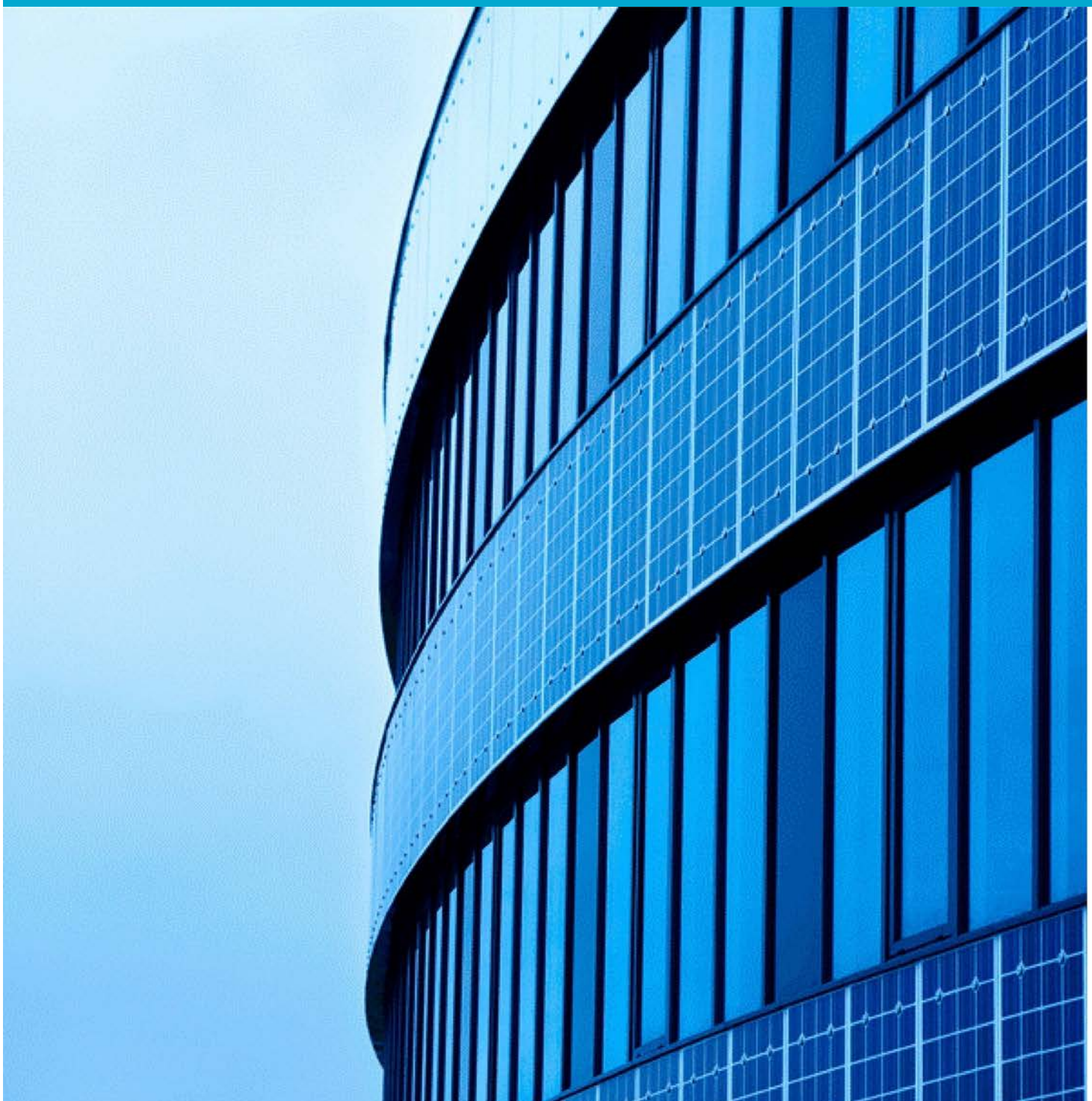
Incedo™ Open

Operator Guide

ASSA ABLOY
Opening Solutions

assaabloy.com

Experience a safer
and more open world



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

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

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

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

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

Program version:
Main document number: S005624
Date published: 2021-09-09
Language: en-GB

1 General Information

1.1 Introduction

Incedo™ Open is a cloud based access control system. A large range of both offline and online electronic access control (EAC) components, such as electric strikes and readers, can be connected and managed.

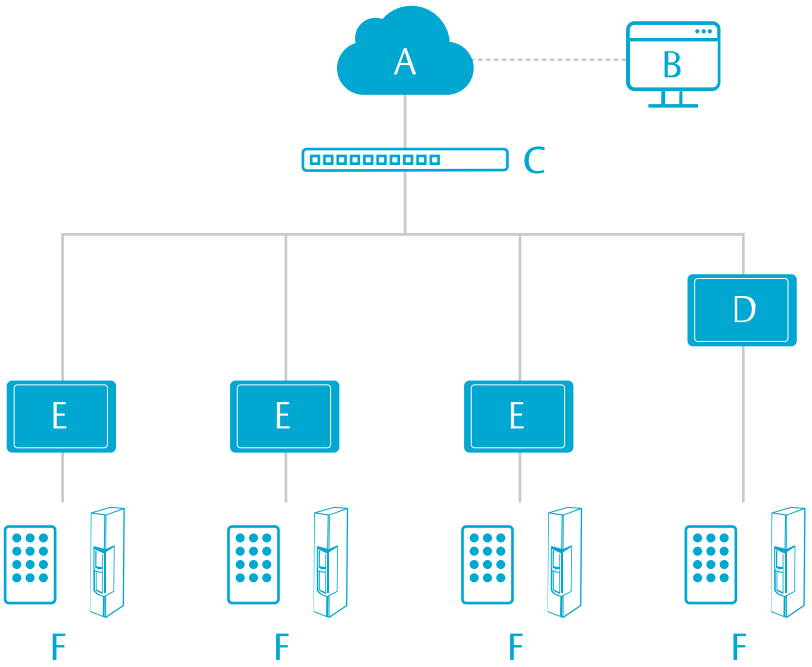
The Incedo™ Open web application allows operators to plan and configure the hardware, set up schedules, manage access rights, review logs, manage credentials, and more.

1.2 About this Manual

This manual describes Incedo™ Open, and how to set up, configure, and perform daily tasks in Incedo™ Open.

1.3 System Overview

Two different controller units are used to integrate online EAC components with the Incedo™ Open cloud service: Controllers (InControl 3270) and Device converters (ToConnect 3270). The InControl 3270 Controller also includes an integrated Device converter.



A) The cloud service

B) Incedo™ Open web application

C) Network router and firewall

D) Controller

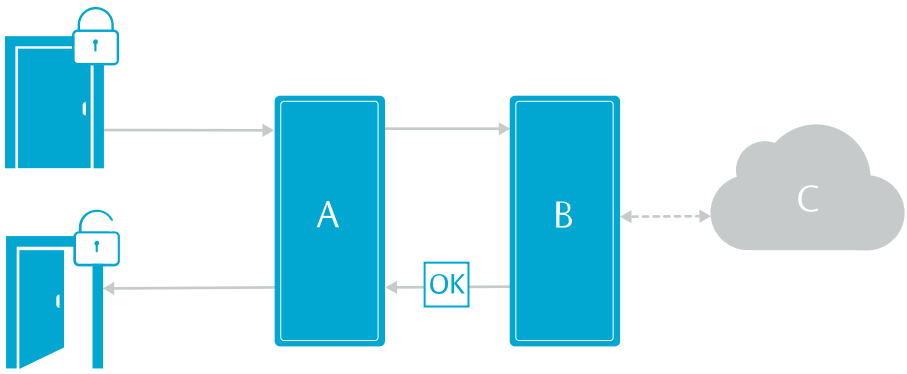
E) Device converter

F) EAC components

Device converters (E) and IP devices (for example WellCom) communicate with their parent Controller (D) over a local network. Controllers communicate with the cloud service (A) over an internet connection. EAC components (F) can be connected to either controller unit. The web application (B) is used to set up and manage EAC systems.

1.4 Door Opening Process

The following describes the basic door opening process for online locks.



A) Device converter

B) Controller

C) The Incedo™ Open cloud service

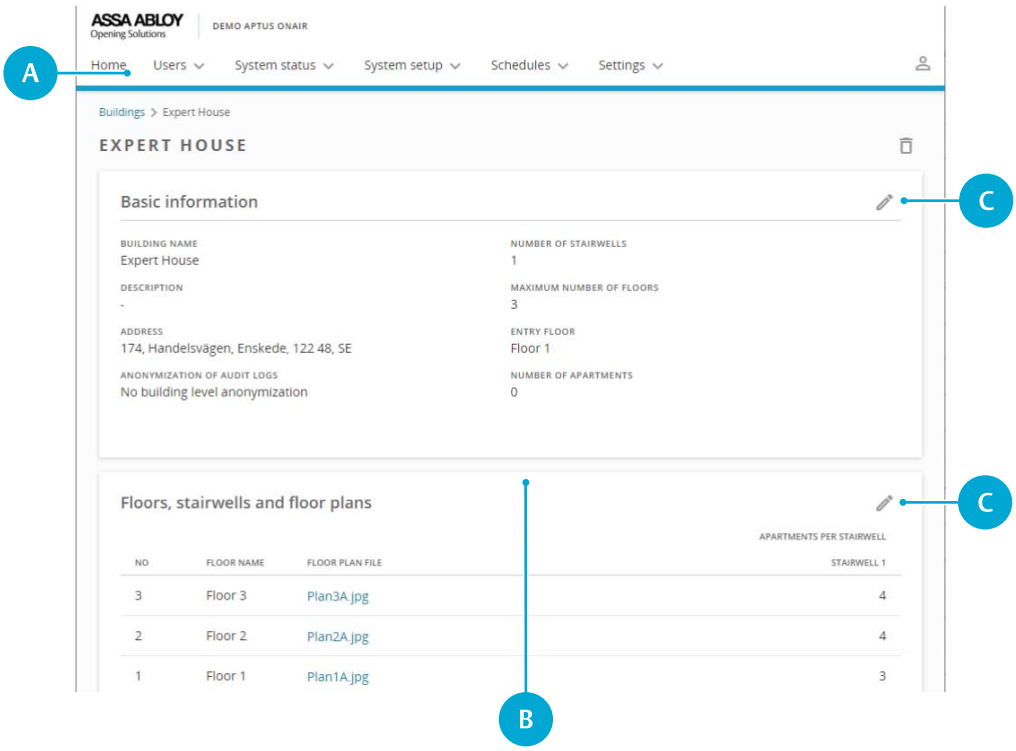
When a credential is presented to a reader, the credential number is sent to the Controller (B) via the Device converter (A). An access decision is made in the Controller based on the credential's access profiles. If access is granted, an open lock command is sent to the Device converter, to unlock the door.

The Controller regularly contacts the cloud service (C) for updates on access rights and configurations.

1.5 Web Application Overview

The user interface of the web application consists of a main menu, a main application area and context dependent menus or edit icons.

The different functions of the application are accessed from the main menu (A). Most items can be edited and viewed from menus or icons (C) in the main application area (B).



A) Main menu

B) Main application area

C) Context dependent menu or edit icon

1.6 System Requirements

System requirements for the Incedo™ Open web application:

- Google Chrome version 50 or higher
- Windows 8 or higher
- Internet connection

2 Quick Start

A typical Incedo™ Open system installation could be outlined as follows:

1. A new system is created by ASSA ABLOY Opening Solutions and a system owner is assigned. An email with instructions on how to proceed is sent to the new system owner.

   NOTE!
   Make sure that the web application is opened in a supported web browser. Check Section 1.6 *"System Requirements"*, page 9 for a list of supported browsers.

2. The system owner logs in and sets up different roles, adds operators such as system admins, installers, receptionists, and more. See Section 5.1 *"Adding a Role"*, page 28 and Section 5.2 *"Adding an Operator"*, page 28.

3. The system owner selects whether PULSE encryption keys are unique per building or shared by all buildings in the system. See Section 3.8.2 *"PULSE Encryption Keys"*, page 21.

   NOTE!
   This setting can only be changed while no building has been added to the system.

4. A new building with one or several floors is added. See Section 6.2 *"Adding a Building"*, page 31. If administrating a residential building, also add apartments and leases. See Section 6.3 *"Adding an Apartment"*, page 32 and Section 5.4 *"Adding a Lease"*, page 29.

5. Door types are defined, to be used later when doors are added to the building. See Section 6.5.1.1 *"Adding a Door Type"*, page 33.

6. Controller units are added. Each Controller unit must have the latest firmware version installed. See Section 6.5.2 *"Adding a Controller"*, page 34 and Section 9.3 *"Upgrading Controller Firmware"*, page 63.

7. Doors are added. See Section 6.5.3.1 *"Adding a Door"*, page 35.

8. The added components are ordered from ASSA ABLOY Opening Solutions or a reseller, and installed on the premises. For more information on how to install EAC hardware, see Incedo™ Open: InControl 3270 and ToConnect 3270 Installation Guide.

9. The installed online hardware devices are marked as mounted in the Incedo™ Open web application by mapping their unique MAC Addresses to the doors and controller units in the hardware planner. See Section 6.6.1 *"Mounting a Controller"*, page 36, and Section 6.6.2 *"Mounting a Door or Device"*, page 37.

10. Calendars and hardware schedules are defined, to be used later when doors are configured. See Section 7.6 *"Adding a Calendar"*, page 57, Section 7.3 *"Adding an Operational Schedule"*, page 56, and Section 7.4 *"Adding a Security Schedule"*, page 56.

11. The mounted components are configured using different schedules, time-settings, and other device-specific configurations. See Section 6.7.1 *"Configuring a Door"*, page 39.

12. Access areas, offline door groups, and access schedules are defined. See Section 6.8.1 *"Adding an Access Area"*, page 41, Section 6.8.2 *"Adding an Offline Door group"*, page 41, Section 7.1 *"Adding an Access Schedule"*, page 55, and Section 7.2 *"Adding an Offline Access Schedule"*, page 55.

13. Access areas and offline door groups are combined with schedules into access profiles. See Section 6.4 *"Adding an Access Profile"*, page 32.

14. Credential types might have to be added before credentials can be handled in the system. See Section 6.13 *"Adding a Credential Type"*, page 53.

15. Users can be added, assigned access profiles, and handed out credentials. For more information, see Section 5.3 *"Adding a User"*, page 28, and Section 8.1 *"Creating and Handing Out a Credential"*, page 59.

