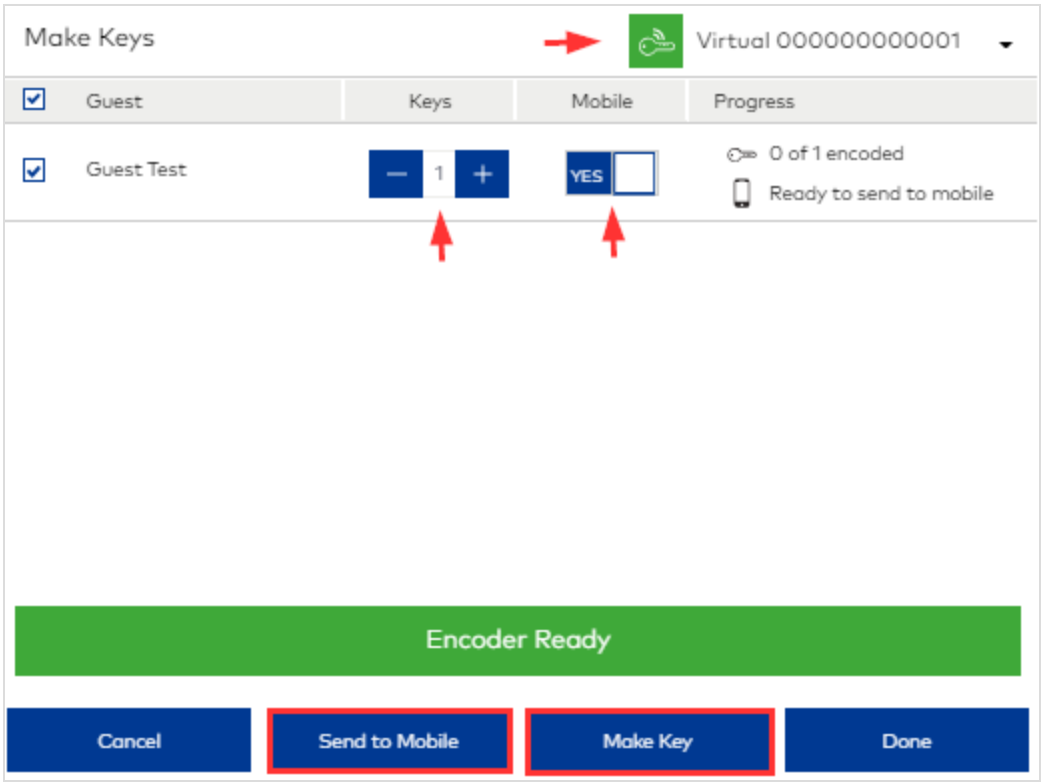


5. Make keys or, if Remote Lock Management is enabled, update keys remotely. The option that you choose depends on whether Remote Lock Management is enabled and the changes made to the registration:

- If Remote Lock Management is enabled and the modification was a room change and/or a guest extended their stay, click **Update Keys Remotely** (see

above figure). For all other modifications, click **Make Keys**.

- If Remote Lock Management is not enabled, click **Make Keys**.



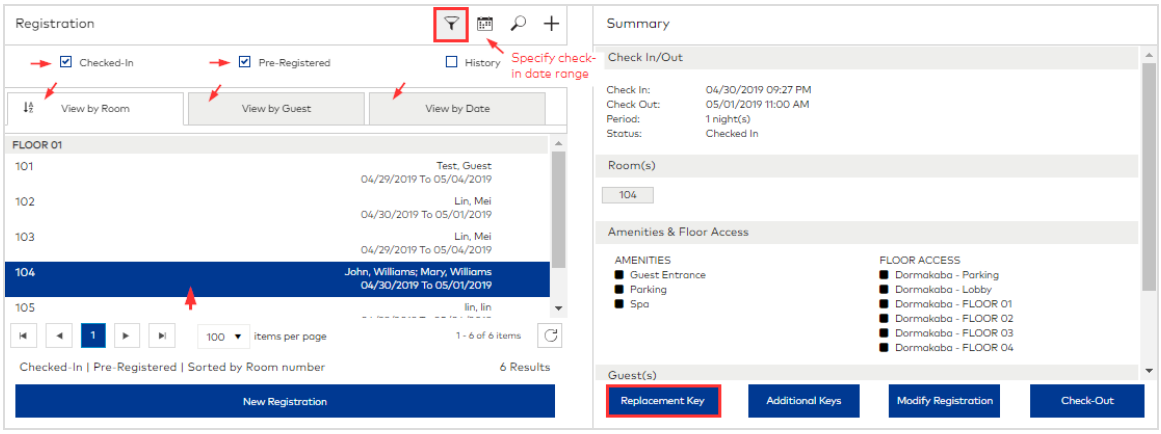
6. (*conditional*) Select the guests for whom you want to make keys, specify the number of keys to make, and select whether to make mobile keys.
7. Make physical and/or mobile keys:
   - To make physical keys, select an encoder that is online and available to the workstation, then click **Make Key**. When prompted, present a key to the encoder.
   - To make mobile keys, click **Send to Mobile**.
8. When prompted that keys were made successfully or the mobile key request was submitted, click **Done**. Verify mobile key status in the Summary > Guest(s) section. The status displays Delivering, Delivered, Failed. To view the most current status, refresh the Guest Registration page.

Replace Guest Keys

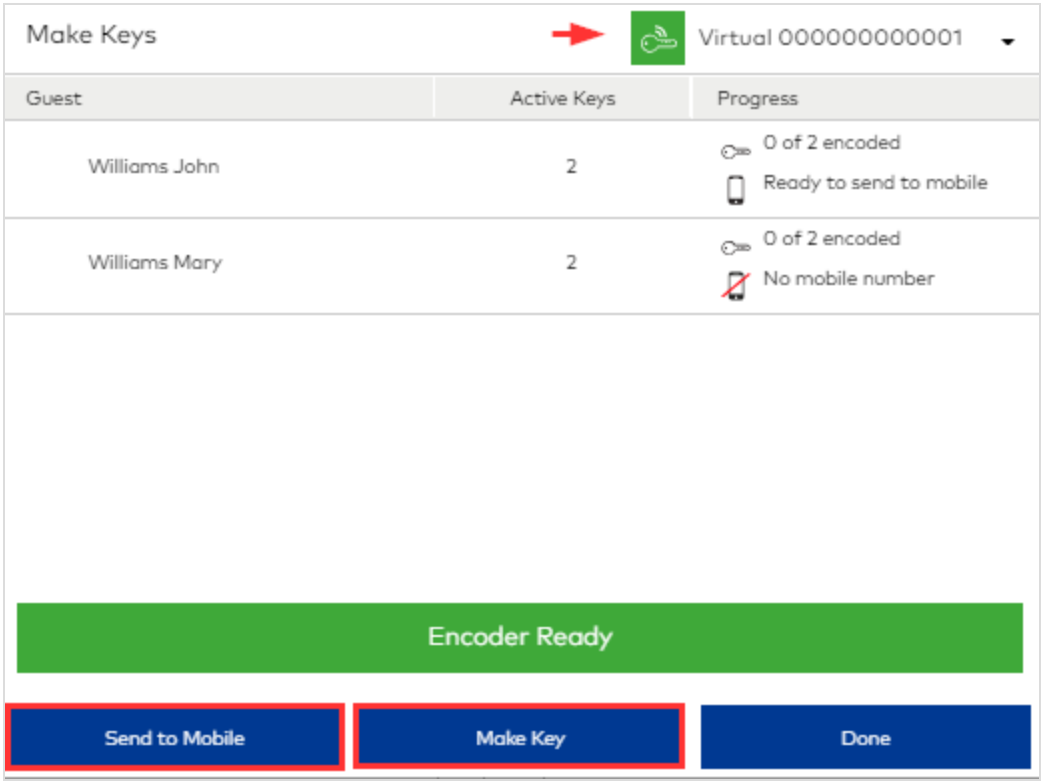
When you make Replacement Keys, new keys are made for each guest in the registration. If only physical keys were made, all keys in the registration are replaced. If only mobile keys were made, all mobile keys in the registration are replaced. If both physical and mobile keys were made, then you can choose to replace the physical keys, the mobile keys or both. After a Replacement Key (physical or mobile) is presented at an authorized access point, all previously active keys are invalid at that access point.

To replace guest keys:

1. Go to Guest Registration.



2. Select a registration. There are multiple options for finding a registration. You can filter the list to show only registrations that are checked in or pre-registered or both. You can constrain the list by specifying a check-in date range. You can search for a registration by room or suite number. Finally, you can use the page navigation tools and viewing options (by room, guest name or date) to browse the list of registrations.
3. Click **Replacement Key**.



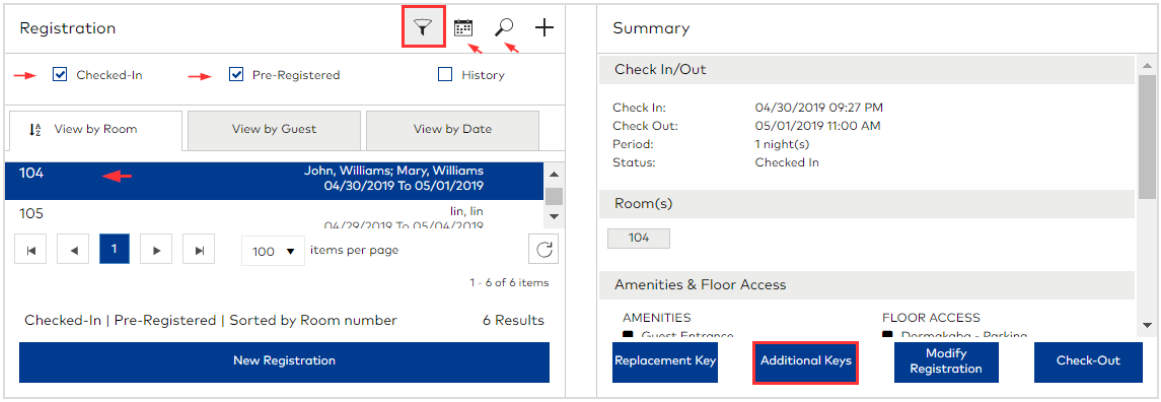
4. Make physical and/or mobile keys:
   - To make physical keys, select an encoder that is online and available to the workstation, then click **Make Key**.
   - To make mobile keys, click **Send to Mobile**.
5. When prompted that keys were made successfully or the mobile key request was submitted, click **Done**. Verify mobile key status in the Summary > Guest(s) section. The status displays Delivering, Delivered, Failed. To view the most current status, refresh the Guest Registration page.

Make Additional Guest Keys

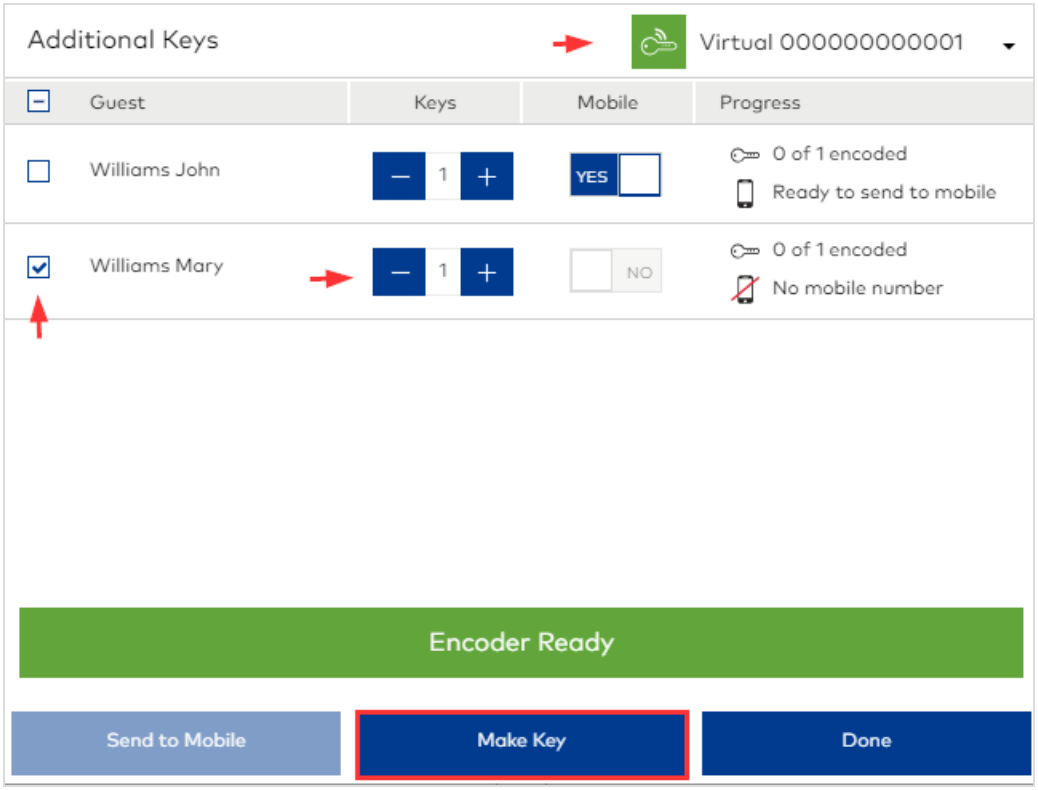
When guests request additional keys, you can make copies of their active keys without affecting access.

To make additional keys:

1. Go to Guest Registration.
2. Select a registration. There are multiple options for finding a registration. You can filter the list to show only registrations that are checked in or pre-registered or both. You can constrain the list by specifying a check-in date range. You can search for a registration by room or suite number. Finally, you can use the page navigation tools and viewing options (by room, guest name or date) to browse the list of registrations.



3. Click **Additional Keys**.



4. Select the guests for whom you want to make keys and specify the number of keys to make for each.
5. Make physical and/or mobile keys:
   - To make physical keys, select an encoder that is online and available to the workstation, then click **Make Key**. When prompted, present a key to the encoder.
   - To make mobile keys, click **Send to Mobile**.

> If you want to make mobile keys but no mobile number is defined for the guest, you must modify the registration to add the mobile phone number. After modifying a registration, you are prompted to make new keys.

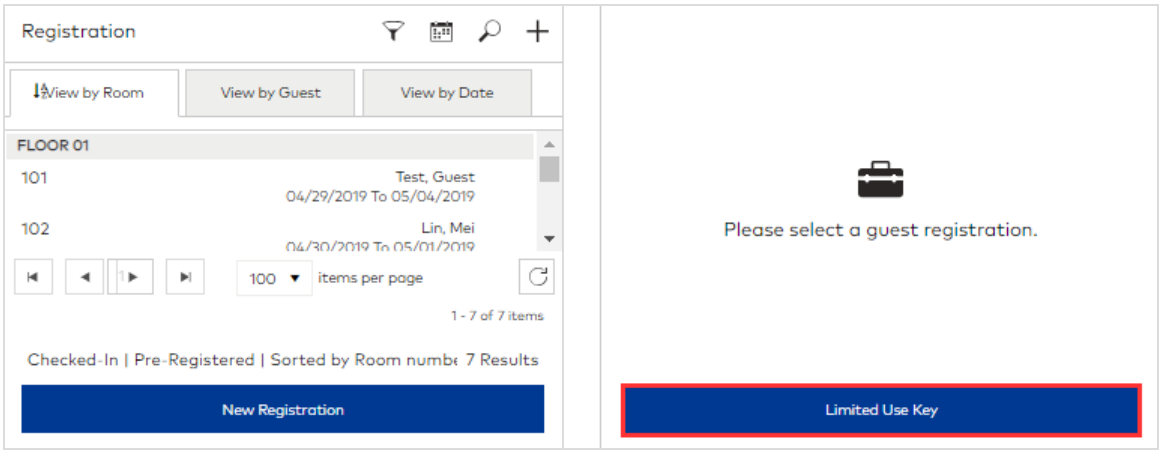
6. When prompted that keys were made successfully or the mobile key request was submitted, click **Done**. Verify mobile key status in the Summary > Guest(s) section. The status displays Delivering, Delivered, Failed. To view the most current status, refresh the Guest Registration page.

Make a Limited Use Guest Key

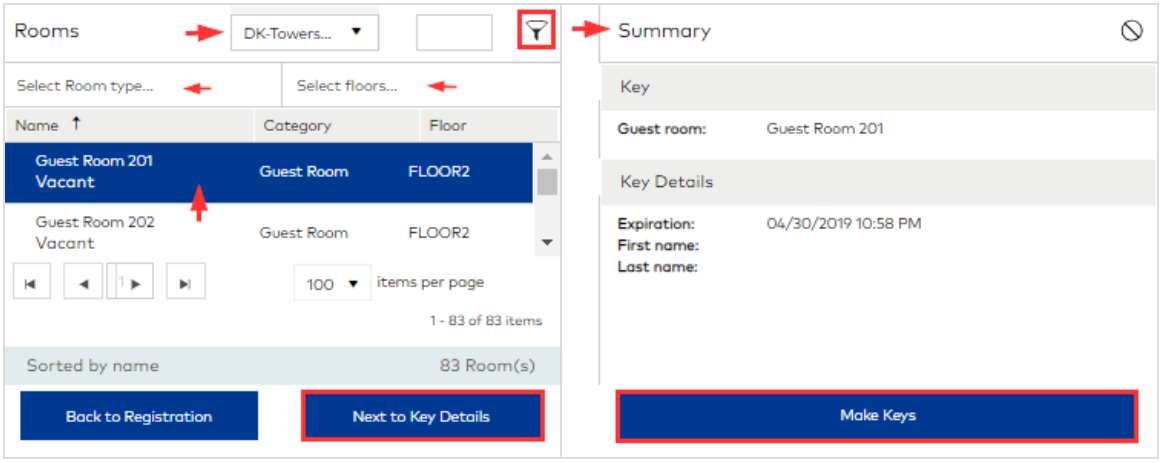
Limited Use Keys are most often used when a guest returns after check-out for an item left in the room. For guests, the key is valid for a single use or until expiration.

To make a Limited Use Guest Key:

1. Go to Guest Registration.



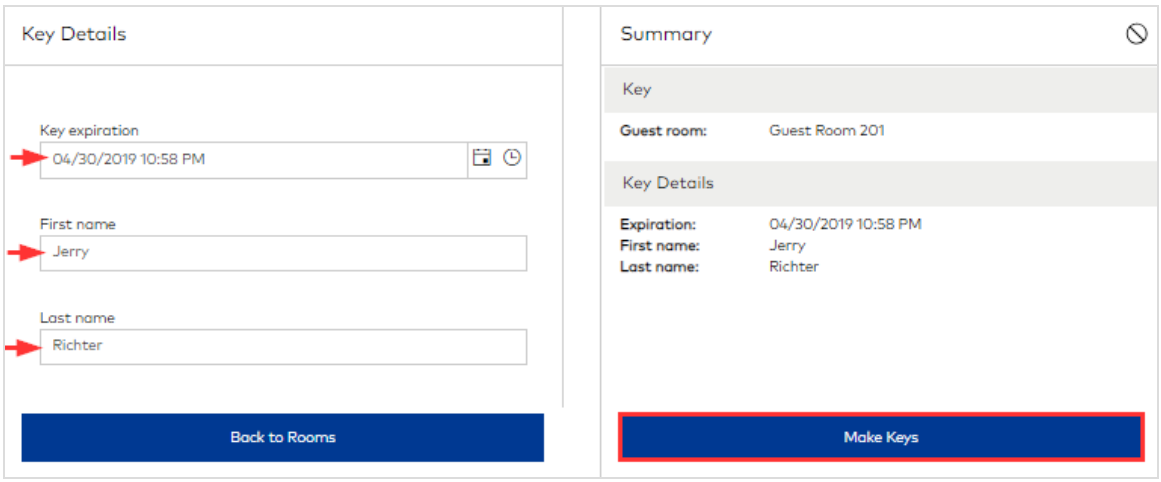
2. Click **Limited Use Key**.



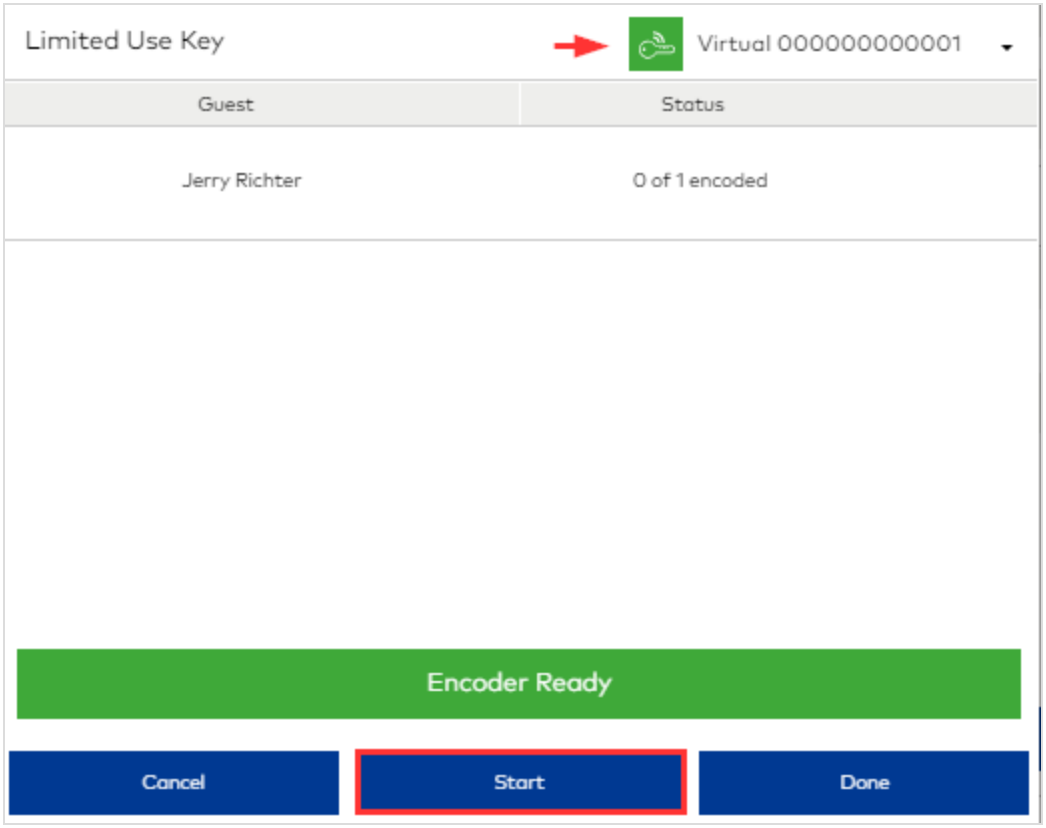
3. Select a room. You can select a different building and filter options based on room type (guest room or suite) and floor location. Use the page navigation tools

to browse vacant rooms.

4. Take one of the following actions:
   - If you do not need to specify a guest or customize the expiration date, click **Make Keys** and proceed to step 8.
   - To specify a guest or modify the expiration date, click **Next to Key Details**.



5. Specify first and last names of the guest.
6. (*optional*) Modify the expiration details.
7. Click **Make Keys**.

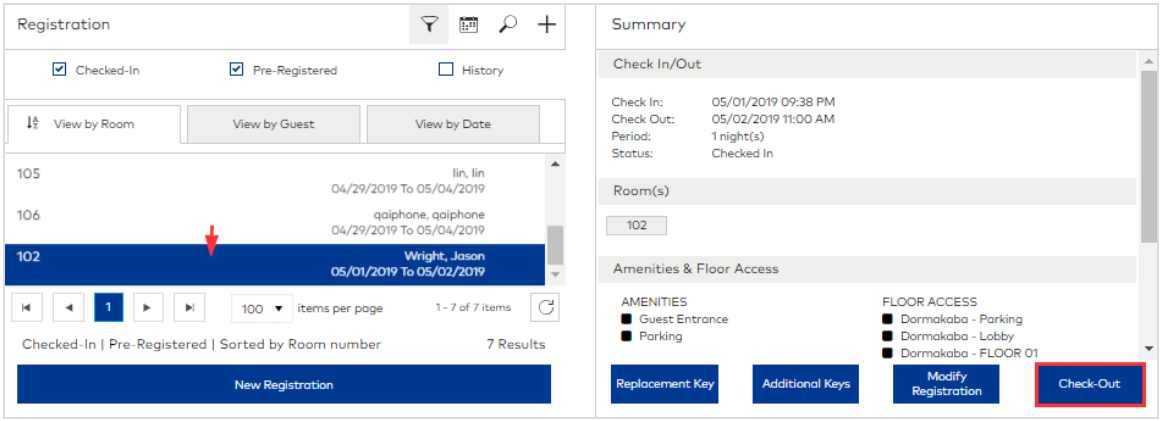


8. Select an encoder that is online and available to the workstation, then click **Start**. When prompted, present a key to the encoder.
9. When prompted that keys were made successfully, click **Done**.

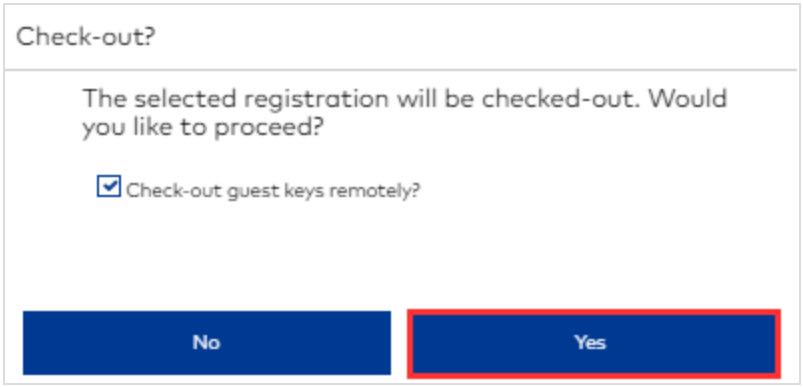
Check Out a Registration

To check out a registration:

1. Go to Guest Registration.

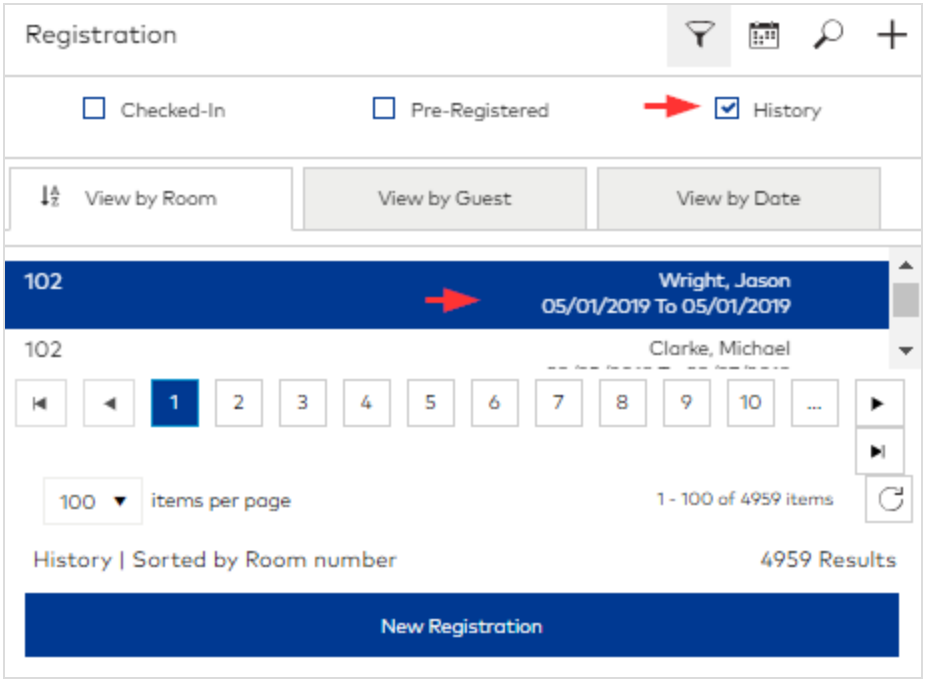


2. Select the registration that you want to check out. There are multiple options for finding a registration. You can filter the list to show only registrations that are checked in or pre-registered or both. You can constrain the list by specifying a check-in date range. You can search for a registration by room or suite number. Finally, you can use the page navigation tools and viewing options (by room, guest name or date) to browse the list of registrations.
3. Click **Check Out**.



4. When prompted to confirm checkout, click **Yes**. If Remote Lock Management is enabled, you can check out guest keys remotely (which immediately invalidates guest keys upon check-out). In all other cases, guest keys are invalid when they expire or when New Keys for the same room/s are presented to the relevant access points.

The registration is now listed when the Historical filter is enabled.



Staff

This section includes the following subjects:

Learning about Staff Management and Staff Keys

The keys that authorize personnel, contractors and emergency officials to enter access points are staff keys. The credentials encoded on staff keys are defined in **Access Management** > **Credential Management**. Before making a staff key, learn more about each credential class type and the default credential class. For more information, see Credential Management in *Learning about Access Management*.

- **Emergency**—The principal property of the Emergency class type is that keys encoded with this class always override a projected dead bolt or active privacy switch. As such, reserve this class for senior management and emergency personnel.
- **Grand Master**—This is a general purpose class intended for the highest levels of access among staff. The class shares the same properties as the Emergency class except that keys never override a deadbolt or privacy switch.
- **Master**—This is a general purpose class intended for most staff keys.
- **Limited Use Staff**—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 Keys. For example, if the limit is six, the key opens the lock the first six consecutive times then expires.

For keys made using the Emergency, Grand Master and Master class type, additional access points (all access point types except common areas and elevator readers) can be added at key-making time. (Additional Access must be enabled in System Settings > Staff Keys.)

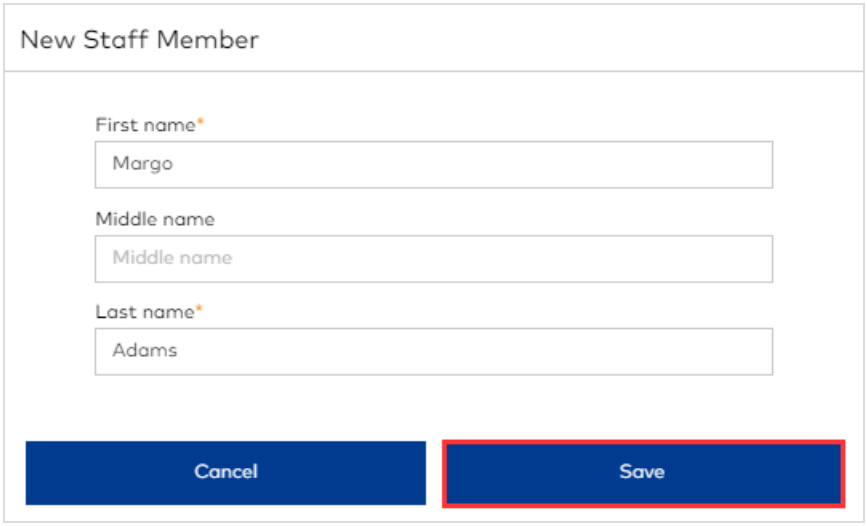
Add Staff Members

Staff members are the key holders in your organization. You must add all staff who will be issued a key.

