

Ambiance

User Guide

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

www.dormakaba.com

Copyright © dormakaba 2026
All rights reserved.

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

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

Subject to technical changes.

Table of contents

About this document	8
Welcome to Ambiance	9
Configuration	11
Site configuration workflow	13
Configure System Settings	14
Learning about System Settings	15
General Settings	21
Guest Registration Settings	22
Security Settings	24
Staff Key Settings	35
Failsafe Key Settings	36
Key Expiration Settings	37
Email Configuration Settings	39
Database backup settings	40
Folio Settings	44
PMS Settings	47
Return UID Interface Settings	52
Staff key validation settings	53
Advanced Settings	55
Licensing Settings	58
Build Your Property	59
Learning about Property Builder	60
Add buildings	66
Add floors	68
Add guest rooms	71
Add suites	77
Add foyer doors	82
Associate access points to foyer door	84
Add guest common areas	86
Add staff common areas	92
Add meeting rooms	98
Add restricted areas	101
Add elevators	104
Configure Access	109

Learning about Access Management	110
Add auto-unlatch schedules	113
Add access schedules	115
Add shift schedules	117
Create access point groups	119
Add credentials	121
Assign schedules	125
Configure access profiles for limited-access common areas	126
Configure Devices	131
Learning about Device Management	132
Add encoders	135
Configure and commission staff key validator devices	139
Program Locks	142
Learning about Programming & Auditing	143
Program locks	146
Review & Customize Roles	148
Learning about Role Management	149
Review pre-defined roles	150
Configure custom roles	151
Add Operators	152
Learning about Staff Management	153
Configure operators	154
Import staff list	161
Use Ambiance	163
Guest Registration	165
Learning about Guest Registration	166
Add a guest registration	170
Modify a guest registration	177
Replace guest keys	180
Make additional guest keys	182
Make a limited-use guest key	185
Check out a registration	187
Staff	188
Learning about Staff Management and Staff Keys	189
Add staff members	190
Import staff member list	193

Make Emergency keys	195
Make Grand Master keys	198
Make Master keys	203
Make Limited Use Staff keys	207
Replace staff keys	210
Invalidate staff access	212
Test key files	217
Programming/Auditing	219
Reprogram locks	220
Audit locks	222
Audit online access points	223
System Keys	224
Learning about System Keys	225
Block and unblock keys	227
Cancel keys	231
Diagnostic keys	233
Electronic lockout keys	235
Failsafe keys	237
Inhibit keys	238
Latch and unlatch keys	240
Primary and secondary program keys	242
Resequencing keys	245
Special function keys	247
Monitoring	248
Learning about Monitoring	249
Monitor keys	250
Reports	251
Access Point Audit Report	252
System Activity Report	253
Staff Access Report	255
Roles and Rights Report	256
Property Configuration Report	257
Operator Report	258
Key Expiration Report	259
Key/User Assignment Report	260
Elevator Configuration Report	261

Credential/Access Point Assignment Report	262
Toolbar Basics	263
Navigate Ambiance	264
Set operator preferences	266
Install / update Ambiance Client	268
Select default encoder	269
Read key/erase key/access tracking report	270
View notifications	274
Physical keys	276
Digital keys	278
Remote Lock Mgmt	282
Introduction	283
Enable and configure online communication	284
Gateways & Paired Access Points	291
Manage online device configuration	292
Registered gateways and paired access points	294
Program Devices	299
Program devices	300
Notification Management	301
Learning about Notification Management	302
Add notification groups	304
Monitoring (RLM)	306
Learning about Monitoring	307
View metrics	308
Monitor online operations	309
Monitor online events	311
Monitor access point status	314
Reports (RLM)	315
Online Access Points Status Report	316
Online Gateway Status Report	317
Online Paired Access Point Report	318
Troubleshooting	319
Services Manager	320
Troubleshooting PMS	324
Troubleshooting encoders	326
Troubleshooting locks	330

Log data	336
Glossary	337
Index	346

About this document

Validity

This document describes the product:

Product designation:	Ambiance
----------------------	----------

Version:	2.15
----------	------

Target audience

This document is for all Ambiance Operators: Administrator, Site Configurator, Staff Manager and Front Desk Agent.

Purpose and objective

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

Additional documents

Ambiance Installation Guide v 2.15 PK3722-EN

Ambiance Release Notes v 2.15 PK3702

Ambiance Enhanced Key Security for Upgrades 2.15 PK3777

Welcome to Ambiance

Ambiance® is the leading-edge access management software for the hospitality industry. Developed for security and designed for users, the application streamlines access control management and integrates seamlessly into any hotel IT infrastructure. Ambiance provides an efficient and user-friendly method to establish and manage multisite property access. Flexible configuration and integration options showcase a robust feature set. Guided workflows simplify property configuration, staff management, key issuance, and guest registration. Configurable user permissions secure system access. Lock and system data collection supports detailed access point audits and reporting. Remote lock management provides immediate and convenient control of access points. An extensive library of web services and APIs are available for third-party integrations. Ambiance also supports market-demand technologies including Bluetooth® and enhanced key security. The browser-based Ambiance Client provides system access 24/7 from any device on the property network.

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 Ambiance.
- "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.
- "Remote Lock Management" provides information related to the licensed feature Online Communication and all other features that require Online Communication.
- "Troubleshooting" contains problem-solving information produced by dormakaba field technicians.
- The Glossary defines terms used in the product.
- The Table of Contents and Index provide alternative means of finding information.

Additionally, contextual help is available in the product.

Installation

Installing the 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.
- [Device Management](#) where you configure encoders. If licensed for online communication, you can also work with gateways and paired access points.

- [Programming & Auditing](#) where you access the data transfer function required to program and audit locks. If online communication is enabled, you can also audit online access points.
- [Notifications Management](#) where you create logical groupings of notifications to which operators can subscribe. The module is only active when licensed for online communication.
- [Role Management](#) where you create and configure Operator roles and the associated rights.
- [Staff 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 online communication is enabled, you can also audit online access points.
- [System Keys](#) where you encode special purpose keys.
- [Monitoring](#) where you check the status of all keys made in Ambiance. If licensed for online communication, you can also monitor operations, events and paired access point status.
- [Reports](#) where you generate current and historical reports for every aspect of your site.

Access to 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 section includes the following subjects:

Site configuration workflow	13
Configure System Settings	14
Learning about System Settings	15
General Settings	21
Guest Registration Settings	22
Security Settings	24
Staff Key Settings	35
Failsafe Key Settings	36
Key Expiration Settings	37
Email Configuration Settings	39
Database backup settings	40
Folio Settings	44
PMS Settings	47
Return UID Interface Settings	52
Staff key validation settings	53
Advanced Settings	55
Licensing Settings	58
Build Your Property	59
Learning about Property Builder	60
Add buildings	66
Add floors	68
Add guest rooms	71
Add suites	77
Add foyer doors	82
Associate access points to foyer door	84
Add guest common areas	86

Add staff common areas	92
Add meeting rooms	98
Add restricted areas	101
Add elevators	104
Configure Access	109
Learning about Access Management	110
Add auto-unlatch schedules	113
Add access schedules	115
Add shift schedules	117
Create access point groups	119
Add credentials	121
Assign schedules	125
Configure access profiles for limited-access common areas	126
Configure Devices	131
Learning about Device Management	132
Add encoders	135
Configure and commission staff key validator devices	139
Program Locks	142
Learning about Programming & Auditing	143
Program locks	146
Review & Customize Roles	148
Learning about Role Management	149
Review pre-defined roles	150
Configure custom roles	151
Add Operators	152
Learning about Staff Management	153
Configure operators	154
Import staff list	161

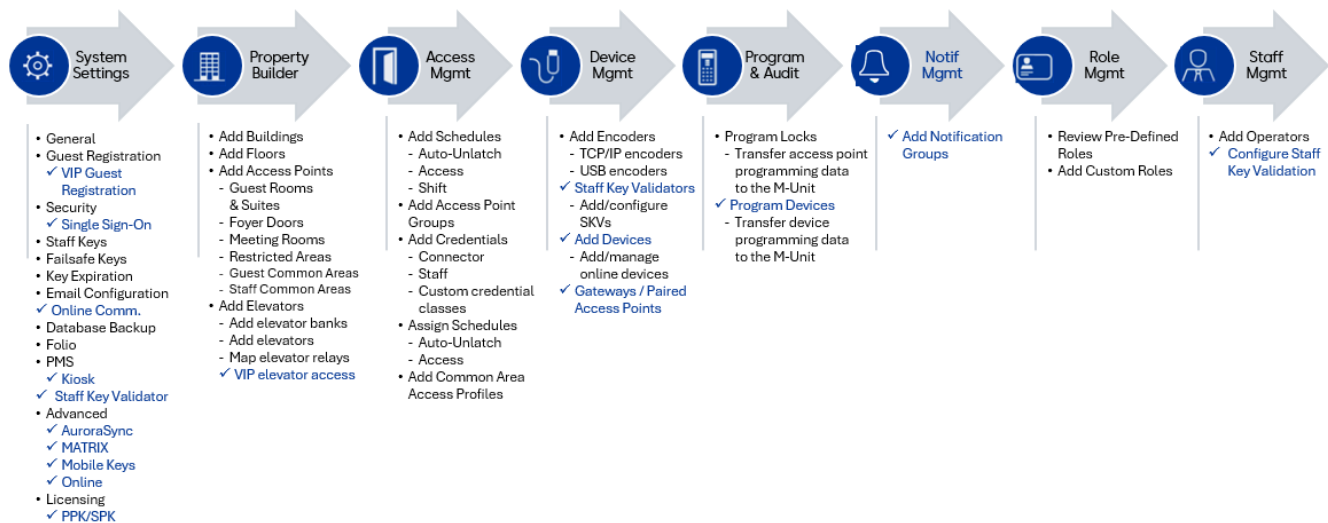
Site configuration workflow

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. Licensed features are listed in parentheses.



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

Ambiance workflow



After site configuration, remember to ...

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

Step 1

Configure System Settings

This section includes the following subjects:

Learning about System Settings	15
General Settings	21
Guest Registration Settings	22
Security Settings	24
Staff Key Settings	35
Failsafe Key Settings	36
Key Expiration Settings	37
Email Configuration Settings	39
Database backup settings	40
Folio Settings	44
PMS Settings	47
Return UID Interface Settings	52
Staff key validation settings	53
Advanced Settings	55
Licensing Settings	58

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 is not offered during the process of making keys.

Configure System Settings

To configure system settings:

- Go to the [System Settings](#) module and specify settings for each category.

Configure system-wide defaults and enable licensed options. To make site configuration more efficient, 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 basic site information and enable phone/mobile number validation override. With the exception of the site name and site image, all settings have system defaults. None of the options in this category require attention.

Guest Registration

Configure defaults for the Guest Registration module. Most settings have system defaults. 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.



VIP guest registration is a licensed feature that is disabled by default. When VIP guest registrations is enabled, additional settings must be configured. In addition the following system settings require attention:

- PMS authentication ([System Settings > Security > PMS](#))
- LGS SOAP API shared-with registrations ([System Settings > PMS > Web Service](#))
- Online communication ([System Settings > Advanced > Enable online communication](#) and [System Settings > Advanced > Online Communication](#))

Security

Configure settings related to account security and lock access, disable/enable enhanced security mode, obtain the Maintenance Unit security password when enhanced security mode is enabled, enable PMS client certificate authentication, enable device security after an upgrade, configure browser certificate options, and enable and configure single sign-on. The following situations require manual configuration:

- Disable authentication for PMS
- Disable authentication for Maintenance Unit accounts
- Enable client certificate validation for PMS requests
- Enable device security after an upgrade
- Enable/disable Enhanced Security Mode



The following licensed features are also accessible:

- KIOSK– Enable and generate new client certificate for kiosks
- Single Sign-On – Enable and configure single sign-on.

Staff Keys

Configure how many times a [Limited Use Key](#) can be used and select whether to display the menu to add additional 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 two sets of three keys for each guest room and suite door.

Key Expiration

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

Email

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

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

Online Communication

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

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

Database Backup



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

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

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

Refer to the following table for backup/archive details.

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



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

Folio

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 encode on the key. The PMS and POS systems are responsible for reading, validating and utilizing the data.

Folio data is stored on Track 2 (sector 8 for VIP guest keys) of guest keys, an area that does not use dormakaba encryption thereby allowing any third-party access to the data.

The folio data format is determined by PMS and third-party requirements. The following data formats are supported:

- Auto-Format - Room & Check-In/Check-Out—MIFARE Ultralight AES and MIFARE Ultralight C keys are not supported. Based on the room number and check-in/check-out dates. This option requires that all guest room and suite access point names site-wide be numeric only.
- PMS and/or User Interface—Based on a custom folio layout defined in Ambiance that structures data on Track 2/8 according to the selected standard (ASCII or ANSI/ISO). Typically, this format is used to associate a guest registration with an account or guest/staff ID. The following data encoding standards are supported:
 - ASCII data format—The format code is 3. Standard ASCII format.
 - ISO/ANSI BCD data format (1)—The format code is a single numeric character established by the PMS or POS system. The character code is numeric only, must be a binary-coded decimal (BCD) 5-bit subset with odd parity and padded with zeros. Mobile keys are only supported when using the LGS SOAP API protocol.
 - ISO/ANSI BCD data format (2)—There is no format code or character code padding. The character code which is numeric only and must be a binary-coded decimal (BCD) 5-bit subset with odd parity. Mobile keys are only supported when using the LGS SOAP API protocol.

For technical details about folio formats, ask dormakaba Support for the document *Ambiance Folio Data Formats*.

PMS

Select and configure a PMS (Property Management System) protocol. Options include:

- LGS REST API (dormakaba). For details about the API, obtain the specification *LGS REST API* (PK3759) from a dormakaba Support technician.
- FIAS (Oracle®). Shared-with registrations support.
- LGS SOAP API (dormakaba). Shared-with registrations support. For details about the API, obtain the specification *LGS SOAP API* (PK3765) from a dormakaba Support technician.
- OPERA (Oracle).
- IRS/PRS (dormakaba)
- LGS REST API (KF2, dormakaba). For details about the API, obtain the specification *LGS REST API - KF2* (PK3775) from a dormakaba Support technician.
- BART (dormakaba). For details about the API, obtain the specification *LGS BART API* (PK3774) from a dormakaba Support technician.
- SkyTouch® (SkyTouch). For details about the API, obtain the specification *LGS SkyTouch API* from a dormakaba Support technician.



KIOSK is a licensed feature that is disabled by default. Enable to process PMS requests for kiosks.

Shared-With Registrations

Shared-with registrations is a feature supported for LGS SOAP API and FIAS protocols. When enabled, up to four registrations can share access to one guest room. Check-out dates and the assignment of additional rooms, amenities and floors can be different for each shared-with registration. The shared room (or main room) is established as the first room specified in the original registration.

Example

Registration 1: Room 100 (main room), Room 101, Pool

Registration 2: Room 100, Room 102, Pool, Daycare

Registration 3: Room 100, Room 103 , Gym, Business Center, VIP Lounge

Registration 4: Room 100, Room 104, Pool, Gym, Daycare

Shared-with registrations must be created (and modified) in the PMS interface. Although the registrations are listed in Guest Registration, [Check-out](#) is the only action that can be performed in the Ambiance user interface or PMS interface.

Modifying shared-with registrations

All modifications must be made in the PMS interface. Modifications made to a shared-with registration apply only to the registration being modified. You can:

- Add vacant rooms
- Remove rooms
- Extend the check-out date and time
- Move a guest from a shared-with registration to a vacant room (Any guest in the original shared-with registration, can also move to the same room. For example, if Guest1 and Guest2 are assigned to MainRoom100 and Guest1 moves to vacant RoomX, then Guest2 can also move to (now occupied) RoomX.)



An existing guest cannot be added to a shared-with registration. (You must check-out the exiting guest, then add as a new guest; presuming this does not exceed the maximum shares).

Invalidating access

There are several ways to invalidate access for shared-with registrations:

- [Check outs](#)—Shared-with registrations can be checked out using the PMS interface and Ambiance user interface. When a shared-with registration is checked out, the main room is available for a new guest to join. When Online Communication is enabled, you can perform a remote check-out. Otherwise, Block Keys must be made and presented to relevant access points.

- **Block/Inhibit/ELO Keys**—These system keys can be used to invalidate access for shared-with registrations. When Online Communication is enabled, the command can be sent remotely. Otherwise, keys must be made and presented to relevant access points.
- **New Keys**—New Keys invalidate access as follows:
 - Making a New Key for Guest1 with a shared registration invalidates all previous keys for Guest1. No other guest access is affected.
 - After the maximum number of shared-with registrations is reached, making a New Key for a new registration for the main room may invalidate all access to all previous shared-with registrations for the main room. The result depends on options selected when making the registration.

Extended Support

Ambiance extends support for shared-with registrations to all System Keys and Keyscan Aurora. For details about working with shared-with registrations, refer to the [PMS Interface Reference](#).

Staff Key Validators

Staff key validation is a licensed Ambiance option that reinforces access control by validating staff keys daily. The SKV (staff key validator) device, installed at a central location, includes a touchscreen terminal and RFID encoder. The touchscreen guides staff through the required steps, while the encoder validates their key, captures access-tracking data, and updates the key with the latest access permissions assigned to that staff member.

Staff key validation works exclusively with credentials defined using the Master credential. Refer to the release notes for detailed requirements.

Return UID Interface

Ambiance supports integration with third-party destination elevator control systems to direct guests and other key holders to the elevator associated with their assigned rooms. Integration options support using a virtual UID or RFID key UID. Additional documentation resources are available depending on the selected interface type. For TCP/IP, refer to *Ambiance / Return UID - TCP/IP* (PK3763-EN); for REST, refer to *Ambiance / Return UID - REST* (PK3762-EN). Both documents can be obtained from your dormakaba Support technician.

Staff key validation

Staff key validation is a licensed Ambiance option that reinforces access control by validating staff keys daily. The SKV (staff key validator) device, installed at a central location, includes a touchscreen terminal and RFID encoder. The touchscreen guides staff through the required steps, while the encoder validates their key, captures access-tracking data, and updates the key with the latest access permissions assigned to that staff member.

Staff key validation works exclusively with credentials defined using the Master credential. Refer to the release notes for detailed requirements.

Advanced

Change key technology settings and configure defaults for pre-registrations.



The following licensed features are also accessible:

- Mobile keys—Enable mobile keys.
- Online communication—Enable Online Communication. For more information, see "Working with Online Communication" on the Help Home page.
- MATRIX—For more information, see *Ambiance MATRIX Integration* (PK3770).
- AuroraSync—For more information, see *Ambiance Aurora Integration* (PK3768).

Licensing

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

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

General Settings

Configure basic site settings.

1. Go to [System Settings > General](#).

General Settings

Site name

BDM Heritage Hotel

System default language

Automatic Language Detection ▼

Time Zone

(UTC-05:00) Eastern Time (America/New_York) ▼

Date format

MM/dd/yyyy ▼

Time format

hh:mm (AM/PM) ▼

Allow phone/mobile number validation override

NO

Background image



Reset Image Upload Image

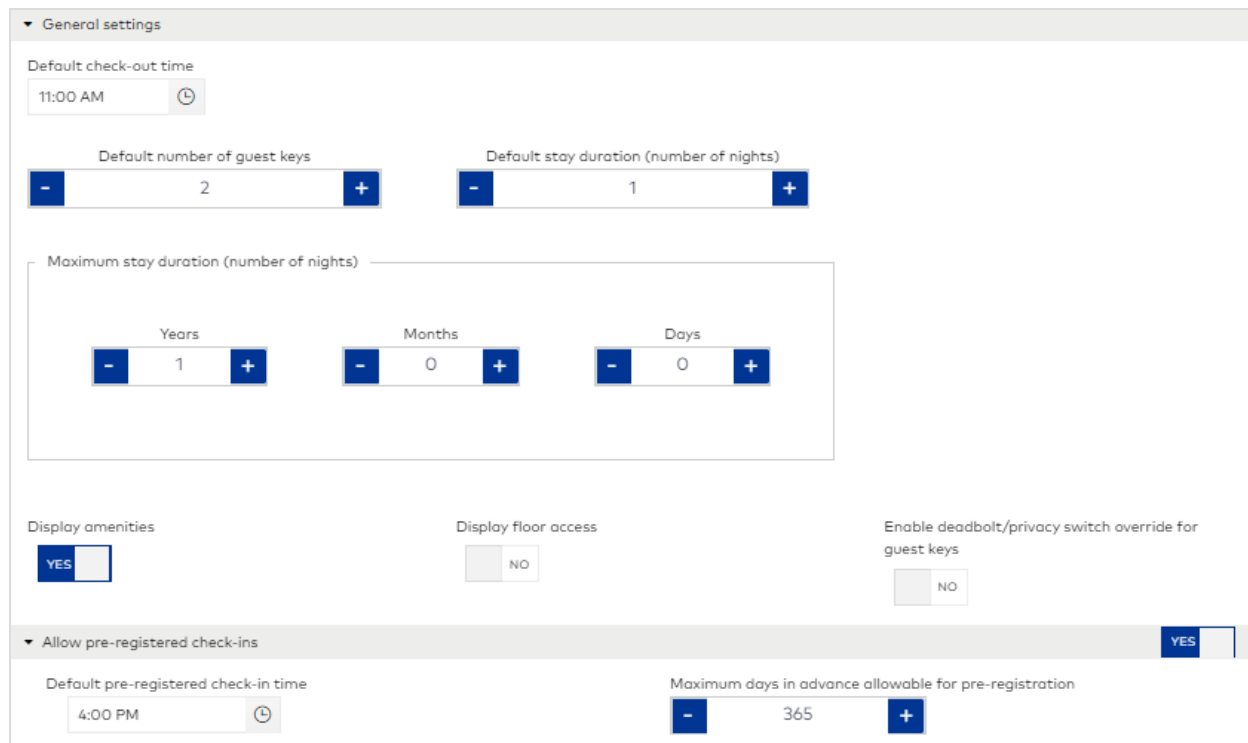
2. For [Site name](#), specify the name of the property. Max characters: 30. The site name appears in reports. Default: My Site.
3. For [System default language](#), select the default language for the user interface. The default is to detect the browser language. The UI displays in the selected language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

Guest Registration Settings

Configure system-wide defaults for the [Guest Registration](#) module.

1. Go to [System Settings > Guest Registration](#).
2. Configure options in the following sections:
 - General settings
 - Allow pre-registered check-ins
 - Enable VIP guest registrations
3. Click [\(Save\)](#) .

General Settings



General settings

Default check-out time
11:00 AM 

Default number of guest keys:  

Default stay duration (number of nights):  

Maximum stay duration (number of nights)

Years:   Months:   Days:  

Display amenities: ☒ YES ☐ NO

Display floor access: ☐ YES ☒ NO

Enable deadbolt/privacy switch override for guest keys: ☐ YES ☒ NO

Allow pre-registered check-ins ☒

Default pre-registered check-in time: 4:00 PM 

Maximum days in advance allowable for pre-registration:  

- Select the default check-out time for all guest registrations. The value can be modified when registering a guest. Default: 11am.
- 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.
- Specify the default number of nights for a single guest registration. The value can be modified when registering a guest. Default: 1.
- Specify the maximum number of nights for a single guest registration. Default: 365.
- Select whether to display amenities (guest common areas) associated with a guest registration. Default: YES.
- *(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 guest 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.
- Select whether guest keys (including failsafe keys) can override the deadbolt/privacy switch for assigned room and suite room doors. If you change this setting, you must program (reprogram) affected access points. Default: NO.
 - When set to NO, active guest keys are denied access when the deadbolt/privacy switch is engaged. Only Emergency keys can open the lock.

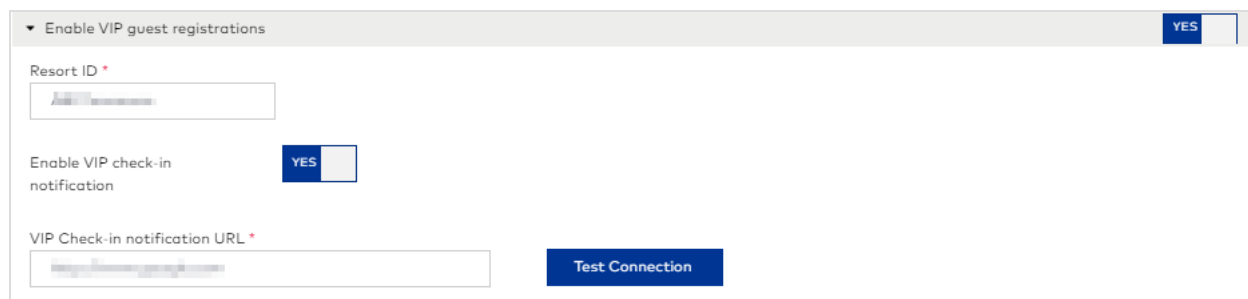
- When set to YES, current new and duplicate guest keys are granted access regardless of whether the deadbolt/privacy switch is engaged (initial access assumes the deadbolt/privacy switch is disengaged); the next new and duplicate keys are granted access only when the deadbolt/privacy switch is disengaged.

Pre-Registrations

- Select whether to allow pre-registrations. This feature lets you create (and modify) registrations for a guest stay in the future. Default: YES.
- Select the default check-in time for all guest registrations. The value can be modified when registering a guest. Default: 3pm.
- Specify the maximum number of days that a guest registration can be made before the check-in date. Default: 365.

VIP Guest Registrations

This section displays when licensed for VIP guest registrations.



▼ Enable VIP guest registrations YES

Resort ID *

Enable VIP check-in notification YES

VIP Check-in notification URL *

Test Connection

- Select **YES** to enable VIP guest registrations. When enabled, keys can be encoded with VIP guest access. Default: NO.



Modifying this setting requires reprogramming some access points and re-encoding all keys.

- Specify the unique ID for the VIP resort. The Resort ID specified in PMS booking requests must be identical to the Resort ID specified in Ambiance [System Settings](#). VIP uses the ID to authenticate the site. Valid chars: 0-9/a-z/A-Z, Max chars: 20.
- Select **YES** to enable VIP check-in notifications. When enabled, Ambiance notifies the PMS when a VIP guest registration is checked in. A valid Web service URL is required.
- Specify the Web service URL for Ambiance to send VIP-related notifications to the PMS.

Security Settings

Security settings protect account access. All settings in this category (except [PCI-DSS](#)) are populated with recommended or moderate values.



All sample values in the figures reflect the system defaults.

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

Password Criteria

Security Settings PCI-DSS ☒ YES

▼ Password Criteria

Minimum password length (min 7 - max 20)	7
Minimum lowercase characters (a-z)(max 5)	1
Minimum uppercase characters (A-Z)(max 5)	1
Minimum numerical characters (0-9)(max 5)	1
Minimum special characters (~!@#\$%^&_)(max 5)	1

- **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 when PCI-DSS enabled, 6-20 when PCI-DSS disabled.
- **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

Password expiration days	90
Enable password expiration notification	☒ YES ☐
Notification days prior to expiration	7

- **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

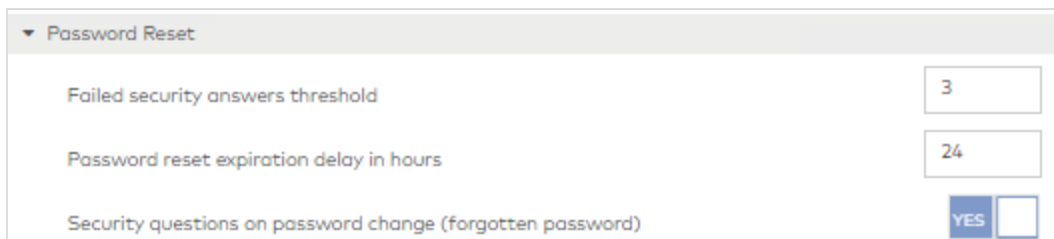


▼ Password History

Number of previous passwords to check

- **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



▼ Password Reset

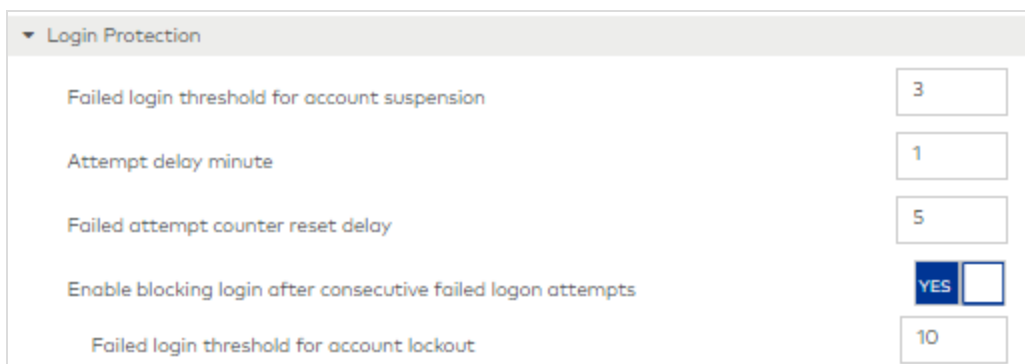
Failed security answers threshold

Password reset expiration delay in hours

Security questions on password change (forgotten password) ☒ YES ☐

- **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



▼ Login Protection

Failed login threshold for account suspension

Attempt delay minute

Failed attempt counter reset delay

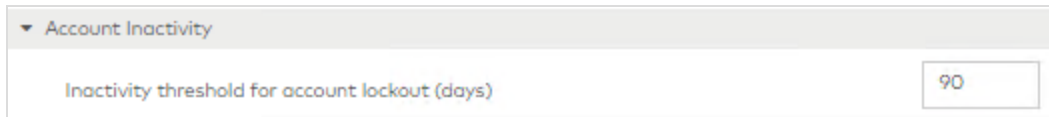
Enable blocking login after consecutive failed logon attempts ☒ YES ☐

Failed login threshold for account lockout

- **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: 3-30.
- **Attempt delay minute**—Specify the number of minutes to suspend an account. Valid values: 1-30.

- **Failed attempt counter reset delay**—Specify the number of minutes to suspend an account when the [Failed login threshold for account suspension](#) is reached. Valid values: 1-30.
- **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

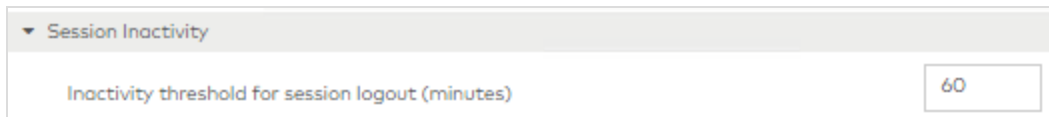


▼ Account Inactivity

Inactivity threshold for account lockout (days)

- **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



▼ Session Inactivity

Inactivity threshold for session logout (minutes)

- **Inactivity threshold for session logout (minutes)**—Specify the number of minutes after which an active Ambiance session with no activity ends. When the threshold is reached, the operator must log in again. Valid values: 5-360.

Maintenance Unit



▼ Maintenance Unit

Enable Maintenance Unit authentication ☒

Expire access point programming data after

Days: Hours:

- 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. Defaults: YES, 1 day and 0 hours.
- Specify the number of days and hours after which the data on the M-Unit cannot be transferred. Default: 1 day, 0 hours.

PMS

PMS

Enable PMS authentication

YES

Validate client certificate

YES

Validate certificate expiration

YES

Certificate Information

Subject: O=dormakaba, CN=LockServer Self-Signed Root CA

Issuer: O=dormakaba, CN=LockServer Self-Signed Root CA

Valid From: 02/01/2023 04:17

Valid To: 07/31/2023 05:17

Thumbprint:

Generate new certificate

- Select whether to require authentication for PMS requests. When authentication is enabled, PMS requests are not processed until the user name and password specified in the request are authenticated against the PMS operator user name and password configured in [Staff Management](#). Required for enhanced security mode. Default: YES.
- [Validate client certificate](#)—(LGS SOAP API or LGS REST API) Select whether to validate the client certificate for each PMS request. Required to validate certificate expiration. Default: NO. When enabled, the following settings display:
 - [Validate certificate expiration](#)—Select whether to validate the certificate expiration for each PMS request. When set to YES and the certificate is expired, PMS requests are not processed. [Validate client certificate](#) must be set to YES. Default: YES.
 - [Generate new certificate](#)—A certificate is automatically generated for fresh installs. Click to generate a certificate valid for one year. Ambiance generates the certificate regardless of whether the current certificate is current or expired. Certificates are stored in the Personal and Trusted Root Certification Authorities folders on the local machine. For details about exporting/importing the certificate, refer to the API documentation.

Lock Access



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

Lock Access

Escape/return

Enable escape/return functionality for

Guest rooms/suites

NO

Meeting rooms

NO

Restricted areas

NO

Guest common areas

NO

Staff common areas

NO

Escape/return delay (seconds)

—

60

+

Quick relatch

Enable quick relatch functionality for

Guest rooms/suites

NO

Meeting rooms

NO

Restricted areas

NO

Guest common areas

NO

Staff common areas

NO

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



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

Disability mode

Disability mode

Disability delay (seconds)

- 15 +

Display disability option in Guest Registration ☐ NO

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

RAC5 option

Changes to this setting may require reprogramming locks.

RAC5 Unlock delay (seconds)

- 4 +

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

HTTPS Certificate

▼ HTTPS Certificate

HTTPS certificate expiration warning (days)

- 30 +

Certificate friendly name

Server_Server_20180401_1700_100_1_1

Enable automatic CAPI store certificate renewal ☒ YES

Do not use expired certificates ☒ YES

When Ambiance is deployed with an SSL certificate:

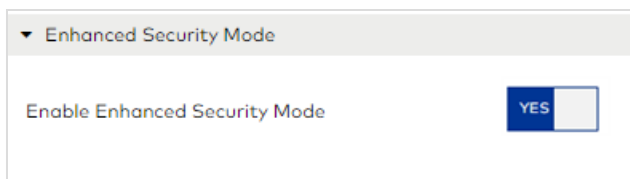
- Specify the number of days before the certificate expires to start receiving a daily warning. Default: 30. Valid values: 0-365.

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

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

Enhanced Security Mode

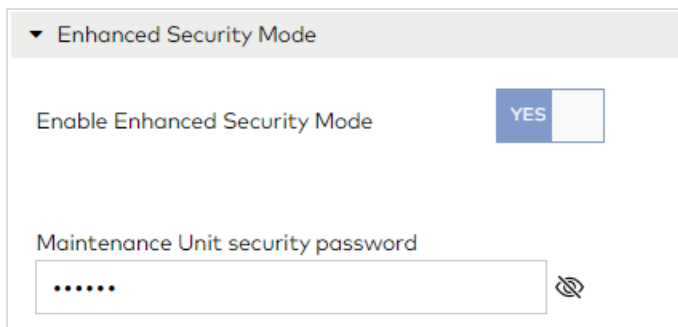
The option to use high security keys is enabled by default.



▼ Enhanced Security Mode

Enable Enhanced Security Mode ☒ YES

The [Maintenance Unit security password](#) populates upon configuring the initial encoder and is required to program access points (when enhanced security mode is enabled).



▼ Enhanced Security Mode

Enable Enhanced Security Mode ☒ YES

Maintenance Unit security password 

To disable enhanced security mode, change the switch to **NO**.

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

For a comprehensive list of requirements and step-by-step instructions to enable enhanced security mode, refer to *Ambiance Enhanced Key Security for Upgrades* (PK3777).

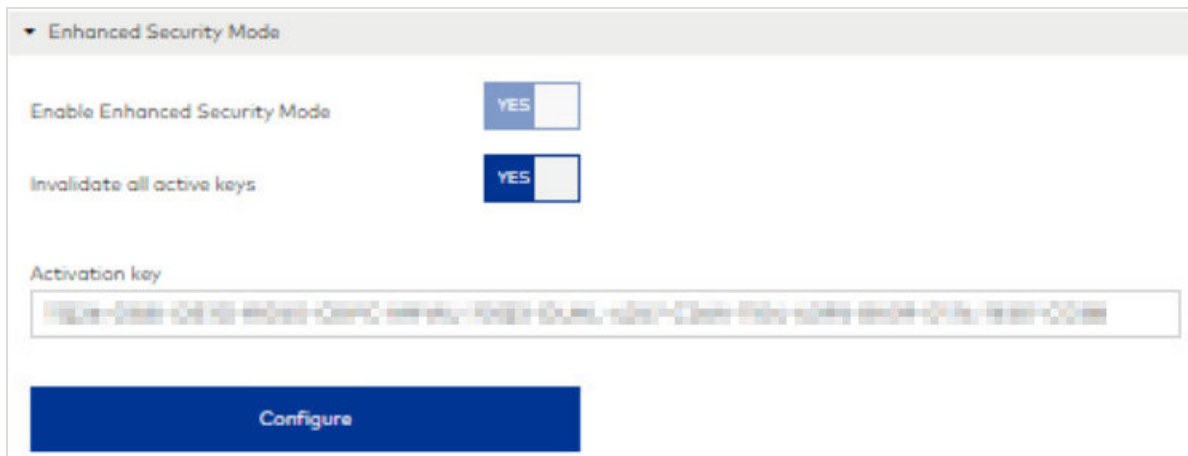


Enabling this option requires specific encoders (part 75720). At least one encoder must be configured before enabling enhanced security mode.



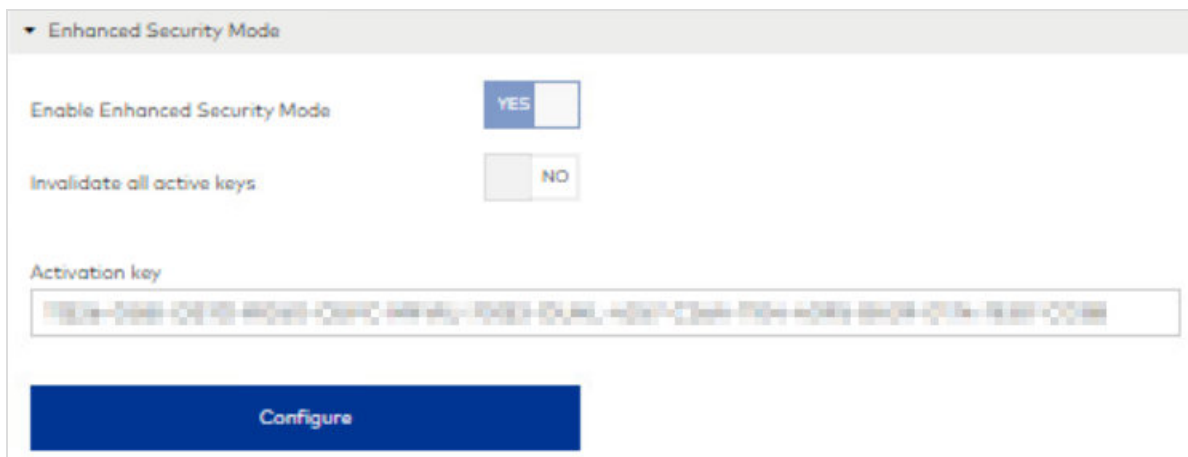
Before enabling enhanced security mode, obtain a valid 64-character activation key from dormakaba Support. Configuration requires that the Ambiance server has access to the internet.

1. Change the [Enhanced Security Mode](#) switch to **YES**. Read the warning and select **YES** to continue.
2. Select whether to invalidate all active keys:
 - **YES**—Select this option to start using enhanced security mode upon reprogramming access points (step 8).



The screenshot shows the 'Enhanced Security Mode' configuration window. It has a title bar with a dropdown arrow and the text 'Enhanced Security Mode'. Below the title bar, there are two settings: 'Enable Enhanced Security Mode' with a blue 'YES' button, and 'Invalidate all active keys' with a blue 'YES' button. Below these settings is a text field for the 'Activation key' containing a 64-character hexadecimal string. At the bottom of the window is a large blue button labeled 'Configure'.

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



The screenshot shows the 'Enhanced Security Mode' configuration window. It has a title bar with a dropdown arrow and the text 'Enhanced Security Mode'. Below the title bar, there are two settings: 'Enable Enhanced Security Mode' with a blue 'YES' button, and 'Invalidate all active keys' with a grey 'NO' button. Below these settings is a text field for the 'Activation key' containing a 64-character hexadecimal string. At the bottom of the window is a large blue button labeled 'Configure'.

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



Enhanced security mode cannot be disabled after clicking [Configure](#).

5. Go to [Programming & Auditing > Programming](#) and reprogram access points. Specify the M-Unit security password when prompted.
 - If all keys were invalidated in step 2, locks accept only enhanced security keys after reprogramming.
 - If keys were not invalidated in step 2, locks accept enhanced security keys and active legacy keys after reprogramming.
6. Go to [System Keys > Failsafe Keys](#) and re-encode Failsafe keys.



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

7. When ready to finalize the transition to enhanced key security, click [Terminate active legacy keys](#).
8. Go to [Programming & Auditing > Programming](#) and reprogram access points again. Specify the M-Unit security password when prompted. After reprogramming, locks accept only enhanced security keys.

Single Sign-On

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

Enabling SSO

Before enabling SSO, establish the following prerequisites:

- Be prepared to log in to your SSO account during the configuration process.
1. To enable SSO, change the [Enable single sign-on](#) switch to **YES**. At present, only the SAML authentication protocol is supported. SAML uses XML to exchange messages.

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

Single Sign-On

To enable single sign-on, please sign in with your single sign-on account credentials. Click CONTINUE to proceed.

ContinueCancel

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

Single Sign-On

Single sign-on has been successfully enabled.
IMPORTANT: To enable other operators to log in, please ensure their single sign-on account is defined in *Staff Management/Operator*.

OK



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

Disabling SSO

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

1. To disable SSO, change the [Enable single sign-on](#) switch to NO.

Revert to standard authentication

You are about to return to standard authentication.

IMPORTANT: After this change, all operators must be redesignated in Staff Management before access is restored.

To continue, please enter your new login credentials.

Username *

Password *

Password confirmation *

Cancel

Save

2. Specify a new login username.
3. Specify and confirm a new password.
4. Click [Save](#).

Information

Single sign-on is now disabled. Operator login credentials saved successfully.

OK

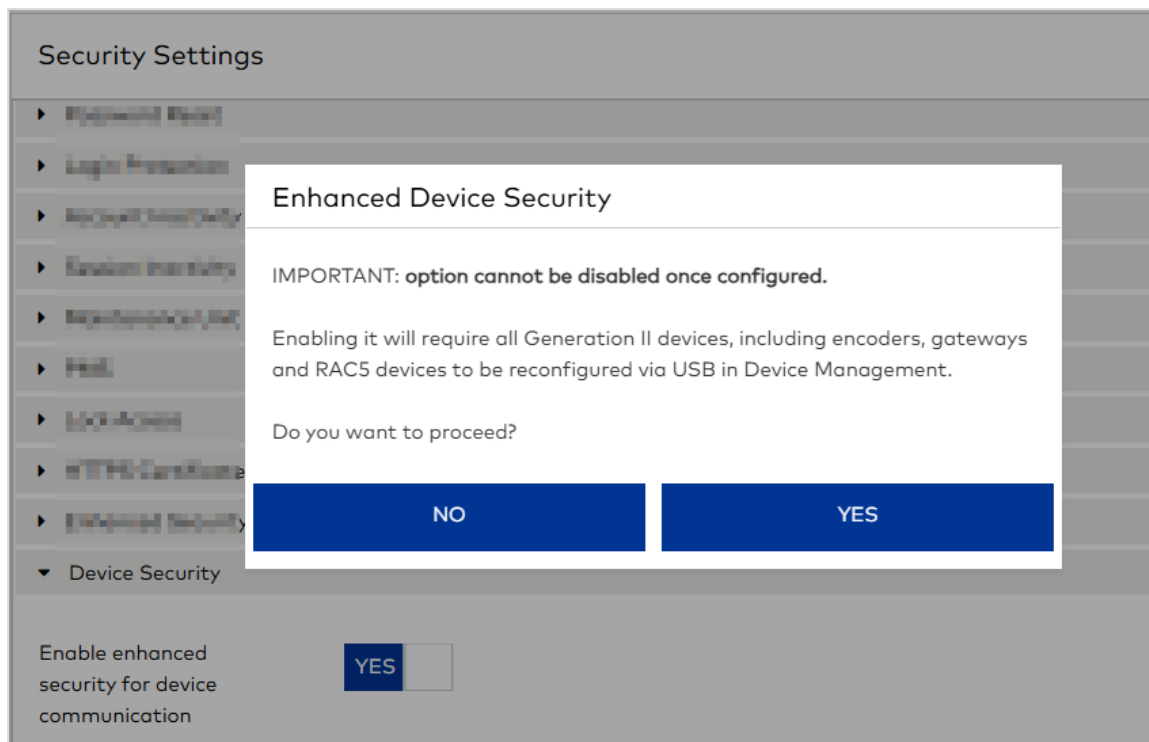


As the operator who reverted to standard authentication, you are now the only operator who can log in to Ambiance. You must now go to Staff Management and re-designate operators.

Device Security

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

1. To enable device security, change the [Enable enhanced security for device communication](#) switch to **YES**.



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

After device security is enabled, Ambiance:

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

Staff Key Settings

Configure system-wide defaults for Staff Keys.

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

Staff Key Settings

Maximum number of times Limited Use keys are valid

- +

Display additional access

YES ☐

2. Specify the number of times a Limited Use Key can be utilized. Default: 6. Valid values: 1-6.
3. 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.
4. 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 to guests in the event of a system or power failure. The recommendation is to create and maintain two sets of three keys for each guest room and suite door. After one set of Failsafe keys is issued and used, make another set of Failsafe keys to replace the used set. Locks only accept keys from the two most recent Failsafe key sets.

Using a Failsafe Key invalidates previous guest key access to guest rooms, suite common doors and suite inner doors.

1. Go to [System Settings > Failsafe Keys](#).

Failsafe Key Settings



Default number of keys

– 3 +

Default stay duration (days)

– 1 +

Default check-out time



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

Key Expiration Settings

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



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

1. Go to [System Settings > Key Expiration](#).

Key Expiration Settings

Search Credential class

☐	Credential class / Key type	Years	months	Days
☐	EMERGENCY (CUSTOM#1)	1	0	0
☐	Electronic Lockout Toggle	1	0	0
☐	Emergency	1	0	0
☐	FLOOR MASTER KEYS	1	0	0
☐	Grand Master	1	0	0
☐	Inhibit	1	0	0
☐	Latch	1	0	0
☐	Limited Use Staff	1	0	0
☒	Master	1	0	0
☐	Toggle Latch/Unlatch	1	0	0
☐	Unlatch	1	0	0
☐	Van Master	1	0	0
☐	Block Keys	1	0	0
☐	Cancel Keys	1	0	0
☐	Resequence Keys	1	0	0
☐	Unblock Keys	1	0	0

Cancel

Edit

Save

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

Set expiration for credential class / key type

Years

—

1

+

months

—

0

+

Days

—

0

+

Cancel

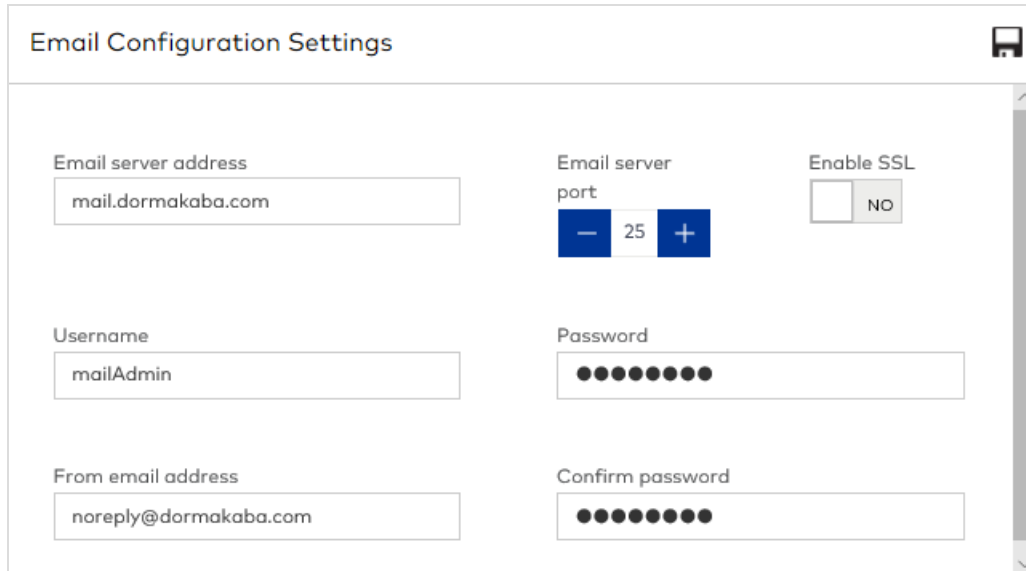
Done

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

Email Configuration Settings

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

1. Go to *System Settings > Email*.



The screenshot shows the 'Email Configuration Settings' form. It has a title bar with the text 'Email Configuration Settings' and a save icon. The form contains several input fields and a checkbox. The 'Email server address' field contains 'mail.dormakaba.com'. The 'Email server port' field is a numeric spinner set to '25'. The 'Enable SSL' checkbox is currently unchecked, with the label 'NO' next to it. The 'Username' field contains 'mailAdmin'. The 'Password' field is masked with ten dots. The 'From email address' field contains 'noreply@dormakaba.com'. The 'Confirm password' field is also masked with ten dots. A vertical scrollbar is visible on the right side of the form.