2.1 Quick Start: External Alarm

This quick start outlines how to control and manage an external alarm zone from an already configured Incedo™ Open system.

1) Plan the alarm area doors and I/O to line up with the external alarm zone.

   For more information, see Section 3.9.2 *"Alarm Areas"*, page 24 and Section 4.3 *"Planning Alarm Area for an External Alarm Zone"*, page 27.

2) Add or edit one or several alarm schedules.

   The schedules are used for alarm related functions such as scheduled alarm manoeuvres, delayed arming, and alarm privileges. For more information, see Section 7.5 *"Adding an Alarm Schedule"*, page 57.

3) Add the alarm area.

   For more information, see Section 6.9.1 *"Adding or Editing an Alarm Area"*, page 42.

4) Configure the alarm area.

   For more information, see Section 6.9.2 *"Configuring an Alarm Area"*, page 43.

   Ensure that the settings correspond to the external alarm's configuration.

5) Mount the alarm area.

   This will map the external alarm commmunication functions to hardware outputs and inputs on a controller unit (InControl 3270 or ToConnect 3270). For more information, see Section 6.9.3 *"Mounting an Alarm Area"*, page 45.

6) Connect the external alarm to the selected controller unit.

   For more information, see Incedo™ Open: InControl 3270 and ToConnect 3270 User Guide.

7) Handle user privileges for the new alarm area.

   Add alarm privileges to new or existing access profiles. For more information, see Section 6.4 *"Adding an Access Profile"*, page 32.

8) The alarm area is now ready for daily tasks.

   - To monitor, arm and disarm alarm areas remotely, see Section 9.4 *"Controlling Alarms"*, page 64.
   - To arm, disarm, or delay arming from a reader, see Section 11.3 *"Arming or Disarming an Alarm Area From Reader"*, page 72.

For more information, see Section 3.9.1 *"External Alarms"*, page 23.

2.2 Quick Start: PULSE

This is a general workflow on how to get started with PULSE. The process involves installing the AADC mobile application, setting up a PULSE updater, and adding PULSE locks.

1) Go to **Settings » Credential types** and make sure a credential type of the PULSE format is available. See Section 6.13 *"Adding a Credential Type"*, page 53.

2) Install and log in to the ASSA ABLOY Device Configurator (AADC) mobile application.

   See Section 6.10.1 *"Installing ASSA ABLOY Device Configurator"*, page 46.

3) Set up at least one PULSE updater (WellCom or Desktop Updater).

   - Desktop Updater (DU): first add the DU to a building, then install the Desktop Updater PC application and configure the DU.

     See Section 6.10.2 *"Adding a Desktop Updater"*, page 47 and Section 6.10.3 *"Installing a Desktop Updater"*, page 48.

   - WellCom: configure the WellCom unit. See Section 6.10.4 *"Configuring WellCom 4707 as a PULSE Updater"*, page 51.

4) Add and configure PULSE locks to the EAC system.

   a) Add offline doors with PULSE locks. See Section 6.5.1.1 *"Adding a Door Type"*, page 33 and Section 6.5.3.1 *"Adding a Door"*, page 35.

   b) Configure the PULSE locks. See Section 6.7.1 *"Configuring a Door"*, page 39.

   c) Add the PULSE locks to offline door groups and access areas.

      Offline access schedules do not apply to PULSE locks. For more information, see Section 3.4 *"Access Concepts"*, page 14.

   d) Program the PULSE locks. See Section 6.11 *"Programming a PULSE Lock"*, page 52.

The system is now ready for performing daily tasks with PULSE keys and locks. See Section 8.1 *"Creating and Handing Out a Credential"*, page 59, Section 8.2 *"Handing In a Credential"*, page 59, Section 8.3 *"Blocking a Credential"*, page 60, and Section 9.6 *"PULSE: Audit Logs"*, page 65.

3 Concepts And Features

3.1 Buildings, Floors and Doors

To organise the online and offline components of a system, Incedo™ Open uses a hierarchy of buildings, floors and doors.

Building A building is a real estate object with an official address. The official addresses are taken from OpenStreetMap (openstreetmap.org).

Floor A building contains at least one floor, with doors between areas. Floors can be based on floor plan drawings uploaded as image files to the web application.

Door A door may contain access control components, such as a reader and an electric strike. Doors are further divided into online doors and offline doors.

Door type A door type is a template for a door setup. Doors are linked to the door type by a door name. Any edit of a door type, or of a specific door, will convert the affected door to a custom door.

Custom door A custom door is a door that is not associated with any door type.

Online door Access decisions for an online door are handled by the parent Controller , which is in regular contact with the Incedo™ Open cloud service.

Offline door Access decisions are handled by the door, based on the information stored in the offline credentials. An updater is used to update the credentials.

Door side Door sides are used when defining access areas for online doors and some offline doors.
Door sides are used when defining access areas, and where applicable, alarm areas for online doors and some offline doors.

To add a building and floors, see Section 6.2 *"Adding a Building"*, page 31. To add doors, see Section 6.5.3.1 *"Adding a Door"*, page 35

3.2 Apartments and Leases

In addition to the concepts in Section 3.4 *"Access Concepts"*, page 14, apartments and leases are used to administer residential buildings. Apartments and leases are designed to aid the administration of standardised access rights, typically with a set end date. However, the features also aid administration of apartments in a broader sense, by listing email, phone numbers, and other data of residents.

Apartment An apartment is added to a specific stairwell and floor of a building, and can be associated with access profiles to control access to specific doors and areas that are part of the EAC system. The access profiles may be unique for each apartment, for example apartment door and storage, or be of a more general type, for example entrance and common areas. Even mechanical keys (for example padlock keys) that are not part of the EAC system can be added with an ID.

Lease A lease is based on an apartment, and grant users (residents) the access rights associated with the apartment, for the specified lease period. Additional access profiles can be added for the lease.

Stairwell A stairwell is used to organise the apartments of a building. A building contains at least one stairwell.

For more information, see Section 6.3 *"Adding an Apartment"*, page 32 and Section 5.4 *"Adding a Lease"*, page 29.

3.3 Users and Roles

There are two types of users in the Incedo™ Open web application: **users** and **operators**.

User A user can be assigned access profiles, leases and credentials. Users can be assigned access profiles and credentials.

Operator An operator have log-in rights to the web application, and is assigned to administer parts of Incedo™ Open, or the system as a whole.

Role A role defines the set of read and write privileges for an operator.

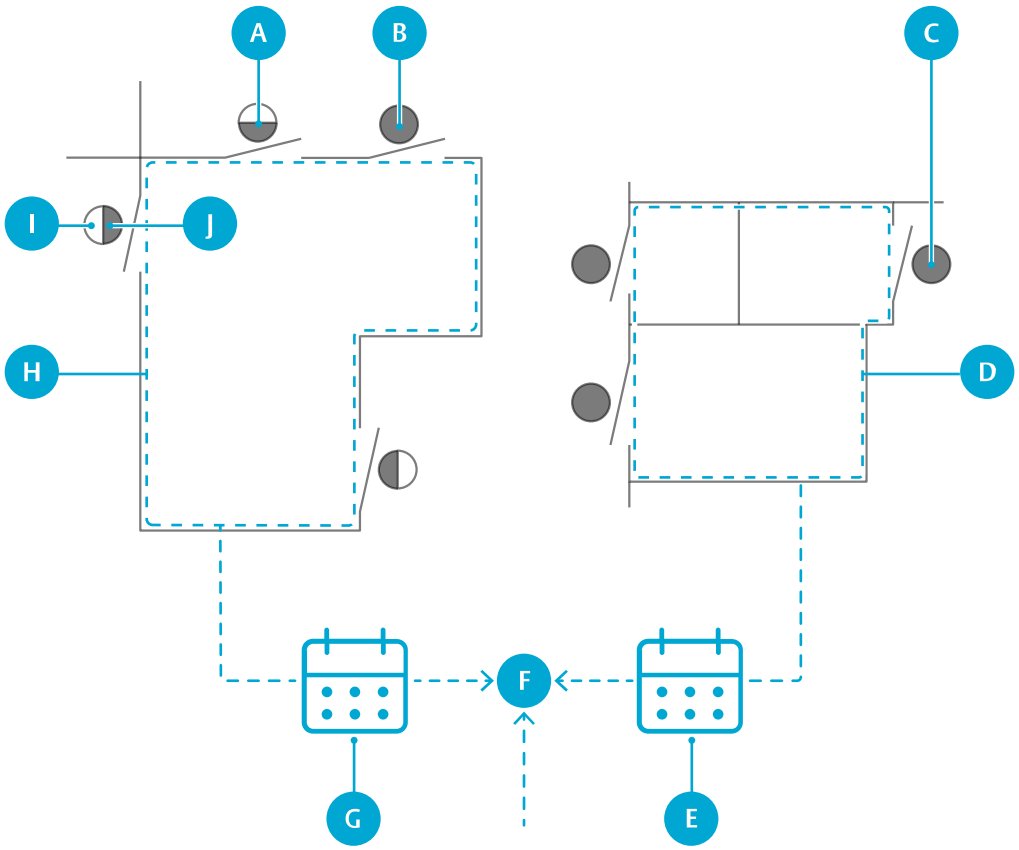
System owner The system owner is a special role for the first operator's account of a system. It has the most complete set of privileges. There can only be one system owner, to change the system owner, contact ASSA ABLOY Opening Solutions.

HINT!
Using roles, an installer could be limited to only read and write in the hardware mounting view, and a receptionist to the items available from the home view, while a system administrator could have full access rights.

For more information, see Section 5.3 *"Adding a User"*, page 28, Section 5.2 *"Adding an Operator"*, page 28, and Section 5.1 *"Adding a Role"*, page 28.

3.4 Access Concepts

Door opening decisions in Incedo™ Open depend on a collection of access concepts described below. The figure shows how these concepts are connected:



A) Online door

B) Offline door (in access area)

C) Offline door (in offline door group)

D) Offline door group

E) Offline access schedule

F) Access profile, containing one or several access areas and offline door groups

G) Online access schedule

H) Access area

I) Online door side leading into access area

J) Online door side leading out of access area

Access concepts in detail

Access area An access area (H) is a section of a floor enclosed by online doors (A) and offline doors (B) leading into it. Normally, credentials are required to enter. For more information, see Section 6.8.1 *"Adding an Access Area"*, page 41.

Offline door group An offline door group (D) can only be used with offline doors (C). It may include doors from the same or different floors of a building, or even different buildings, which allows defining door groups with specific access rights in distributed areas. As the memory size is limited in locks, the use of door groups enables access to an unlimited number of locks by using a single memory slot for credentials in the lock. For online doors, these memory limitations do not apply. For more information, see Section 6.8.2 *"Adding an Offline Door group"*, page 41.

Online access schedule An online access schedule (G) is a weekly schedule to enable or disable access rights to access areas (H) based on time slots. Online access schedules are based on calendars. Special days defined in the selected calendar are handled separately. For more information, see Section 7.1 *"Adding an Access Schedule"*, page 55.

Offline access schedule An offline access schedule (E) is a weekly schedule to enable or disable access rights to offline door groups (D) based on time slots. Two time slots per day are allowed, and each Incedo™ Open system is limited to seven offline access schedules. For more information, see Section 7.2 *"Adding an Offline Access Schedule"*, page 55.

Exception day A day in a calendar that is handled separately in online access schedules. For example, this could be used to set special access hours for a holiday, such as New Year's Eve, or any other exception day.

Revalidation period A revalidation period is the time between an offline credential's update, and the time when the validity expires. It is set for the entire system.
A new period is started when a non-blocked offline credential is presented to an updater. For more information, see Section 10.2 *"Setting an Offline Revalidation Period"*, page 67.

Access profile An access profile (F) holds a combination of access areas (H), offline door groups (D), and online (G) and offline access (E) schedules. Online access is granted based on an access area within the time period specified in the selected access schedule. Offline access is granted based on offline door group membership or access area membership within the time period specified in the selected access schedules. Offline credentials are further restricted by the credential re-validation period. Users are granted access rights based on their assigned access profiles. For more information, see Section 6.4 *"Adding an Access Profile"*, page 32.

The offline access concepts are based on OSS Mifare Desfire specification 1.00, with some additional restrictions. For more technical information on how the online concepts are applied when a credential is presented to a reader, see Section 1.4 *"Door Opening Process"*, page 8.

When to Use Access Areas or Offline Door Groups

Online doors can only be included in access areas, and offline doors can be included in both access areas and offline door groups.

As offline door groups only require one memory slot to store the group ID for an unlimited amount of doors, it is more efficient compared to access areas that require one memory slot (door ID) per included offline door.

On the other hand, adding or removing a lock from an offline door group requires physical access to the lock for reprogramming. Changes of a credential's access area containing an offline lock only requires a credential update.

Offline credentials are limited in memory size. The limited memory size improves the read and write speed when credentials are presented to a reader.

3.5 Calendars and Schedules

Schedules, based on calendars, are used to control access during specific time slots in Incedo™ Open. The time slot function depends on the schedule type and application. Time slots are either on or off.

Calendars use standard weeks, and then exception days such as holidays are defined per calendar year. When planning for the next year, the dates of the exception days must be manually added for the new calendar year. Editing a calendar affects any schedule based on it.

Schedule type	Time slot function	Description
Online access schedule	Always access	Enables or disables access rights to access areas. Exception days are handled separately. Paired with access areas in access profiles.
Offline access schedule	Always access	Enables or disables access rights to offline door groups. Paired with offline door groups and access areas in access profiles. Limitations: No exception days. Two time slots per day, and seven offline access schedules are allowed per Incedo™ Open system. **NOTE!** PULSE locks do not support schedules.
Operational schedule	Always on (function active)	Defines when a hardware function is on or off. Examples include door configurations such as unlocked schedules and exit button schedules.
Security schedule	As selected	Sets the security level for a door side. Card + PIN is default. Different security levels can be used for different time slots. Available levels for time slots: Card, Unlock code, Card or unlock code, Card + PIN or unlock code, No access. The two sides of a door can have different security levels. For example, it is common to have a different security level to enter an access area than to leave the same area.
Alarm schedule	Active (function on)	Defines when an external alarm function is active. Alarm schedules are used to schedule the arming of alarm areas, as well as to schedule other functions.