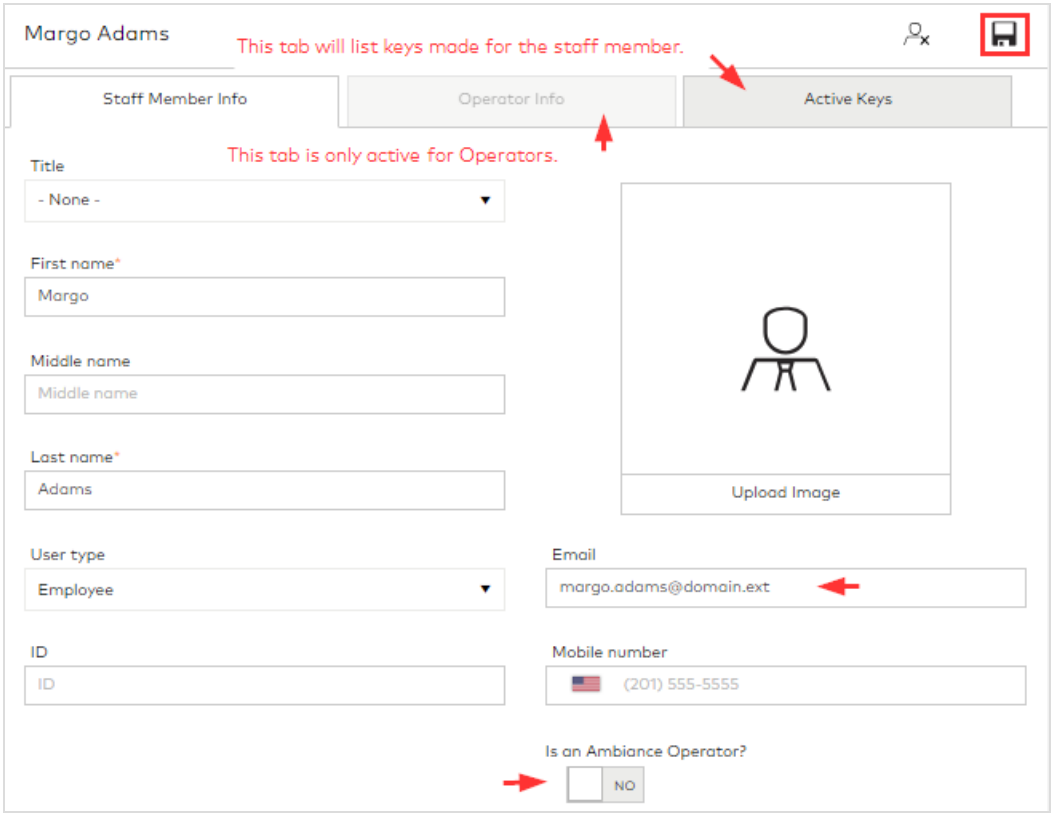
> If you are adding a staff member who you want to designate as an Operator, see Configure Operators in Site Configuration.

To add a staff member:

1. Go to Staff 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.
4. Click **Save**. Ambiance creates a staff profile and displays the **Staff Info** tab. No other options are required unless you want to send automated emails to the staff member or designate the staff member as an Operator.



5. (*recommended*) For **Email**, specify a valid email address for the staff member. An email address is required to send automated emails regarding account access. (For Operators, the email address can be changed in account Preferences.)
6. Click (Save) .

Make Staff Keys

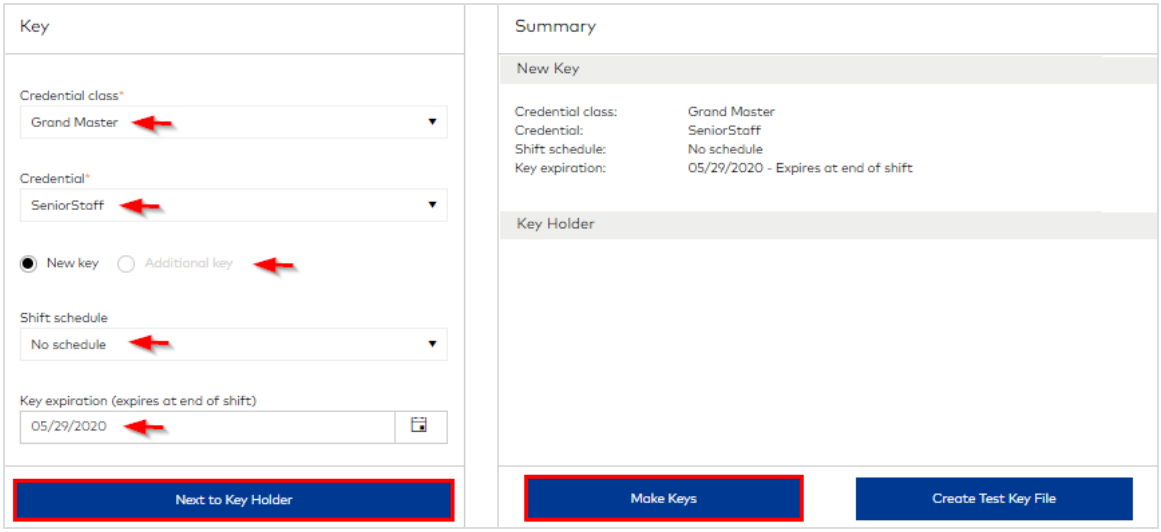
Before making a staff key, see Learning about Staff Management and Staff Keys and Learning about Access Management to learn more about each credential class type and the default credential class.

This topic provides instructions for making the following types of keys:

- Make an Emergency Key or (Grand) Master Staff Key
- Make a Standard Staff Key
- Make a Limited Use Staff Key

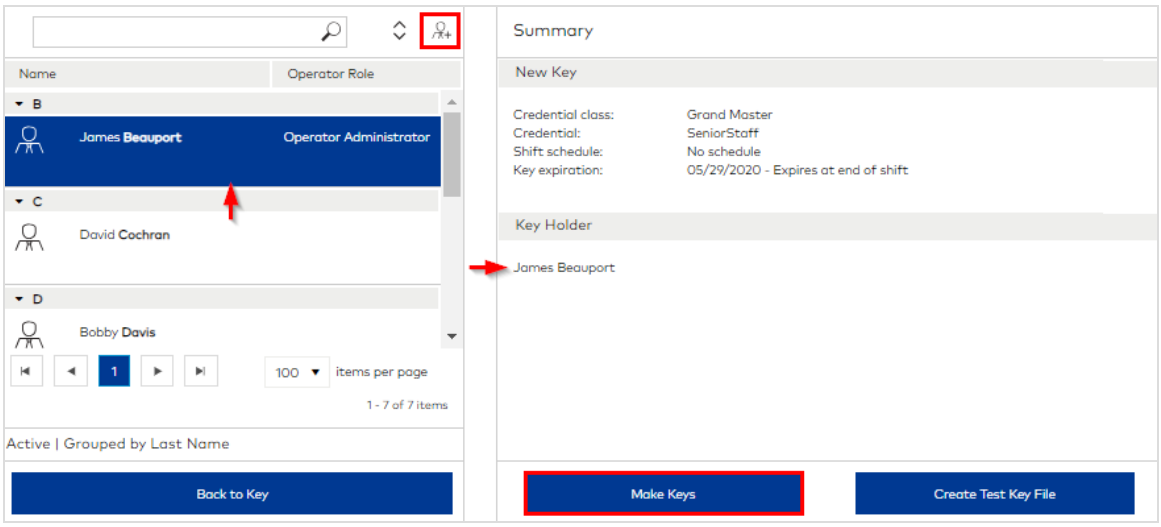
Make an Emergency Key or (Grand) Master Staff Key

1. Go to Staff Keys.

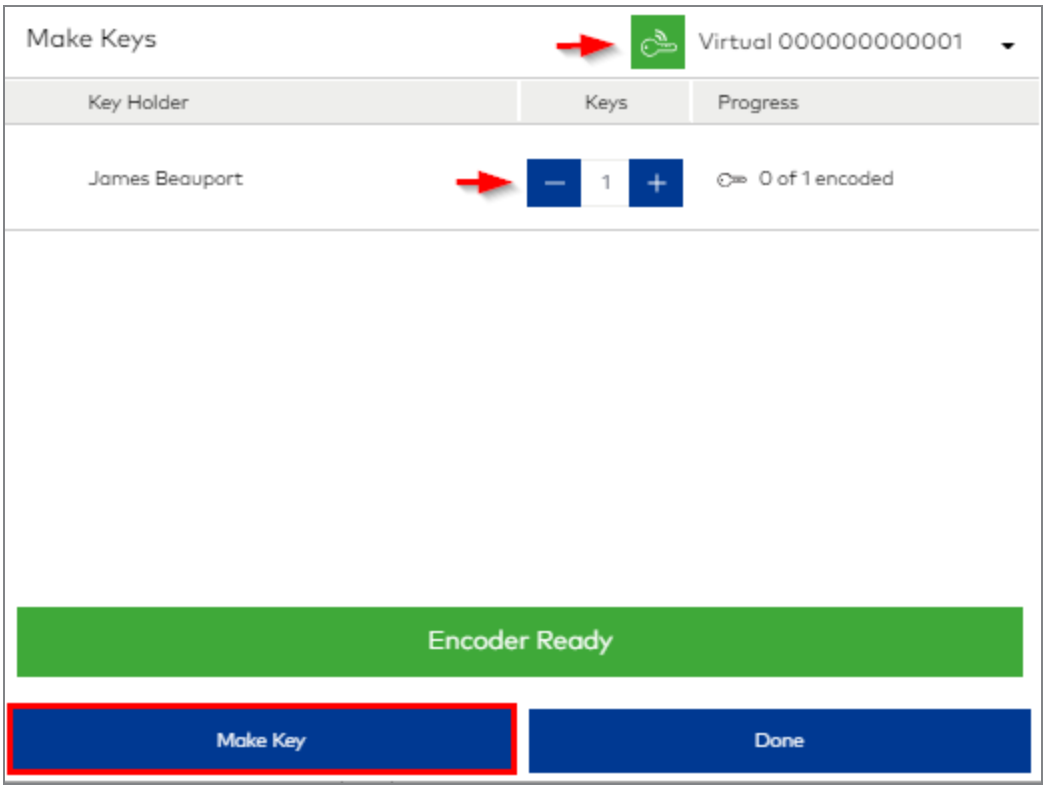


2. Select the Emergency or Grand Master credential class. Only those classes for which credentials are defined are listed.
3. Select a credential.
4. Select whether to make a New or Additional key. Making a New key invalidates the selected credential on all active keys. Making Additional keys (copies) has no effect on existing active keys.

5. (*optional*) Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. (*optional*) Specify a date after which the key is invalid.
7. (*optional*) Click **Next to Key Holder**. Select the staff to whom you want to assign the key. To add a staff member, click (Add) , specify first and last names, then click **Save**.



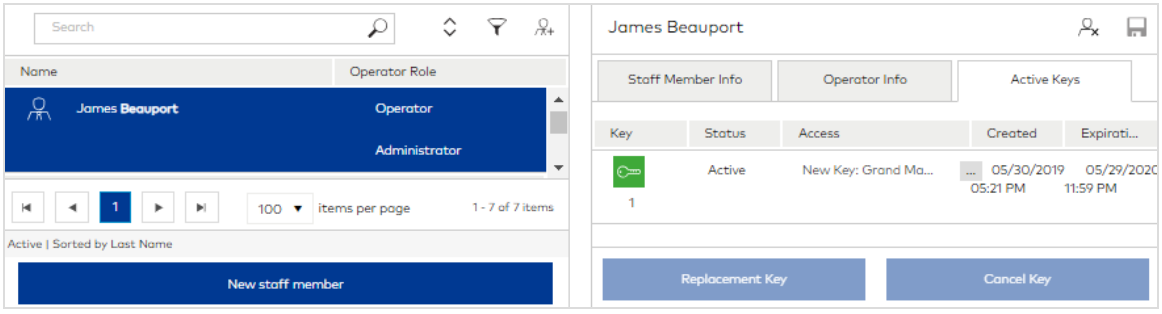
8. Click **Make Keys**:



   - To make a mobile key, click **Send to mobile**. Mobile keys must be enabled and a mobile phone number must be specified in the staff member profile.
   - To make physical keys, specify the number of keys to make, select an encoder that is online, click **Make Key**, then present keys to the encoder (as prompted).

9. When prompted that keys were made/sent successfully, click **Done**. You can verify that a mobile key was delivered in Staff Management.

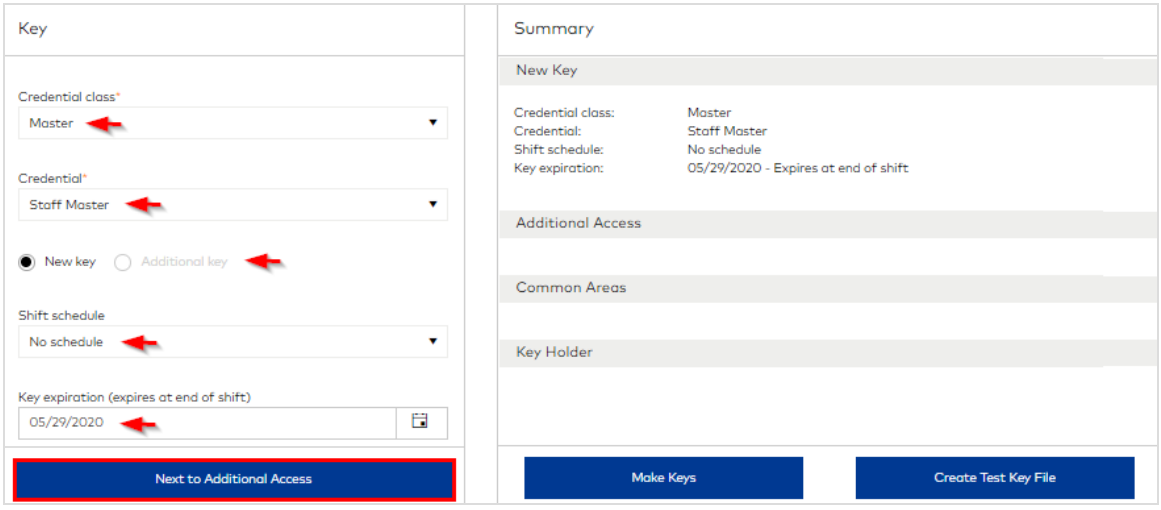
The key is listed on the Active Keys tab in the staff member profile.



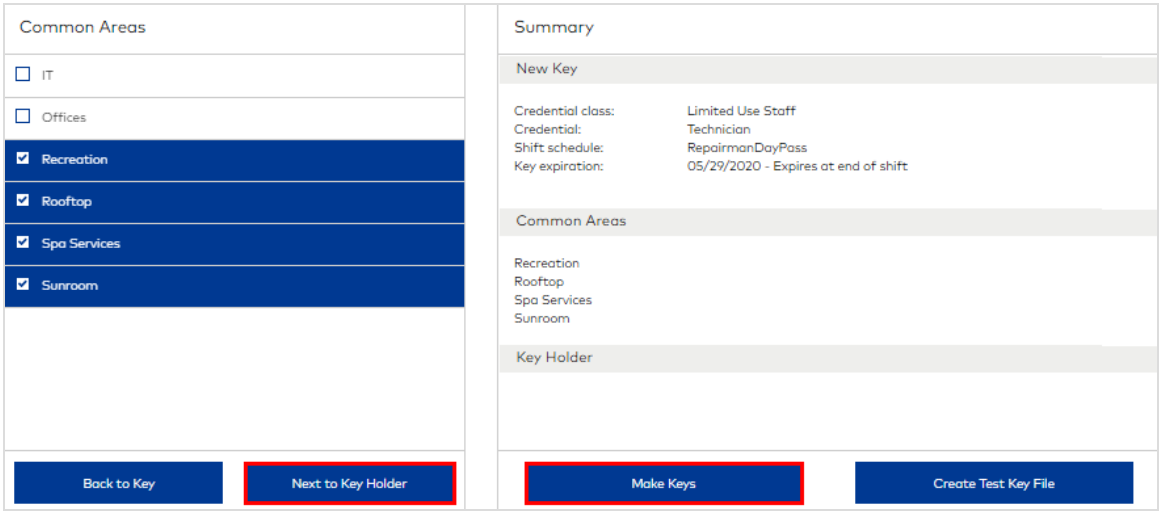
Make a Standard Staff Key

Follow these instructions when making a key based on the Master class type.

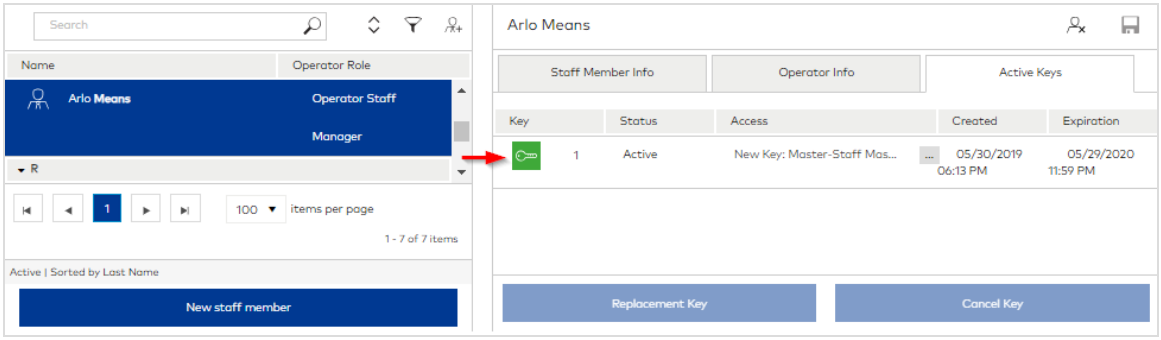
1. Go to Staff Keys.



2. Select a credential class. Only those classes for which credentials are defined are listed.
3. Select a credential.
4. Select whether to make a New or Additional key. Making a New key invalidates the selected credential on all active keys. Making Additional keys (copies) has no effect on existing active keys.
5. (*optional*) Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. (*optional*) Specify a date after which the key is invalid.
7. The menu option that displays depends on whether additional access points are available to add to the key and whether a Staff Common Area Profile is associated with the selected credential. Take one of the following actions:
   - Click **Next to Additional Access** and proceed to the next step.
   - Click **Next to Common Areas** and proceed to step 9.
   - If neither menu option displays, proceed to step 10.



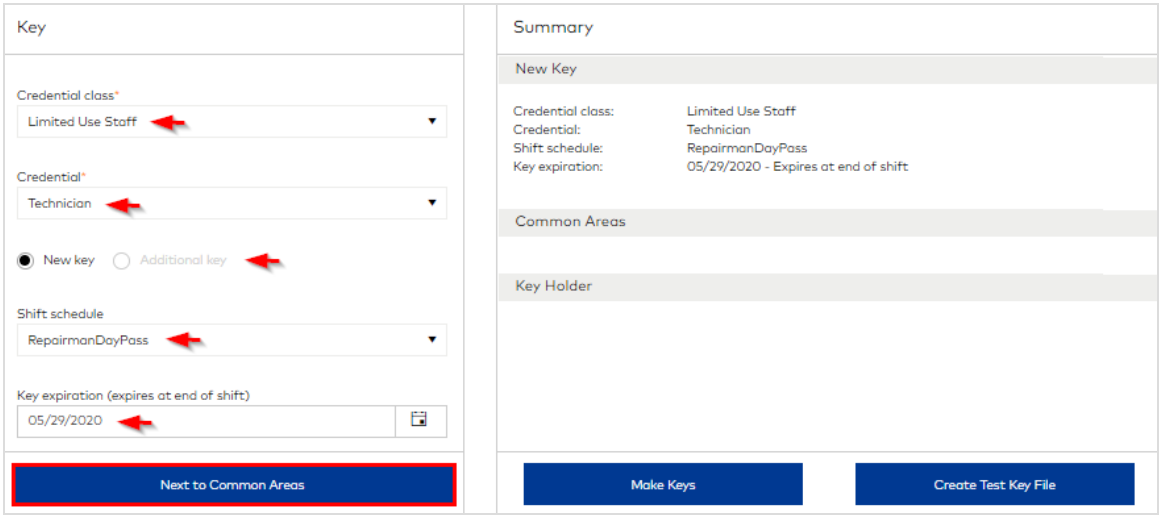
8. Select the additional access points that you want to add to the key. You can select a different building and search for access points by name. All access point types except common areas and elevator readers can be added at key-making time. The next step depends on whether a Staff Common Area Profile is associated with the selected credential. Take one of the following actions:
   - If yes, click **Next to Common Areas** and proceed to the next step.
   - If no, proceed to step 10.
9. Select the limited-access common areas to authorize on the key.
10. (*optional*) Click **Next to Key Holder**. Select the staff to whom you want to assign the key. To add a staff member, click (Add) , specify first and last names, then click **Save**.
11. Click **Make Keys**:
    - To make a mobile key, click **Send to mobile**.
    - To make physical keys, specify the number of keys to make, select an encoder that is online, click **Make Key**, then present keys to the encoder (as prompted).
12. When prompted that keys were made/sent successfully, click **Done**. You can verify that a mobile key was delivered in Staff Management. The key is listed on the Active Keys tab in the staff member profile.



Make a Limited Use Staff Key

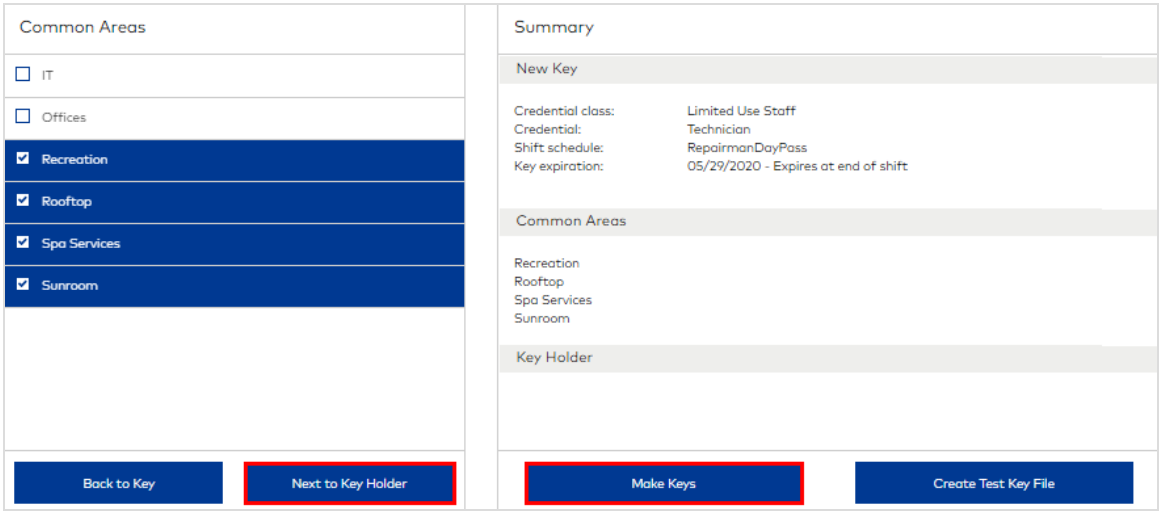
Follow these instructions when making a key based on the Limited Use Staff class type.

1. Go to Staff Keys.



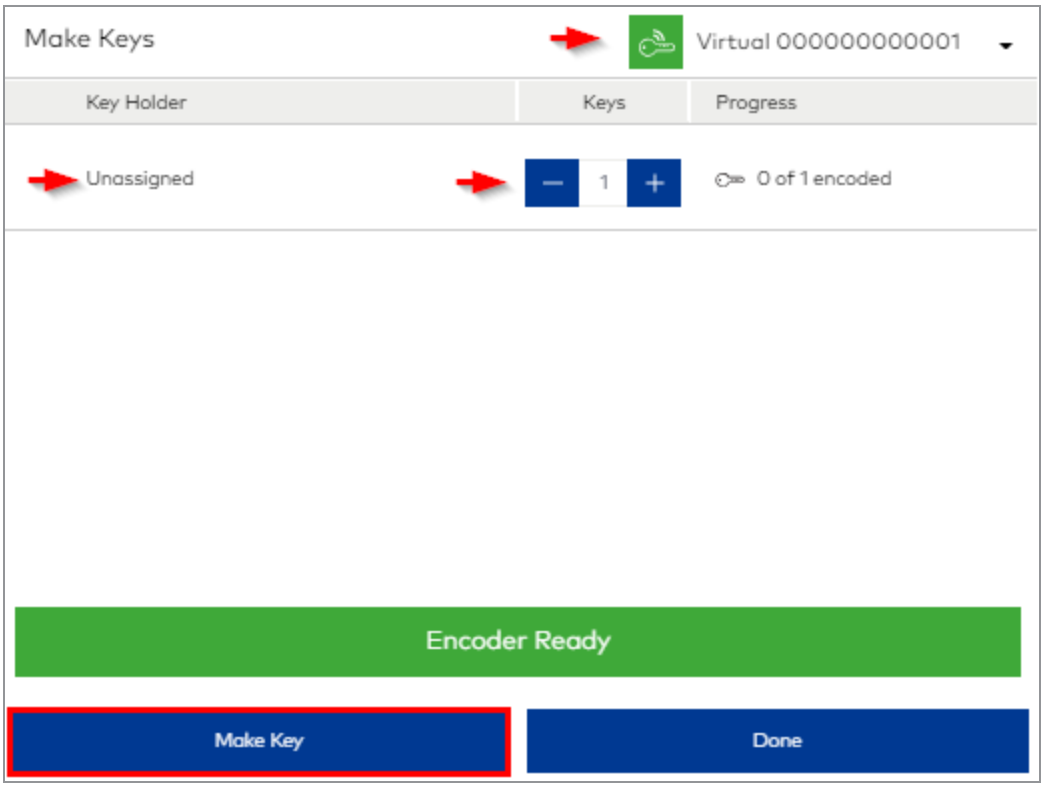
2. Select a credential class. Only those classes for which credentials are defined are listed.
3. Select a credential.
4. Select whether to make a New or Additional key. Making a New key invalidates the selected credential on all active keys. Making Additional keys (copies) has no effect on existing active keys.
5. (*optional*) Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. (*optional*) Specify a date after which the key is invalid.

7. The menu option that displays depends on whether a Staff Common Area Profile is associated with the selected credential.
   - If yes, click **Next to Common Areas** and proceed to the next step.
   - If no, proceed to step 9.



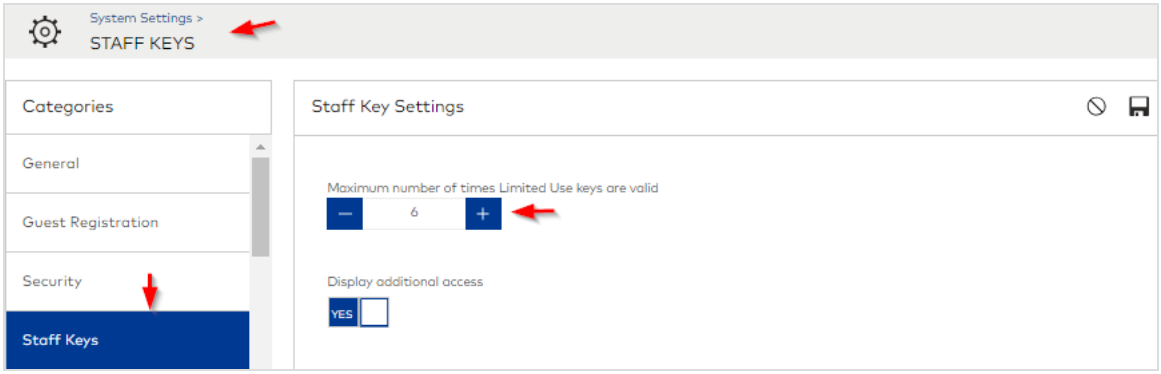
8. Select the limited-access common areas to authorize on the key.
9. (*optional*) Click **Next to Key Holder**. Select the staff to whom you want to assign the key. To add a staff member, click (Add) , specify first and last names, then click **Save**.

10. Click **Make Keys**:



- To make a mobile key, click **Send to mobile**.
- To make physical keys, specify the number of keys to make, select an encoder that is online, click **Make Key**, then present keys to the encoder (as prompted).

11. When prompted that keys were made/sent successfully, click **Done**. You can verify that a mobile key was delivered in Staff Management. Because we did not assign a key holder, the key cannot be viewed in a staff profile. Use of the key is limited to the number of times specified in System Settings.

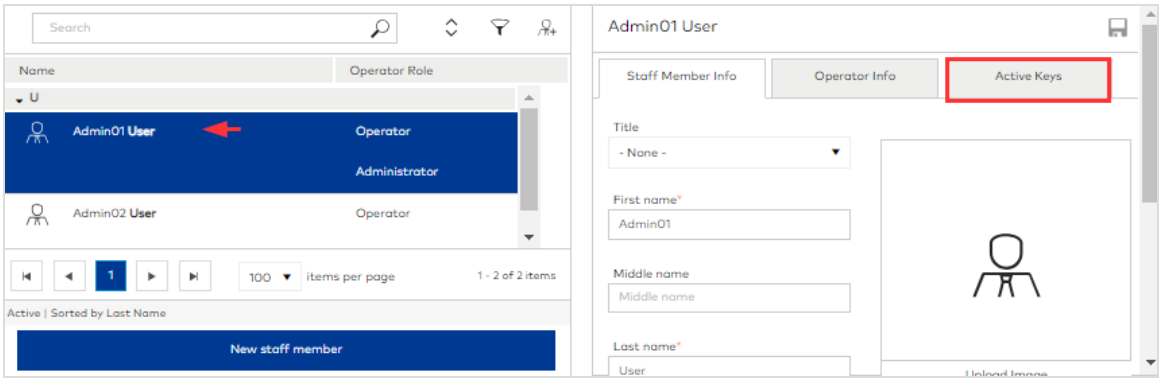

System Settings >
STAFF KEYS
Categories
General
Guest Registration
Security
Staff Keys
Staff Key Settings
Maximum number of times Limited Use keys are valid
6
Display additional access
YES

Replace Staff Keys

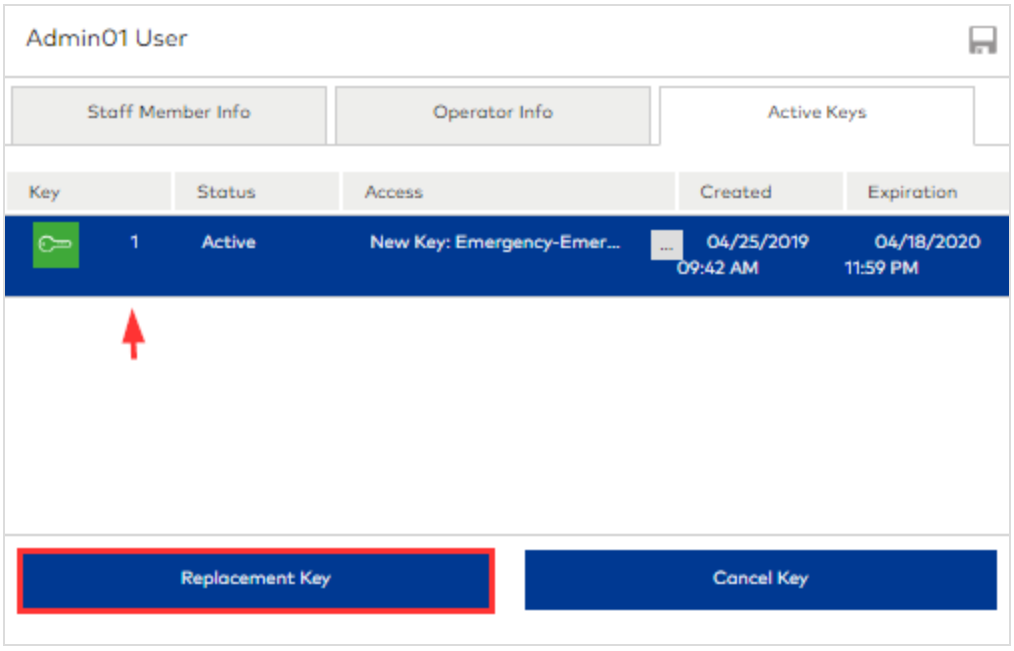
Replacement Keys are made to replace a damaged or worn-out key. They do not invalidate previously active keys.