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

Database backup settings



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

Refer to the following table for backup details.

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



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

Storing backups on a remote server

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

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

On the Ambiance Server:

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

On the remote server:

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



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

Configure backups

Configure scheduled database backups.

1. Go to [Systems Settings > Database Backup](#).

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

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



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

4. General settings:



Perform this task:

☐ Never

☒ Daily

Backup time

3:00 AM 

Days

☒ Su ☒ Mo ☒ Tu ☒ We ☒ Th ☒ Fr ☒ Sa

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

Configure data retention

To configure data retention:

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

The screenshot shows the 'Data retention' configuration window. It includes the following settings:

- Purge every:** A numeric input set to 2, followed by a unit dropdown set to 'weeks'.
- Purge historical guest registrations older than:** A numeric input set to 3, followed by a unit dropdown set to 'Months'.
- Purge system activities older than:** A numeric input set to 3, followed by a unit dropdown set to 'Months'.
- Purge notifications older than:** A numeric input set to 3, followed by a unit dropdown set to 'Months'.
- Enable archiving:** A toggle switch set to 'YES'.
- Archiving directory:** A text input field containing '\\ServerIpOrName\SharedArchiveFolder'.
- Enable purging:** A toggle switch set to 'YES'.

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

Folio Settings

Select a folio format and, depending on the option that you select, define folio options.



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



If an Operator changes the folio data format, all keys encoded with the previous mode cause folio to display as unrecognized format.

To configure a guest folio:

1. Go to [System Settings > Folio](#).

The screenshot shows a web interface for 'Guest folio' settings. A dropdown menu for 'Folio format' is open, displaying three options: 'None' (highlighted in blue), 'Auto-format - room & check-in/out', and 'PMS and/or user interface'.

2. Select the required folio format:
 - [Auto-format - room & check-in/out](#)—MIFARE Ultralight C keys are not supported. 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 guest room and suite 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 define a custom folio layout. There is no limitation to the number of fields, however, the maximum PMS input characters (data and field delimiters) depends on the data format and RFID key type. When mobile keys are enabled, you can also reserve character positions for mobile key folios. Select the data format:
 - Use ASCII data format
 - Use ANSI/ISO BCD data format (1)—Mobile keys are only supported when using the LGS SOAP API protocol. MIFARE Image for PMS encoder 0 requests (LGS SOAP API and LGS REST API only). This format includes the numeric format identifier and padding.
 - Use ANSI/ISO BCD data format (2)—Mobile keys are only supported when using the LGS SOAP API protocol. MIFARE Image for PMS encoder 0 requests (LGS SOAP API and LGS REST API only). This format excludes the numeric format identifier and padding.
3. For each field that you want to add:
 - a. Click [Add field](#).

Add layout field

Name Arcade	Required ☐ NO
Category BOOLEAN	Default value ☐ NO
Special characters !@#\$%^&*0123456789-._+=	Min Char 1
	Max Char 1
Cancel	Done

- b. Configure the following options:
- **Name**—Specify a unique and descriptive name. Valid values: !@#\$%-+=*
 - **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.
 - **Min Char/Max Char**—The total number of characters allowable for PMS input depends on the selected data format and the RFID key type used when making the key. Although the UI allows a maximum of 48 characters for all data formats, characters in excess of the following constraints are truncated:
 - ASCII
 - MIFARE Ultralight C keys: 24
 - MIFARE Plus/MIFARE Classic: 48
 - BCD format 1
 - MIFARE Ultralight C keys: 33
 - MIFARE Plus/MIFARE Classic: 35
 - BCD format 2
 - MIFARE Ultralight C keys: 33 (with limitation)
 - MIFARE Plus/MIFARE Classic: 40

The figure in the following step shows that a total of 3 characters are used. Additional fields in the folio layout may add up to 45 characters for MIFARE Plus/MIFARE Classic keys or 21 characters for MIFARE Ultralight C keys.
- c. When ready, click [Done](#). Repeat this step for each field that you want to define. You can define a maximum of 20 fields.

Guest folio

Folio format

PMS and/or user interface

☒ Use ASCII data format

☐ Use ANSI/ISO BCD data format (1)

☐ Use ANSI/ISO BCD data format (2)

User interface folio layout

Add field

Name	Field type	Special	Min Char	Max Char	Required	Default data	
Parking Gate	BOOLEAN		1	1	YES	0	
Water Park	BOOLEAN		1	1	NO	0	
Arcade	BOOLEAN		1	1	NO	0	

4. (conditional) In the **Mobile key folio masking** section, select which characters of the folio received from the PMS will be sent to the mobile device. For example, if PMS sends folio "123456" and the first three character positions of the folio are selected, "123" folio is sent to the mobile device.

Mobile key folio masking

☐ All

Select PMS folio characters (position) which should be sent to mobile key

☒ 1

☐ 7

☐ 13

☐ 19

☐ 25

☐ 31

☒ 2

☐ 8

☐ 14

☐ 20

☐ 26

☐ 32

☒ 3

☐ 9

☐ 15

☐ 21

☐ 27

☐ 33

☐ 4

☐ 10

☐ 16

☐ 22

☐ 28

☐ 34

☐ 5

☐ 11

☐ 17

☐ 23

☐ 29

☐ 6

☐ 12

☐ 18

☐ 24

☐ 30

5. Click (Save)

PMS Settings

Select the PMS (Property Management System) protocol used by your organization. When you change the selection, the corresponding service restarts automatically.



If you are licensed for online communication, the corresponding service restarts automatically when online features are activated or disabled.

To configure PMS settings:

1. Go to [System Settings > PMS](#).
2. Select and configure the protocol for communication between the PMS and Ambiance Servers.
3. Click [\(Save\)](#)

OPERA

Oracle Outbound API—Ambiance supports the Oracle Outbound API. For detailed configuration instructions, refer to documentation published by Oracle. While there are no integration settings to configure in Ambiance, PMS credentials are required. dormakaba provides the following values for configuration for the OPERA integration:

- **Service Account**—PMS operator login username configured at [Staff Management > operator profile > Operator Info](#) tab.
- **Service Account key**—PMS operator login password configured at [Staff Management > operator profile > Operator Info](#) tab.
- **OAuth Token URL**—Use the following URL to request a token:
 - Request a token by sending an HTTPS POST request to Ambiance web API:
 - `https://Ambiance_IP_address/WebAPI/connect/token`.
 - The request body is x-www-form-urlencoded with the following parameters in key-value form. Request token sample query
`grant_type=password&username={UserName}&password={Password}&client_secret={PMS_Service_Secret}&client_id=\" { \"PMS_Service_ClientId\" } \"&scope=pms_api\", \"offline_access\"`
 - Renewing a token requires only the Content-Type header and the following parameters: client_id, client_secret, refresh_token. Renew token sample query:
`grant_type=refresh_token&client_secret={PMS_Service_Secret}&client_id={PMS_Service_ClientId}&refresh_token=\" { \"RefreshToken\" }`
- **RESTAPI BaseURL / Service Path**—Use the following endpoint:
 - `http://<<Ambiance_IP_address>>:5120/fof/v1/hotels/{ {hotel_id} }/roomKeysOutbound` or `https://<<Ambiance_IP_address>>:5121/fof/v1/hotels/{ {hotel_id} }/roomKeysOutbound`
- **Domain URL for connection with dormakaba**—Specify the address to the Ambiance server.
Example: `https://hostname.com:port#`
 - HTTPS is required.
 - Port 443 is the dormakaba default.
- **Device IP/Encoder Number**—Specify the value configured at [Device Management > Encoders > PMS Encoder ID](#).

For detailed configuration instructions, refer to OPERA outbound integration documentation published by Oracle.

LGS REST API

Use for Web Service connections that use REST requests secured with token-based authentication. When licensed for kiosks, see also [System Settings > Security](#) to manage client certificate authentication.

▼

LGS REST API

Enable LGS REST API

YES

Authentication

Client ID*

Secret key*

Enable key issuance notifications

YES

Key issuance notification callback URL*

- **Enable LGS REST API**—Set this option to **YES**.
 - **Client ID/Secret key**—The unique identifier and unique key used to obtain and renew an authentication token. For Client ID: 32; For Secret key: 6-512 chars.
 - **Enable key issuance notifications**—When set to **YES**, Ambiance sends a notification to the PMS each time a key is created. A separate notification is sent for each key created. Third parties must first register a callback URL and optional security token.
 - **Key issuance notification callback URL**—The callback URL to use for sending notifications.

FIAS

Use FIAS from Oracle for an IP-based connection.

▼

FIAS

TCP/IP port

—

8265

+

Enable shared-with registrations

NO

Return elevator floor access information

NO

- **TCP/IP port**—Specify the TCP/IP port for connecting to the PMS server.
- **Enable shared-with registrations**. When enabled, up to four registrations can share access to one guest room. Check-out dates and the assignment of additional rooms, amenities and floors can be different for each shared-with registration. The shared room (or main room) is established as the first room specified in the original registration. Shared-with registrations must be created (and modified) in the PMS interface.
- **Return elevator floor access information**. If set to **YES** and if encoder=0 in Key Request and Key Modify operations, Ambiance returns the elevator mask bit information in addition to the 17 bytes of access data. Example:\$3AAA...AAA30313241EEE...EEE45463030 where "AAA..." is the 17 bytes access data and "EEE..." is the elevator mask bit data. Default: NO.

04/2026

Ambiance

48

LGS SOAP API

Use for Web Service connections that use SOAP requests. Optionally, enable shared-with registrations. When licensed for kiosks, see also [System Settings > Security](#) to manage client certificate authentication.

▼ LGS SOAP API

Enable shared-with registrations

NO

Enable HTTPS

NO

TCP/IP port

- 80 +

Web Service URL

http://localhost/MessengerPMSWS.asmx

- **Enable shared-with registrations.** When enabled, up to four registrations can share access to one guest room. Check-out dates and the assignment of additional rooms, amenities and floors can be different for each shared-with registration. The shared room (or main room) is established as the first room specified in the original registration. Shared-with registrations must be created (and modified) in the PMS interface.
- Select whether to enable secure communication between Ambiance and the PMS server. Default: NO.
- Specify the port number for communication between Ambiance and the PMS. Defaults: HTTP=80/HTTPS=443.
- The LGS SOAP API URL is a read-only field.

IRS/PRS

IRS/PRS—For IP-based connections, select IRS and specify the TCP/IP port for connecting to the PMS server. For serial port connections, select PRS and specify the following settings:

- **Port**—Communication port on the PMS server used for connecting to the Ambiance Server.
- **Baud**—Transmission speed. Default: 9600.
- **Parity**—Specify whether to use a parity bit, and if using, whether the data character is always odd or even. Default: Even.
- **Data bits**—Specify the number of bits used to represent one data character. Default: 7.
- **Stop bits**—Specify the bit to indicate the end of a data character. Default: 1.
- **Enable expanded key name**—Select whether to extend the key name size from 5 to 15. Default: NO.
- **Enable checksum**—Select whether to perform data validation on communication between the PMS and Ambiance servers. Default: NO.
- **Ignore check-out requests**—If set to YES, Ambiance ignores all check-out requests sent from IRS/PRS. (This setting is not populated by configuration file.) Default: NO.
- **Flow control**—Select the method to control transmission when receiving a message.

IRS/PRS

☒ Enable IRS

TCP/IP port

-

8264

+

☐ Enable PRS

Port

COM1

Baud

9600

Parity

Even

Data bits

-

7

+

Stop bits

-

1

+

Flow control

None

Enable expanded key name

NO

Enable checksum

NO

Ignore check-out requests

NO

LGS REST API (KF2)

REST API (KF2) is for connections using a Web service with REST requests. Settings:

- Select the maximum number of RFID keys per request. Valid values: 1-25. Default: 6.
- Select whether to enable HTTPS for secure communication between the PMS and Ambiance servers. Default: YES. When HTTPS is enabled, go to [System Settings > Security > HTTPS Certificate](#), and set [Enable automatic CAPI store certificate renewal](#) to YES.
- Specify the port number. Default: 9090. The default value is good for both HTTP and HTTPS. After saving the settings, bind the certificate to the port.
- Specify the Web service URL for REST requests.

LGS REST API (KF2)

Maximum RFID keys per request

-

6

+

Enable HTTPS

YES

TCP/IP port

-

9090

+

Web service URL

https://*:9090/

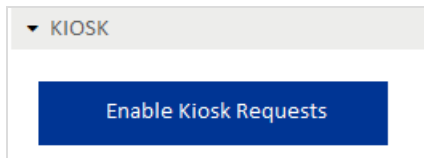
KIOSK

KIOSK is a licensed feature that is disabled by default. Enable/disable kiosk PMS requests. See also [System Settings > Security](#) to manage client certificate authentication.

04/2026

Ambiance

50



Return UID Interface Settings

Ambiance integrates with third-party elevator systems to direct guests and other key holders to the elevator associated with their assigned rooms. The interface type depends on the device/technology where the credential is encoded. Supported key types: MIFARE Classic (Mini/1k/4k), MIFARE Plus; SRK reader does not support MIFARE Ultralight C. Guest keys support single guest/suite room only because only one floor can be sent to the elevator interface.

1. Go to *System Settings > Return UID Interface*.

The screenshot shows the 'Return UID Interface Settings' configuration page. At the top, there is a toggle switch for 'Enable return UID interface' set to 'YES'. Below this is a 'Mode' section with two radio button options: 'Use virtual UID' and 'Use RFID card UID', with the latter being selected. Underneath is a 'Communication settings' section. It contains two radio button options: 'TCP/IP address' (selected) and 'Server name'. Below these are input fields for 'TCP/IP address *' (containing 'xxx.xxx.xxx.xxx') and 'TCP/IP port' (a numeric spinner set to '4040').

- **Virtual UID**—Select this type when the credential is encoded on a device that uses a device/technology other than RFID (such as mobile keys).
- **RFID UID**—Select this type when the credential is encoded on a device that uses RFID technology (such as physical keys made in Ambiance).
- **TCP/IP address/servername**—Specify the TCP/IP address and port number or server name of the elevator system. Defaults: 4040/xxx.xxx.xxx.xxx. Valid ports: 0-65535

Staff key validation settings

Configure staff key validator device settings.

Staff Key Validator Settings

Device settings

PIN length

-
7
+

Enable access tracking read back

YES

Validation period before shift starts (minutes)

-
15
+

Display language

English

Validation period after shift starts (minutes)

-
30
+

Staff profile settings

Enable key validation for new staff members

YES

Enable overtime for new staff members

NO

Default overtime (hours)

-
1
+

- Go to [System Settings > Staff Key Validator](#).
- Configure device settings:
 - PIN length**—Select the number of digits for PIN codes. Valid range: 4-7. Default: 7. Modifying this setting after the Staff Key Validator is in use requires all staff members subject to staff key validation to create new PINs.
 - Validation period before shift starts (minutes)**—Select the number of minutes before the start of a shift that staff members can validate their key at an access point (thereby gaining access). Valid range: 15-60. Default: 15. See also [Access Management > Shift Schedules](#).
 - Validation period after shift starts (minutes)**—Select the number of minutes after the start of a shift that staff members can validate their key at an access point (thereby gaining access). Valid range: 30-180. Default: 30. See also [Access Management > Shift Schedules](#).
 - Display language**—Select the language for the staff key validator device interface. Default: English.
 - Enable access tracking read back**—Select whether to YES/NO switch. Default: YES. When enabled, 12 months of access tracking is retained.
- Configure staff profile settings:
 - Enable key validation for new staff members**—Select whether all new staff members are required to validate keys at access points where a staff key validator device is installed. Default: YES
 - Enable overtime for new staff members**—When YES, the validation period before shift starts Default: NO

- **Default overtime (hours)**—Select the number of hours in a given day that overtime is authorized for staff members. Range: 1-16 hours. Default: 1.

4. Click **(Save)** .

Advanced Settings

To configure advanced settings:

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

Guest Pre-Registration

▼ Guest pre-registration

Pre-registered sequence numbers to skip (per day)

—

2

+

Pre-registered duplicate IDs to skip (per day)

—

2

+

- 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).
- 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.
- Click (Save) .

RFID key types

If displayed, click the [Information](#) button in this section to read the security advisory.



dormakaba recommends upgrading to MIFARE Ultralight AES for increased security.

Enhanced Key Security enabled

▼ RFID key types

Enhanced Key Security

☒ MIFARE DESFire EV2/EV3

☒ MIFARE Ultralight AES

☒ MIFARE Ultralight C

☒ MIFARE Plus

Standard Key Security

☐ MIFARE DESFire EV2/EV3

☐ MIFARE Ultralight C

Legacy Key Security

☐ MIFARE Plus

Enhanced Key Security disabled

RFID key types

Enhanced Key Security

- ☒ MIFARE DESFire EV2/EV3
- ☐ MIFARE Ultralight AES
- ☐ MIFARE Ultralight C
- ☐ MIFARE Plus

Standard Key Security

- ☒ MIFARE DESFire EV2/EV3
- ☒ MIFARE Ultralight C

Legacy Key Security

- ☐ MIFARE Plus

Information



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

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

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

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

- **Guest keys**—All access points more than one is considered additional.
- **Staff keys**—All access points that are added at key-encoding time (excluding the access points assigned to the selected credential) are considered additional.

Key technology limits for additional access points:

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

Mobile keys

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



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



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

MATRIX

MATRIX integration is a licensed feature that is disabled by default. If the Ambiance deployment is connecting with a MATRIX web server, set the soft-switch to **YES**.

Online communication

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

If the Ambiance deployment is licensed for Remote Lock Management, set the soft-switch to **YES**. For more information, see [Remote Lock Management](#).

Keyscan Aurora

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

Licensing Settings

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

1. Go to *System Settings > Licensing*.

Licensing

Activation key

XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX

Activated licenses:

- Mobile Keys
- AuroraSync
- Emergency Keys
- Online
- VIP Guest Registrations
- Kiosk
- PPK/SPK Storage
- Single Sign-On (SSO)
- Staff Key Validation

2. Specify a valid activation key.

3. Click (Save) .

Activated licenses are displayed.

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

Step 2

Build Your Property

This section includes the following subjects:

Learning about Property Builder	60
Add buildings	66
Add floors	68
Add guest rooms	71
Add suites	77
Add foyer doors	82
Associate access points to foyer door	84
Add guest common areas	86
Add staff common areas	92
Add meeting rooms	98
Add restricted areas	101
Add elevators	104

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

Ambiance supports a maximum of 8,192 access points per site of which 4,095 may be for guest access point types (guest rooms, foyer doors, and suites).

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

- **Guest Room**—An access point assigned to a guest during guest registration.
- **Suite**—An access point that is a connected series of guest rooms including a common door and one or more inner door access points.
- **Foyer Door**—An access point that is a common door to associated guest rooms and suites. Access to the individual guest rooms and suites is managed independently.
- **Restricted Area**—An access point type intended for staff only for back-of-the-house access. For example, the Electrical Room would be a restricted area.
- **Meeting Room**—An access point type 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 Area**—An access point type where general access is configured for guests. Access may be unlimited or limited.
- **Staff Common Area**—An access point where general access is configured for staff. Access may be unlimited (for staff) or limited.
- **Elevator**—An access point that provides access to building floors. An elevator bank is a group of elevators that share the same floor mapping.

Configuring floors and access points

During the process of adding floors and access points in Property Builder, the access point names that you will see in 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. Valid alphanumeric characters: A-Z, 0-9. Valid special characters: -#%!=,,:_()?*'<>/+.

Name formats

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

Likewise, access point names are formed the same way with an additional option to format the name using numbers or text. Some access point types, such as common areas, are more suitable for using the text format, *Lobby* for example. If you use the number format, the floor number and 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.

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.

Batch access point creation

To facilitate quick setup, Ambiance allows batch creation of guest rooms, restricted areas, and meeting rooms. You can add multiple access points 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.

Include in mobile keys download file

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

Lock models

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

Ambiance supports the following lock models:

- [Saflock Quantum/Saflok Confidant and Confidant NFC/Saflok RT, Saflok RT+/RCU \(Remote Controller Unit\)/Pixel and Pixel+/Saffire LX \(L, M & P\)](#)
- [Saffire LX \(D & I\)/Saflok MT](#)
- [RAC5 XT and RAC5 Lite](#)— RAC5 XT is for online systems; RAC5 Lite does not support Remote Lock Management. Each RAC5 XT device can be mapped to a single access point or two different access points. Manually configure the number of access points to map by modifying the **DEVICES** switch on each RAC5 XT device. For more information, refer to RAC5 documentation.



All lock models for Guest Room, Suite Common Door and Suite Inner Door, and Foyer 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 all access points).

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.



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

Unlimited 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.

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

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 access by staff/vendors, such as an office, kitchen area, and supply closets. When you create a Staff Common Area access point, you have the option to enable limited access.



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

Unlimited staff common areas

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

Limited-access staff common areas

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

- limit access based on credential—access must be configured in [Access Management > Credential Management](#).
- limit access based on common area access profile—access must be configured in [Access Management > Common Area Access](#).

When creating the limited common area, you must also select a common area ID. The ID is a numeric value used by the system to synchronize with third-party PMS (Application Programming Interface) settings. The limit is 12 which includes IDs for limited common areas and elevators.

Elevators

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

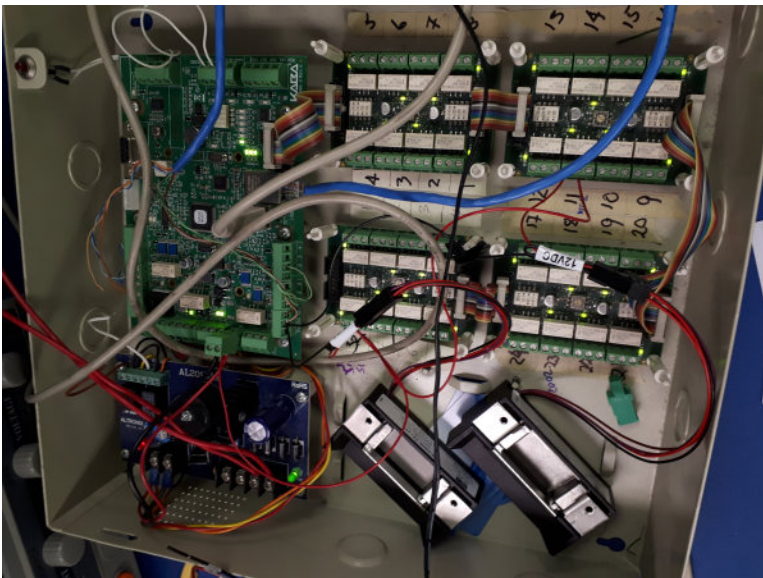
Floor mapping

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:

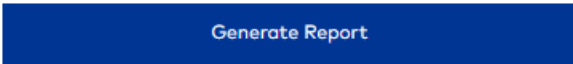
- [EMCC - Expanded Multi-Channel Controller](#)—Eight panels with 16 relays per panel.
- [MCC 12 - Multi-Channel Controller](#) (Legacy mode supported)—One panel with 12 relays.
- [MCC 8 - Multi-Channel Controller](#) (Legacy mode supported)—One panel with 8 relays.
- [ECU - Elevator Controller Unit](#)—One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

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



The relays on three of the panels are labeled 1-24. When mapping floor access in 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.

Elevator Bank: North Elevator		 
Floor	Panel / Relay - Standard Floor Access	
 FLOOR0	P1R1	
 FLOOR1	P1R2	
 FLOOR2	P1R3	
 FLOOR3	P1R4	
 FLOOR4	P1R5	
 FLOOR5	P1R6	
 FLOOR6	P1R7	
 FLOOR7	P1R8	
 FLOOR8	P1R9	
 FLOOR9	P1R10	
 FLOOR10	P1R11	
		

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.



When the licensed feature VIP Guest Registration is enabled and the selected elevator controller is RAC5, VIP floor mapping can be configured to automatically enable the relay associated with the floor where the VIP guest room / suite is located. For example, when a VIP guest lodging on Floor 10 presents their key to the elevator reader, the elevator automatically opens on Floor 10 without requiring the guest to select a Floor option.

The following figure shows floor mapping when VIP Guest Registration is enabled and the control panel is RAC5.

Elevators

ElevatorBank1

RACS - Remote Access

Elevator1

1 Reader(s): Elevator1

Panel 1

P1R1

P1R2

P1R3

P1R4

P1R5

P1R6

P1R7

P1R8

Panel 2

Panel 3

Panel 4

Panel 5

Panel 6

Panel 7

Panel 8

Elevator Bank: ElevatorBank1

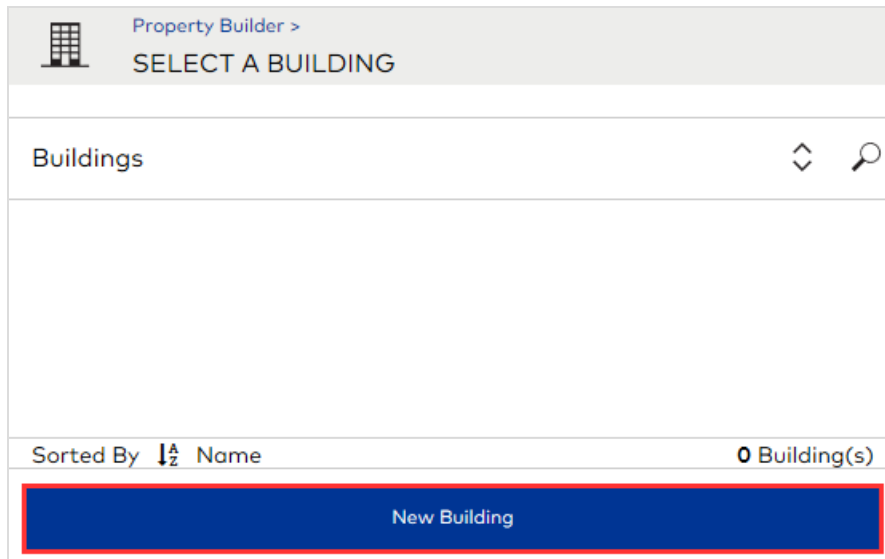
Floor	Panel / Relay - Standard Floor Access	Panel / Relay - VIP Floor Access
FLOOR1	P1R1 X	
FLOOR2	P1R1 X	
FLOOR3	P1R1 X	
FLOOR4	P1R2 X	
FLOOR5	P1R3 X	
FLOOR6	P1R4 X	
FLOOR7	P1R5 X	
FLOOR8	P1R6 X	
FLOOR9	P1R7 X	
FLOOR10	P1R1 X	P1R8 X

Add buildings

Buildings are the independent structures on your site.

To add buildings:

1. Go to [Property Builder](#).



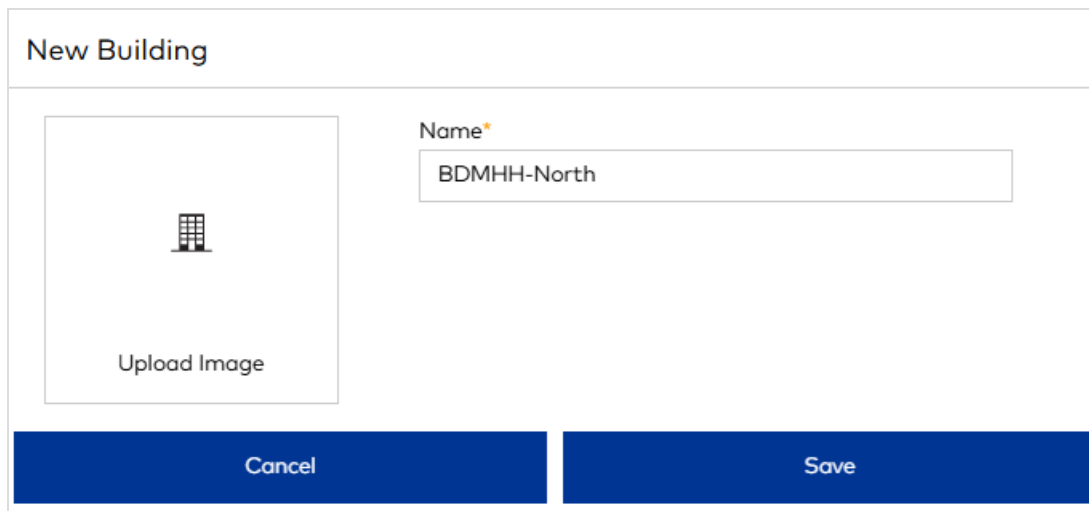
Property Builder >
SELECT A BUILDING

Buildings

Sorted By Name 0 Building(s)

New Building

2. Click New Building.



New Building

Upload Image

Name*
BDMHH-North

Cancel Save

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.

Buildings

▼ B

BDMHH-North

...

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.

Buildings

B

BDMHH-North

Sorted By 1 Building(s)

New Building

Summary

Building

BDMHH-North

0 Floor(s)

0 Access Point(s)

Floors & Access Points

Elevators

- 3. Click [Floors & Access Points](#).

Access Points

Name

Type

Lock profile

No items to display

Sort By Name

0 Access Point(s)

Back to Buildings

New Floors

Delete Access Points

- 4. Click [New Floors](#).

Create Floors

Floor

Advanced Format

From

–

0

+

To

–

9

+

Description:

Description

Preview

10 Floor(s)

FLOOR0, FLOOR1, FLOOR2, FLOOR3, FLOOR4...

Cancel

Save

- 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.
- (optional) Add a description for the floor or range of floors.
- (optional) Specify any of the following options on the [Advanced Format](#) tab:

Create Floors

Floor

Advanced Format

FLOOR

n

nn

nnn

None

Suffix

Above existing floors

Below existing floors

Preview

10 Floor(s)

FLOOR0, FLOOR1, FLOOR2, FLOOR3, FLOOR4...

Cancel

Save

- **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).
- Click **Save**.

Access Points

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

0

100

No items to display

Sort By

Name

0 Access Point(s)

Back to Buildings

New Floors

Delete Access Points

Add guest rooms

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



To import guest room access point types, see [Import guest rooms list](#).

To add guest rooms:

1. Go to [Property Builder](#).
2. Select a building.
3. Click [Floors & Access Points](#).

Summary

Select Access Point(s)

New Access Points

4. Click [New Access Points](#).

Create Access Points

Guest Room
Suite
Foyer Door
Restricted Area
Meeting Room
Guest Common Area
Staff Common Area

Cancel

Next

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

Create Access Point: Guest Room

Access Point

Advanced Format

Prefix

Prefix

Floor number format

n

nn

nnn

None

Separator text

Separator text

Room number format

n

nn

nnn

None

Suffix

Suffix

Preview

10 Access Point(s)

301, 302, 303...

Back to Type Selection

Cancel

Save

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

Access Points

☐	Name	Type	Lock profile
▼ ☐	FLOOR1 (0 Access Point(s))		...
▼ ☐	FLOOR2 (0 Access Point(s))		...
▶ ☐	FLOOR3 (10 Access Point(s))		...
▶ ☐	FLOOR4 (10 Access Point(s))		...
▶ ☐	FLOOR5 (10 Access Point(s))		...
▶ ☐	FLOOR6 (10 Access Point(s))		...
▶ ☐	FLOOR7 (10 Access Point(s))		...
▶ ☐	FLOOR8 (10 Access Point(s))		...
▶ ☐	FLOOR9 (10 Access Point(s))		...

⏮

⏪

1

⏩

⏭

100 ▼

1 - 70 of 70 items

Sort By Name

70 Access Point(s)

Back to Buildings

New Floors

Delete Access Points

Import guest rooms list

This menu option is only available when the *Import access point list* system right is enabled in *Role Management > Property Builder*.

To import a guest room list:

1. Prepare the data file.
2. Go to [Property Builder](#).
3. For the building where you want to add guest rooms, [\(More\)...](#) > [Import Access Point List](#).
4. Navigate to and select the file that you want to import, then click [Open](#). Supported files type: csv. The following figures show valid csv file formats. The following rules apply:
 - The file type must be .csv (.csv UTF-8 for non-English languages).
 - ACCESSPOINT is required.
 - The floor *Unknown* is created for any access point that does not have a designated floor.
 - If the floor name in the csv file does not exist, the floor is created.
 - If the floor name in the csv file is an exact match to an existing floor name, the access point is added to the existing floor.

The screenshot shows an Excel spreadsheet with the following data:

	A	B	C
1	ACCESS POINT	FLOOR	
2	100	Floor1	
3	101	Floor1	
4	102	Floor1	
5	103	Floor1	
6	104	Floor1	
7	105	Floor1	
8	200	Floor2	
9	201	Floor2	
10	202	Floor2	
11	203	Floor2	
12	204	Floor2	
13	205	Floor2	

A red box labeled "Required" points to the "ACCESS POINT" header in cell A1. The Notepad window shows the following CSV data:

```
notepadimport1.csv - Notepad
File Edit Format View Help
apNotepadA,apNotepadFloor
apNotepadB,apNotepadFloor
apNotepadC,apNotepadFloor
apNotepadD,apNotepadFloor
apNotepadE,apNotepadFloor
```



If rooms have already been created, you are prompted to proceed. Click [YES](#) to proceed.

5. When prompted, select a lock profile for the access points.
6. When notified the import is successful, click [OK](#). The following figure shows the import of access points using the .csv created in Notepad.

Access Points

<

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](#).

Create Access Points

Guest Room

Suite

Foyer Door

Restricted Area

Meeting Room

Guest Common Area

Staff Common Area

Cancel

Next

- 5. Select [Suite](#), then click [Next](#). The first options that you define are for the Common Door.

Create Access Points: Suite

Access Point - Common Door

Advanced Format - Common Door

Floors *

FLOOR3 x

Lock profile

Saflok Quantum ▼

☒ Include in mobile keys download file

Format

Number ▼

Access Point number

—

1

+

Description

Description

Common door preview

301

Back to Type Selection

Cancel

Next to Inner Doors

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

If you plan to implement Folios using the Auto-Format option, then all suite access points site-wide must be numeric only.
-
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:

Create Access Points: Suite

Access Point - Common Door

Advanced Format - Common Door

Prefix

S-

Floor number format

n

nn

nnn

None

Separator text

Separator text

Room number format

n

nn

nnn

None

Suffix

Suffix

Common door preview

S-301

Back to Type Selection

Cancel

Next to Inner Doors

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

Create Access Points: Suite

Access Point - Inner Door

Advanced Format - Inner Door

Lock profile

Saflok Quantum

☒ Include in mobile keys download file

Format

Alphabetical

From

— A +

To

— B +

Description

Description

Suite preview

S-301 (301A, 301B)

Back to Common Door

Cancel

Save

14. For **Lock profile**, select the lock model.
15. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
16. For **Format**, select whether to identify the access points using alphabetic characters, numbers, or text. If using letters or numbers, specify the range of access points to add; and, if adding more than one access point, select a numbering pattern for incrementing numbers.
17. (*optional*) Add a description for the access point or range of access points.
18. (*optional*) If you selected to format access point names using alphabetic characters or numbers, specify any of the following options on the **Advanced Format** tab:

Create Access Points: Suite

Access Point - Inner Door

Advanced Format - Inner Door

Prefix

Prefix

Separator text

Separator text

Suffix

Suffix

Suite preview

S-301 (301A, 301B)

Back to Common Door

Cancel

Save

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

19. Click **Save**.

Access Points

☐	Name	Type	Lock profile
☐	S-301	Suite	...
☐	S-301	Suite Common Door	Saflok Quantum ...
☐	301A	Suite Inner Door	Saflok Quantum ...
☐	301B	Suite Inner Door	Saflok Quantum ...

Add foyer doors

A Foyer Door is an access point type that serves as a common door for access to guest rooms and suites associated with the door.

To add foyer doors:

1. Go to [Property Builder](#).
2. Select a building.
3. Click [Floors & Access Points](#).
4. Click [New Access Points](#).

Create Access Points

Guest Room

Suite

Foyer Door

Restricted Area

Meeting Room

Guest Common Area

Staff Common Area

Cancel Next

5. Select [Foyer Door](#), then click [Next](#).

Create Access Point: Foyer Door

Floors * Lock profile

FLOOR1 Saflok Quantum

Access point name *

Day Camp

Include in mobile keys download file YES ☐

Back to Type Selection Cancel Save

6. Select the floor where you want to add the Foyer Door.
7. Select the lock model.
8. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.

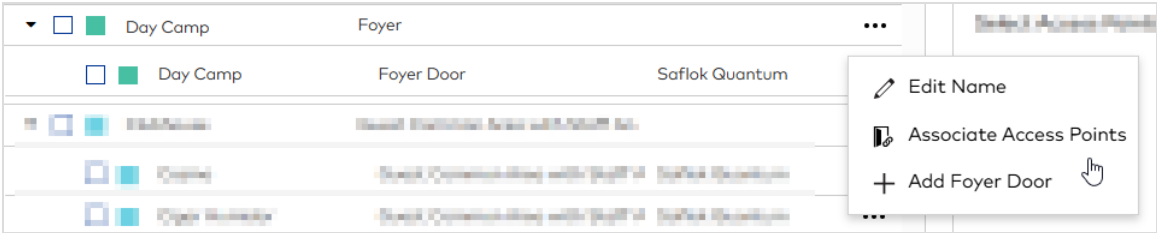
9. Specify a descriptive name for the access point.
10. [Include in mobile keys download file](#)—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
11. Click [Save](#).

Associate access points to foyer door

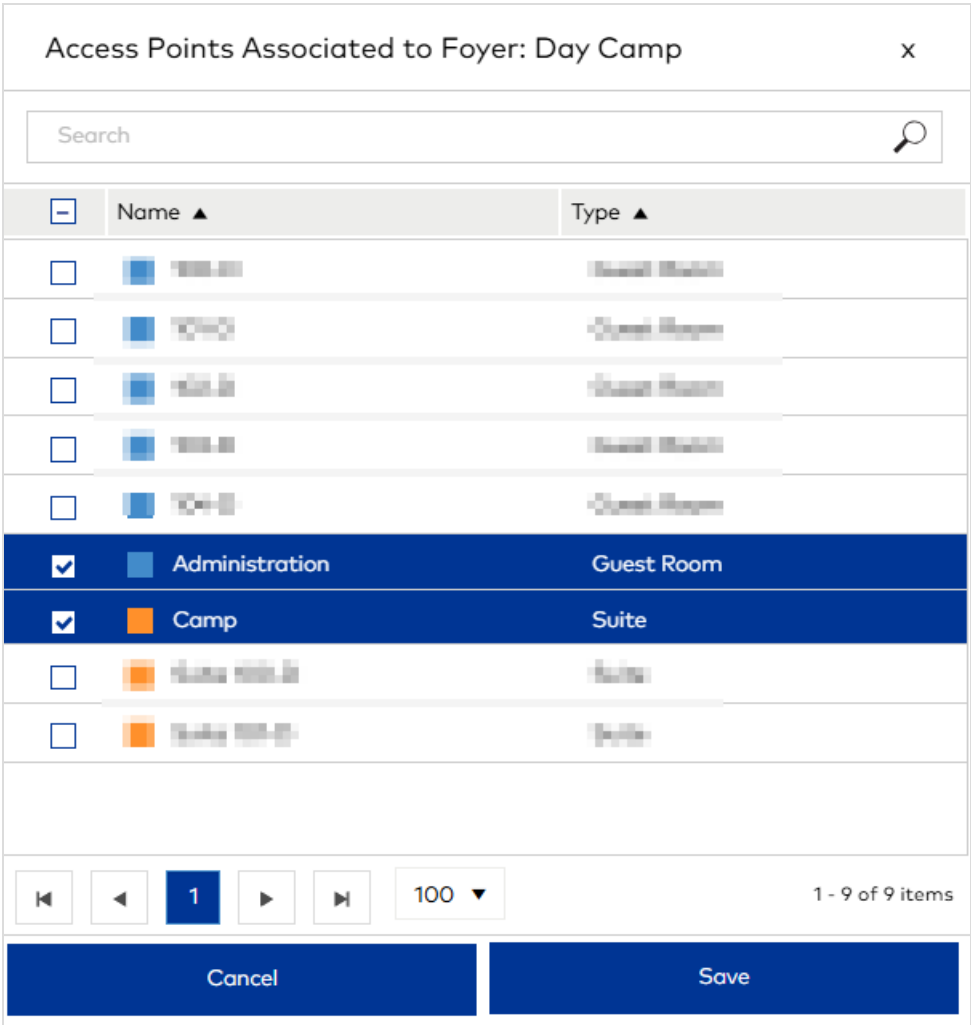
A Foyer Door is an access point type that serves as a common door for access to guest rooms and suites associated with the door.

To associate or disassociate guest rooms and suites to a foyer door:

- 1. Go to [Property Builder](#).
- 2. Select a building.
- 3. Click [Floors & Access Points](#).
- 4. For the Foyer Door that you want to work with, click **...** (More) > [Associate Access Points](#).



- 5. Select access points to associated with the Foyer Door. Deselect access points to disassociate from the Foyer Door.



6. When ready, click [Save](#). The selected access points now display subordinate to the Foyer Door. The deselected access points display at the root level of the assigned floor.

▼	☐	☒	Day Camp	Foyer		...
	☐	☒	Day Camp	Foyer Door	Saflok Quantum	...
	☐	☒	Administration	Guest Room	Saflok Quantum	...
▼	☐	☒	Camp	Suite		...
	☐	☒	Camp	Suite Common Door	Saflok Quantum	...
	☐	☒	CampA	Suite Inner Door	Saflok Quantum	...
	☐	☒	CampB	Suite Inner Door	Saflok Quantum	...

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."

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](#).

Create Access Points

Guest Room

Suite

Foyer Door

Restricted Area

Meeting Room

Guest Common Area

Staff Common Area

Cancel

Next

5. Select [Guest Common Area](#), then click [Next](#).

Create Access Points: Guest Common Area

Access Point

Advanced Format

Floors *

FLOOR1 x

Common area name*

Guest Lounge

☐ Enable limited access

Enable staff access by

☒ Credential assignment
 ☐ Common area access profile assignment

Lock profile

Saflok Quantum ▼

☒ Include in mobile keys download file

Format

Text ▼

Description

Description

Access point name*

Guest Lounge

Preview

1 Access Point(s)

Guest Lounge

Back to Type Selection

Cancel

Save

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 can be implicitly accessed 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. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
 11. [Include in mobile keys download file](#)—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
 12. For [Format](#), select whether to identify the access points using numbers or text.
 - If you select [Number](#), specify the range of access points to add and, if adding more than one access point, select a numbering pattern for incrementing the numbers.
 - If you select [Text](#), specify a unique access point name.
 13. (*optional*) Add a description for the access point or range of access points.
 14. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the [Advanced Format](#) tab:
 - [Prefix](#)—Specify the text to display before the main number. Include spaces where appropriate.
 - [Separator text](#)—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
 - [Suffix](#)—Specify the text to display after the main number. Include spaces where appropriate.
 - [Floor number format](#)—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select [n](#) for 1, [nn](#) for 01, [nnn](#) for 001. To hide the floor number in the access point name, select [None](#).
 - [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](#).
 15. Click [Save](#).

Access Points ↕ 🔍			
☐	Name	Type	Lock profile
▼ ☐	FLOOR1 (3 Access Point(s))		...
☐	 Conference Room	Meeting Room	Saflok Quantum ...
▼ ☐	 Guest Lounge	Guest Common Area Group	...
☐	 Guest Lounge	Guest Common Area	Saflok Quantum ...
☐	 IT Office	Restricted Area	Saflok Quantum ...

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](#).

Create Access Points: Guest Common Area

Access Point

Advanced Format

Floors *

FLOOR1 x

Common area name *

Pool

☒ Enable limited access

Enable staff access by

☐ Credential assignment
 ☒ Common area access profile assignment

Common area ID

12

Lock profile

Saflok Quantum

☒ Include in mobile keys download file

Format

Text

Description

Description

Access point name *

Pool

Preview

1 Access Point(s)

Back to Type Selection

Cancel

Save

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. For **Common area ID**, accept the value that the system automatically populates.
11. For **Lock profile**, select the lock model.

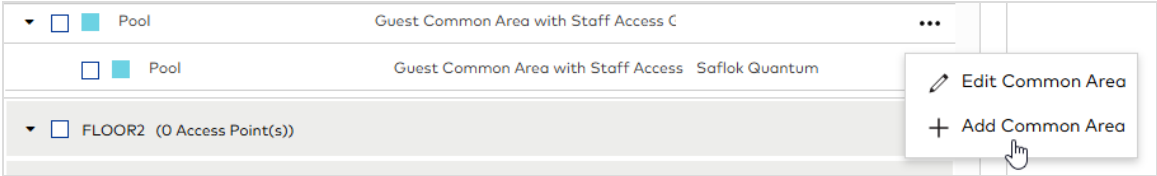
12. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
13. [Include in mobile keys download file](#)—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
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.
 - [Separator text](#)—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
 - [Suffix](#)—Specify the text to display after the main number. Include spaces where appropriate.
 - [Floor number format](#)—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select [n](#) for 1, [nn](#) for 01, [nnn](#) for 001. To hide the floor number in the access point name, select [None](#).
 - [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](#).

Access Points			
☐	Name	Type	Lock profile
▼ ☐	FLOOR1 (4 Access Point(s))		...
☐	Conference Room	Meeting Room	Saflok Quantum
▼ ☐	Guest Lounge	Guest Common Area Group	...
☐	Guest Lounge	Guest Common Area	Saflok Quantum
☐	IT Office	Restricted Area	Saflok Quantum
▼ ☐	Pool	Guest Common Area with Staff Access C	...
☐	Pool	Guest Common Area with Staff Access	Saflok Quantum

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*.

Add Common Area

Common area name

Lap Pool

Lock profile

Saflok Quantum

☒ Include in mobile keys download file

Cancel

Save

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

Access Points				
☐	Name	Type	Lock profile	
☐	Pool	Guest Common Area with Staff Access C		...
☐	Lap Pool	Guest Common Area with Staff Access	Saflok Quantum	...
☐	Pool	Guest Common Area with Staff Access	Saflok Quantum	...

Add staff common areas

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

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

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

- [Adding Unlimited Staff Common Areas](#)
- [Adding Limited-Access Staff Common Areas](#)
- [Adding Common Areas to Common Area Groups](#)

Adding unlimited staff common areas

Unlimited staff common areas are added to every staff key.

1. Go to [Property Builder](#).
2. Select a building.
3. Click [Floors & Access Points](#).
4. Click [New Access Points](#).