For more information, see, Section 7.1 *"Adding an Access Schedule"*, page 55, Section 7.2 *"Adding an Offline Access Schedule"*, page 55, Section 7.3 *"Adding an*

Operational Schedule", page 56, Section 7.4 *"Adding a Security Schedule"*, page 56, Section 7.5 *"Adding an Alarm Schedule"*, page 57, and Section 7.6 *"Adding a Calendar"*, page 57.

3.6 Credentials

Credentials are used for authentication, that is, to verify the identity of a user. Credentials can be a card or a key, used with or without a secret PIN, or a user code.

Credential Formats

Different credential types might require different credential formats to ensure correct readings in readers and updaters.

For more information on the correct credential formats for the installed set of readers and credential types, refer to the device's documentation, or contact your ASSA ABLOY Opening Solutions representative.

For more information, see Section 6.13 *"Adding a Credential Type"*, page 53.

Credential Handling

Credentials are managed with the following operations:

Create credential — The **create credential** operation is used to create a credential of a specific type for a user. The custody of the credential is either set to handed out out or handed in.

Hand in — The **hand in** operation is the act of returning handed out credentials. The user is no longer associated with the handed in credentials. Credentials can then be handed out to another user.

Block — The **block** operation is the act of blocking credentials in the system. This is useful if credentials are lost. A blocked PULSE key cannot be reused.

For more information, see , Section 8.1 *"Creating and Handing Out a Credential"*, page 59, Section 8.2 *"Handing In a Credential"*, page 59, and Section 8.3 *"Blocking a Credential"*, page 60.

3.7 Anonymisation Features and Data Retention

Incedo™ Open offers anonymisation features and fixed-term data retention to address user integrity concerns. Anonymisation can be set on four different levels, and if any applies to a logging event, user names and credential numbers are omitted from the log entry.

Anonymisation level	Feature(s)
User	• Anonymises credential number and name in audit logs per user for all doors, including doors marked as sensitive. Used when an apartment resident requests to be anonymised on all doors. See Section 5.3 *"Adding a User"*, page 28. • Allows each user to be excluded from audit logs for doors marked as sensitive. The information is not stored and can therefor not be retrieved in any way.
Door	Allows doors to be marked as sensitive. This function is applied regardless of security level (for example card and PIN). For GDPR compliance reasons, this feature is strongly recommended on apartment doors. See Section 6.7.1 *"Configuring a Door"*, page 39.
Building	Anonymises names and credential numbers for events with one factor authentication. One factor authentication is when one item is required for access (for example a card or a user code). Two factor authentication is when two items are required for access, for example a card and a PIN code. Applies to audit logs for an entire building. See Section 6.2 *"Adding a Building"*, page 31.
System	Anonymises credential numbers and names in audit log entries older than a set number of days. See Section 10.1 *"Configuring System Settings for Logs"*, page 66.

Data in logs (audit, operator, system, incident / monitoring) is retained for a set number of days. Log entries older than the set number of days will be deleted during night. If the number of days is changed, log entries older than the new value is deleted as soon as possible. As PULSE locks lack clocks, data retention in PULSE locks is managed by a limit on the allowed number of stored logs.

Data retention feature	Description
Deletion of log entries in • audit logs • operator logs • system logs and incident / monitoring logs	All log entries older than a set number of days are deleted. The number of days is set separately for different types of logs. See Section 10.1 *"Configuring System Settings for Logs"*, page 66.
Audit logs in PULSE locks	A PULSE lock is allowed to store a set number of audit log entries. The number of log entries is set separately for sensitive doors and normal doors respectively. These settings do not affect manually entered values for individual doors. See Section 10.1 *"Configuring System Settings for Logs"*, page 66.
Handling audit logs when deleting users	The user's audit logs are handled differently for sensitive doors and normal doors. See Section 10.1 *"Configuring System Settings for Logs"*, page 66.

3.8 PULSE Concepts

3.8.1 Understanding PULSE

PULSE is an offline locking system fully integrated in Incedo™ Open.

A PULSE locking system consists of PULSE keys, PULSE locks, readers, and updaters that are configured with the same set of encryption keys.

The default setting is that each building has its own unique encryption key. There is also an option where all buildings within an Incedo™ Open system share the same encryption key. This option must be selected before the first building is created and cannot be changed after a building has been added to the system. See Section 3.8.2 *"PULSE Encryption Keys"*, page 21.

PULSE technology
Access decisions are handled by the PULSE lock, based on the information stored in the PULSE key.

The energy required for access control and unlocking a lock is generated from the movement when inserting the PULSE key. This eliminates the need for batteries in locks and keys.

PULSE key information flow
A PULSE key stores the following information:

- Lock IDs for the locks it has access to
- Group IDs for the offline door groups it has access to
- Audit logs for the key and the locks it has interacted with.
- A blocklist, a timestamped list of blocked offline credentials

When a PULSE key is inserted in a PULSE lock, the blocklist is transferred to the lock if it has a more recent timestamp than the lock. The lock IDs and group IDs in the key are matched against the corresponding information in the lock.

If there is a match in lock IDs or group IDs, and if the lock does not consider the PULSE key blocked or to have an expired validity, access is granted. The interaction between the key and the lock is added to the audit log.

Lock IDs in PULSE keys are part of Access areas, and Group IDs in groups are part of offline door groups.

PULSE key blocking process
When an operator blocks a PULSE key credential in the system, the credential is still valid. To complete the blocking process, the affected PULSE key and the affected PULSE locks must be updated. The PULSE key is updated by any PULSE updater. To update the locks, non-blocked PULSE keys must be updated and propagate the new blocklist to the relevant locks and then be updated again to transfer their audit logs to the system.

Capacity
One Incedo Open system can contain an unlimited number of PULSE locking systems.

Each PULSE locking system can handle up to 65535 PULSE locks and and up to 65535 Offline door groups.

Each PULSE key can handle up to 10 different PULSE locking systems. For each PULSE locking system, the PULSE key can handle up to a total of 255 PULSE locks and Offline door

groups. For example, if a key has access to 240 individual PULSE locks, it can also have access to 15 Offline door groups.

3.8.2 PULSE Encryption Keys

For Incedo Open, there are are two options for PULSE encryption keys. Either there is one unique key for each building, or there is one key for all the buildings in the Incedo Open system. A number of issues are handled differently between the two options.

NOTE!
The encryption key setting can only be changed while no building has been added to the system.

Issue	One encryption key per building	One encryption key for all buildings in the Incedo Open system
Blocklist	One credential blocklist per building. Maximum 80 blocked credentials per building.	One credential blocklist for all buildings. Maxmimum 80 blocked credentials in total.
PULSE updaters	Readers and entry phones can only update accesses for the building they are located in. Each Desktop Updater can be used for up to 10 buildings, and must be connected to each of the buildings.	Readers and entry phones can update accesses for all buildings. All Desktop Updaters connected to the system can update accesses for all buildings.
Access to offline door groups	When a PULSE key is updated, the following offline door groups are written to the key: the ones that contain at least one door located in a building belonging to the same PULSE locking system as the key.	When a PULSE key is updated, all offline door groups that exist in the Incedo Open system are written to the key.

For more information, see Section 6.1 *"Selecting PULSE Encryption Key Mode"*, page 31.

3.8.3 PULSE Updater Devices

To introduce changes in the access rights of a PULSE locking system, the keys in the system must be updated. Changes include handing out and handing in keys as well as changes in access profiles containing PULSE locks. PULSE keys are updated with a PULSE updater device.

For each PULSE locking system, at least one PULSE updater must be available in the Incedo™ Open web application.

All PULSE updater devices must be configured using the AADC mobile application.

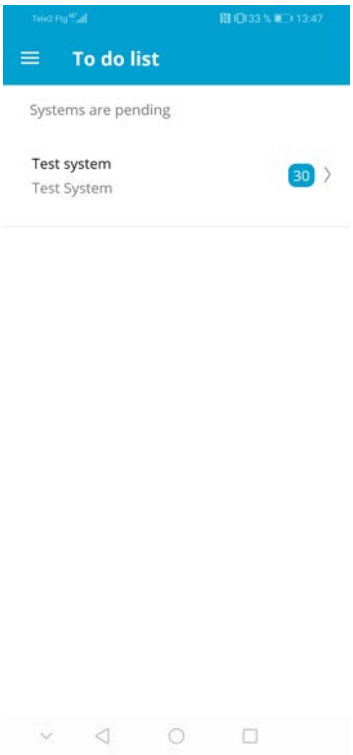
PULSE Updater Device	Information
Desktop Updater	A USB device that requires a PC running the Desktop Updater PC application. Can handle more than one PULSE locking system and up to 10 buildings in total.
WellCom unit	Can handle one PULSE locking system.

Reading key numbers
When the Desktop Updater detects a key that is not found in the system, the updater automatically reads and copies the credential number to a text field in the PC application. This streamlines the handing out procedure of a PULSE key. Alternatively, automatic copying can be disabled or set to be applied for all PULSE keys, handed out or not.

For more information, see Section 2.2 *"Quick Start: PULSE"*, page 12 and Section 6.10 *"PULSE Installation"*, page 46.

3.8.4 ASSA ABLOY Device Configurator

The ASSA ABLOY Device Configurator (AADC) is an Android mobile application used to configure PULSE locks and PULSE updaters (Desktop Updaters, WellCom units). The application lists the available EAC systems and components.



A PULSE lock is configured using a programming device (PPD200/PPD201), a USB PULSE key adapter for Android devices. A Desktop Updater or a WellCom unit is configured over NFC by placing the Android device on top of it. AADC also includes troubleshooting functions for sharing logs with ASSA ALBOY support, and reading PULSE lock serial numbers.

Requirements:

- NFC-enabled Android device* (Android 5.0 Lollipop or later)
- Micro-USB port or USB-C to Micro-USB adapter

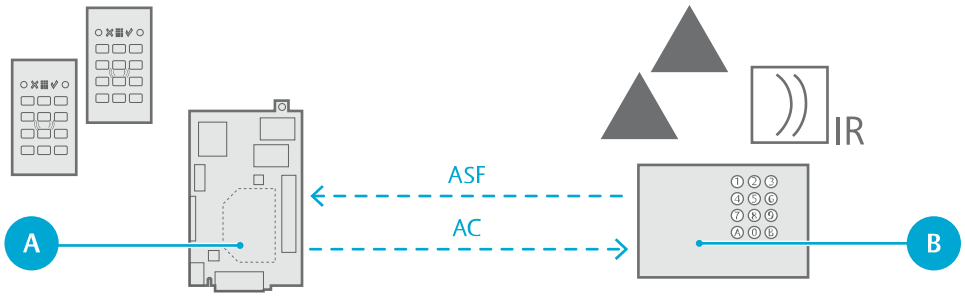
*Apple devices are not supported.

To install the mobile application, see Section 6.10.1 *"Installing ASSA ABLOY Device Configurator"*, page 46.

3.9 External Alarm Concepts

3.9.1 External Alarms

Alarm systems are usually set up in zones, where each zone contains the sensors for a part of a building or property. In Incedo™ Open, external alarms are controlled and monitored zone-by-zone.



A) Incedo™ Open controller unit

B) External alarm panel

Users with alarm privileges can arm or disarm an external alarm zone from designated readers. Operators with sufficient privileges can monitor, arm, or disarm the external alarm zone from the web application.

For each external alarm zone to control, a corresponding alarm area is set up in the web application. The alarm area is defined by the door sides leading into it, and is used to request the arming or disarming of the external alarm zone. Alarm areas follow the actual statuses of their associated external alarm zones.

Interactions with the external alarm zone

When an alarm area is armed, a pre-alarm period starts. The doors leading into the alarm area are blocked, but can still be exited. Optionally, people can be alerted by devices such as buzzers controlled by pre-alarm relays. At the end of the pre-alarm period, an arming request is sent, and doors are blocked from both sides. If an alarm status feedback signal is received from the external alarm, the status is changed to armed.

When an alarm area is disarmed, the disarming request for the external alarm zone is sent without delay. Once the external alarm zone is disarmed, the status is changed to disarmed. The doors are unblocked.

For more information, see Section 3.9.2 *"Alarm Areas"*, page 24, and Section 2.1 *"Quick Start: External Alarm"*, page 11.

3.9.2 Alarm Areas

An alarm area is used to control an external alarm zone, and is defined by the doors leading into it. The alarm area is the basis for scheduling, alarm privileges, configurations, and exceptions for the external alarm zone. Incedo™ Open can request the arming or disarming of an external alarm zone, but the alarm area status follows the actual status of the external alarm zone.

Communication

Incedo™ Open uses the following inputs and outputs to communicate with each external alarm zone:

Alarm status feedback (ASF)	An analogue input set up to receive alarm zone status signals from the external alarm zone. Controls the status of the alarm area.
Alarm control relay (AC)	A relay used to send arming and disarming requests to the external alarm zone. Additional AC relays can be added to control other functions, such as light fixtures.

Pre-alarm relay (PA) Optional. A relay that is activated during the pre-alarm period. Can for example be used to drive sirens and strobe lights.

Status

An alarm area can have one of the following statuses:

Status	I/O	Alarm area behaviour
Disarmed	ASF: Inactive AC: Inactive PA: Inactive	The doors of the alarm area function normally.
Pre-alarm	ASF: Inactive AC: Inactive PA: Active	The readers leading into the alarm area are typically blocked during the pre-alarm period. Normally, the alarm area can be exited. When the pre-alarm period expires, an arming request is made.
Arming*	ASF: Inactive AC: Active PA: Inactive	The doors of the alarm area are blocked from both sides. Exceptions for individual doors can be configured for users with alarm privileges. The ASF input is expected to activate. If the ASF is not given within the configured timeout period, the request is aborted and the status is returned to disarmed.
Armed	ASF: Active AC: Active PA: Inactive	The doors of the alarm area are blocked from both sides. Exceptions for individual doors can be configured for users with alarm privileges.
Disarming*	ASF: Active AC: Inactive PA: Inactive	The doors of the alarm area are blocked from both sides. Exceptions for individual doors can be configured for users with alarm privileges. The ASF input is expected to deactivate. If the ASF does not deactivate within the configured timeout period, the status is returned to armed.

*When arming or disarming an alarm zone directly from the external alarm, arming or disarming statuses will not be set for the alarm area.

For more information, see Section 2.1 *"Quick Start: External Alarm"*, page 11 and Section 6.9.3 *"Mounting an Alarm Area"*, page 45.