To make a Replacement Key:

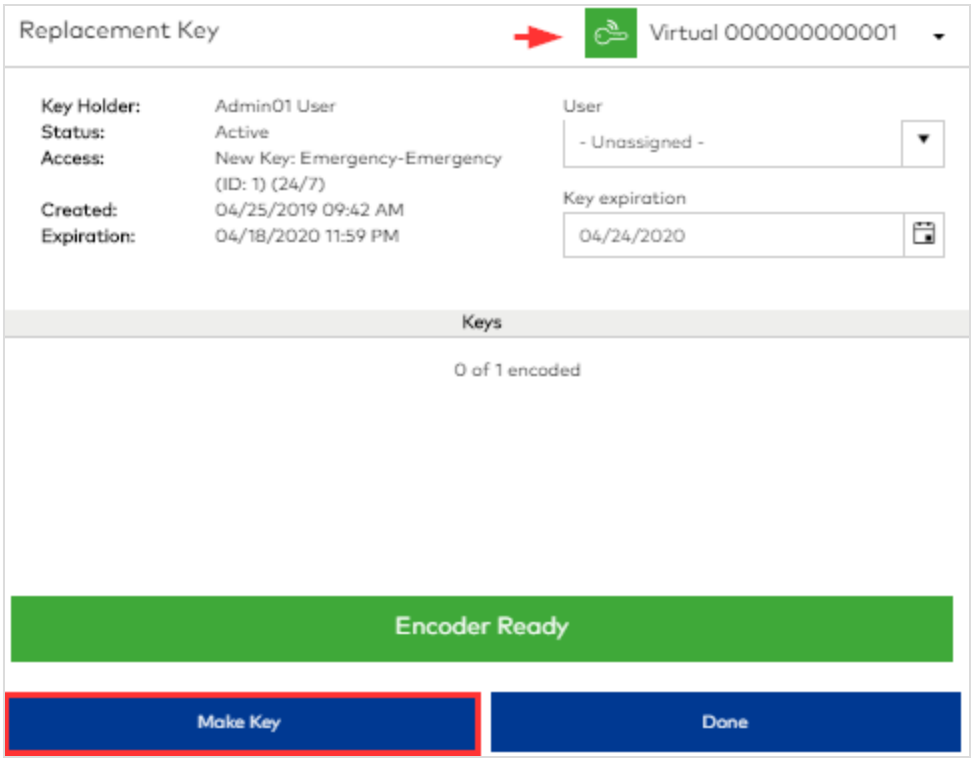
1. Go to Staff Management.



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



4. Select the key that you want to replace.
5. Click **Replacement Key**.



6. Select an encoder  that is online and available to the workstation.
7. (*optional*) Select the staff to whom you want to assign the key.
8. (*optional*) Specify a date after which the key is invalid.
9. Click **Make Key**.
10. Present a key to the encoder.
11. When prompted that the key was made successfully, click **Done**.

Invalidate Staff Access

There are multiple options when you need to invalidate staff access. The best method depends on the Ambiance modules authorized for your Operator account and the reason that you want to invalidate access.

Here's the situation ...

Find the situation that most fits and review the recommended option.

You need to stop an Operator from logging in to Ambiance.	**Block the Operator** The Operator cannot log in to Ambiance (until unblocked), but all active keys assigned to the Operator remain valid.
A staff member left permanently.	**Make Cancel Keys and Deactivate Staff Member** Make a Cancel Key for each active key assigned to the staff member, then deactivate the staff member. You can make Cancel Keys directly in Staff Management or System Keys. For mobile keys, you can send the Cancel Key directly to the mobile device.
A staff member left temporarily.	**Make Cancel Keys** Make a Cancel Key for each active key assigned to the staff member. You can make Cancel Keys directly in Staff Management or System Keys. You can optionally deactivate the staff member then re-activate them upon return. For mobile keys, you can send the Cancel Key directly to the mobile device.
A staff key was lost or stolen.	**Make New Keys or Make Cancel Keys** ❑ If the staff member is the only person with a key to the credential, make New Keys. ❑ If multiple staff members are issued keys with the same credential, make Cancel Keys for each active key assigned to the staff member.
You need to temporarily stop all staff from entering a guest room.	**Make Block Keys** Invalidates all staff keys for the selected guest room/suite door. If the intention is to suspend access temporarily, then you can make Unblock Keys to re-establish access.
You need to temporarily stop all non-Emergency personnel from entering one or more guest rooms.	**Make Electronic Lockout Keys** Temporarily invalidates all non-emergency keys. When electronic lockout is active, only a key with the Emergency credential can open the lock.

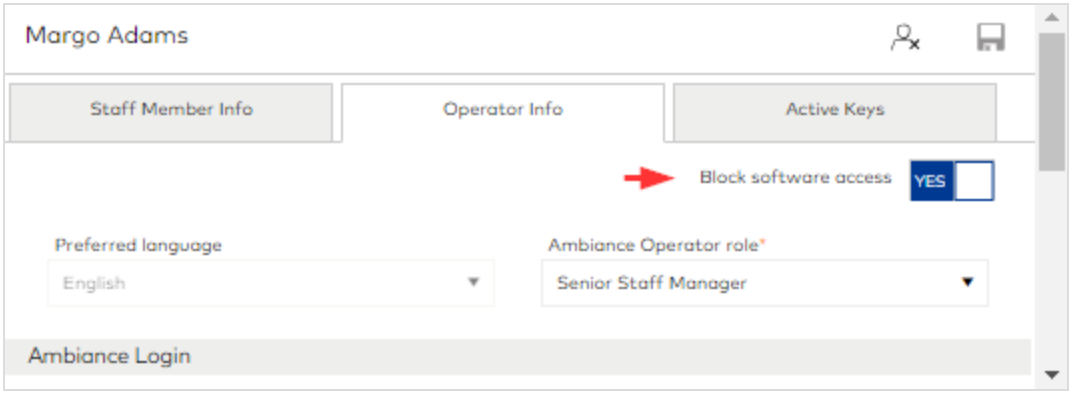
⚠ Don't forget that access remains valid until the Cancel/Block/ELO/New keys are presented to locks.

Block/Unblock Operator Access

Blocking an Operator prevents the Operator from logging in to Ambiance. 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 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.

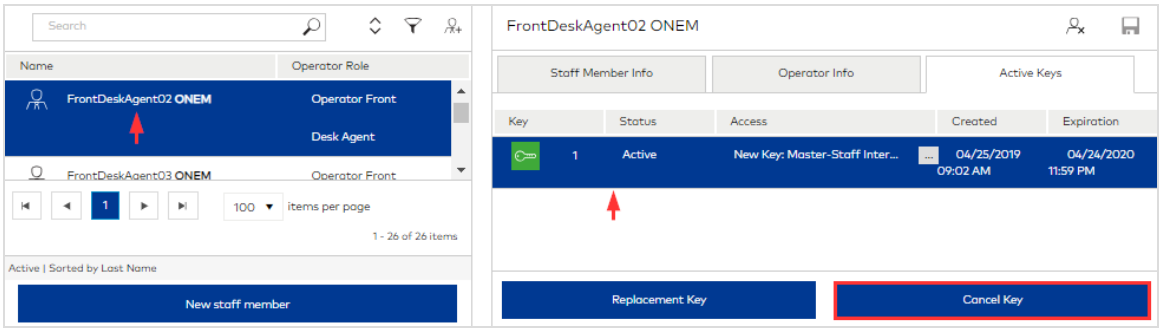
Make Cancel Keys

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

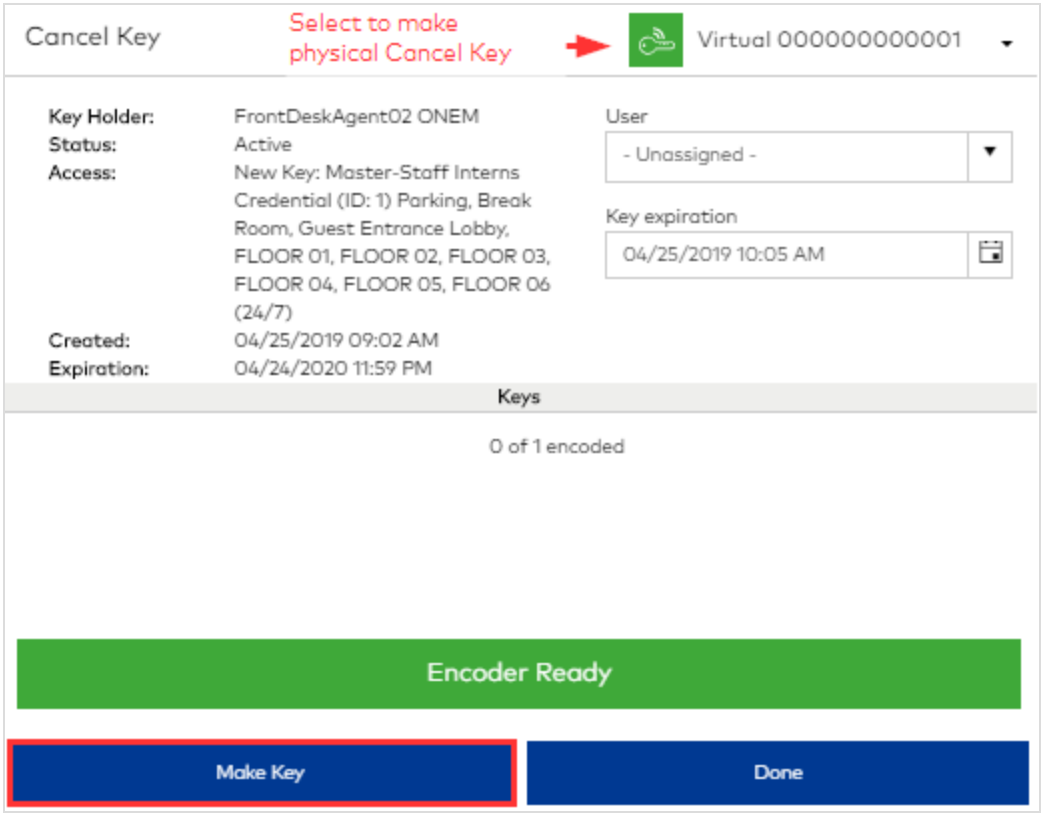
can be made to cancel staff keys in the Staff Management module (see below) and in the System Keys module.

> When making a Cancel Key to invalidate staff access, you must select the same credential class/credential that is encoded on the key that you want to cancel.

1. Go to Staff Management.
2. Select a staff member.
3. Click the **Active Keys** tab.
4. Select the key that you want to cancel.



5. Click **Cancel Key**.



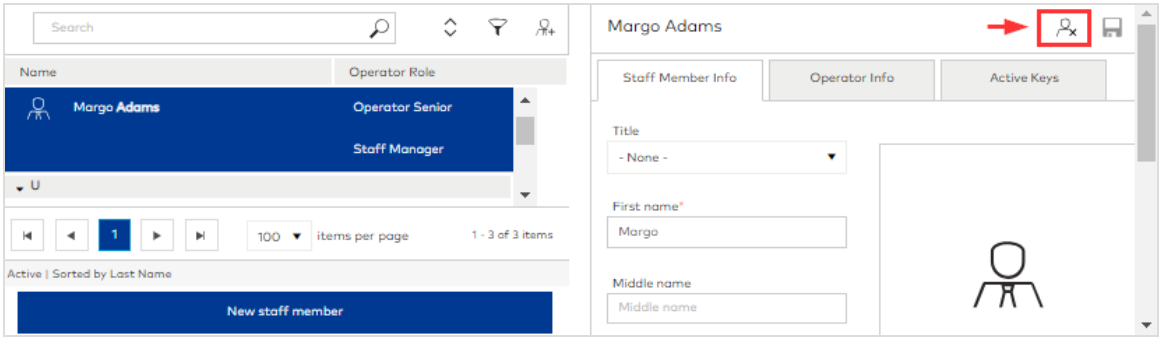
6. (*optional/physical keys only*) Select the staff to whom you want to assign the key.
7. (*optional/physical keys only*) Specify a date after which the Cancel Key is invalid.
8. Perform one of the following:
   - If you are canceling a physical key, select an encoder that is online, click **Make Cancel 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 Active Keys tab in the staff member profile.

Deactivate Staff

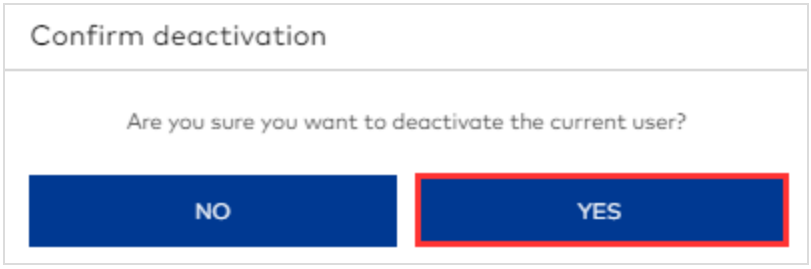
Deactivated staff are denied access to all access points. Additionally, staff who have been promoted to Operator are prevented from logging in to Ambiance. Staff may be automatically deactivated due to security controls such as failing to renew an expired

password. If a staff member is automatically deactivated, you must (re)activate the staff member manually.

1. Go to Staff Management.



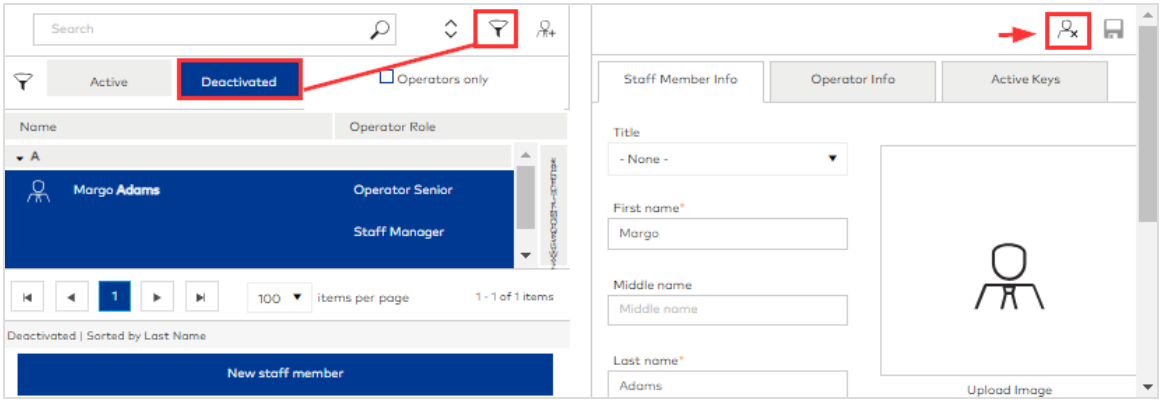
2. Select a profile.
3. Click (Deactivate user) .



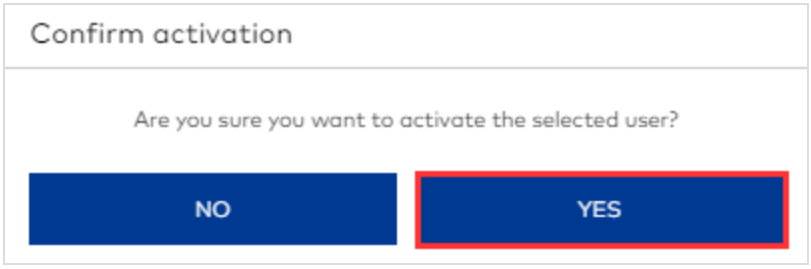
4. Click **YES** to confirm.

Activate Staff

1. Go to Staff 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 Ambiance login.

Make New Keys

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

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 access, you must select the same credential class/credential that is encoded on the key that you want to block.

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**.

Programming / Auditing

This section includes the following subjects:

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 Ambiance. For a list of when access points (locks) must be reprogrammed, see Access Point Programming Required.

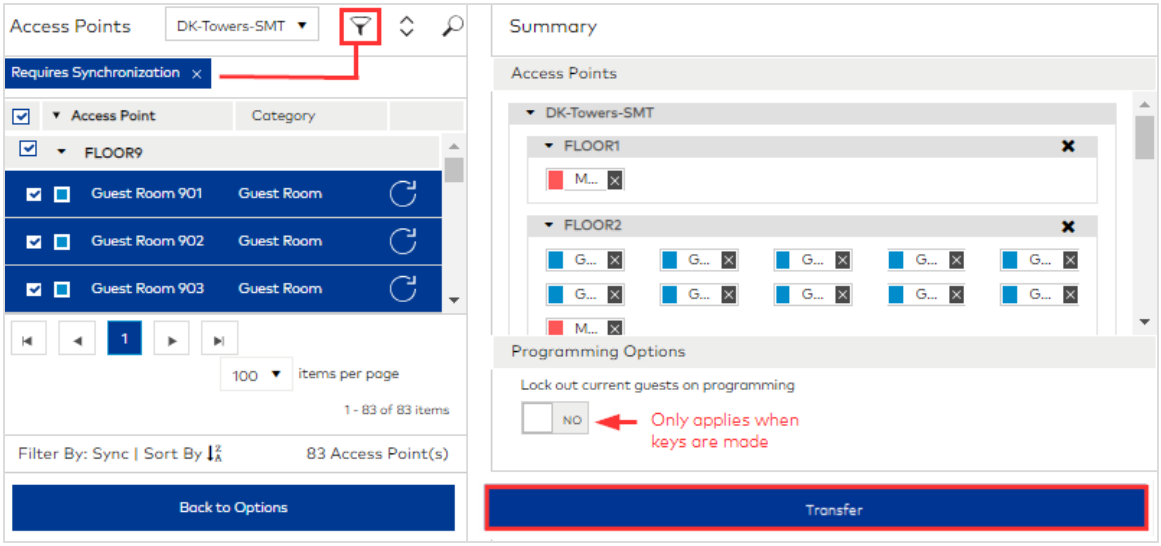
Some programming steps are performed on the M-Unit (Maintenance Unit). For official instructions, refer to the documentation distributed with your device. If M-Unit authentication is enabled in System Settings > Security, M-Unit credentials must be configured for at least one Operator in Staff Management.

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:

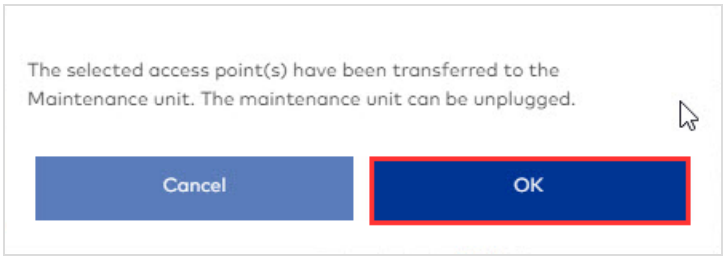
```
C:\windows\system32\CheckNetIsolation.exe LoopbackExempt -a -
n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
```

To reprogram locks:

1. Go to Programming/Auditing.
2. Click **Programming**.



3. Select the access points that you want to synchronize with Ambiance 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.
4. For **Lock out current guest on programming**, select whether to invalidate all active keys issued to guests after programming the lock. If you select **Yes**, New (Guest) Keys must be made and issued after the locks are programmed.
5. Connect the M-Unit to the workstation.
6. In Ambiance , 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.



7. Click **OK**.
8. Disconnect the M-Unit from the workstation.
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.

Audit locks

The Ambiance data transfer function enables individual lock audits to track and store historical activity about access points. The data that is collected from locks and transferred to Ambiance is stored in the Ambiance database and available when generating Access Point Audit Reports.

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 in Staff Management 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 Ambiance workstation.

9. In Ambiance, 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 Ambiance.
13. Click **Transfer**.
14. When prompted that the transfer is complete, click **OK**. All interrogation files are stored on the Ambiance server and are accessible from the Access Point Audit Report.

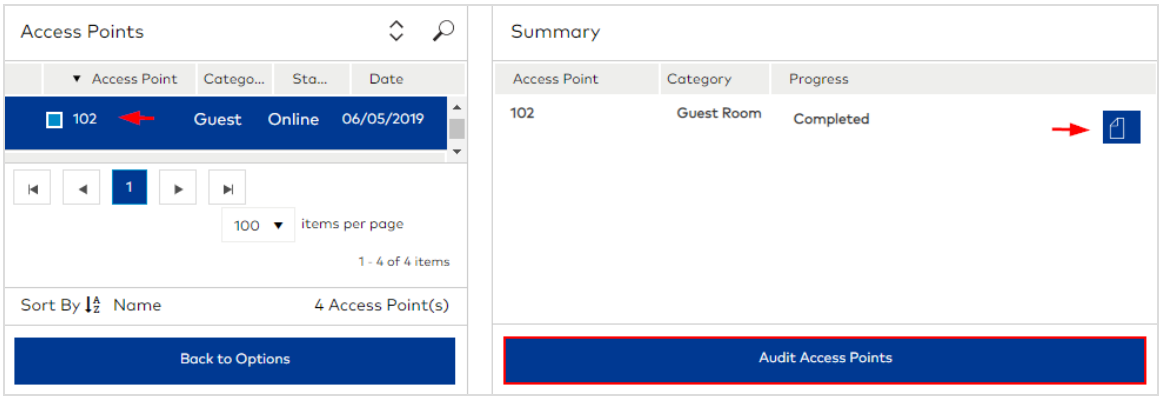
Audit online access points

When Remote Lock Management is enabled in System Settings, online access points can be audited directly in Ambiance. 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: Guest Room, Suite, Meeting Room, 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.
2. Click **Online Access Points**.



3. Select an access point.
4. 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

The System Keys module is used to encode keys for immediate intervention and to perform advanced operational programming.

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 Guest Room 100. Before making a Block Key, you must know the credential class and credential 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. Remote operation is supported.

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 block. A Cancel Key must be presented to all access points for which the original key has credentials. 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. Remote operation is supported.

Inhibit Keys

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

Special Function Keys

Special Function Keys (SFKs) are paired with Primary Program Keys (PPKs) to perform system-level operations on a lock.

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 Guest Room 100. Before making a Block Key, you must know the credential class and credential that you want to block.

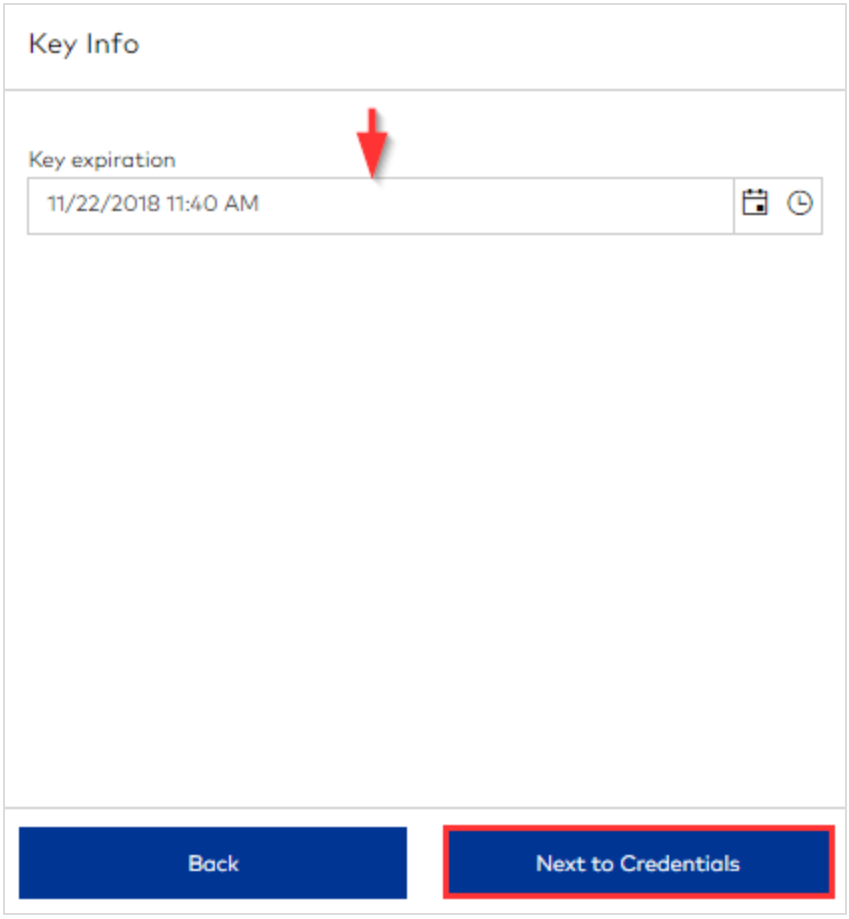
Block Keys can be used to invalidate:

- Guest Keys
- Staff Keys
- ELO Keys
- Latch/Unlatch/Toggle Latch/Unlatch Keys
- Inhibit Keys

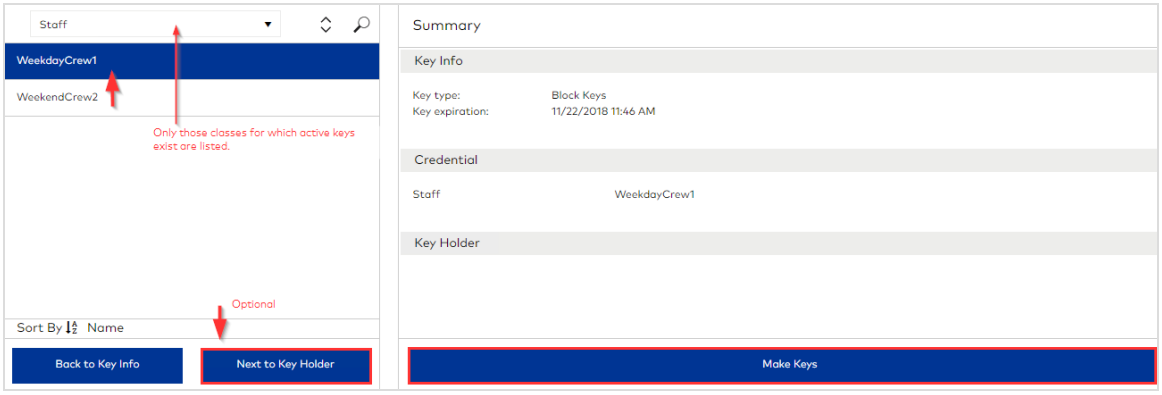
If the intent is to temporarily block access, you can use an Unblock Key to unblock a key that was previously blocked by a Block Key.

Make Block Keys

1. Go to System Keys.
2. Click **Block Keys**.



3. Specify expiration details.
4. Click **Next to Credentials**.

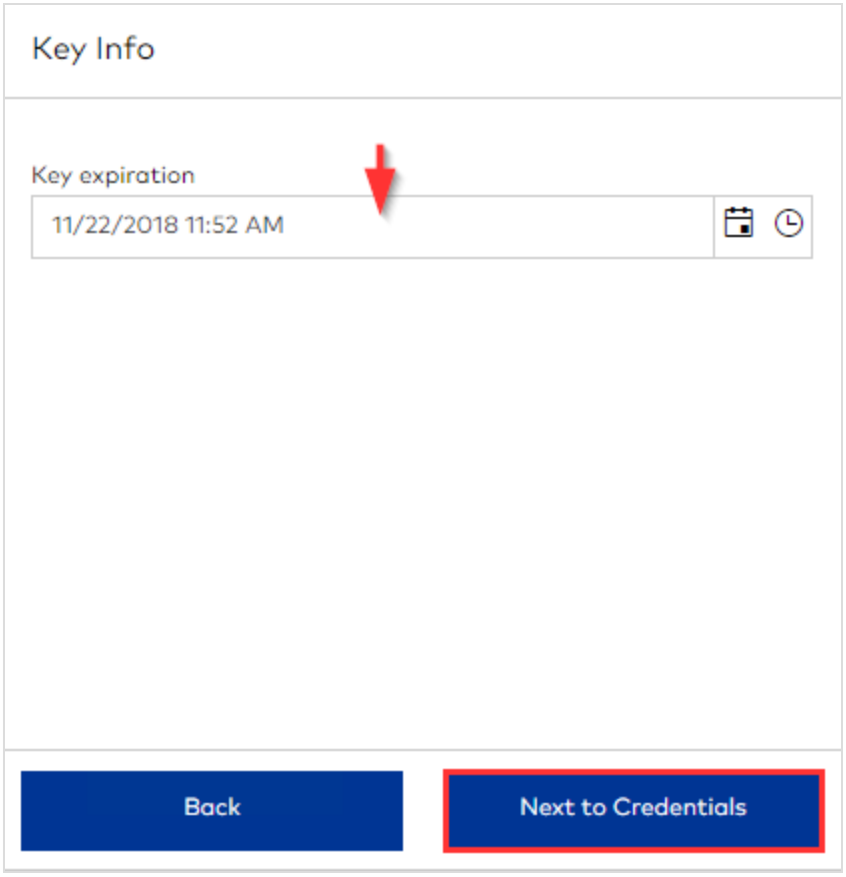


5. Select the credential class under which the credential you want to block is defined. Only those classes for which active keys exist are listed.
6. Select the credential (or access point) encoded on the key that you want to block.
7. (*optional*) Click **Next to Key Holder** and select the staff to whom you want to assign the key. To add a staff member, click (Add) +, specify first and last names, then click **Save**.
8. Click **Make Keys** or, if Remote Lock Management is enabled, **Block Keys Remotely**. Proceed only if you are making a physical key.
9. Select an encoder  that is online.
10. Present a key to the encoder.
11. Click **Start**.
12. When notified that keys were made successfully, click **Done**.