Create Access Points
Guest Room
Suite
Foyer Door
Restricted Area
Meeting Room
Guest Common Area
Staff Common Area
Cancel Next

5. Select [Staff Common Area](#), then click [Next](#).

Create Access Points: Staff Common Area

Access Point

Advanced Format

Floors *

FLOOR0 x

Common area name *

Staff Lounge

☐ Enable limited access

Lock profile

Saffire LX

Format

Text

Description

Description

Access point name *

Staff Lounge

Preview

1 Access Point(s)

Staff Lounge

Back to Type Selection

Cancel

Save

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

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

▼ ☐ ☒ Staff Lounge	Staff Common Area Group	...
☐ ☒ Staff Lounge	Staff Common Area	Saffire LX

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](#).

Create Access Points: Staff Common Area

Access Point

Advanced Format

Floors *

FLOOR1 x

Common area name*

Kitchen

☒ Enable limited access

Common area ID : 2

Lock profile

Saffire LX ▼

Format

Text ▼

Description

Description

Access point name*

Kitchen

Preview

1 Access Point(s)

Kitchen

Back to Type Selection

Cancel

Save

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

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

▼ ☐ ☒ Kitchen	Staff Common Area Group	...
☐ ☒ Kitchen	Staff Common Area	Saffire LX ...

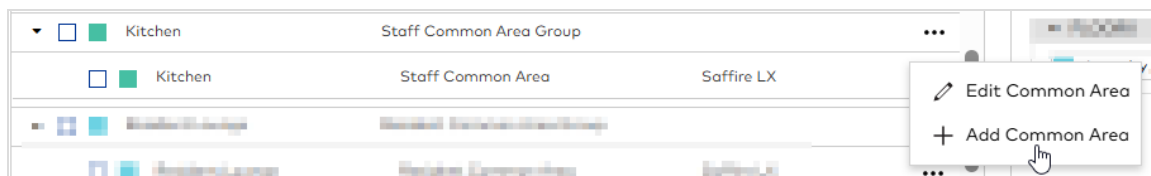


Before staff can be issued a key that authorizes access to limited-access staff common areas, you must either add the common area to the assigned staff credential or associate the common area with the assigned staff credential in [Access Management > Common Area Access](#).

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](#).

Add Common Area

Common area name

Lock profile
 ▼

4. Specify a unique name for the common area.
5. For [Lock profile](#), select the lock model.

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

▼ ☐ ☒ Kitchen	Staff Common Area Group	...
☐ ☒ Kitchen	Staff Common Area	Saffire LX
☐ ☒ Supply Closet	Staff Common Area	Saffire LX

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 one or more floors where you want add the access points.
5. Click [New Access Points](#).

Create Access Points	
Guest Room	
Suite	
Foyer Door	
Restricted Area	
Meeting Room	
Guest Common Area	
Staff Common Area	
Cancel	Next

6. Select [Meeting Room](#), then click [Next](#).

Create Access Point: Meeting Room

Access Point

Advanced Format

Floors *

FLOOR1 x

Lock profile

Saflok Quantum ▼

☒ Include in mobile keys download file

Format

Text ▼

Description

Description

Access point name *

Conference Room

Preview

1 Access Point(s)

Conference Room

Back to Type Selection

Cancel

Save

7. For [Lock profile](#), select the lock model.
8. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
9. [Include in mobile keys download file](#)—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
10. For [Format](#), select whether to identify the access points using numbers or text.
 - If you select [Number](#), specify the range of access points to add and, if adding more than one access point, select a numbering pattern to use how to increment the numbers.
 - If you select [Text](#), specify a unique access point name.
11. (*optional*) Add a description for the access point or range of access points.
12. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the [Advanced Format](#) tab:
 - [Prefix](#)—Specify the text to display before the main number. Include spaces where appropriate.
 - [Separator text](#)—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
 - [Suffix](#)—Specify the text to display after the main number. Include spaces where appropriate.
 - [Floor number format](#)—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select [n](#) for 1, [nn](#) for 01, [nnn](#) for 001. To hide the floor number in the access point name, select [None](#).

- **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**.

Access Points				
☐	Name	Type	Lock profile	
▼ ☐	FLOOR1 (2 Access Point(s))			...
☐	Conference Room	Meeting Room	Saflok Quantum	...

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](#).

Create Access Points

Guest Room

Suite

Foyer Door

Restricted Area

Meeting Room

Guest Common Area

Staff Common Area

Cancel

Next

- 5. Select [Restricted Area](#), then click [Next](#).

Create Access Point: Restricted Area

Access Point

Advanced Format

Floors *

FLOOR1 x

Lock profile

Saflok Quantum ▼

☒ Include in mobile keys download file

Format

Text ▼

Description

Description

Access point name *

Electrical Room

Preview

1 Access Point(s)

Electrical Room

Back to Type Selection

Cancel

Save

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. (RAC5 devices only) Select the sound level of the audible beeps when the device is connected to the workstation and when keys are made. Default: High.
9. **Include in mobile keys download file**—(*optional*) When licensed for mobile keys, select this option if the lock is equipped to accept mobile key credentials. By selecting the option, the access point is listed in the mobile keys download file, a report generated from the Buildings context menu in Property Builder. This option is informational only and has no impact on the mobile key feature.
10. For **Format**—Select whether to identify the access points using numbers or text.
 - If you select **Number**, specify the range of access points to add and, if adding more than one access point, select a numbering pattern to use how to increment the numbers.
 - If you select **Text**, specify a unique access point name.
11. (*optional*) Add a description for the access point or range of access points.
12. (*optional*) If you selected to format access point names using numbers, specify any of the following options on the **Advanced Format** tab:
 - **Prefix**—Specify the text to display before the main number. Include spaces where appropriate.
 - **Separator text**—Specify the text to display between the floor number and access point number. Include spaces where appropriate.
 - **Suffix**—Specify the text to display after the main number. Include spaces where appropriate.

- **Floor number format**—Select how many digit positions to display for floor numbers. Leading zeros occur before the first non-zero digit. For example, select **n** for 1, **nn** for 01, **nnn** for 001. To hide the floor number in the access point name, select **None**.
- **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**.

☐	☒	Electrical Room	Restricted Area	Saflok Quantum	...
--------------------------	-------------------------------------	-----------------	-----------------	----------------	-----

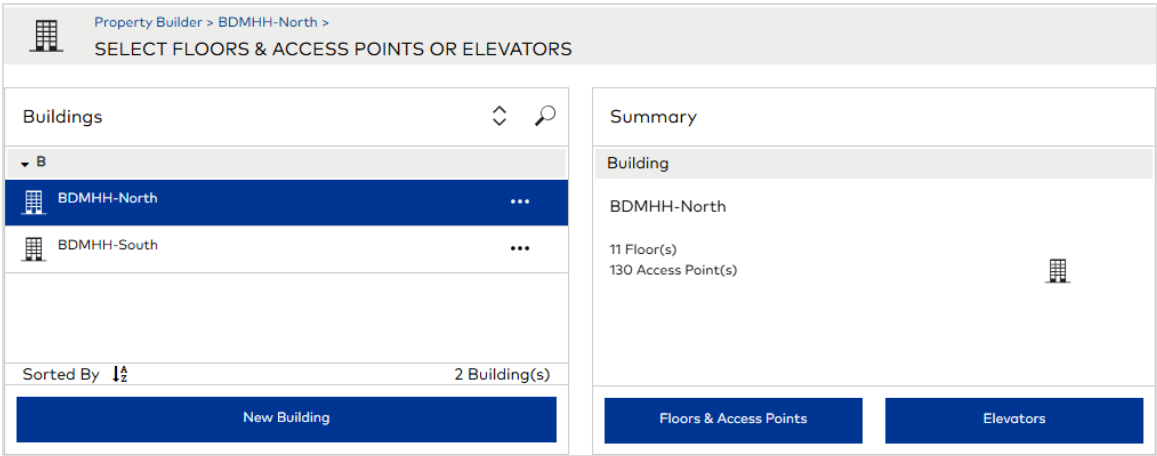
Add elevators

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*.

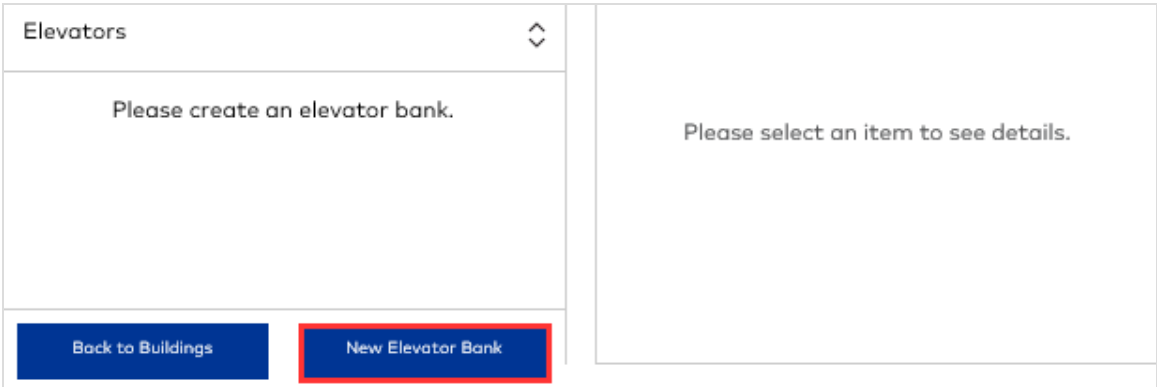
Add elevator banks

To add an elevator bank:

- 1. Go to [Property Builder](#).
- 2. Select a building.



- 3. Click [Elevators](#).



- 4. Click [New Elevator Bank](#).

New Elevator Bank

Name

North Elevator

Elevator controller profile

MCC 12 - Multi-Channel Controller

☐ Legacy mode

Cancel

Save

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

Elevators

North Elevator

MCC 12 - Multi-Channel

...

Panel 1

P1R1

P1R2

P1R3

P1R4

P1R5

P1R6

P1R7

P1R8

P1R9

P1R10

P1R11

P1R12

Back to Buildings

New Elevator Bank

Add elevators

To add an elevator:

- 1. Go to [Property Builder](#).
- 2. Select a building.
- 3. Click [Elevators](#).

4. Select the elevator bank where you want to add the elevator.
5. Click [New Elevator](#).

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

Map floor access

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

To map floor access:

1. Go to [Property Builder](#).
2. Select a building.
3. Click [Elevators](#).

4. Select the elevator bank where you want to map floor access. If the elevator bank contains at least one elevator, the list of floors in the building are displayed.
5. Select a Panel to configure.
6. Drag-and-drop panel relays (PnRn)  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. If VIP Guest Registration is enabled and the elevator controller is RAC5, drag-and-drop panel relays to floors in the Standard Access and VIP Access columns. The following rules apply:
 - The same relay can only be mapped in one column.
 - For VIP access, the same relay can only be mapped to a single floor.
 - The maximum number of distinct panels that can be mapped to VIP floor access is 4.
 - Standard access to a floor must be mapped before assigning a relay to the same floor for VIP access.
7. Click (Save) .

Elevator Bank: North Elevator




Floor	Panel / Relay - Standard Floor Access
≡ FLOOR0	P1R1 ×
≡ FLOOR1	P1R2 ×
≡ FLOOR2	P1R3 ×
≡ FLOOR3	P1R4 ×
≡ FLOOR4	P1R5 ×
≡ FLOOR5	P1R6 ×
≡ FLOOR6	P1R7 ×
≡ FLOOR7	P1R8 ×
≡ FLOOR8	P1R9 ×
≡ FLOOR9	P1R10 ×
≡ FLOOR10	P1R11 ×

New Elevator

Generate Report

The following figure shows floor mapping when VIP Guest Registration is enabled and the control panel is RAC5.

Elevators

ElevatorBank1

RACS - Remote Access

Elevator1

1 Reader(s): Elevator1

Panel 1

P1R1

P1R2

P1R3

P1R4

P1R5

P1R6

P1R7

P1R8

Panel 2

Panel 3

Panel 4

Panel 5

Panel 6

Panel 7

Panel 8

Elevator Bank: ElevatorBank1

Floor

Panel / Relay - Standard Floor Access

Panel / Relay - VIP Floor Access

FLOOR1	P1R1	X	
FLOOR2	P1R1	X	
FLOOR3	P1R1	X	
FLOOR4	P1R2	X	
FLOOR5	P1R3	X	
FLOOR6	P1R4	X	
FLOOR7	P1R5	X	
FLOOR8	P1R6	X	
FLOOR9	P1R7	X	
FLOOR10	P1R1	X	P1R8 X

Step 3

Configure Access

This section includes the following subjects:

Learning about Access Management	110
Add auto-unlatch schedules	113
Add access schedules	115
Add shift schedules	117
Create access point groups	119
Add credentials	121
Assign schedules	125
Configure access profiles for limited-access common areas	126

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 required for all sites. Optionally, you can add shift schedules and create access point groups before defining credentials.  Shift Schedules control when staff keys are valid. You can apply a shift schedule to a credential.  Access Point Groups create logical groupings of access points to add to credentials.  Credential Management create and configure credentials for staff keys.	Common Areas If you created any common areas with limited access enabled, you must configure common area access.  Common Area Access configure guest and staff access to limited-access common areas. Staff access is configured by creating a profile that associates limited-access common areas to credentials. Guest access is configured by creating a profile that associates limited-access common areas to guest rooms/suite rooms.	Scheduling Scheduling is an optional feature that lets you define and assign schedules for common areas and restricted areas.  Auto-Unlatch Schedules control when access points can be accessed without a key.  Access Schedules control when access points can be accessed with a valid key.  Access Point Scheduling assign Auto-Unlatch and Access schedules to access points. Schedules are applied when locks are programmed.
--	--	--

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 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.

For LGS SOAP API, Ambiance offers the guest-level Connector credential to support room sharing. If a guest room that is assigned to a Connector credential is selected during guest registration, all guest rooms associated with that credential are also selected. A guest room can be in only one Connector credential. If the guest rooms are associated with a foyer group, then the Connector class is implicitly applied to the foyer group. Guest rooms that are added to or removed from a Connector credential require reprogramming. The [Reports](#) module references the Connector credential class when selecting options for the [Credential/Access Point Assignment Report](#).

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:

Credential class selected when making a key

- For keys made using the [Emergency](#) or [Grand Master](#) credential class type, there are two ways to add common area access to staff keys. The common area must either be in the credential selected at key-making time or you select the common area as an additional access point at key-making time (additional access must be enabled).
- 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.

Options selected when making the access point

- **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. (For the Master class only, you can also add the common area as an additional access point at key-making time if additional access is enabled.)
 - 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. (For the Master class only, you can also add the common area as an additional access point at key-making time if additional access is enabled.)
 - 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. However, the floor access listed in the [Summary](#) section lists the floors where these access points are located.

Scheduling

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

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

Add auto-unlatch schedules

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

- common areas
- restricted areas
- meeting rooms



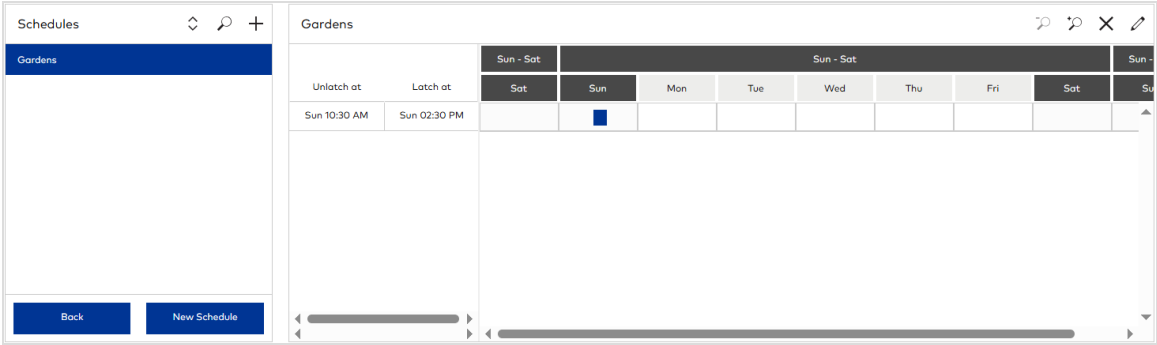
Every time that you assign/unassign a schedule or edit a schedule, you must program (or reprogram) affected access points.

To add a schedule:

1. Go to [Access Management > Auto-Unlatch Schedules](#).
2. Click **(Add)** .

3. Specify a descriptive name for the schedule.
4. (optional) Specify a description for the schedule.
5. Click [Add Period](#).

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



9. Click (Save) .

Edit a schedule

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

Delete a schedule

1. Select a schedule.
2. Click (Delete) .
3. Click [YES](#) to confirm .

Add access schedules

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

- common areas
- elevator readers



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

To add a schedule:

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

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



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

5. Click **Add Period**.

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

General Information

Schedule name*

Pool

Schedule description

normal hours

Back to Schedules

Schedule

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
all day							
05:00 AM							
06:00 AM							
07:00 AM							
08:00 AM							
09:00 AM	09:00 AM - 10:00 PM	09:00 AM - 10:00 PM	09:00 AM - 10:00 PM	09:00 AM - 10:00 PM	09:00 AM - 10:00 PM	09:00 AM - 10:00 PM	09:00 AM - 10:00 PM
10:00 AM							
11:00 AM							
12:00 PM							
01:00 PM							
02:00 PM							
03:00 PM							
04:00 PM							
05:00 PM							
06:00 PM							
07:00 PM							
08:00 PM							
09:00 PM							
10:00 PM							
11:00 PM							

Add Period

10. Click (Save) .

Edit a schedule

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

Delete a schedule

- Select a schedule.
- Click (Delete) .
- Click **YES** to confirm.

Add shift schedules

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

- common areas
- restricted areas

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

To add a schedule:

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

General Information

Schedule name*

Shift1

Schedule description

Description

Back to Schedules

Schedule

Sunday

Monday

Tuesday

Wednes

Thursda

Friday

Saturda

all day

12:00 AM

01:00 AM

02:00 AM

03:00 AM

04:00 AM

05:00 AM

06:00 AM

07:00 AM

08:00 AM

09:00 AM

Add Period

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

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

5. Click **Add Period**.

Add Period

Access from

5:00 AM

Until

1:00 PM

☒ All

☒ Su

☒ Mo

☒ Tu

☒ We

☒ Th

☒ Fr

☒ Sa

Cancel

OK

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

The screenshot shows a 'Schedules' window with a sidebar on the left containing a 'Shift1' button. The main area displays a grid for 'Shift1'. The grid has columns for each day of the week (Sunday through Saturday) and rows for time slots from 'all day' down to '02:00 PM'. A blue block is present in the grid, spanning from 05:00 AM to 01:00 PM on all days. At the bottom of the sidebar are 'Back' and 'New Schedule' buttons. The top right of the grid has icons for search, zoom, close, and edit.

10. Click **(Save)** .

Edit a schedule

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

Delete a schedule

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

Create access point groups

Organizing access points into logical groups based on location or intended use facilitates the assignment of credentials. To add an access point group:

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

General Information

Access Point Group name*

North

Description

all guest rooms and suites in North

Back to Access Point Groups

Next to Access Points

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

Access Points

BDMHH-...

NAME

ÉTAGES

806

807

808

809

810

101 - 129 of 129 items

Sort By Name 129 Access Point(s)

Back to Access Point Groups

Save

Summary

Access Point Group

Name: North

Description: all guest rooms and suites in North

Access Points

BDMHH-Nord

ÉTAGES

301 301A 301B 302 302A 302B 303 304 305 306 307 308 309 310 S-301 S-302

ÉTAGES

501 501A 501B 502 502A 502B 503 504 505 506 507 508 509 510 S-501

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

Edit access point groups

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



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

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

Delete an access point group

1. Select an access point group.
2. Click [\(Delete\)](#) .
3. Click [YES](#) to confirm.

Add credentials

The only credentials that you need to add during site configuration are for staff keys.

To add a credential:

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

Credential Information

Credential name*

Security

Description

for first responders

Credential class*

Emergency ▼

Default shift schedule

24/7 ▼

Access Point Groups

North × South × ×

Back to Credentials

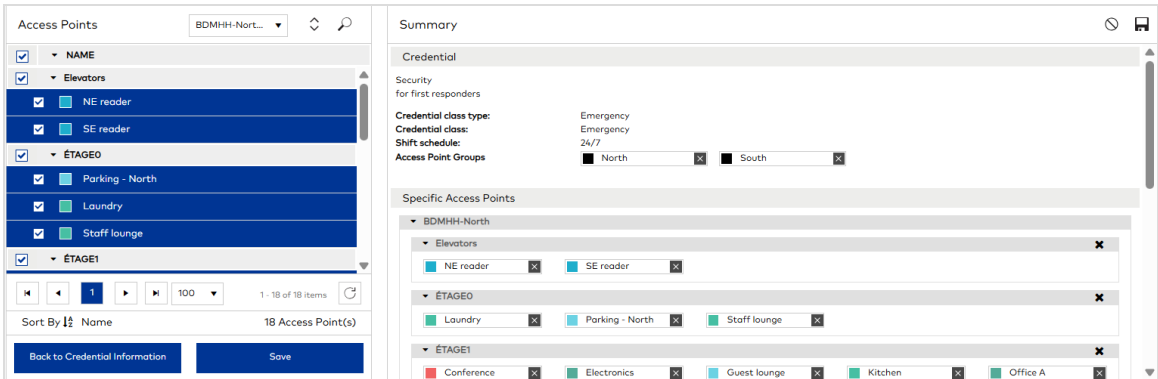
Next to Access Points

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



You can also create a custom credential class. If you want to create a custom class, select [Edit Credential Classes](#).

6. 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.) Not available for Connector credentials.
7. Select the access point groups that you want to add to the credential. Not available for Connector credentials.
8. Click [Next to Access Points](#).



9. Select the access points that you want to add to the credential. You can add access points from different buildings. Access points that are included in any selected access point groups are not listed.

 When adding staff common areas or guest common areas with staff access enabled to a Limited Use Staff or Master credential, you must also ensure that the same common area is also associated with the credential in [Access Management > Common Area Access](#).

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

The 'Key' creation form contains the following elements:

- Credential class***: A dropdown menu with 'Emergency' selected.
- Credential***: A dropdown menu with 'Security' selected.
- Key type**: Two radio buttons. 'New key' is selected. The other option is 'Additional key (Key IDs remaining: 255/255)'.
- Shift schedule**: A dropdown menu with '24/7' selected.
- Key expiration (expires at end of shift)**: A date field showing '07/14/2026' with a calendar icon.
- Next to Key Holder**: A large blue button at the bottom.

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](#).

Credential Class List		+	×	✎
Credential class	Credential class type			
Done				

2. Click [\(Add\) +](#).

Credential Class Edit	
Credential class name*	Inspector
Credential class type	Limited Use Staff ▼
Description	Description
Cancel Save	

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](#).

Credential Class List		+	×	✎
Credential class	Credential class type			
☐ Inspector	Limited Use Staff			
Done				

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 key.

Credentials

Inspector

Inspector

This is a credential made using the credential class.

Back

New Credential

Key

Credential class*
Inspector

Credential*
Inspector

New key

Additional key (Key IDs remaining: 255/255)

Shift schedule
24/7

Key expiration (expires at end of shift)
07/14/2026

Next to Common Areas & Floor Access

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

System Rights		Key Rights		
Rights	Administrator	Front Desk Agent	Site Configurator	Staff Manager
Inhibit	☒	☐	☒	☐
Inspector	☒	☐	☒	☐
Make additional key	☒	☐	☒	☐
Make block key	☒	☐	☒	☐
Make cancel key	☒	☐	☒	☐
Make new key	☒	☐	☒	☐
Make replacement key	☒	☐	☒	☐
Make resequence key	☒	☐	☒	☐
Make unblock key	☒	☐	☒	☐

04/2026

Ambiance

124

Assign schedules

Auto-Unlatch schedules can be assigned to common areas accessible by guests/staff, meeting rooms and restricted areas.



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

To assign schedules to an access point:

- 1. Go to [Access Management > Access Point Scheduling](#).

Access Points

Restricted Area

Parking - North
Guest Common Area

Pool
Guest Common Area

Spa
Guest Common Area

Staff lounge
Staff Common Area

Teams Room
Meeting Room

BDMHH-South

Back

Pool

Auto-Unlatch Schedule

24/7

Access Schedules

Guest

Piscine

Staff - Master

24/7

Staff - Limited Use Staff

24/7

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

Configure access profiles for limited-access common areas

Create and configure profiles that associate 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 registration and then associating common areas to guest rooms and suite rooms.

Add a guest profile

1. Go to [Access Management > Common Area Access](#).
2. Click (Add) +.



New Profile

Profile name*

Amenities

Profile type

Guest ▼

Cancel Save

3. Specify a descriptive name for the profile.
4. Select profile type Guest.
5. Click [Save](#). The profile is added to the list.

Associate common areas to guest rooms/suite rooms/meeting rooms

To associate guest rooms to common areas:

1. Go to [Access Management > Common Area Access](#).

Profile Setup

Profile | Access Points

Profile name*
Amenities

Profile type
Guest

☒	Common Area	Default Access
☒	Business Center	YES
☒	Clubhouse	NO
☒	Fitness	YES
☒	Gardens	YES
☒	Guest laundry	YES
☒	Guest laundry - S	YES
☒	Parking - North	NO

2. Select an existing common area profile or add a new profile.
3. On the [Profile](#) tab, select the common areas that you want to configure for access in this profile and whether to enable default access for each common area that you select. When default access is enabled, the common area is automatically added to guest registrations.

Profile Setup

Profile | Access Points

BDMHH-North

NAME

ÉTAGE3

☒	301	Amenities
☒	302	Amenities
☒	303	Amenities
☒	304	Amenities
☒	305	Amenities
☒	306	Amenities
☒	307	Amenities

1 - 86 of 86 items

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

Common Area Profiles				
Amenities				101

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 > Common Area Access](#).
2. Click (Add) +.

New Profile

Profile name*

Staff of the Month

Profile type

Staff ▼

Credential class type

Master ▼

Cancel

Save

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

Associate common areas to credentials

To associate guest rooms to common areas:

1. Go to [Access Management > Common Area Access](#).
2. Select an existing common area profile or add a new profile.

Profile Setup ✕ 📄

Profile

Credentials

Profile name*

Profile type

Credential class type

☐	Common Area	Default Access
☐	Business Center	NO
☒	Clubhouse	NO
☐	Gardens	NO
☐	Kitchen	NO
☐	Laundry	NO
☐	Parking - North	NO
☐	Pool	NO
☐	Rooftop terrace	NO
☒	Spa	NO

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

Profile Setup ✕ 📄

Profile

Credentials

☒ **Master** ⌵

☒	Housekeeping1-N	Staff of the Month
☒	Housekeeping1-S	Staff of the Month
☒	Housekeeping2-N	Staff of the Month
☒	Housekeeping2-S	Staff of the Month
☒	Housekeeping3-N	Staff of the Month
☒	Housekeeping3-S	Staff of the Month

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

Common Area Profiles		  
Amenities		101
Staff of the Month		6

Step 4

Configure Devices

This section includes the following subjects:

Learning about Device Management	132
Add encoders	135
Configure and commission staff key validator devices	139

Learning about Device Management

[Device Management](#) is the Ambiance module where you configure encoders.



When licensed for Staff Key Validation, you can also configure SKV (staff key validator) devices.



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

Encoders

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



When licensed for the Staff Key Validator (SKV), up to 25 encoders can be designated for staff key validation. Encoders designated for SKV, are not available for key encoding.

Ambiance supports the following:

- dormakaba RFID Encoder I—Legacy encoders. Unsupported configuration for enhanced security mode.
- dormakaba RFID Encoder II—Required for enhanced security mode. The part number 75720 displays on the underside of the encoder. For each encoder, Ambiance generates client-side and server-side certificates to secure communication. By default, certificates are valid for two years and renew automatically 30 days prior to expiration. Device certificates are active for fresh installations. For upgrades, device certificates must be activated at [System Settings > Security > Device Security](#).

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

Prerequisites

The following prerequisites are automatically met during initial Ambiance installation:

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

USB connection method

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

TCP/IP connection method

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

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



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

Staff key validation

Staff key validation is a licensed Ambiance option that reinforces access control by validating staff keys daily. The SKV (staff key validator) device, installed at a central location, includes a touchscreen terminal and RFID encoder. The touchscreen guides staff through the required steps, while the encoder validates their key, captures access-tracking data, and updates the key with the latest access permissions assigned to that staff member.

Staff key validation works exclusively with credentials defined using the Master credential. Refer to the release notes for detailed requirements.

By default, only Administrator and Site Configurator roles have the right to add and configure Staff Key Validator devices.

Registered gateways and paired access points

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

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

For each gateway Gen II and RAC5 device, Ambiance generates a client-side certificate to secure communication. By default, certificates are valid for two years and renew automatically 30 days prior to expiration. Device certificates are active for fresh installations. For upgrades, device certificates must be activated at [System Settings > Security > Device Security](#).

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.

The following M-Units are supported:

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

M-Unit authentication is enabled by default but can be disabled in [System Settings > Security](#). When authentication is enabled, M-Unit credentials must be configured for at least one Operator in [Staff Management](#).

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

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



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



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

Add encoders

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



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

To add encoders:

1. Connect the encoder via USB to the workstation. The initial configuration of an encoder requires that you connect the encoder to the 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](#). (If online communication is enabled, click [Encoders](#).)
3. Click [New Encoder](#).

BDMHH_North



Encoder name*

BDMHH_North

Encoder type

dormakaba RFID Encoder II

PMS Encoder ID

19

Reference firmware version

N/A

Encoder MAC address*

000E2A01211F

Current firmware version

2.13

Enable audio feedback

YES☐

Update Firmware

☐ USB

☒ TCP/IP

Obtain an IP address automatically

YES☐

Encoder IP address*

xxx.xxx.xxx.xxx

☐ Server IP

☒ Server name

Subnet mask*

xxx.xxx.xxx.xxx

Server name*

Server name

Default gateway*

xxx.xxx.xxx.xxx

The following figures shows configuration when encoder is designated for staff key validation.

4. Select whether to use this encoder for staff key validation. When **YES**, the encoder is not available to encode keys, and the connection method must be TCP/IP. A maximum of 25 encoders can be designated for staff key validation. Default: NO.
5. For **Encoder name**, specify a unique name that does not exceed 50 characters. This name displays in the list of encoders.
6. The encoder type is detected based on firmware version:
 - **dormakaba RFID Encoder I**—Legacy encoders. Unsupported configuration for enhanced security mode.
 - **dormakaba RFID Encoder II**—Required for enhanced security mode. The part number 75720 displays on the underside of the encoder. Unsupported configuration when Enhanced Security Mode is disabled.
7. (*conditional*) If integrating a third-party PMS, specify a number to identify the encoder. Valid values: 0-99. Not used when encoder designated for staff key validation.
8. Select the encoder MAC address. The value is automatically detected when you connect the encoder to the workstation.
9. Select whether the encoder emits audible beeps when a successful connection is made with the workstation and when making keys.
10. **TCP/IP or USB**—Select the method to connect the encoder with the workstation after initial configuration. If you change the connection type from TCP/IP to USB or from USB to TCP/IP you must reinitialize (unplug/replug) the encoder.
 - Specify TCP/IP settings to define the network configuration for the encoder device:
 - **Obtain an IP address automatically**—Select one of the following:
 - **Yes**—This is the default setting. A dynamic encoder IP address, subnet mask and default gateway are assigned.
 - **No**—Consult with your network administrator to obtain values for the encoder IP address, subnet mask, and default gateway.
 - Configure one of the following:
 - **Server IP**—IP address of the Ambiance server.
 - **Server name and local DNS IP address**—Name of the Ambiance server. If specifying server name, the encoder and server must be on the same domain. If you choose to use a static IP address and specify the server name, the IP address of the local domain name server is required.

- Click [Save Changes](#). The encoder is added to the list of encoders. If you selected the USB connection method, the encoder must remain connected to the workstation via USB. TCP/IP encoders must be connected to the network before the status changes to [Online](#).



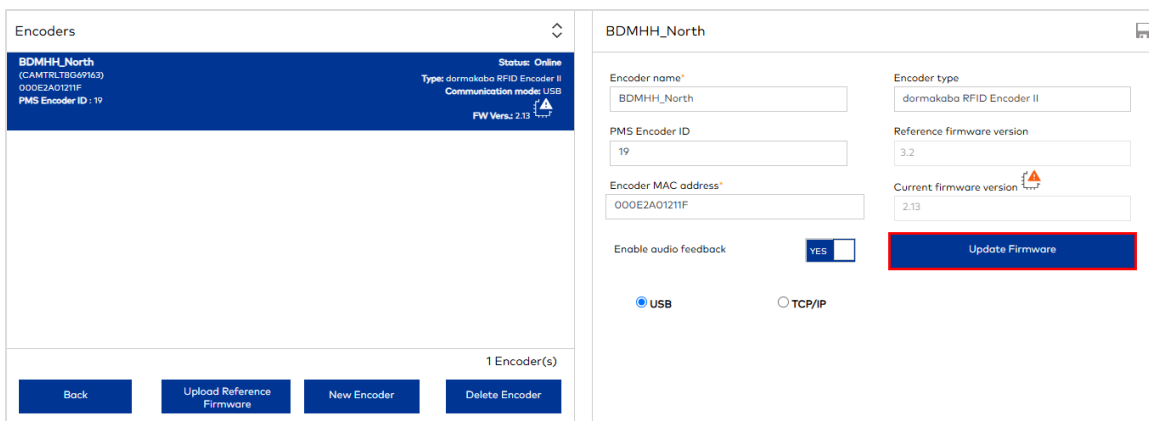
Update encoder firmware

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

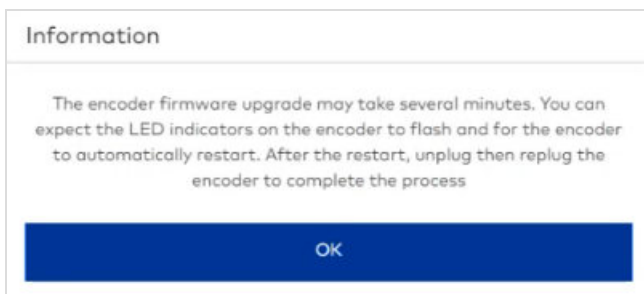


Before performing the following steps, obtain the latest recommended firmware version file from dormakaba Support.

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



- Select the encoder that requires a firmware update.
- Click [Update Firmware](#).



- Click [OK](#) to acknowledge the update may take several minutes. Expect the LED indicators on the encoder to flash. When the update is complete, the encoder restarts.
- After the restart, unplug then replug the encoder.

Edit encoders

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

Delete encoders

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

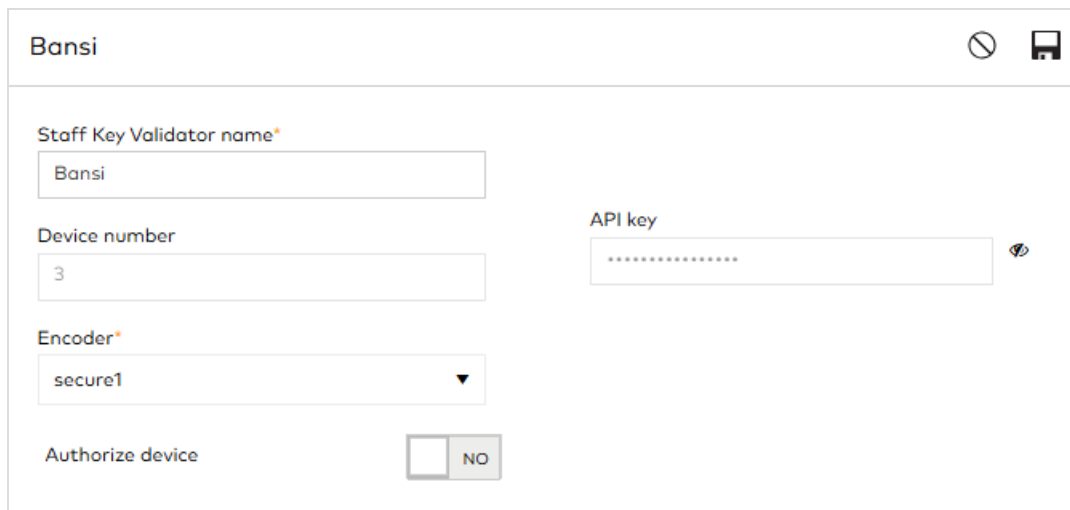
Configure and commission staff key validator devices

Add, commission, modify, and delete SKV (staff key validator) devices.

Adding an SKV device

To add an SKV device configuration:

1. Click [New Staff Key Validator](#).

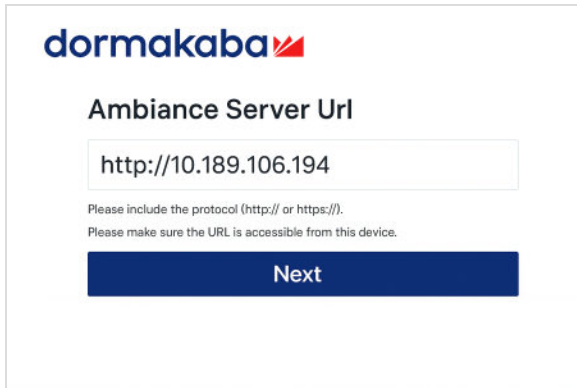


2. Specify a unique and descriptive name for the device. Maximum characters: 25.
3. Select an encoder to use with the device. The selection list only includes available encoders that are designated for use with staff key validation.
4. Click [\(Save\)](#) .
- The device number and API key are automatically populated read-only fields. The device number and an internal device ID identify the unique SKV device. The API key is used for request authorization. To view the API key, click [\(Show\)](#) .
5. For [Authorize device](#), select [YES](#) to enable this device for staff key validation. The device must also be provisioned prior to validating staff keys.

Commission an SKV device

The device must be configured before commissioning. Prepare to commission by obtaining the values for device ID and API key.

1. Power up the SKV device by connecting it to the Ethernet.
2. Specify the HTTPS host name or static IP address, then click [Next](#). This prompt is only displayed when the IP address/host name is not yet configured.



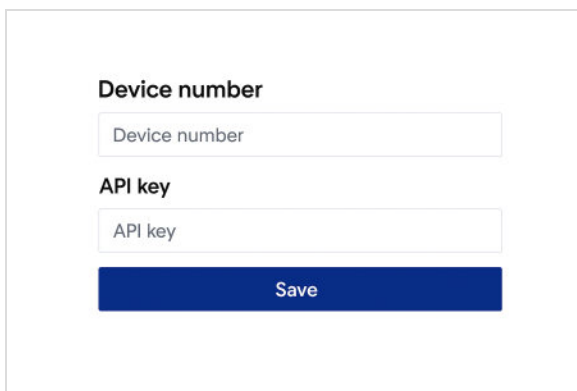
dormakaba

Ambiance Server Url

Please include the protocol (http:// or https://).
Please make sure the URL is accessible from this device.

Next

3. Specify the device number and API key. Obtain the values from [Device Management > Staff Key Validators](#). This prompt is only displayed when the values are not yet configured.

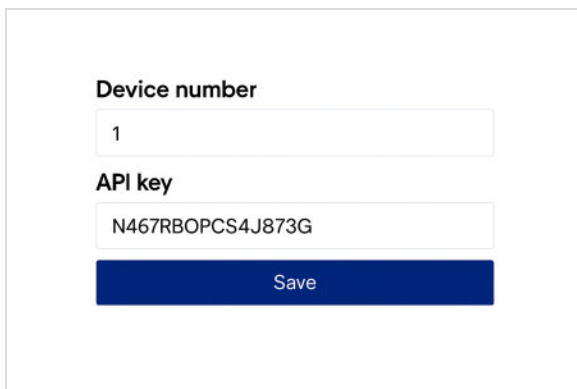


Device number

API key

Save

4. Click [Save](#).



Device number

API key

Save

If the device is defined in Ambiance with a matching device number and API key, the settings are stored in the device, and the unique device ID is linked to the device number. Commissioning is complete.

SKV device error messages

The SKV device may present the following error messages:

- Unable to authenticate this device (*nnn*). Please verify configuration.
Issued for the following reasons (per Device Management/Staff Key Validators):
 - 001—Invalid SKV device ID
 - 002—Invalid API key

- 003—Invalid device number
- Key validation is not authorized on this device. Please verify configuration.
 - Issued when device is not authorized (per Device Management/Staff Key Validators)
- Unable to validate your key. Please try again.

Issued for the following reasons:

 - When PIN length is invalid (per System Settings/Staff Key Validator/Device Settings)
 - When no active or inactive staff member has a matching PIN in the database
 - PIN belongs to an active staff member but for which key validation is disabled (per Staff Management/*staff profile*/Staff Key Validator)
 - PIN belongs to a deactivated staff member (per Staff Management/Deactivated staff members)
- Your shift has not started. Please come back later.
 - Issued when the PIN is entered before the validation period has started (per System Settings/Staff Key Validator/Device Settings)
- Your shift has already started and the validation period is expired. Please contact your administrator.
 - Issued when the PIN is entered after validation period has ended (per System Settings/Staff Key Validator/Device Settings)

Modifying an SKV device

To modify an SKV device configuration:

1. Select the SKV device configuration that you want to modify.
2. Modify options.
3. Click [\(Save\)](#) .

Deleting an SKV device

To delete an SKV device configuration:

1. Select the SKV device configuration that you want to delete.
2. Click [Delete Staff Key Validator](#).
3. Click [OK](#) to confirm. The encoder designated for the SKV device remains unavailable for non-SKV use.

Step 5

Program Locks

This section includes the following subjects:

Learning about Programming & Auditing	143
Program locks	146

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. During programming, 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.



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

Transferring data from the M-Unit to a workstation requires the Ambiance Client. Download and install the client from the main toolbar in the [Programming & Auditing](#) or [Device Management](#) module.



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



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

Programming locks

Each lock must be programmed with the respective access definition configured in 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	Description
	Guest Room
	Guest Common Area
	Suite Common Door
	Suite Inner Door
	Foyer Door
	Meeting Room
	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
 - Foyer 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.
- After enabling Enhanced Security Mode.
- After terminating active legacy keys under Enhanced Security Mode.

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 for which a mobile key is issued must be reprogrammed.

System Settings > Online Communication > Rx-Link

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

Programming devices

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

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

Auditing locks

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

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

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

Auditing online access points

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

Online access points can be audited directly in Ambiance.

Program locks



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

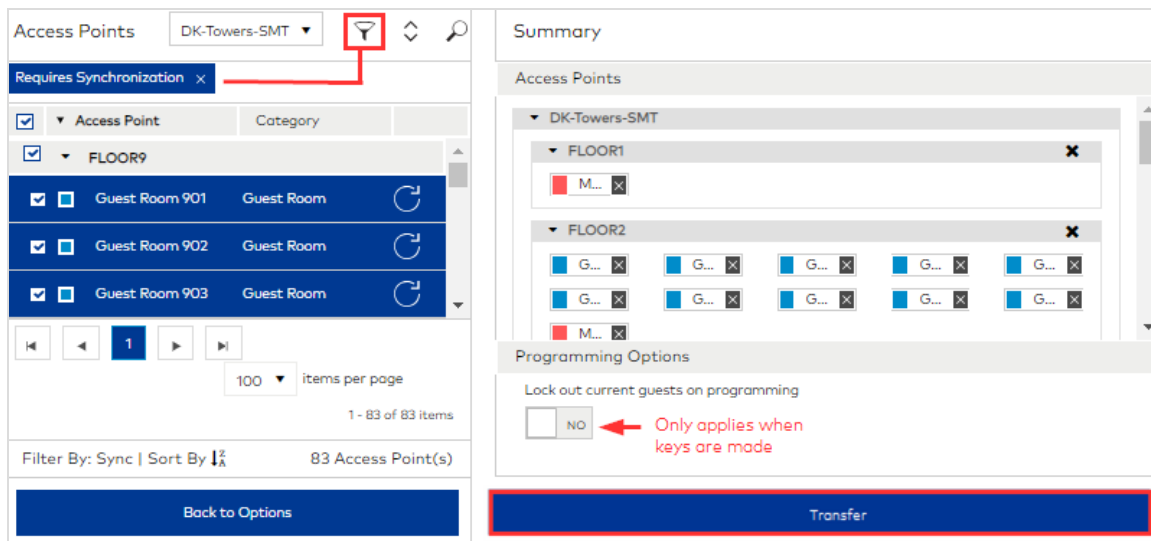


A Microsoft issue prevents the Edge browser from detecting/connecting to the Maintenance Unit. Consequently, access points cannot be programmed or audited without intervention. Open the Command prompt and issue the following command:

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

To program locks:

1. Go to [Programming & Auditing > Programming](#).

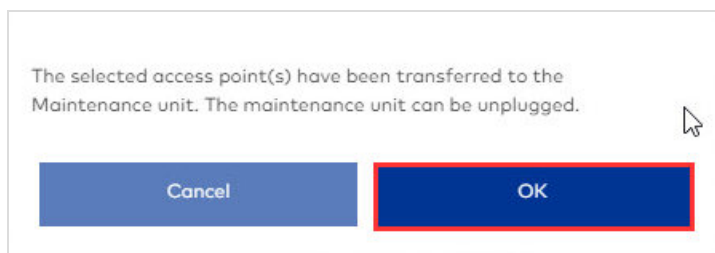


2. Select the access points that you want to synchronize with Ambiance configuration data. You can select access points from different buildings and filter the list to show only access points that require synchronization. The selected access points display in the [Summary](#) section organized by building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



The [Lock out current guest on programming](#) option only applies when keys have already been made and issued.

3. Connect the M-Unit to the workstation.
4. 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.



5. Click [OK](#).
6. Disconnect the M-Unit from the workstation. The remaining steps are on the M-Unit.

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



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



If issues arise when programming locks, create and present an LED Diagnostics Key in [System Keys](#) and see "Troubleshooting locks."

Step 6

Review & Customize Roles

This section includes the following subjects:

Learning about Role Management	149
Review pre-defined roles	150
Configure custom roles	151

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. Role Management is only accessible to operators assigned the Administrator or Site Configurator role.

Predefined and custom roles

When assigning roles to Operators, you can use the predefined roles or create custom roles. 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.

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



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

Rights

There are two types of rights in 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](#).

System Rights	Key Rights			
	Administrator	Front Desk Agent	Site Configurator	Staff Manager
► Rights	☐	☐	☐	☐
► Access Management	☒	☐	☒	☐
► Device Management	☒	☐	☒	☐
► Guest Registration	☒	☒	☒	☒
► Monitoring	☒	☐	☒	☐
► Programming & Auditing	☒	☐	☒	☐
► Property Builder	☒	☐	☒	☐
► Read Keys	☒	☒	☒	☒
► Reports	☒	☐	☒	☐
► Staff Keys	☐	☐	☐	☐

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



The Staff Manager role and custom roles based on Staff Manager include full access to all functions in Staff Management including the ability to change operator passwords. dormakaba recommends adding custom roles to optimize operator access.

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 [\(Add\) +](#).

New Role

Role name

Senior Front Desk Agent

Based on

Front Desk Agent

Cancel

Save

- 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.

The Staff Manager role and custom roles based on Staff Manager include full access to all functions in Staff Management including the ability to change operator passwords. dormakaba recommends adding custom roles to optimize operator access.

- 5. Click [Save](#).

Rights	Key Rights				
	Administrator	Front Desk Agent	Site Configurator	Staff Manager	Senior Front Desk Agent
Access Management	☒	☐	☒	☐	☐
Device Management	☒	☐	☒	☐	☐
Guest Registration	☒	☒	☒	☒	☒
Monitoring	☒	☐	☒	☐	☐
Programming & Auditing	☒	☐	☒	☐	☐
Property Builder	☒	☐	☒	☐	☐
Read Keys	☒	☐	☒	☒	☐
Reports	☒	☐	☒	☐	☒
Staff Keys	☐	☐	☐	☐	☐

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

Step 7

Add Operators

This section includes the following subjects:

Learning about Staff Management	153
Configure operators	154
Import staff list	161

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 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.