4 Planning Strategies

When planning a new system, it is important to recognise the needs of its intended users. The size and door count of a building, the distribution of online and offline doors, special security considerations for particular doors, and the overall security level are all factors to consider.

For more information, see Section 4.1 *"Online and Offline Components"*, page 26 and Section 4.2 *"Online System Design"*, page 26.

4.1 Online and Offline Components

Incedo™ Open can combine online and offline components on the same platform. Online components can be accessed regularly via Controllers (InControl 3270), and system changes such as blocked credentials and new access rights can be rolled out in seconds.

Offline components, on the other hand, have no direct connection to the cloud service. Changes in offline access rights must be enforced by scanning credentials in updaters, or by reprogramming doors. Offline blocklists can be slowly propagated to locks through other user's credentials, or by physically walking to the lock with updated credentials. Offline locks offer a simpler physical installation, with zero cabling needs.

Doors to be accessed a couple of times a day by a few users, with infrequent changes in access rights, may benefit from the easier installation offered by offline locks. Frequently used doors for multiple users are typically fitted with online door components.

A well designed system brings out the best of both worlds, combining online and offline components.

NOTE!

Offline Aperio locks can be opened by blocked credentials until the revalidation period has passed, unless the lock has an updated blocklist.

PULSE locks can be opened by blocked credentials until the lock is updated with a blocklist containing the credential.

4.2 Online System Design

To optimise an online Incedo™ Open system for a specific building and use case, several factors must be considered. The following concepts are central when designing a system.

Distribution of controller units

At least one Controller (InControl 3270) must be added per building, and each Controller can serve up to 16 Device converters (ToConnect 3270). Doors with online components include a Device converter in the web application.

Since the Controller includes a Device converter, one door per Controller can be directly connected. This can be convenient when a Controller is placed close to a door.

Network communication

All communication between Device converters, IP devices, and their parent Controllers is handled on local networks. Controllers also require Internet access to communicate with the cloud service. If the cloud service is unavailable but the local network is intact, a Controller can still handle access decisions for its connected Device converters.

No special attention is needed when assigning IP-addresses, as controller units are identified using unique MAC addresses. IP devices can either be identified by the MAC address, or a local IP address assigned by a local network DHCP server. It may be required to enter the unique MAC addresses of all equipment in the DHCP server, to assign fixed IP

addresses instead of the dynamic IP addresses assigned by default. Contact the local network owner or administrator to ensure correct configuration of the network parameters.

Cat5e (or higher) unshielded twisted-pair (UTP) cables are recommended to connect the network equipment.

Backup power

By installing uninterruptable power supply (UPS) solutions for controller units, door components, and network equipment, resilience is built into the system. Access decisions and the unlocking of doors require power for door components, Device converters, Controllers and local network equipment.

Local networks in a building

To ensure stability, it is recommended to deploy a local network exclusive to Incedo™ Open components. The EAC system could also be divided between several networks, as long as Device converters and their parent Controllers are connected to the same network.

For a specific critical door, a dedicated network together with a UPS and a single Controller could be an option. This would provide the highest level of reliability, should the power grid or Internet connection go down.

NOTE!

Wireless network equipment is not supported.

4.3 Planning Alarm Area for an External Alarm Zone

When planning Incedo™ Open systems, ensure that the door sides defining alarm areas are aligned with the external alarm zones. Perimeter protection such as contact detectors on doors and windows should outline the alarm area. Internal protection such as motion detectors should be mounted to exclusively cover the alarm area.

16 alarm areas can be added per Incedo™ Open system, and up to four alarm areas can be handled by a Controller. The four alarm areas can be controlled directly, or from its connected Device converters. All Device converters and devices in an alarm area must be connected to the same Controller.

Preparing the external alarm system

Each external alarm zone must be set up to be armed from an analogue input. The input is to be connected to the alarm control relay (AC). If the alarm system so requires, dual loop resistors can be connected at the AC relay's end near the terminal.

Each external alarm zone must also be set up to activate an alarm status feedback (ASF) relay when armed. See instructions on how to mount an alarm area in the Incedo™ Open User Guide. The relay on the external alarm panel is to be connected to the controller unit's ASF input.

Connections

To connect the ASF input, AC relays, and pre-alarm relay for an alarm area, any analogue input and relay on the designated alarm area Controller and any of its Device converters can be used. This includes Device converters that are not part of the same alarm area.

To control alarm areas from the parent Controller, it must also be added as a door and mounted as a Device converter in the Incedo™ Open web application. A controller unit placed near the external alarm control panel could be used to handle several alarm areas. If more connectivity is needed, an optional relay board can be used.

5 Operators, Users and Roles

5.1 Adding a Role

1) In **Settings » Roles**, click **+ Create new**.

2) Enter a **Name**, and optionally, a **Description**.

3) For every functionality (privilege) to add, select **Read access** or **Read and write access**. Leave the privileges that are not needed, set to **No access**.

4) Review the information, and click **Create role**.

5.2 Adding an Operator

1) In **Settings » Operators**, click **+ Create new**.

2) Add the contact information.

Entry field	Description
First name*	The first name of the operator.
Last name*	The surname of the operator.
E-mail*	A valid email address.
Phone	A valid phone number.
Company	Name of the operator's organisation.

*Required information.

3) Select a role for the operator.

For more information about roles, see Section 3.3 *"Users and Roles"*, page 14.

4) Review the information, and click **Create operator**.

The new operator receives an email with instructions on how to proceed.

> **NOTE!**
> Links in the email must be opened in a supported browser. Check Section 1.6 *"System Requirements"*, page 9 for a list of supported browsers.

5.3 Adding a User

1) In **Users » Users**, click **+ Create new**.

2) Add the basic information.

Entry field	Description
First name*	The first name of the user.
Last name*	The surname of the user.
E-mail	A valid email address.

Entry field	Description
Phone	Enter a valid phone number, followed by the country code selected in the dropdown field.
PIN code	PIN code used for credentials (e.g. cards). Can be shown in plain text by clicking **Show PIN**. PIN codes must be 4 characters long, digits only.

*Required information.

3) Optional: Select **Anonymise audit log** to enable anonymisation of audit log entries involving the user.

   For more information, see Section 3.7 *"Anonymisation Features and Data Retention"*, page 18.

4) Optional: Select **Do not store audit logs for sensitive doors**.

5) Click **Next**.

6) Optional: **+ Add access profile** .

Entry field	Description
Access profile	List of available access profiles.
Valid from (YYYY-MM-DD)	Date from which the access profile is included in access decisions for a user.
Valid to (YYYY-MM-DD)	Date from which the access profile is excluded in access decisions for a user. Can also be set to **Indefinitely**, that is, with no end date.

   To add one more access profile, repeat step. Remove access profile by clicking on the dustbin icon next to it.

7) Optional, if creating a user with a lease: Select **Connect user to lease**, and select a lease.

   Also select **Visible in entry phone list**, to list the user in the entry phone list.

8) Click **Next**.

9) Optional: To create a credential for the user, click **+ Add credential**.

   For more information on how to create and hand out a credential, see Section 8.1 *"Creating and Handing Out a Credential"*, page 59.

5.4 Adding a Lease

1) In **Users » Leases**, click **+ Create new**.

2) Select **Building**, **Stairwell**, **Floor**, and **Apartment**.

3) Click **Next**.

4) Optional: Edit the **Lease name**.

   A default name is automatically filled in.

5) Click **Next**.

6) Select a lease **Start** date and time.

7) Either set an **End** date and time, or select **No end date**, which means that the lease will be valid until further notice.

8) Click **Next**.

9) Some access profiles may already be included with the apartment, but additional access profiles can be added to the lease.

   Optional: For each additional access profile to add:

   a) Under **Available lease specific access profiles**, select an access profile.

   b) Click **Add**.

10) Click **Next**.

11) For each user (resident) to add: Either click **Add a new user** and follow the instructions, or search for an existing user in the search field.

    To search, at least three letters must be entered in the search field. For more information on the new user parameters, see Section 5.3 *"Adding a User"*, page 28.

12) Click **Next**.

13) Optional: For each resident, set the access to **Lease specific profiles**, and **Apartment specific profiles**, respectively.

14) Click **Next**.

15) Review the information and click **Confirm**.

For more information, see Section 3.2 *"Apartments and Leases"*, page 13.

6 System Setup

6.1 Selecting PULSE Encryption Key Mode

1) In **Settings » System settings**, select mode for PULSE encryption keys.

Mode	Details
PULSE encryption keys are unique per building in the system	For more information, see Section 3.8.2 *"PULSE Encryption Keys"*, page 21. (Default.)
PULSE encryption keys are shared by all buildings in the system	For more information, see Section 3.8.2 *"PULSE Encryption Keys"*, page 21.

NOTE!
This setting can only be changed while no building has been added to the system.

6.2 Adding a Building

1) In **System setup » Buildings**, click **+ Create new**.

2) Enter the basic information.

Entry field	Description
Building name*	A descriptive name of the building.
Description	Additional information about the building.
Address*	An OpenStreetMap address.
Number of stairwells*	Physical or figurative stairwells of the building. That is, areas to access the floors of the building.
Maximum number of floors	Physical or figurative floors of the building, to which hardware components and areas can be added.
Entry floor*	Physical entry floor. This ensures that apartment default names are generated correctly. For Sweden, please refer to Lantmäteriet on the link below for more information: www.lantmateriet.se/globalassets/fastigheter/fastighetsinformation/instruktioner_lagenhetsnumrering.pdf

*Required information.

3) Optional: Click **Anonymisation of audit logs for one factor authentication** to enable anonymisation on building level.

Audit logs for two factor authentication events (card + PIN) and events where access was denied will not be anonymised. PULSE and Aperio devices only support one factor authentication. For more information, see Section 3.7 *"Anonymisation Features and Data Retention"*, page 18.

4) Click **Next**.

5) Optional: For each floor:

- Replace the generic **Floor name**.

- Upload a **Floor plan file**.

  Floor plans make planning and building management easier. Supported file formats: .png, .jpg.

- Replace the generic **Stairwell name**.
- If required, click **Add stairwell** to add another stairwell and replace the generic name.

6) Click **Next**.

7) Review the summary, and click **Create building**.

6.3 Adding an Apartment

1) In **System setup » Apartments**, click **+ Create new**.

2) Select **Building**, **Stairwell**, and **Floor**.

3) Optional: Enter a custom **Apartment name**.

   A default name is automatically filled in.

   The naming format follows "Instruktioner för lägenhetsnumrering" (2014), issued by Lantmäteriet.

4) Click **Next**.

5) Optional: To associate an access profile with the apartment, **Select access profile name**, and click **Add**.

   Any added access profile is available for selection when adding a new lease on the apartment.

6) Click **Next**.

7) Optional: For each available entry phone to add, select it under **Entry phone** and click **Add**.

8) Optional: To associate a mechanical key with the apartment:

   a) Under **Key destination**, enter a descriptive text.

   b) Enter the **Key identification number**.

      The key identification number is typically a marking found on the key.

   c) Click **Add**.

9) Review the information, and click **Confirm** to save.

For more information, see Section 3.2 *"Apartments and Leases"*, page 13.

6.4 Adding an Access Profile

1) In **System setup » Access profiles**, click **+ Create new**.

2) Enter a **Name**, and optionally, a **Description**.

3) To add an access area :

a) Click **+ Add access area**.

b) Select an **Access area**.

c) For any included online components: Select an **Online access schedule**.

d) For any included offline components: Select an **Offline access schedule**.

e) Optional: Select **Unlock code allowed**. Enables unlocking with credentials of format User code (code only).

f) To add another access area, click **+ Add access area**.

4) To add an offline door group:

a) Click **+ Add offline door group**.

b) Select an **Offline door group**.

c) Select an **Offline access schedule**.

d) Optional: Select **Unlock code allowed**. Enables unlocking with credentials of format User code (code only).

e) To add another offline door group, click **+ Add offline door group**.

5) To add an alarm area:

a) Click **+ Add alarm area**.

b) Select an **Alarm area**.

c) Select an **Alarm schedule**.

d) Select **Alarm privileges**.

Parameter	Description
Disarm	Permission to disarm the access area when the alarm schedule is active.
Arm	Permission to arm the access area when the alarm schedule is active.

e) To add another alarm area, click **+ Add alarm area**.

6) Review the information, and click **Create access profile**.

For more information, see Section 3.4 *"Access Concepts"*, page 14.

6.5 Hardware Planning

6.5.1 Managing Door Types

6.5.1.1 Adding a Door Type

1) In **System setup » Planning » Hardware planning**, select **Building** and **Floor**.

2) Click **Add door type**.

3) Enter a door type **Name**.

4) Select **Mode**, **Online** or **Offline**, depending on door type.

5) Add or remove hardware components.

   Hardware components are added on door level, or for each door side. For a complete list, see Section 11.2 *"Door Hardware Components"*, page 71.

6) Click **Save**.

For more information, see Section 3.1 *"Buildings, Floors and Doors"*, page 13.

6.5.1.2 Editing and Deleting Door Types

1) To edit a door type:

   a) In **System setup » Planning » Hardware planning**, select **Building** and **Floor**.

   b) Under the **Floor plan**, locate the door type and click the **Edit** icon. If needed, click the **Scroll** (arrow) icon to scroll through the door types.

   c) Optional: Edit the **Name**.

   d) Add or remove hardware components.

      Hardware components are added at the door level, or for a door side. For a complete list, see Section 11.2 *"Door Hardware Components"*, page 71.

   e) Click **Save**.

2) To delete a door type:

   Under the **Floor plan**, locate the door type and click the **Delete** (trash can) icon. If needed, click the **Scroll** (arrow) icon to scroll through the door types.

   Doors assigned to the deleted door type are converted to custom doors.

For more information, see Section 3.1 *"Buildings, Floors and Doors"*, page 13 and Section 6.5.1.1 *"Adding a Door Type"*, page 33.

6.5.2 Adding a Controller

Each Controller (InControl 3270) can handle up to 16 doors. For more information, see Section 4.2 *"Online System Design"*, page 26.

1) In **System setup » Planning » Hardware planning**, select **Building** and **Floor**.

2) From the list of doors and devices under the **Floor plan**, drag-and-drop a Controller onto the **Floor plan**.

3) Recommended: Under **Hardware set-up / plan**, edit the **Controller name**.

4) Click **Save**.

Make sure that the Controller unit has the latest firmware installed. See Section 9.3 *"Upgrading Controller Firmware"*, page 63.