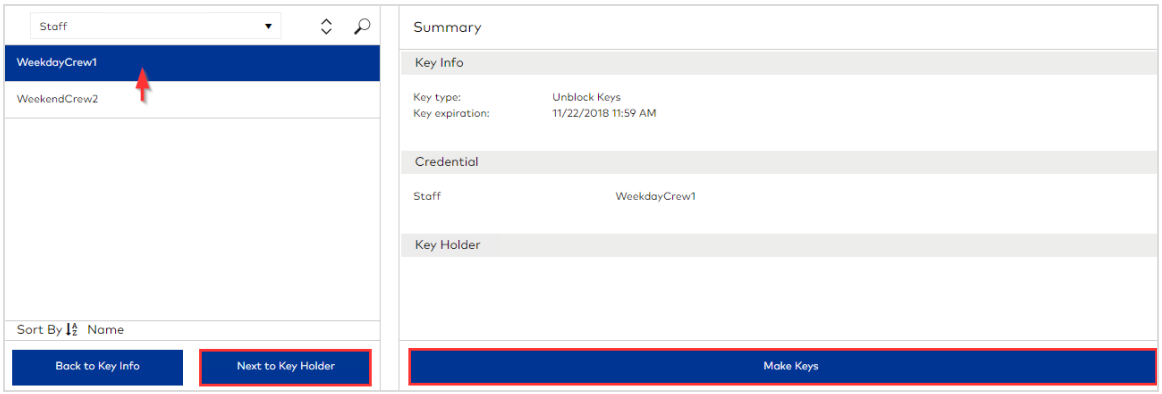
Make Unblock Keys

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.
2. Click **Unblock Keys**.



3. Specify expiration details.
4. Click **Next to Credentials**.



5. 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.
6. Select the credential (or access point) encoded on the key that you want to unblock.
7. (*optional*) Click **Next to Key Holder** and select the staff to whom you want to assign the key. To add a staff member, click (Add) +, specify first and last names, then click **Save**.
8. Click **Make Keys** or, if Remote Lock Management is enabled, **Unblock Keys Remotely**. Proceed only if you are making a physical key.
9. Select an encoder  that is online.
10. Present a key to the encoder.
11. Click **Start**.
12. When prompted that keys were made successfully, click **Done**.

Cancel Keys

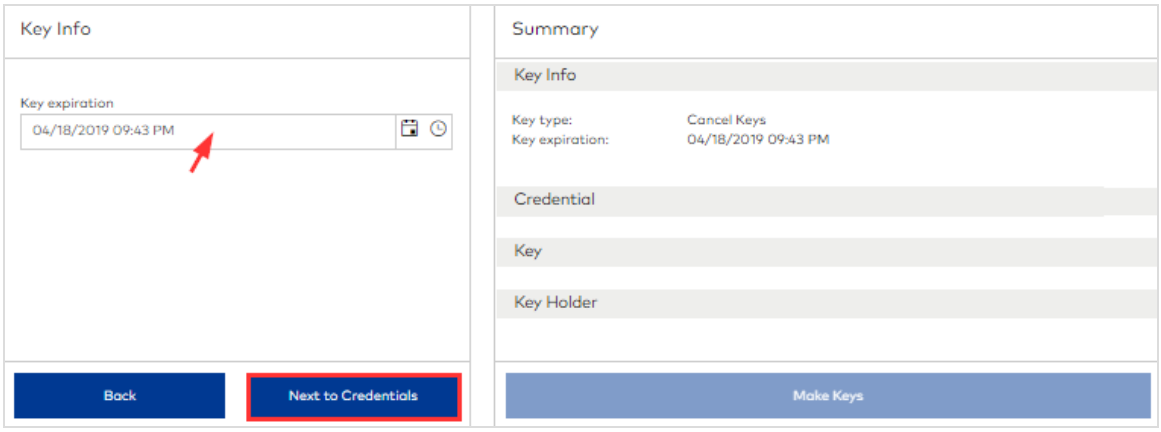
Make a Cancel Key to permanently invalidate a specific key instance. Before making a Cancel Key, you must know the credential class and credential that you want to cancel. A Cancel Key must be presented to all access points for which the original key has credentials.

Cancel Keys can be used to invalidate:

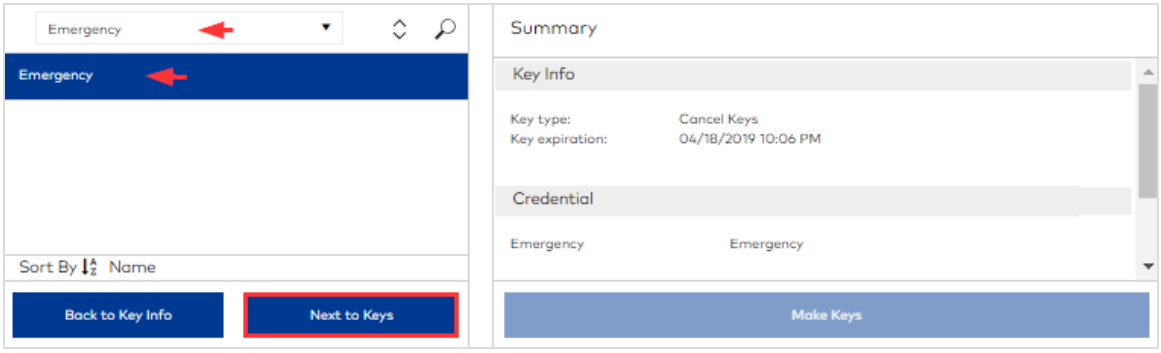
- Staff Keys
- ELO Keys
- Latch/Unlatch/Toggle Latch/Unlatch Keys
- Inhibit Keys

To make Cancel Keys:

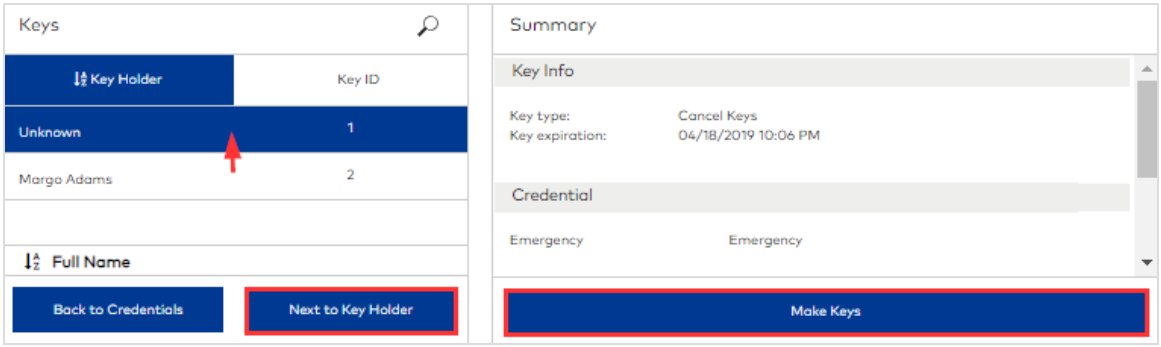
1. Go to System Keys.
2. Click **Cancel Keys**.



3. Specify expiration details.
4. Click **Next to Credentials**.



5. Select the credential class under which the credential you want to cancel is defined. Only those classes for which active keys exist are listed.
6. Select the credential or access point encoded on the key that you want to cancel.
7. Click **Next to Keys**.



8. Select the key that you want to cancel. You can view the list of keys by Key Holder or by Key ID.
9. (*optional*) Click **Next to Key Holder** and select the staff to whom you want to assign the key. To add a staff member, click (Add) **+**, specify first and last names, then click **Save**.
10. Click **Make Keys** or, if Remote Lock Management is enabled, **Cancel Keys Remotely**. Proceed only if you are making a physical key.
11. Select an encoder  that is online.
12. Present a key to the encoder.
13. Click **Start**.
14. When notified that keys were made successfully, click **Done**.

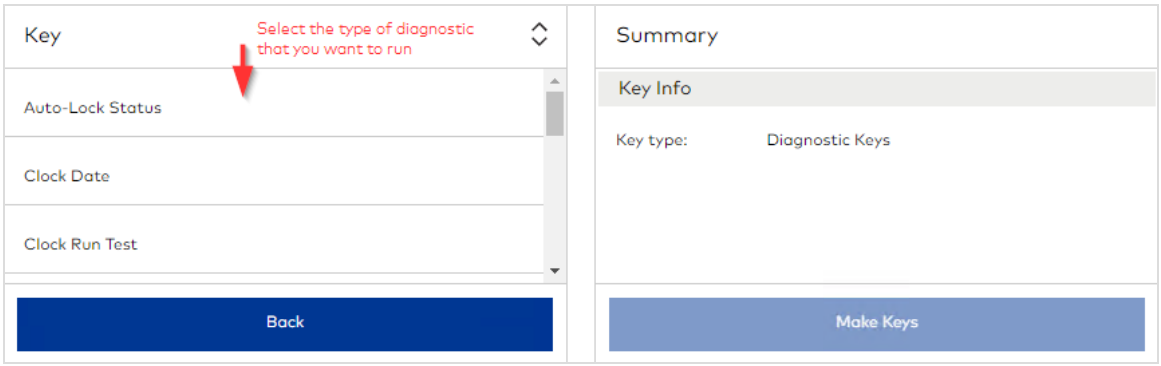
Diagnostic Keys

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.

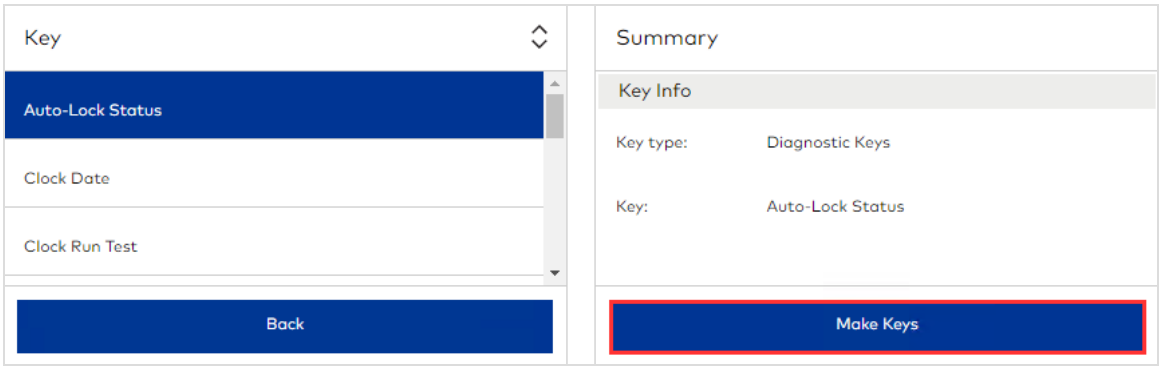
Make Diagnostic Keys

1. Go to System Keys.
2. Click **Diagnostic Keys**.



3. 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.



4. Click **Make Keys**.
5. Select an encoder  that is online.
6. Present a key to the encoder.
7. Click **Start**.
8. When prompted that keys were made successfully, click **Done**.

Diagnostic Results

For details about interpreting a flash sequence, see Appendix C: Light Indicator Reference.

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

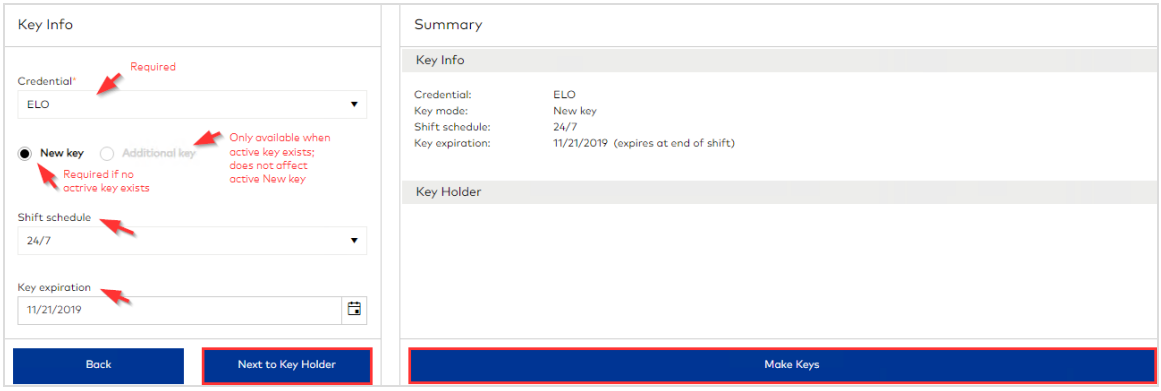
ELO (Electronic Lockout) Keys temporarily invalidate all non-emergency keys by double locking the door from the outside (activating the privacy switch or deadbolt). When an electronic lockout is active, only a key with the Emergency credential can open the lock. When the electronic lockout is removed, 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:

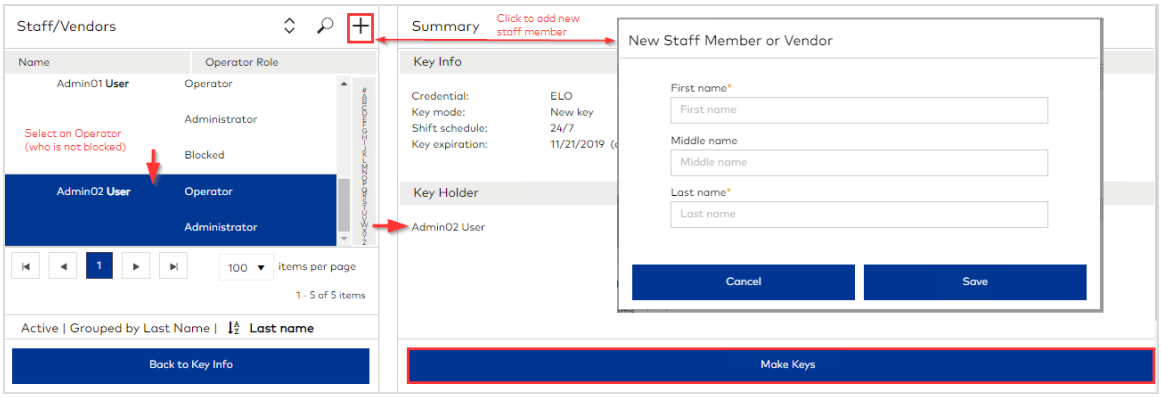
> The credential selected by default (**ELO**) or a custom credential based on the ELO credential class is required.

1. Go to System Keys.
2. Click **Electronic Lockout Toggle Keys**. The default credential **ELO** is required.



3. 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.
4. 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.
5. Specify expiration details.

6. (*optional*) Click **Next to Key Holder** and select the staff 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** or, if Remote Lock Management is enabled, **Electronically Lockout Keys Remotely**. Proceed only if you are making a physical key.
8. Select an encoder  that is online.
9. Click -/+ to specify how many keys to make.
10. Present a key to the encoder.
11. Click **Start**.
12. When prompted that keys were made successfully, click **Done**.

Electronic Lockout Key LED Flash Sequence

For details about interpreting a flash sequence, see Appendix C: Light Indicator Reference.

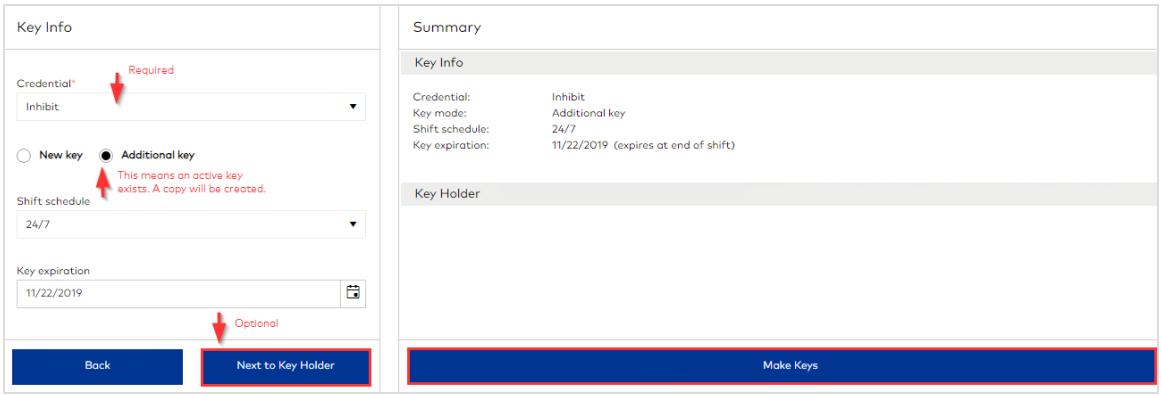
- The following LED flash sequence indicates the electronic lockout is activated:
  - Red (1) Yellow (12)
- The following LED flash sequence indicates the electronic lockout is removed:
  - Green (1) Yellow (12)

Inhibit Keys

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

Make Inhibit Keys

1. Go to System Keys.
2. Click **Inhibit Keys**. The default credential **Inhibit** is required.



3. 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.
4. 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.
5. Specify expiration details.
6. (*optional*) Click **Next to Key Holder** and select the staff 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** or, if Remote Lock Management is enabled, **Inhibit Keys Remotely**. Proceed only if you are making a physical key.

8. Select an encoder  that is online.
9. Click -/+ to specify the number of keys to make.
10. Present a key to the encoder.
11. Click **Start**.
12. When prompted that keys were made successfully, click **Done**.

Inhibit Key LED Flash Sequence

For details about interpreting a flash sequence, see Appendix C: Light Indicator Reference.

- 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)

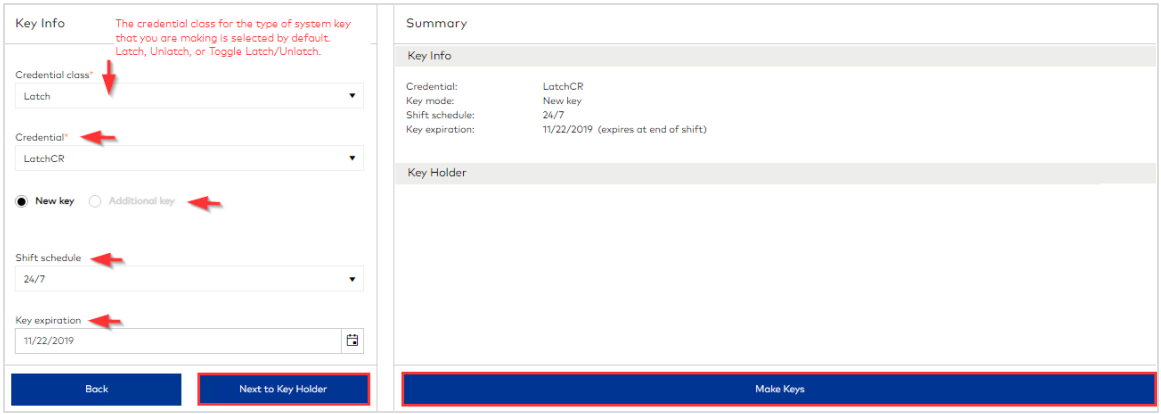
Latch and Unlatch Keys

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**—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 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. Click -/+ to specify the number of keys to make.
12. Present a key to the encoder.
13. Click **Start**.
14. When prompted that keys were made successfully, click **Done**.

Primary and Secondary Program Keys

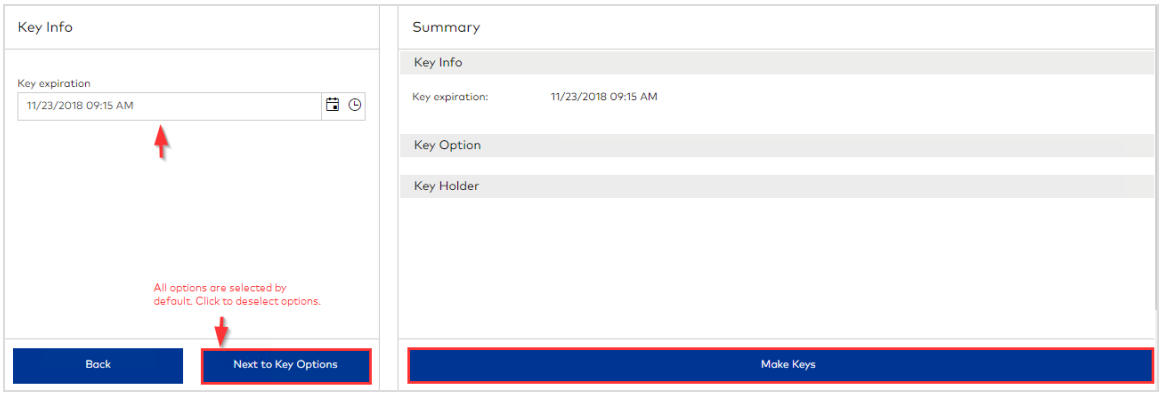
Primary Program Keys (PPKs) put the lock into programming mode and are used in conjunction with Program Information (PI) Keys and Program Status (PS) Keys to program locks and authorize special functions (see Create a Special Function Key). They are also used to reprogram the current Secondary Program Key (SPK) or remaster a different SPK.

While PPKs are non-opening keys, they allow doors to be opened when the lock is in Mode 3 due to a problem with the programming chip in the lock's circuit board. Mode 3 is identified by two green and yellow flashes followed by all lights flashing four times. Use the PPK followed by a valid master key to open the door, remove the lock and replace the circuit board.

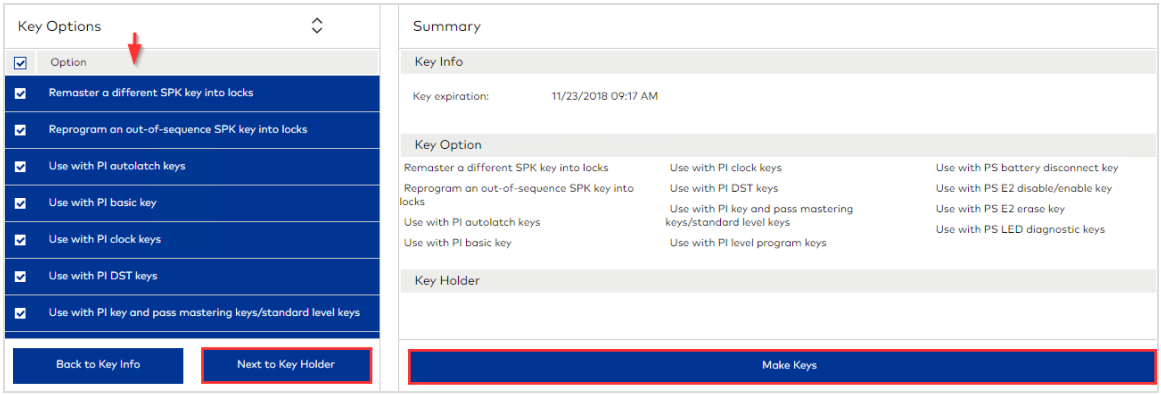
Secondary Program Keys (SPKs) reprogram or resynchronize the current Primary Program Key (PPK) into access points and remaster a different PPK into a lock. Essentially, an SPK is a backup to the PPK but does not put locks into programming mode.

Make Primary Program Key

1. Go to System Keys.
2. Click **Primary Program Keys**.



3. Specify expiration details.
4. Click **Next to Key Options**.



5. 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**

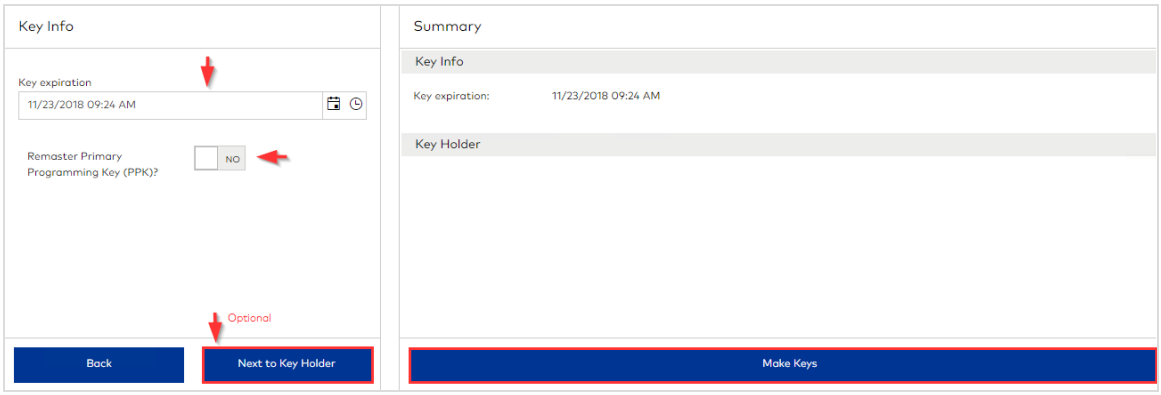
- **Use with PS battery disconnect key**—Select this option to encode a PPK that authorizes a key to shut down the lock before the lock battery disconnects.

6. (*optional*) Click **Next to Key Holder** and select the staff 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**.
8. Select an encoder  that is online.
9. Present a key to the encoder.
10. Click **Start**.
11. When prompted that keys were made successfully, click **Done**.

Make Secondary Program Key

To make a Secondary Program Key:

1. Go to System Keys.
2. Click **Secondary Program Keys**.



3. Specify expiration details.
4. 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.

5. (*optional*) Click **Next to Key Holder** and select the staff 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 prompted that keys were made successfully, click **Done**.

Secondary Program Key LED Flash Sequence

For details about interpreting a flash sequence, see Appendix C: Light Indicator Reference.

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.

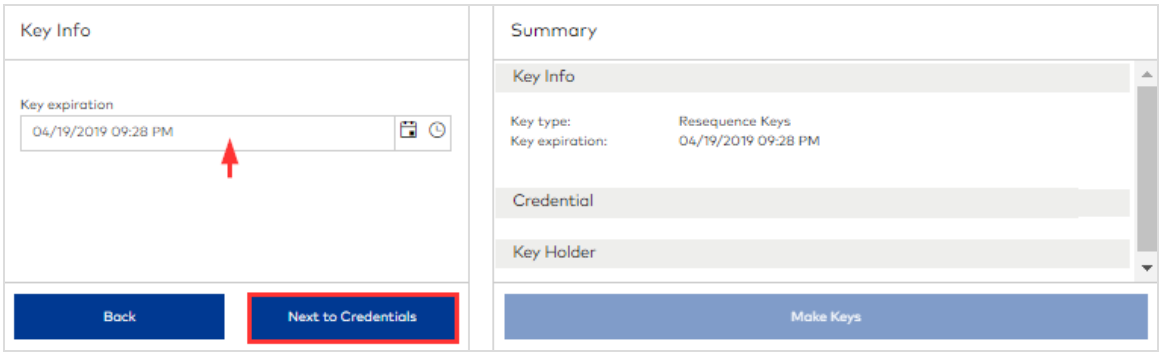
> The need to use a Resequence Key is rare. Staff can troubleshoot the lock to determine if the cause of the lock error is a corrupt sequence number.

Resequence Keys can be used to correct the sequence on:

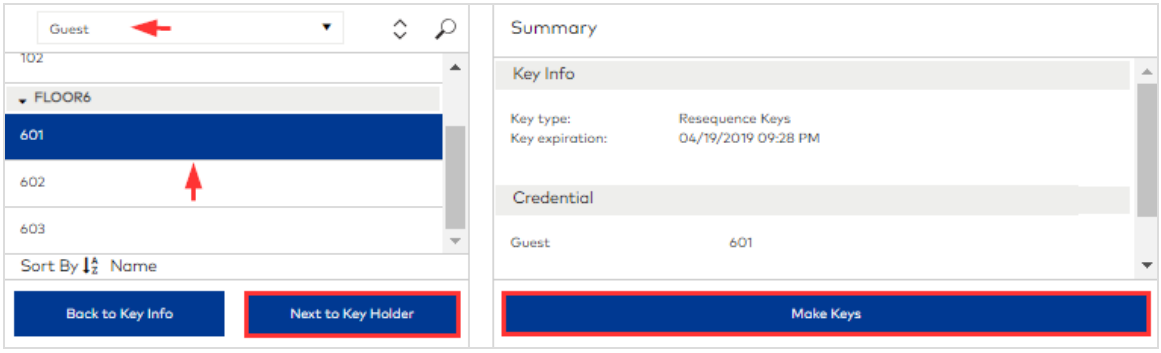
- Guest Keys
- Staff Keys
- ELO Keys
- Latch/Unlatch/Toggle Latch/Unlatch Keys
- Inhibit Keys

To make Resequence Keys:

1. Go to System Keys.
2. Click **Resequence Keys**.



3. Specify expiration details.
4. Click **Next to Credentials**.



5. 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.
6. 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.
7. (*optional*) Click **Next to Key Holder** and select the staff to whom you want to assign the key. To add a staff member, click (Add) +, specify first and last names, then click **Save**.
8. Click **Make Keys**.
9. Select an encoder that is online.
10. Present a key to the encoder.
11. Click **Start**.
12. When prompted that keys were made successfully, click **Done**.

Resequence Key LED Flash Sequence

For details about interpreting a flash sequence, see Appendix C: Light Indicator Reference.

- 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 guest levels, a new guest key must be made if a red flash precedes the green/yellow flashes.

Special Function Keys

Special Function Keys (SFKs) are paired with Primary Program Keys (PPKs) to perform system-level operations on a lock.

> SFKs 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.

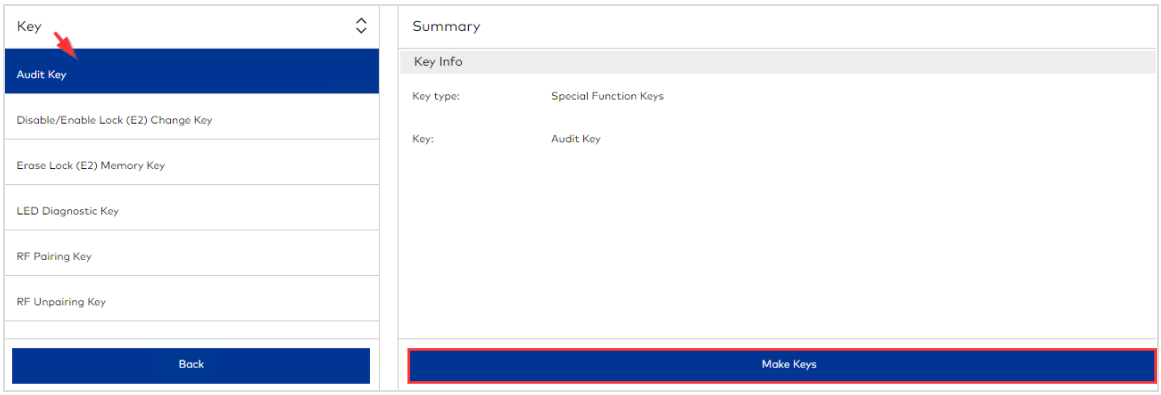
Special Function Key Types

The following types of Special Function Keys can be made in System Keys:

- **Audit Key**—Select this option to make a key that interrogates a lock to obtain status and diagnostic data. After auditing a lock with an Audit Key, present the key to the encoder and click the Read Key button in the Ambiance 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. The Audit Key is most efficient for auditing less than five access points. When an audit must be performed on more than five access points, use the M-Unit to interrogate locks.
- **Disable/Enable Lock (E2) 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 (E2) 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 hub. This key type only displays if Remote Lock Management is enabled.
- **RF Unpairing**—Select this option to make a key that disconnects a lock from the paired hub. This key type only displays if Remote Lock Management is enabled.