You can add staff manually or import a list.

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 and notifications are enabled. The option to designate the staff member as an Operator is on this tab.
- **Operator Info**—This tab is where Operator access is configured. The tab is only active if the staff member is designated as an Operator.
- **Assigned Keys**—This tab lists active keys assigned to the staff member. You can cancel and/or replace keys in the list.
- **Staff Key Validation**—This tab displays when licensed for staff key validation. When displayed, enable and configure staff key validation settings for the staff member. Settings in the staff profile override system settings. By default, only Administrator and Site Configurator roles have the right to set staff key validator settings.

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).

Importing staff

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

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 defined in [Access Management > Credential Management](#) that may include access to any access point type.

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 [Assigned Keys](#) tab in the profile.

Staff keys are valid in staff and guest common areas and elevator controllers until key expiration is reached. Note that staff keys with the status *Obsolete* continue to allow access to common areas and elevator controllers until key expiration.

For information about invalidating staff access, see [Invalidating staff access](#).

Configure operators

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

Refer to the following sections:

- [Add staff member](#)
- [Enable and configure staff key validation](#)
- [Designate staff member an operator](#)
- [Select / change default software language for operator](#)
- [Assign / change operator role](#)
- [Change operator login password \(SSO disabled only\)](#)
- [Add / update Maintenance Unit credentials](#)
- [Add / update PMS operator login credentials](#)

Add staff member

To add a staff member:

1. Go to [Staff Management](#).
2. Click (Add) .

New Staff Member

First Name*

Jon

Middle Name

Middle Name

Last Name*

Do

Cancel

Save

3. Specify the name of the staff member. Use the middle name to distinguish between staff with the same first and last names. Max chars per field: 25.
4. Click [Save](#). Ambiance creates a profile and displays the [Staff Member Info](#) tab.

The screenshot shows a staff profile form for 'Jon Do'. The form has three tabs: 'Staff Member Info', 'Operator Info', and 'Assigned Keys'. The 'Staff Member Info' tab is active. It contains the following fields: 'First Name' (Jon), 'Middle Name' (Middle Name), 'Last Name' (Do), 'User type' (Employee), 'ID' (33332154), 'Email' (jdo@domain.com), 'Mobile Number' (+12818218212), and 'Is an Ambiance Operator?' (NO). There is also a placeholder for a profile picture with an 'Upload Image' button.

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. Click [Save](#).

Enable and configure staff key validation

Settings in the staff profile override system settings.

The screenshot shows a staff profile form for 'Admin01 User'. The form has four tabs: 'Staff Member Info', 'Operator Info', 'Assigned Keys', and 'Staff Key Validation'. The 'Staff Key Validation' tab is active. It contains the following fields: 'Enable key validation for this staff member' (YES), 'PIN' (empty), 'Enable overtime for this staff member' (YES), 'Authorized overtime (hours)' (1), 'Overtime starts' (02/03/2026), and 'Overtime ends' (02/03/2026).

1. In the staff profile, select the [Staff Key Validation](#) tab.
2. Select whether to enforce staff key validation for the staff member. When **YES**, the staff member must gain access at access points where staff key validators are installed, and use their unique PIN and key.
3. The PIN is a unique numeric code assigned to the staff member. Ambiance automatically generates the code based on the PIN length system setting. Click (View)  to see the code.
4. Select whether to enable overtime for this staff member. When **YES**, staff member access is based on the following two settings and the system settings [Validation period before shift starts](#) and [Validation period after shift starts](#). Default: **NO**
 - [Authorized overtime \(hours\)](#)—Select the number of hours in a given day that overtime is authorized for the staff member. Range: 1-16 hours. Default: 1.
 - [Overtime starts](#)—Select the date when overtime authorization starts.
 - [Overtime ends](#)—Select the date when overtime authorization ends.
5. Click [Save](#).

Designate staff member as operator

1. Go to [Staff Management](#) and select a staff profile.
2. On the Staff Member Info tab, set the [Is an Ambiance Operator](#) switch to **YES**.
 - SSO is disabled.

Operator Settings

Ambiance Operator role *

Administrator ▼

Username*

jondo

Password*

.....

Password confirmation*

.....

☒ Force password change on logon

Cancel

Save

- SSO is enabled.

Operator Settings

Ambiance Operator role *

Administrator ▼

User ID*

jdo@domain.com

Cancel

Save

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

SSO is disabled:

The screenshot shows the configuration page for 'Jon Do'. At the top, there are three tabs: 'Staff Member Info', 'Operator Info' (which is active), and 'Assigned Keys'. Below the tabs, there is a 'Block software access' toggle set to 'NO'. Underneath, there are two dropdown menus: 'Default software language' set to 'Automatic Language Detection' and 'Ambiance Operator role*' set to 'Administrator'. The page is divided into three main sections for login: 'Ambiance Login', 'Maintenance Unit Login', and 'PMS Operator Login'. Each section has a 'Username' input field and a 'Change Password' or 'Add/Update Username & Password' button. In the 'Ambiance Login' section, the password status is shown as 'Valid until 09/07/2025 05:26 PM'. At the bottom, there are 'Cancel' and 'Save' buttons.

SSO is enabled:

Jon Do

Staff Member Info Operator Info Assigned Keys

Block software access ☐ NO

Default software language
Automatic Language Detection

Ambiance Operator role*
Administrator

Ambiance Login

User ID
jdo@domain.com

Maintenance Unit Login

Username:
Username

Add/Update Username & Password

PMS Operator Login

Username:
Username

Add/Update Username & Password

Cancel Save

Select / change default software language

1. Go to [Staff Management](#) and select a staff profile.
2. Click the [Operator Info](#) tab.
3. Select the default software language. The operator can change the language in account [Preferences](#).
4. Click [Save](#).

Assign / change operator role

1. Go to [Staff Management](#) and select a staff profile.
2. Click the [Operator Info](#) tab.
3. Select an operator role. The list of roles is populated by the roles created in the [Role Management](#) module.
4. Click [Save](#).

Change operator login password (SSO disabled only)

Only available when SSO is disabled.

1. Go to [Staff Management](#) and select a staff profile.
2. Click the [Operator Info](#) tab.
3. In the Ambiance Login section, click [Change Password](#). Specify and confirm a new password, then click [Save](#). You must communicate account credentials to the operator.
4. (*recommended*) To force the operator to change the password upon initial login, select [Force password change on login](#).
5. Click [Save](#).

Add / update Maintenance Unit login credentials

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

1. Go to [Staff Management](#) and select a staff profile.
2. Click the [Operator Info](#) tab.
3. In the Maintenance Unit Login section, click [Add/Update Username & Password](#).

Maintenance Unit Operator Info

Username*

Password*

Password confirmation*

Cancel

Save Changes

4. Specify a username.
5. Specify and confirm a password.
6. Click [Save Changes](#).

Add / update PMS operator login credentials

When PMS authentication is enabled, the PMS Operator Login section displays. Credentials must be configured for at least one operator. To disable PMS authentication, see [System Settings > Security > PMS integration](#).

1. Go to [Staff Management](#) and select a staff profile.
2. Click the [Operator Info](#) tab.
3. In the PMS Operator Login section, click [Add/Update Username & Password](#).

PMS Operator Info

Username*

Password*

Password confirmation*

Cancel

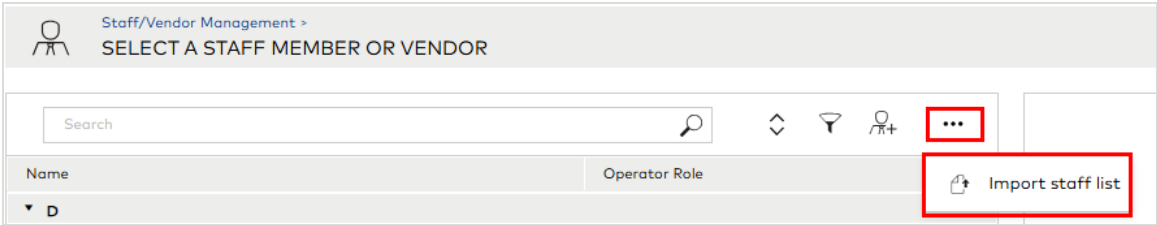
Save Changes

4. Specify a username.
5. Specify and confirm a password. Valid values: 3-15 lowercase alphanumeric characters. Legacy IRS/PRS limits the password to 10 characters.
6. Click [Save Changes](#).

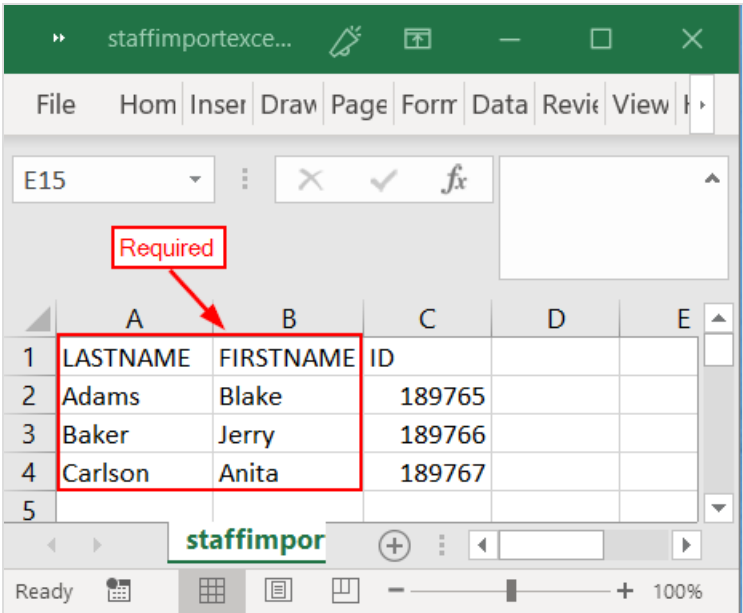
Import staff list

To import staff:

- 1. Go to [Staff Management](#).
- 2. Click [\(More\)](#) > [Import staff list](#).



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



If staff member profiles have already been created, you are prompted to proceed. Click [YES](#) to proceed.

- 4. When notified the import is successful, click [OK](#).

Search

Name	Operator Role
Blake Adams	
B	
Jerry Baker	
C	
Anita Carlson	
U	
Admin01 User	Operator Administrator
Admin02 User	Operator Administrator

1

100

items per page

1 - 5 of 5 items

Active | Sorted by Last Name

New staff member

Use Ambiance

This section includes the following subjects:

Guest Registration	165
Learning about Guest Registration	166
Add a guest registration	170
Modify a guest registration	177
Replace guest keys	180
Make additional guest keys	182
Make a limited-use guest key	185
Check out a registration	187
Staff	188
Learning about Staff Management and Staff Keys	189
Add staff members	190
Import staff member list	193
Make Emergency keys	195
Make Grand Master keys	198
Make Master keys	203
Make Limited Use Staff keys	207
Replace staff keys	210
Invalidate staff access	212
Test key files	217
Programming/Auditing	219
Reprogram locks	220
Audit locks	222
Audit online access points	223
System Keys	224
Learning about System Keys	225
Block and unblock keys	227

Cancel keys	231
Diagnostic keys	233
Electronic lockout keys	235
Failsafe keys	237
Inhibit keys	238
Latch and unlatch keys	240
Primary and secondary program keys	242
Resequence keys	245
Special function keys	247
Monitoring	248
Learning about Monitoring	249
Monitor keys	250
Reports	251
Access Point Audit Report	252
System Activity Report	253
Staff Access Report	255
Roles and Rights Report	256
Property Configuration Report	257
Operator Report	258
Key Expiration Report	259
Key/User Assignment Report	260
Elevator Configuration Report	261
Credential/Access Point Assignment Report	262
Toolbar Basics	263
Navigate Ambiance	264
Set operator preferences	266
Install / update Ambiance Client	268
Select default encoder	269
Read key/erase key/access tracking report	270
View notifications	274
Physical keys	276
Digital keys	278

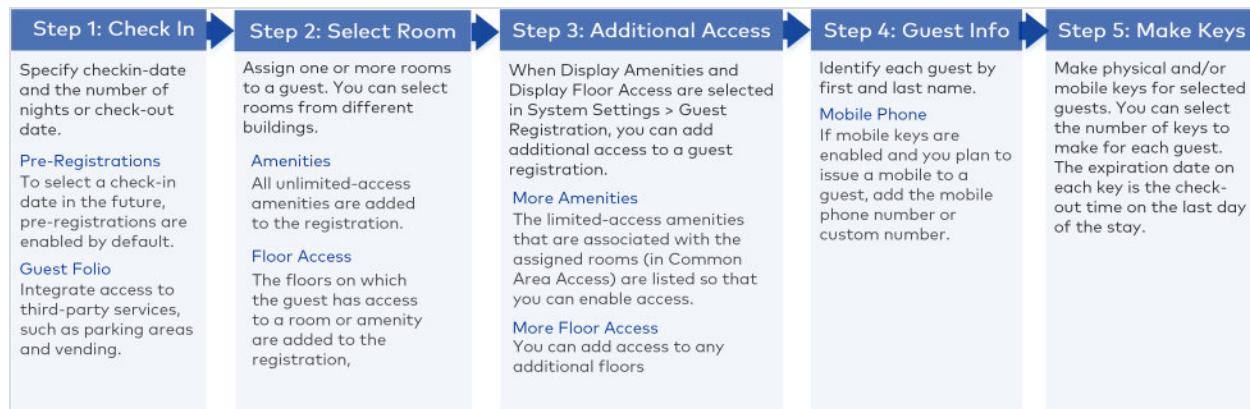
Guest Registration

This section includes the following subjects:

Learning about Guest Registration	166
Add a guest registration	170
Modify a guest registration	177
Replace guest keys	180
Make additional guest keys	182
Make a limited-use guest key	185
Check out a registration	187

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. The last step before making the key is to add guest information. 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.

In some cases, selecting a guest room adds access to additional guest rooms. For more information, see [Connector Credentials](#) below.

For RAC5 devices, you can also enable a disability option in the [Summary](#) section to extend the time that a lock remains open when a valid guest key is presented. The disability option is only displayed when the feature is enabled in [System Settings > Security > Lock Access](#).

The final step when making a guest registration is to make keys. You make any number of keys for each guest in the registration.



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. All keys in the registration are replaced. After a Replacement Key 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. Access (to common areas/elevators) remains

valid until the key expiration date/time. An alternative is to use the Block Key to invalidate access to all access point types; however, after the Block Key is presented to the respective locks, the Unblock Key will not restore access to common areas.



When online communication is enabled, settings in [System Settings > Online Communication > Online Operations](#) are available to enable remote guest check-out for guest rooms/suites/meeting rooms and guest common areas/elevators. When remote guest check-out settings are enabled, Ambiance offers the option to check out guests remotely in [Guest Registration](#).

When the system setting to enable remote check-out of guest common areas/elevators is disabled, access (to common areas/elevators) remains valid until the key expiration date/time. An alternative is to use the Block Key (or Block access remotely) to invalidate access to all access point types; however, after the Block Key is presented (or sent remotely) to the respective locks, the Unblock Key will not restore access to common areas.

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.

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.

Connector credentials



Connector credentials are supported only with the LGS SOAP API. Connector credentials are not supported for shared-with registrations.

A Connector credential is a guest-level credential that associates two or more guest rooms on the same floor. The credential is defined in [Access Management > Credential Management](#).

When a guest room that is associated with a Connector credential is added to a registration, all guest rooms in the same credential are also added. When a guest room assigned to a connector is removed from a registration, all guest rooms in the Connector credential are removed from the registration. If a guest room that is assigned to a Connector credential is selected during guest registration, all guest rooms associated with that credential are also selected. When a guest room assigned to a connector is removed from a registration, all guest rooms in the Connector credential are removed from the registration.

Not all room-sharing is alike. What's the difference between Connector credentials, shared-with registrations, and foyer doors?

- A Connector credential is for a single registration with access to all guest rooms associated with the credential. Guest rooms added to a Connector credential must be on the same floor. Guests must be added to the registration to gain access. Supported for LGS SOAP API.
- Shared-with is for multiple registrations (maximum 4) with access to all guest rooms/suites associated with each registration. Supported for LGS SOAP API and FIAS.
- A foyer door is an access point type, a common door to guest rooms and suites. Access to the individual guest rooms and suites is managed independently. However, guest rooms and suites can be added to Connector credentials. Full support.

Shared-with registrations



Shared-with registrations are supported with the LGS SOAP API and FIAS protocols. Shared-with registrations do not support Connector credentials.

When enabled, up to four registrations can share access to one guest room. Check-out dates and the assignment of additional rooms, amenities and floors can be different for each shared-with registration. The shared room (or main room) is established as the first room specified in the original registration.

Example

Registration 1: Room 100 (main room), Room 101, Pool

Registration 2: Room 100, Room 102, Pool, Daycare

Registration 3: Room 100, Room 103 , Gym, Business Center, VIP Lounge

Registration 4: Room 100, Room 104, Pool, Gym, Daycare

Shared-with registrations must be created (and modified) in the PMS interface. Although the registrations are listed in Guest Registration, [Check-out](#) is the only action that can be performed in the Ambiance user interface or PMS interface.

Modifying shared-with registrations

All modifications must be made in the PMS interface. Modifications made to a shared-with registration apply only to the registration being modified. You can:

- Add vacant rooms
- Remove rooms
- Extend the check-out date and time
- Move a guest from a shared-with registration to a vacant room (Any guest in the original shared-with registration, can also move to the same room. For example, if Guest1 and Guest2 are assigned to MainRoom100 and Guest1 moves to vacant RoomX, then Guest2 can also move to (now occupied) RoomX.)



An existing guest cannot be added to a shared-with registration. (You must check-out the exiting guest, then add as a new guest; presuming this does not exceed the maximum shares).

Invalidating access

There are several ways to invalidate access for shared-with registrations:

- [Check outs](#)—Shared-with registrations can be checked out using the PMS interface and Ambiance user interface. When a shared-with registration is checked out, the main room is available for a new guest to join. When Online Communication is enabled, you can perform a remote check-out. Otherwise, Block Keys must be made and presented to relevant access points.
- [Block/Inhibit/ELO Keys](#)—These system keys can be used to invalidate access for shared-with registrations. When Online Communication is enabled, the command can be sent remotely. Otherwise, keys must be made and presented to relevant access points.
- [New Keys](#)—New Keys invalidate access as follows:
 - Making a New Key for Guest1 with a shared registration invalidates all previous keys for Guest1. No other guest access is affected.
 - After the maximum number of shared-with registrations is reached, making a New Key for a new registration for the main room may invalidate all access to all previous shared-with registrations for the main room. The result depends on options selected when making the registration.

Extended support

Ambiance extends support for shared-with registrations to all System Keys and Keyscan Aurora. For details about working with shared-with registrations, refer to the [PMS Interface Reference](#).

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.

VIP guest keys

VIP guest registration is a licensed feature to support access management policies at exclusive properties. VIP guest keys can be made only in the PMS interface. Although VIP guest registrations are listed in Ambiance, no action can be taken in the User Interface. VIP keys can be made for individual guest rooms and suites. Only the LGS SOAP API protocol supports making VIP keys for guest rooms that are assigned to a Connector credential. VIP also supports shared-with registrations; however, guest rooms assigned to a Connector credential and suites cannot be shared.

Add a guest registration

Use the express or standard method to add a guest registration.

Express check-in

- 1. Go to Guest Registration.

Check In/Out

Check In date

07/08/2025 02:00 PM

Check Out date

07/09/2025 11:00 AM

Number of nights

-

1

+

Rooms

Rooms

301

Add Rooms

Folio

Parking*

1

Arena*

YES

Registrations

Room List

Amenities & Floors

- 2. On the Check In page, select the check-in date and either the number of nights or check-out date.
- 3. Specify the access point name/number for at least one guest room or suite, then click [Add Rooms](#). Separate multiple rooms with a semicolon. Access point names are case-sensitive.
- i

If you select a guest room that is assigned to a Connector credential or foyer group, then all access points associated with the credential or Foyer group are also selected.
- 4. Select available options: folio access, amenity and floor access, guest information, and disability access for RAC5 devices. Amenity and floor access cannot be selected until a room is added. To add guests, click [Amenities](#) then [Guests](#).

Summary

Check In/Out

Check In: Now
Check Out: 07/09/2025 11:00 AM
Period: 1 night(s)

Folio

Parking: * 1
Arena: * YES

Room(s)

301

Amenities & Floor Access

AMENITIES

☒ Business Center
☒ Fitness Center
☒ Gardens Tea Room
☒ Guest Laundry
☒ Guest Laundry - S
☒ Guest Lounge
☒ Pool

FLOOR ACCESS

☒ BDMHH-Nord - FLOORF1
☒ BDMHH-Nord - FLOORF2
☒ BDMHH-Nord - FLOOR3
☒ BDMHH-Nord - FLOOR5

Options

Enable disability option on guest keys ☐ NO

Guests

Andy Andrews

Make Keys

- Click [Make Keys](#).
- Select an encoder that is online and available to the workstation.
- Select the guests for whom to make keys.
- Select the number of keys to make per guest.
- Click [Make Keys](#).
- Present a key to the encoder (as prompted).
- When notified the key request is complete, click [Done](#). The registration is listed on the Registrations page.

Registration

View by Room

View by Guest

View by Date

FLOOR3

301

Andrews, Andy
07/08/2025 To 07/09/2025



When making mobile keys, select to make 1 key, set the Mobile soft-switch to YES, then click [Send to Mobile](#). When notified that the key request is complete, click [Done](#).

Verify mobile key status in the [Summary > Guests](#) section. The status displays *Delivering*, *Delivered*, *Failed*. To view the most current status, refresh the [Guest Registration](#) page.

Standard check-in

- 1. Go to [Guest Registration](#).
- 2. On the Check-In 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.

Check In/Out

Check In date

07/08/2025 02:24 PM

Number of nights

-

1

+

Check Out date

07/09/2025 11:00 AM

Rooms

101; 102; 103

Add Rooms

Folio

Parking⁺

1

Arena⁺

NO

Registrations

Room List

Amenities & Floors

- 3. Click Room List.

Rooms

BDMHH Nord

Search

Vacant

Occupied

All

Name ↑	Type	Floor
Vacant	Suite	FLOOR4
401 Vacant	Guest Room	FLOOR4
402 Vacant	Guest Room	FLOOR4
403 Vacant	Guest Room	FLOOR4
404 Vacant	Guest Room	FLOOR4
405 Vacant	Guest Room	FLOOR4

1 - 84 of 84 items

Sorted by name

84 Room(s)

Back to Check In

Amenities & Floors

Summary

Check In/Out

Check In: Now

Check Out: 07/09/2025 11:00 AM

Period: 1 night(s)

Folio

Parking⁺

1

Arena⁺

NO

Room(s)

401

Amenities & Floor Access

AMENITIES

Business Center

Fitness Center

Gardens Tea Room

Guest Laundry

Guest Laundry - S

FLOOR ACCESS

BDMHH Nord - FLOORF1

BDMHH Nord - FLOORF2

BDMHH Nord - FLOOR3

BDMHH Nord - FLOOR4

BDMHH Nord - FLOOR5

Make Keys

- 4. 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.



If you select a guest room that is assigned to a Connector credential or foyer group, then all access points associated with the credential or Foyer group are also selected.

5. Depending on the options available, click [Amenities & Floors](#), [Amenities](#), or [Floors](#) and 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 rooms (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](#).)

The image displays two screenshots of the 'Amenities & Floor Access' interface. The top screenshot shows the 'Amenities' tab selected, with a list of amenities including Business Center, Clubhouse, Fitness Center, Gardens Tea Room, Guest Laundry, Guest Laundry - S, Guest Lounge, and Parking - North. The 'Summary' panel on the right shows check-in/out times and room selection. The bottom screenshot shows the 'Floors' tab selected, with a list of floors (FLOOR0 to FLOOR7) and the same 'Summary' panel.

6. Click [Guests](#) and specify the first and last names of the guest. Click [\(Add\)+](#) for each additional guest that you want to add.

Guests

First Name *

Last Name *

Mobile Key

Bill

Bailey

NO

Amenities & Floors

Summary

Check In: Now

Check Out: 07/09/2025 11:00 AM

Period: 1 night(s)

Folio

Parking: 1

Arena: NO

Room(s)

401

Amenities & Floor Access

AMENITIES

Business Center

Fitness Center

Gardens Tea Room

Guest Laundry

Guest Laundry - S

Guest Lounge

Parking - North

Pool

FLOOR ACCESS

BDMHH-Nord - FLOOR0

BDMHH-Nord - FLOORF1

BDMHH-Nord - FLOORF2

BDMHH-Nord - FLOORF3

BDMHH-Nord - FLOORF4

BDMHH-Nord - FLOORF5

Options

Enable disability option on guest keys

NO

Guests

Bill Bailey

Make Keys

7. RAC5 devices only. If displayed in the Summary section, you can enable the disability option to extend the time a lock remains open after a valid guest key is presented.
8. Click Make Keys.

Make Keys

BDMHH_North

Guest

Keys

Progress

☒

Bill Bailey

-

1

+

0 of 1 encoded

Ready to start

Cancel

Start

Done

9. Select an encoder that is online and available to the workstation.
10. Select the guests for whom to make keys.
11. Select the number of keys to make per guest.
12. Click Make Keys.
13. Present a key to the encoder (as prompted).
14. When notified the key request is complete, click Done.

Registration

</



When making mobile keys, select to make 1 key, set the Mobile soft-switch to YES, then click [Send to Mobile](#). When notified that the key request is complete, click [Done](#).

Verify mobile key status in the [Summary > Guests](#) section. The status displays *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. Click [Registrations](#).

The screenshot displays the 'Registration' management interface. On the left, a table lists registrations by room number, guest name, and dates. Room 401 is highlighted. On the right, a 'Summary' panel provides details for the selected registration, including check-in/out times, folio information, and room assignment. At the bottom, a navigation bar includes buttons for 'Replacement Key', 'Additional Keys', 'Modify Registration' (highlighted with a red box), and 'Check-Out'.

Registration		
View by Room	View by Guest	View by Date
FLOOR3		
301	Andrews, Andy	07/08/2025 To 07/09/2025
FLOOR4		
401	Bailey, Bill	07/08/2025 To 07/09/2025
FLOOR5		
501	Kilman, Kimberly	07/08/2025 To 07/09/2025

1 - 3 of 3 items

Checked-In | Pre-Registered | Sorted by Room number | 3 Results

New Registration

Summary

Check In/Out

Check In: 07/08/2025 02:24 PM
 Check Out: 07/09/2025 11:00 AM
 Period: 1 night(s)
 Status: Checked In

Folio

Parking: 1
 Arena: YES

Room(s)

401

Amenities & Floor Access

AMENITIES

- ☒ Business Center
- ☒ Fitness Center

FLOOR ACCESS

- ☒ BDMHH-Nord - FLOOR0
- ☒ BDMHH-Nord - FLOORF1

Replacement Key | Additional Keys | **Modify Registration** | Check-Out

3. 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.
4. Click [Modify Registration](#).
5. Make any of the following modifications:
 - 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. If you select a guest room that is assigned to a Connector credential or foyer group, then all access points associated with the credential or Foyer group are also selected.
 - 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.

- RAC5 devices only. If displayed in the [Summary](#) section, you can select/deselect the disability option.

Summary

Check In/Out

Check In: 07/08/2025 02:24 PM
Check Out: 07/09/2025 11:00 AM
Period: 1 night(s)

Folio

Parking: * 1
Arena: * YES

Room(s)

401

Amenities & Floor Access

AMENITIES

☒ Business Center
☒ Fitness Center
☒ Gardens Tea Room
☒ Guest Laundry
☒ Guest Laundry - S
☒ Guest Lounge
☒ Parking - North
☒ Pool
☒ Spa

FLOOR ACCESS

☒ BDMHH-Nord - FLOOR0
☒ BDMHH-Nord - FLOORF1
☒ BDMHH-Nord - FLOORF2
☒ BDMHH-Nord - FLOOR3
☒ BDMHH-Nord - FLOOR4
☒ BDMHH-Nord - FLOOR5

Options

Enable disability option on guest keys ☐ NO

Guests

Bill Bailey
Belinda Bailey

Make Keys

Update Keys Remotely

6. Click [Make Keys](#).

Make Keys



BDMHH_North

Guest	Keys	Progress
☒ Belinda Bailey	-1+	0 of 1 encoded
☐ Bill Bailey	-1+	0 of 1 encoded

Ready to start

Cancel

Start

Done

7. Select the guests for whom you want to make keys, specify the number of keys to make,, then click [Make Keys](#).
- 

When online communication is enabled and the modification was a room change and/or a guest extended their stay, click [Update Keys Remotely](#)
8. When notified that the key request is complete, click [Done](#).
- 

Key requests may include a combination of physical and mobile keys. When making mobile keys, select to make 1 key, set the Mobile soft-switch to YES, then click [Send to Mobile](#). When notified that the key request is complete, 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. All keys in the registration are replaced. After a Replacement Key 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. Click [Registrations](#).

The screenshot shows the 'Registration' interface. On the left, there's a list of registrations grouped by floor (FLOOR3, FLOOR4, FLOOR5). The first registration in FLOOR3 is for 'Andrews, Andy' in room 301, with a date range of 07/08/2025 To 07/09/2025. Below the list are navigation controls and a 'New Registration' button. On the right, the 'Summary' panel shows details for the selected registration: Check In/Out dates, Check In/Out times, Period, Status, and Checked In status. Below this, there's a 'Folio' section with 'Parking' and 'Arena' details. At the bottom, there's a 'Room(s)' section with '301' listed. The 'Amenities & Floor Access' section is also visible, with a 'Replacement Key' button highlighted in red.

3. 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.
4. Click [Replacement Key](#).

The screenshot shows the 'Make Keys' interface. At the top, there's a 'Make Keys' button and a dropdown menu showing 'BDMHH_North'. Below this is a table with three columns: 'Guest', 'Active Keys', and 'Progress'. The first row shows 'Andy Andrews' with '1' active key and '0 of 1 encoded'. Below the table, there's a green bar with the text 'Ready to start'. At the bottom, there are two blue buttons: 'Start' and 'Done'.

5. Select an encoder that is online and available to the workstation, then click [Make Keys](#).
6. When notified that the key request is complete, click [Done](#).



If mobile keys are enabled and both physical and mobile keys were made, then you can choose to replace the physical keys, the mobile keys or both. To make mobile keys, click [Send to Mobile](#).

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. Click [Registrations](#).
- 3. 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.

Registration

View by Room

View by Guest

View by Date

A

Andrews, Andy

Room(s): 301

07/08/2025 To 07/09/2025

B

Bailey, Bill

Room(s): 401

07/08/2025 To 07/09/2025

K

Kilman, Kimberly

Room(s): 501

07/08/2025 To 07/09/2025

1 - 3 of 3 items

Checked-In | Pre-Registered | Sorted by Last Name

3 Results

New Registration

Summary

Check In/Out

Check In: 07/08/2025 02:39 PM

Check Out: 07/09/2025 11:00 AM

Period: 1 night(s)

Status: Checked In

Folio

Parking: 1

Arena: YES

Room(s)

501

Amenities & Floor Access

AMENITIES

Business Center

Clubhouse

FLOOR ACCESS

BDMHH-Nord - FLOOR0

BDMHH-Nord - FLOORF1

Replacement Key

Additional Keys

Modify Registration

Check-Out

- 4. Click [Additional Keys](#).

Make Keys

BDMHH_North

Guest

Keys

Mobile

Progress

Kimberly Kilman

- 1 +

YES

0 of 1 encoded

Ready to send to mobile

Ready to start

Cancel

Send to Mobile

Make Key

Done

- 5. Select the guests for whom you want to make keys and specify the number of keys to make for each.
- 6. Select an encoder that is online and available to the workstation, then click [Make Key](#). When prompted, present a key to

04/2026

Ambiance

182

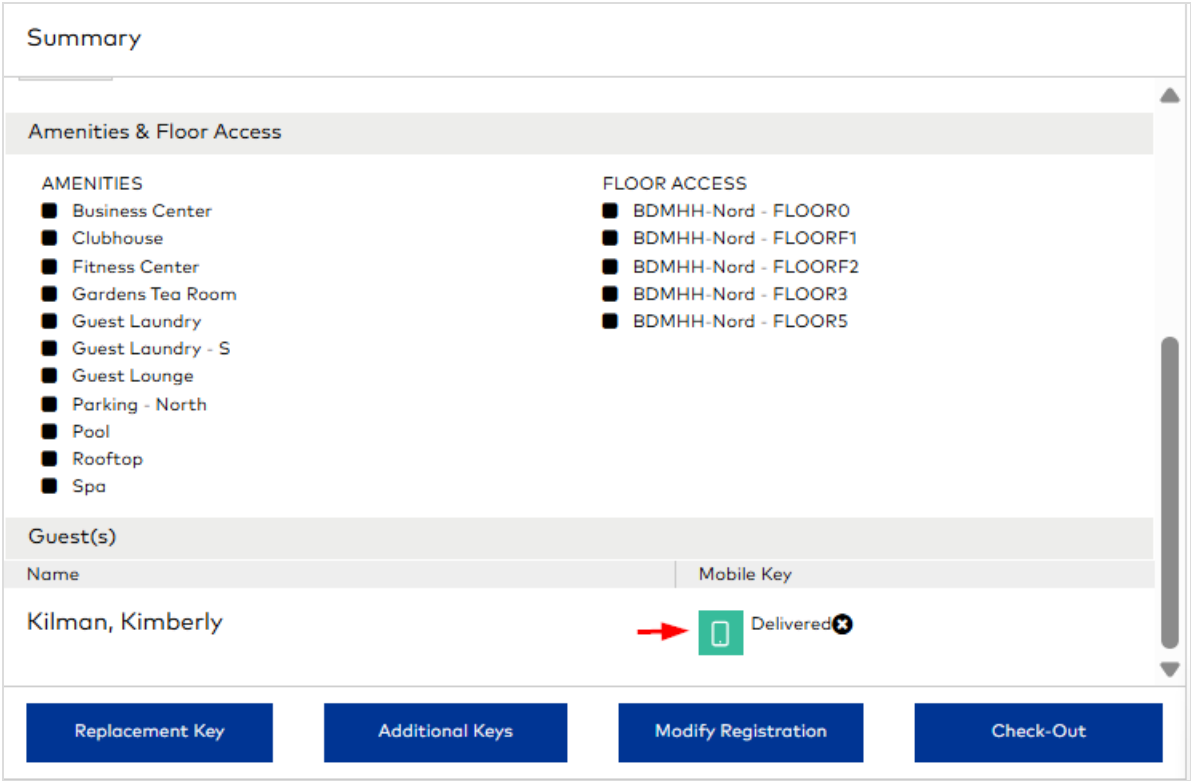
- the encoder.
7. When notified that the key request is complete, click [Done](#).



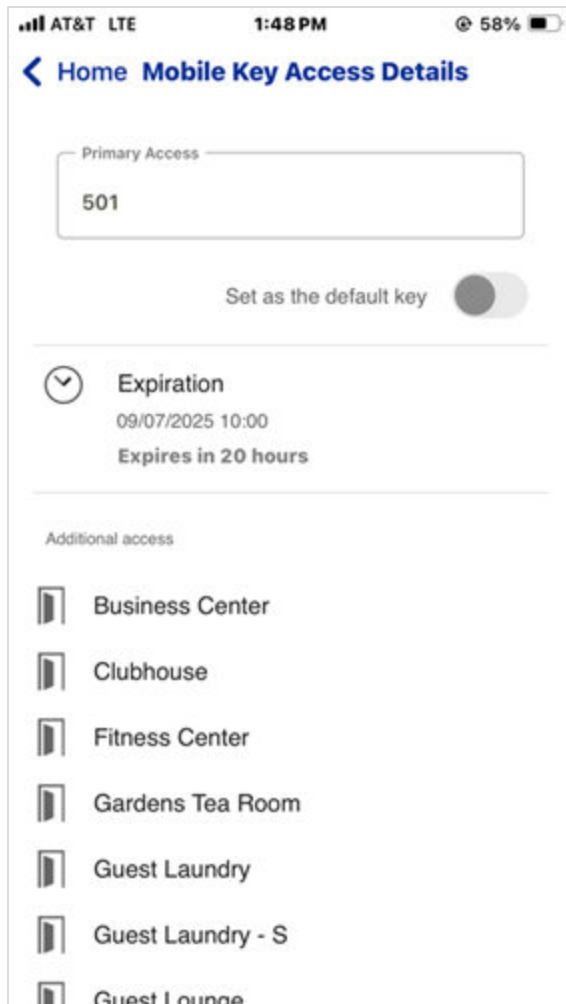
To make mobile keys, click [Send to Mobile](#). If you want to make mobile keys but no mobile number is defined for the guest, you must modify the registration to add the mobile phone number.

Verify mobile key status in the [Summary > Guests](#) section. The status displays [Delivering](#), [Delivered](#), [Failed](#). To view the most current status, refresh the [Guest Registration](#) page. Check for the key in the mobile app.

The following figure shows where to verify mobile key delivery status.



The following figure shows access in the dormakaba BlueSky app.



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 [Registrations](#).

Registration

View by Room

View by Guest

View by Date

FLOOR4

401

Bayley, Belinda Bayley

07/08/2025 To 07/09/2025

FLOOR5

501

Kilman, Kimberly

07/08/2025 To 07/09/2025

1

100

1 - 2 of 2 items

Checked-In | Pre-Registered | Sorted by Room number

2 Results

New Registration

Please select a guest registration.

Limited Use Key

- 3. Click [Limited Use Key](#).

Rooms

BDMHH-Nord

Search

Name ↑

Type

Floor

Conference Room Vacant

Meeting Room

FLOORF1

Teams Room Vacant

Meeting Room

FLOORF1

301 Vacant

Guest Room

FLOOR3

302 Vacant

Guest Room

FLOOR3

303 Vacant

Guest Room

FLOOR3

1

100

1 - 83 of 83 items

Sorted by name

83 Room(s)

Back to Registration

Next to Key Details

Summary

Key

Guest room: 301

Key Details

Expiration: 07/08/2025 04:27 PM

First name:

Last name:

Make Keys

- 4. 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.
- 5. 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](#).

Key Details

Key Expiration

7/8/2025 4:27 PM

First Name

Andy

Last Name

Andrews

Back to Rooms

Summary

Key

Guest room:

301

Key Details

Expiration:

07/08/2025 04:27 PM

First name:

Andy

Last name:

Andrews

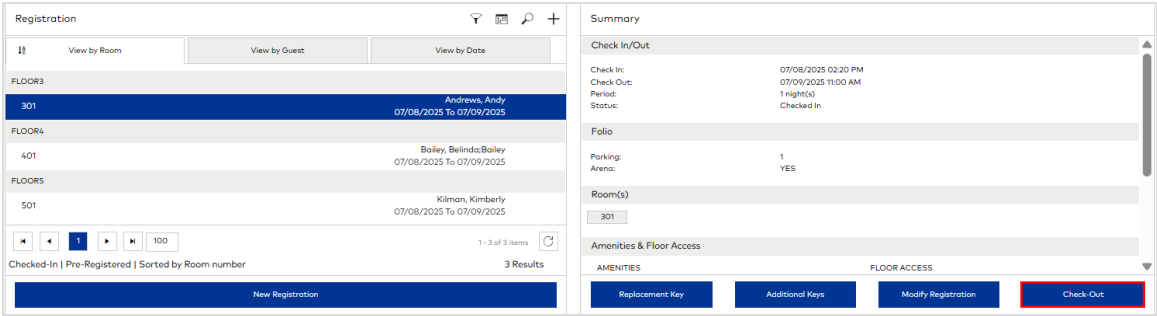
Make Keys

- 6. Specify first and last names of the guest.
- 7. (*optional*) Modify the expiration details.
- 8. Click [Make Keys](#).
- 9. Select an encoder that is online and available to the workstation, then click [Make Keys](#).
- 10. Present a key to the encoder (as prompted).
- 11. When notified that the key request is complete, click [Done](#).

Check out a registration

To check out a registration:

- 1. Go to [Guest Registration](#).
- 2. Click [Registrations](#).

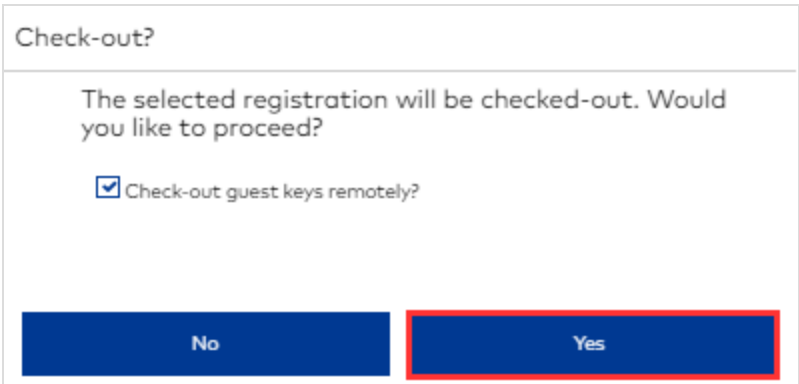


- 3. Select the registration that you want to check out. There are multiple options for finding a registration. You can filter the list to show only registrations that are checked in or pre-registered or both. You can constrain the list by specifying a check-in date range. You can search for a registration 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.

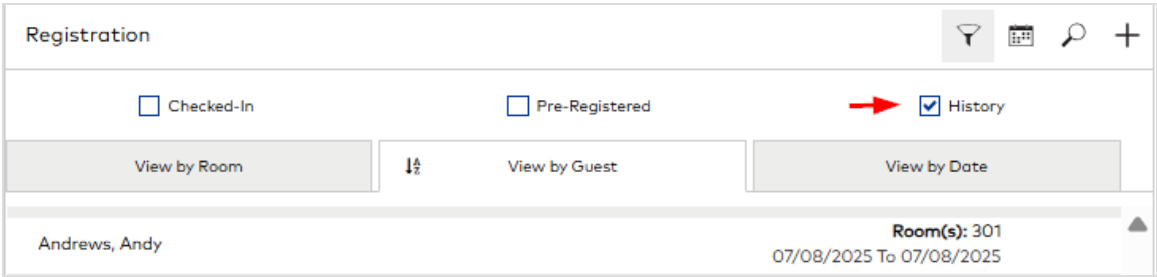


When online communication and remote guest check-out are enabled, Ambiance presents the option to check-out guest keys remotely. Depending on settings selected in [System Settings > Online Communication > Online Operations](#), the guest keys are remotely invalidated for guest rooms/suites/meeting rooms and guest common areas/elevators.

- 4. Click [Check Out](#).



- 5. When prompted to confirm checkout, click [Yes](#).
- The registration is now listed when the historical filter is selected.



Staff

This section includes the following subjects:

Learning about Staff Management and Staff Keys	189
Add staff members	190
Import staff member list	193
Make Emergency keys	195
Make Grand Master keys	198
Make Master keys	203
Make Limited Use Staff keys	207
Replace staff keys	210
Invalidate staff access	212
Test key files	217

Learning about Staff Management and Staff Keys

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 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.

You can add staff manually or import a list.

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 and notifications are enabled. The option to designate the staff member as an Operator is on this tab.
- **Operator Info**—This tab is where Operator access is configured. The tab is only active if the staff member is designated as an Operator.
- **Assigned Keys**—This tab lists active keys assigned to the staff member. You can cancel and/or replace keys in the list.
- **Staff Key Validation**—This tab displays when licensed for staff key validation. When displayed, enable and configure staff key validation settings for the staff member. Settings in the staff profile override system settings. By default, only Administrator and Site Configurator roles have the right to set staff key validator settings.

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).

Importing staff

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

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 defined in [Access Management > Credential Management](#) that may include access to any access point type.

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 [Assigned Keys](#) tab in the profile.

Staff keys are valid in staff and guest common areas and elevator controllers until key expiration is reached. Note that staff keys with the status *Obsolete* continue to allow access to common areas and elevator controllers until key expiration.

For information about invalidating staff access, see [Invalidating staff access](#).

Add staff members

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

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



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

To add a staff member:

1. Go to [Staff Management](#).
2. Click [\(Add\)](#) .

New Staff Member

First Name*

Jon

Middle Name

Middle Name

Last Name*

Do

Cancel

Save

3. Specify the name of the staff member. Use the middle name to distinguish between staff with the same first and last names. Max chars per field: 25.
4. Click [Save](#). 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, enable notifications for the staff member or designate the staff member as an Operator.



If phone/mobile number validation override is enabled in [System Settings](#), Operators can permit use of unknown numbers.

Jon Do

Staff Member Info | Operator Info | Assigned Keys

First Name*
Jon

Middle Name
Middle Name

Last Name*
Do

User type
Employee

ID
33332154

Email
jdo@domain.com

Mobile Number
+12818218212

Is an Ambiance Operator?
☐ NO

Upload Image

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 and to send notifications via email. (For Operators, the email address can be changed in account [Preferences](#).)
6. Select whether to enable notifications and, if enabled, select the notification groups to subscribe for the staff member.
7. Click ([Save](#)) .



When licensed for staff key validation, go to the Staff Key Validation tab to enable and/or configure staff key validation.

Enable and configure staff key validation

Settings in the staff profile override system systems.

Admin01 User

Staff Member Info

Operator Info

Assigned Keys

Staff Key Validation

Enable key validation for this staff member

☒ YES

PIN *



Enable overtime for this staff member

☒ YES

Authorized overtime (hours)

Overtime starts

Overtime ends

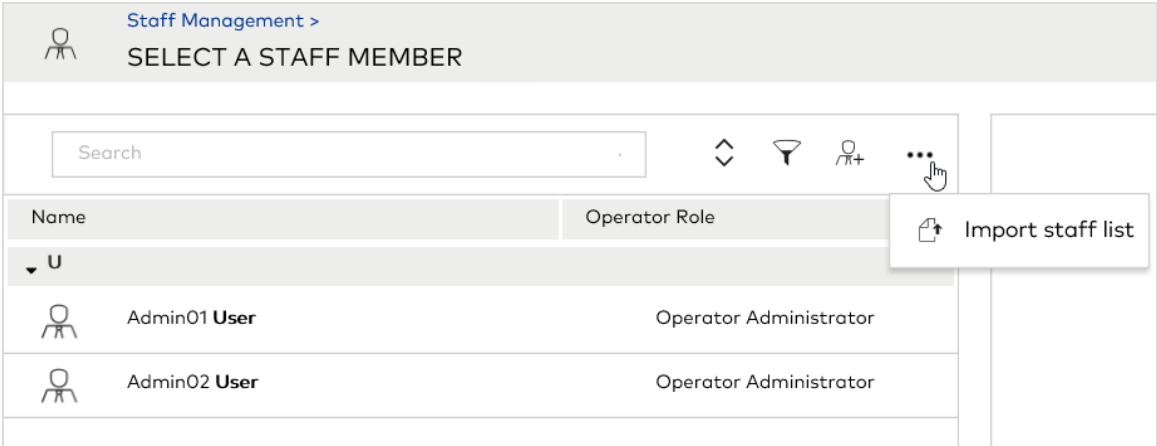


1. Select whether to enforce staff key validation for the staff member. When **YES**, the staff member must gain access at access points where staff key validators are installed, and use their unique PIN and key.
2. The PIN is a unique numeric code assigned to the staff member. Ambiance automatically generates the code based on the PIN length system setting. Click (View)  to see the code.
3. Select whether to enable overtime for this staff member. Default: NO
 - **Authorized overtime (hours)**—Select the number of hours in a given day that overtime is authorized for the staff member. Range: 1-16 hours. Default: 1.
 - **Overtime starts**—Select the date when overtime authorization starts.
 - **Overtime ends**—Select the date when overtime authorization ends.
4. Click **Save**.