6.5.3 Managing Doors

6.5.3.1 Adding a Door

For each online door, a Device converter is implied, but not shown in the web interface. One door can also be directly connected to a Controller, since a Device converter is included in each Controller.

It is recommended that a Controller is added before adding its doors (up to 16 doors per Controller).

1) In **System setup » Planning » Hardware planning**, select **Building** and **Floor**.

2) To add a door:

   a) Under the **Floor plan**, locate the door type that you want to add. If needed, click the **Scroll** (arrow) icon to scroll through the door types.

      For more information, see Section 6.5.1.1 *"Adding a Door Type"*, page 33.

   b) Drag-and-drop the door type onto the **Floor plan**.

   c) Optional: To align the door sides in the floor plan, repeatedly click the rotation symbol.

   d) Recommended: Under **Door details**, edit the **Door name**.

   e) Optional: Under **Hardware set-up / plan**, edit the door level and side level hardware components.

      For a complete list, see Section 11.2 *"Door Hardware Components"*, page 71.

      WARNING!
      Edited doors are converted to custom doors.

3) For every online door:

   a) Select the door in the **Floor plan**, or under **Doors & Devices**.

   b) Under **Door details**, select a **Controller**.

4) Click **Save**.

For more information, see Section 3.1 *"Buildings, Floors and Doors"*, page 13, Section 6.5.2 *"Adding a Controller"*, page 34, and Section 4.2 *"Online System Design"*, page 26.

6.5.3.2 Editing a Door

1) To edit a door:
   a) In **System setup » Planning » Hardware planning**, select **Building** and **Floor**.
   b) In the **Floor plan**, select the door.
   c) Under **Hardware set-up / plan**, edit the name and door type, and change or delete hardware components.

      Hardware components are added at the door level, or for a door side. For a complete list, see Section 11.2 *"Door Hardware Components"*, page 71.

2) To delete a door:

   In the **Floor plan**, select the door and click on the **Delete** (trash can) icon.

   A door cannot be deleted, until all connected offline door groups are removed.

3) Click **Save**.

For more information, see Section 3.1 *"Buildings, Floors and Doors"*, page 13.

6.6 Hardware Mounting

Hardware mounting means that every hardware component is marked as correctly installed and ready for use in the system. For online devices the hardware address to the device is entered and the network connection can be tested. For offline devices the serial number must be entered.

- To mount a Controller, see Section 6.6.1 *"Mounting a Controller"*, page 36.
- To mount a Device converter with door components, or a device, see Section 6.6.2 *"Mounting a Door or Device"*, page 37.

For information on how to install Controllers and Device converters, see Incedo™ Open: InControl 3270 and ToConnect 3270 Installation Guide.

6.6.1 Mounting a Controller

This section describes how to mount a Controller (InControl 3270) for communication with the cloud and Device converters (ToConnect 3270). To use the Controller's inputs, outputs, and interfaces, it must also be mounted as a Device converter.

1) In **System setup » Planning » Hardware mounting**, select **Building** and **Floor**.
2) Under **Doors & devices**, locate the Controller (InControl 3270) and click **Mount**.
3) Enter the MAC address of the Controller (InControl 3270).

> **NOTE!**
> Not to be confused with the MAC adress of the Device converter (ToConnect 3270). For information on how to locate MAC addresses, see Incedo™ Open: InControl 3270 and ToConnect 3270 Installation Guide.

4) Click **Test connection**.

   For a successful test, the cloud service is able to communicate with the Controller matching the entered MAC address.

   If the test fails, ensure that the entered MAC address is correct, and that the Controller has an Internet connection. Allow some time for the Controller to communicate with the cloud service.

5) If the test is successful, select **This device is mounted**.

   The Controller InControl 3270 is now ready for use.

6) Click **Save**.

For more information on how to mount a Device converter, see Section 6.6.2 *"Mounting a Door or Device"*, page 37.

6.6.2 Mounting a Door or Device

Only online doors and devices need to be mounted in the web application.

1) In **System setup » Planning » Hardware mounting**, select **Building** and **Floor**.

2) Under **Doors & devices**, locate the door to be mounted and click **Mount** or **Edit**.

3) In the **Mounting** tab, select **ToConnect**.

   Mounting status and connection status is displayed below. If the Device converter is expanded with a relay board, this will be indicated.

4) Enter the MAC address.

   For more information on how to locate the MAC address, see Incedo™ Open: InControl 3270 and ToConnect 3270 Installation Guide.

5) Click **Test connection**.

   For a successful test, the cloud service is able to communicate with the Controller (InControl 3270), a Device converter (ToConnect 3270) or device matching the entered MAC address.

   If the test fails, ensure that the entered MAC address is correct, and that the Device converter or device is connected to the same network as its parent Controller. The Controller must have Internet access. Allow some time for the Controller to communicate with the cloud service.

6) If the test is successful, select **This device is mounted**.

7) For each **Door level** component:

   a) Select a component.

   b) Follow the instructions.

Table 1. Relay mounting options.

Parameter	Value	Description
Select analogue port	RE1-RE2 Relay board: RE3-RE8	Relays on the controller unit. Relays on the controller unit or relay board.

Table 2. Analogue input mounting options.

Parameter	Value	Description
Select analogue port	IN1-IN3 Relay board: IN4-IN7	Physical input on the controller unit. Physical input on the controller unit or relay board.
Double balanced	Selected/De-selected	Enables or disables dual loop (double end-of-line-resistor) mode.
Resistor value R1	1000-4700 Ω	Component value for resistor R1.
Resistor value R2	1000-4700 Ω	Component value for resistor R2.

c) Select **This device is mounted**.

8) For each **Side 1** and **Side 2** component

a) Select a component.

b) Follow the instructions.

Table 3. Hi-O push button mounting options.

Parameter	Value	Description
Select DIP switch	On/Off	The physical DIP switch setting must correspond to this setting.

Table 4. Hi-O display offline updater mounting options.

Parameter	Value	Description
Select DIP switch	On/Off	The physical DIP switch setting on the component must correspond to this setting.
Set SIO mode address (1-99)	1-99	Hi-O address. For more information, see the component's documentation.

Table 5. RS-485 device mounting options.

Parameter	Value	Description
Enter serial no	Serial number	The RS485 component's serial number, for more information, see the component's documentation.

Table 6. WellCom mounting options

Parameter	Value	Description
Enter IP number or MAC address	IP number/MAC address	The (local) IP number of the component, or the MAC address. For more information, see the component's documentation.

c) Select **This device is mounted**.

HINT!
The available analogue inputs and outputs can also be reviewed and selected from the **Inputs/Outputs** tab.

6.7 Hardware Configuration

6.7.1 Configuring a Door

1) In **System setup » Planning » Hardware configuration**, select a **Building** and **Floor**.

2) For each online door to configure:

   a) In the **Floor plan** or under **Doors**, select an online door.

   b) Under **Settings on door level**, set the **Unlocked schedule** and **Motor lock unlocked schedule**.

   c) Under **Setting on side 1** and **Settings on side 2**, select **Security schedule**.

   For more information, see Section 3.4 *"Access Concepts"*, page 14.

   d) Optional: Select **Sensitive door**.

   For more information, see Section 3.7 *"Anonymisation Features and Data Retention"*, page 18.

   e) Click **Advanced door configuration**.

   f) Under **Settings on door level**, review or configure the parameters.

Parameter	Description
Time settings	
Permitted door opening time	The time a door is allowed to be open.

Parameter	Description
Unlocked time when the door is not opened	Interval before an unlocked door is locked if it has not been opened.
Delay time before locking	Time interval between a door closing event and re-locking.
Temporary alarm bypass settings	
Delayed time before unlock	Time interval between a positive access decision and an open lock command. Useful to prevent false alarms.
Delayed time before alarm sensor reactivation after door is closed	Time interval between a door closing event and deactivation of the alarm bypass relay. Useful to prevent false alarms
Activate alarm sensor when door is open too long	Activates a relay output when the Permitted door opening time is exceeded.
Buzzer settings	
Door opened too long schedule	Operational schedule to engage or disable the reader's internal buzzer function when the permitted door opening time is exceeded.
Door forced open schedule	Operational schedule to engage or disable the reader's internal buzzer function when a forced open event occurs.
Lock settings	
Unlocked schedule	An operational schedule. Defines when the door (electric strike) will be unlocked.
Motor lock unlocked schedule	Operational schedule, same as for the basic settings. Defines when the motor lock is unlocked.
Security lock settings	Defines whether a motor lock is unlocked directly, as defined by the **Motor lock unlocked schedule**, or delayed until the first valid passage.
Emergency exit siren settings	
Emergency siren active time	The active time period for a siren after pressing an emergency exit button.

g) Under **Settings on side 1** and **Settings on side 2**, review or configure the parameters.

Parameter	Description
Security level schedule	Security schedule. Defines time slots with different security levels for a door. Default level is card and PIN. For more information, see Section 3.4 *"Access Concepts"*, page 14.
Exit button schedule	Defines the operational schedule for the exit button. Outside the defined time period, the exit button will not work.

h) Click **Apply**, then **Save**.

3) For each offline door to configure:

   a) Under **Floor plan** or **Doors**, select an offline door.

   b) Optional: Select **Sensitive door**.

   c) Optional for PULSE locks: Change the number of audit logs that can be stored in the PULSE lock.

   d) Using an external configuration tool, complete the offline door configuration:

      - To configure an Aperio door, see Section 6.12 *"Exporting Aperio Offline Configuration"*, page 53.
      - To program a PULSE door, see Section 6.11 *"Programming a PULSE Lock"*, page 52.

For more information, see Section 3.5 *"Calendars and Schedules"*, page 17 and Section 3.7 *"Anonymisation Features and Data Retention"*, page 18.

6.8 Access Handling

6.8.1 Adding an Access Area

The access area concept is explained in Section 3.4 *"Access Concepts"*, page 14.

1) In **System setup » Planning » Access areas**, click **Add access area**.

2) Enter the access area details.

Entry field	Description
Name*	Descriptive name of the access area.
Description	Additional text.
In building*	The designated building for the access area.
On floor*	The designated floor for the access area.

*Required information.

3) Click **Next**.

4) Select all the door sides leading into the access area.

5) Click **Next**.

6) Review the information, and click **Confirm**.

6.8.2 Adding an Offline Door group

The offline door group concept is explained in Section 3.4 *"Access Concepts"*, page 14.

1) In **System setup » Planning » Offline door groups**, click **+ Create new**.

2) Enter a **Name**, and optionally, a **Description**.

3) Click **Next**.

4) Select a **Building** and a **Floor**.

5) In the **Floor plan**, or under **Doors**, select offline doors for the group.

6) Click **Include in group**.

7) Click **Next**.

8) Review the information and click **Confirm**.

6.9 Alarm Planning

6.9.1 Adding or Editing an Alarm Area

If editing the doors of an existing alarm area, start from *Step 3*.

All door sides (Device converter ToConnect 3270) in an alarm area must share the same parent Controller (InControl 3270). Ensure that the alarm area corresponds to the external alarm zone. For more information, see Section 3.9.2 *"Alarm Areas"*, page 24.

1) In **System setup » Planning » Alarm planning**, click **+ Create alarm area**.

2) Enter the alarm area details.

Entry field	Description
Name*	Descriptive name of the alarm area. Also used to identify the alarm area in the alarm control view.
Description	Additional information about the alarm area.

*Required information.

3) From the tree view, expand a building by clicking on the left-hand side arrow.

The floors of the building are shown.

4) Expand each floor from which to select door sides.

The access areas and other doors and devices for the floor are shown.

5) Select all door sides leading into the alarm area.

- To include all door sides from an access area, tick the left-hand side box.

  Access areas are only used for selection, there is no connection between access areas and alarm areas. Individual doors can be deselected.

- To include individual door sides from an access area, expand the access area and select the door sides.

- To include door sides that are not part of an access area, for each floor, expand **Other doors and devices** and select the door sides.

Door sides already in use by other alarm areas can not be selected.

6) Review the information, and click **Save**.

7) Configure the alarm area.

For more information, see Section 6.9.2 *"Configuring an Alarm Area"*, page 43.

For more information, see Section 3.9.1 *"External Alarms"*, page 23.

6.9.2 Configuring an Alarm Area

If a new alarm area is being created, start from *Step 4*.

1) In **System setup » Planning » Alarm planning**, from the tree view, select a building by clicking on the left-hand side arrow.

   The tree view is expanded to show the floors of the building.

2) Expand the floor of the alarm area.

   Alarm areas with doors from multiple floors are listed under each included floor.

3) Click to select the alarm area.

4) Under **Alarm area details**, review and edit the parameters.

Parameter	Description and available options
Name	Required. Descriptive name of the alarm area. Also used to identify the alarm area in the alarm control panel.
Description	Additional information about the alarm area.
Disarm on unlocking	Users with alarm privileges disarm the alarm when unlocking a door with card and PIN. Alarm privileges are set in access profiles. For more information, see Section 6.4 *"Adding an Access Profile"*, page 32.
Scheduled alarm manoeuvre (automatic arm/disarm)	• No scheduled alarm manoeuvre: Default. The alarm area is armed and disarmed manually. • Alarm schedule selected: The alarm is armed, and optionally disarmed according to the selected alarm schedule. For more information, see Section 7.5 *"Adding an Alarm Schedule"*, page 57.
Only arm according to schedule	Available when alarm manoeuvres are scheduled. The alarm area is automatically armed according to the selected schedule, but must be disarmed manually.
Arm and disarm according to schedule	Available when alarm manoeuvres are scheduled. The alarm area is automatically armed and disarmed according to the selected schedule.
Pre-alarm time	The pre-alarm period in minutes or seconds. The period starts when an alarm area is armed manually or according to schedule. If mounted, a pre-alarm relay is activated during the period. For example, an alarm area with a pre-alarm time of 5 minutes set to arm at 10:00 will start the pre-alarm period at 10:00. An arming request will be sent at 10:05.
Block entrance readers during pre-alarm time	When the alarm area is in a pre-alarm period, the readers leading into the area are blocked. Readers leading out of the alarm area are not affected by this setting.