Make Special Function Keys

1. Go to System Keys.
2. Click **Special Function Keys**.



3. Select the type of special function that you want to run.
4. Click **Make Keys**.
5. Select an encoder  that is online.
6. Present a key to the encoder.
7. Click **Start**.
8. When prompted that keys were made successfully, click **Done**.

Monitoring

This section includes the following subjects:

Learning about Monitoring

The Monitoring module is where you can stay informed about remote lock management/online communication. The Metrics section provides a real-time snapshot of the hubs 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 hubs. In addition, the Monitoring module provides information about all keys made in Ambiance. 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.

Monitor Online Operations

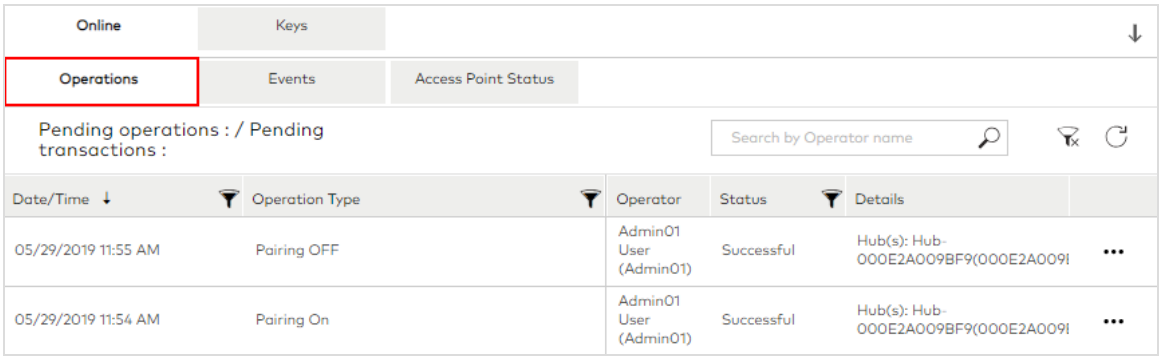
The Operations tab beneath the Metrics section lists the commands and related details sent to hubs and paired access points. Commands are issued from Device Management > Hubs & Paired Access Points. Transaction details are reported for each operation.

View Operations

To monitor operations:

» Go to Monitoring. Operations are displayed beneath the Metrics section.

> Collapse the Metrics section to show only the list of operations.



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 hubs 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 and user 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.

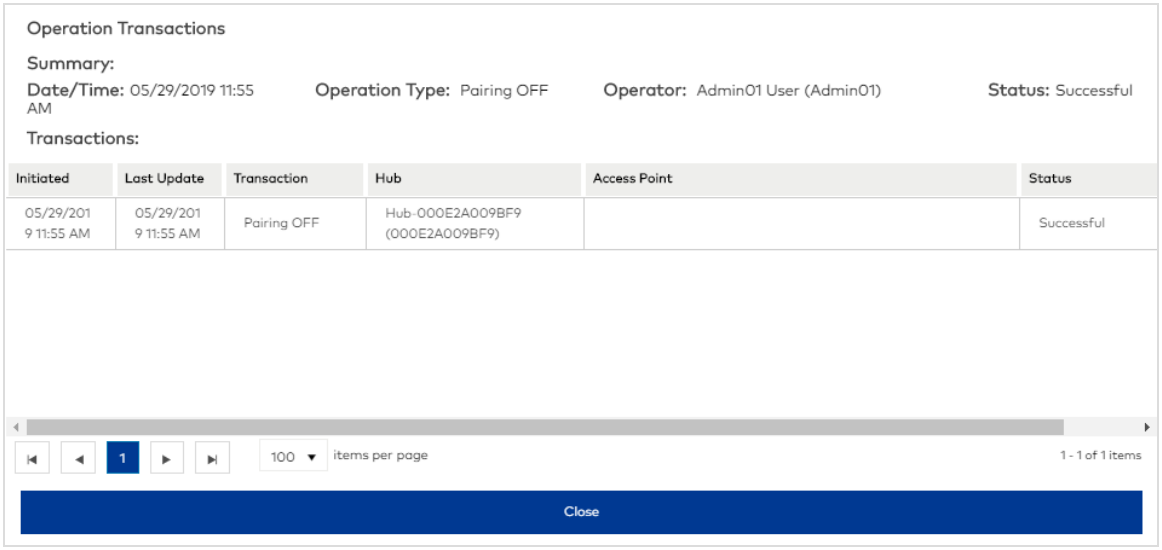
- Details—More information about the operation.

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 Operation Transactions 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).
- Hub—The hub 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

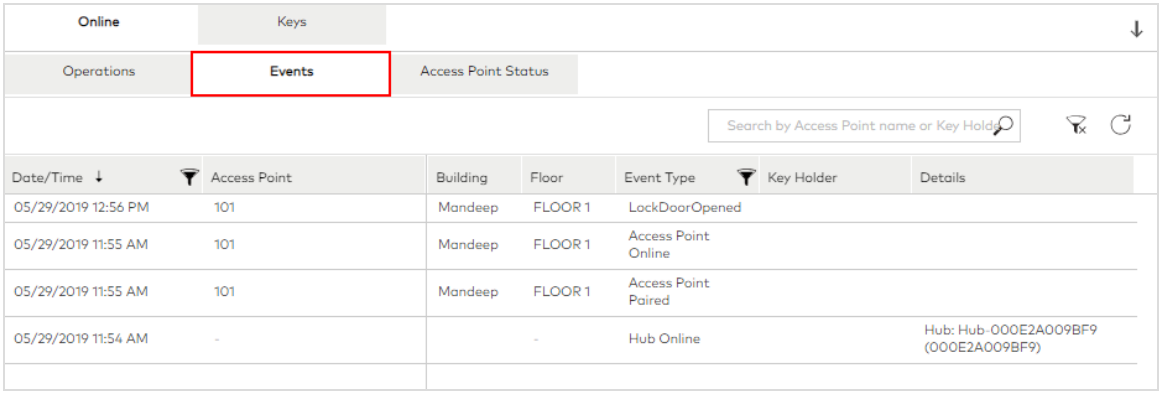
- Click any column to sort the list. When done, click Close.

Monitor Online Events

Events related to hubs and paired access points are listed. The list includes events for all key types (guest/staff/system keys) and changes to hub/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:

- Date/Time—Date and time the event occurred. 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: Guest 1 (for guests) and Unassigned (for staff or system keys). You can search for events based on the key holder name.
- Details—More information about the event (for example, Door Ajar / Short ajar - Guest). 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

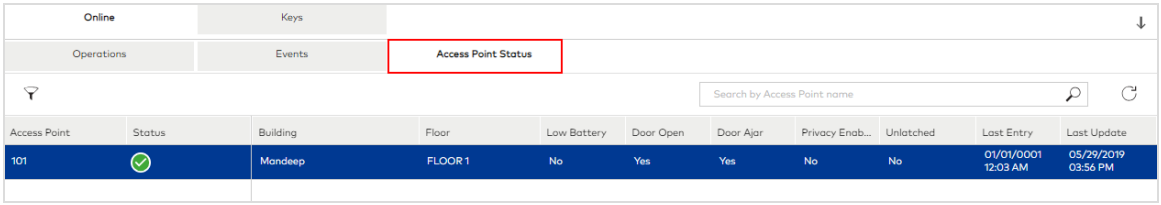
- To filter data, (Filter)  in the column heading row, select the information that you want to display, then click Filter. The (Filter Applied) icon  indicates that a filter is applied to the column.
- To clear filters for a column, click (Filter Applied)  > Clear.
- To clear all filters, click (Remove Filters)  .
- Click any column to sort the list.
- To refresh data, click (Refresh)  .

Monitor Access Point Status

The Access Point Status tab beneath the Metrics section lists the status of paired access points.

To view access point status:

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.
- 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.
- 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.

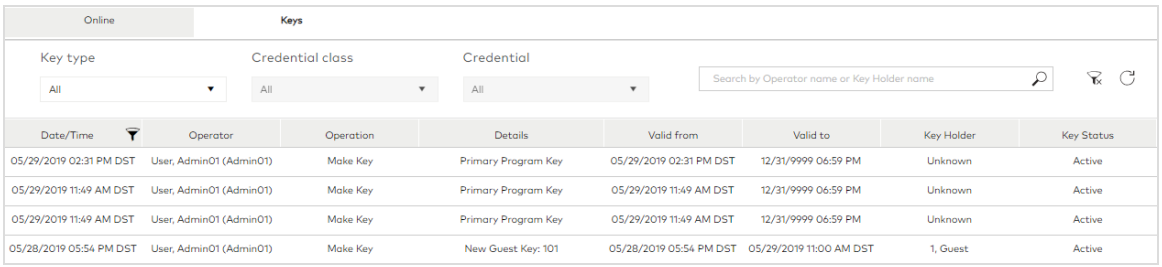
Customize the Display

- 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) .

Monitor Keys

The Monitoring module is where you can see the status for all guest, staff 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 Remote Lock Management 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.
- Operator—The full name and user 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.
- Operation—The MAKE KEY command.
- Details—The type of key (guest/staff/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—The name of the key holder. Defaults: Guest 1 (for guests) and Unassigned (for staff or system keys). You can search for keys used by a specific key holder.
- Key Status—For physical keys: Pre-registered/Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.

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) .

Reports

This section includes the following subjects:

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 Ambiance. 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.

Generate Report

1. Go to Reports > Access Point Audit Report.
2. Select the access point for which you want to transfer data to Ambiance. 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.

- 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
- 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**.
4. Because all classes are selected by default, deselect any class that you want to exclude from the report.
5. 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

- Credential Class
- Status—For physical keys: Pre-registered/Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- Key Holder
- Expiration Date
- Key Instance

Key/User Assignment Report

Generate this report to identify the keys assigned to guests or staff. 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 the type of user (Guest or Staff). The report lists key assignments for the selected type.
3. (*Staff type only*) Select whether to include active keys, inactive keys, or both in the report. (All keys with a status other than "Active" are considered inactive.)
4. Select whether to index the report by user type (Guest or Staff) or key credential.
5. Click **Next to Credential Classes**.
6. Because all classes are selected by default, deselect any class that you want to exclude from the report.
7. Click **Generate**.

View Report Details (Guest)

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
- Total keys assigned
- Site
- Report generated by
- Report generated on
- Guest Name (when displayed by Key)
- Credential Class
- Access Points (when displayed by Key)
- Status
- Key Request Date

- Creation Date/Valid from
- Expiration Date/Expiration

View Report Details (Staff)

- Displayed by
- Total keys assigned
- Site
- Report generated by
- Report generated on
- User Name
- Credential Class
- Credential
- Additional Access
- Status
- Key Request Date
- Creation Date
- Expiration Date

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 hubs.
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 hubs 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 Hub Status Report

Generate this report to view hub status information.

Generate Report

1. Go to Reports > Online Hub Status Report.
2. Select whether to include online and/or offline hubs.
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
- Hub
- Type
- Mac Address
- Status (Online/Offline)
- Antenna
- Last Update
- FW Vers Hub
- FW Vers AVR
- FW Vers Ember

Online Paired Access Point Report

Generate this report to display which access points are currently paired to hubs.

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.

- Hub (Name)
- Paired Access Points
- Unpaired Access Points

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 Ambiance software.
3. Click **Next to Operator Roles**.
4. Because all roles are selected by default, deselect any role that you want to exclude from 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.

- 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**.
6. Because all access point types are selected by default, deselect any type that you want to exclude from 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.

- 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 Ambiance 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 Ambiance 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 Access Report

Generate this report to view historical information about staff access.

Before you can generate this report, you must obtain and read the physical key assigned to staff. 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 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: Pre-registered/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 guest (physical/mobile keys), staff (physical/mobile) and system keys, then click **Next to Credential Classes** and deselect the classes to exclude from the report.
   - If you select **System** and remote lock management is enabled, select whether to include Offline or Online operations.
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.

- Date range
- Number of transactions
- Site
- Report generated by
- Report generated on
- Credential Classes
- Operators—The full name and user name of the Operator who was logged in when the key was encoded.
- Key Request Date
- Operator

- Credential
- Key Type
  - Guest (Physical)
  - Guest (Mobile)
  - Staff (Physical)
  - Staff (Mobile)
  - System
- Key Mode
  - Additional
  - New
- Status—For physical keys: Pre-registered/Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- Mobile Number
- Key Holder

View Report Details (System)

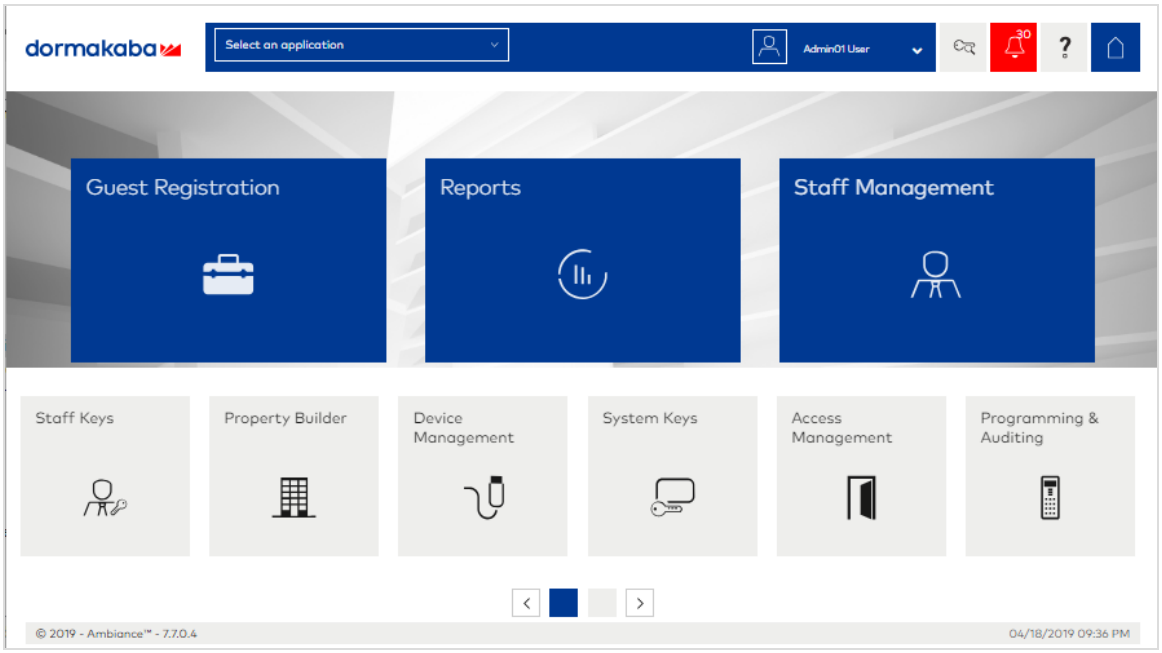
- Date range
- Number of transactions
- Site
- Report generated by
- Report generated on
- Operators
- Transaction Date
- Operator—The full name and user name of the Operator who was logged in when the key was encoded.
- Operation
- Details
- Transaction Status

Toolbar Basics

This section includes the following subjects:

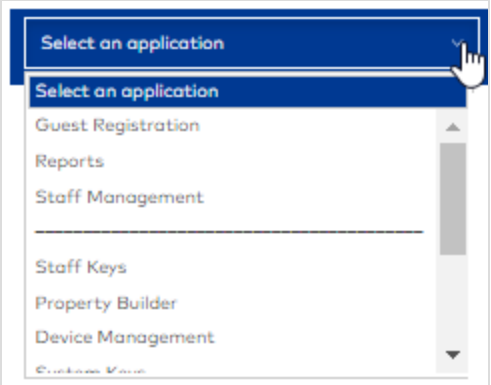
Navigating Ambiance

Ambiance 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 Ambiance toolbar. The first three items in the list show the favorites. All other modules are listed in alphabetic order.



To navigate Ambiance 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 Ambiance toolbar.

Go to the Welcome Page or Log Out

- To go to the Ambiance welcome page, click (Home) .
- To log out of Ambiance, click ***account user name*** > **Log Out**.

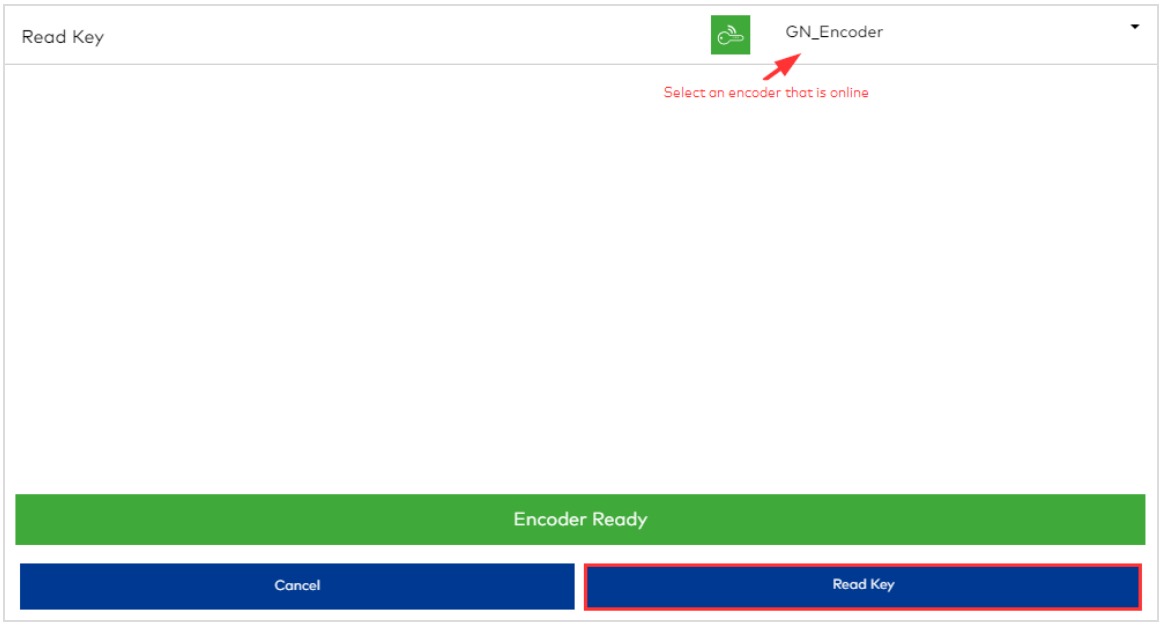
Read Key/Erase Key

Learn the status of any key by using the Ambiance key reader accessible from the main toolbar. After successfully reading a key, you can erase all Ambiance configuration data encoded on the key.

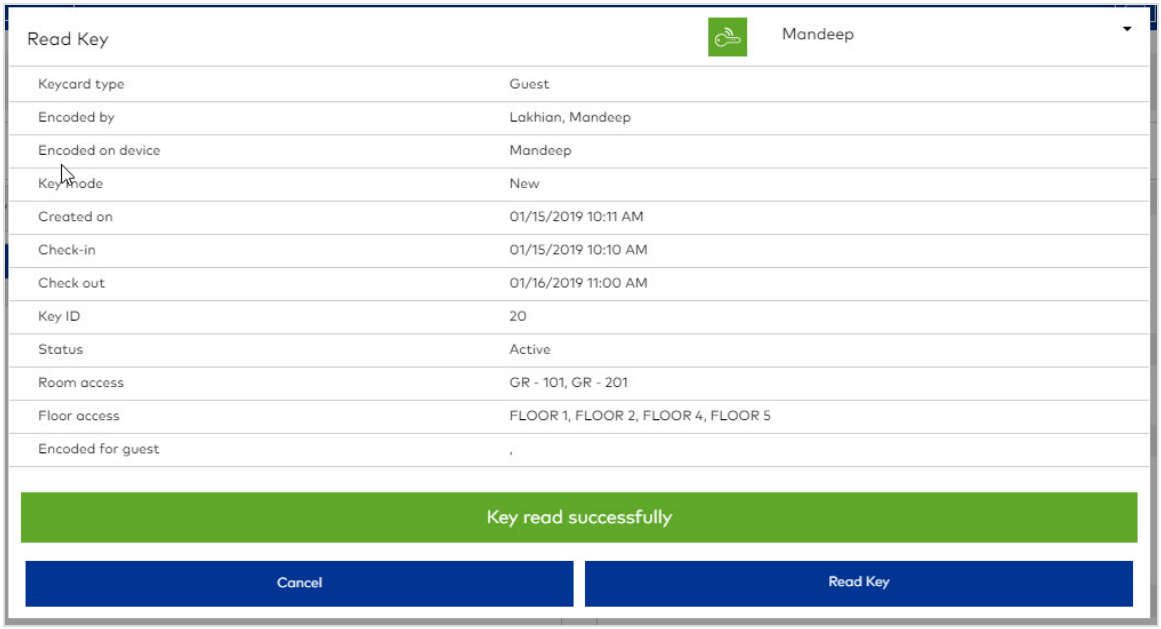
Read Key

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 Guest Keys:

- Keycard type
- Encoded by
- Encoded on device
- Key mode
- Created on
- Check-in
- Check out
- Key ID
- Status—For physical keys: Pre-registered/Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- Guest Room access
- Common area access
- Floor access
- Encoded for guest

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

You can erase any key (guest/staff/system) only directly after the key is read.

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.

View Notifications

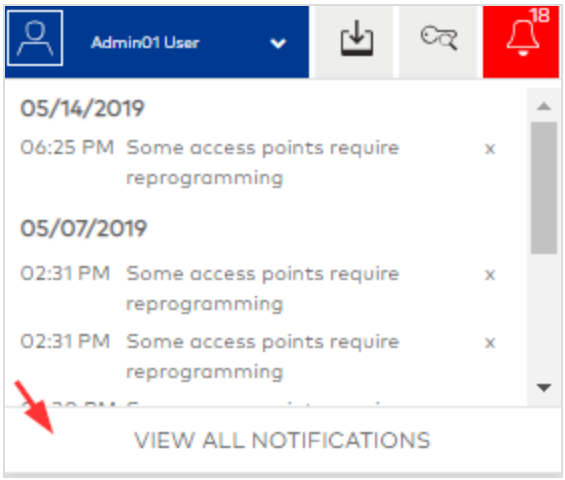
Notifications keep staff members informed about operations and events related to remote lock management (hubs and paired access points). For example, a notification lets you know when a guest key is used or a door is ajar.

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.

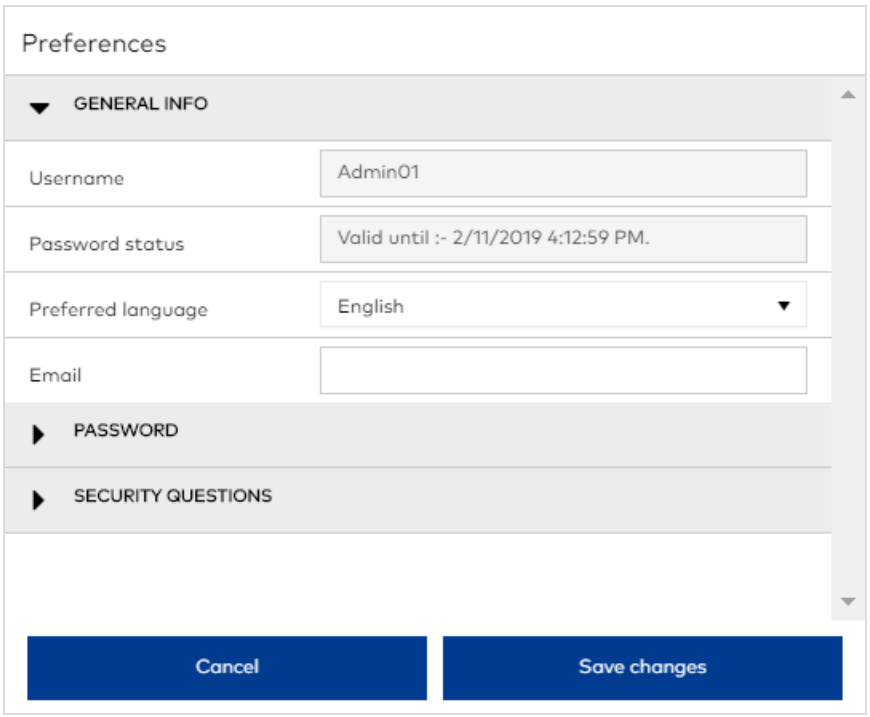
Use the Notifications toolbar to search notifications and take any of the following actions:

- 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)  .

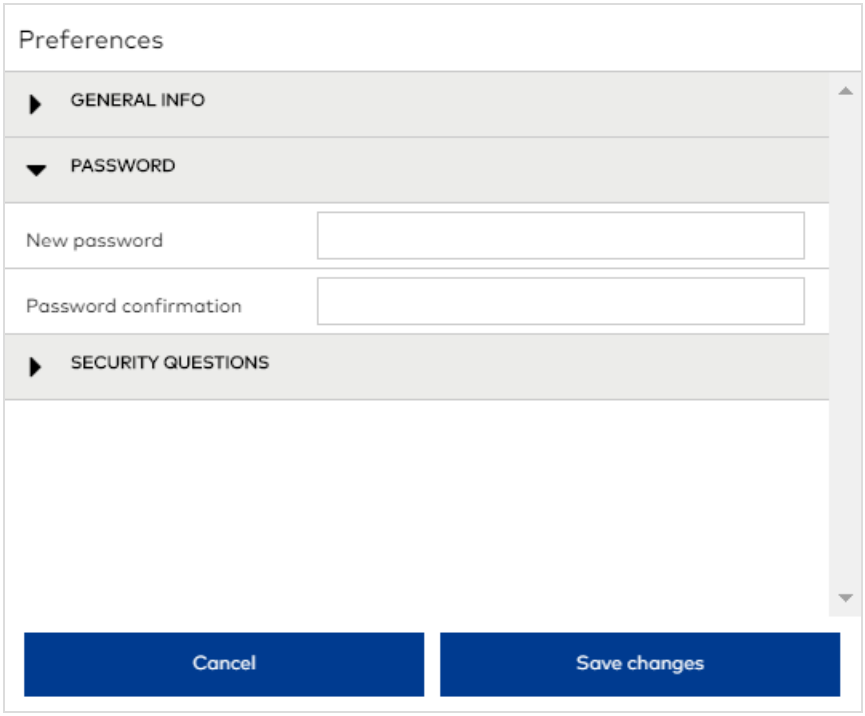
Set Account Preferences

To set account preferences:

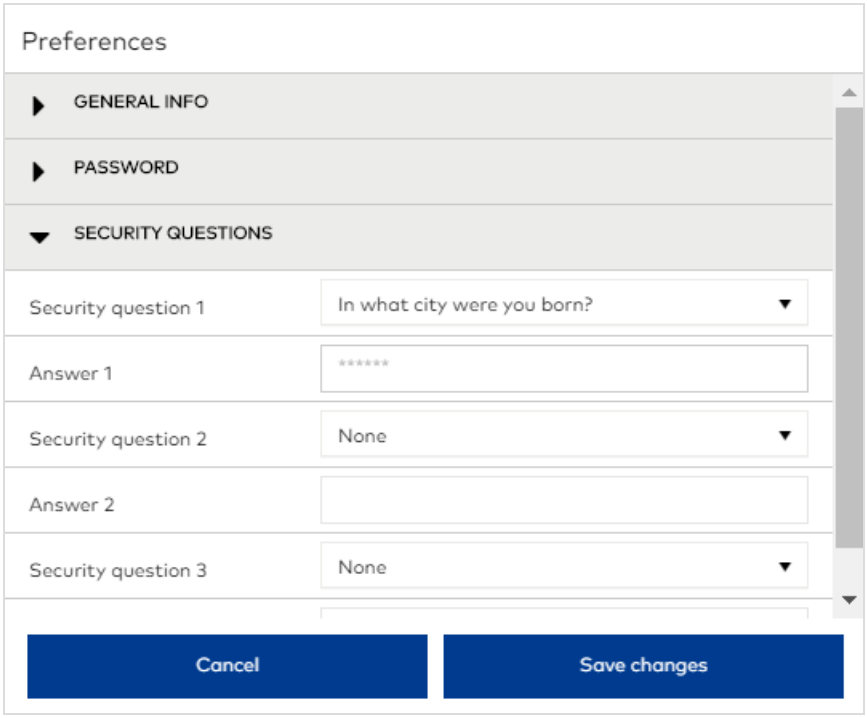
1. On the main toolbar, click ***account user name*** > **Preferences**. The user name and password status display. Note the expiration details for the Ambiance account password.



2. Select the preferred language for the account holder.
3. Specify an email address to associate with the account. Ambiance sends automated emails regarding account status to the specified email. The email address specified in the Operator profile is linked with the email address in account Preferences.



4. Open the Password section to change the Ambiance account password.



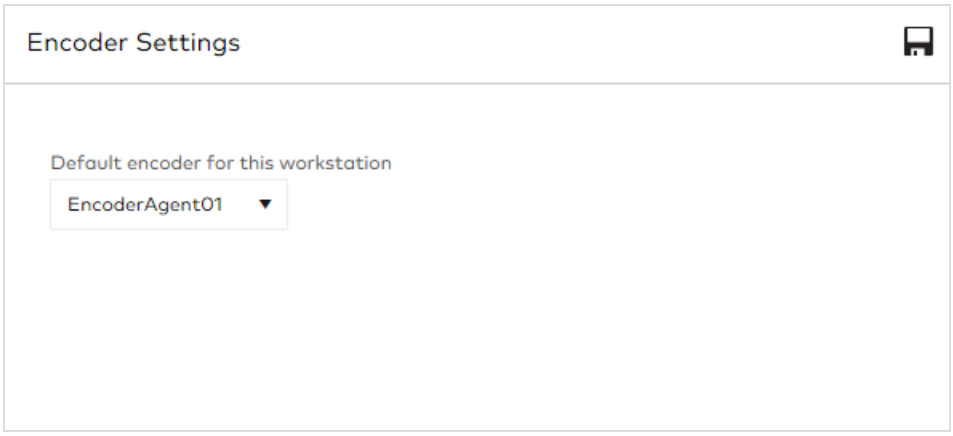
5. Open the Security Questions section to select and provide responses to the challenge questions when required to submit a request to retrieve or reset the password.
6. Click **Save changes**. After saving the preferences, the screen refreshes in the selected language.