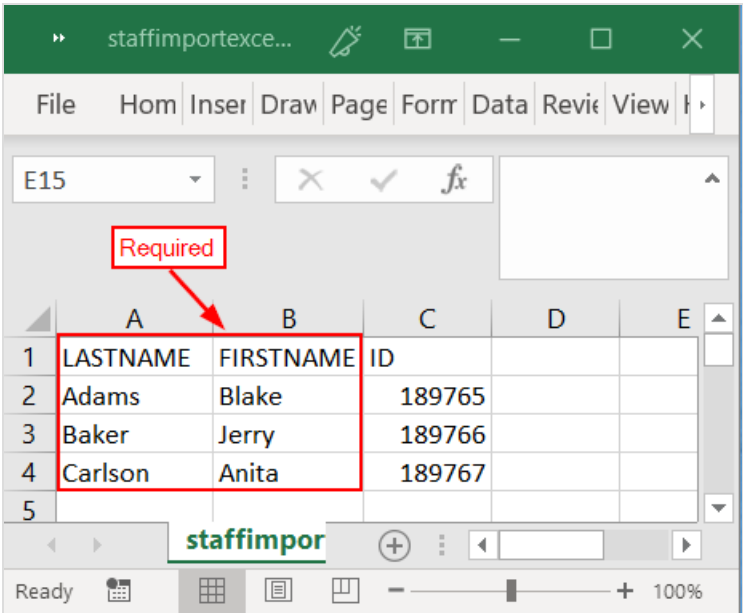
Import staff member list

To import staff:

- 1. Go to [Staff Management](#).
- 2. Click [\(More\)...](#) > [Import staff list](#).



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



If staff member profiles have already been created, you are prompted to proceed. Click [YES](#) to proceed.

- 4. When notified the import is successful, click [OK](#).

Search

Name	Operator Role
Blake Adams	
B	
Jerry Baker	
C	
Anita Carlson	
U	
Admin01 User	Operator Administrator
Admin02 User	Operator Administrator

1

100 items per page

1 - 5 of 5 items

Active | Sorted by Last Name

New staff member

Make Emergency keys

1. Go to [Staff Keys](#).
2. Select the [Emergency](#) credential class or a custom class based on the same type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.

Key

Credential class*

Emergency ▼

Credential*

Security ▼

☒ New key ☐ Additional key (Key IDs remaining: 255/255)

Shift schedule

24/7 ▼

Key expiration (expires at end of shift)

09/04/2026 

Next to additional access points

4. Select whether to make a [New](#) or [Additional](#) key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Take any of the following steps:
 - Click [Next to additional access points](#). This option is only presented when [Display additional access](#) is enabled in [System Settings > Staff Keys](#). Select the additional access points to add on the key. All access point types are listed. You can select access points from different buildings. The maximum access points that you can select are: 120 (4k keys), 94 (1k keys), 25 (mobile keys). Selected access points are added to the [Summary](#) section (listed by building and floor).

Access Points

BDMHH-Sou...

Administration

BDMHH-So...

FLOOR1

Camp

BDMHH-So...

FLOOR1

CampA

BDMHH-So...

FLOOR1

CampB

BDMHH-So...

FLOOR1

Casino

BDMHH-So...

FLOOR1

Cigar Humidor

BDMHH-So...

FLOOR1

Day camp

BDMHH-So...

FLOOR1

Office A-S

BDMHH-So...

FLOOR1

Platinum Lounge

BDMHH-So...

FLOOR1

Vault

BDMHH-So...

FLOOR1

Guest laundryS

BDMHH-So...

FLOOR5

1

100

1 - 17 of 17 items

Back to Key

Next to Key Holder

Summary

New Key

Credential class:

Emergency

Credential:

Security

Shift schedule:

24/7

Key expiration:

09/04/2026 12:00 AM- Expires at end of shift

Access Points

BDMHH-South

FLOOR1

Administration

Camp

CampA

CampB

Day camp

Office A-S

FLOOR5

Guest laundryS

ÉTAGE10

Rooftop terrace

Floor Access

FLOOR ACCESS

BDMHH-North - FLOOR0

BDMHH-North - FLOOR1

Make Keys

- Click [Next to Common Areas](#). (Aurora / MATRIX integrations only).
- Click [Next to Key Holder](#). Select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\)](#) , specify first and last names, then click [Save](#).

8. Click [Make Keys](#).



To make a mobile key, click [Send to mobile](#).

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

Make Keys

BDMHH_North

Key Holder	Keys	Progress
Anna Mahler	-1+	0 of 1 encoded No mobile number

Ready to start

Send to Mobile

Make Key

Done

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

13. When notified that the key request is complete, click [Done](#).
- The key is listed on the [Assigned Keys](#) tab in the staff member profile.

Anna Mahler					
Staff Member Info		Operator Info		Assigned Keys	
Key	Access	Creation Date	Expiration Date	Stat...	
	New Key: Emergency-Security (ID...	09/04/2025 02:40 PM	09/04/2026 11:59 PM	Active	

You can verify that a mobile key was delivered in [Staff Management](#).

Make Grand Master keys

1. Go to [Staff Keys](#).
2. Select the [Grand Master](#) credential class or a custom class based on the same type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.

Key

Credential class*

Grand Master ▼

Credential*

Maintenance ▼

☒ New key
 ☐ Additional key (Key IDs remaining: 255/255)

Shift schedule

24/7 ▼

Key expiration (expires at end of shift)

09/04/2026 

Next to additional access points

When you select a credential, floor access is dynamically selected based on the location of access points to be authorized on the key.

4. Select whether to make a [New](#) or [Additional](#) key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Take one of the following actions:
 - Click [Next to additional access points](#). This option is only presented when [Display additional access](#) is enabled in [System Settings > Staff Keys](#). Select the additional access points to add on the key. All access point types are listed. You can select access points from different buildings. The maximum access points that you can select are: 120 (4k keys), 94 (1k keys), 25 (mobile keys). Selected access points are added to the [Summary](#) section (listed by building

and floor).

Access Points

BDMHH-Nor...

Staff lounge	BDMHH-No...	FLOOR0
Kitchen	BDMHH-No...	FLOOR1
Spa	BDMHH-No...	FLOOR1

1

100

1 - 3 of 3 items

Back to Key

Next to Floor Access

Summary

New Key

Credential class:Grand Master

Credential:Maintenance

Shift schedule:24/7

Key expiration:09/04/2026 12:00 AM- Expires at end of shift

Access Points

BDMHH-North

FLOOR0

Staff lounge

FLOOR1

Kitchen

Floor Access

FLOOR ACCESS

BDMHH-North - FLOOR0

BDMHH-North - FLOOR1

BDMHH-North - FLOOR2

BDMHH-North - FLOOR3

BDMHH-North - FLOOR4

BDMHH-North - FLOOR5

BDMHH-North - FLOOR6

Make Keys

- Click [Next to Floor Access](#), [Next to Common Areas](#) or [Next to Common Areas & Floor Access](#). Select the common area and floor access to add on the key. Common areas are only presented when Ambiance is integrated with Aurora or MATRIX. By default, floor access is dynamically selected based on the location of access points to be authorized on the key.

Floor Access

Floors

▼ BDMHH-North

☒ FLOOR0

☒ FLOOR1

☒ FLOOR2

☒ FLOOR3

☒ FLOOR4

☒ FLOOR5

☒ FLOOR6

☒ FLOOR7

☒ FLOOR8

☒ FLOOR9

Back to Access Points

Next to Key Holder

- Click [Next to Key Holder](#). Select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\)](#) , specify first and last names, then click [Save](#).

8. Click [Make Keys](#):



To make a mobile key, click [Send to mobile](#).

- Specify the number of keys to make.
- Select an encoder that is online.
- Click [Make Key](#).
- Present keys to the encoder (as prompted).

Make Keys

BDMHH_North

Key Holder	Keys	Progress
Janice Bula	- 1 +	0 of 1 encoded No mobile number

Ready to start

Send to Mobile

Make Key

Done

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

13. When notified that the key request is complete, click [Done](#).
- The key is listed on the [Assigned Keys](#) tab in the staff member profile.

Janice Bula

Staff Member Info

Operator Info

Assigned Keys

Key	Access	Creation Date	Expiration Date	Status
	New Key: Grand Master-Maintenance... ...	09/04/2025 02:52 PM	09/04/2026 11:59 PM	Active

Access

New Key: Grand Master-Maintenance (ID: 1) Kitchen, Staff lounge FLOOR0, FLOOR1, FLOOR2, FLOOR3, FLOOR4, FLOOR5, FLOOR6, FLOOR7, FLOOR8, FLOOR9, FLOOR10 (24/7)

Cancel



You can verify that a mobile key was delivered in [Staff Management](#).

Make Master keys

1. Go to [Staff Keys](#).
2. Select the [Master](#) credential class or a custom class based on the same type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.

Key

Credential class*

Master

Credential*

Housekeeping1-N

☒ New key

☐ Additional key (Key IDs remaining: 254/255)

Shift schedule

Shift1

Key expiration (expires at end of shift)

09/04/2026

Next to additional access points

When you select a credential, floor access is dynamically selected based on the location of access points to be authorized on the key.

4. Select whether to make a [New](#) or [Additional](#) key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Take one of the following actions:
 - Click [Next to additional access points](#). This option is only presented when [Display additional access](#) is enabled in [System Settings > Staff Keys](#). Select the additional access points to add on the key. You can select access points from different buildings. The maximum access points that you can select are: 120 (4k keys), 94 (1k keys), 25 (mobile keys). Selected access points are added to the [Summary](#) section (listed by building and floor).

Access Points			BDMHH-No...		FLOOR1
Electronics	BDMHH-N...	FLOOR1			
Office A	BDMHH-N...	FLOOR1			
Office B	BDMHH-N...	FLOOR1			

Summary	
New Key	
Credential class:	Master
Credential:	Housekeeping1-N
Shift schedule:	Shift1
Key expiration:	09/04/2026 12:00 AM- Expires at end of shift

Access Points	
▼ BDMHH-North	
▼ FLOOR1	
☒ Office A	☒ Office B

Common Areas & Floor Access	
COMMON AREAS	FLOOR ACCESS
☒ Staff lounge	☒ BDMHH-North - FLOOR0 ☒ BDMHH-North - FLOOR1 ☒ BDMHH-North - FLOOR3 ☒ BDMHH-North - FLOOR4 ☒ BDMHH-North - FLOOR5 ☒ BDMHH-North - FLOOR6 ☒ BDMHH-North - FLOOR7 ☒ BDMHH-North - FLOOR8

Back to Key
Next to Common Areas & Floor Access
Make Keys

- Click Next to Common Areas, Next to Floor Access, or Next to Common Areas & Floor Access.

Common Areas & Floor Access	
Common Areas	Floors
☐ Clubhouse ☐ Spa ☒ Staff lounge	▼ BDMHH-North ☒ FLOOR0 ☒ FLOOR1 ☐ FLOOR2 ☒ FLOOR3 ☒ FLOOR4 ☒ FLOOR5 ☒ FLOOR6 ☒ FLOOR7 ☒ FLOOR8

Back to Access Points
Next to Key Holder
Back to Access Points
Next to Key Holder

- When the **Common Areas** tab is displayed, three specific access point types are listed: 1) Unlimited Staff Common Areas. These are selected by default and cannot be deselected. 2) Limited Guest Common Areas with staff access configured by Common Area Access profile. These can be selected/deselected. 3) limited Staff Common Areas selected in the Common Area Access profile associated with the selected credential. These can be selected/deselected.

- When the [Floor Access](#) tab is displayed, all floors where elevator access is configured are listed. By default, floor access is dynamically selected based on the location of access points to be authorized on the key.



Take caution to not remove default floor access.

- Click [Next to Key Holder](#). Select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\)](#) , specify first and last names, then click [Save](#).

8. Click [Make Keys](#).



To make a mobile key, click [Send to mobile](#).

- Specify the number of keys to make.
- Select an encoder that is online.
- Click [Make Key](#).
- Present keys to the encoder (as prompted).

Make Keys



BDMHH_North ▼

Key Holder	Keys	Progress
Pamela Jackson	- 1 +	 0 of 1 encoded  No mobile number

Ready to start

Send to Mobile

Make Key

Done



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

13. When notified that the key request is complete, click [Done](#).

The key is listed on the [Assigned Keys](#) tab in the staff member profile.

Pamela Jackson					
Staff Member Info		Operator Info		Assigned Keys	
Key	Access		Creation Date	Expiration Date	Status
	New Key: Master-Housekeeping1-N (ID: 1) Offic...		09/04/2025 03:16 PM	09/04/2026 01:00 PM	Active



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

Make Limited Use Staff keys

1. Go to [Staff Keys](#).
2. Select the [Limited Use Staff](#) credential class or a custom class based on the same type. Only those classes for which credentials are defined are listed.
3. Select a credential. Only those credentials made using the selected class are listed.

Key

Credential class*

Limited Use Staff ▼

Credential*

Interns ▼

☒ New key
 ☐ Additional key (Key IDs remaining: 255/255)

Shift schedule

Shift1 ▼

Key expiration (expires at end of shift)

09/04/2026 

Next to Common Areas & Floor Access

When you select a credential, floor access is dynamically selected based on the location of access points to be authorized on the key.

4. Select whether to make a [New](#) or [Additional](#) key. New keys invalidate existing active keys for the selected credential at all access points except common areas. Additional keys (copies) have no effect on existing active keys.
5. Select a shift schedule. The selected shift schedule determines the days and hours that the key is valid.
6. Specify a date after which the key is invalid.
7. Take one of the following actions:
 - Click [Next to Common Areas](#), [Next to Floor Access](#), or [Next to Common Areas & Floor Access](#).
 - When the [Common Areas](#) tab is displayed, three specific access point types are listed: 1) Unlimited Staff Common Areas. These are selected by default and cannot be deselected. 2) Limited Guest Common Areas with staff access configured by Common Area Access profile. These can be selected/deselected. 3) Limited Staff Common Areas selected in the Common Area Access profile associated with the selected credential. These can be selected/deselected.
 - When the [Floor Access](#) tab is displayed, all floors where elevator access is configured are listed. By default, floor access is dynamically selected based on the location of access points to be authorized on the key.



Take caution to not remove default floor access.

Common Areas & Floor Access

Common Areas

Floors

☒ Staff lounge

Back to Key

Next to Key Holder

Common Areas & Floor Access

Common Areas

Floors

BDMHH-North

☒ FLOOR0

☒ FLOOR1

☐ FLOOR2

☒ FLOOR3

☐ FLOOR4

☒ FLOOR5

☐ FLOOR6

Back to Key

Next to Key Holder

- Click [Next to Key Holder](#). Select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\)](#) , specify first and last names, then click [Save](#).

8. Click [Make Keys](#).



To make a mobile key, click [Send to mobile](#).

- specify the number of keys to make.
- Select an encoder that is online.
- Click [Make Key](#).
- Present keys to the encoder (as prompted).

Make Keys



BDMHH_North

Key Holder

Keys

Progress

Raja Patel

-

1

+

 0 of 1 encoded

 No mobile number

Ready to start

Send to Mobile

Make Key

Done



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

13. When notified that the key request is complete, click [Done](#).

The key is listed on the [Assigned Keys](#) tab in the staff member profile.

Raja Patel

Staff Member Info

Operator Info

Assigned Keys

Key	Access	Creation Date	Expiration Date	Status
	New Key: Limited Use Staff-Interns (ID: 1) St	09/04/2025 03:26 PM	09/04/2026 01:00 PM	Active

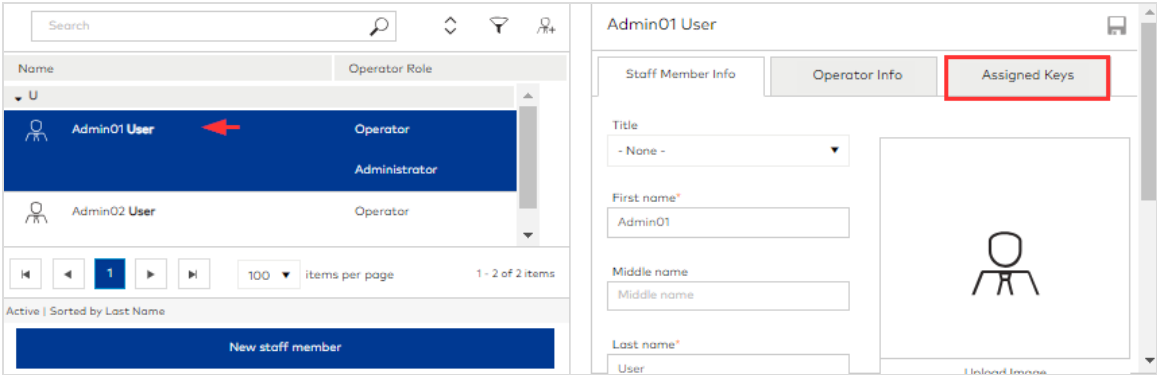


You can verify that a mobile key was delivered in Staff Management.

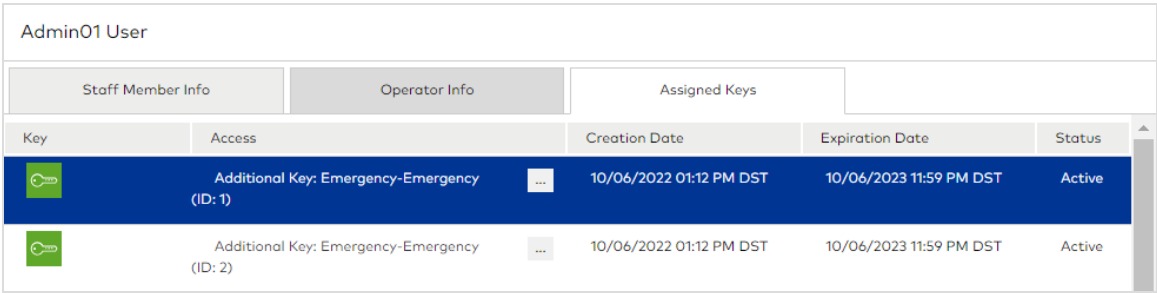
Replace staff keys

Staff Keys that are defective or lost can be replaced.

- 1. Go to [Staff Management](#).



- 2. Select the staff member whose key you want to replace.
- 3. Click the [Assigned Keys](#) tab.



- 4. Select the key that you want to replace.
- 5. Click [Replace Defective Key](#) or [Replace Lost Key](#).

Replace Defective Key

 Virtual 000000000001

Key Holder:	Admin01 User
Status:	Active
Access:	Additional Key: Emergency-Emergency (ID: 1) (24/7)
Created:	10/06/2022 01:12 PM
Expiration:	10/06/2023 11:59 PM

Keys

0 of 1 encoded

Ready to start

Make KeyDone

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



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

Invalidate staff 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.



You need to remove Operator access from a staff member



Demote operator

Change the [Is an Ambiance Operator](#) switch in the operator profile to **NO**. Without operator access, the staff member cannot log in to Ambiance.



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 Cancel Keys

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 when invalidating access using a physical key, access remains valid until the physical Cancel/Block/ELO/New key is presented to relevant locks.

Block/unblock operator access

Blocking an Operator prevents the Operator from logging in to 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.

The screenshot shows the profile page for Margo Adams. The 'Operator Info' tab is selected. A red arrow points to the 'Block software access' toggle switch, which is currently in the 'YES' position. Below this, there are two dropdown menus: 'Preferred language' set to 'English' and 'Ambiance Operator role*' set to 'Senior Staff Manager'. At the bottom, there is a button labeled 'Ambiance Login'.

4. For [Block software access](#):
 - To block access, slide the switch to [YES](#).
 - To unblock access, slide the switch to [NO](#).
5. Click [YES](#) to confirm.

Demote operator

To permanently remove operator access from a staff member:

1. Go to [Staff Management](#).
2. Select the operator profile.
3. On the [Staff Member Info](#) tab, change the [Is an Ambiance Operator?](#) switch to [NO](#).
4. Click [YES](#) to confirm. The [Operator Info](#) tab and access to Ambiance is disabled.

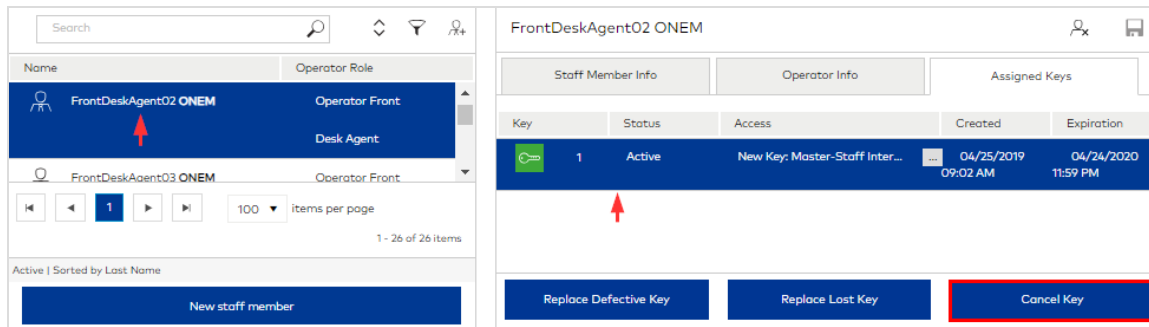
Cancel a specific staff key

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 [Assigned Keys](#) tab.
4. Select the key that you want to cancel.



FrontDeskAgent02 ONEM

Staff Member Info Operator Info Assigned Keys

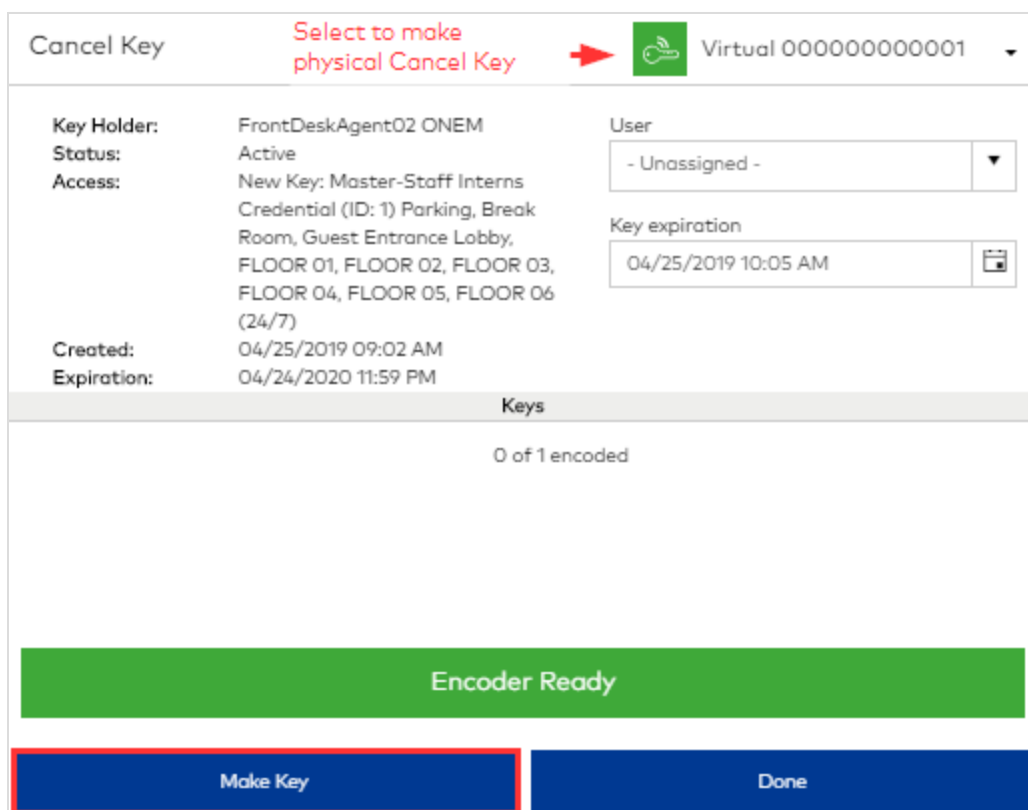
Key	Status	Access	Created	Expiration
1	Active	New Key: Master-Staff Inter...	04/25/2019 09:02 AM	04/24/2020 11:59 PM

Replace Defective Key Replace Lost Key **Cancel Key**

5. Click [Cancel Key](#)



To cancel a mobile key remotely, click [Cancel Mobile Key](#).



Cancel Key

Select to make physical Cancel Key → Virtual 000000000001

Key Holder: FrontDeskAgent02 ONEM
 Status: Active
 Access: New Key: Master-Staff Interns Credential (ID: 1) Parking, Break Room, Guest Entrance Lobby, FLOOR 01, FLOOR 02, FLOOR 03, FLOOR 04, FLOOR 05, FLOOR 06 (24/7)
 Created: 04/25/2019 09:02 AM
 Expiration: 04/24/2020 11:59 PM

User: - Unassigned -
 Key expiration: 04/25/2019 10:05 AM

Keys
 0 of 1 encoded

Encoder Ready

Make Key Done

6. (optional) Select the staff to whom you want to assign the key.
7. (optional) Specify a date after which the Cancel Key is invalid.
8. Select an encoder that is online.
9. Click [Make Key](#).
10. Present a key to the encoder.
11. When notified that the key request is complete, click [Done](#).

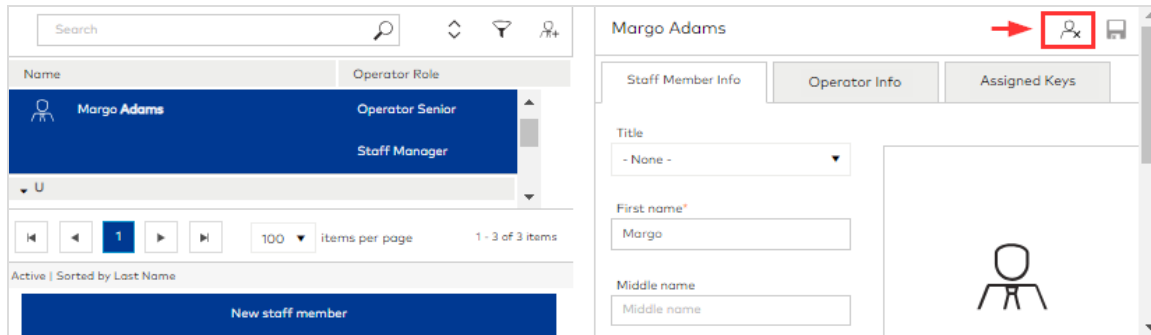


Physical Cancel Keys must be presented to access points to invalidate a mobile key. You can verify mobile keys are canceled on the [Assigned Keys](#) tab in the staff member profile.

Deactivate a staff member

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.

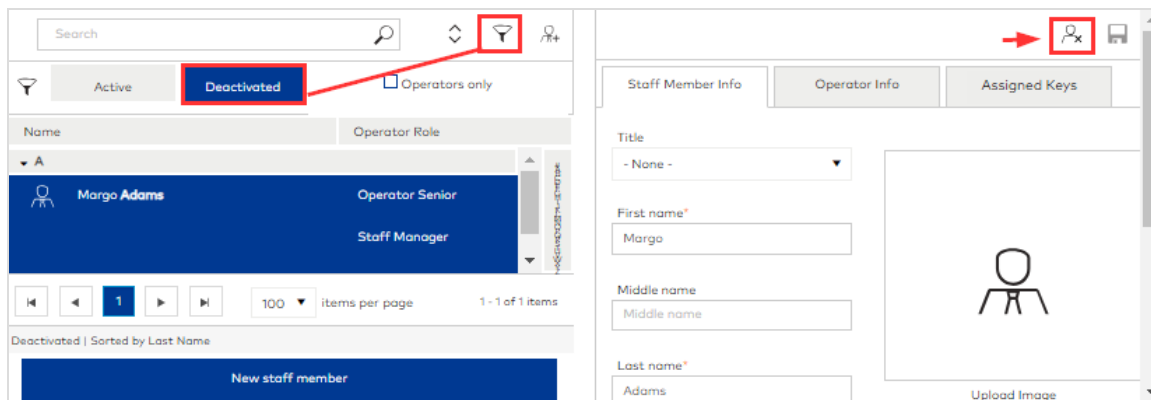
1. Go to **Staff Management**.



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 excluding common areas 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.



New keys do not invalidate access to common areas on existing keys. Common area access is valid until key expiration. If the credential includes access to common areas, make Cancel keys to invalidate access (instead of New keys).

Block staff access to a specific credential

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.



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

For instructions, see [Block/Unblock Keys](#).

Temporarily invalidate all non-emergency access

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](#).

Test key files

Test key files are used by customers who conduct key testing before making keys. The function is available for staff keys only when the Enable test key file creation right is enabled in Role Management for the active Operator. Test key files contain all of the information that will be encoded on the actual staff keys.

System Rights	Key Rights					
► Rights	Administrator	Front Desk Agent	Site Configurator	Staff Manager	Mobile key tester	Super key test
► Read Keys	☒	☐	☒	☒	☒	☒
► Reports	☒	☐	☒	☐	☐	☒
▼ Staff Keys	☐	☐	☐	☐	☒	☒
Enable Test Key File Creation	☐	☐	☐	☐	☒	☒
Staff Key Encoding	☒	☐	☒	☒	☒	☒
► Staff Management	☒	☐	☒	☒	☒	☒
► System Keys	☒	☐	☒	☐	☐	☒
► System Settings	☒	☐	☒	☐	☐	☒



The Enable test key file creation right is disabled in all default roles. You must create a custom role to enable the right.

To make a test key file:

1. Go through the same steps that you would to make a staff key.

Summary

Additional Key

Credential class: Master
 Credential: Another Master all rooms
 Shift schedule: No schedule
 Key expiration: 06/04/2020 - Expires at end of shift

Common Areas

Key Holder

Make Keys

Create Test Key File

2. Click Create Test Key File (instead of Make Keys).

Create Test Key File

File password

File password confirmation

Cancel

Create File

3. Specify and confirm a password for the file.
4. Click [Create File](#). The file (.ekf) is generated and accessible from the system tray.



Programming/Auditing

This section includes the following subjects:

Reprogram locks	220
Audit locks	222
Audit online access points	223

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 > Programming](#).

The screenshot shows the 'Programming' interface in Ambiance. On the left, under 'Access Points', the 'DK-Towers-SMT' dropdown is selected. A red box highlights the 'Requires Synchronization' filter. Below it, a table lists access points like 'Guest Room 901', 'Guest Room 902', and 'Guest Room 903'. On the right, the 'Summary' section shows a tree view of 'DK-Towers-SMT' with 'FLOOR1' and 'FLOOR2' expanded. 'FLOOR1' shows 'M...' and 'FLOOR2' shows multiple 'G...' entries. Below this, the 'Programming Options' section has a checkbox for 'Lock out current guests on programming' with a red arrow pointing to it and the text 'Only applies when keys are made'. At the bottom right, a red box highlights the 'Transfer' button.

2. 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.
3. 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.
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.

The screenshot shows a confirmation dialog box with the text: "The selected access point(s) have been transferred to the Maintenance unit. The maintenance unit can be unplugged." At the bottom, there are two buttons: "Cancel" and "OK". The "OK" button is highlighted with a red box.

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



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

Audit locks

This procedure documents how to audit locks using the M-Unit procedure. If fewer than five locks are being audited for troubleshooting purposes, using an Audit Key is an alternative to the M-Unit procedure. Refer to "Special Function Keys" in [System Keys](#).



Some steps are performed on the M-Unit (Maintenance Unit). For official instructions, refer to the documentation distributed with your device. If M-Unit authentication is enabled in [System Settings > Security > M-Unit](#) credentials must be configured in [Staff 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

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

When online communication is enabled in [System Settings](#), online access points can be audited directly in 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 > Online Access Points](#).
2. Select an access point.
3. Click [Audit Access Points](#).

When the audit is complete, the file is accessible from the [Summary](#) section.

System Keys

System Keys

This section includes the following subjects:

Learning about System Keys	225
Block and unblock keys	227
Cancel keys	231
Diagnostic keys	233
Electronic lockout keys	235
Failsafe keys	237
Inhibit keys	238
Latch and unlatch keys	240
Primary and secondary program keys	242
Resequence keys	245
Special function keys	247

Learning about System Keys

The [System Keys](#) module is used to encode keys for immediate intervention and to perform advanced operational programming.

System keys and supported access point types

All access point types are supported for all system keys with the following exceptions:

- Diagnostic keys are not compatible with NFC lock models: RT+, Saffire, MT6, and Confidant NFC.
- Failsafe keys do not support staff common areas and restricted areas.
- Inhibit keys do not support staff common areas and restricted areas.
- Unblock keys do not support common areas.

Block and unblock keys

Make a Block Key to invalidate all instances of a specific credential. For example, make a Block Key to invalidate all active keys for Guest Room 100. When making a Block Key, you must select the credential class and credential encoded on the key that you want to block. If the intent is to temporarily block access, you can use an Unblock Key to unblock a key that was previously blocked by a Block Key.



When the licensed feature online communication is enabled, remote operation is supported.



Remember that the block key must be presented at access points before access is blocked.

Cancel keys

Make a Cancel Key to permanently invalidate a specific key instance. When making a Cancel Key in System Keys, you must select the credential class and credential encoded on the key that you want to cancel. A Cancel Key must be presented to all access points for which the original key has credentials.



When the licensed feature online communication is enabled, remote operation is supported.

Diagnostic keys

Diagnostic Keys query locks to extract and report the status of various lock functions and are most often used for troubleshooting. Results of the query are communicated by an LED flash sequence.

ELO keys

ELO (Electronic Lockout) Keys temporarily invalidate all non-emergency keys by double locking the door from the outside (activating the privacy switch or deadbolt). When an electronic lockout is active, only a key with the Emergency credential can open the lock. When the electronic lockout is removed, normal key access resumes. ELO Keys are toggle keys. The behavior of the key alternates (applies lockout/removes lockout) each time it is presented to the lock.



When the licensed feature online communication is enabled, remote operation is supported.

Failsafe keys

Failsafe Keys are backups of individual guest room keys that are made in advance and maintained in complete sets to be issued in the event a system or power failure. All Failsafe Keys are encoded with default floor and amenity access.

The recommendation is to create and always retain three sets of two keys for each guest room and suite door. You can make as many key sets as you require; however, when a key from one set is presented to the lock, all keys from a previously used set are invalidated.

Default settings for Failsafe Keys are defined in [System Settings > Failsafe Keys](#).



It is critical that Failsafe Keys are current and stored in an efficient filing system at a secure location.

Inhibit keys

Inhibit Keys are used to permanently cancel current 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 guest room even if the dead bolt or privacy switch is active.



When the licensed feature online communication is enabled, remote operation is supported.

Latch, unlatch and toggle latch/unlatch keys

Latch Keys disable passage mode. Access is restricted to only those people with keys encoded with the applicable credential. Unlatch Keys enable passage mode. Passage mode is a lock state during which the access controls programmed in the lock are suspended allowing unrestricted access. Toggle Latch/Unlatch Keys enable and disable passage mode, alternately.

Primary and secondary program keys

Primary Program Keys (PPKs) put the lock into programming mode and are used in conjunction with Program Information (PI) Keys and Program Status (PS) Keys to program locks and authorize special functions (see Create a Special Function Key). They are also used to reprogram the current Secondary Program Key (SPK) or remaster a different SPK. Secondary Program Keys (SPKs) reprogram or resynchronize the current Primary Program Key (PPK) into access points and remaster a different PPK into a lock. Essentially, an SPK is a backup to the PPK but does not put locks into programming mode.

Resequence keys

Resequence Keys resynchronize a specific key credential in access points. The Resequence Key is used to update the sequence number stored in the lock's memory when the number of new keys made but not used in the lock exceeds the programmed sequence range for that key.



When the licensed feature online communication is enabled, remote operation is supported.

Special function keys

Special function keys are paired with primary program keys to perform system-level operations on a lock.

Block and unblock keys

Create a Block Key to block all active key instances of a specific credential. Before making a Block Key, you must know the credential class and credential (or access point) that you want to block.



Before blocking a common area, note that the Unblock Key does not restore access to common areas for the key when access to the common area is based on a common area profile.

Block Keys can be used to invalidate:

- 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 > Block Keys*.

The screenshot shows a web interface for creating a block key. The main section is titled 'Key Info'. Below this title, there is a 'Key expiration' label followed by a text input field containing '11/22/2018 11:40 AM'. To the right of the input field are two small icons: a calendar and a clock. At the bottom of the form, there are two buttons: a blue 'Back' button and a blue 'Next to Credentials' button. The 'Next to Credentials' button is highlighted with a red rectangular border. A red arrow points to the 'Key expiration' input field.

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

4. Select the credential class under which the credential you want to block is defined. Only those classes for which active keys exist are listed.
5. Select the credential (or access point) that you want to block. You can select an access point from a different building.
6. Take any of the available actions or proceed to the next step:
 - Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add) +**, specify first and last names, then click **Save**.
7. Click **Make Keys**.



if online communication is enabled, you can also click [Block Keys Remotely](#).

8. Select an encoder that is online.
9. Present a key to the encoder (as prompted).
10. Click **Start**.
11. When notified that the key request is complete, click **Done**.

Remember that physical keys must be presented to locks.

Make unblock keys

Unblock Keys unblock all instances of a specific credential in access points which have been previously blocked using the Block Key.

1. Go to [System Keys > Unblock Keys](#).

Key Info

Key expiration

11/22/2018 11:52 AM

Back

Next to Credentials

2. Specify expiration details.
3. Click [Next to Credentials](#).

Staff

WeekdayCrew1

WeekendCrew2

Sort By Name

Back to Key Info

Next to Key Holder

Summary

Key Info

Key type:

Unblock Keys

Key expiration:

11/22/2018 11:59 AM

Credential

Staff

WeekdayCrew1

Key Holder

Make Keys

4. Select the credential class for the credential or access point encoded on the key that you want to unblock. Only those classes for which active keys exist are listed.
5. Select the credential (or access point) encoded on the key that you want to unblock.
6. (optional) Click [Next to Key Holder](#) and select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\) +](#), specify first and last names, then click [Save](#).
7. Click [Make Keys](#).



If online communication is enabled, you have the option to click [Unblock Keys Remotely](#).

8. Select an encoder that is online.
9. Present a key to the encoder (as prompted).
10. Click [Start](#).
11. When notified that the key request is complete, click [Done](#).

Remember that physical keys must be presented to locks.

Cancel keys

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

!

When using a Cancel key to invalidate a staff key, the status of the staff key must be Active to invalidate access to common areas. If the key status is Obsolete, access to the common areas remains valid until key expiration.

Cancel keys can be used to invalidate:

- staff keys
- ELO keys
- Latch/Unlatch/Toggle Latch/Unlatch keys
- Inhibit keys

To make cancel keys:

1. Go to [System Keys > Cancel Keys](#).

Key Info

Key expiration

04/18/2019 09:43 PM

Back

Next to Credentials

Summary

Key Info

Key type:Cancel Keys

Key expiration:04/18/2019 09:43 PM

Credential

Key

Key Holder

Make Keys

2. Specify expiration details.
3. Click [Next to Credentials](#).

Emergency

Emergency

Sort By Name

Back to Key Info

Next to Keys

Summary

Key Info

Key type:Cancel Keys

Key expiration:04/18/2019 10:06 PM

Credential

Emergency

Emergency

Make Keys

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

Keys

Key Holder

Key ID

Unknown1

Margo Adams2

Full Name

Back to Credentials

Next to Key Holder

Summary

Key Info

Key type: Cancel Keys

Key expiration: 04/18/2019 10:06 PM

Credential

EmergencyEmergency

Make Keys

7. Select the key that you want to cancel. You can view the list of keys by Key Holder or by Key ID.

8. (optional) Click [Next to Key Holder](#) and select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\) +](#), specify first and last names, then click [Save](#).

9. Click [Make Keys](#).
- If online communication is enabled, you can also click [Cancel Keys Remotely](#).
10. Select an encoder that is online.

11. Present a key to the encoder (as prompted).

12. Click [Start](#).

13. When notified that the key request is complete, click [Done](#).

Diagnostic keys

Diagnostic keys query locks to extract and report the status of various lock functions and are most often used for troubleshooting. Results of the query are communicated by an LED flash sequence.



A simpler alternative to making diagnostic keys is to use the M-Unit (Maintenance Unit) to run a diagnostic on locks. The results of the query are in readable text format instead of an LED flash sequence.

Diagnostic keys are not compatible with newer NFC lock models: RT+, Sapphire, MT6 and Confidant NFC.

Make diagnostic keys

1. Go to *System Keys > Diagnostic Keys*.

Key	Summary
Select the type of diagnostic that you want to run Auto-Lock Status Clock Date Clock Run Test	Key Info Key type: Diagnostic Keys
Back	Make Keys

2. Select the type of diagnostic that you want to run.
 - **Auto-Lock Status**—Select this option to query the lock for Auto-Latch Schedules.
 - **Clock Date**—Select this option to query the lock for the date.
 - **Clock Run Test**—Select this option to test the lock clock function.
 - **Clock Time**—Select this option to query the lock for the time.
 - **Deadbolt Switch Status**—Select this option to query whether the lock deadbolt is projected or retracted.
 - **EPROM Version**—Select this option to retrieve the version of the micro-controller in the lock.
 - **Knob Switch Status**—Select this option to determine whether the lock is engaged or open.
 - **Last 2 LPI Records**—Select this option to query the lock for the two most recent errors.
 - **LED Lights Test**—Select this option to test the lock LED.
 - **Low Battery Status**—Select this option to learn the remaining battery charge for the lock.
 - **Motor Switch + Lock State**—Select this option to retrieve the status of the lock motor and lock state.
 - **Verify Lock Version**—Select this option to retrieve the lock firmware version.

Key	Summary
Auto-Lock Status Clock Date Clock Run Test	Key Info Key type: Diagnostic Keys Key: Auto-Lock Status
Back	Make Keys

3. Click [Make Keys](#).
4. Select an encoder that is online.
5. Present a key to the encoder (as prompted).
6. Click [Start](#).
7. When notified that the key request is complete, click [Done](#).

Diagnostic results

For details about interpreting a flash sequence, see "Troubleshooting Locks."

LED flash sequence

Each color of light has a different base value:

- Green=100
- Yellow=10
- Red=1

To interpret a response, multiply the number of times that each color flashes by the base value. For example, if the sequence of lights is two yellow flashes followed by three red flashes, the response value is 23.

$\text{Yellow}(10) \times 2 + \text{Red}(1) \times 3 = 23$

Diagnostic elements

Each Diagnostic Key provides several pieces of information. Each piece of information is known as an element, and you must be familiar with the elements that will be displayed in order to understand the response.

For example, the Display Clock Time Key will give you information on the following elements:

- Date/Time/DST Problem (if any) (0-4)
- DST Status (0-1)
- Hours (In Military Time) (0-23)
- Minutes (0-59)

When you use the card, the response begins and ends with a delimiter that consists of all three lights flashing simultaneously. This delimiter is also used to separate the responses to each element.

Electronic lockout keys

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

ELO keys are toggle keys. The behavior of the key alternates (applies lockout/removes lockout) each time it is presented to the lock.

To make ELO keys:

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

1. Go to [System Keys > Electronic Lockout Toggle Keys](#). The default credential [ELO](#) is required.

Key Info

Credential*

Electronic Lockout Toggle

☒ New key

☐ Additional key

Shift schedule

24/7

Key expiration

07/30/2026 11:50 AM

Back

Next to Key Holder

Summary

Key Info

Credential class:Electronic Lockout Toggle

Credential:Electronic Lockout Toggle

Key mode:New key

Shift schedule:24/7

Key expiration:07/30/2026 11:50 AM (expires at end of shift)

Key Holder

Make Keys

2. Select whether to make a New or Additional key. If no active key exists, a New key is required. If an active key exists, [Additional key](#) is the selected default. Making an Additional key (copy) has no effect on existing active keys. Making a New key when an active key exists, invalidates the previously active key.
3. Select a shift schedule. To enable 24/7 access, select [24/7](#). To review shift schedule details, see [Access Management > Shift Schedules](#). The selected shift schedule determines the days and hours that the key is valid.
4. Specify expiration details.
5. (optional) Click [Next to Key Holder](#) and select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\) +](#), specify first and last names, then click [Save](#).
6. Click [Make Keys](#).

 If online communication is enabled, you have the option to click [ELO Keys Remotely](#).

7. Select an encoder that is online.
8. Present a key to the encoder (as prompted).
9. Click [Start](#).
10. When notified that the key request is complete, click [Done](#).

Electronic lockout key LED flash sequence

For details about interpreting a flash sequence, see "Troubleshooting Locks."

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

Failsafe keys

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

Using a Failsafe Key invalidates previous guest key access to guest rooms, suite common doors and suite inner doors.

To create a Failsafe key set:

1. Go to [System Keys > Failsafe Keys](#).

The screenshot displays the 'Failsafe Keys' configuration interface. On the left, under the 'Access Points' section, a list of rooms is shown for 'FLOOR3'. Room '301' is highlighted. Below the list are navigation buttons (Previous, First, Next, Last) and a pagination indicator '1 - 100 of 101 items'. A 'Sort By' dropdown is set to 'Name'. At the bottom left is a 'Back' button. The right panel, titled 'Summary', shows the configuration for the selected access point '301'. It includes fields for 'Stay duration (days)' set to 1, 'Check-out time' set to 11:00 AM, and 'Number of keys' set to 3. Each of these fields has minus and plus buttons for adjustment. At the bottom right is a 'Make Keys' button.

2. Select an access point. You can select an access point from any building on site.
3. Specify the number of nights access to the Guest Room is enabled.
4. Specify the time after which the key expires (on the final day the key is active).
5. Specify the number of keys to make.
6. Click [Make Keys](#).
7. Select an encoder that is online.
8. Specify the number of keys to make.
9. Present a key to the encoder (as prompted).
10. Click [Start](#).
11. When prompted that keys were made successfully, click [Done](#).

Inhibit keys

Inhibit Keys are used to permanently cancel current 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.

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

Make inhibit keys

1. Go to [System Keys > Inhibit Keys](#). The default credential **Inhibit** is required.

Key Info

Credential*

Inhibit

☒ New key

☐ Additional key

Shift schedule

24/7

Key expiration

07/30/2026 12:06 PM

Back

Next to Key Holder

Summary

Key Info

Credential class:

Inhibit

Credential:

Inhibit

Key mode:

New key

Shift schedule:

24/7

Key expiration:

07/30/2026 12:06 PM (expires at end of shift)

Key Holder

Make Keys

2. Select whether to make a New or Additional key. if no active key exists, a New key is required. if an active key exists, **Additional key** is the selected default. Making an Additional key (copy) has no effect on existing active keys. Making a New key when an active key exists, invalidates the previously active key.
3. Select a shift schedule during which the key is valid. To enable 24/7 access, select **24/7**. To review shift schedule details, see [Access Management > Shift Schedules](#). The selected shift schedule determines the days and hours that the key is valid.
4. Specify expiration details.
5. (optional) Click **Next to Key Holder** and select the staff member to whom you want to assign the key. To add a staff member, click **(Add) +**, specify first and last names, then click **Save**.
6. Click **Make Keys**.
7.  If online communication is enabled, you have the option to click [Inhibit Keys Remotely](#).
-
8. Select an encoder that is online.
9. Present a key to the encoder (as prompted).
10. Click **Start**.
11. When notified that the key request is complete, click **Done**.

Inhibit key LED flash sequence

For details about interpreting a flash sequence, see "Troubleshooting Locks."