Parameter	Description and available options
Delayed arming (buy time)	• Never delay alarm arming: The alarm is always armed according to the selected alarm schedule. • Alarm schedule selected: A user with arm privileges for the alarm area can delay the scheduled arming by a predefined buy time period. For more information, see "Buying time".
Delayed arming (time setting)	Available when buy time is scheduled. Defines the buy time period in hours or minutes.
Permanent alarm status	When the alarm area is armed, the readers' alarm status LEDs are permanently on.
Alarm LED status on access attempt	Sets when a reader's alarm status LED should indicate that the alarm area is armed. Options: • Show for people with alarm privileges: The indication is restricted to users with alarm privileges for the alarm area. • Show for everyone: The indication is shown on all users' access attempts. • Show for no one: No indication is shown.
Timeout settings for alarm status feedback.	Timeout period in seconds for the external alarm to give alarm status feedback after an arming request. If no alarm status feedback is given, the alarm area is considered disarmed.

5) Click **Save**.

6) To configure alarm area settings for individual door sides, expand the alarm area.

   For each door:

   a) Select the door side.

   b) Review and edit the parameters.

Parameter	Description
Allow arming	The door side can be used for arming actions.
Allow disarming	The door side can be used for disarming actions.
Allow users to enter an armed alarm area (users with alarm privileges)	The function can be used when arming and disarming actions are handled from a reader or external alarm panel inside the alarm area.
Unlock door when disarming	When the alarm area is disarmed from the door, it is unlocked as with a normal passage. Normally, alarm manoeuvres and the unlocking of doors are handled as separate events.
Allow exceptions from <alarm area name>	Toggles the available exception parameters.

Parameter	Description
Permanent alarm status	Available when exceptions are allowed: When the alarm area is armed, the reader's alarm status LED is permanently on.
Block entrance readers during pre-alarm time	Available when exceptions are allowed: When the alarm area is in a pre-alarm period, the reader leading into to the area is blocked.

7) Click **Save**.

8) Optional: To edit the doors, click **Edit doors in alarm area**.

   For more information, see Section 6.9.1 *"Adding or Editing an Alarm Area"*, page 42.

For more information, see Section 3.9.1 *"External Alarms"*, page 23 and Section 3.9.2 *"Alarm Areas"*, page 24.

6.9.3 Mounting an Alarm Area

This section describes how to map (mount) the alarm area's I/O functions to the inputs and outputs of a controller unit (ToConnect 3270 or InControl 3270), or to an optional relay board. For more information, see Section 4.3 *"Planning Alarm Area for an External Alarm Zone"*, page 27.

Each alarm area must include the following mounted inputs and outputs:

Function	Quantity	I/O
Alarm status feedback (ASF)	1	IN1-IN3 Relay board: IN4-IN7
Alarm control relay (AC)	1 or more	RE1-RE2 Relay board: RE3-RE8

Optional:

Function	Quantity	I/O
Pre-alarm relay	0 or more	RE1-RE2 Relay board: RE3-RE8

1) In **System setup » Planning » Hardware mounting**, select **Building** and **Floor**.

2) Under **Doors & devices**, locate the door to use for external alarm communication, and click **Mount** or **Edit**.

3) Select the **Inputs/Outputs** tab.

4) From the drop-down menu of the selected Alarm Status Feedback input, select **Alarm Status Feedback <alarm area>**.

5) From the drop-down menu of the selected Alarm Control Relay output, select **Alarm Control Relay <alarm area>**.

   Optional: Select any additional Alarm Control Relay output.

6) Optional: From the drop-down menu of any selected Pre-Alarm Relays, select **Pre-Alarm Relay <alarm area>**.

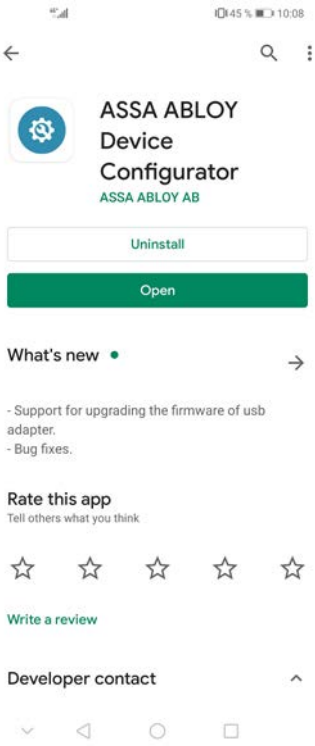
7) Click **Save**.

For more information, see Section 3.9.1 *"External Alarms"*, page 23, Section 3.9.2 *"Alarm Areas"*, page 24, and Incedo™ Open: InControl 3270 and ToConnect 3270 Installation Guide.

6.10 PULSE Installation

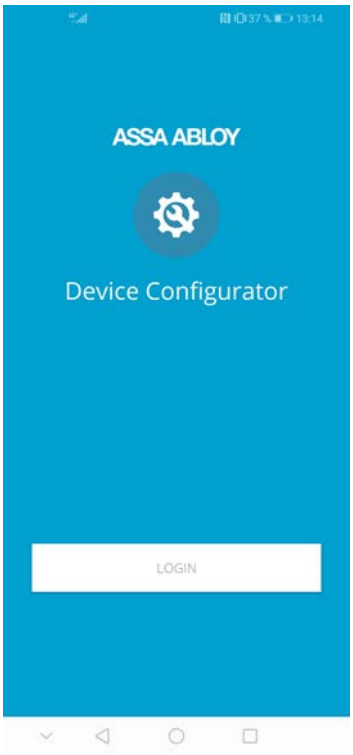
6.10.1 Installing ASSA ABLOY Device Configurator

1) From Google Play Store, download and open the **ASSA ABLOY Device Configurator (AADC)**.



2) Log in with Incedo™ Open credentials.

   If the credentials are valid for more than one system, a system must be selected.



3) When asked to allow AADC to access photos, media and files, click **ALLOW**.

   AADC needs these permissions to work correctly.

For more information, see Section 3.8.4 *"ASSA ABLOY Device Configurator"*, page 22.

6.10.2 Adding a Desktop Updater

One Desktop Updater (DU) can be used for more than one PULSE locking system and up to 10 buildings in total.

Add a Desktop Updater to a building in the Incedo™ Open web application:

1) In **System setup » Buildings**, select a building.

2) Under **Desktop updaters**, click the **Edit** icon and then **Connect desktop updater » Create new desktop updater**.

3) Enter the information.

Entry field	Description
Name*	Name of the Desktop Updater. For example the name of the housing society, or building.
Description	Additional identifying information.
Select buildings	The current building is pre-selected. Add up to a maximum of 10 buildings.

*Required information.

NOTE!
The DU memory allows for up to 10 buildings. Removing a building will not free up memory space in the DU.

4) Click **Create**.

The DU is now added in the Incedo™ Open system. In order to use the DU, the DU PC application must be installed on a PC and the DU must be configured using the AADC mobile application. For more information, see, see Section 6.10.3 *"Installing a Desktop Updater"*, page 48.

6.10.3 Installing a Desktop Updater

Prerequisites:

- PC running Windows 8 or later (32-bit or 64-bit version)
- USB port
- Desktop Updater added in the Incedo™ Open system

1) Download and install the Desktop Updater PC application.
   a) Download 64-bit version:
   https://d1rs7kespbo4zq.cloudfront.net/AssaAbloy_Pulse_windows-x64.exe

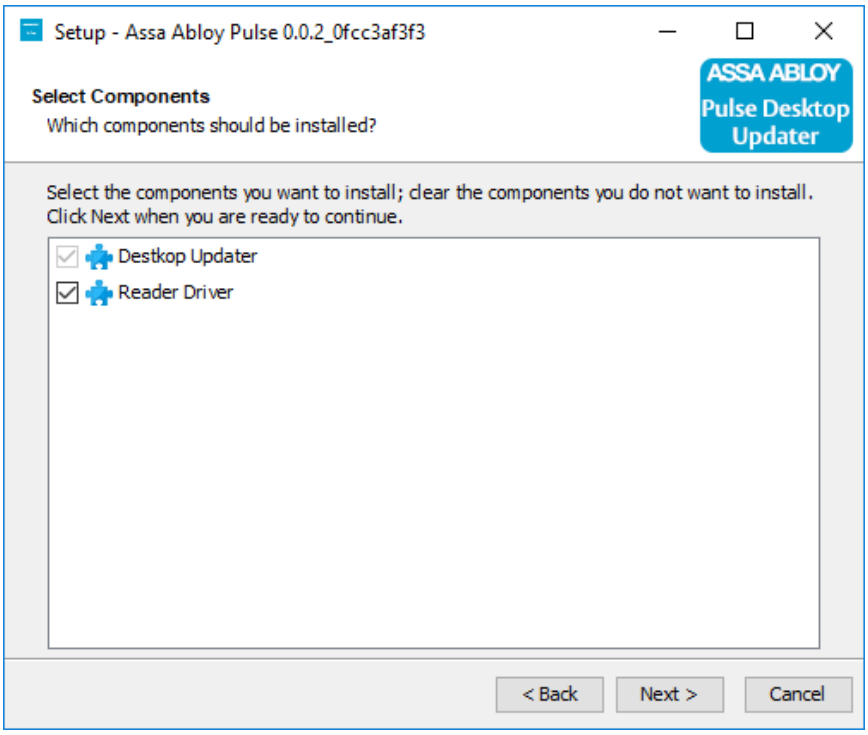
   Or, download 32-bit version:
   https://d1rs7kespbo4zq.cloudfront.net/AssaAbloy_Pulse_windows.exe

   HINT!
   Most modern PCs support the 64-bit version. If you have an old PC you may determine whether your PC has 32-bit or 64-bit Operating System by checking the **System type** in the **System Information** properties window of the PC.

   b) Run the installer file as an administrator.

   c) Select application language, accept the license agreement, and select the destination directory.

   d) When asked, select to install **Desktop Updater** with **Reader Driver**.



e) Finish the installer and launch the application.

When successfully installed, a Desktop Updater icon will appear in the taskbar.

f) From **Taskbar » Desktop Updater » Sign in**, log in to the PC application, using your Incedo™ Open AADC credentials.

2) Using a USB cable, connect the Desktop Updater to the PC.

A blue light indicates that the connection process is complete.

3) Using ASSA ABLOY Device configurator (AADC), configure the Desktop Updater.

a) Enable NFC on the Android device.

b) Open AADC.

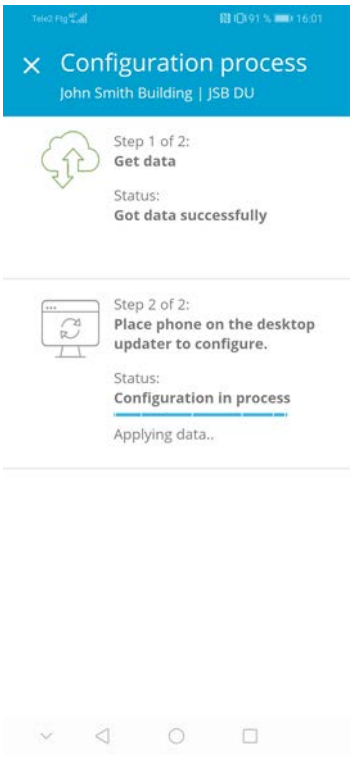
If prompted to log in, see Section 6.10.1 *"Installing ASSA ABLOY Device Configurator"*, page 46.

c) Under **To do list**, select a PULSE locking system.

d) From the list of **PENDING DEVICES**, select the Desktop Updater.

e) Click **Configure**, and place the Android device on top of the Desktop Updater.

When the Desktop Updater is configured, it will flash between light blue and deep blue.



4) Using your Incedo™ Open credentials, log in to the Desktop Updater PC application.

The Desktop Updater can now be used to update PULSE keys.

5) Optional: Change the Reading key number mode.

In **Taskbar » Desktop Updater » Reading key number**, select credential number mode.

Mode	Description
Normal	Default. If the credential is not found in the system, the credential number is copied to a text field.
Force	When a PULSE key is updated, the credential number is always copied to a text field.
Off	Automatic copying of the credential number is disabled.

For more information about the Desktop Updater, see Section 3.8.3 *"PULSE Updater Devices"*, page 22.

6.10.4 Configuring WellCom 4707 as a PULSE Updater

Prerequisites:

- The WellCom unit is mounted in the Incedo™ Open system.
- NFC-enabled Android device (Android 5.0 Lollipop or later) with the application ASSA ABLOY Device Configurator (AADC) installed.
- You know where on the Android device the NFC antenna is located. This information should be available in the user information of the device.

1) Enable NFC on the Android device.

2) Turn off and turn on the WellCom unit. Wait until it has restarted.

> **NOTE!**
> Finish the configuration within 7 minutes after restart. After 7 minutes the WellCom unit stops listening for the AADC app.

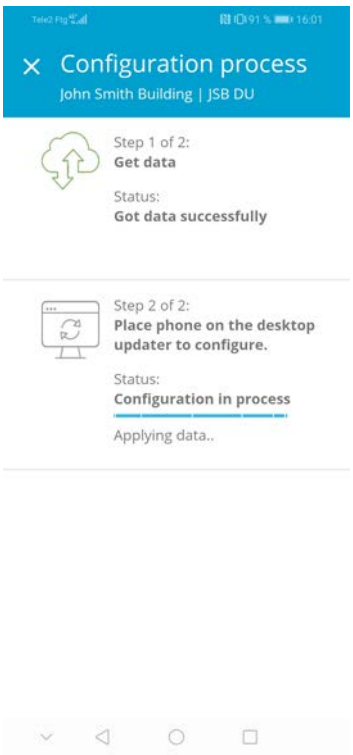
3) Open AADC.

   If prompted to log in, see Section 6.10.1 *"Installing ASSA ABLOY Device Configurator"*, page 46.

4) Under **To do list**, select a PULSE locking system.

5) From the list of **PENDING DEVICES**, select the WellCom unit.

6) Click **Configure** in AADC.



7) Place the Android device with the NFC antenna on top of the antenna symbol on the WellCom unit. Hold it in place until the configuration is completed.

8) The WellCom unit can now be used to read and update PULSE keys.

Verify the configuration by using the WellCom unit to update a PULSE key, see Section 8.5 *"PULSE Key Update"*, page 61.

For more information about PULSE updater devices , see Section 3.8.3 *"PULSE Updater Devices"*, page 22.

6.11 Programming a PULSE Lock

PULSE locks are programmed using the programming device (PPD200/PPD201) with an Android device running the ASSA ABLOY Device Configurator (AADC) mobile application. For more information, see Section 3.8.4 *"ASSA ABLOY Device Configurator"*, page 22.

1) Log in to AADC.

2) From the **To do list**, select a PULSE locking system.

   A PULSE locking system in AADC corresponds to a building in the web application.