Select Default Encoder

You can set the default encoder in the System Settings module or from the Set Default Encoder dialog accessible from the main Ambiance toolbar in modules where you make keys. At key-making time, you can always select any encoder that is online and available to the workstation.

Set the default encoder in System Settings

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

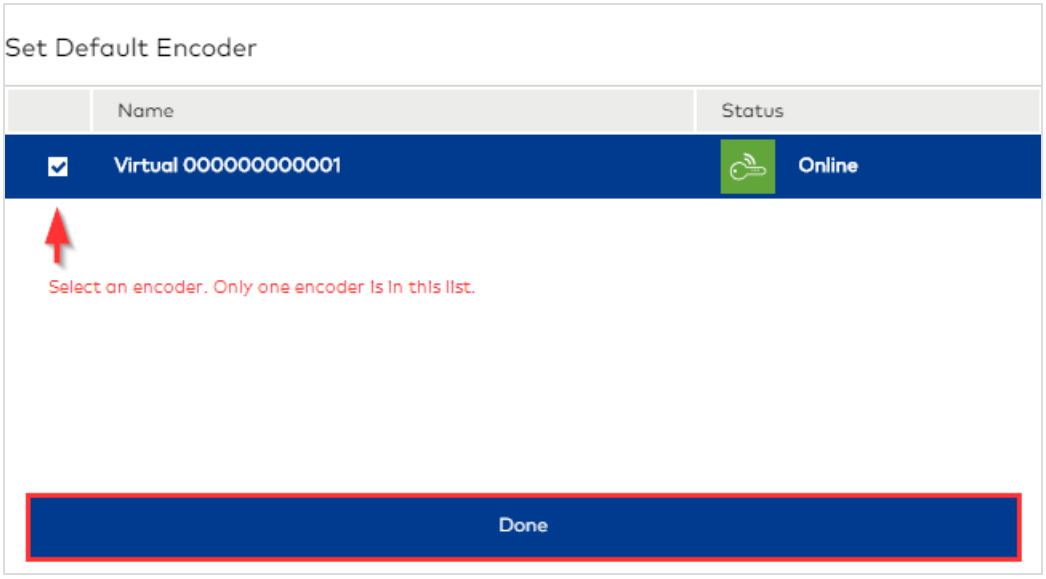


3. Select the encoder to automatically populate when making keys. If you do not select a default encoder, you can select an encoder at key-making time. Default: none.
4. Click (Save) .

Set the default encoder in the Set Default Encoder dialog

1. Go to any module in which keys are made (Guest Registration, Staff Management, Staff Keys, System Keys).

2. Click (Encoder status)  in the main Ambiance toolbar.



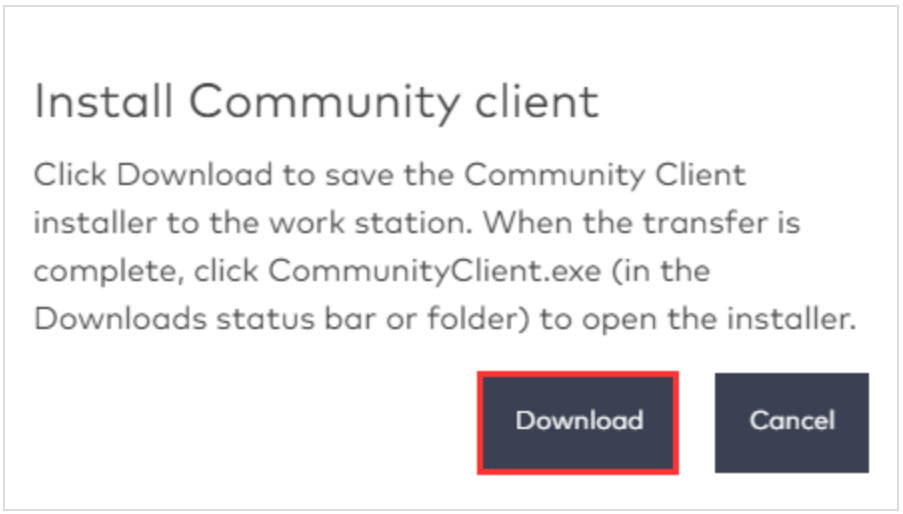
3. Select the encoder to automatically populate when making keys. If you do not select a default encoder, you can select an encoder at key-making time.
4. Click **Done.**

Update Ambiance Client

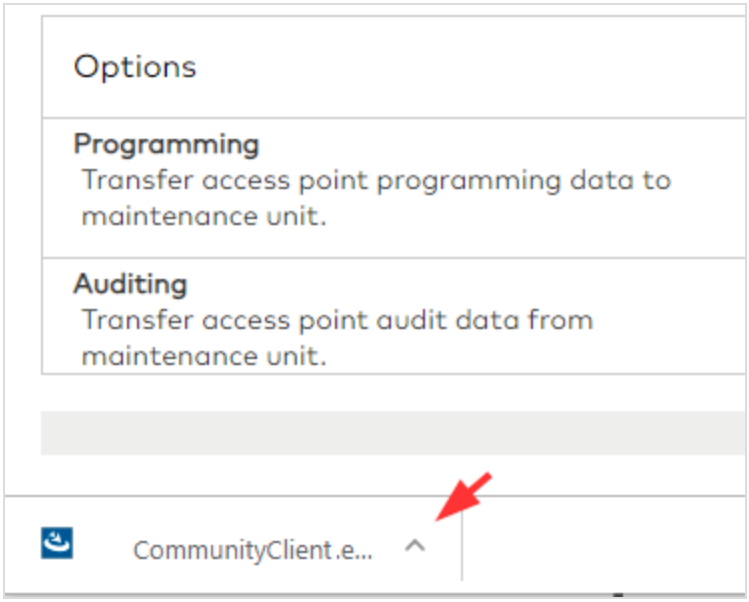
Perform the installation as a Local Administrator (not Network Administrator).

1. Go to Device Management or Programming/Auditing.

2. Click (Install Ambiance Client) .



3. Click **Download**.



4. When the download is complete, click **AmbianceClient.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).
6. The Setup Status page displays while the Client is installed.
7. On the Update Complete page, click **Finish**.

Working with ...

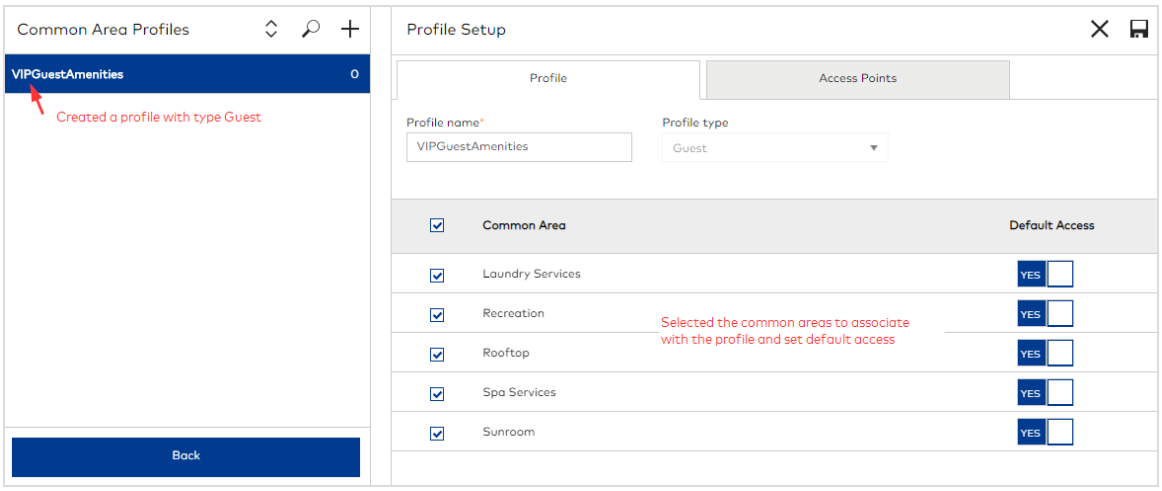
This section includes the following articles:

Common Areas

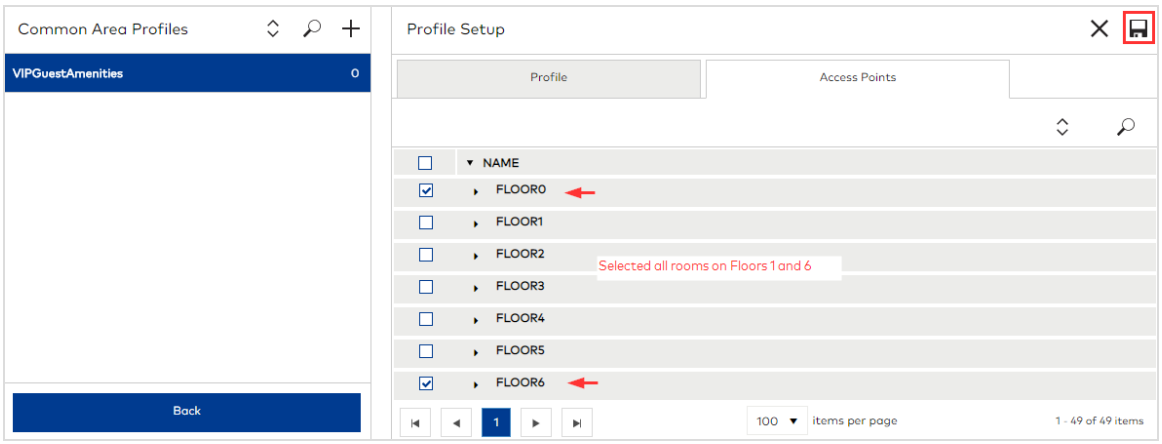
Access to limited-access common areas (amenities) requires configuration in Access Management > Common Area Access.

Guest Access

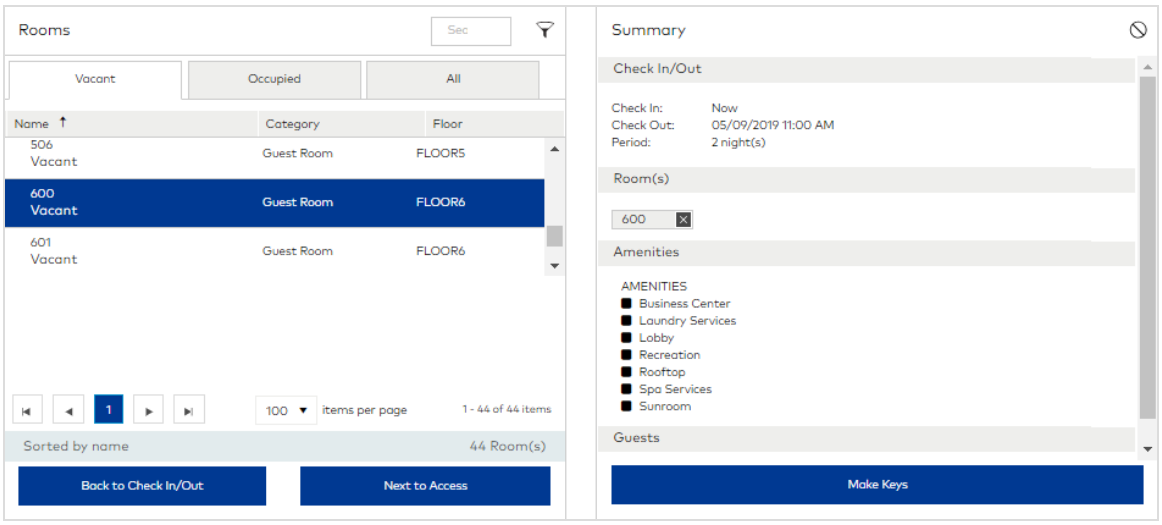
Guest access to limited common areas can be configured after adding the common areas in Property Builder. The following figure shows the VIPGuestAmenities profile with the type Guest. Five common areas are selected to associate with the profile.



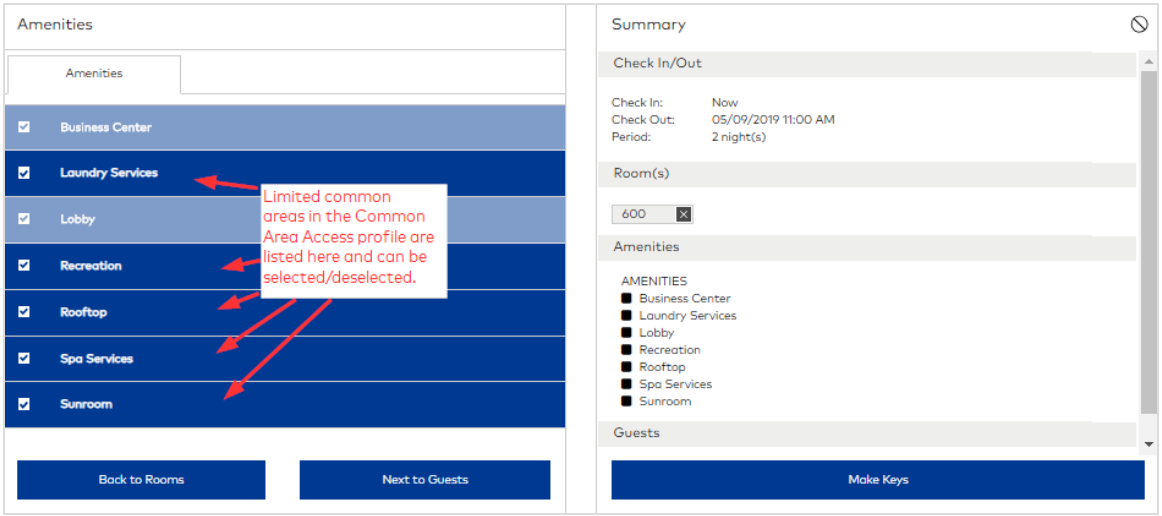
The next step is to click the Access Points tab and select the guest rooms to associate with the profile. The following figure shows that all guest rooms on floors 0 and 6 are selected.



When one of the guest rooms associated with the VIPGuestAmenities profile is assigned to a guest, the common areas are added to the guest registration. The default access is reflected but can be changed directly in the guest registration.



When you proceed to the Access menu in the guest registration, all limited common areas selected in the Common Area Access profile are listed and can be selected and deselected.

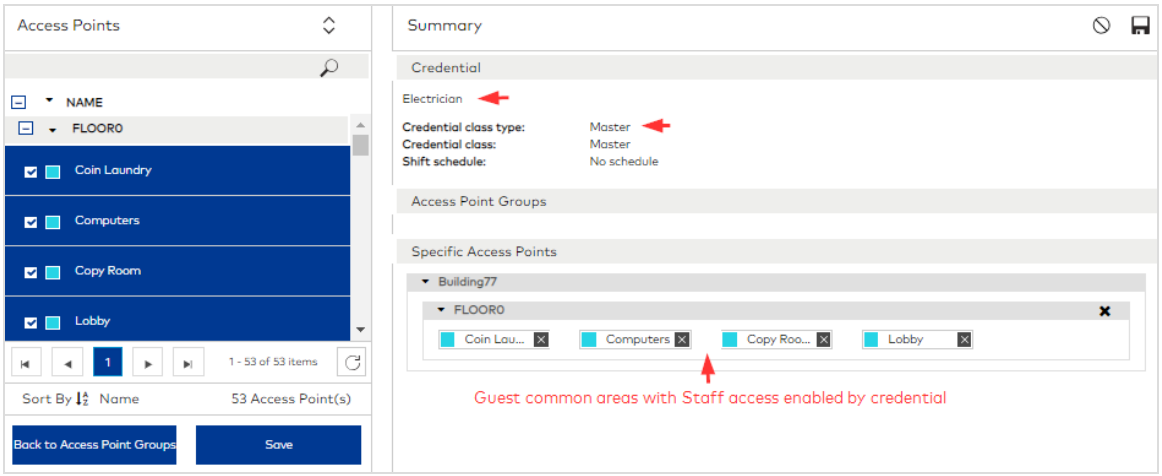


Staff Access

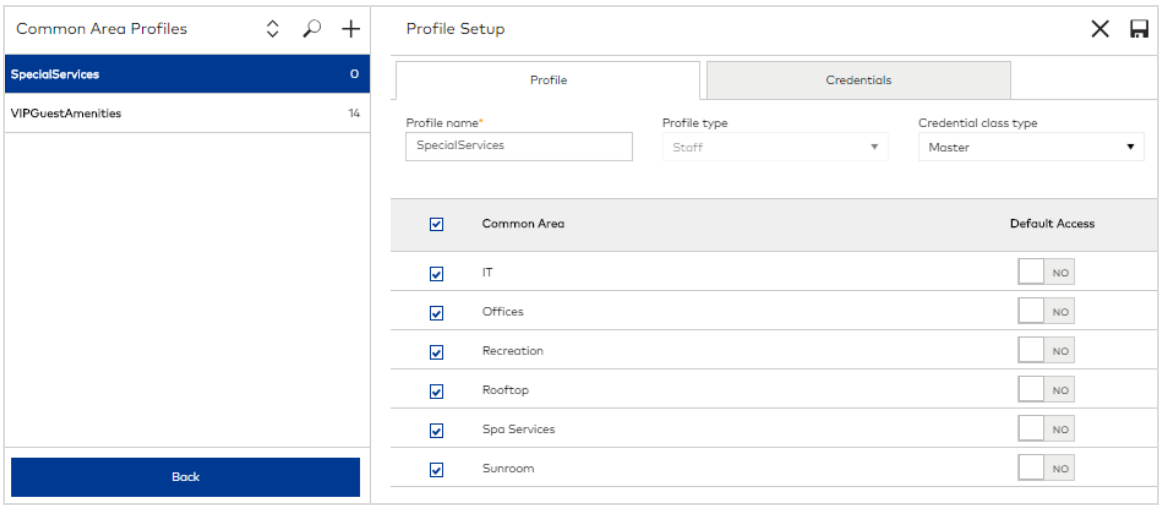
Staff access to limited common areas must be configured after adding credentials because common area access profiles are associated with a credential and not specific access points.

If you want to authorize common areas on a staff key, the profile type that you create in Common Area Access must be the same as the credential class type for the staff key. The example below shows how to make a common area access profile for a Master credential/key.

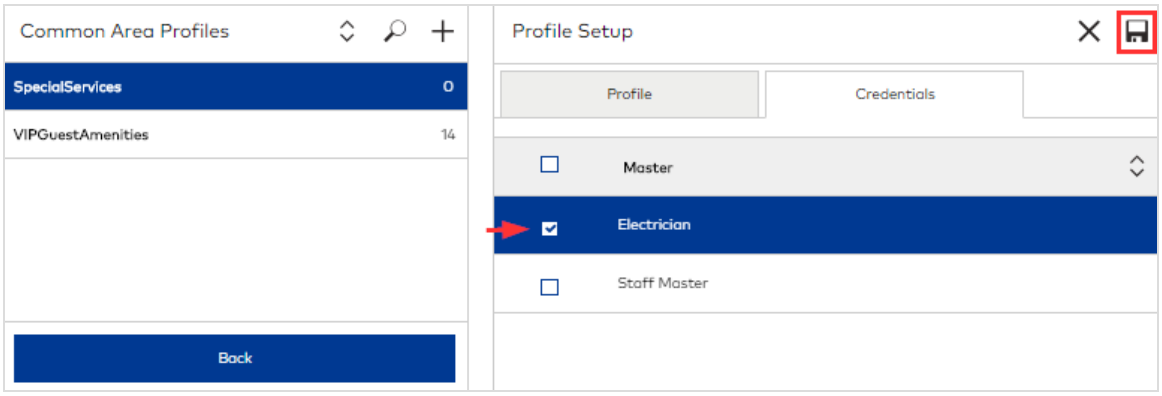
The following figure show the Electrician credential made with the Master credential class type/credential class.



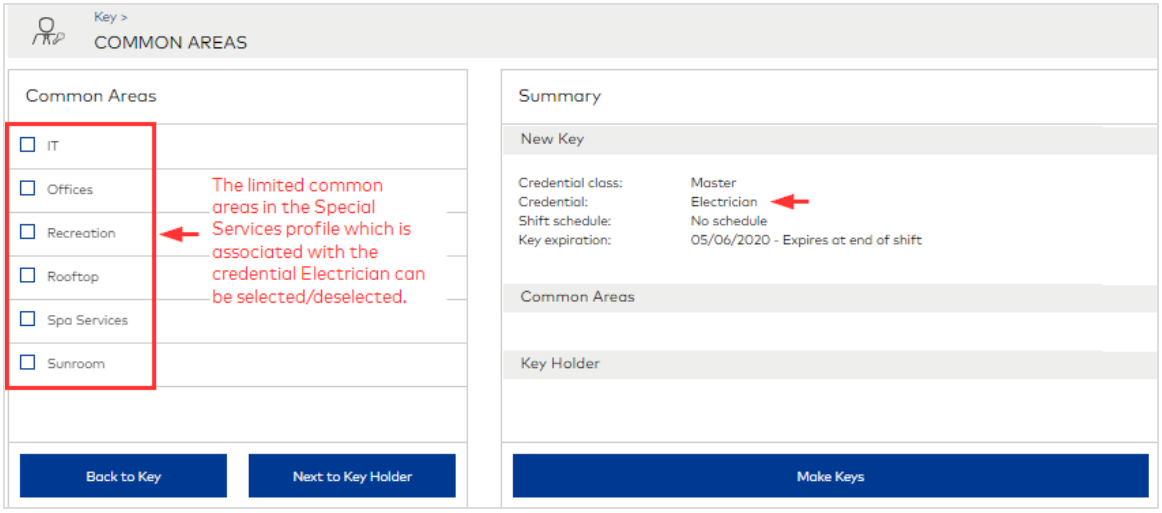
If we want the ability to add limited common areas on keys made with this credential, we create a common area access profile with the type Master. The following figure shows the Master profile with six common areas selected. Because default access is not enabled for any of the selected common areas, access must be enabled at key-making time.



Our next step is to associate the profile with one or more credentials and click Save.



When we make a key using the Electrician credential, the common areas are displayed and can be selected/deselected at key-making time.


Key >
COMMON AREAS
Common Areas
IT
Offices
Recreation
Rooftop
Spa Services
Sunroom
The limited common areas in the Special Services profile which is associated with the credential Electrician can be selected/deselected.
Back to Key
Next to Key Holder
Summary
New Key
Credential class: Master
Credential: Electrician
Shift schedule: No schedule
Key expiration: 05/06/2020 - Expires at end of shift
Common Areas
Key Holder
Make Keys

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 Guest Keys have a key mode: New or Additional. When you make the first key for a credential (a room or combination of guest rooms), 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 room 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.

Making Keys

Making 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 guest. 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.

Key Status

The following key statuses are used in Ambiance:

- Pre-registered—Keys that have been made but are not yet valid (due to pre-registrations).
- Active—Keys that are valid and available for use.

> Failsafe Keys always display the status Active.

- Expired—Keys that are invalid because the expiration date arrived.
- Returned—Keys that have been erased.
- Obsolete—Keys that are invalid because a New Key with the same credential was made.

Mobile Keys

Mobile keys work with your mobile application to offer guests 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

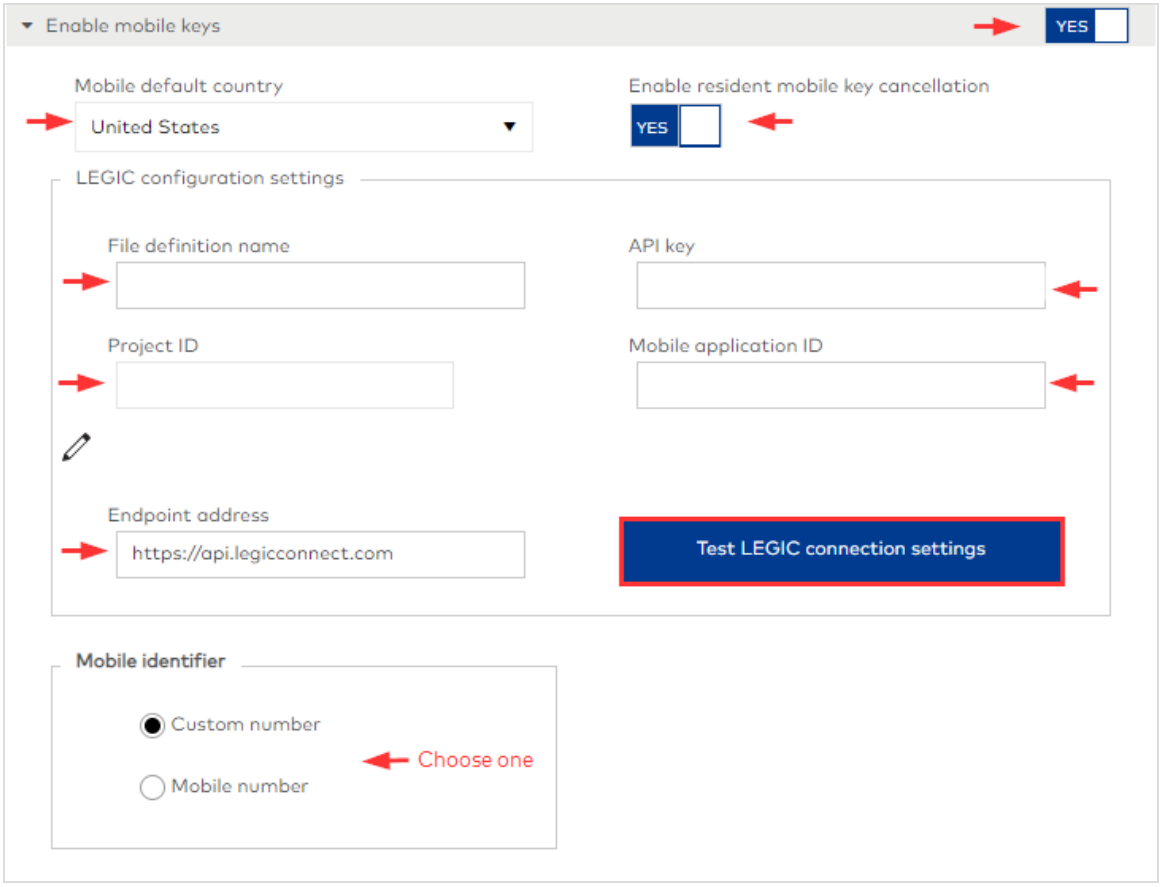
The requirements to use the feature are straightforward:

- Mobile keys must be enabled in **System Settings** > **Advanced Settings**.
- The guest profile must include a valid mobile or custom number.
- Guests must download, install and register their mobile number with your mobile application.

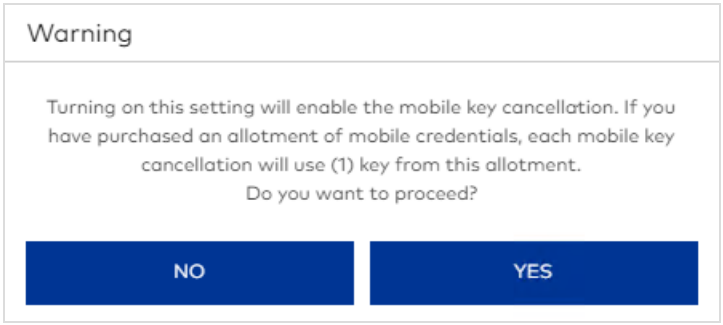
Enable Mobile Keys

To enable and configure mobile keys:

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



3. Set the **Enable mobile keys** switch to **YES**.
4. For **Mobile default country**, select the default country for mobile numbers. The corresponding country code is retrieved for the mobile number.
5. If you want the ability to cancel mobile keys, set the **Enable guest 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.



6. For **LEGIC configuration settings**, a dormakaba Customer Service technician provides valid values.

Mobile-Enabled Access Points

When mobile keys are enabled in System Settings, the option **Enabled for mobile keys** is available when creating and editing access points. Although the option is strictly informational, it is required to include an access point in the file download of mobile-enabled access points from the Property Builder *Buildings* menu.

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, the status in Ambiance indicates whether the guest has registered their mobile phone number:

- **Delivering - Mobile registered**—Keys that are in the process of being delivered. Ambiance detects the mobile device is registered with your mobile application.
- **Delivering - Mobile not registered)**—Keys that are in the process of being delivered. Ambiance cannot detect the mobile device.

When the status of the key is **Delivered**, guests can use the mobile key by opening your mobile application and following the screen prompts. (If the key is never delivered, the status displays **Failed**.)

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 have reached expiration also remains **Delivered**.

dormakaba BlueSky Installation

The BlueSky app is free and consumes 44.6 MB. During installation, guests may receive the following prompts:

- **Allow notifications**—The selected response does not affect the operation of mobile keys.
- **Make data available to Bluetooth devices**—Guests must select **OK** because the mobile app communicates with locks using Bluetooth technology.
- **Country**—Guests must select the country associated with the mobile phone number. Upon selection, the country code is populated.
- **Mobile phone number**—Guests must specify the complete phone number including any regional or area codes.
- **Privacy Policy**—Guests must accept the private policy.
- **Share usage patterns**—The selected response does not affect the operation of mobile keys.

Keyscan Aurora

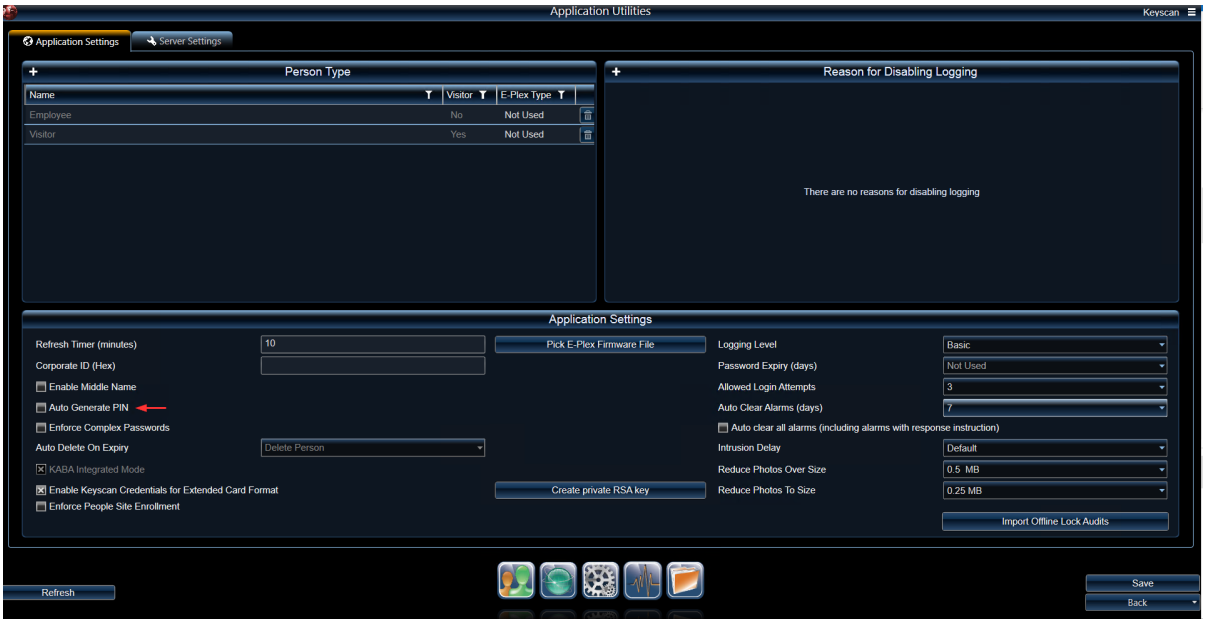
Ambiance™ integrates with Keyscan© Aurora to offer a centralized access management system for sites that use Keyscan devices to control access to common areas.