- The following LED flash sequence displays when an Inhibit Key is first presented:
 - Red (1) Yellow (12)

- The following LED flash sequence displays when the lock has already been inhibited:
 - Yellow (12)

Latch and unlatch keys

The following system keys latch and unlatch locks:

- **Latch keys**—Disable passage mode. Access is restricted to only those people with keys encoded with the applicable credential.
- **Unlatch keys**—Enable passage mode. Passage mode is a lock state during which the access controls programmed in the lock are suspended allowing unrestricted access.
- **Toggle latch/unlatch keys**—Enable and disable passage mode. Passage mode is a lock state during which the access controls programmed in the lock are suspended allowing unrestricted access. A toggle key alternatives behavior each time the key is presented to the lock.

To make Latch, Unlatch, and Latch/Unlatch Keys:

1. Go to [System Keys](#).
2. Select the type of key to make:
 - [Latch Keys](#)
 - [Unlatch Keys](#)
 - [Toggle Latch/Unlatch](#)

Key Info	Summary										
Credential class* Latch ▼ Credential* Latch ▼ ☒ New key ☐ Additional key Shift schedule 24/7 ▼ Back Next to Key Holder	Key Info <table> <tr> <td>Credential class:</td> <td>Latch</td> </tr> <tr> <td>Credential:</td> <td>Latch</td> </tr> <tr> <td>Key mode:</td> <td>New key</td> </tr> <tr> <td>Shift schedule:</td> <td>24/7</td> </tr> <tr> <td>Key expiration:</td> <td>07/30/2026 12:13 PM (expires at end of shift)</td> </tr> </table> Key Holder Make Keys	Credential class:	Latch	Credential:	Latch	Key mode:	New key	Shift schedule:	24/7	Key expiration:	07/30/2026 12:13 PM (expires at end of shift)
Credential class:	Latch										
Credential:	Latch										
Key mode:	New key										
Shift schedule:	24/7										
Key expiration:	07/30/2026 12:13 PM (expires at end of shift)										

3. The credential class selected by default ([Latch](#), [Unlatch](#), [Toggle Latch/Unlatch](#)) or a custom credential class based on the respective type is required.
4. Select the credential that you want to latch, unlatch, or latch/unlatch.
5. Select whether to make a New or Additional key. If no active key exists, a New key is required. If an active key exists, [Additional key](#) is the selected default. Making an Additional key (copy) has no effect on existing active keys. Making a New key when an active key exists, invalidates the previously active key.
6. Select a shift schedule during which the key is valid. To enable 24/7 access, select [24/7](#). To review shift schedule details, see [Access Management > Shift Schedules](#). The selected shift schedule determines the days and hours that the key is valid.
7. Specify expiration details.
8. (optional) Click [Next to Key Holder](#) and select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\) +](#), specify first and last names, then click [Save](#).
9. Click [Make Keys](#).
10. Select an encoder that is online.
11. Specify the number of keys to make.
12. Present a key to the encoder.

13. Click [Start](#).
14. When notified that the key request is complete, click [Done](#).

Primary and secondary program keys

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

Make primary program key

1. Go to *System Keys > Primary Program Keys*.

Key Info Key expiration 07/31/2025 04:00 PM  	Summary Key Info Key expiration: 07/31/2025 04:00 PM Key Option
Back Next to Key Options	Make Keys

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

Key Options ☒ Option ☒ Remaster a different SPK key into locks ☒ Reprogram an out-of-sequence SPK key into locks ☒ Use with PI autolatch keys ☒ Use with PI basic key ☒ Use with PI clock keys ☒ Use with PI DST keys ☒ Use with PI key and pass mastering keys/standard level keys	Summary Key Info Key expiration: 07/31/2025 04:00 PM Key Option
Back to Key Info Next to Key Holder	Make Keys

4. Select options to encode on the key. All options are selected by default.



All PI options remain in the software to support legacy systems. For guidance on these options, contact dormakaba Technical Support.

- **Remaster a different SPK key into locks**—This option is only selected in rare cases when the PPK has been compromised and must be remastered. Before remastering the SPK, you must use the SPK to remaster a new PPK.

Select this option to encode a PPK that authorizes a key to reprogram a Secondary Program Key.

- [Reprogram an out-of-sequence SPK key into locks](#)—This option is only selected in rare cases. Select this option to encode a PPK that authorizes a key to reprogram a Secondary Program Key.
 - [Use with PI autolatch keys](#)—Select this option to encode a PPK that authorizes a key to program auto-latch/unlatch schedules in the lock.
 - [Use with PI basic key](#)
 - [Use with PI clock keys](#)—Select this option to encode a PPK that authorizes a key to synchronize the lock clock.
 - [Use with PI DST keys](#)—Select this option to encode a PPK that authorizes a key to update daylight savings time settings in the lock.
 - [Use with PI key and pass mastering keys/standard level keys](#)
 - [Use with PI level program keys](#)
 - [Use with PS battery disconnect key](#)—Select this option to encode a PPK that authorizes a key to shut down the lock before the lock battery disconnects.
5. (optional) Click [Next to Key Holder](#) and select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\) +](#), specify first and last names, then click [Save](#).
 6. Click [Make Keys](#).
 7. Select an encoder that is online.
 8. Present a key to the encoder.
 9. Click [Start](#).
 10. When notified that the key request is complete, click [Done](#).

Make secondary program key

To make a Secondary Program Key:

1. Go to [System Keys > Secondary Program Keys](#).

Key Info	Summary
Key expiration 07/31/2025 04:00 PM   Remaster Primary Programming Key (PPK)? ☒ YES ☐	Key Info Key expiration: 07/31/2025 04:00 PM Key Holder
Back Next to Key Holder	Make Keys

2. Specify expiration details.
3. Select whether to remaster the PPK. Remastering a PPK is a rare occurrence and is used to reprogram the current PPK or remaster a different PPK into a lock. This remastering should only be made at the direction of dormakaba Technical Support. If you select to remaster, all keys become invalid and all locks must be reprogrammed.
4. (optional) Click [Next to Key Holder](#) and select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\) +](#), specify first and last names, then click [Save](#).
5. Click [Make Keys](#).
6. Select an encoder that is online.

7. Present a key to the encoder.
8. Click [Start](#).
9. When notified that the key request is complete, click [Done](#).

Secondary program key LED flash sequence

For details about interpreting a flash sequence, see "Troubleshooting Locks."

The following LED flash sequence displays when an SPK is first presented:

Yellow (slow flashing for 20 seconds)

Resequencing keys

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

Resequencing Keys can be used to correct the sequence on:

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

Make resequencing keys

1. Go to *System Keys > Resequencing Keys*.

Key Info

Key expiration

07/30/2026 04:02 PM



Back

Next to Credentials

Summary

Key Info

Key type:

Resequencing Keys

Key expiration:

07/30/2026 04:02 PM

Credential

Key Holder

Make Keys

Resequencing Keys Remotely

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

The screenshot shows a web interface for managing keys. On the left, a dropdown menu is set to 'Master'. Below it, a list of credentials is shown, with 'Housekeeping1-N' highlighted in blue. At the bottom of this list is a 'Sort By' section with a dropdown set to 'Name' and a 'Back to Key Info' button. On the right, a 'Summary' section contains three sub-sections: 'Key Info' (Key type: Resequence Keys, Key expiration: 07/30/2026 04:02 PM), 'Credential' (Credential class: Master, Credential: Housekeeping1-N), and 'Key Holder'. At the bottom of the right pane is a 'Make Keys' button.

4. Select the credential class. Select the credential class for the credential or access point encoded on the key that you want to resequence. Only those classes for which active keys exist are listed.
5. Select the credential. Select the credential (or access point) encoded on the key that you want to resequence. You can select a credential from any building.
6. (optional) Click [Next to Key Holder](#) and select the staff member to whom you want to assign the key. To add a staff member, click [\(Add\) +](#), specify first and last names, then click [Save](#).
7. Click [Make Keys](#).



If online communication is enabled, you can also click [Resequence Keys Remotely](#).

8. Select an encoder that is online.
9. Present a key to the encoder (as prompted).
10. Click [Start](#).
11. When notified that the key request is complete, click [Done](#).

Resequence key LED flash sequence

For details about interpreting a flash sequence, see "Troubleshooting Locks."

- The following LED flash sequence displays when a Resequence Key is first presented:
 - Green and Yellow (6)
- The following LED flash sequence displays when a Resequence Key is presented to a lock that is not out of sequence:
 - Yellow (6)

When using a Resequence Key for guest levels, a new guest key must be made if a red flash precedes the green/yellow flashes.

Special function keys

Special function keys are paired with primary program keys to perform system-level operations on a lock.



Special function keys are supported for legacy systems. A simpler alternative to making SFKs is to use the M-Unit (Maintenance Unit) to interrogate (audit) a lock. All data that can be obtained by using an SFK is included in audit reports.

Special function key types

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

- **Audit Key**—Requires 4K key. Select this option to make a key that audits a lock to obtain status and diagnostic data. A maximum of 172 records can be stored on an Audit Key. After auditing a lock with an Audit Key, present the key to the encoder and click the Read Key button in the 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.
- **Disable/Enable Lock Change Key**—Select this option to make a key that disables all key and M-Unit access to the lock where the key is presented.
- **Erase Lock Memory Key**—Select this option to make a key that removes all programming stored in the lock memory.
- **LED Diagnostic Key**—Select this option to make a key that performs diagnostics on access points.
- **RF Pairing**—Select this option to make a key that connects a lock to the configured gateway. This key type only displays if online communication is enabled.
- **RF Unpairing**—Select this option to make a key that disconnects a lock from the paired gateway. This key type only displays if online communication is enabled.

Make special function keys

1. Go to *System Keys > Special Function Keys*.

Key Audit Key Disable/Enable Lock (E2) Change Key Erase Lock (E2) Memory Key LED Diagnostic Key RF Pairing Key RF Unpairing Key Back	Summary Key Info Key type: Special Function Keys Key: Audit Key Make Keys
--	--

2. Select the type of special function that you want to run.
3. Click **Make Keys**.
4. Select an encoder that is online.
5. Present a key to the encoder.
6. Click **Start**.
7. When notified that the key request is complete, click **Done**.

Monitor

Monitoring

This section includes the following subjects:

Learning about Monitoring	249
Monitor keys	250

Learning about Monitoring

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.



The Monitoring module includes additional features when online communication is enabled. See [Monitoring \(Remote Lock Management\)](#).

Monitor keys

The **Monitoring** module is where you can see the status for all 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 online communication is enabled, click the **Keys** tab.)

Online		Keys						
Key type		Credential class		Credential		Search by Operator name or Key Holder name		
All		All		All				
Date/Time	Operator	Operation	Details	Valid from	Valid to	Key Holder	Key Status	
05/29/2019 02:31 PM DST	User, Admin01 (Admin01)	Make Key	Primary Program Key	05/29/2019 02:31 PM DST	12/31/9999 06:59 PM	Unknown	Active	
05/29/2019 11:49 AM DST	User, Admin01 (Admin01)	Make Key	Primary Program Key	05/29/2019 11:49 AM DST	12/31/9999 06:59 PM	Unknown	Active	
05/29/2019 11:49 AM DST	User, Admin01 (Admin01)	Make Key	Primary Program Key	05/29/2019 11:49 AM DST	12/31/9999 06:59 PM	Unknown	Active	
05/28/2019 05:54 PM DST	User, Admin01 (Admin01)	Make Key	New Guest Key: 101	05/28/2019 05:54 PM DST	05/29/2019 11:00 AM DST	1, Guest	Active	

The following information is reported for each key:

- **Date/Time**—Date and time the key was encoded. You can filter the list based on date and time. A maximum of 60 transactions display.
- **Operator**—The full name of the Operator who was logged in when the key was encoded. You can search for keys that were used by a specific Operator.
- **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.
- **Aurora Status**—When Aurora is enabled, the status of the key in the Aurora system (Synchronized/Failed/Pending/Not applicable) and the date/time the status was first attained. You can filter the list of keys based on the Aurora status.

Customize the Display

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

Reports

Reports

This section includes the following subjects:

Access Point Audit Report	252
System Activity Report	253
Staff Access Report	255
Roles and Rights Report	256
Property Configuration Report	257
Operator Report	258
Key Expiration Report	259
Key/User Assignment Report	260
Elevator Configuration Report	261
Credential/Access Point Assignment Report	262

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.



Transferring lock audit data from the M-Unit to a workstation requires the Ambiance Client. Download and install the client from the main toolbar in the [Programming & Auditing](#) or [Device Management](#) module.

Generate report

1. Go to [Reports > Access Point Audit Report](#).
2. Select the access point for which you want to transfer data to 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

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 online communication 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 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
- Additional Access/Common Areas

View report details (system)

- Date range
- Number of transactions

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

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

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

Property Configuration Report

Generate this report to view the access point configuration for your site.

Generate report

1. Go to [Reports > Property Configuration Report](#).
2. Select a building.
3. Click [Next to Floors](#).
4. Select the floors to include in the report.
5. Click [Next to Access Point Types](#).
Because all access point types are selected by default, deselect any type that you want to exclude from the report.
6. Click [Generate](#).

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Total access points
- Report generated by
- Report generated on
- Buildings
- Floors
- Sequence (Seq)
- Access Point
- Access Point Type
- Lock/Device Model
- Building Name
- Floor Name

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](#).
Because all roles are selected by default, deselect any role that you want to exclude from the report.
4. Click [Generate](#).

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Operator status
- Operator roles
- Total operators
- Site
- Report generated by
- Report generated on
- Operator Name
- User Name
- Role
- Assign Date
- Status
 - Active
 - Deactivated
 - Blocked

Key Expiration Report

Generate this report to identify keys that are approaching expiration. The lists of credential classes/credentials that you can select to include in the report include both default and custom classes/credentials. However, the list reflects only those classes/credentials for which keys have been made. If the class or credential has not yet been assigned and encoded on a key, it does not display in the list.

Generate report

1. Go to [Reports > Key Expiration Report](#).
2. Because all classes are selected by default, deselect any class that you want to exclude from the report.
3. Click [Next to Credentials](#).
4. Because all credentials are selected by default, deselect any credential that you want to exclude from the report.
5. Click [Next to Date Range](#).
6. Specify the time span to include in the report.
7. Click [Generate](#).

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

The report shows the following details for all current and expired keys for the selected options.

- Date Range
- Total keys assigned
- Site
- Report generated by
- Report generated on
- Credentials
- Credential Class
- Credential (key ID)
- Additional Access/Common Areas
- Creation Date
- Expiration Date
- Key Holder
- Status—For physical keys: Pre-registered/Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.

Key/User Assignment Report

Generate this report to identify the keys assigned to staff. The report includes a list of all access points encoded on each assigned key.

Generate report

1. Go to [Reports > Key/User Assignment Report](#).
2. Select whether to include active keys, inactive keys, or both in the report. (All keys with a status other than "Active" are considered inactive.)
3. Select whether to index the report by staff member name or key credential.
4. Click [Next to Credential Classes](#).
5. Because all classes are selected by default, deselect any class that you want to exclude from the report.
6. Click [Generate](#).

View report details

- Displayed by
- Total keys assigned
- Site
- Report generated by
- Report generated on
- Key Holder
- Credential Class
- Credential
- Additional Access/Common Areas
- Status
- Key Request Date
- Creation Date
- Expiration Date

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

Credential/Access Point Assignment Report

Generate this report to display credential/access point assignments. The lists of credential classes/credentials that you can select to include in the report include both default and custom classes/credentials. However, the list reflects only those classes/credentials for which keys have been made. If the class or credential has not yet been assigned and encoded on a key, it does not display in the list.

Generate report

1. Go to [Reports > Credential/Access Point Assignment Report](#).
2. Select one of the following index options:
 - [Access Point](#)
 - [Credential](#)
3. Click [Next to Credential Classes](#).
Because all classes are selected by default, deselect any class that you want to exclude from the report.
4. Click [Generate](#).

View report details (access point)



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Displayed by
 - Access Point
- Total keys
- Site
- Report generated by
- Report generated on
- Credential Class(es)
- Access Point
- Credential class
- Credential

View report details (credential)

- Displayed by
 - Credential
- Total keys
- Site
- Report generated by
- Report generated on
- Credential Class(es)
- Credential Class
- Credential
- Access Point

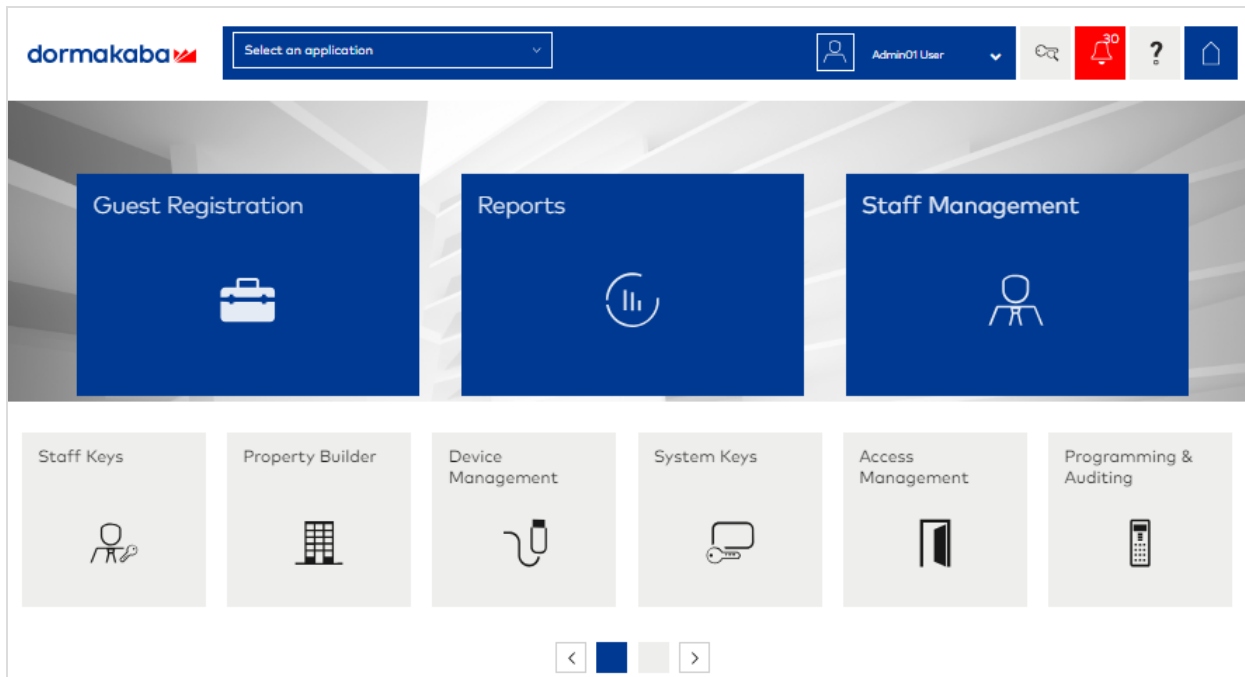
Toolbar Basics

This section includes the following subjects:

Navigate Ambiance	264
Set operator preferences	266
Install / update Ambiance Client	268
Select default encoder	269
Read key/erase key/access tracking report	270
View notifications	274
Physical keys	276
Digital keys	278

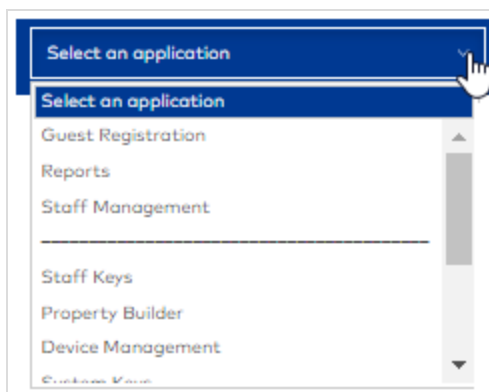
Navigate Ambiance

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 Home page or log out

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

Set operator preferences

To set operator preferences:



1. On the main toolbar, click *operator user name* > **Preferences**.
2. Refer to the section that applies to your environment:
 - [Single sign-on is disabled](#)
 - [Single sign-on is enabled](#)
3. Click **Save**. After saving the preferences, the screen refreshes in the selected language.



Operators are permitted a single active login. If an operator is logged in at one workstation then logs in at a different workstation, the initial connection is closed.

Single sign-on is disabled

GENERAL section

▼ GENERAL INFO	
Username	Admin01
Password status	Valid until 02/23/2025 01:45 PM.
Preferred language	English ▼
Email	

- Username is a read-only option that displays the operator user name.
- Password status is a read-only option that displays the expiration details for the Ambiance account password.
- Select the preferred language for the account holder. The default is to detect and display the UI in the browser language. For Ambiance to detect and display the UI in the browser language, the language setting in both [Systems Settings > General](#) and [Preferences](#) must both be [Automatic Language Detection](#).
- For Email, specify an email address to associate with the account for notifications. Ambiance sends automated emails regarding account status. The email address specified in the operator profile is linked with the email address in account Preferences.

PASSWORD section

▼ PASSWORD	
Current Password	
New Password	
Confirm Password	

Change the Ambiance account password. To view values, click . Default password requirements: minimum of eight characters that include at least one of the following: uppercase letters, lowercase letters, numerals and special characters. Password criteria and expiration are based on settings in [System Settings > Security](#).

SECURITY QUESTIONS section

▼ SECURITY QUESTIONS	
Security question 1	What is your favourite movie? ▼
Answer 1	
Security question 2	What is your favourite colour? ▼
Answer 2	
Security question 3	None ▼
Answer 3	

Select and provide responses to the challenge questions when required to submit a request to retrieve or reset the password.

Single sign-on is enabled

GENERAL section

▼ GENERAL INFO	
Preferred language	English ▼
Email	

- Select the preferred language for the account holder. The default is to detect and display the UI in the browser language. For Ambiance to detect and display the UI in the browser language, the language setting in both [Systems Settings > General](#) and [Preferences](#) must both be [Automatic Language Detection](#).
- For Email, specify an email address to associate with the account for notifications. Ambiance sends automated emails regarding account status. The email address specified in the operator profile is linked with the email address in account Preferences.

LOGIN section

▼ LOGIN	
User ID	User ID

The User ID is a read-only field that reflects the value specified at [Staff Management > Operator Info](#).

Install / update Ambiance Client

The Ambiance Client is required to encode and read keys, and to use the M-Unit to program and audit locks and devices. The Ambiance Client and Ambiance Server must be the same version to ensure proper key-encoding operations. Upon login, Ambiance detects the Client version and if it is older than the Server version, prompts you to download and install the current Client.

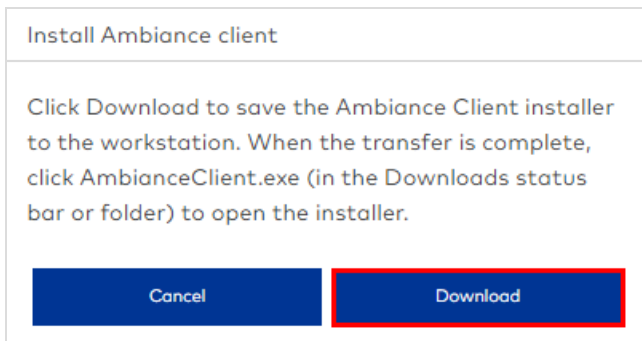


Perform the installation as a Local Administrator (not Network Administrator).

1. Go to [Device Management](#) or [Programming & Auditing](#).



2. Click (Install Ambiance Client) .



3. Click [Download](#). A total of three files are required `Ambiance_Client.exe`, `serverURL.config`, and `token.txt`. The download process can take up to one minute.
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). The [Setup Status](#) page displays while the Client is installed.
6. On the [Update Complete](#) page, click [Finish](#).



Ambiance installs a workstation-specific certificate to verify the browser and M-Unit to the Ambiance server. The certificate is valid for two years and renews automatically.

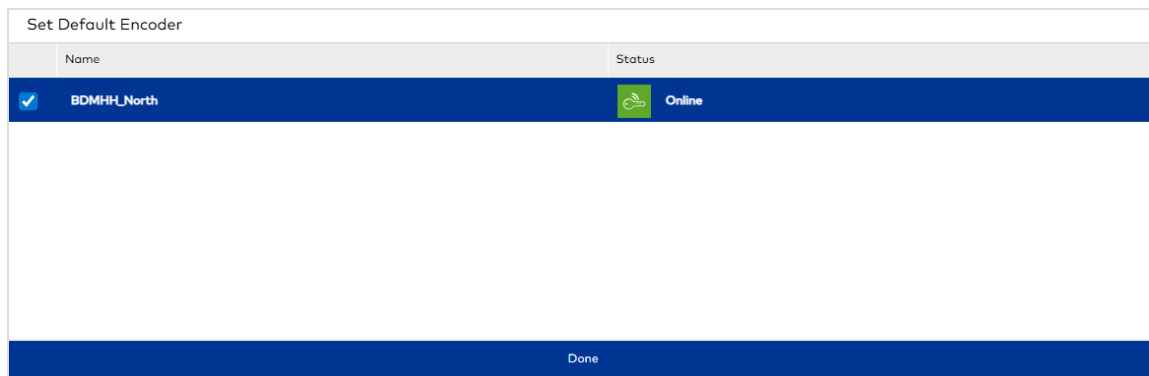
Select default encoder

You can set the default encoder from the main Ambiance toolbar in modules where keys are made. At key-making time, you can always select any encoder that is online and available to the workstation.

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



2. In the toolbar, click (Encoder status) .



3. Select the encoder to automatically populate when making keys.
4. Click [Done](#).

Read key/erase key/access tracking report

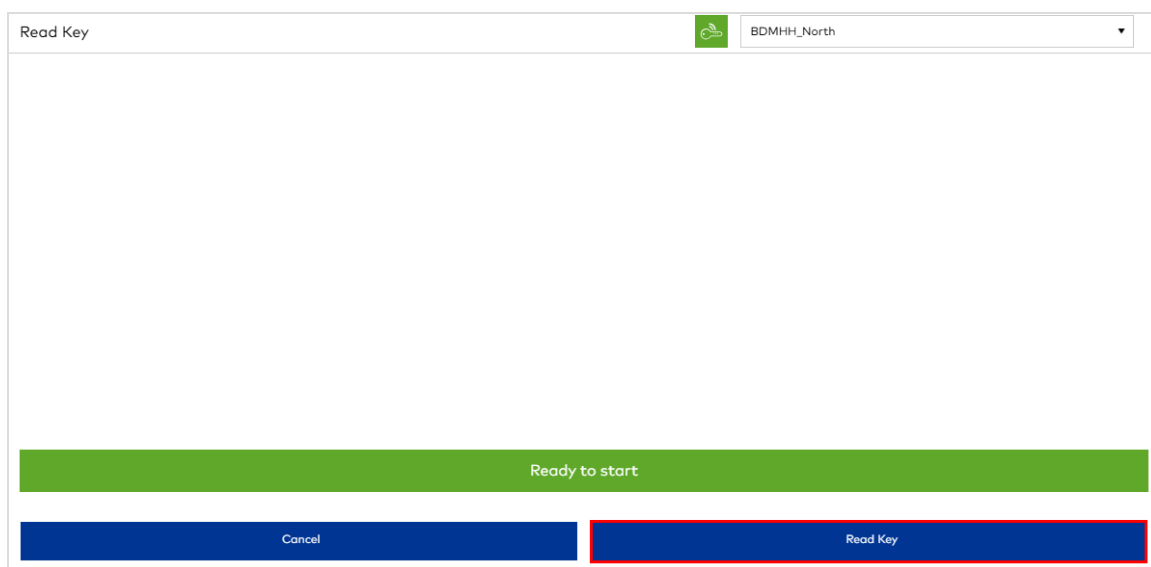
Learn the status of any key by using the Ambiance key reader accessible from the main toolbar. After successfully reading a key, you can erase all configuration data encoded on the key and generate an access report.

Read key

To read any key:



1. On the main toolbar, click (Read Keys) .



2. Select an encoder that is online and available to the workstation.
3. Present a key to the encoder.
4. Click [Read Key](#).

Read Key	
Keycard type	Guest
Encoded by	User, Admin01
Encoded on device	BDMHH_Nord
Key mode	Additional
Created on	07/14/2025 03:56 PM
Check-in	07/14/2025 03:53 PM
Check out	07/15/2025 11:00 AM
Key ID	2
Status	Active
Room access	401
Amenity access	Business Center, Fitness, Gardens, Guest laundry, Guest laundry - S, Guest lounge, Parking - North, Pool, Spa

* Deleted item(s)

Key read successfully

Cancel
View Guest Access Report
Read Key
Erase 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
- 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

This function is not supported when Enhanced Security Mode is enabled. However, high security keys can be re-encoded at the same site using the same Ambiance database.

You can erase any key (guest/staff/system) only directly after the key is read. Erasing a key removes all configuration data encoded on the key.

To erase a key:

1. After the key is successfully read, click [Erase Key](#).
2. Click [YES](#) to confirm.
3. When done, click [OK](#).

Keys that are erased show as "Returned" in reports and [Monitoring > Keys](#).

Read Key Access Report

After reading a key, you can generate a detailed list of the access points the key can access. This report is only available when access data is on the key, and the active operator is authorized to generate the report.



Access reports include a maximum of 72 or 408 events for 1k/4k keys respectively. MIFARE mini keys do not retain access tracking data. For VIP guest registrations, the limitations are 36 and 372.

To generate a report:

1. After the key is successfully read, click [View Guest Access Report](#).
2. After the key is successfully read, click [View Staff Access Report](#).

Access details

- Date Range—The dates and times during which the events included in the report occurred.
- Access Events—The number of records in the report.
- Key Holder—The name of the guest or staff member.
- Access—The access points authorized for the key holder.
- Check In—The date and time access is valid.
- Check Out—The data and time access is invalid.
- Key status—The current state of the key. For physical keys: Pre-registered/Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- Seq—The order in which an event occurred.
- Event Date—The date and time the event occurred.
- Access Point—The access point to which the key was presented.
- Access Granted—Indicates whether access was granted when the key was presented.
- Time Set—Indicates whether the lock clock is set properly. If No, then the reported Event Date may be wrong. The most common reason for the lock clock to not be set is replacing a depleted battery. For Online systems, a lock clock syncs with the online system when batteries are replaced. For offline systems, staff members can use an M-Unit to reset a lock clock.
- Dead Bolted—Indicates whether the deadbolt was engaged at the time of the event.
- Low Battery—Indicates whether the battery was low at the time of the event.
- Lock Prob?—Indicates a problem with the lock at the time of the event.
- Lock Latched—Indicates whether the lock was latched at the time of the event.
- New Key—Indicates whether the key is New. If the key is not New, it is an Additional Key.

Staff access details

- Date Range—The dates and times during which the events included in the report occurred.
- Access Events—The number of records in the report.
- Credential —The name of the credential and key mode (New or Additional).
- Shift schedule—The name of any shift schedule assigned to the key.
- Expiration—The date and time after which access on the key is invalid.

- Key status—The current state of the key. For physical keys: Pre-registered/Active/Expired/Obsolete/Returned. For mobile keys: Delivering/Delivered/Failed/Canceling/Canceled/Expired/Obsolete.
- Seq—The order in which an event occurred.
- Event Date—The date and time the event occurred.
- Access Point—The access point to which the key was presented.
- Access Granted—Indicates whether access was granted when the key was presented.
- Time Set—Indicates whether the lock clock is set properly. If No, then the reported Event Date may be wrong. The most common reason for the lock clock to not be set is replacing a depleted battery. For Online systems, a lock clock syncs with the online system when batteries are replaced. For offline systems, staff members can use an M-Unit to reset a lock clock.
- Dead Bolted—Indicates whether the deadbolt was engaged at the time of the event.
- Low Battery—Indicates whether the battery was low at the time of the event.
- Lock Prob?—Indicates a problem with the lock at the time of the event.
- Lock Latched—Indicates whether the lock was latched at the time of the event.
- First Key Use—Indicates whether the key has been used to access a space.

View notifications

Ambiance offers notifications to keep operators informed about system events.



When online communication is enabled, notifications keep staff members informed about operations and events related to online communication (gateways and paired access points). For example, a notification lets you know when a key is used or a door is ajar.



To view recent notifications:

- » Click **(Notifications)**  on the main toolbar. Recent notifications are listed showing the date, time and command result. To delete a recent notification, click **(Delete)** x.

To view all notifications:

- » Click **(Notifications)**  > **VIEW ALL NOTIFICATIONS** on the main toolbar. The list of notifications includes events selected in the notification groups to which the current Operator subscribes.

TODAY - 07/14/2025		
07/14/2025 10:15 AM	Some access points require reprogramming	x
07/14/2025 10:14 AM	Some access points require reprogramming	x
07/14/2025 10:07 AM	Some access points require reprogramming	x
07/14/2025 10:05 AM	Some access points require reprogramming	x
07/14/2025 10:04 AM	Some access points require reprogramming	x
07/14/2025 10:03 AM	Some access points require reprogramming	x
07/14/2025 10:03 AM	Some access points require reprogramming	x
07/14/2025 10:03 AM	Some access points require reprogramming	x
07/14/2025 10:02 AM	Some access points require reprogramming	x
07/14/2025 10:01 AM	Some access points require reprogramming	x
07/14/2025 10:01 AM	Some access points require reprogramming	x
07/14/2025 10:00 AM	Some access points require reprogramming	x
Clear All		View All Notifications

The following information is displayed for each notification:

- **Notification**—The notification text/online event.
- **Category**—The type of notification: General or Online.
- **Date/Time**—The date and time the event occurred.
- **Details**—More information about the event, such as the command sent, and if applicable, the names of paired access points.

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

- Delete notifications—Select one or more notifications, then click **(Delete)** .
- Clear notifications from the Recent notifications list—Select one or more notifications, then click **(Mark as Read)** .

- Filter notifications by notification, category, and date/time—Click [\(Filter\)](#) , select [From](#) and [To](#) dates, then click [Filter](#). To clear a column filter, click [\(Filter Applied\)](#) , then [Clear](#). To clear all filters, click [\(Reset Filters\)](#) .
- Show/hide notification event types—Click  and select the event categories to include in the list ([General](#) and [Online](#)).
- Refresh the data—Click [\(Refresh\)](#) .

General events

The basic notification feature includes only the following event:

- [Some access points require reprogramming](#)—Notifies when it is necessary to resynchronize Ambiance configuration data for the access points listed in the Details column.

Online events

- [Access point offline](#)—Notifies that there is no communication between the lock and the gateway.
- [Access point online](#)—Notifies that the lock is online and in communication with the gateway.
- [Access Point Paired](#)—Notifies that an access point was paired to a gateway.
- [Door ajar clear \(door secure\)](#)—Door previously ajar has now been closed and is secure.
- [Door ajar generic](#)—Notifies that a door is in an open state.
- [Door ajar 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](#)—Notifies a door ajar (long) has been left open by a staff member for a longer time interval, indicating an unusual state, a possible intrusion in progress.
- [Door ajar staff short](#)—The door ajar (short) notifies a door has been left open by a staff member for a short time interval.
- [Door latched](#)—Notifies that a door is closed with the lock engaged.
- [Door open](#)—The lock's anti-pick mechanism is out. This is the default state of the door.
- [Door unlatched](#)—Notifies that the lock motor has been disengaged and the door can be opened without a key.
- [Generic egress](#)—Egress is an open door event.
- [Guest key used](#)—Date and time that a key was used at the access point.
- [Guest key used \(first entry\)](#)—Notifies a guest has accessed the lock for the first time.
- [Gateway offline](#)—Gateway is currently not communicating with the Ambiance Server.
- [Gateway online](#)—Displays all gateways that are online and visible in the Monitoring module.
- [Low battery](#)—The battery state is low and requires replacement.
- [Low battery clear \(battery normal\)](#)—The low battery notification has been cleared; the battery was replaced or the problem resolved.
- [Mechanical key override](#)—Notifies a lock override, accessing a lock with a mechanical key.
- [Operation failed](#)—The specified operation was not successful. When available, the reason is indicated.
- [Privacy disabled/deadbolt retracted](#)—Notifies the status of the deadbolt as disengaged.
- [Privacy enabled/deadbolt engaged](#)—Notifies that the deadbolt or privacy switch is engaged.
- [Access point programming required](#)—Lock may require resequencing or synchronization with Ambiance configuration data.
- [Staff key used](#)—Notifies that a staff key has accessed the lock.
- [Standing intruder](#)—Alert: Possible standing intruder. Multiple keys presented at a single access point.
- [System key Used](#)—Notifies that a System key was presented to the lock.
- [Wandering intruder](#)—Alert: Possible wandering intruder. Key presented at multiple access points.

Physical keys

A key is any device on which a credential is encoded for the purpose of controlling access and/or performing system or programmatic operations. Examples include key cards and key fobs.

Selecting a Key Mode (New/Additional)

All 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 guest 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.

Unused keys

For security reasons, dormakaba imposes a maximum on the number of unused keys that can be issued for a given credential. For example, when more than 15 keys are issued but never presented to Room 100, the access point becomes "out of sequence" and denies access to all of the keys.

To restore key access, reprogram the access point using the Maintenance Unit or resequence the access point using the Resequence Key. After the access point is resequenced, the access point accepts the most recently issued key.

The maximum number of unused keys before resequencing is required depends on the key type:

- Guest Keys
 - Room, Suite , Foyer Door, Connector keys=15
 - Limited Use=3
- Staff Keys
 - All classes=unlimited
- System Keys
 - Failsafe, Latch, Unlatch, Toggle Latch/Unlatch=15
 - ELO=3
 - Inhibit=0
 - PPK/SPK=0

Key status

The following statuses apply to guest keys, staff keys, and specific system keys (ELO, Inhibit, Latch, Unlatch, Toggle Latch/Unlatch).

Physical keys only:

- **Pre-registered**—Keys that have been made but are not yet valid (due to pre-registrations).
- **Active**—Keys that, according to Ambiance, are valid and available for use. This includes keys for which an Unblock key was made and keys that were unblocked remotely. Failsafe Keys always have the status Active.
- **Returned**—Keys that have been erased.

Digital keys only :

- **Delivering - Mobile registered**—Keys that are in the process of being delivered. The dormakaba server detects the mobile device is registered with the mobile application/dormakaba BlueSky.
- **Delivering - Mobile not registered**—Keys that are in the process of being delivered. cannot detect the mobile device.
- **Delivered**—Keys that are valid and available for use, and keys that are invalid because the expiration date arrived.
- **Canceling**—Keys that are in the process of being deleted from the mobile device.
- **Canceled**—Keys that have been deleted from the mobile device.
- **Failed**—Keys that were never delivered to the mobile device.

All keys:

- **Expired**—Keys that are invalid because the expiration date arrived.
- **Obsolete**—Keys may be obsolete when: a) a New key with the same credential was made, b) access was removed prior to expiration. Keys that are obsolete may include one of the following sub-statuses:
 - **Obsolete (blocked)**—Keys for which a Block key was made and keys for which a Block key was sent remotely.
 - **Obsolete (canceled)**—Keys for which a Cancel key was made and keys for which a Cancel key was sent remotely.



Obsolete keys continue to allow access to common areas until key expiration.

Digital keys

Digital keys offer guests the convenience of using their phone to access their room and hotel amenities. dormakaba supports the following digital key types:

- mobile keys
- Apple Wallet keys
- Apple Watch keys
- Google Wallet keys

Digital keys work in combination with hotel-specific mobile apps or the dormakaba BlueSky app for mobile keys to provide guests a fast, secure, and convenient way to access their rooms and amenities.

For wallet keys, guests can tap their device to unlock doors—even in Express Mode, which works without waking or unlocking the phone. If the phone battery runs low, the key continues to function for up to five hours. Guests can also securely share their digital room key with trusted companions.

Typically, additional cost is associated with using mobile keys. Consult LEGIC or your mobile network provider for details.

Requirements

- Mobile keys must be enabled in [System Settings > Advanced Settings](#). Required for all digital keys.
- Mobile wallet settings are required to issue Apple Wallet, Apple Watch, and Google Wallet keys.
- The guest / staff member profile must include a valid mobile or custom number.
- Guests / staff must download, install and register their mobile number with the mobile application.

Enable digital keys

To enable and configure digital keys:

1. Go to [System Settings > Advanced](#).
2. Set the [Enable mobile keys](#) switch to **YES**.
3. For [Mobile default country](#), select the default country for mobile numbers. The corresponding country code is retrieved for the mobile number.
4. For LEGIC, BLE, and mobile wallet settings, a dormakaba Customer Service technician provides valid values.
5. Select whether to use mobile phone numbers or custom numbers. A custom number is a unique numeric identifier that is used as an alternative to a mobile number. Key generation and cancellation work the same for mobile and custom numbers. LEGIC can recognize a key holder based on mobile or custom number.



Custom numbers are only supported when mobile keys are made/issued from the PMS.

6. Select whether to send a text message to recipients of mobile keys to notify them that their device is not registered with the mobile application. If you select **YES**, you must also specify the message text to send, an SMS Gateway account key (see Swift SMS Gateway), and at least one link where the mobile application can be downloaded.

Mobile key download file

From the Buildings context menu in Property Builder, you can download a file that lists all access points that were configured with the option [Include in mobile keys download file](#) selected. The option serves to identify the locks that are equipped to accept mobile key credentials.

The following figure shows the option to select in Property Builder.

Create Access Point: Guest Room

Access Point Advanced Format

Floors *

FLOOR3 × FLOOR4 × FLOOR5 × FLOOR6 × FLOOR7 × FLOOR8 ×
FLOOR9 ×

Lock profile
Saflok Quantum ▼

☒ Include in mobile keys download file

Format Numbering Pattern
Number Continuous ▼

From To Description
— 1 + — 10 + Description

Preview 10 Access Point(s)
301, 302, 303...

Back to Type Selection Cancel Save

The following figure shows where to get the download file in Property Builder.

Buildings

▼ B

BDMHH-North ...

BDMHH-South

Summary

Building

BDMHH-North

Edit Building

Delete Building

Download mobile enabled access points file

Import access point list

To download the file:

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, Ambiance detects the mobile provider connection and checks to make sure the mobile application has been downloaded onto the mobile device. If no connection is detected, the failure is reported in [Monitoring](#) >

[Report](#) and [Reports > System Activity Report \(Keys\)](#). If a connection is detected but the mobile application is not on the device, a text message can be sent to the mobile device prompting the user to download the app.



The option [Send download mobile application SMS notification](#) must be enabled in [System Settings > Advanced Settings > Enable mobile keys](#).

When a connection is detected and the the mobile application is installed on the mobile device, 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 the mobile application.
- [Delivering - Mobile not registered](#)—Keys that are in the process of being delivered. Ambiance cannot detect the mobile device.



When connection to a mobile phone is not detected, Ambiance retries every 5 minutes for 24 hours.

Unused keys

For security reasons, dormakaba imposes a maximum on the number of unused keys that can be issued for a given credential. For example, when more than 15 keys are issued but never presented to Room 100, the access point becomes "out of sequence" and denies access to all of the keys.

To restore key access, reprogram the access point using the Maintenance Unit or resequence the access point using the Resequencing Key. After the access point is resequenced, the access point accepts the most recently issued key.

The maximum number of unused keys before resequencing is required depends on the key type:

- Guest Keys
 - Room, Suite , Foyer Door, Connector keys=15
 - Limited Use=3
- Staff Keys
 - All classes=unlimited
- System Keys
 - Failsafe, Latch, Unlatch, Toggle Latch/Unlatch=15
 - ELO=3
 - Inhibit=0
 - PPK/SPK=0

Key status

The following statuses apply to guest keys, staff keys, and specific system keys (ELO, Inhibit, Latch, Unlatch, Toggle Latch/Unlatch).

Physical keys only:

- [Pre-registered](#)—Keys that have been made but are not yet valid (due to pre-registrations).
- [Active](#)—Keys that, according to Ambiance, are valid and available for use. This includes keys for which an Unblock key was made and keys that were unblocked remotely. Failsafe Keys always have the status Active.
- [Returned](#)—Keys that have been erased.

Digital keys only :

- **Delivering - Mobile registered**—Keys that are in the process of being delivered. The dormakaba server detects the mobile device is registered with the mobile application/dormakaba BlueSky.
- **Delivering - Mobile not registered**—Keys that are in the process of being delivered. cannot detect the mobile device.
- **Delivered**—Keys that are valid and available for use, and keys that are invalid because the expiration date arrived.
- **Canceling**—Keys that are in the process of being deleted from the mobile device.
- **Canceled**—Keys that have been deleted from the mobile device.
- **Failed**—Keys that were never delivered to the mobile device.

All keys:

- **Expired**—Keys that are invalid because the expiration date arrived.
- **Obsolete**—Keys may be obsolete when: a) a New key with the same credential was made, b) access was removed prior to expiration. Keys that are obsolete may include one of the following sub-statuses:
 - **Obsolete (blocked)**—Keys for which a Block key was made and keys for which a Block key was sent remotely.
 - **Obsolete (canceled)**—Keys for which a Cancel key was made and keys for which a Cancel key was sent remotely.



Obsolete keys continue to allow access to common areas until key expiration.

dormakaba BlueSky installation

The BlueSky app is free and consumes 34 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.
- **Terms of use and Privacy Policy**—Guests must accept the terms of use and private policy.
- **Share usage patterns**—The selected response does not affect the operation of mobile keys.



If a BlueSky registrant deletes the app, a mobile key must be sent again after the registrant re-installs the app.

Remote Lock Mgmt



This chapter is for the licensed feature online communication.

This section includes the following subjects:

Introduction	283
Enable and configure online communication	284
Gateways & Paired Access Points	291
Manage online device configuration	292
Registered gateways and paired access points	294
Program Devices	299
Program devices	300
Notification Management	301
Learning about Notification Management	302
Add notification groups	304
Monitoring (RLM)	306
Learning about Monitoring	307
View metrics	308
Monitor online operations	309
Monitor online events	311
Monitor access point status	314
Reports (RLM)	315
Online Access Points Status Report	316
Online Gateway Status Report	317
Online Paired Access Point Report	318

Introduction

Deployment of online communication involves configuring gateways to work with the Ambiance Server. Gateways are the network devices which are paired to access points for online communication (to perform remote operations and receive access point events). When a gateway is listed in [Device Management](#) and the connectivity status is Online, access points can be paired. Multiple gateways can be connected to Ambiance, but an access point can be paired with only one gateway.

After configuration is complete, remote commands can be sent to gateways and paired access points. All command requests and results occur in real-time.

The [Device Management](#), [Monitoring](#), [Notification Management](#) and [Reports](#) modules all provide ways to stay informed about the devices and communication that support online communication.

Enable and configure online communication

To enable online communication:

» Go to *System Settings > Advanced > Enable online communication* and set the soft-switch to YES.

Enable online communication	☒ YES
-----------------------------	---

After enabling online communication, the [Online Communication](#) category displays.



For Control 4 devices, the only relevant option is to ensure [Using dormakaba Gateway I devices](#) is selected.

1. Go to *System Settings > Online Communication*
2. Configure settings in each of the following sections:
 - Online Operations
 - Communication Settings
 - Notifications
 - Rx-Link (if using)
 - INNCOM Communication (if using)
3. Click (Save) .

Online operations

▼ Online Operations	
Enable remote guest check-out in rooms	☒ YES
Grace period to block guest keys in rooms upon early check-out or room move (minutes)	Disabled ▼
Enable remote guest check-out in common areas and elevators	☐ NO

- 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 guest registration 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.
- [Enable remote guest check-out in common areas and elevators](#)— Set to YES to enable remote check-out of guest common areas and elevators in Guest Registration. Default: NO. When disabled, access (to common areas/elevators) remains valid until the key expiration date/time.



Enabling remote guest check-out for guest common areas and elevators may significantly impact the network and online performance.

Communication settings

- **Gateway update status sent every**—Specify the frequency to update gateway status. Valid values: 1-255. Default: 1.
- **Access point wake-up interval**—Specify the frequency at which access points verify if the paired gateway has received remote operation requests. Default: 2.
- Select whether to use a server name or static IP address and specify details. The value that you specify overwrites any value specified for IP Server/Server Name when configuring a gateway in [Device Management](#).
- Select the type of devices used in the deployment:
 - **Using: Gateway I; Legacy MFC; Messenger 3rd party**—Select this option is using any of the following:
 - Gateway I devices
 - Legacy MFC elevator controller
 - Messenger 3rd Party (INNCOM, Interel, Telkonet, Control4)
 - **Using: Gateway II; Rx-Link**—Select this option if using any of the following:
 - Gateway II devices
 - Rx-Link



The option Using Gateway II; Rx-Link requires using the Zigbee Generation II antenna with minimum firmware version (see the Device Requirements section in the Release Notes) and reprogramming all online access points.