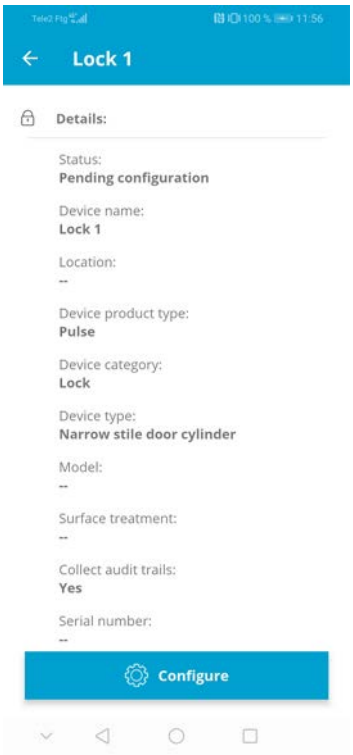
3) Select the PULSE lock.

   The PULSE lock must be added in the web application. For more information, see Section 6.5.3.1 *"Adding a Door"*, page 35.

4) Connect the programming device to the Android device, using the USB cable.

5) Insert the key end of the programming device into the PULSE lock and turn it as a key.

   AADC will notify when the programming process is complete.



6) When the programming is complete, remove the programming device from the PULSE lock.

6.12 Exporting Aperio Offline Configuration

Aperio locks are planned and grouped inside the Incedo™ Open web application, and then updated and configured using the PAP tool, a PC application to set up and program Aperio based products.

The export function in the web application creates an .xml file containing information such as offline door groups and names, to be imported into the PAP tool.

1) In **Settings » Export offline configuration**, click **Export**, and save the .xml file.

2) In the PAP tool, import the file.

6.13 Adding a Credential Type

1) In **Settings » Credential types**, click **+ Create new**.

2) Enter a **Name**, and optionally, a **Description**.

3) Select between the available **Formats**.

Format	Comment
Desfire	DESFire UID (Pando)
Mifare	Mifare UID Classic (Pando)
Offline	DESFire OSS Offline
Prox	UID 5 byte (Öppna, factory configuration)
Prox4	Mifare Classic 4 byte UID (Öppna configured for Full-ID)

Format	Comment
Prox7	Mifare Classic 7 byte UID, DESFire UID, or PULSE UID (Öppna configured for Full-ID)
Pulse	PULSE
Unlock Code	For card readers with key pad

4) Click **Create**.

For more information on credential formats, see Section 3.6 *"Credentials"*, page 18.

7 Managing Schedules

7.1 Adding an Access Schedule

An online access schedule enables or disables access rights to access areas based on time slots. As an option, it is possible to use exception days from a calendar to have other time slots for specific days. Online access schedules are paired with access areas into access profiles.

1) In **Schedules » Access schedules online**, click **+ Create new**.
2) Enter a **Name**, and optionally, a **Description**.
3) Select a calendar.

   For more information on calendars, see Section 7.6 *"Adding a Calendar"*, page 57.
4) Click **Next**.
5) In the **Setup standard week** calendar, click-and-drag to select **Always access** time slots.
6) Optional: Click on a time slot to edit the start time, end time, as well as start and end day, in a pop-up dialogue.
7) For each type of special day, in the **Setup special days** calendar, click-and-drag to select **Always access** time slots.
8) Review the information, and click **Confirm**.

For more information, see Section 3.5 *"Calendars and Schedules"*, page 17 and Section 3.4 *"Access Concepts"*, page 14.

7.2 Adding an Offline Access Schedule

An offline access schedule enables or disables access rights to offline door groups, based on time slots from standard week calendars, without exception days. Offline access schedules are paired with offline door groups and access areas into access profiles.

1) In **Schedules » Access schedules offline**, click **+ Create new**.
2) Enter a **Name**, and optionally, a **Description**.
3) Click **Next**.
4) In the **Setup standard week** calendar, click-and-drag to select **Always access** time slots.

> **NOTE!**
> Offline locks do not use special days, only standard weeks (Monday-Sunday). Aperio locks have a built-in clock and can handle schedules. PULSE locks do not have a clock, and can thus not handle schedules.

5) Optional: Click on a time slot to edit the start time, end time, as well as start and end day, in a pop-up dialogue.

6) Review the information and click **Confirm**.

For more information, see Section 3.5 *"Calendars and Schedules"*, page 17 and Section 3.4 *"Access Concepts"*, page 14.

7.3 Adding an Operational Schedule

An operational schedule defines when a hardware function is on or off. Examples include door configurations such as unlocked schedules and exit button schedules.

1) In **Schedules » Operational Schedules**, click **+ Create new**.

2) Enter a **Name**, and optionally, a **Description**.

3) Select a **Calendar**.

4) Click **Next**.

5) In the **Setup standard week** calendar, click-and-drag to select **Always on** time slots.

6) For each type of special day, in the **Setup special days** calendar, click-and-drag to select **Always on** time slots.

7) Optional: Click on a time slot to edit the start time, end time, as well as start and end day, in a pop-up dialogue.

8) Click **Next**.

9) Review the operational schedule information, and click **Confirm**.

For more information, see Section 3.5 *"Calendars and Schedules"*, page 17.

7.4 Adding a Security Schedule

A security schedule can be set, to define time slots when different security levels apply to a door side. The default level is Card + PIN. The two sides of a door can have different security levels.

1) In **Schedules » Security Schedules**, click **+ Create new**.

2) Enter a **Name**, and optionally, a **Description**.

3) Select a **Calendar**.

4) Click **Next**.

5) To set the security schedule for a standard week:

   a) Click-and-drag to select a time slot.

   b) Click the time slot and select a security level.

      The time slot can also be edited (start time, end time, start day, and end day).

c) Click **Done**.

d) Repeat as needed.

6) Click **Next**.

7) For each day in the **Setup special day** list, select the day and do the following. *Step 5*.

a) Click-and-drag to select a time slot.

b) Click the time slot and select a security level.

The time slot can also be edited (start time, end time, start day, and end day).

c) Click **Done**.

d) Repeat as needed.

8) Click **Next**.

9) Review the security schedule information, and click **Confirm**.

For more information, see Section 3.5 *"Calendars and Schedules"*, page 17.

7.5 Adding an Alarm Schedule

An alarm schedule defines when an external alarm function is active. It is used to schedule the arming and disarming of alarm areas, as well as for other functions such as alarm privileges and delayed arming.

1) In **Schedules » Alarm Schedules**, click **+ Create new**.

2) Enter a **Name**, and optionally, a **Description**.

3) Select a **Calendar**.

4) Click **Next**.

5) In the **Setup standard week** calendar, click-and-drag to select **Active** time slots.

6) For each type of special day, in the **Setup special days** calendar, click-and-drag to select the **Active** time slots.

7) Optional: Click on a time slot to edit the start time, end time, as well as start and end day, in a pop-up dialogue.

8) Click **Next**.

9) Review the information, and click **Confirm**.

For more information, see Section 3.5 *"Calendars and Schedules"*, page 17 and Section 3.9.1 *"External Alarms"*, page 23.

7.6 Adding a Calendar

1) In **Schedules » Calendars**, click the **Edit** icon and then **Add new calendar**.

2) Enter a **Calendar name**, and optionally, a **Description**.

3) To add an exception day type, under **Exception days**, enter a name, and click **Add new type**.

4) To add an exception day in the calendar:

   a) Select **Month** and under **OVERVIEW**, select a calendar day.

   b) Select the exception day type.

   c) Click **Save**.

For more information, see Section 3.5 *"Calendars and Schedules"*, page 17.

8 Daily Tasks

8.1 Creating and Handing Out a Credential

When creating a credential (for example a key, a card or a user code) in the system, the credential is connected to a selected user and the user's access profiles.

1) In **Home**, click **Create credential**.
2) Search for, or select a user from the list.

   To search, enter at least three letters in the search field.
3) Select the **Credential type** for the credential.

   For more information, see Section 3.6 *"Credentials"*, page 18.
4) For key or card, enter the credential number:
   - Enter the **Credential number** manually. This could be a physical marking on the card or key.
   - If a PULSE key is selected and a Desktop Updater is installed and configured to read key numbers:
     a) Click anywhere in **Credential number** to highlight the field.
     b) Place the PULSE key on the Desktop Updater.

        The PULSE key is updated, and the credential number pasted to the credential number field. For more information, see Section 8.5 *"PULSE Key Update"*, page 61.
5) Optional: add **Label** text.
6) For key or card: make sure that **Custody** is set to **Handed out**.
7) For user code: enter a 6 digit **Code** or select **Use PIN code as unlock code**.
8) Review the information, and click **Create**.
9) Offline credentials: Update the key with an updater before use.

NOTE!
For credentials with multiple credential types, the hand out must be repeated for each type using the same credential number.

For more information on hand out procedures, see Section 3.6 *"Credentials"*, page 18.

8.2 Handing In a Credential

A hand in disconnects a user's access profiles from a credential (for example a key or a card).

1) In **Home**, click **Hand in**.
2) Search for, or select a user from the list.

To search, enter at least three letters in the search field.

3) Select the credential(s) to hand in.

> **NOTE!**
> For mechanical credentials with multiple credential types, all credentials sharing the same credential number must be selected.

4) Review the information, and click **Hand in**.

5) Offline credentials: Present the credential to an updater before use.

   For more information, see Section 8.5 *"PULSE Key Update"*, page 61.

For more information on credential management, see Section 3.6 *"Credentials"*, page 18.

8.3 Blocking a Credential

1) In **Home**, click **Block**.

2) Search for, or select a user from the list.

   To search, enter at least three letters in the search field.

3) From the list, select any credential to block.

4) Click **Block**.

   Offline credentials retain their validity until one of the following events:

   - The credential's re-validation period is expired
   - The credential is presented to an updater
   - The credential is inserted into a lock with an updated blocklist.

For more information about credential management, see Section 3.6 *"Credentials"*, page 18.

8.4 Unlocking a Door Remotely

1) In **Home**, click **Unlock doors**.

2) Select a **Building** and a **Floor**.

3) In the **Floor plan**, click on the door that you want to unlock.

> **HINT!**
> Disconnected doors are marked in the list under **Doors**, and cannot be unlocked.

4) In the door's pop-up menu, click **Unlock**.

5) Click **Done**.

8.5 Updating a Pulse Key

A PULSE key is updated by placing it on top of a PULSE updater device (Desktop Updater or WellCom 4707). When updating a PULSE key, the following actions are executed:

- Current time stamp is transferred to the key.
- The PULSE key re-validation period is updated.
- Access rights are updated.
- The blocklist is transferred to the PULSE key. The blocklist will be distributed to any PULSE lock to which the key is inserted, if the timestamp in the lock is older than in the key.
- Audit logs for the key are transferred to the Incedo Open system.
- For Desktop Updaters: depending on Reading key number mode, the PULSE key credential number is copied to the currently active text field, if the field is editable.

  For more information, see Section 6.10.3 *"Installing a Desktop Updater"*, page 48, Section 8.5.1 *"Updating a PULSE Key with a Desktop Updater"*, page 61, and Section 8.5.2 *"Updating a PULSE Key with WellCom 4707"*, page 61.

8.5.1 Updating a PULSE Key with a Desktop Updater

1) Log in to the Desktop Updater PC application.
   a) Right-click the Desktop Updater icon in the taskbar, and select **Sign in**.
   b) Log in using your Incedo™ Open credentials.
2) Place the PULSE key on top of the Desktop Updater.

   The Desktop Updater PC application will notify when the update is complete.

> **NOTE!**
> If the PULSE key is not found in the system, the PC application will show an error message and copy the credential number to a text field, to facilitate the task of handing out the credential.

For more information, see Section 6.10.3 *"Installing a Desktop Updater"*, page 48 , and Section 3.8.3 *"PULSE Updater Devices"*, page 22 .

8.5.2 Updating a PULSE Key with WellCom 4707

The WellCom unit must be configured for reading and updating PULSE keys. See Section 6.10.4 *"Configuring WellCom 4707 as a PULSE Updater"*, page 51.

1) Place the PULSE key on top of the antenna symbol on the WellCom unit.

   The credential number of the key is read and access is granted or denied.

   If access is granted, the key is updated. The user may be prompted to not remove the key until the update is completed.

For more information, see Section 3.8.3 *"PULSE Updater Devices"*, page 22.

8.6 Checking Pulse Device Status

Incedo™ Open lists devices in the system that have been added but not configured. Also, each ongoing process of blocking a PULSE key credential is listed. For more information, see Section 3.8.1 *"Understanding PULSE"*, page 20.

1) Go to **System Setup » Configuring and Blocking Offline Locks** to check configuration status and progress of blocking PULSE keys.

   For more information about configuring Desktop Updaters, see Section 6.10.3 *"Installing a Desktop Updater"*, page 48.

   For more information about configuring PULSE locks, see Section 6.11 *"Programming a PULSE Lock"*, page 52.

   For more information about configuring Wellcom 4707, see Section 6.10.4 *"Configuring WellCom 4707 as a PULSE Updater"*, page 51.

9 System Status and Maintenance

9.1 System Overview

The **System Overview** lists the system status based on buildings, and includes a map for geographical overview and selection. The list can be filtered to only display buildings with issues, or all buildings.

In **System status » System overview**, the issues of a building can be expanded by clicking the listed **Issue(s)**. A building can also be viewed in detail by clicking the specific **Location name**.

For more information, see Section 9.2 *"Controller Troubleshooting Functions"*, page 63 and Section 9.3 *"Upgrading Controller Firmware"*, page 63.

9.2 Controller Troubleshooting Functions

Controllers (InControl 3270) are equipped with functions to assist troubleshooting. If the connection between the Incedo™ Open cloud service and one or several Controllers is lost, the first step is to check the Internet connection, local network equipment and cables.

1) In **System overview**, under **Issues**, click on a line to expand the issues of a building.
2) In the expanded section, under **Location name**, click on a Controller.
3) Click on a troubleshooting function and follow the instructions.

Function	Description
RETRIEVE database and log files	Downloads files from the Controller. Execute this function if requested by local support.
Resend all data	Resends the database in the cloud service to the Controller. This can solve issues caused by firmware updates and incomplete databases. All data must be resent after replacing an existing Controller. Only execute this function if requested by local support.
Restart Controller	Reboots the Controller.

NOTE!
Downloaded files may contain sensitive information and should be handled with security in mind.