Step 1: Install and Configure Keyscan Aurora

Install and configure Keyscan Aurora. For requirements and instructions, refer to Keyscan documentation on the dormakaba website. This is a prerequisite because Aurora Access Groups must be configured before integrating with Ambiance.

To ensure that all access points are synchronized, configure Aurora PIN settings:

1. Log in to Keyscan Aurora.
2. Select Application Management > Application Utilities.
3. Verify the **Auto Generate PIN** option is disabled.
4. Save your changes.



Step 2: Enable Aurora Integration

> The Ambiance Server and Client must be installed to perform this step.

The first step after Keyscan Aurora is installed and the Aurora Access Groups are configured is to enable Aurora integration in Ambiance. This step establishes a connection between the Ambiance Server and the Aurora Server.

To enable Aurora integration:

1. Go to **Systems Settings** > **Advanced Settings**.
2. For the option **Enable Aurora Integration**, set the switch to **YES**.
3. Specify the IP address or server name of the Aurora server. Dynamic and static IPs are supported. If you specify a server name, DNS must be configured.
4. Specify valid credentials to access the Aurora server. Optionally, click **Test Connection** to verify the connection.
5. Click (Save).

Upon saving connection details, Ambiance tests the connection. If successful, Ambiance enables the **Aurora Access Groups** tab for common areas in Property Builder. The tab does not display unless Aurora integration is enabled.

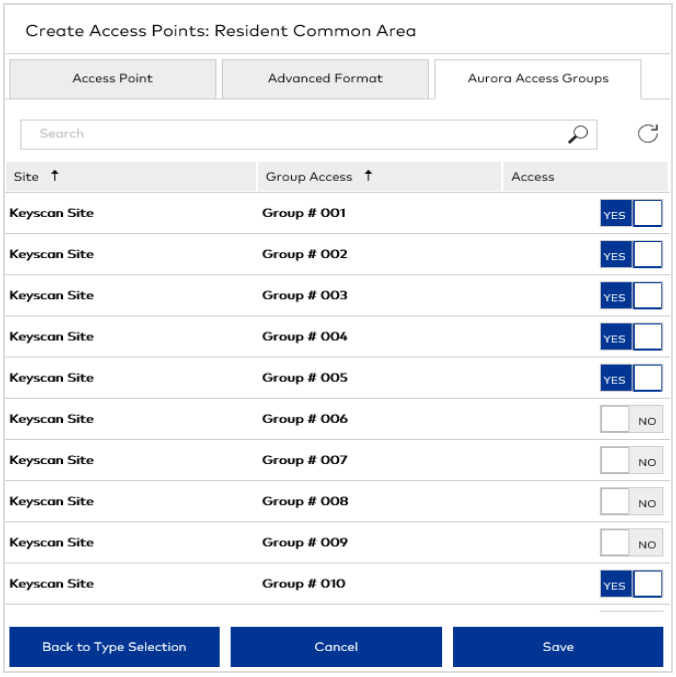
Next step: Configure common areas.

Step 3: Configure Common Areas

After Aurora integration is enabled, go to Property Builder and configure guest and staff common areas for Aurora Access Groups.

Configuring Common Areas During Initial Deployment

If this is the initial deployment of Ambiance, this step involves creating guest and staff common area access points. When you add a Guest Common Area (or Staff Common Area), the **Aurora Access Groups** tab displays.

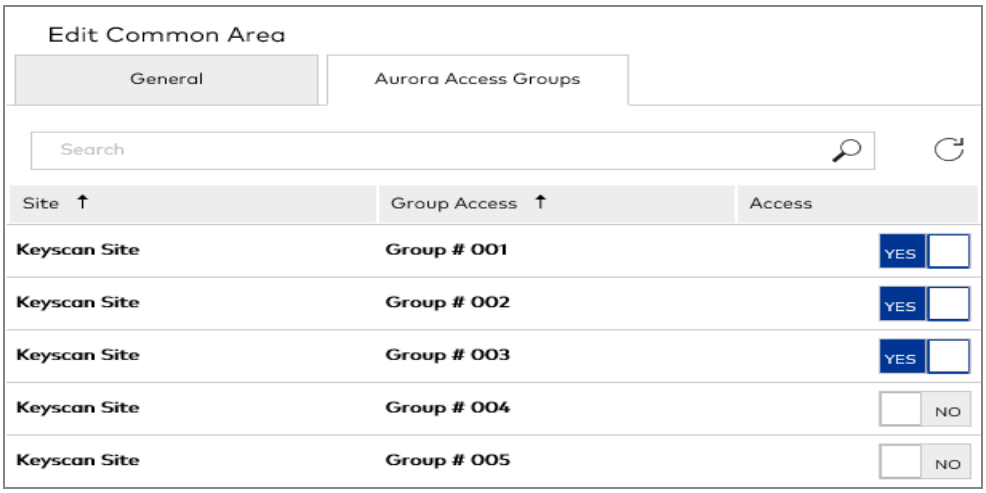


Use the switch to enable or disable access for each Keyscan Aurora site and group. You can search for access groups by name and sort the list by site or access group. You can also refresh the list to display current data from the Aurora Server.

Next step: If this is the initial deployment of Ambiance or if no keys have yet been made, your work is done. When you make keys that include access to common areas, Ambiance automatically synchronizes key information with the Aurora Server.

Configuring Common Areas Post-Deployment

If you are integrating Aurora after the initial Ambiance deployment, this step involves editing existing guest and staff common areas.



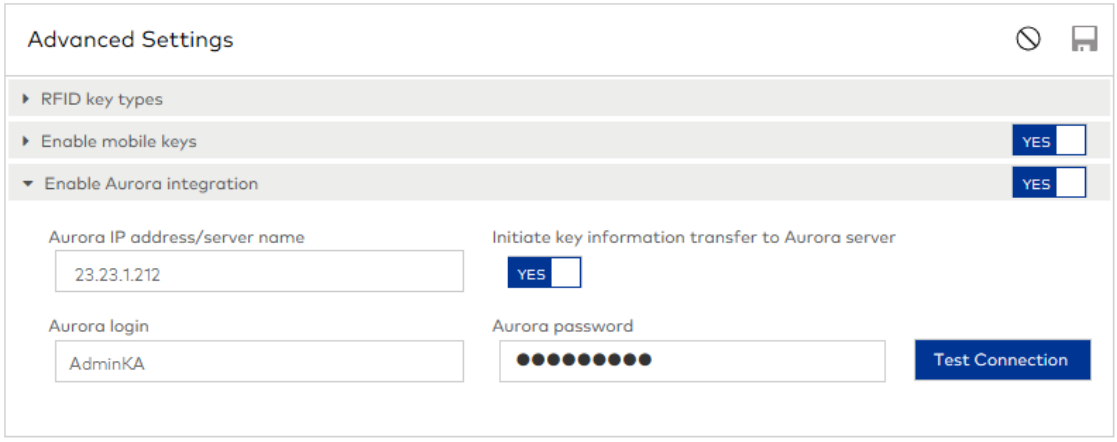
On the **Aurora Access Groups** tab, use the switch to enable or disable access for each Keyscan Aurora site and group. You can search for access groups by name and sort the list by site or access group. You can also refresh the list to display current data from the Aurora Server.

Next step: If you are integrating Aurora after the initial Ambiance deployment and keys have been made, you must manually initiate the data synchronization.

Step 4: Synchronize Ambiance with Aurora

This step only applies when Aurora is integrated with Ambiance after the initial deployment of Ambiance and keys have already been made. Because the changes to common area configurations affect existing keys, you must manually initiate data synchronization to update key information on the Aurora Server.

⚠ Before initiating the key information transfer, ensure that Aurora Access Group configuration for all guest and staff common areas is complete. If you initiate the process before completing the configuration, affected keys will provide partial access.



To initiate data synchronization:

1. Go to **Systems Settings** > **Advanced Settings** > **Enable Aurora Integration**.
2. For the option **Initiate key information transfer to Aurora server**, set the switch to **YES**. A warning displays reminding you that all access group configurations for common areas should be complete before proceeding.
3. Click **YES** to proceed.

The synchronization process starts and continues until complete. When the process is complete, the switch returns to the default state (**NO**). Ordinarily, this step is not required again because key information for all future keys is automatically sent to Aurora. However, if the synchronization is initiated before Aurora Access Group configuration for common areas is complete, you must monitor the synchronization process and re-initiate when the option is available.

> The best practice is to start the process during a time when existing keys are least likely to be used. Depending on the number of existing active keys, the synchronization process may take a few hours. During this time, access group configuration data for affected keys may provide partial access.

Remote Lock Management

Deployment of remote lock management involves configuring hubs to work with the Ambiance Server. Hubs are the network devices used to connect the access point configuration data in Ambiance to the locks installed at access points. When a hub is listed in Device Management and the connectivity status is Online, access points can be paired. Multiple hubs can be connected to Ambiance, but an access point can be paired with only one hub.

After configuration is complete, remote commands can be sent to hubs 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 remote lock management.

This article includes the following topics:

Enable and Configure Remote Lock Management

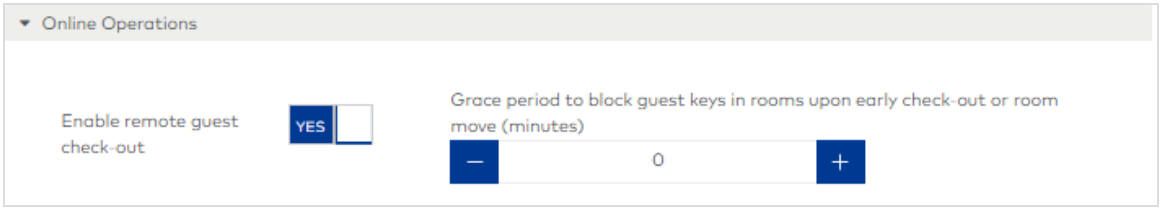
Enable remote lock management and configure online communication in System Settings.

To enable Remote Lock Management:

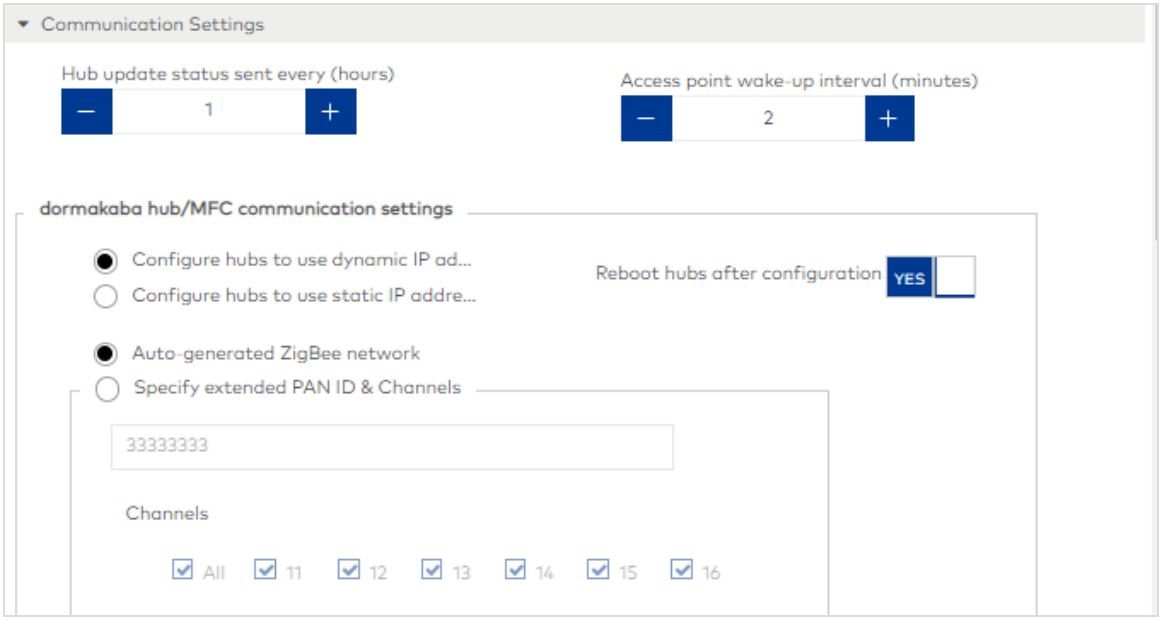
» Go to System Settings > Advanced > Enable remote lock management and set the soft-switch to YES.

After enabling remote lock management, the Online Communication category displays.

1. Go to System Settings > Online Communication.

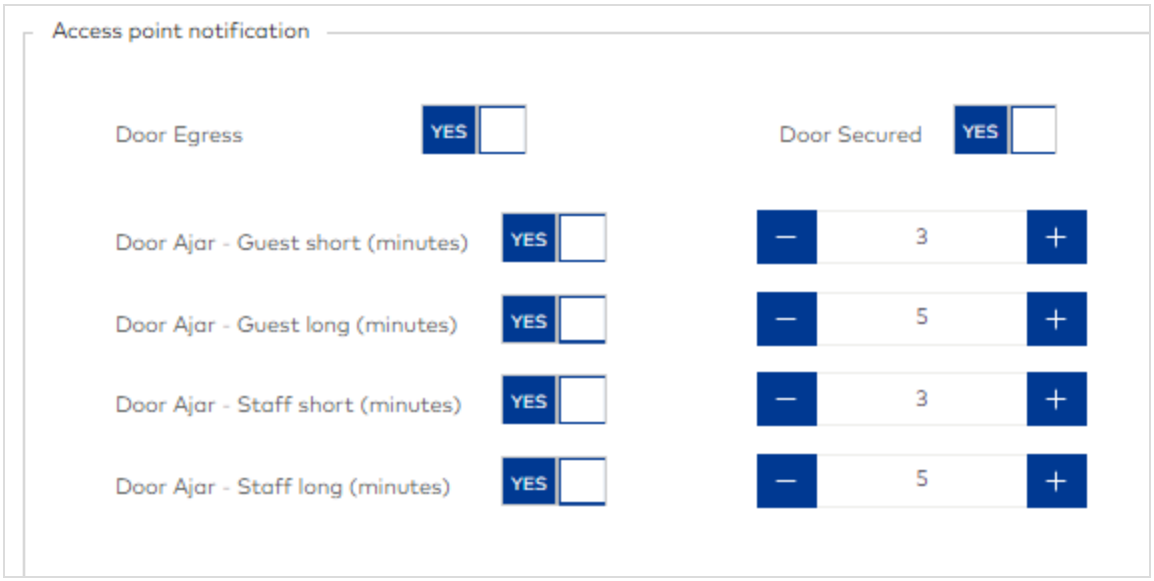


2. Set Enable guest check-out to YES. This allows you to check out guests remotely in Guest Registration. Default: YES.
3. Specify the number of minutes that guest keys remain valid after changes have been made to a guest registration and the keys are updated remotely. For example, if you changed the room assignment for a guest, access to the new room begins as soon as the keys are updated remotely, but access to the original room is not canceled until the number of minutes specified as the grace period is reached. Default: 5.



4. Configure the following communication settings:
   - Hub update status sent every—Specify the frequency to update hub status. Valid values: 1-255. Default: 1.
   - Access point wake-up interval—Specify the frequency at which access points verify if the paired hub has received remote operation requests. Default: 2.
   - Reboot Hub Immediately—Select whether a hub restarts after the **Set communication settings** command has been sent to the hub in Device Management > Hubs & Paired Access Points.
   - Configure hubs to use dynamic IP addresses (DHCP)—If enabled, hubs resolve their own IP address. A DHCP server is required for this option.
   - Configure hubs to use static IP addresses—If enabled, each hub must be configured with a unique IP address.
   - Select whether to allow hubs to automatically generate the most appropriate ZigBee communication channels or specify a unique extended PAN (Personal Area Network) ID and select the channels for hub and access point communication. The extended PAN ID must be eight alphabetic 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.

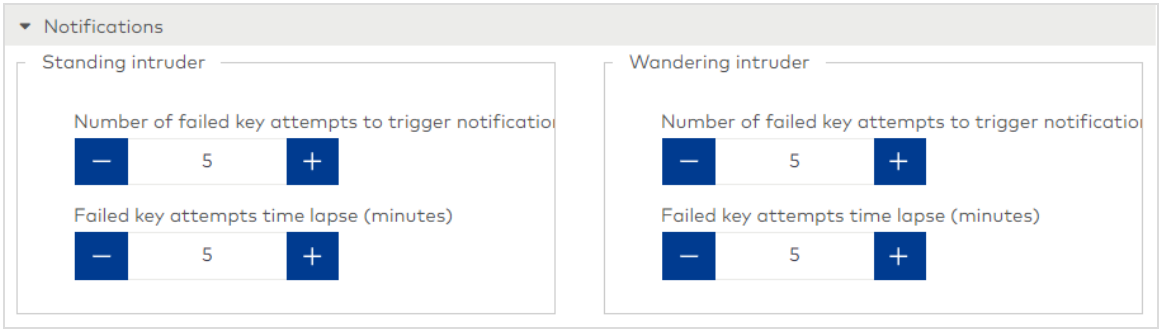
dormakaba recommends using the default auto-generated feature to allocate the required channels automatically.



5. Select the access point notifications that you want to receive:
   - 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 - Guest short (minutes)—Select YES to send a notification that a door has been left open by a guest for a short period of time, for example the time it would take to vacate a room. Specify the number of minutes after which the notification is sent.
   - Door Ajar- Guest long (minutes)—Select YES to send a notification that a door has been left open by a guest for a longer period of time, indicating an usual state or potential intrusion. Specify the number of minutes after which the notification is sent.
   - Door Ajar - Staff short (minutes)—Select YES to send a notification that a door has been left open by a staff member for a short period of time, 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 long (minutes)—Select YES to send a notification that a door has been left open by a staff member for a longer period of time, 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.



6. Configure intruder alert notifications. 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.

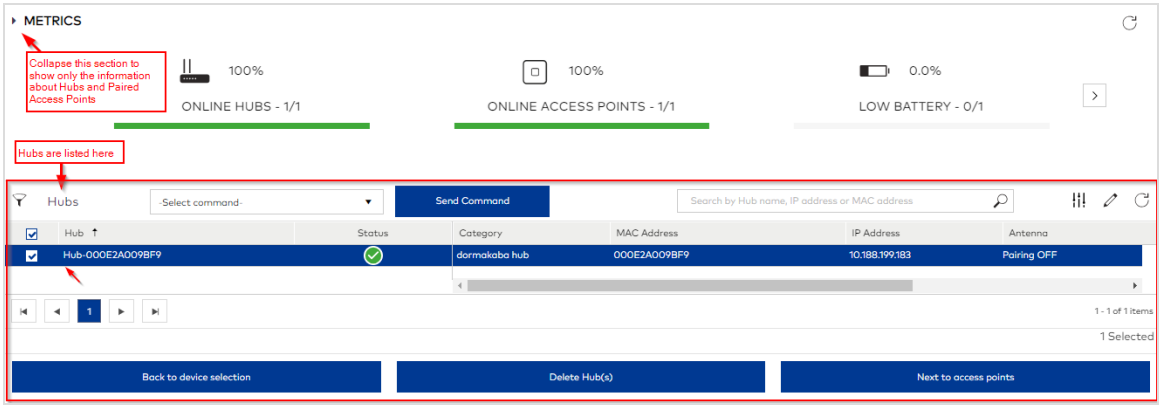
- Failed key attempts time lapse—Specify the number of minutes within which the number of failed key attempts (at different access points) must occur before a notification is triggered. Default: 5. Valid values: 1-10.

7. Click (Save).

Hubs

To view the list of hubs connected to the Ambiance Server:

1. Go to Device Management.
2. Click **Hubs & Paired Access Points**.



Hubs and their respective status' are listed by name beneath the metrics section. Color codes reflect the hub state. Green indicates no attention is required. Yellow indicates the situation may require attention. Red indicates the hub is offline or not working properly.

Use the Hubs toolbar to issued commands, search hubs (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.
  - 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—Hub antenna states (Disabled/Pairing On/Pairing Off).

  - Last communication—The date and time of the most recent and successful communication with the hub.
  - FW Vers. AVR/FW Vers. Hub/FW Vers. Ember—ZigBee RF board firmware version.

- To refresh the data, click (Refresh) .

Edit Hub Name

1. Select a hub.
2. Click (Edit) .
3. Modify the name.
4. Click **Save**.

Delete Hub(s)

You can only delete hubs that are offline.

1. Select the hub/s that you want to delete.
2. Click **Delete Hub(s)**.
3. Click **YES** to confirm.

Issue Hub Commands

1. Select one or more hub/s.
2. Select one of the following commands:
   - Deactivate Antenna—Disables the selected hub(s) from the network and deactivates the hub antenna. When the command result is successful, the antenna status is Deactivated (in the Monitoring module).
   - Get Access Point Status—Requests the connectivity status (Online/Offline) for all paired access points.
   - Get Hub Firmware Status—Requests the hub firmware version installed on the hub.
   - Get Hub Status—Requests the hub 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).
   - Pairing ON—Enables Pairing Mode. When the command result is successful, the antenna status is Pairing On (in the Monitoring module).

> ⚠ To eliminate the risk of binding access points to the wrong hub, dormakaba strongly recommends that only one hub be in Pairing Mode at a time. After all access points are paired to a hub, send the Pairing OFF command to the hub to disable Pairing Mode.

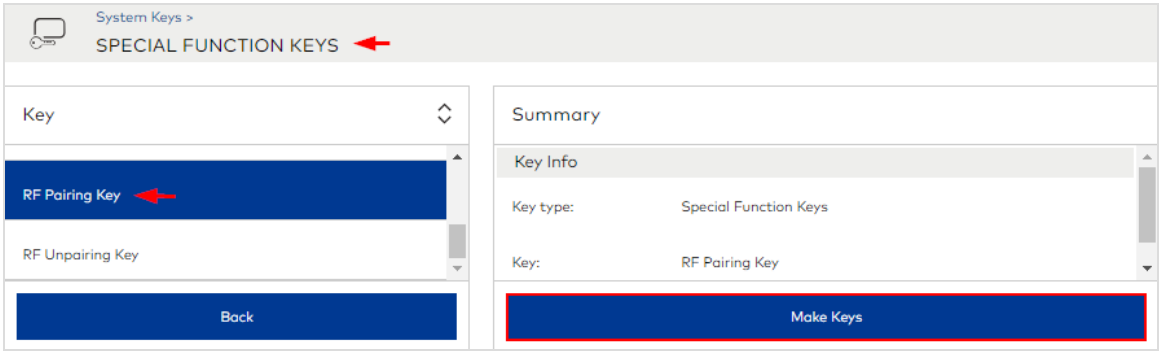
- Reset Hub—Performs a soft reset on the selected hub/s.
- Set Clock and Lock Event Mask—Sends the server time and the access point event notification settings (defined in System Settings > Online Communication > Communication Settings).
- Set Communications Settings—Sends the communication configuration settings (defined in System Settings > Online Communication > Communication Settings > Hub update status, Access point wake-up, Hub update status).
- Unpair All Access Points—Unpairs all access points.
- 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

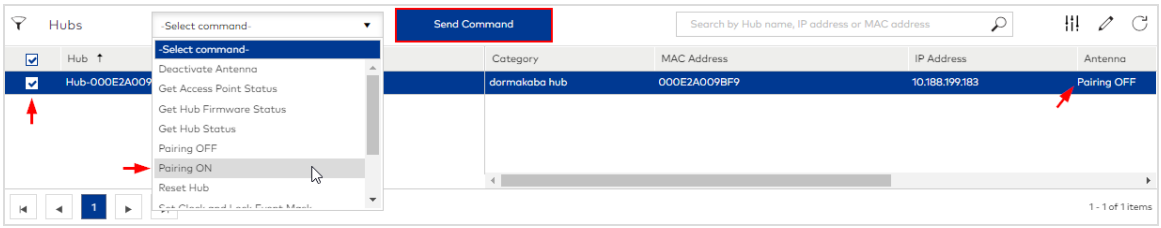


1. Go to System Keys.
2. Click **Special Function Keys**.
3. Select **RF Pairing Key**.
4. Click **Make Keys**.

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

1. Go to Device Management.
2. Click **Hubs & Paired Access Points**.
3. Select the hub where you want to pair access points.



4. Select the command **Pairing ON** (to activate the hub antenna and put the hub in Pairing Mode).
5. Click **Send Command**.
6. When notified the command is sent, click **OK**.
7. Present the RF Pairing Key to every access point that you want to pair to the hub.

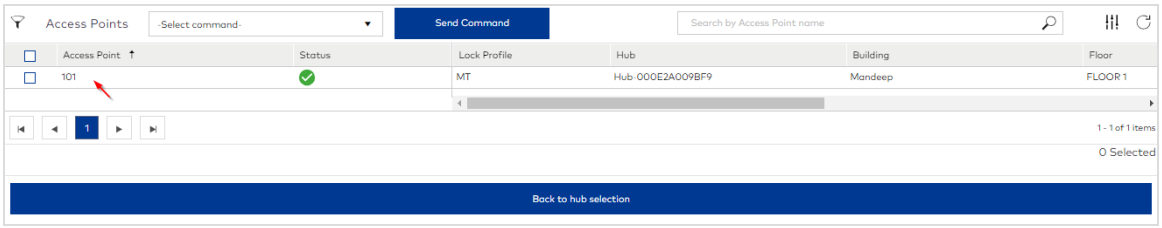
> ⚠ To eliminate the risk of binding access points to the wrong hub, dormakaba strongly recommends that only one hub be in Pairing Mode at a time. After all access points are paired to a hub, send the Pairing OFF command to the hub to disable Pairing Mode.

8. In Ambiance, select the hub that is in Pairing On mode.
9. Select the command **Pairing OFF** (to deactivate the antenna and disable Pairing Mode).
10. Click **Send Command**.
11. When notified the command is sent, click **OK**.

Paired Access Points

To view the access points that are paired to a hub:

1. Go to Device Management.
2. Click **Hubs & Paired Access Points**.
3. Select the hub where the access point/s are paired.
4. Click **Next to access points**.



The access points that are paired with the selected hub and their respective status' are listed by name. Color codes reflect the state of the access point. Green indicates no attention is required. Yellow indicates the situation may require attention. Red indicates the access point is offline or not working properly.

Use the Access Points toolbar to issue commands, search access points (by name) and take the following actions:

- 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.
  - Hub—The hub 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.
- Last communication—The date and time of the most recent and successful communication with the hub.
- 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.
- 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/FW Vers. AVR/FW Vers. Ember/FW Vers. Quantum—ZigBee RF board firmware version.

- To refresh the data, click (Refresh) .

Monitoring

The Monitoring module provides current and immediate status of the devices that support remote lock management. The metrics summary provides a real-time snapshot of the hubs and paired access points on site. For example, you can see at a glance the connectivity status for all hubs and access points, 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, events and the status of all access points paired with hubs.

> Access to data in the Monitoring module is configured in Role Management. By default, the Administrator and Site Configurator roles have full access.

Remote Lock Metrics

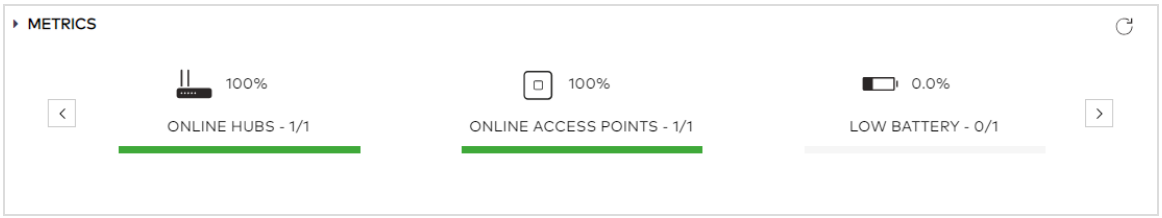
To view metrics:

In Monitoring:

» Go to Monitoring.

In Device Management:

» Go to Device Management > **Hubs & Paired Access Points**.



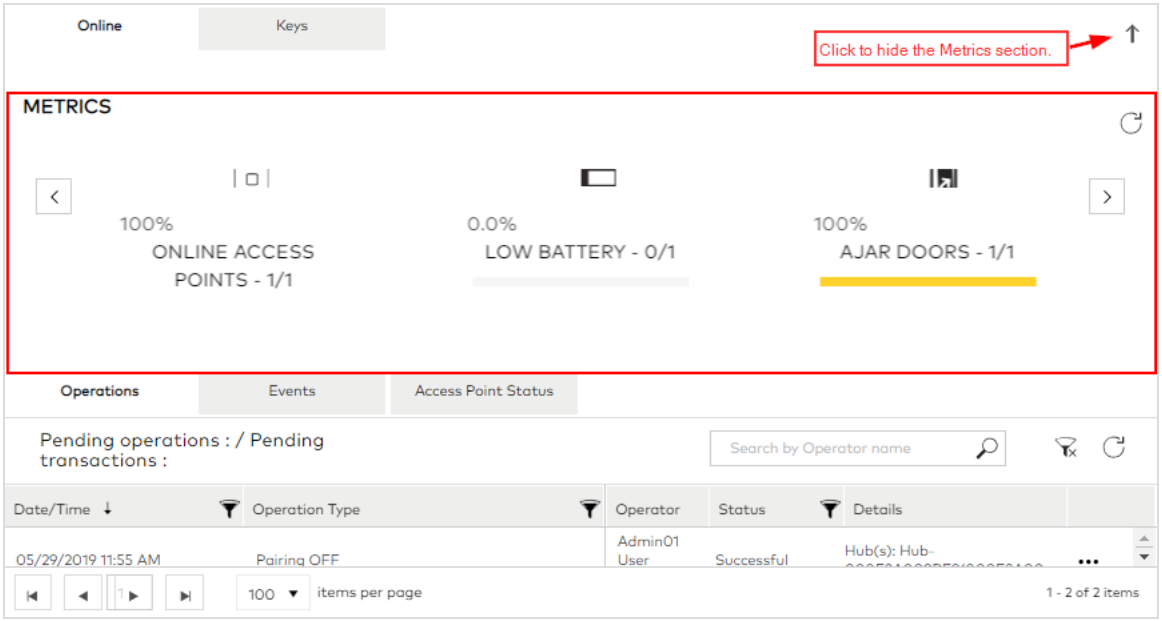
The Metrics section is expanded for view by default. Color codes reflect the state of the data. Green indicates no attention is required. Yellow indicates the situation may require attention.