RAC5-MFC/XT are supported in both modes.



Gateway II and RAC5 MFC/XT devices must be configured in [Device Management](#).

- Configure gateways to use dynamic IP addresses (DHCP) or static IP addresses. If using dynamic IP addresses, gateways resolve their own IP address. A DHCP server is required for this option. If using static IP addresses, each gateway must be configured with a unique IP address.

- Select whether a gateway restarts after the [Set communication settings](#) command has been sent to the gateway in [Device Management > Gateways & Paired Access Points](#).
- Select whether to allow gateways to automatically generate the most appropriate ZigBee communication channels or specify a unique extended PAN (Personal Area Network) ID and select the channels for gateway and access point communication. The extended PAN ID must be eight alphanumeric characters. If the extended PAN ID is set to 0 (zero), the ZigBee network automatically generates an ID. Channels 15, 20, and 25 are recommended for minimal WiFi interference.



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

Notifications

Set alerts for potential intruders and access point events.

Notifications

Standing intruder

Number of failed key attempts to trigger notification

- 5 +

Failed key attempts time lapse (minutes)

- 5 +

Wandering intruder

Number of failed key attempts to trigger notification

- 5 +

Failed key attempts time lapse (minutes)

- 5 +

Access point notifications

Door Egress

YES

Door Ajar - Generic

YES

Door Secured

YES

Door Ajar - Guest short (minutes)

- 3 +

Door Ajar - Guest long (minutes)

- 5 +

Door Ajar - Staff short (minutes)

- 3 +

Door Ajar - Staff long (minutes)

- 5 +

Potential intruders

This section describes the alerts that you can set for potential intruders. The behavior that alerts the system about a potential intruder is the number of failed key attempts within a specified amount of time. The settings to trigger notification can be set for standing and wandering intruders. A standing intruder is when the failed key attempts occur at the same access point; for example, someone acquired several keys and presents each to the same access point. A potential wandering intruder is when the failed key attempts occur at different access points; for example, someone found a key in the parking lot and walks the hallway presenting the key to each access point.

- Standing intruder
 - [Number of failed key attempts to trigger notification](#)—Specify how many failed key attempts at the same access point (within the specified time lapse) trigger an intruder alert notification. Default: 5. Valid values: 3-10.
 - [Failed key attempts time lapse](#)—Specify the number of minutes within which the number of failed key attempts (at the same access point) must occur before a notification is triggered. Default: 5. Valid values: 1-10.

- Wandering intruder
 - [Number of failed key attempts to trigger notification](#)—Specify how many failed key attempts at different access points (within the specified time lapse) trigger an intruder alert notification. Default: 5. Valid values: 3-10.
 - [Failed key attempts time lapse](#)—Specify the number of minutes within which the number of failed key attempts (at different access points) must occur before a notification is triggered. Default: 5. Valid values: 1-10.

Access point notifications

Select the access point events for which to receive notification:

- [Access Point Event Notification](#)—Lists access point door parameters which must be set to [YES](#) to enable access point status notifications.
- [Egress](#)—Select [YES](#) to send a notification about an open door event.
- [Door Secured](#)—Select [YES](#) to send a notification that a door is locked securely.
- [Door Ajar - Generic](#)—Select [YES](#) to send notifications for all Door Ajar events. If NO is selected, enable or disable each Door Ajar event.
- [Door Ajar - 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 (one minute), for example the time it would take to vacate a room. Specify the number of minutes after which the notification is sent.
- [Door Ajar - 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 (two minutes), 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 (one minute), for example the time it would take to vacate a room. Specify the number of minutes after which the notification is sent.
- [Door Ajar - Staff 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 (two minutes), indicating an usual state or potential intrusion. Specify the number of minutes after which the notification is sent.



Default time intervals for access point event notifications should be based on practical best practices with security considerations.

Rx-Link



For complete Rx-Link documentation, refer to *AmbianceRx-Link Deployment and Support Manual* and *Ambiance Rx-Link Partner Integration Specifications*.

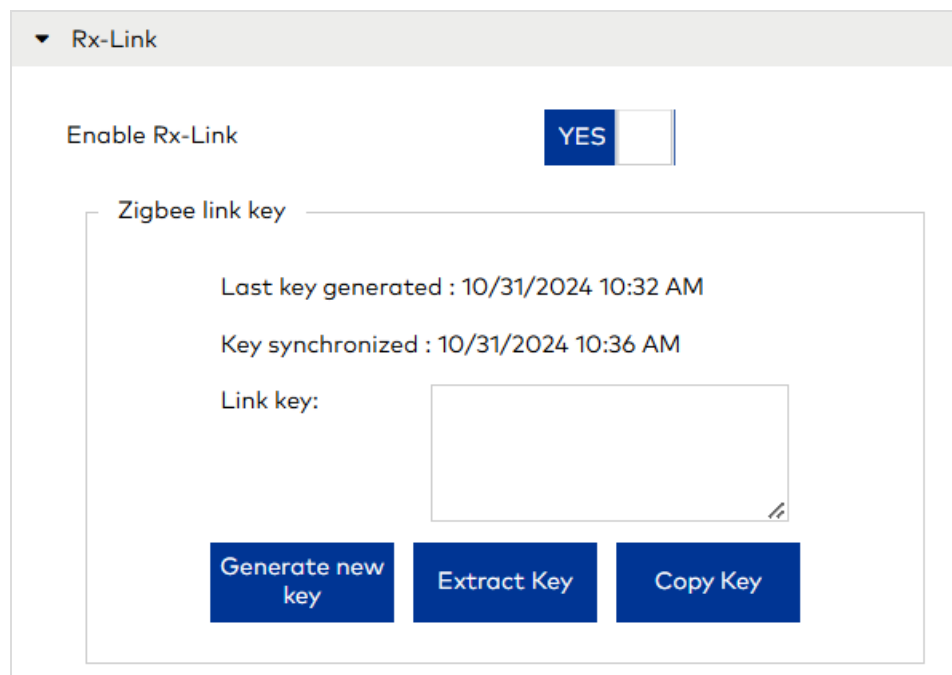
The Rx-Link section displays when the communication setting [Using: Gateway II; RAC5-MFC/XT; Rx-Link](#) is selected.

Select whether to enable Rx-Link. When enabled, Rx-Link Settings Management in Role Management System Rights is exposed with the default settings that authorize the Administrator and Site Configurator roles.



When you modify this setting (enable or disable) or generate a new third-party Zigbee link key, all access points must be reprogrammed.

Zigbee link key



The screenshot shows a window titled "Rx-Link" with a dropdown arrow. Below the title is a toggle switch for "Enable Rx-Link" which is currently set to "YES". Underneath, there is a section titled "Zigbee link key" containing the following information:

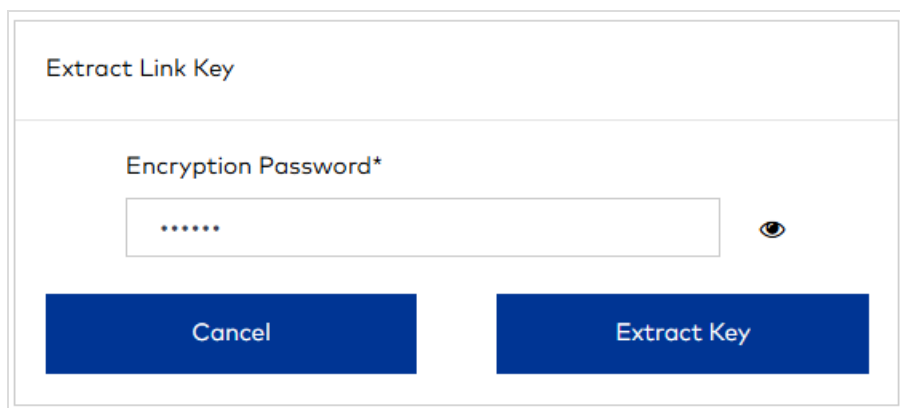
- Last key generated : 10/31/2024 10:32 AM
- Key synchronized : 10/31/2024 10:36 AM
- Link key: [A large empty text box with a small icon in the bottom right corner.]

At the bottom of the "Zigbee link key" section are three buttons: "Generate new key", "Extract Key", and "Copy Key".

If you enable Rx-Link, Zigbee link key information is displayed (the date/time of the most recent key and when the key was synchronized). Click [Generate new key](#) to generate the initial or a new link key.

For third parties that require the link key be shared in a readable format, extract the link key:

1. Click [Extract Key](#).



The screenshot shows a dialog box titled "Extract Link Key". It contains a label "Encryption Password*" above a text input field. The input field contains six dots, indicating a password. To the right of the input field is an eye icon. At the bottom of the dialog are two buttons: "Cancel" and "Extract Key".

2. Specify a password for the key. Minimum chars: 6.
3. Click [Extract Key](#). The link key displays in a readable format.
4. Click [Copy Key](#) to copy the Link key value onto the clipboard.

Rx-Link

Enable Rx-Link

YES

Zigbee link key

Last key generated : 08/07/2024 03:20 PM

Key synchronized : 10/23/2024 09:54 AM

Link key:

dXNIckdlbmVyYXRIZFBhc3NIZEtIeVdpdGhBZGRpdGlvbmFsU2VjdXJpdHk=

Generate new key

Extract Key

Copy Key

Rx-Link authentication

RX-Link authentication

User*

Audience key*

.....

User key*

.....

Secret key*

.....

Third-Party URL*

Third-Party token URL

Third-Party refresh token URL

Configure authentication options:

- **User**— The unique ID provided by the third party for authentication to acquire a token. Valid length: 1-2,048 characters. Not required when using the WebSocket protocol.
- **User key**—The password provided by the third party that pairs with the User. Valid length: 1-2,048 characters. Not required when using the WebSocket protocol.
- **Audience key**—An API key (paired with the Secret key) that is required by a third-party to acquire an authentication token from the dormakaba server. The token eliminates the need to always submit the User/User key settings with each request. Valid value: 9b55561a54b94e2db01e15f337e902bb
- **Secret key**—A unique API key (paired with the Audience key) that is required by a third party to acquire an authentication token from the dormakaba server. The token eliminates the need to always submit the User/User key settings with each request. Valid length: 1-2,048 characters. Must be 64 bytes in length.
- **Third-Party URL**—Uri of the third-party bridging service to initiate Web requests made by dormakaba to the IoT controller. Represents the endpoint.
- **Third-Party token URL**—Third-party Uri to request a token.
Example: https://vriot.local-mqtt.video54.local/v1/oauth/login.
- **Third-Party refresh token URL**—The third-party Uri to refresh the token. Example: https://vriot.local-mqtt.video54.local/v1/oauth/refresh.

INNCOM communication

For integrations with INNCOM, select the enable switch to **YES**.

▼ Enable Inncom communication **YES**

Enable secured communication **YES**

Inncom username* Inncom password*

Certificate file name*

Certificate password* Certificate server name*

If the option to secure communication is enabled, configure the following options:

- **INNCOM username/password**—Specify INNCOM account credentials so that Ambiance can connect to the INNCOM server. Value length per setting: 5-25 characters .
- **Certificate file name/password**—Specify the full path to the certificate file name (for example, c:\Program Files\dormakaba\InncomCertificate\Kaba_VHE_Client_cert.pfx) and password on the INNCOM server used to secure communication between Ambiance and INNCOM. Value length: Unlimited (file name), 5-25 characters (password).
- **Certificate server name**—Specify the IP address of the INNCOM server. Value length: 5-25 characters. Default: inncom.com.

Gateways

Gateways & Paired Access Points

This section includes the following subjects:

Manage online device configuration	292
Registered gateways and paired access points	294

Manage online device configuration

You can add, configure and delete devices in the [Device Management](#) module. All device types can be configured in Device Management. RAC5 MFC/XT devices can also be programmed using the M-Unit (see [Programming /Auditing > Programming](#)).

Add online devices

1. Go to [Device Management](#). > [Online Device Configuration](#).

2. Click [New Device](#).
3. Specify a unique name that does not exceed 60 characters. This name displays in the list of devices.
4. Select the device type: Gateway II, RAC5-MFC or RAC5-XT.
5. Select the MAC address of the device that you want to configure. The MAC address of the device is automatically detected when the device is connected to the workstation.
6. Select whether the gateway obtains an IP address automatically. If **NO**, specify a valid static IP address, port number, subnet mask and default network gateway IP address. (The network gateway is not the dormakaba gateway.)
7. Select whether the gateway will contact the Ambiance Server using the IP address or server name. If using the server name, you must also specify the IP address or domain name of the local DNS Server.



The Server IP or Server Name value that you specify must refer to the same server specified in [System Settings > Online Communication > Communication Settings](#).

8. Specify the port number for the gateway to communicate with the Ambiance Server.
9. Take one of the following actions:
 - When the device is attached to the workstation and the MAC address is populated, click [Configure Device](#). The device configuration is saved to the Ambiance database. Wait 20 seconds or Power OFF/ON the gateway device. When the gateway is commissioned, disconnect the device from the USB cable and connect it to the Ethernet (POE or external power supply).
 - When the intent is to save device configuration settings only, click [Save Device Configuration](#).

Edit device configuration

1. Select a device.
2. Modify options.
3. Click [Save Device Configuration](#).

Delete a device

1. Select a device.
2. Click [Delete Device](#).
3. Click [YES](#) to confirm.

Registered gateways and paired access points

To work with gateways (and paired access points) that are connected to the Ambiance Server:

1. Go to *Device Management > Registered Gateways & Paired Access Points*.

Gateway	Status	Type	MAC Address	IP Address	Antenna
GatewayII		dormakaba Gateway II	000E2A7002AA	192.168.0.178	Pairing OFF
RACS-MFC		dormakaba RACS	000E2A01182E	192.168.0.156	Pairing OFF
RACS-XT		dormakaba RACS XT	000E2A010C81	192.168.0.239	Pairing OFF

Registered gateways

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

Use the Gateways toolbar to issued commands, search gateways (by name, IP and MAC address) and take the following actions:

- To filter based on connectivity status, click **(Filter)** and select the status types (Online/Offline) to list.
- To show/hide columns, click and select the information that you want to display. The following columns can be displayed:
 - **All**—Select this option to show all columns.
 - **Type**—The type of gateway.
 - **MAC Address**—Unique MAC address for each device.
 - **IP Address**—Unique Ethernet address for each device. The IP address is dynamic if a DHCP is assigned; otherwise, the IP address is static.
 - **Antenna**—Gateway antenna states (Disabled/Pairing On/Pairing Off).
 - **Last offline**—The date and time the gateway was most recently offline.
 - **Last Communication**—The date and time of the most recent and successful communication with the gateway.
 - **FW Vers. Gateway**—The current firmware version of the gateway device that runs at all times except during a firmware upgrade.
 - **FW Ver AVR**—The firmware version of the AVR (automatic voltage regulator) that runs at all times except during an upgrade of the AVR firmware.
 - **FW Vers Ember**—An electronic component on the RF board that runs at all times.
 - **FW Vers Boot**—The firmware version of the gateway that runs during an upgrade of the Main gateway firmware.
- To refresh the data, click **(Refresh)** .

Edit gateway name

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

Delete gateway/s

You can only delete gateways that are offline.

1. Select the gateway/s that you want to delete.
2. Click [Delete Gateway\(s\)](#).
3. Click [YES](#) to confirm.

Issue gateway commands

1. Select one or more gateway/s.
2. Select one of the following commands:
 - [Clear gateway buffer](#)—Deletes buffer data on all devices connected to the gateway. The buffer is automatically cleared prior to upgrading firmware. (Not supported for C4 devices.)
 - [Deactivate Antenna](#)—Disables the selected gateway/s from the network and deactivates the gateway antenna. When the command result is successful, the antenna status is Deactivated (in the [Monitoring](#) module). (Not supported for C4 devices.)
 - [Get Access Point Status](#)—Requests the connectivity status (Online/Offline) for all paired access points.
 - [Get Gateway Firmware Status](#)—Requests the gateway firmware version installed on the gateway. (Not supported for C4 devices.)
 - [Get Gateway Status](#)—Requests the gateway connectivity status (Online/Offline).
 - [Pairing OFF](#)—Disables Pairing Mode. When the command result is successful, the antenna status is Pairing Off (in the [Monitoring](#) module). (Not supported for C4 devices.)
 - [Pairing ON](#)—Enables Pairing Mode. When the command result is successful, the antenna status is Pairing On (in the [Monitoring](#) module). (Not supported for C4 devices.)



Important! To eliminate the risk of binding access points to the wrong gateway, dormakaba strongly recommends that only one gateway be in Pairing Mode at a time. After all access points are paired to a gateway, send the Pairing OFF command to the gateway to disable Pairing Mode. As a precaution, Pairing ON mode changes to Pairing OFF after 15 minutes.

- [Reset Gateway](#)—Performs a soft reset on the selected gateway/s. (Not supported for C4 devices.)
 - [Set Clock and Lock Event Mask](#)—Sends the server time and the access point event notification settings (defined in [System Settings > Online Communication > Notifications](#)).
 - [Set Communications Settings](#)—Sends the communication configuration settings (defined in [System Settings > Online Communication > Online Communication Settings > Gateway update status, Access point wake-up, Gateway update status](#)).
 - [Unpair all Access Points](#)—Unpairs all access points. (Not supported for C4 devices.)
 - [Upgrade firmware](#)—Update the system-level software installed in the gateway. Prior to the upgrade, you must obtain the required file from dormakaba Support. This command applies to Gateway II devices only. (Not supported for C4 devices.)
 - [Verify Assignment](#)—Requests connectivity status from paired access points.
3. Click [Send Command](#).
 4. When notified the command is sent, click [OK](#).

Pair Access Points

Before you can pair access points, you must make an RF Pairing Key in [System Keys](#).

Make RF pairing key

1. Go to [System Keys](#).
2. Click [Special Function Keys](#).
3. Select [RF Pairing Key](#).
4. Click [Make Keys](#).
5. Select an encoder  that is online, present a key to the encoder, then click [Start](#).
6. When prompted that the key was made successfully, click [Done](#).

Pair access points



For Control 4 devices, skip directly to step 6.

1. Go to [Device Management > Registered Gateways & Paired Access Point](#).
2. Select the gateway where you want to pair access points.
3. Select the command [Pairing ON](#) (to activate the gateway antenna and put the gateway in Pairing Mode).
4. Click [Send Command](#).
5. When notified the command is sent, click [OK](#).
6. Present the RF Pairing Key to every access point that you want to pair to the gateway.



To eliminate the risk of binding access points to the wrong gateway, dormakaba strongly recommends that only one gateway be in Pairing Mode at a time. After all access points are paired to a gateway, send the [Pairing OFF](#) command to the gateway to disable Pairing Mode. As a precaution, [Pairing ON](#) is automatically changed to [Pairing OFF](#) after 15 minutes.

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

Paired access points

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

1. Go to [Device Management > Registered Gateways & Paired Access Points](#).
2. Select the gateway where the access point/s are paired.
3. Click [Next to access points](#).

Device Management >
REGISTERED GATEWAYS & PAIRED ACCESS POINTS

► METRICS

Access Points -Select command- Send Command Search by Access Point name 🔍 🔧 📊 🔄

☐	Access Point ↑	Status	Lock profile	Gateway	Building	Floor
☐	201	🟢	SAFFIRELX	GatewayII	Hilton	FLOOR2
☐	Cafeteria	🟢	RACS	RACS-XT	Hilton	FLOOR1
☐	RACS-MFC	🟢	RACS	RACS-MFC		

1 - 3 of 3 items
0 Selected

[Back to gateway selection](#)

The access points that are paired with the selected gateway and their respective status' are listed by name.



For RACS XT devices, you must trigger an event before the access point displays in the list. The simplest way to trigger an event is to present any key (valid or invalid) to the lock.

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

- Issue one of the following commands:
 - [Get Access Point Firmware Status](#)—Requests the current lock firmware version. (Not supported for Control 4 devices.)
 - [Get Access Point Status](#)—Gateway requests a full update to access point status.
 - [Set UTC Offset and Lock Event Mask](#)—Sends the server time and the access point event notification settings (defined in *System Settings > Online Communication > Notifications*).
 - [Unpair Access Point](#)—Unbind the access point from the gateway. This command is useful during gateway maintenance, when you need to pair an access point to a different gateway. (Not supported for Control 4 devices.)



If you want to associate an existing access point with a new room, you need to unpair and delete (or just delete) the existing access point on the Online Access Points page. Then, the "new" access point must be reprogrammed and paired to the gateway.

- [Upgrade firmware](#)—Request firmware upgrade. (Not supported for Control 4 devices.)
- [Verify Assignment](#)—Requests the gateway where access points are paired and the connectivity status.
- To filter based on connectivity status, click [\(Filter\)](#) and select the connectivity status (Online/Offline) as well as the monitored states (Low Battery/Door Open/Door Ajar/PrivacyEnabled/Unlatched) to list.
- To show/hide columns, click and select the information that you want to display. The following columns can be displayed:
 - [All](#)—Select this option to show all columns.
 - [Lock profile](#)—The lock model installed at the access point.
 - [Gateway](#)—The gateway to which the access point is paired.
 - [Building](#)—The building where the access point is located.
 - [Floor](#)—The building level where the access point is located.
 - [Low Battery](#)—Indicates whether the lock battery is low (TRUE=YES/FALSE=NO). You can filter the list to show access points with a low battery.
 - [RF signal](#)—Indicates whether the signal between the gateway and paired access point is weak or normal.
 - [Last offline](#)—The date and time the gateway was most recently offline.
 - [Last communication](#)—The date and time of the most recent and successful communication with the gateway.

- **Door Open**—Indicates whether the door is open. You can filter the list to show access points with an open door.
- **Door Ajar**—Indicates whether the door has been open beyond a predefined threshold. You can filter the list to show access points with a door ajar.
- **Door Ajar by**—Indicates the key type that was presented to open the door that is now in Door Ajar status.
- **Door Ajar Since**—Indicates the date and time the door became considered ajar (not open).
- **Privacy Enabled**—Indicates whether the deadbolt or privacy switch is engaged at the access point. You can filter the list to show access points with privacy enabled.
- **Unlatched**—Indicates if the access point is currently in Unlatched Mode (allowing unlimited access without a key). You can filter the list to show access points that are unlatched.
- **Last Entry**—The date and time of the most recent entry to the access point.
- **Date/Time Error**—Indicates whether the date and time require synchronizing.
- **FW Vers. Lock (Main)**—The current firmware version of the lock that runs at all times except during a firmware upgrade.
- **FW Vers. Lock (Boot)**—The current firmware version of the lock that runs during a firmware upgrade.
- **FW Vers. AVR (Main)**—The firmware version of the AVR (automatic voltage regulator) that runs at all times except during an upgrade of the AVR firmware.
- **FW Vers. AVR (Boot)**—The firmware version of the AVR (automatic voltage regulator) that runs during an upgrade of the AVR firmware.
- **FW Vers. Ember**—An electronic component on the RF board that runs at all times.
- **FW Vers. Quantum**—ZigBee RF board firmware version.
- To refresh the data, click **(Refresh)** .

Program Devices

Program Devices

This section includes the following subjects:

Program devices	300
-----------------------	-----

Program devices

RAC5-MFC/XT devices can be programmed using the M-Unit. Gateway II devices are configured/programmed in [Device Management > Online Device Configuration](#). A device must be reprogrammed any time configuration data affecting the device is modified in Ambiance.



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](#).

To program devices:

1. Go to [Programming & Auditing > Programming](#).
2. Click [Next to Devices](#).

3. Select the devices that you want to synchronize with Ambiance configuration data. The selected items display in the [Summary](#) section.
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.
8. On the M-Unit menu, select [TOOLS / Next Page / Configure RAC5](#). Device names display in groups of five. Use the [PREV](#), [NEXT](#) and [SEARCH](#) options to navigate and refine the list of names. Use the UP and DOWN arrow keys to make a selection.
9. Select the device name, then press [ENTER](#).
10. Select the type of cable (probe) that you are using to connect the M-Unit to the device.
11. When prompted, connect the cable to the device. Programming starts immediately. If the device has already been programmed, the M-Unit issues a message requesting confirmation to overwrite the existing programming.
12. When prompted that programming is complete, click [OK](#).

Notification Management

This section includes the following subjects:

Learning about Notification Management	302
Add notification groups	304

Learning about Notification Management

Notifications, conveniently accessible from the main Ambiance toolbar, keep staff members informed about online operations and events as well as the status of online access points. For example, a notification lets you know when a 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 online notifications are available:

- [Access point offline](#)—Notifies that there is no communication between the lock and the gateway.
- [Access point online](#)—Notifies that the lock is in communication with the gateway and online.
- [Door ajar clear \(door secure\)](#)—Door previously ajar has now been closed and is secure.
- [Door ajar generic](#)—Notifies that a door is in an open state.
- [Door ajar 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 (two minutes), 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 (one minute), 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 (two minutes), 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 (one minute), for example the time it would take to vacate a room.
- [Door latched](#)—Notifies that a door is closed with the lock engaged.
- [Door open](#)—Notifies when the lock's anti-pick mechanism is out. This is the default state of the door.
- [Door unlatched](#)—Notifies that the lock motor has been disengaged and the door can be opened without a key.
- [Fire alarm activated](#)—RAC5 MFC/XT notification only. An event that notifies when the fire alarm for the access point is activated.
- [Fire alarm deactivated](#)—RAC5 MFC/XT notification only. An event that notifies when the fire alarm for the access point is deactivated.
- [Gateway error code updated](#)—Notifies that an error code was issued for a gateway. The update may indicate that the gateway is in a good state (error code=0) or that an error has occurred.
- [Gateway offline](#)—Notifies that a gateway is currently not communicating with the Ambiance Server.
- [Gateway online](#)—Notifies that a gateway is communicating with the Ambiance Server.
- [Generic egress](#)—Notifies that a door open event occurred.
- [Guest key used](#)—Notifies that a guest key was presented to a lock. Details include the date/time that the key was presented.
- [Guest key used \(first entry\)](#)—Notifies a guest key was presented to a lock for the first time.
- [Low battery](#)—Notifies that the battery state is low and requires replacement. Ambiance sends a single low battery event/notification until batteries are changed. After batteries are changed, Ambiance sends a [Low battery clear \(battery normal\)](#) event/notification.
- [Low battery clear \(battery normal\)](#)—Notifies that the low battery status is cleared. The battery was replaced or the problem resolved.
- [Mechanical key override](#)—Notifies a lock override, accessing a lock with a mechanical key.
- [Operation failed](#)—Notifies the specified operation was unsuccessful. When available, the reason is indicated.
- [Privacy disabled/deadbolt retracted](#)—Notifies the status of the deadbolt as disengaged.
- [Privacy enabled/deadbolt engaged](#)—Notifies that the deadbolt or privacy switch is engaged.
- [Remote unlock close](#)—RAC5 MFC/XT notification only. The elevator door/lock that was unlatched remotely is now latched.
- [Remote unlock open](#)—RAC5 MFC/XT notification only. The elevator door/lock was unlatched remotely.
- [Request to exit close](#)—RAC5 MFC/XT notification only. A request to remotely unlatch the elevator door/lock was closed.
- [Request to exit open](#)—RAC5 MFC/XT notification only. A request to remotely unlatch the elevator door/lock is active.
- [Staff key used](#)—Notifies that a Staff key accessed a lock.

- **Standing intruder**—Alert: Possible standing intruder. Multiple keys presented at a single access point.
- **System key used**—Notifies that a System key was presented to a lock.
- **VIP access**—Notifies that a VIP guest key was presented to a lock. Details include the date/time that the key was presented.
- **VIP first access**—Notifies a VIP guest key was presented to a lock for the first time.
- **VIP operation failed**—Notifies the specified operation was unsuccessful. When available, the reason is indicated.
- **Wandering intruder**—Alert: Possible wandering intruder. Key presented at multiple access points.



Email and web service notifications are deleted from the Ambiance database after they are successfully sent.

Add notification groups

To add notification groups:

1. Go to [Notification Management](#).

Notification Group Information

Notification group name*

Battery Notifications

Notification methods

Email

YES

Web Service

NO

[-] Notifications

☐ Gateway online

☐ Generic egress

☒ Low battery

☒ Low battery clear (battery normal)

☐ Mechanical key override

☐ Operation failed

☐ Privacy disabled/deadbolt retracted

☐ Privacy enabled/deadbolt engaged

☐ Remote unlock close

Back to Notification Groups

Next to Access Points

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](#).

Access Points

▼ Name **Selected all access points**

- ☒ FLOOR0
- ☒ FLOOR1
- ☒ FLOOR2
- ☒ FLOOR3
- ☒ FLOOR4

1 - 61 of 61 items

Sort By **Name** 61 Access Point(s)

[Back to Events](#) **Save**

Summary

Notification Group Info

Notification Group	Notifications
Battery Notifications	Low battery Low battery clear (battery normal)
Notification methods	Email

Access Points

▼ Building77

▼ FLOOR0

Grid of access point icons for FLOOR0

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

User type
Employee

Email
Email

ID
ID

Mobile number
(201) 555-5555

Notification groups
Battery Notifications x

Enable Notification
YES ☐

Monitor (RLM)

Monitoring (RLM)

This section includes the following subjects:

Learning about Monitoring	307
View metrics	308
Monitor online operations	309
Monitor online events	311
Monitor access point status	314

Learning about Monitoring

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.

The Monitoring module is also where you can stay informed about online communication. The Metrics section provides a real-time snapshot of the gateways and access points on site. For example, you can see at a glance whether any locks have a low battery, if any doors are open, and how many access points have the deadbolt or privacy switch enabled. Beneath the metrics summary, detailed listings show remote lock operations and events and the status of all access points paired with gateways.

Access to data in the [Monitoring](#) module is configured in [Role Management](#). By default, the Administrator and Site Configurator roles have full access.

View metrics

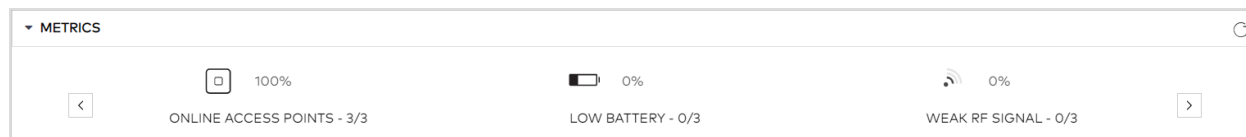
To view metrics:

In **Monitoring**:

» Metrics display by default.

In **Device Management**:

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



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

- **ONLINE GATEWAYS**—Percentage and total number of gateways currently online.
- **ONLINE ACCESS POINTS**—Percentage and total number of access points currently online.
- **LOW BATTERY**—Percentage and number of access points with a low battery. Zero percent indicates no access points signal a low battery.
- **WEAK RF SIGNAL**—Indicates whether the signal between the gateway and paired access point is weak or normal.
- **AJAR DOORS**—Percentage and number of access points with an open door.
- **PRIVACY ENABLED**—Percentage and number of access points with the deadbolt or privacy switch engaged.
- **DOORS UNLATCHED**—Percentage and number of access points with doors that are closed yet there is unlimited access without a key. Zero percent indicates no doors are unlatched, which means a key is required for entry.

At any time, you can expand or collapse the section.

Color codes reflect the state of the data. Green indicates no attention is required. Yellow indicates the situation may require attention.

Monitor online operations

The Operations tab beneath the Metrics section lists the commands and related details sent to gateways and paired access points. Commands are issued from [Device Management > Registered Gateways & Paired Access Points](#). Transaction details are reported for each operation.

View operations

To monitor online operations:

» Go to [Monitoring](#). Operations are displayed beneath the [Metrics](#) section.



Collapse the [Metrics](#) section to show only the list of operations.

Monitoring

Online

Keys

METRICS

Operations

Events

Access Point Status

Pending operations : 7 / Pending transactions : 0

☐ View system level operations

Search by Operator name

Date/Time	Operation Type	Operator	Status	Details	
10/31/2022 4:08 PM DST	Get gateway status	Admin01 User (Admin01)	Pending	Gateway(s): RACS-MFC(000E2A01B2E),XT3(),GatewayII(000E2A7002AA),XT(000E2A010C81),MFCQ	...
10/31/2022 4:06 PM DST	Get gateway status	Admin01 User (Admin01)	Pending	Gateway(s): MFCQ,RACS-MFC(000E2A01B2E),RACS-XT(000E2A010C81),GatewayII(000E2A7002AA),XT3()	...
10/31/2022 4:05 PM DST	Get gateway status	Admin01 User (Admin01)	Successful	Gateway(s): RACS-XT(000E2A010C81),RACS-MFC(000E2A01B2E),GatewayII(000E2A7002AA)	...
10/31/2022 4:04 PM DST	Get gateway status	Admin01 User (Admin01)	Successful	Gateway(s): RACS-MFC(000E2A01B2E)	...
10/31/2022 4:00 PM DST	Get gateway status	Admin01 User (Admin01)	Pending	Gateway(s): XT3(),MFCQ,RACS-MFC(000E2A01B2E),GatewayII(000E2A7002AA),RACS-XT(000E2A010C81)	...
10/31/2022 3:59 PM DST	Get gateway status	Admin01 User (Admin01)	Successful	Gateway(s): GatewayII(000E2A7002AA),RACS-MFC(000E2A01B2E),RACS-XT(000E2A010C81)	...

The following information is reported for each operation:

- **Date/Time**—The date and time when the operation occurred. You can filter the list based on date and time.
- **Operation Type**—Command sent to gateways and access points (for example, Pairing Off/On/Set Clock/Lock Event Mask). You can filter the list based on operation type.
- **Operator**—The full name of the Operator who was logged in when the operation occurred. You can search for commands that were sent when a specific Operator was logged in.
- **Status**—Command result (for example, Failed/Successful/Pending/Partially Successful). If the status is Failed, a reason is provided. You can filter the list based on status.
- **Details**—More information about the operation.

Customize the display

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

View Transaction Details

» Select an operation and click **(More)** .

Operation Transactions

Summary:

Date/Time: 10/31/2022 4:05 PM

Operation Type: Get gateway status

Operator: Admin01 User (Admin01)

Status: Successful

Details: Gateway(s): RAC5-XT(000E2A010C81),RAC5-MFC(000E2A01182E),GatewayII(000E2A7002AA)

Transactions:



Initiated	Last Update	Transaction	Gateway	Access Point	Status
10/31/2022 4:05 PM	10/31/2022 4:05 PM	Get gateway status	GatewayII (000E2A7002AA)		Successful
10/31/2022 4:05 PM	10/31/2022 4:05 PM	Get gateway status	RAC5-XT (000E2A010C81)		Successful
10/31/2022 4:05 PM	10/31/2022 4:05 PM	Get gateway status	RAC5-MFC (000E2A01182E)		Successful





1





100 ▾

1 - 3 of 3 items

Close

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

- **Initiated**—The date and time the command was issued.
- **Last Update**—The date and time the status was updated (either a response or timeout).
- **Transaction**—The type of transaction (for example, Key update/ADD KEY/BLOCK KEY/PAIRING ON/PAIRING OFF).
- **Gateway**—The gateway name and MAC address.
- **Access Point**—If the transaction involves an access point, the access point name; otherwise, the field is blank.
- **Status**—Command result (for example, Failed/Successful/Pending/Partially Successful). If the status is Failed, a reason is provided.

Customize the Display

- Click any column to sort the list. When done, click [Close](#).

Monitor online events

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

To monitor events:

1. Go to [Monitoring](#).
2. Beneath the [Metrics](#) section, click the [Events](#) tab.

Monitoring

Online

Keys

METRICS

Operations

Events

Access Point Status

Search by Access Point name or Key Holder name

Server Date/Time	Access Point Date/Time	Access Point	Building	Floor	Event Type	Possible Key Holder(s)	Details
10/31/2022 4:08 PM	10/31/2022 4:08 PM	-		-	Gateway Offline	Hub: XT3 ()	
10/31/2022 4:08 PM	10/31/2022 4:08 PM	-		-	Gateway Offline	Hub: MFC ()	
10/31/2022 4:06 PM	10/31/2022 4:06 PM	-		-	Gateway Offline	Hub: XT3 ()	
10/31/2022 4:06 PM	10/31/2022 4:06 PM	-		-	Gateway Offline	Hub: MFC ()	
10/31/2022 4:04 PM	10/31/2022 4:04 PM	RACS-MFC			Door ajar	Door ajar guest long	
10/31/2022 4:03 PM	10/31/2022 4:03 PM	Cafeteria	Hilton	FLOOR1	Door ajar	Door ajar guest long	
10/31/2022 4:02 PM	10/31/2022 4:02 PM	RACS-MFC			Door ajar	Door ajar guest short	
10/31/2022 4:02 PM	10/31/2022 4:02 PM	RACS-MFC			Access Point Online		
10/31/2022 4:01 PM	10/31/2022 4:01 PM	Cafeteria	Hilton	FLOOR1	Door ajar	Door ajar guest short	
10/31/2022 4:01 PM	10/31/2022 4:01 PM	Cafeteria	Hilton	FLOOR1	Access Point Online		
10/31/2022 4:00 PM	10/31/2022 4:00 PM	-		-	Gateway Offline	Hub: MFC ()	
10/31/2022 4:00 PM	10/31/2022 4:00 PM	-		-	Gateway Offline	Hub: XT3 ()	

1

2

3

4

100

1 - 100 of 369 items

The following information is reported for each event:

- **Server Date/Time**—Date and time when access point events are received by the server. You can sort and filter the list based on date and time.
- **Access Point Date/Time**—Date and time when the event occurred in the access point. You can filter the list based on date and time.
- **Access Point**—The name of the access point. You can search for events that occurred for a specific access point.
- **Building**—The building where the access point is located. This column only displays when multiple buildings are defined.
- **Floor**—The building floor on which the access point is located.
- **Event Type**—The type of event or type of key used (for example, Door Ajar or System Key Used). You can filter the list based on event type.
- **Key Holder**—The name of the key holder. Defaults: Guest 1 (for guests) and Unassigned (for staff or system keys). You can search for events based on the key holder name.
- **Possible Key Holder(s)**—The name of one possible key holder. Defaults: Guest 1 (for guests) and Unassigned (for staff or system keys). You can search for events based on the key holder name. In cases where a key ID is reused, the key holder may be one of multiple.
- **Details**—More information about the event (for example, Door Ajar / Short ajar - 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](#))  then [Clear](#).
- To clear all filters, click ([Remove Filters](#)) .

- Click any column to sort the list.
- To refresh data, click [\(Refresh\)](#) .

Events

The following events are reported:

- [Access point offline](#)—Occurs when there is no communication between the lock and the gateway.
- [Access point online](#)—Occurs when the lock is in communication with the gateway and online.
- [Door ajar clear \(door secure\)](#)—Occurs when a door previously ajar is closed and secure.
- [Door ajar generic](#)—Occurs when a door is in an open state.
- [Door ajar guest long](#)—Occurs when a door ajar extends beyond the configured threshold. The door ajar (long) event occurs when a door has been left open for a longer time interval (two minutes), indicating an unusual state, a potential intrusion.
- [Door ajar guest short](#)—Occurs when a door has been left open for a short time interval (one minute), for example the time it would take to vacate a room.
- [Door ajar staff long](#)—Occurs when a door ajar extends beyond the configured threshold. The door ajar (long) event occurs when a door has been left open for a longer time interval (two minutes), indicating an unusual state, a potential intrusion.
- [Door ajar staff short](#)—Occurs when a door has been left open for a short time interval (one minute), for example the time it would take to vacate a room.
- [Door latched](#)—Occurs when a door is closed with the lock engaged.
- [Door open](#)—Occurs when the lock's anti-pick mechanism is out. This is the default state of the door.
- [Door unlatched](#)—Occurs when the lock motor has been disengaged and the door can be opened without a key.
- [Fire alarm activated](#)—RAC5 MFC/XT event only. Occurs when the fire alarm for the access point is activated.
- [Fire alarm deactivated](#)—RAC5 MFC/XT event only. Occurs when the fire alarm for the access point is deactivated.
- [Gateway Error Code Updated](#)—Occurs when an error code for a gateway is issued. The update may indicate that the gateway is in a good state (error code=0) or that an error has occurred.
- [Gateway offline](#)—Occurs when a gateway moves into the Offline state. The gateway is not communicating with the Ambiance server.
- [Gateway online](#)—Occurs when a gateway moves into the Online state. The gateway is communicating with the Ambiance server.
- [Generic egress](#)—Occurs when a door opens.
- [Guest key used](#)—Occurs when a guest key is presented to an access point. Details include the date/time that the guest key was presented to the lock.
- [Guest key used \(first entry\)](#)—Occurs when a guest has accessed the lock for the first time.
- [Low battery](#)—Occurs when the battery moves into the Low battery state. The battery requires replacement. Ambiance sends a single low battery event/notification until batteries are changed. After batteries are changed, Ambiance sends a [Low battery clear \(battery normal\)](#) event/notification.
- [Low battery clear \(battery normal\)](#)—Occurs when the Low battery state is cleared. The battery was replaced or the problem was resolved.
- [Mechanical key override](#)—Occurs when a lock is accessed with a mechanical key (a lock override).
- [Operation failed](#)—Occurs when an operation is unsuccessful. When available, the reason is indicated.
- [Privacy disabled/deadbolt retracted](#)—Occurs when the privacy switch or deadbolt moves into the disengaged state.
- [Privacy enabled/deadbolt engaged](#)—Occurs when the privacy switch or deadbolt moves into the engaged state.
- [Remote unlock close](#)—RAC5 MFC/XT event only. Occurs when the elevator door/lock that was unlatched remotely is latched.
- [Remote unlock open](#)—RAC5 MFC/XT event only. Occurs when the elevator door/lock is unlatched remotely.
- [Request to exit close](#)—RAC5 MFC/XT event only. Occurs when a request to remotely unlatch the elevator door/lock is completed.

- **Request to exit open**—RAC5 MFC/XT event only. Occurs when a request to remotely unlatch the elevator door/lock is issued.
- **Staff key used**—Occurs when a Staff key accesses a lock.
- **Standing intruder**—Alert: Possible standing intruder. Multiple keys presented at a single access point.
- **System key used**—Occurs when a System key is presented to a lock.
- **VIP Access**—Occurs when a VIP key is presented to a lock. Details may include: VIP access granted, VIP access denied, Access denied (unknown VIP key), or VIP token not in lock.
- **VIP First Access**—Occurs when a VIP key is first presented to a lock.
- **Wandering intruder**—Alert: Possible wandering intruder. Key presented at multiple access points.

Monitor access point status

The [Access Point Status](#) tab beneath the [Metrics](#) section lists the status of paired access points.

To view the status about paired access points:

1. Go to [Monitoring](#).
2. Beneath the [Metrics](#) section, click the [Access Point Status](#) tab.

Monitoring

Online

Keys

METRICS

Operations

Events

Access Point Status

Search by Access Point name

Access Point	Status	Building	Floor	Low Batt...	RF Signal	Door Open	Door Ajar	Door Ajar by	Door Ajar Si...	Privacy E...	Unlatched	Last Entry	Last Update
RACS-MFC				NO	Normal	YES	YES	Guest	10/31/2022 4:02 PM	NO	NO	10/31/2022 9:47 AM	10/31/2022 4:04 PM
Cafeteria		Hilton	FLOOR1	NO	Normal	YES	YES	Guest	10/31/2022 4:01 PM	NO	NO	10/31/2022 9:47 AM	10/31/2022 4:03 PM
201		Hilton	FLOOR2	NO	Normal	NO	NO			NO	NO	10/28/2022 11:37 AM	10/31/2022 3:55 PM

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. Ambiance sends a single low battery event/notification until batteries are changed. After batteries are changed, Ambiance sends a [Low battery clear \(battery normal\)](#) event/notification.
- **RF Signal**—Indicates whether the signal between the gateway and paired access point is weak or normal.
- **Door Open**—Indicates whether the door is open. You can filter the list to show access points with an open door.
- **Door Ajar**—Indicates whether the door has been open beyond a predefined threshold. You can filter the list to show access points with a door ajar.
- **Door Ajar by**—Displays when Door Ajar event occurs. Indicates the key type that was presented to open the door that is now in Door Ajar status.
- **Door Ajar Since**—Displays when Door Ajar event occurs. Indicates the date and time the door became considered ajar (not open).
- **Privacy Enabled**—Indicates whether the deadbolt or privacy switch is engaged at the access point. You can filter the list to show access points with privacy enabled.
- **Unlatched**—Indicates if the access point is currently in Unlatched Mode (allowing unlimited access without a key). You can filter the list to show access points that are unlatched.
- **Last Entry**—The date and time of the most recent entry to the access point.
- **Last Update**—The current lock firmware version.

Customize the display

- To filter data, click [\(Filter\)](#) and select the information that you want to display.
- Click any column to sort the list.
- To refresh data, click [\(Refresh\)](#) .

Reports (RLM)

Reports (RLM)

This section includes the following subjects:

Online Access Points Status Report	316
Online Gateway Status Report	317
Online Paired Access Point Report	318

Online Access Points Status Report

Generate this report to display Online Access Points Status.

Generate report

1. Go to [Reports > Online Access Points Status Report](#).
2. Select whether to include online and/or offline gateways.
3. Select the status options to include in the report: All/Low Battery/Door Open/Door Ajar/Privacy Enabled/Unlatched.
4. Select whether to display firmware versions.
5. Click [Generate](#).

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

The report shows the following details for all current online gateways and access point status.

- Access Point
- Building
- Floor
- Status
- Low Battery
- Door Open
- Door Ajar
- Privacy Enabled
- Lock Latched
- Last Entry
- Last Update
- FW Vers Locks
- FW Vers AVR
- FW Vers Ember
- FW Vers Quantum

Online Gateway Status Report

Generate this report to view gateway status information.

Generate report

1. Go to [Reports > Online Gateway Status Report](#).
2. Select whether to include online and/or offline gateways.
3. Select whether to include relevant firmware versions.
4. Click [Generate](#).

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

- Communication Status
- Display Firmware Version
- Site
- Report generated by
- Report generated on
- Gateway
- Type
- Mac Address
- Status (Online/Offline)
- Antenna
- Last Update
- FW Vers Gateway
- FW Vers AVR
- FW Vers Ember

Online Paired Access Point Report

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

Generate report

1. Go to [Reports > Online Paired Access Point Report](#).
2. Select whether to include offline access points.
3. Click [Generate](#).

View report details



The Reports toolbar is a convenient feature that you can use to navigate, download, print and zoom reports. Multiple download formats are supported.