9.3 Upgrading Controller Firmware

The upgrade feature can be used to upgrade Controllers (InControl 3270) and Device converters (ToConnect 3270) to the latest software version, or to roll back to a previous version.

For information on the appropriate software versions, contact ASSA ABLOY Opening Solutions.

1) In **System overview**, under **Issues**, click on a line to expand a building.
   The building's current issues are listed.
2) In the expanded section, under **Location name**, click on the device.

The current version can also be found in this view.

3) Click **Upgrade now** or **Plan upgrade**.

   If planning an upgrade for later, select a **Start date** and **Start time**.

4) Click **Upload** and select the latest software file.

9.4 Controlling Alarms

The alarm control panel displays all alarm areas available to the operator. Alarm areas can be remotely armed or disarmed, and the status of the alarm areas can be monitored.

1) In **System status » Alarm control**, locate the alarm area.

2) To arm the alarm area, click **Arm**.

   The status is changed to **Arming** while in the pre-alarm period. If the external alarm is successfully armed, the status is changed to **Armed**.

3) To disarm the alarm area, click **Disarm**.

   The status is changed to **Disarming**. If the external alarm is successfully disarmed, the status is changed to **Disarmed**.

NOTE!
Alarm area status is based on the state of the external alarm, not on the actual arming or disarming requests sent from the application.

9.5 Checking Logs

The logs view lists all types of logs available in the system, and includes tools for searching and filtering. Depending on the information needed by an operator, columns can be hidden from the view using the **Edit columns** feature. Some results may be anonymised, based on settings made elsewhere in the system. For more information, see Section 3.7 *"Anonymisation Features and Data Retention"*, page 18.

1) In **System status » Logs**, use the search and filter functions to view the log events that you are interested in.

Table 7. Search and filter functions.

Function	Description
Search	Enter a minimum of three letters to start the search function.
Any time	Filter on start and end dates and times. Includes an option to filter on time intervals per day.
All log types	Filter by log types. See table below.
All buildings	Filter by buildings.
All floors	Filter by floors.
All areas	Filter by access areas.
All doors	Filter by doors.

Table 8. Log types.

Log type	Description
Audit logs	Access related logs.
Incident/monitoring logs	Alerts such as tamper alarms, connection problems etc.
Operator logs	Actions initiated by operators.
System logs	Actions initiated by the system.

For more information on how to retrieve access logs from PULSE locks, see Section 9.6 *"PULSE: Audit Logs"*, page 65.

9.6 PULSE: Audit Logs

When a PULSE key is inserted in a PULSE lock, the interaction between the key and the lock is added to the audit log in the key. When the PULSE key is updated by a PULSE updater, the audit logs for that one key are uploaded to the cloud service.

PULSE locks and keys do not have a clock function as they do not have a battery. When a key is updated, the current time is written to the key. When the key is inserted into a PULSE lock, the lock compares the timestamp in the key with the time stored in the lock, and stores the latest one. The timestamp in the lock is then used in the audit logs. As a consequence, PULSE audit logs will not contain detailed time information.

HINT!
To access audit logs for a particular PULSE key, the key must be updated.

10 System Settings

10.1 Configuring System Settings for Logs

Some options for how logs are deleted, stored, and anonymised can be set on system level.

1) In **Settings » System Settings » Logs**, review or configure the parameters.

Parameter	Description
Audit logs	
Delete after (days)	All audit log entries will be deleted automatically the night after they have been stored in the system for the selected number of days. Default is 14 days.
Anonymise after (days)	All audit log entries will be anonymised automatically the night after they have been stored in the system for the selected number of days. This option can be disabled. Default is anonymisation after 13 days.
Operator logs	
Delete after (days)	All operator log entries will be deleted the night after they have been stored in the system for the selected number of days Default is 100 days.
System logs, incident / monitoring logs	
Delete after (days)	All entries in system logs, incident logs, and monitoring logs will be deleted automatically the night after they have been stored in the system for the selected number of days Default is 100 days.
Default settings - audit logs in PULSE	
Number of audit logs stored in sensitive door locks (*)	A PULSE lock in a sensitive door will store a selected number of audit logs. The default system setting is 1 audit log. **NOTE!** This functionality requires PULSE lock firmware 1.0.10 or newer.

Parameter	Description
Number of audit logs stored in normal door locks (*)	A PULSE lock in a normal door will store a selected number of audit logs. The default system setting is 50 audit logs. If the limit is set to 50, the oldest log will be deleted when the 51st is created. **NOTE!** This functionality requires PULSE lock firmware 1.0.10 or newer.
Audit logs when deleting users	
Two options: • Audit logs for sensitive doors will be deleted from the system. Audit logs for normal doors will be anonymised. • Audit logs will be kept according to system level settings above	-

(*) The number of audit logs can also be set on door level. As soon as the setting on door level changes or the lock is configured with the AADC app, that door level setting is the one that is valid for that PULSE lock, instead of the system setting. See Section 6.7.1 *"Configuring a Door"*, page 39 and Section 6.11 *"Programming a PULSE Lock"*, page 52.

10.2 Setting an Offline Revalidation Period

1) In **Settings » System settings » Revalidation period** area the current offline revalidation period is shown.

   The default is set to: **Offline credentials must be presented to an updater within 999 days.**

2) Click the **Edit** icon to enter edit mode and enter a new revalidation period, in number of days. Or, select **Offline credentials do not need to be revalidated**, which means that the offline credentials will never expire.

For more information, see Section 3.4 *"Access Concepts"*, page 14.

10.3 WellCom RFID Configuration

The WellCom Entry Phone units can be configured with a correct RFID key for using RFID key tags in the system.

1) In **Settings » System settings » RFID Configuration** area, any current DESFire key is shown secretly as a line of asterisks.

2) Click the **Edit** icon to enter edit mode and type the new RFID key. Up to 32 characters (0-9 and A-F only) can be entered.

   The updated welcome screen is shown in the preview to the right. Change the settings until the preview shows what you expect.

3) Click **Save**.

When the RFID key is entered and saved it is pushed out to all the WellCom units in the system. If a new WellCom unit is added later it will also receive the key when connected.

11 Appendix

11.1 Terminology

AADC	ASSA ABLOY Device Configurator, an Android application used to program PULSE locks.
Access area	Section of a floor enclosed by the door sides leading into it.
Access profile	A combination of access areas, offline door groups, and online and offline schedules. A user can be assigned any number of access profiles.
Alarm area	An alarm area is defined by the door sides leading into it. All doors of an alarm area must share the same parent Controller (InControl 3270).
Armed	The status of an external alarm zone set to trigger when detectors are activated. An alarm area follows the status of the external alarm zone.
Block	The act of blocking a user's credentials in the system.
Building	Real estate object with an OpenStreeMap address. Contains one or several floors.
Controller unit	A Controller or a Device converter.
Controller	See InControl 3270.
Credentials	Typically a card, key or tag with an electronic ID, used in combination with a PIN, to prove that a user has the right to access a door, building or other asset.
Desktop updater	USB device used with a PC to update credentials.
Disarmed	The status of an external alarm zone set not to trigger when detectors are activated. An alarm area follows the status of the external alarm zone.
Door	A physical door with hardware components, such as readers and electric strikes, to control access to an area.
Device converter	See ToConnect 3270.
Door side	Online doors and some offline doors are divided into door sides. The two door sides (1 and 2) are used to define access areas, and where applicable, alarm areas.
EAC	Electronic access control (system).
Exception day	A day that is defined as an exception in a calendar and handled separately in schedules. Could be used for holidays.

External alarm panel	The panel of the external alarm system where connections are made for inputs and outputs.
External alarm zone	A group of sensors handled separately by the alarm system.
Floor	Vertical division of a building where doors can be placed.
Hand in	The act of returning handed out credentials and removing any access rights from the credentials.
Hand out	The act of linking a user's access profile to credentials that can then be used to open doors.
Incedo™ Open system	The online and offline Incedo™ Open components of one or several buildings.
InControl 3270	Controller authorising electronic access. Communicates with up to 16 Device converters and the Incedo™ Open cloud service. Each Controller also includes a Device converter, which can be directly connected to a door.
Offline access schedule	Weekly schedule to enable or disable access rights to offline door groups based on time slots.
Offline door	The access decision handled by the lock, using information stored in the credential.
Offline door group	A group of offline doors in a building.
Online access schedule	Weekly schedule to enable or disable access rights to access areas based on time slots. Exception days are handled separately.
Online door	An online door is indirectly connected to the cloud service via a Controller. Access decisions are handled by a parent Controller, which is in regular contact with the cloud service.
Operator	An operator have login rights to the web application, and can be assigned different roles.
PAP tool	PC application used to program and configure Aperio locks.
PCB	Printed circuit board.
PIN	Personal Identification Number, a short password used to authenticate a user accessing a system, e.g. an EAC system.
PoE	Power over Ethernet, a technology to supply power to devices over Ethernet cables. PoE+ is a PoE specification.
PPD200/PPD201	See programming device.
Pre-alarm	A predefined count-down period between an arming request and the actual arming of an alarm area. Enables people to leave the alarm area before arming.

Programming device PPD200/PPD201, A USB PULSE key adapter used with AADC to program PULSE locks.

PULSE locking system The PULSE components of a building. There can be one or several PULSE locking systems per Incedo™ Open system.

Revalidation period The revalidation period defines how long an offline credential is valid after an update. It is set for the entire system, and is used for both Aperio and PULSE.

RFID Radio-frequency identification. A standardised technology that uses electromagnetic fields to identify and track RFID tags that are moved into close range from an RFID reader.

Role Defines the set of read and write privileges for an operator.

RTC Real-Time Clock.

System owner A special role for the first operator's account in a new system.

ToConnect 3270 Device converter connecting EAC components to the local network. Communicates with the parent Controller.

UPS Uninterruptable Power Supply. A device that supplies backup power to the connected electrical equipment in the event of a power outage.

User A person who uses the system, for example to open doors with handed out credentials. Can be assigned access profiles and leases.

11.2 Door Hardware Components

The hardware components and functions supported by Incedo™ Open are listed below.

Table 9. Door level functions and components

Function	Hardware I/O	Description
Electric strike (relay)	RE1-RE2 Relay board: RE3-RE8	Activates an electric strike.
Electric strike (Hi-O)	Hi-O bus	Activates and communicates with an electric strike.
Motor lock (Hi-O)	Hi-O bus	Activates and communicates with a motor lock.
External door sensor (analogue in)	IN1-IN3 Relay board: IN4-IN7	Indicates an open door. Normal mode or dual loop.
Alarm bypass (relay)	RE1-RE2 Relay board: RE3-RE8	Bypasses an external alarm sensor on normal door openings.
Pre alarm (relay)	RE1-RE2 Relay board: RE3-RE8	Activates the selected relay during the pre alarm period. External alarm function.
Alarm control (relay)	RE1-RE2 Relay board: RE3-RE8	Sends a request to arm an alarm area. External alarm function.

Function	Hardware I/O	Description
ASF, Alarm status feedback (analogue in)	IN1-IN3 Relay board: IN4-IN7	Confirms that an alarm area is armed (mormal mode or dual loop). External alarm function.
Siren	RE1-RE2 Relay board: RE3-RE8	Activates a siren for the emergency exit function.
Additional relay board	ADD-ON CARD connector	Adds relays RE3-RE8 and analogue inputs IN4-IN7 (Relay board 400RC64).

Table 10. Door side functions and components

Function	Hardware I/O	Description
Exit button (analogue in)	IN1-IN3 Relay board: IN4-IN7	Requests a door opening. Normal mode or dual loop.
Exit button (Hi-O)	Hi-O bus	Requests a door opening.
Emergency exit button	1x IN1-IN3, 1x RE1-RE2 Relay board: 1x IN4-IN7, 1x RE3-RE8	Opens an NC configured electric strike directly, and activates an analogue input (normal mode or dual loop). Emergency exit function.
Pando Display (Hi-O)	Hi-O bus	Connects a reader.
Pando Display Offline Updater (RS-485)	RS-485 bus	Connects an updater and reader.
Pando Secure (Hi-O)	Hi-O bus	Connects a reader.
Pando Mini (Hi-O)	Hi-O	Connects a reader.
Öppna readers (RS-485)	RS-485 bus	Connects a reader.
WellCom	Free RJ-45 on InControl 3270 or ToConnect 3270 Local network	Connects an entryphone.

11.3 Arming or Disarming an Alarm Area From Reader

This section describes how to arm, disarm, or delay the scheduled arming (buying time) of an alarm area from a Pando Secure reader or a Pando Display reader. One reader can never control more than one alarm area.

To control an alarm area, the user needs an access profile with the appropriate privileges. For more information, see Section 6.4 *"Adding an Access Profile"*, page 32.

1) To arm an alarm area:
   a) Press **B**.
   b) Present the credentials (card or key) to the reader.
   c) Enter the PIN.

      Depending on the alarm area configuration, the reader may indicate the alarm status.

2) To disarm or delay the scheduled arming of an alarm area:

a) Press **A**.

b) Present the credentials (card or key) to the reader.

c) Enter the PIN.

Depending on the alarm area configuration:

- The reader may indicate the alarm status
- The door unlocks after successfully disarming the alarm area.

HINT!
When a delayed scheduled arming action expires, after the buying time, the alarm area will be rearmed provided that it is still scheduled for arming.

11.4 Unlocking Using Code Only

Incedo™ Open offers the possibility to open doors with code only, using credential types of the format User code.

To use this feature, the settings for the door must allow the use of code only and the door must be equipped with a device with a keypad.

1) Enter a valid code on the reader.

WellCom Entry Phone: The door is unlocked if access is granted. No other indication whether access was granted or denied.

Pando reader: The door is unlocked if access is granted. The display indicates granted access.

2) Öppna reader: press OK button.

The door is unlocked if access is granted, and the backlight turns green. Red backlight: access denied.

ASSA ABLOY
Opening Solutions

ASSA ABLOY
Opening Solutions Sweden AB
P.O. Box 371
SE-631 05 Eskilstuna
Sweden

Customer support:
0771 640 640 (national)

Denmark:
+45 4454 4600 (multi-family and commercial)
technicalsupport.dk.openingsolutions@assaabloy.com
Norway:
+47 6924 5200 (multi-family and commercial)
technicalsupport.no.openingsolutions@assaabloy.com
Sweden:
+46 31 68 97 30 (multi-family), +46 8 775 16 60 (commercial)
technicalsupport.se.openingsolutions@assaabloy.com