- ONLINE HUBS—Percentage and total number of hubs currently online.
- ONLINE ACCESS POINTS—Percentage and total number of access points currently online.

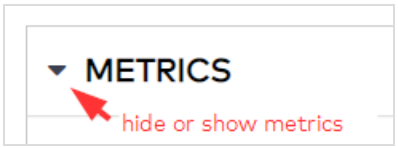
- LOW BATTERY—Percentage and number of access points with a low battery. Zero percent indicates no access points signal a low battery.
- AJAR DOORS—Percentage and number of access points with an open door.
- PRIVACY ENABLED—Percentage and number of access points with the deadbolt or privacy switch engaged.
- 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.

In Monitoring:



In Device Management:

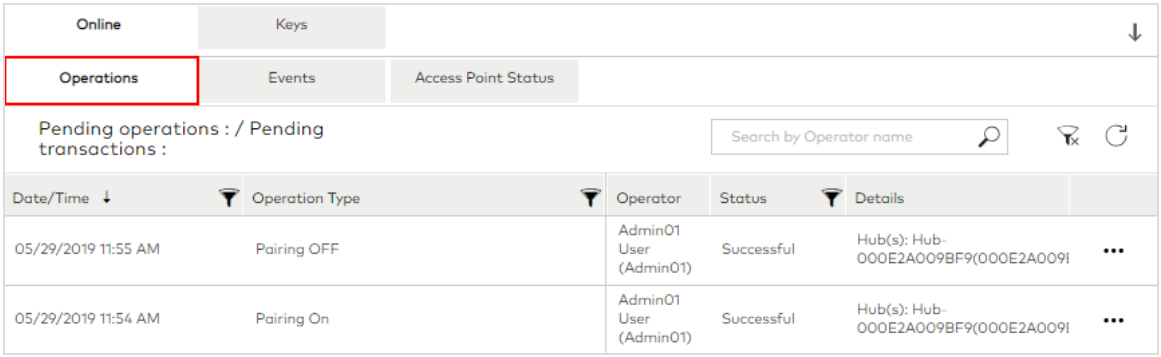


Online Operations

To view 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 hubs 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 and user 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.

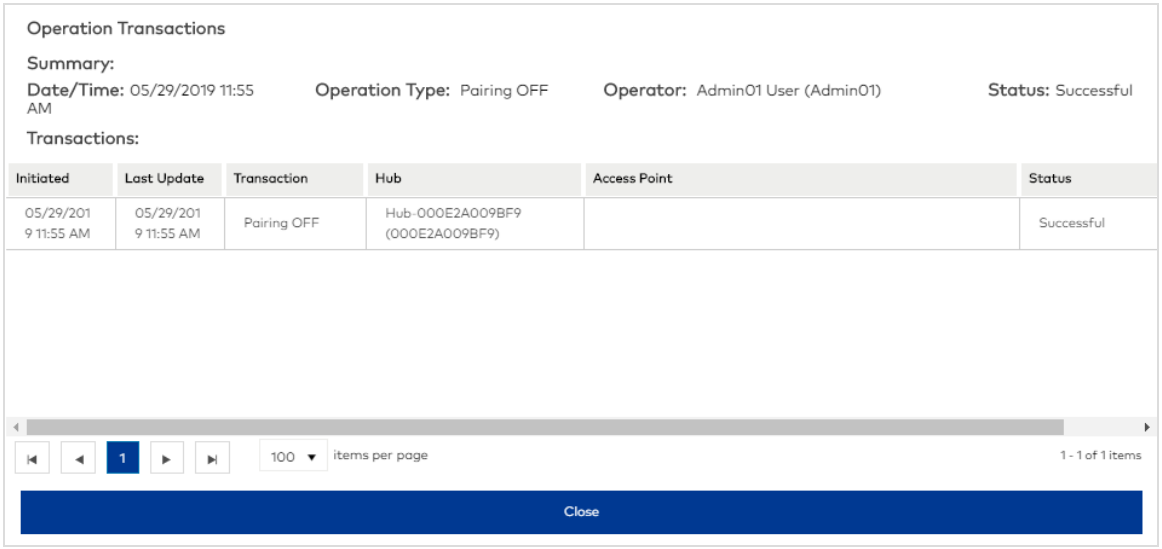
Customize the Display

- 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) ▪▪▪.



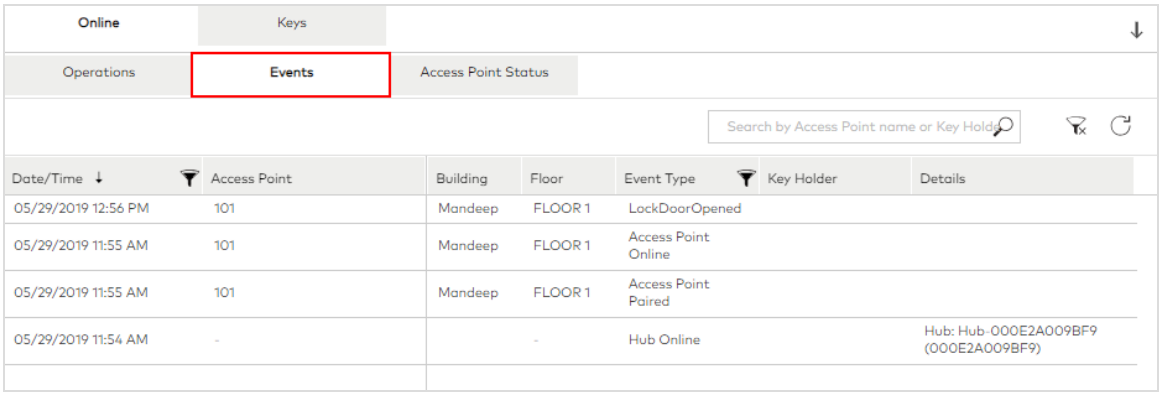
In addition to the information in the Operations list, the following transaction details are displayed:

- 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).
- Hub—The hub 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.

Online Events

To view online operations:

1. Go to Monitoring.
2. Beneath the Metrics section, click the **Events** tab.



Events related to hubs and paired access points are listed. The list includes events for all key types (guest/staff/system keys) and changes to hub/access point status.

The following information is reported for each event:

- Date/Time—Date and time the event occurred. 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: Guest 1 (for guests) and Unassigned (for staff or system keys). You can search for events based on the key holder name.
- Details—More information about the event (for example, Door Ajar / Short ajar - Guest). For all key types, details include the type of key, the credential class and the credential. For keys, details include whether access was allowed or denied.

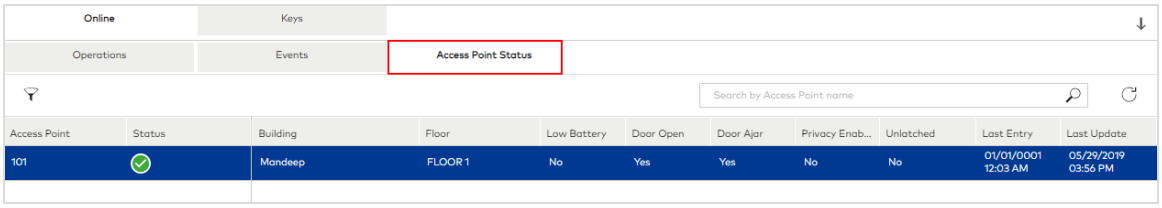
Customize the Display

- 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)  > Clear.
- To clear all filters, click (Remove Filters)  .
- Click any column to sort the list.
- To refresh data, click (Refresh)  .

Paired Access Point Status

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.
- 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.
- 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.

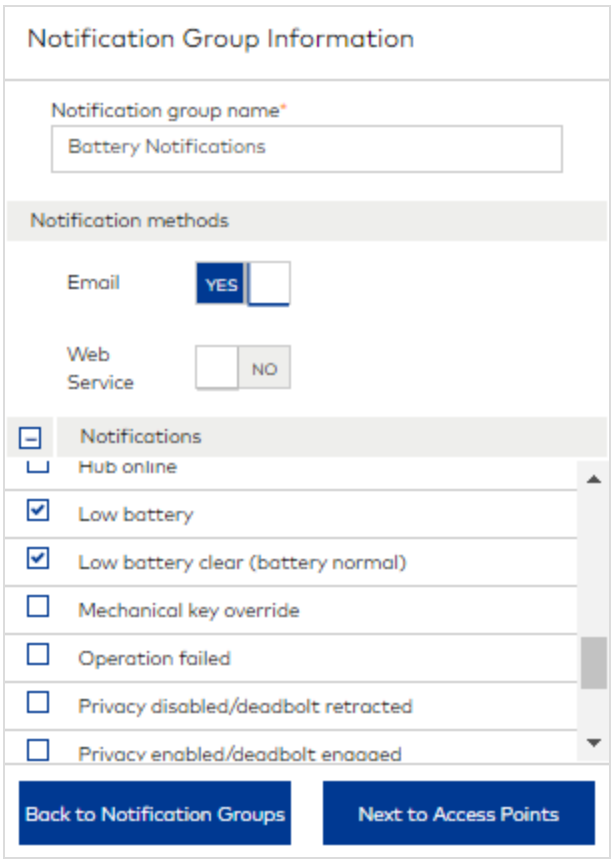
- To refresh data, click (Refresh) .

Notification Management

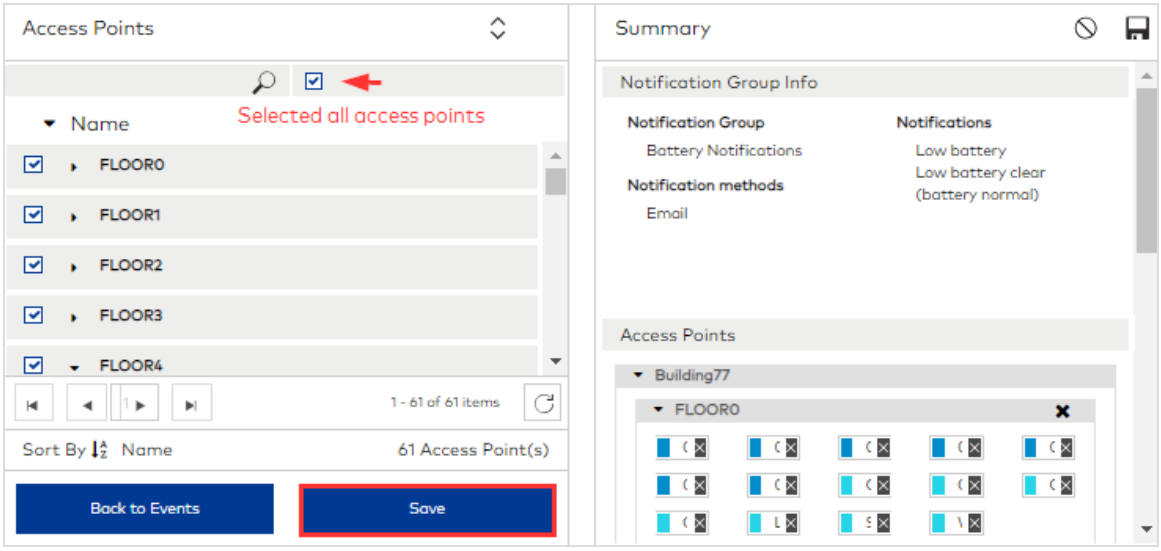
Notifications keep staff members informed about operations and events related to remote lock management (hubs and paired access points). For example, a notification lets you know when a guest key is used or a door is ajar.

To add notification groups:

1. Go to Notification Management.

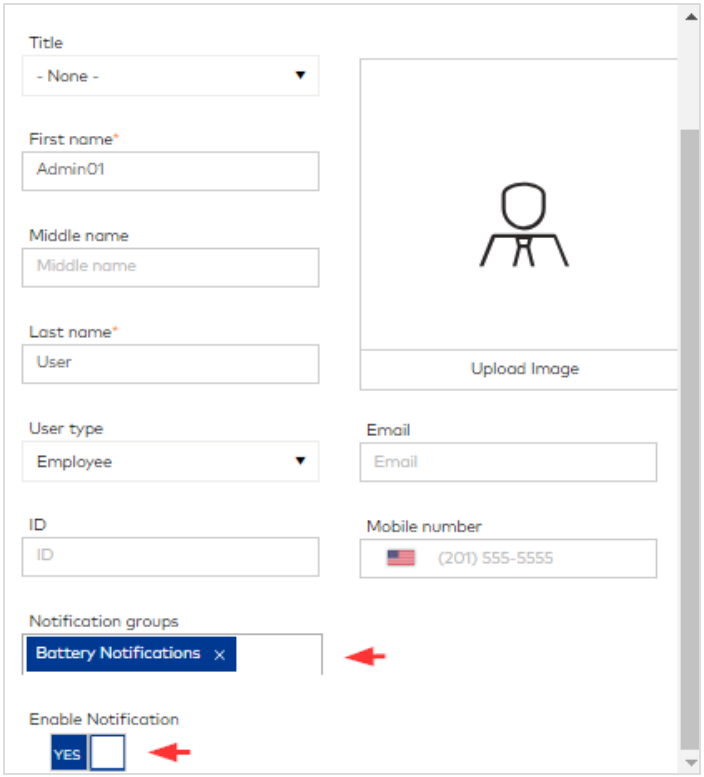


2. Click **New Notification Group**.
3. Specify a descriptive name for the group.
4. Select whether to enable Email notification. When this option is selected, staff who are subscribed to the group receive notification by email.
5. Select the notifications that you want to add to the group.
6. Click **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 profiles in Staff Management.



View Notifications

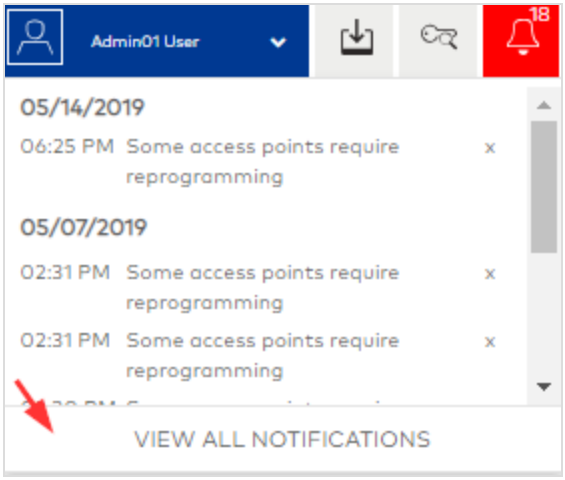
Notifications keep staff members informed about operations and events related to remote lock management (hubs and paired access points). For example, a notification lets you know when a guest key is used or a door is ajar.

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:

- Command result—The command result (Failed/Successful/Pending/Partially Successful).
- Type—The connectivity status (Online/Offline) of the hub, and if applicable, paired access points.
- Date/Time—The date and time the event occurred.
- Details—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 types to include in the list (General, Group Event/Transaction Event, None, Online, Operation Event, Statistical Event, System Event).
- Refresh the data—Click (Refresh) .

Online Reports

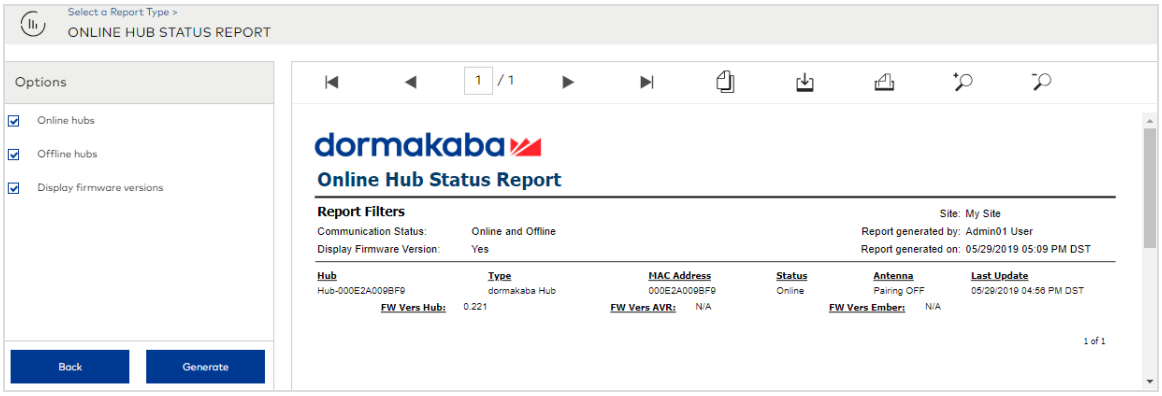
The following Ambiance reports support remote lock management:

- Online Access Point Status Report
- Online Hub Status Report
- Online Paired Access Point Status

To generate a report:

1. Go to Reports.
2. Select the report that you want to generate.
3. Select available options.
   - Connectivity status (online/offline)
   - Status options: All/Low Battery/Door Open/Door Ajar/Privacy Enabled/Unlatched.
   - Firmware versions
4. Click **Generate**.

The following figure shows a sample Online Hub Status Report.



Troubleshooting

This section includes the following articles:

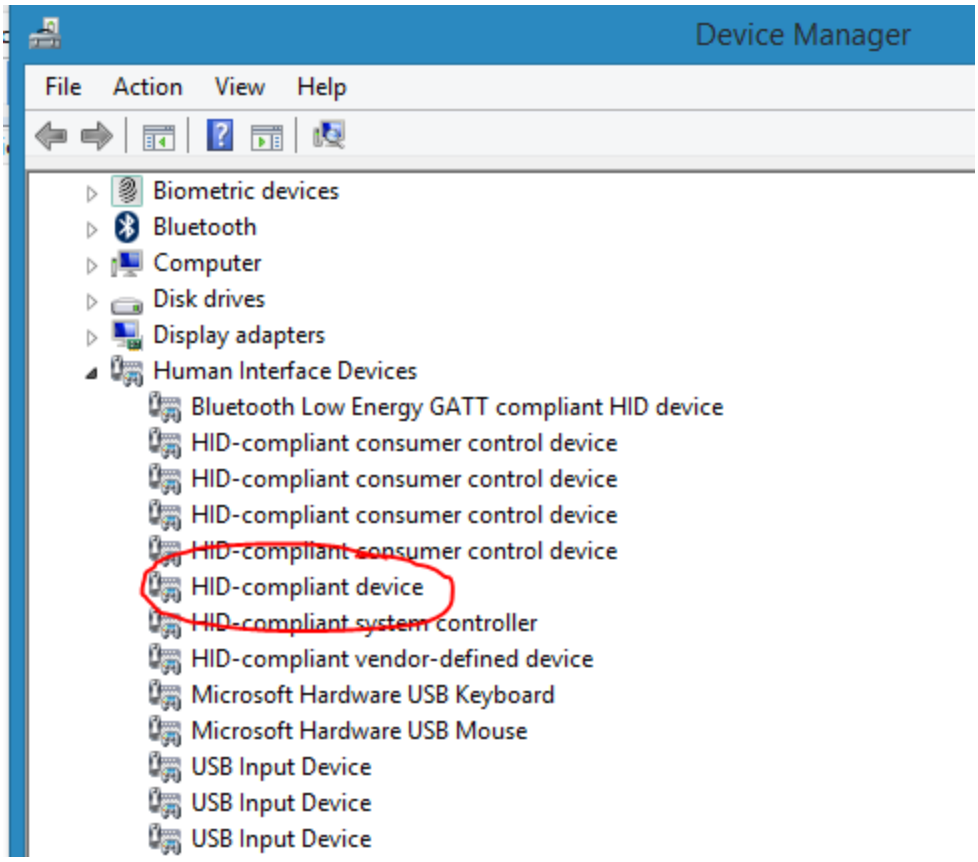
Troubleshooting Encoders

When encoding or reading a key fails, an information box identifies the following problems:

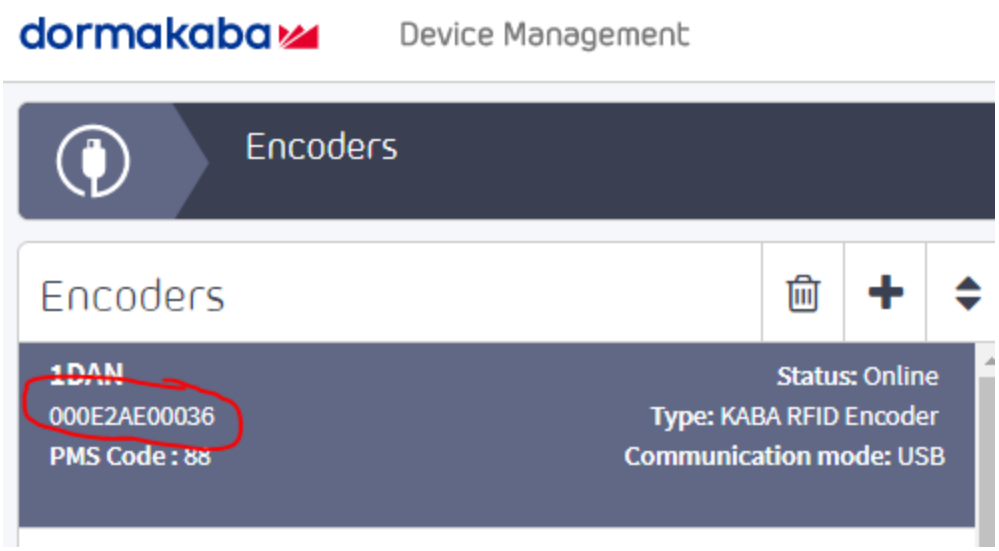
- When communication between the encoder and workstation fails.
- When the encoder is offline.
- When the encoder is busy.
- When a key is not presented to the encoder within the expected delay.
- When the key is damaged, corrupt or uses unsupported technology.

Use the following steps to troubleshoot encoders:

1. Make sure that the Ambiance Client Service is running on the workstation.
2. 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\Ambiance 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 Ambiance Server (typically, configured during initial server installation).

Troubleshooting Locks

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.

Green Light

A green light will flash for approximately six seconds when a correct key is used. This light 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

1. 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.

2. 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:

a. The door has been electronically double locked by an electronic lockout key.

b. The Guest key has been automatically inhibited, or the lock has been inhibited by the inhibit key.

c. The key was programmed with an expiration date and time. The light indicates that the key was used after this expiration date and time.

d. 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.

3. Two Yellow Flashes

Two yellow flashes indicate that an incorrect key was used in the lock.

4. One Yellow before Green or Yellow

The master key being used is about to expire. This light will appear seven days prior to the expiration date.

Red Light

Alternately Flashing Red Light

A red light will flash alternately with another light when the lock batteries are low.

Simultaneously Flashing Red Light

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 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:

1. An invalid key shutdown is in effect.

2. The key switch is broken.

3. The lock batteries are dead.

6.3 Invalid Lock and Mode Indicators

The SAFLOK is 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. 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 E2 has failed. No key will open the lock, and the lock must be drilled to access the room.

2. 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 E2 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.

3. 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.

4. 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.

5. 2 Red Flashes. Then All Lights Flash (4 Times) These lights indicate that the lock is in Mode 4, and that the storage chip (E2) is disabled. Use the PPK key followed by the E2 Disable/Enable key to enable the lock.

6. 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.

GLOSSARY

A

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 Group

Logical grouping of one or more access points that facilitates the assignment of credentials to all access points in the group.

Access Point Type

Functional classification of an access point. The access point types in Ambiance include guest rooms, suites, guest and staff common areas, meeting rooms, restricted areas and elevators.

Access Schedule

Day and time constraints that control when a common area for guests and/or staff is accessible.

Amenities

Guest common areas. Depending on how the common area is defined in Property Builder and how the common area access profile that contains the common area is configured, access to an amenity may be included in guest registrations by default or may require manual selection.

Auto-Unlatch Schedule

Schedule defined with day and time periods allowing passage without credentials. Auto-Unlatch schedules can be created for common areas (guest and/or staff), meeting rooms and restricted areas.

B

Block Keys

Keys that temporarily block all key instances of a specific credential at access points.

C

Cancel Keys

Keys that permanently invalidate a specific key instance.

Common Area Access Profile

Configuration that defines the common areas that are accessible for selected guest rooms and suites or for selected staff credentials, and whether access is included by default or must be manually selected.

Credential

1) Configuration in Ambiance that consists of select 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. For guests, credentials are implicitly associated as the guest room or suite assigned during guest registration. For staff, credentials are created

in Access Management > Credential Management and configured as staff credentials (for making staff keys) or system credentials (for making system keys).

Credential Class

Organizational label used to group credentials based on the level and type of access. Staff credential classes include Emergency, Grand Master, Master and Limited Use Staff. System credential classes include Latch, Unlatch and Toggle Latch/Unlatch. You can also create custom credential classes.

Credential Class Type

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. The credential class types used for staff keys are: Emergency, Grand Master, Master and Limited Use Staff. The credential class types used for system keys are: Latch, Unlatch and Toggle Latch/Unlatch.

D

Diagnostic Keys

System keys that query 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 Keys

(ELO) System keys that temporarily invalidate all non-Emergency Keys. 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.

Elevator

Type of access point intended to provide access to building floors. Elevators are grouped by Elevator Bank.

Elevator Bank

Group of elevators that are configured for access to the same floors.

Emergency

Credential class type/class. Overrides deadbolt/privacy switch.

Encoder

Embedded device used to encode keys with data. To make keys, an encoder must be online and accessible to the Ambiance workstation.

F

Failsafe Keys

Backup keys for a guest room or suite made in advance and maintained in complete sets to be issued in the event a system or power failure prevents making keys.

Folio (guest)

Data format for encoding third-party POS (point-of-sale) features, such as a parking service or vending supplier.

G

Grand Master Keys

1) Credential class. As a guideline, the Grand Master class should be used for credentials that open all access points excluding locks with the deadbolt thrown or privacy switch set. In practice, the Grand Master class opens all access points assigned to the Grand Master class. 2) Key on which a Grand Master credential is encoded.

Guest Common Area

Type of access point where general access is configured for guests (with or without staff access) and may be limited based on credential or common area access profile. Common areas included on guest reservations are listed as amenities.

Guest Limited Use Keys

Keys issued to a guest that provide one-time access to a guest room or suite. Most often, Limited Use Keys for guests are issued when a guest returns after check-out for an item left in the room.

Guest Preregistration

Guest reservation made for a date in the future. The record is stored in the Ambiance database.

Guest Registration

Guest registration made for the current date. The record is stored in the Ambiance database.

Guest Room

Type of access point assigned to a guest during guest registration.

H

Hub

Hubs are the network devices used to connect the access point configuration data in Ambiance to the locks installed at access points.

I

Inhibit Keys

Keys that permanently cancel all access for a current guest. Most often, Inhibit Keys are used by staff after cleaning a room that a guest vacates before their key expires. Inhibit Keys invalidate all guest keys (including Failsafe Keys) encoded with access to the room even if the dead bolt or the privacy switch is set.

K

Key

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.

Key Holder

Guest or staff in possession of at least one key instance.

Key Instance

Specific key among multiple keys that are encoded with the same credential.

L

Latch Keys

Keys that disable passage mode and reinstate the access controls programmed in the lock.

Lock Profile

Lock or elevator controller device model.

M

Maintenance Unit (M-Unit)

Hand-held embedded device used to transfer data between Ambiance and locks.

Master Keys

1) Credential class. As a guideline, the Master class should be used for general purpose staff credentials. In practice, the Master class opens all access points assigned to the Master class. 2) Key on which a Master credential is encoded.

Meeting Room

Type of access point intended to accommodate special events for the public and/or registered guests. An Auto-Unlatch schedule can be assigned to a meeting room.

Mobile Key

Virtual key issued to a guest or staff mobile phone.

O

Operator

Staff member who is assigned a role that is configured to authorize access to Ambiance modules and features.

P

Passage Mode

Lock state during which the access controls programmed in the lock are suspended allowing unrestricted access.

PCI-DSS

Payment Card Industry-Data Security Standard. Information security standard that provides additional login protection.

Primary Program Keys

System keys that authorize the function of another system key.

Property Management System

Software used in the hospitality industry to manage property, operations and people. Ambiance integrates with leading PMSs to provide secure access control management using MICRO FIAS, Saflok Web Service, and Saflok IRS protocols.

R

Reader

Embedded device installed in elevators that reads access control data stored on keys. Based on the data, access is allowed or denied.

Remote Lock Management

A licensed feature that refers to wireless communication for the purpose of updating remote devices. In Ambiance RX, remote communication is used to perform online access point operations and to receive online access point events.

Resequence Keys

Keys that resynchronize a specific key credential in access points.

Restricted Area

Type of access point intended for staff only for back of the house access. Auto-Unlatch and Access schedules can be assigned to a restricted area.

RFID Key Types

Radio Frequency Identification. Type of smart card chip installed on the key. Ambiance supports Mifare Classic (1K, 4K), Plus, Mini and Ultralight C.

Rights (Role Management)

Discrete functions in Ambiance organized by module.

Role (Operator)

1) A group of rights. 2) Mechanism by which administrators enable operator access to Ambiance functions (rights). Principal roles pre-defined in Ambiance include Administrator, Front Desk Agent, Site Configurator, and Staff Manager. Custom roles may also be created and configured.

S

Schedule Period

A span of time. Depending on the type of schedule, multiple periods may be added per day and may span multiple days.

Secondary Program Keys

Keys that reprogram or resynchronize the current Primary Program Key (PPK) into access points and remaster a different PPK into a lock.

Shift Schedule

Day and time constraints applied to staff keys.

Site

A geographical location that consists of one or more buildings.

Special Function Keys

System keys that are used for advanced lock operations. In some cases, the Special Function Key must be used in conjunction with a Primary Program Key.

Staff

Key holders in your organization and operators.

Staff Common Area

A type of access point where general access is configured for staff and may be limited based on credential or common area access profile.

Staff Keys

Keys issued to personnel, vendors and emergency officials.

Staff Limited Use Keys

Keys issued to staff that provide temporary access to an access point for a predefined number of times or until the key expires. The key is valid for seven uses by default or until expiration.

Suite

A connected series of guest rooms that includes a common door and one or more inner door access points.

System Keys

Keys that are used to perform lock or system-level operations.

T

Toggle Latch/Unlatch Keys

Keys that are used to enable and/or disable passage mode. When a toggle key is presented to open (unlatch) an access point, the access point remains open and accessible until the toggle key is presented again to close (latch) the access point.

Toggle mode

A characteristic of a lock or key that alternates behavior (open-secure) each time the key is presented. When a toggle key is presented that opens the lock, the door may close but access remains open until the key is presented again.

U

Unblock Keys

System keys that unblock all instances of a specific credential in access points which were previously blocked using a Block Key.

Unlatch Keys

System keys that enable passage mode.

INDEX

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W