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

Troubleshooting

This section includes the following subjects:

Services Manager	320
Troubleshooting PMS	324
Troubleshooting encoders	326
Troubleshooting locks	330
Log data	336

Services Manager

The Services Manager provides convenient access to post-installation configuration options and troubleshooting. The following actions are available:

- start and stop product services
- open configuration files for product services
- install/renew SSL certificate after installation
- change server IP address
- collect Support information
- open Event Viewer
- open Windows Services

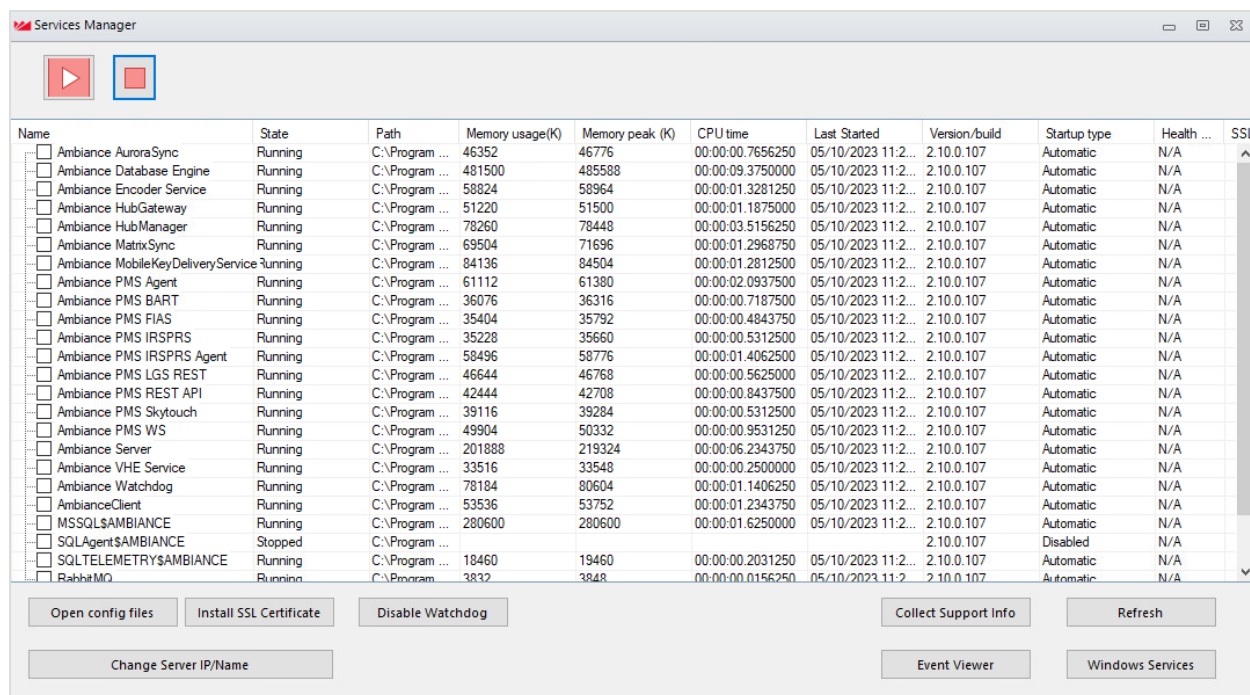
Open the Services Manager

Access the Services Manager on the server from the default location:

C:\Program Files\dormakaba\Ambiance Server\Services\Service Manager\ServiceManager.exe

Access the Services Manager on the workstation from the default location:

C:\Program Files (x86)\dormakaba\Ambiance Client\Services\ServiceManager\ServiceManager.exe



Install / renew SSL certificate after installation

Use the Services Manager to install or renew an SSL certificate on the Ambiance server after installation. Each Ambiance workstation must be updated to use the HTTPS protocol.

Server

1. On the Ambiance server, open the Services Manager.
2. Click **Install SSL Certificate**.
3. Disregard the warning message and click **Yes** to proceed.

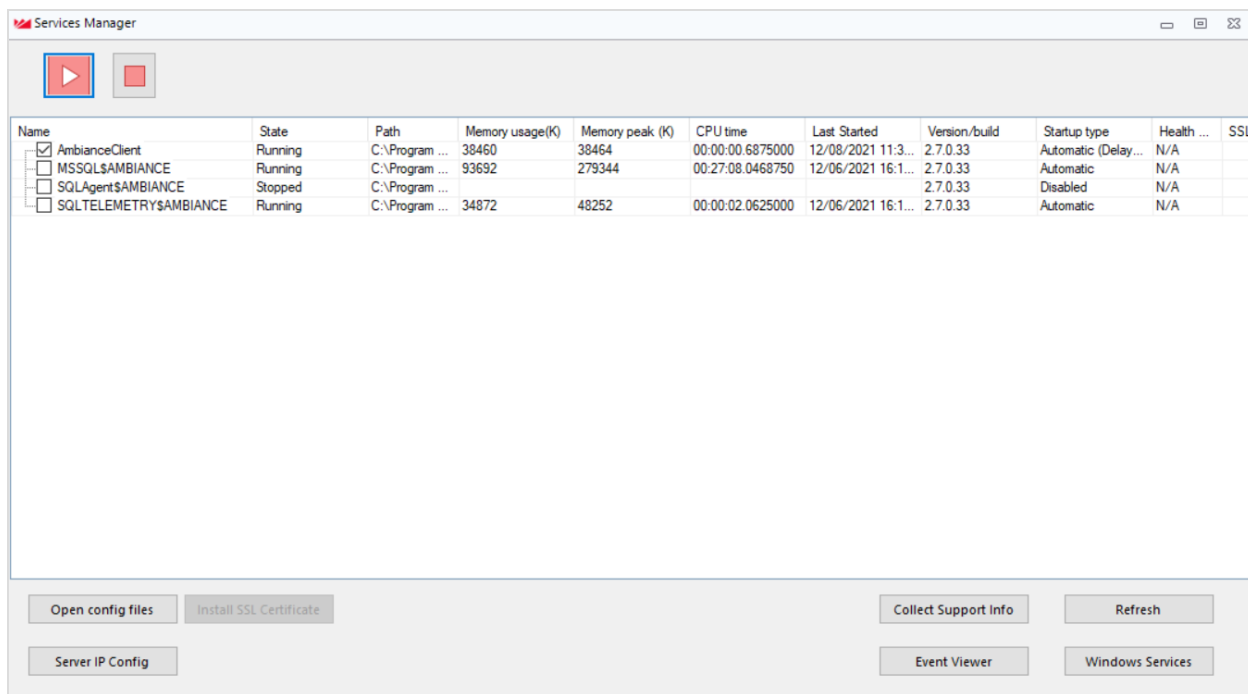


4. If applicable, specify the password for the certificate.
5. Click [Select File](#).
6. Navigate to and select the certificate (.pfx).
7. When notified the certificate was installed successfully, click [OK](#).

Client

The following steps must be performed on each Ambiance workstation.

1. Open the Services Manager.



2. Select the [AmbianceClient](#) service and click  to stop the service.
3. Click [Open Config files](#).
4. Change "WebAPIUrl" and "signalrURL" values to point to **https**:
 - From:


```
<add key="WebAPIUrl" value="http://<Ambiance Server IP>/WebAPI/" />
<add key="SERVICE_URL_WITH_PORT" value="http://localhost:40100" />
```
 - To:


```
<add key="WebAPIUrl" value="https://< Ambiance Server IP>/WebAPI/" />
<add key="SERVICE_URL_WITH_PORT" value="https://localhost:40100" />
```

5. Save and close the configuration file.

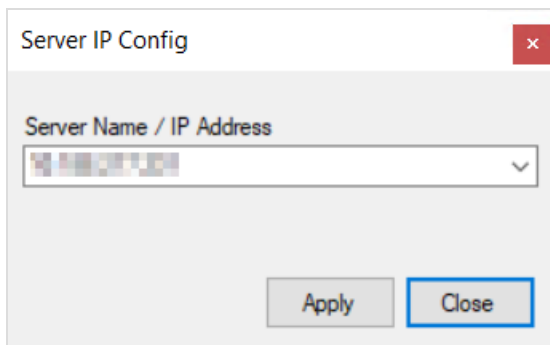
6. Click  to restart the Ambiance Client service.

Change server IP address / name

Use the Services Manager to change the Ambiance server IP address after installation. Changing the IP address requires that the Ambiance client be uninstalled and reinstalled on each workstation.

Server

1. On the Ambiance server, open the Services Manager.
2. Click [Change Server IP/Name](#).
3. Disregard the warning and click [Yes](#) to proceed.
4. Specify the new IP address or name, then click [Apply](#).



5. Restart the Ambiance Server.

Client

The following steps must be performed on each Ambiance workstation.

1. Open the Services Manager.
2. Select the [AmbianceClient](#) service and click  to stop the service.
3. Click [Open config files](#).
4. Change "WebAPIUrl" and "signalrURL" values to point to the new IP address.

- From:

```
<add key="WebAPIUrl" value="https://<Ambiance Server IP>/WebAPI/" />
<add key="signalrURL" value="https://< Ambiance Server IP>/
WebAPI/signalr/" />
```

- To:

```
<add key="WebAPIUrl" value="https://< Ambiance NewServer IP>/WebAPI/" />
<add key="signalrURL" value="https://< Ambiance NewServer IP>/
WebAPI/signalr/" />
```

5. Save and close the configuration file.

6. Click  to restart the Ambiance Client service.

Open configuration files

To open configuration files, select the services for which you want to view the corresponding configuration files, then click [Open config files](#). Each configuration file opens in a separate window.

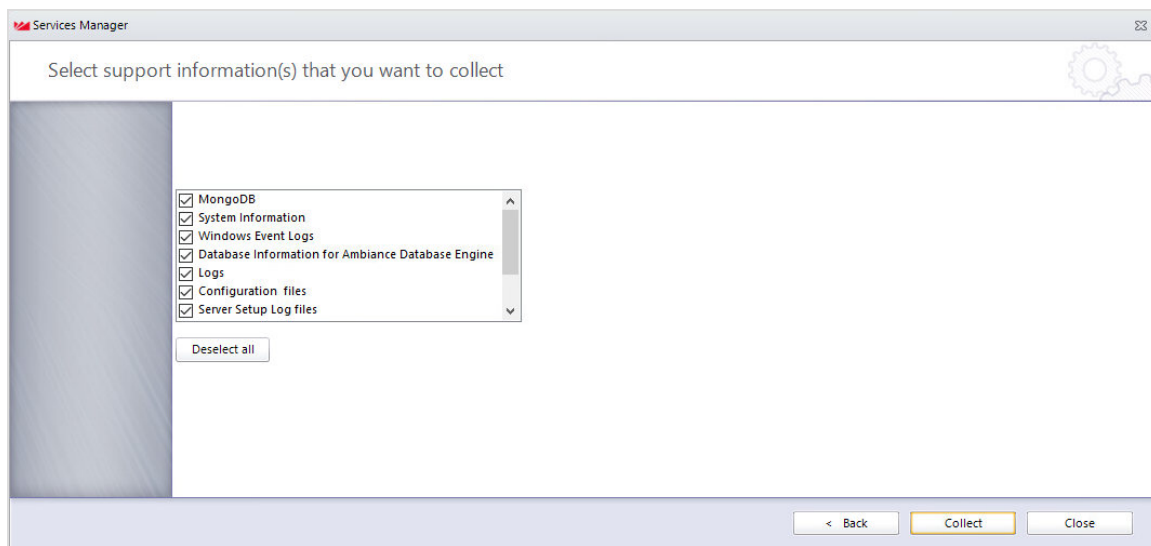
Disable/enable Watchdog

The Services Manager includes a Watchdog feature that performs regular healthchecks on the server. The Watchdog is enabled by default. To disable / enable Watchdog, open Services Manager and click the appropriate button.

Collect support information

Prior to contacting dormakaba for support, collect information about your Ambiance system. Collect information on the server and workstation.

1. Open the Services Manager, then click [Collect Support Info](#).



2. Select the type of support information that you want to collect.
3. Click [Collect](#).
4. Specify a file name, then click [Save](#).

Open Event Viewer

To open Windows Event Viewer app, click [Event Viewer](#).

Open Windows services

To open Windows Services app, click [Windows Services](#).

Troubleshooting PMS

Refer to the troubleshooting information for your selected protocol.



If the Server was recently installed, upgraded or restarted, wait two to three minutes before attempting PMS operations.

IRS and PRS

When using the IRS/PRS protocol, take the following steps to troubleshoot the PMS:

1. Go to [System Settings > PMS > IRS/PRS](#) and enable either the IRS or PRS protocol.
2. Modify the port number (if needed).
3. Make sure that the following services are running:
 - Ambiance PMS Agent
 - Ambiance PMS IRS/PRS
 - Ambiance PMS IRS/PRS Agent
4. Go to `C:\ProgramData\dormaKaba\Ambiance\logs\IRS` and verify activity in the logs. The logs contain any error generated and also keys strings received and sent out.
5. IRS requests come in two different types:
 - Standard key names (5 Characters)
 - Extended default (15 Characters)

To set the key name size you must use Notepad to modify the `Kaba.PMS.IRS.SocketService.Host.exe.config` file found here `C:\Program Files\dormakaba\Ambiance Server\Services\PMS.IRS\`

```
<!-- 15 characters: true or positive number -->
<!-- 5 characters: false, 0 or negative number -->
<add key="IRS.Protocol.LongRoomNumber" value="true" />
```
6. (IRS only) By default, PMS login credentials are required. You can either go to [Staff Management](#) to configure PMS login credentials or go to [System Settings > Security > PMS](#) to disable the requirement to use PMS authentication.
7. (PMSs that require CHECKSUM) Go to `C:\Program Files\dormakaba\Ambiance Server\Services\PMS.IRS\` and edit the `Kaba.PMS.IRS.SocketService.Host.exe.config` file


```
<add key="EnableChecksum" value="1" />
```

FIAS

The only modifications that may be needed for FIAS are the port number and enabling shared-with registrations.

1. Verify the following services are running
 - Ambiance PMS Agent
 - Ambiance PMS FIAS
2. Go to `C:\ProgramData\dormaKaba\Ambiance\logs\FIAS\` and verify activity in the logs. The logs contain any error generated and also keys strings received and sent out.
3. The following settings can be modified in the FIAS configuration file:



The values should not be changed unless requested by the PMS company.

```
<add key="FIAS.Options.FieldList.KR" value="GNKCKTRNWS$2DADTG#GAGDKOSITIK#" />
<add key="FIAS.Options.FieldList.KD" value="GNKCRNWSG#DATI" />
<add key="FIAS.Options.FieldList.KM" value="GNWSKCRNROKOGDG#SIUODT" />
```

```

<add key="FIAS.Options.FieldList.KA" value="WSKCASG#CT$3" /> <!-- Add option to skip KA for certain Record (Default 0 do not skip)-->
<!--<add key="FIAS.Options.SkipAnswer.<RecordId>" value="<0,1>" />-->
<add key="FIAS.Options.SkipAnswer.KR" value="0" />
<add key="FIAS.Options.SkipAnswer.KD" value="0" />
<add key="FIAS.Options.SkipAnswer.KM" value="0" /> <!--DefaultCheckOutTime hh:mm --> <add
key="FIAS.Options.DefaultCheckOutTime" value="" />
<add key="FIAS.Options.DefaultGuestStayDays" value="0" />
<add key="FIAS.Options.CheckOutMinutesToAdd" value="0" />
<add key="FIAS.Options.IntefaceFamily" value="DL" />
<add key="FIAS.Options.VendorSystemVersion" value="1.01" />

```

LGS SOAP API

SOAP 1.1 is the default configuration after installation. When using the Web Service protocol, take the following steps to troubleshoot the PMS:



After an upgrade, reconfigure the LGS SOAP API configuration file settings with the same parameters prior to the upgrade.

- Go to *System Settings > PMS > Web Service* and verify:
 - Port number is 80 for HTTP and 443 for HTTPS.
 - Shared-with registrations is enabled.
- Make sure that the following services are running:
 - Ambiance PMS Agent
 - Ambiance PMS WS
- Go to *Staff Management* and verify that PMS login credentials are defined for at least one Operator. The credentials are set on the *Operator Info* tab.
- Go to C:\ProgramData\dormaKaba\Ambiance\logs\WS\ and verify activity in the logs. The logs contain any error generated and also keys strings received and sent out.

LGS REST API (KF2)

The LGS REST API (KF2) protocol requires that you generate a certificate.

- Go to *System Settings > PMS > Select LGS REST API (KF2)*.
- Click *Generate New Certificate*.
 - Minimum logging is enabled by default. To increase logging, open the *log4net.config* file, change all instances of *WARN* to *ALL*, then restart the service.
 - The default port configuration should be retained unless otherwise requested by the PMS company.



For Agylis and other PMS companies that require a CHECKSUM, Ambiance version 2.0.1.4 (or greater) is required. For Maestro PMS, the room name must remain long.

Troubleshooting encoders

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

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

Is the Ambiance Client required/installed?

You must install the Client on every workstation where a USB encoder and / or Maintenance Unit is required. From Ambiance, download the Client. A total of three files are required: Ambiance_Client.exe, serverURL.config, and token.txt.



Do not install the Client on the Ambiance Server.

Follow the instructions for each of the following wizard pages.

1. On the [Welcome](#) page, click [Next](#).
2. On the [License Agreement](#) page, accept the terms of the license agreement then click [Next](#).
3. On the [Choose Destination Location](#) page, choose where to install Client files, then click [Next](#). The default location is recommended.
4. When notified the installation is successful, click [Finish](#).

Is the encoder connected to the workstation and configured correctly?

The initial configuration of an encoder requires that you connect the encoder to the Ambiance workstation using a USB cable. By default, the device emits an audible beep and flashes a green light to indicate a successful connection. If you configure the encoder to connect using the USB method, the encoder must remain connected to the workstation.

Configure an encoder for USB

1. Plug the encoder into the workstation.
2. In [Device Management](#), click [New Encoder](#).
3. Specify a unique name that does not exceed 50 characters. This name displays in the list of encoders.
4. Specify a number to identify the encoder to the PMS (Property Management System). Valid values: 0-99. (Ambiance currently supports MICRO FIAS, Saflok Web Service, and Saflok IRS.)
5. Select the MAC address of the encoder. The value is automatically detected when you connect the encoder to the workstation.
6. Select [USB](#).
7. Click [Save](#).

Configure an encoder for TCP/IP



Before starting, verify that a port is open for inbound communication on the Ambiance server (typically, configured during initial server installation).

1. Plug the encoder into the workstation.
2. In [Device Management](#), click [New Encoder](#).
3. Specify a unique name that does not exceed 50 characters. This name displays in the list of encoders.

4. Specify a number to identify the encoder to the PMS (Property Management System). Valid values: 0-99. (Ambiance currently supports MICRO FIAS, Saflok Web Service, and Saflok IRS.)
5. Select the MAC address of the encoder. The value is automatically detected when you connect the encoder to the workstation.
6. Select TCP/IP.
7. Select whether to obtain an IP address automatically. If using DHCP, select **YES**.
8. Select whether to use the Server name or IP address, then specify the correct information.
9. If not using DHCP, specify the IP address for the encoder including the subnet mask and default gateway.
10. Click **Save**.

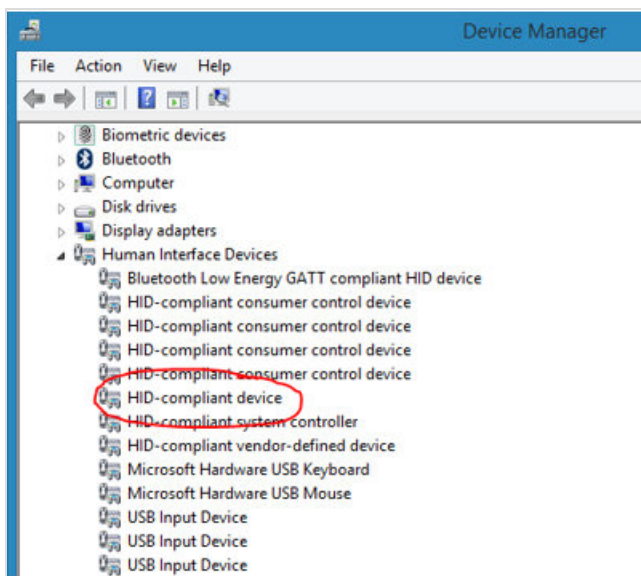
Are you still having a problem encoding or reading keys?

To prepare for troubleshooting, review the following log:

<C:\ProgramData\dormaKaba\Ambiance\logs\Services\DokaClient.exe.log>

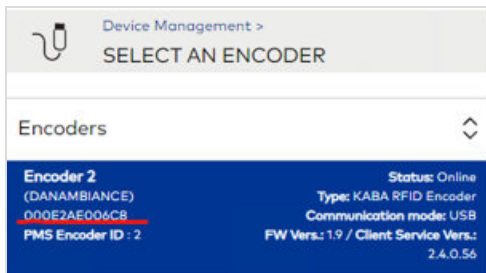
Troubleshooting steps:

1. Make sure that the Ambiance Client Service is running on the workstation. Go to Services and check (or restart) the Ambiance service.
2. Verify the physical connection between the encoder and the workstation. Unplug and plug in the encoder. Make sure that you hear 2 beeps and that the lights are on under the encoder.
3. Verify encoder In Device Manager:
 - a. Unplug the encoder from the workstation.
 - b. Open Device Manager.
 - c. Plug in the encoder.
 - d. Verify that a new HID-Compliant Device appears and it is not in an error state.



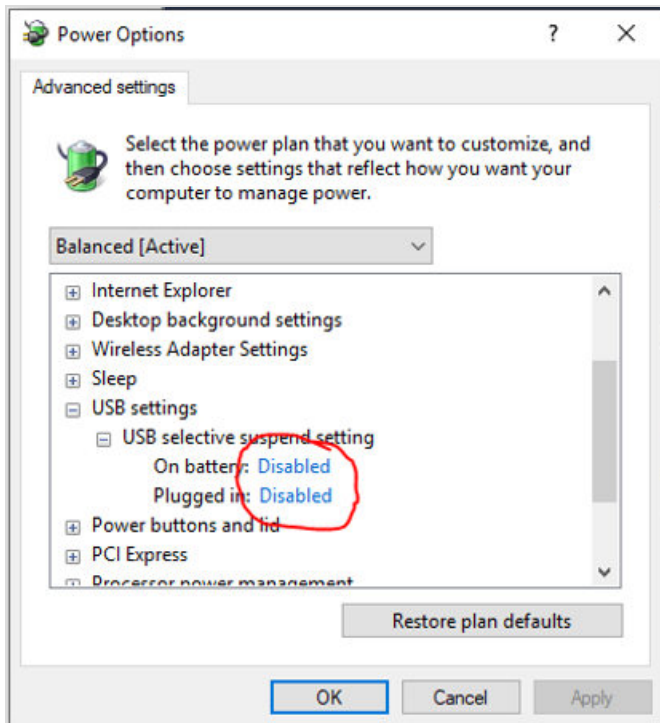
4. Verify IP address:
 - a. Go to: `C:\Program Files (x86)\dormaKaba\Ambiance Client\Services\ClientServices` and open the file [DokaClient.exe.Config](#) (in Notepad).
 - b. Verify that the correct server IP address is in the following lines:


```
<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).

6. If a USB encoder stops working follow these steps on the workstations:
 - a. Go to Control Panel – Power Options.
 - b. Click on Change Plan Settings.
 - c. Click on Change Advanced power settings.
 - d. Select USB settings.
 - e. Select USB Selective suspend setting.
 - f. Change both settings to Disabled.



7. Is the encoder MAC address not showing up after the Client installation?
 - The Server was set up using either the Server name or IP address.
 - Install the Client using the Server name instead of IP address.
 - Perform a hard reset on the encoder:
 - a. Unplug the encoder cable.
 - b. Press and hold the reset button at the back of the encoder.
 - c. Insert the encoder cable to power encoder (while still pressing and holding its reset button).
 - d. Keep pressing and holding the encoder reset button for 2 more second then let go of the reset button. You should hear 5 quick beeps if the encoder reset is successful.



If the problem persists after troubleshooting, contact dormakaba Support.

Troubleshooting locks

Unused keys

For security reasons, dormakaba imposes a maximum on the number of unused keys that can be issued for a given credential. For example, when more than 15 keys are issued but never presented to Room 100, the access point becomes "out of sequence" and denies access to all of the keys.

To restore key access, reprogram the access point using the Maintenance Unit or resequence the access point using the Resequencing Key. After the access point is resequenced, the access point accepts the most recently issued key.

The maximum number of unused keys before resequencing is required depends on the key type:

- Guest Keys
 - Room, Suite, Foyer Door, Connector keys=15
 - Limited Use=3
- Staff Keys
 - All classes=unlimited
- System Keys
 - Failsafe, Latch, Unlatch, Toggle Latch/Unlatch=15
 - ELO=3
 - Inhibit=0
 - PPK/SPK=0

Light Indicators

The three light indicators (green, yellow and red) are located on the face of the lock. These lights provide lock status information when a key is inserted into the lock and removed. When using an RFID lock, the following LED indicators will appear when a RFID card is presented to the lock reader.



The default opening cycle is four seconds but is programmable.

Green Light

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

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

This sequence indicates that the locking mechanism has been released and the door handle can be depressed to open the door. If the handle is not depressed while the green light is flashing, the locking mechanism will be secured, and the key must then be reinserted and removed from the lock to release the latch.

Yellow Light

Flashing Yellow Light (12 Times)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

This flashing yellow light indicates that a correct key has been used in the lock, but the dead bolt or privacy button/switch has been set from inside the room.

Fast Flashing Yellow Light (8 Times)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

This fast flashing yellow light indicates that a correct key has been used in the lock, but entry is denied for one of the following reasons:

- The door has been electronically double-locked by an electronic lockout key.
- The Guest key has been automatically inhibited, or the lock has been inhibited by the inhibit key.
- The key was programmed with an expiration date and time. The light indicates that the key was used after this expiration date and time.
- The Master key was programmed to work only during certain shift hours of the day, or to work only on certain days of the week. The light indicates that the key used was not programmed for that shift or day.

Two Yellow Flashes

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

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

1 Yellow before 7 Green

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

This sequence indicates Master Key is about to expire but access is granted. This light will appear seven days prior to the expiration date.

1 Yellow before 7 Yellow

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

This sequence indicates Master Key is about to expire but access is denied (Privacy=ON). This light will appear seven days prior to the expiration date.

Red Light

Alternately Flashing Red Light

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

OR

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

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

Simultaneously Flashing Red Light

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

OR

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

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)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

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.

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

These lights indicate that the lock was unable to properly read the lock code on the key.

No Lights

If no lights appear when a key is used:

- An invalid key shutdown is in effect.
- The key switch is broken.
- The lock batteries are dead.

Invalid Lock and Mode Indicators

Locks are designed to operate in Mode 2 when it is programmed and properly functioning. If a lock is not operating in Mode 2, and a valid key is used, you will see one of the following patterns. These lights indicate that there is a physical problem with the lock that must be corrected before the lock will allow keys to operate normally.

1 Green, 1 Yellow, 1 Red, Then All Lights Flash (4 Times)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

These lights that the lock is in the Test Mode, and the storage chip has failed. No key will open the lock, and the lock must be drilled to access the room.

All Lights Flash (4 Times)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

These lights indicate that the lock is in Mode 0 and that there is a problem with the circuit board. Use the erase key to change the mode to Mode 1, and program the lock using the LPI probe and terminal. Use the new key to open the door and replace the circuit board.

2 Green. Then All Lights Flash (4 Times)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

These lights indicate that the lock is in Mode 1, and is not programmed. Program the lock using the LPI probe and terminal. Use the new key to open the door and replace the circuit board.

2 Green and Yellow Flashes. Then All Lights Flash (4 Times)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

These lights indicate that the lock is in Mode 3 and that there is a programming problem with the programming chip in the lock's circuit board. Open the door using the PPK key followed by a valid Master key. Remove the lock and replace the circuit board.

2 Red Flashes. Then All Lights Flash (4 Times)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

These lights indicate that the lock is in Mode 4, and that the storage chip is disabled. Use the PPK key followed by the Disable/Enable key to enable the lock.

2 Yellow Flashes, Then All Lights Flash (4 Times)

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

These lights indicate that the lock is in Mode 5, and that there is a problem with the motor switch or the motor is jammed. Open the door using the PPK key followed by a valid Master key. Then, remove the lock and replace the lockset.

Online

1 green, few yellow, 6 green.

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

When passing an RF Pairing key and the pairing is successful.

1 green, few yellow, 2 red.

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

When passing an RF Pairing key and the pairing fails.

2 green, 3 red

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

When passing an RF Unpairing key, this sequence indicates the lock was not paired.

1 green, 3 yellow, 6 red

	Second 1								Second 2								Second 3								Second 4								Second 5								Second 6							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
GREEN																																																
YELLOW																																																
RED																																																

When passing an RF Unpairing key, this sequence indicates the lock was paired and is now unpaired.

Log data

Ambiance logs provide detailed information about all events and system activity that occur during installation (or upgrade) and product use. For Support technicians, logs are the principal troubleshooting resource.

Installation logs

The following Installation logs are located on the server by default at: C:\Ambiance Server:

- MongolInstall (for online communication)
- SetupServer (primary installation log)

The following Installation log is located on the workstation by default at: C:\Ambiance Server:

- SetupClient.LOG

Product logs

Multiple logs are stored by default at: C:\ProgramData\dormaKaba\Ambiance\logs

The logs folder organizes log files as follows:

- FIAS
 - FIAS.log.txt—Data related to the Ambiance PMS FIAS Windows service.
 - PMSIO.txt—Data related to FIAS PMS key encoding.
- IRS
 - IRS.log.txt—Data related to the Ambiance PMS IRSPRS Windows service.
 - PMSIO.TXT—Data related to IRS PMS key encoding.
- IRSAgent—Data related to the Ambiance PMS IRSPRS Agent Windows Service. The IRS Agent serves as an intermediary between PMS IRS and the Ambiance server.
- PMS.LGS.REST—Data related to the LGS REST API Windows service.
- PMS.REST.API—Data related to the LGS REST API (KF2) Windows service.
- PMSAgent—Data related to the Ambiance PMSAgent Windows Service. The PMS Agent serves as an intermediary between all PMSs and the Ambiance server.
- Services—Data related to the various Ambiance Windows services.
- Web
 - reportapi.log.txt—Data related to the IIS component report API used to generate reports.
 - webApi.log.txt—Data related to the Ambiance WebAPI Windows service.
- WS (Web Service)
 - PMSIO.txt—Data related to LGS SOAP API key encoding.
 - WS.log.txt—Data related to the LGS SOAP API Windows service.

Glossary

A

Access Management

The module where you define credentials for staff and system keys, configure and assign schedules, configure common area access, and create logical groupings of access points to facilitate credential assignment.

Access Point

1) Virtual representation of a physical location where passage between two spaces is controlled by a lock. 2) Reader-equipped lock encoded with access control data to allow or deny access based on credentials.

Access Point Audit Report

Detailed historical information about lock events.

Access Point Group

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

Access Point Scheduling

Submodule within Access Management where you assign auto-unlatch and access schedules to access points.

Access Point Status

Current state of the lock installed for a given access point.

Access Point Type (Ambiance)

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

Access Schedule

Day and time constraints that control when an access point is accessible.

Additional Key

Duplicate key. A New key must be active before the option to make an Additional key is enabled. Additional keys do not affect any existing active keys.

Amenities

Guest common areas. Access to an amenity may be included in guest registrations by default or may require manual selection.

Audit

The process of retrieving historical information from an access point.

Auto-Unlatch Schedule

Day and time periods allowing passage without keys.

B**Block Key**

System key that temporarily blocks all keys encoded with a specific credential.

Building

Component in Property Builder that represents a physical structure on the site that contains one or more floors and one or more access points.

C**Cancel Key**

System key that permanently invalidates a specific key instance.

Check-in

The date and time when guest access begins.

Check-out

The date and time when guest access ends.

Common Area Access

Submodule in Access Management where common area profiles are defined to configure access to common areas.

Common Area Profile (Ambiance)

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.

Connector

1) Credential class for guest keys. 2) A Connector credential facilitates guest access to all access points in the credential.

Construction Keys

Keys that secure access points after installation yet prior to locks being programmed. Construction (or Zone) keys are obsolete after locks are programmed.

Credential

1) Configuration that consists of access point groups and/or individual access points for the purpose of authorizing staff access to a physical space or system key functionality. 2) Digital identification code stored on a key that authorizes access where the code is valid.

Credential Class

Organizational label used to group credentials based on the credential class type.

Credential Class Type

A fixed set of access properties from which all credential classes are derived.

Credential Management

Submodule in Access Management where you create and manage credentials.

Credential/Access Point Assignment Report

List of credentials and assigned access points or a list of access points and assigned credentials.

D**Device Management**

The module where you add and configure encoders. If online communication is enabled, you can also configure gateways and paired access points. In cloud environments, you can also configure the cloud gateway when licensed for Cloud Gateway - PMS Bridge.

Diagnostic Key

System key that queries locks to extract and report the status of various lock functions for troubleshooting and reporting. Diagnostic results are communicated by an LED flash sequence.

E**Electronic Lockout (ELO) Key**

1) Credential class for system keys. 2) System key that temporarily invalidate all non-Emergency Keys.

Elevator

A physical structure intended to provide access to building floors.

Elevator Bank

Group of elevators that share the same elevator controller configuration.

Elevator Configuration Report

Detailed information about an elevator bank including elevators and relay-to-floor mapping for each panel.

Elevator Controller Profile

The elevator bank model configuration.

Emergency Key (Ambiance)

1) Credential class type/class that overrides deadbolt/privacy switch. 2) A type of key encoded with a credential based on the Emergency class.

Encoder

Embedded device used to encode keys.

F

Failsafe Key

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

Firmware

Operating software for hardware devices.

Floor

Component in Property Builder that represents a level in a building.

Folio

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

Foyer Door

Guest-level access point type that serves as a common door to one or more guest rooms / suites.

G

Gateway

Gateways are the network devices which are paired to access points for online communication.

Grand Master Key

1) Credential class for staff keys. 2) Key on which a Grand Master credential is encoded.

Guest

Person added in the Guest Registration module for the purpose of assigning guest rooms and/or common area access.

Guest Common Area

Type of access point where general access is configured for guests (with or without staff access).

Guest Registration

1) The module where you add and manage all guest registrations and make keys for guests. 2) The record of a guest stay.

Guest Room

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

I

Inhibit Key

1) Credential class for system keys. 2) System key that permanently cancels all access for a current guest.

K

Key

A transport medium on which a credential is encoded for the purpose of controlling access and/or performing system or programmatic operations. Examples include key cards and key fobs.

Key Expiration Report

Lists the expiration date of active keys.

Key Holder

A person with authorized possession of at least one key.

Key ID

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

Key Mode

Option that you select when making a key: New or Additional.

Key Status

The current state of the key.

Key/User Assignment Report

List of active keys assigned to a given key holder.

L

Latch Key

1) System key credential class. 2) System key that disables passage mode.

Limited Use Key (Guest)

A guest key that is encoded with one-time access to a guest room or suite.

Limited Use Key (Staff)

1) Credential class type/class for staff keys. 2) A staff key that is encoded with temporary access to an access point for a predefined number of times or until the key expires.

Lock Profile

Lock device model.

M

Maintenance Unit (M-Unit)

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

Master Key

1) Credential class for staff keys. 2) A staff key encoded with a credential based on the Master class.

Meeting Room

Type of access point intended to accommodate special events for the public and/or registered guests.

Mobile Key

Virtual key issued to a mobile phone.

Monitoring

The module where you view a list of all keys made by Ambiance. When online communication is enabled, you can also view online metrics, operations, events and access point status.

N

New Key

Key made using mode New. New keys invalidate access to the selected credential on all existing keys.

Notification

Alert issued to notification subscribers.

Notification Group

Logical grouping of one or more notification events configured in the Notification Management module for the purpose of Operator subscription.

Notification Management

The module where you configure and manage the notification groups that can be assigned to staff members.

O

Online Access Point Status Report

Details about current gateways and paired access points.

Online Communication

A licensed feature that refers to wireless communication between access points and Ambiance. Remote communication is used to perform online access point operations and to receive online access point events.

Online Gateway Status Report

Details about current gateways.

Online Paired Access Point Report

Lists the access points paired to a gateway.

Operator

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

Operator Report

Lists Operators, their assigned roles, and the rights associated with each role.

Operator Status

Status of an Operator.

P

Paired Access Point

In online communication, an access point that is connected to a gateway.

Panel/Relay

Electrical component in an elevator controller box with one or more relay switches. A relay is an electrical component that is mapped to specific floors.

Passage Mode

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

PCI-DSS

Information security standard that provides additional login protection.

Period (Schedules)

A span of time selected for schedules in Access Management.

Preregistration (Guest)

Guest registration made for a date in the future.

Primary Program Key

System key that authorizes the function of another system key.

Programming & Auditing

The module where you perform the data transfers necessary to program and audit locks.

Property Builder

The module where you create a virtual representation of the site: buildings, floors and elevators per building, and access points.

Property Configuration Report

Details about the access point configuration for the site.

Property Management System

Software used in the hospitality industry that integrates with Ambiance to make keys.

R

Reader

Embedded device that reads access control data stored on keys.

Replacement Key

An additional key made to replace a lost or defective key.

Reports

The module where you track, investigate and maintain current and historical records for every aspect of your site.

Resequence Key

System key that resynchronizes a specific key credential in access points.

Restricted Area

Type of access point intended for staff access only.

RFID

Radio Frequency Identification. Technology that supports contactless keys.

Rights (Role Management)

Discrete permissions to Ambiance functionality.

Role

A group of rights assigned to an Operator.

Role Management

The module where you configure Operator Roles and the system and key rights associated with each role.

Roles & Rights Report

Lists the roles defined in the Role Management module and the Ambiance functions to which each role has rights.

S

SAML

Security Assertion Markup Language. A authentication protocol based on XML that enables single sign-on capability.

Secondary Program Key

System key that reprograms or resynchronizes the current Primary Program Key (PPK).

Shift Schedule

Day and time constraints applied to staff keys.

Site

Geographical location that consists of one or more buildings.

Special Function Key

System key that is used for advanced lock operations.

Staff

Operators and key holders in your organization.

Staff Access Report

Lists historical information about staff access.

Staff Common Area

Type of access point where general access is configured for staff.

Staff Keys

1) The module where you make keys for staff members. 2) Keys encoded with a staff credential.

Staff Management

The module where you add staff, configure Operators, and manage staff keys.

Suite

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

System Activity Report

Details about the system transaction history.

System Keys

1) The module where you make keys to perform lock or system-level operations. 2) Keys made in the System Keys module.

System Settings

The module where site-wide options, preferences and defaults are specified. Some settings control whether Ambiance features are enabled and how the features operate.

T

Toggle Latch/Unlatch Key

1) System key credential class. 2) System key that is used to enable and/or disable passage mode.

Toggle mode

Feature that alternates the state of a lock to allow/deny access.

U

Unblock Key

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

Unlatch Key

1) System key credential class. 2) System key that enables passage mode (unrestricted access) in the lock.

User Type (Operator profile)

Option selected in staff member profiles that reflects the nature of relationship with the property.

V

VIP

Feature that supports advanced access configurations for licensed properties.

W

workstation

Computer used by Operators to access Ambiance software.

Index

A

Access Management 110

access point

groups 119

mobile-enabled report 278

scheduling 125

types 60

Access Point Audit Report 252

access report, residents/staff/vendors 272

Access schedules 115, 125

access to Ambiance modules 10, 149

account preferences 266

activate staff members 215

adding

access point groups 119

buildings 66

credentials 121

custom Operator roles 151

elevators 104

encoders 135, 139

floors 68

foyer door 82

guest common areas 86

guest registration 170

guest rooms 71, 84

- meeting rooms 98
- notification groups 304
- operators 154
- restricted areas 101
- schedules 113, 115, 117
- staff 190
- staff common areas 92
- suites 77
- additional keys 276
- administrator role 149-150
- archiving historical data 43
- assigning schedules 125
- audit key 247
- audit locks 145, 222
- Audit Report 252
- Aurora, Keyscan 57
- auto-unlatch schedules 113, 125

B

- backing up database 40
- batch creation of access points 60
- Block/Unblock Keys 227
- Block/Unblock Operator access 213
- buildings 66

C

- Cancel Keys 231
- check out guests 187
- client, Ambiance 268
- color codes, access points 143
- common areas, limited access 126
- configuring
 - access to common areas 126

- custom Operator roles [151](#)
- encoders [135](#), [139](#)
- Operators [154](#)
- connector credentials [111](#), [167](#)
- credential class types [110](#), [189](#), [195](#), [198](#), [203](#), [207](#)
- credential classes [110](#), [189](#), [195](#), [198](#), [203](#), [207](#)
- Credential/Access Point Assignment Report [262](#)
- credentials
 - access point groups [119](#)
 - adding [121](#)
 - assignment report [262](#)
 - guest credential class [111](#)
 - learning about [110](#)
 - shift schedules [117](#)
 - staff classes [110](#)
 - system key classes [111](#)
- custom Operator roles [151](#)

D

- database, backing up [40](#)
- date format [21](#)
- deactivating
 - staff [215](#)
- Device Management [132](#)
- device programming [144](#), [300](#)
- Diagnostic Keys [233](#)

E

- Electronic Lockout Keys [235](#), [237](#)
- Elevator Configuration Report [261](#)
- elevators [62](#), [104](#), [261](#)
- ELO Keys [235](#), [237](#)
- Emergency (credential class types/classes) [189](#), [195](#), [198](#), [203](#), [207](#)

- enabling digital keys [278](#)
- enabling mobile keys [56](#)
- encoder firmware update [137](#)
- encoders [132](#), [135](#), [269](#), [324](#), [326](#)
- erase keys [271](#)

F

- Failsafe Keys [36](#)
- failures, reading and encoding keys [271](#)
- firmware update, encoder [137](#)
- floor mapping, elevator [63](#)
- floors, adding [68](#)
- folio settings [44](#)
- foyer door, adding [82](#)
- Front Desk Agent role [149](#)

G

- Grand Master (credential class types/classes) [195](#), [198](#), [203](#), [207](#)
- grouping access points [119](#)
- guest
 - check-out [187](#)
 - keys [182](#)
 - limited use keys [185](#)
 - pre-registration settings [55](#)
 - registrations [170](#)
 - replacing key [180](#)
- guest common areas [61](#)
 - adding [86](#)
- guest rooms
 - importing [74](#)
- guest rooms, adding [71](#), [74](#), [84](#)

H

Home page favorites [264](#)

I

importing

- guest rooms [74](#)

- staff members [161](#), [193](#)

Inhibit Keys [238](#)

invalidate access [227](#), [231](#), [235](#), [237-238](#)

invalidate staff access [212](#)

K

Key Expiration Report [259](#)

key rights [149](#)

Key/User Assignment Report [260](#)

keys

- additional guest keys [182](#)

- Block/Unblock [227](#)

- Cancel Keys [231](#)

- Diagnostic [233](#)

- Electronic Lockout [235](#), [237](#)

- erasing [270-271](#)

- expiration report [259](#)

- Failsafe [36](#)

- Inhibit [238](#)

- invalidate staff access [212](#)

- key mode [276](#)

- Latch/Unlatch [240](#)

- limited use (guests) [185](#)

- Limited Use maximum [35](#)

- mobile [278](#)

- physical [276](#)

- Primary/Secondary Program [242](#)
- reading [270](#)
- replacing guest key [180](#)
- replacing staff key [210](#)
- Resequence [245](#)
- RFID type [55](#)
- Special Function [247](#)
- staff [153](#)
- status [277-278](#), [280](#)
- System [225](#)
- user assignment report [260](#)
- keys, ID reuse [197](#), [201](#), [205](#), [209](#)
- Keyscan Aurora [57](#)
- kiosk, enable for PMS requests [50](#)

L

- language display [21](#), [266](#)
- Latch/Unlatch Keys [240](#)
- LED flash sequence (locks) [330](#)
- LEGIC [56](#), [278](#)
- limited access common areas [126](#)
- limited use guest keys [185](#)
- Limited Use Staff (credential class types/classes) [189](#), [195](#), [198](#), [203](#), [207](#)
- lock programming [146](#), [220](#)
- locks
 - audit [222](#)
 - LED flash sequences [330](#)
 - programming [143](#)
 - troubleshooting [233](#), [330](#)
- logs [336](#)

M

- Maintenance Unit [26](#), [146](#), [220](#), [222](#), [300](#)

Master (credential class types/classes) [195](#), [198](#), [203](#), [207](#)

Matrix [57](#)

meeting rooms, adding [98](#)

Mifare (Classic/Plus) [56](#)

mobile keys [56](#), [278](#)

mobile-enabled access point file download [278](#)

modify guest registration [177](#)

monitory keys [250](#)

N

naming access points [60](#)

navigating modules [264](#)

New Keys [276](#)

notification groups [302](#)

O

online communication [57](#), [247](#), [283](#)

online reporting [316-318](#)

Operator profile [154](#)

Operator Report [258](#)

Operator roles

 custom [151](#)

 predefined [150](#)

Operators

 block/unblock access [213](#)

 configuring [154](#)

 roles [149](#)

P

passage mode [113](#), [240](#)

password

 changing [266](#)

 security settings [24](#)

- PCI-DSS [24](#)
- phone/mobile number validation override [21](#)
- physical keys [276](#)
- PMS
 - authentication [27](#)
 - protocol [47](#)
- possible key holders [197](#), [201](#), [205](#), [209](#)
- pre-registrations (settings) [55](#)
- Primary Program Keys [242](#)
- profile
 - common area access [126](#)
 - Operator [153](#)
 - staff [153](#)
- programming devices [144](#), [300](#)
- programming locks [143](#), [146](#), [220](#)
- Property Builder [60](#)
 - reports [257](#), [261](#)
- Property Configuration Report [257](#)
- protocol, PMS [47](#)

R

- Read Key [270](#)
- registrations
 - check out [187](#)
 - guest [170](#)
 - make additional guest keys [182](#)
 - modify [177](#)
 - VIP [15](#), [23](#)
- remote server backups [40](#)
- replace
 - guest keys [180](#)
 - staff keys [210](#)
- Reports
 - Access Point Audit [252](#)

- Credential/Access Point Assignment [262](#)
- Elevator Configuration Report [261](#)
- Key Expiration Report [259](#)
- Key/User Assignment [260](#)
- mobile-enabled access points [278](#)
- Online Access Point Status [316](#)
- Online Gateway Status [317](#)
- Online Paired Access Point Status [318](#)
- Operator [258](#)
- Property Configuration [257](#)
- Resident/Staff/Vendor Access [272](#)
- Roles (Operator) and Rights [256](#)
- Staff Access [255](#)
- System Activity [253](#)
- Resequence Keys [245](#)
- resident access report [272](#)
- restricted areas, adding [101](#)
- reusing key IDs [197](#), [201](#), [205](#), [209](#)
- RF Pairing Key [247](#)
- RF Unpairing Key [247](#)
- RFID key types [55](#)
- Role Management [149-150](#)
- Roles and Rights Report [256](#)
- Roles, Operator [151](#)

S

- schedules
 - access [115](#)
 - assigning to access points [125](#)
 - auto-unlatch [113](#)
 - shift (staff) [117](#)
- Secondary Program Keys [242](#)
- security settings [24](#)
- shift schedules [117](#)

- single sign-on [31](#)
- site configuration [13](#)
- Site Configurator role [149-150](#)
- Special Function Keys [247](#)
- staff
 - activate [215](#)
 - adding profiles [190](#)
 - automated email [39, 302](#)
 - deactivate [215](#)
 - importing [161, 193](#)
 - invalidate access [212](#)
 - keys [153](#)
 - making keys [195, 198, 203, 207](#)
 - replacing key [210](#)
 - shift schedules [117](#)
- Staff (credential class types/classes) [189](#)
- Staff Access Report [255](#)
- staff common areas
 - adding [92](#)
- staff key validation [19, 53, 155](#)
- staff key validators [139](#)
- Staff Management [153](#)
- Staff Manager role [149](#)
- staff/vendor access report [272](#)
- status, keys [277, 280](#)
- suites, adding [77](#)
- suspend access [227](#)
- System Activity Report [253](#)
- System Keys [225](#)
- system rights [149](#)
- System Settings [15](#)

T

- test key files [217](#)

time drift [143](#)
time format [21](#)
time zone [21](#)
types, access point [60](#)

U

Ultralight C [56](#)
update Ambiance Client [268](#)
user preferences [266](#)

V

validation override, phone/mobile number [21](#)
validation, staff key [19](#), [53](#)
VIP guest registrations [15](#), [23](#)

W

workflow, site configuration [13](#)
workstation, Ambiance [268](#)



www.dormakaba.com

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
Canada
T: +1 877 468-3555

www.dormakaba.com