Product manual

ABB i-HD

ABB i-HD management software
# Table of contents

1. Notes on the instruction manual ................................................................. 4  
2. Intended use .............................................................................................. 4  
3. Commissioning .......................................................................................... 5  
   3.1 System requirements .............................................................................. 5  
   3.2 Installing the software ............................................................................ 6  
   3.3 Initial setup ............................................................................................. 11  
   3.4 Login screen .......................................................................................... 16  
   3.5 Home screen .......................................................................................... 18  
   3.6 Settings .................................................................................................. 19  
      3.6.1 Viewing the version ........................................................................ 19  
      3.6.2 Language setting ............................................................................ 20  
      3.6.3 Third party authority settings ......................................................... 21  
      3.6.4 Abnormal devices .......................................................................... 24  
      3.6.5 Onvif IP-Camera settings .............................................................. 25  
      3.6.6 Time sync setting .......................................................................... 28  
      3.6.7 Alarm notification settings ............................................................. 30  
      3.6.8 Alarm last time settings ................................................................. 31  
      3.6.9 Agbox settings .............................................................................. 32  
4. Operation ................................................................................................... 33  
   4.1 Typical application ................................................................................ 33  
   4.2 Adding devices ...................................................................................... 34  
      4.2.1 Adding devices via scan ................................................................. 34  
      4.2.2 Adding devices manually .............................................................. 37  
      4.2.3 Importing a building structure via App ......................................... 40  
      4.2.4 Removing the devices ................................................................. 43  
   4.3 Managing the trusted devices ............................................................... 45  
      4.3.1 Managing the trusted devices for outdoor station ....................... 45  
      4.3.2 Managing the trusted devices for IP actuator .............................. 48  
      4.3.3 Emergency unlock ....................................................................... 51  
   4.4 User management ................................................................................ 55  
      4.4.1 Adding users ................................................................................ 55  
      4.4.2 Managing users ............................................................................ 57  
      4.4.3 Removing users ........................................................................... 59  
   4.5 Managing permissions ......................................................................... 60  
      4.5.1 Assigning the outdoor stations to a user ....................................... 61  
      4.5.2 Assigning the ID authentications to a user ................................. 63  
      4.5.3 Assigning the unlock passwords to a user .................................... 68  
      4.5.4 Assigning the faces to a building ................................................ 71  
      4.5.5 Removing the outdoor stations from a user .............................. 76  
      4.5.6 Removing ID authentications from a user ................................. 78  
      4.5.7 Removing the unlock passwords from a user ......................... 80  
      4.5.8 Removing the QR codes from a user .......................................... 82  
      4.5.9 Removing the faces from a building ......................................... 83  
   4.6 Configuring the devices ....................................................................... 85  
      4.6.1 Configuring the indoor station .................................................... 85
4.6.2 Configuring the outdoor station .......................................................... 98
4.6.3 Configuring the mini outdoor station .................................................. 126
4.6.4 Configuring the guard unit ................................................................. 138
4.6.5 Configuring the IP actuator ................................................................. 141
4.7 Managing the backup .............................................................................. 146
  4.7.1 Creating the backup ........................................................................... 146
  4.7.2 Restoring the backup ......................................................................... 148
  4.7.3 Removing the backup ......................................................................... 149
  4.7.4 Exporting the backup ........................................................................ 150
  4.7.5 Importing the backup ........................................................................ 151
4.8 Updating the firmware ........................................................................... 153
4.9 Restoring to factory default ..................................................................... 159
4.10 Notification ............................................................................................ 160
  4.10.1 Call list ........................................................................................... 160
  4.10.2 Unlock list ....................................................................................... 162
  4.10.3 Alarm list ......................................................................................... 164
  4.10.4 Device fault ..................................................................................... 167
  4.10.5 System log ....................................................................................... 171
4.11 Message center ...................................................................................... 173
  4.11.1 Creating a message ......................................................................... 173
  4.11.2 Replying to a message ..................................................................... 174
4.12 Cloud setting ......................................................................................... 175
  4.12.1 Log in the cloud .............................................................................. 175
  4.12.2 Log out the cloud ........................................................................... 176
  4.12.3 Exporting topology ......................................................................... 177
  4.12.4 Cloud backup or restore ................................................................. 178
  4.12.5 Reviewing the owners ..................................................................... 181
  4.12.6 Managing the residents ................................................................. 182
5 Cyber security ........................................................................................... 186
  5.1 Disclaimer ............................................................................................. 186
  5.2 Performance and service and network performance ............................. 186
  5.3 Deployment guideline .......................................................................... 188
  5.4 Upgrading ............................................................................................. 188
  5.5 Backup/restore ..................................................................................... 189
  5.6 Malware prevention solution ............................................................... 189
6 Notice ......................................................................................................... 190
1  Notes on the instruction manual

Please read through this manual carefully and observe the information it contains. This will assist you in preventing injuries and damage to property and ensure both reliable operation and a long service life for the device.

Please keep this manual in a safe place. If you pass the device on, also pass on this manual along with it. ABB accepts no liability for any failure to observe the instructions in this manual.

2  Intended use

As a part of the ABB-Welcome IP system, this device can only be used with accessories from the system
3 Commissioning

3.1 System requirements

PC performance
- Win7 and Win10 operating system are supported (2017 version or above is recommended).
- Windows Home version is not supported.
- CPU speed cannot be less than 1GHz.
- Memory cannot be less than 4GB; 8GB or above is recommended.
- The disk space is not less than 1TB.

User interface
Commissioning is always carried out via the browser.
The recommended browsers are:
- Firefox (from version 9)
- Google Chrome
- Safari

Welcome app
For the installation of the Welcome App you require a smartphone or tablet with an Android (from 4.0) or iOS (from iOS 7) operating system.
3.2 Installing the software

**Note**
The old version needs to be uninstalled before installing a new version.

Uninstalling the old version

**Warning**
All the data including the certificates will be cleared when you uninstall the management software. Please create a backup and export to the other folder on the PC.

**Note**
If the management is installed the first time, uninstall operations can be ignored.

Please follow the steps below:

1. On the PC management software catalog, double click to run "Stop.bat".
2. On the same catalog, double click to run "unins000.exe".
3. Make sure the PC management software catalog has been removed from the PC.
Installing a new version

Please follow the steps below:

[1] On the PC, double click to run "pcmgr-setup_Vx.x_yyyymmdd.exe".
[2] Select the language from the drop-down list.
[3] Click "OK".
[4] Click "Next".
[5] Click "I accept the agreement".
[6] Click "Next".
[7] Click "Next".
[8] The system default is c disk, you can click "Browse" to change a new folder.
[9] Click "Next".
[10] Click "Next".
[11] Click "Install" and click "Finish" after the installation is complete.
3.3 Initial setup

**Note**
Please insert the USB key before the initial setup. This USB key cannot be plugge out when the program is running.

Double click the program icon " " to run the program. A DOS window will be displayed on the screen. Do not close this DOS window to ensure the program is carried out normally.

And a URL "127.0.0.1" will be displayed on the screen. Click "Advance".
Then click "Proceed to ..." to access the security webpage.

Now follow the steps below:
[1] Choose language
[2] Accept end user licence

[4] Accept data privacy

Data privacy

We take the protection of your personal data very seriously and follow the legally valid regulations regarding data protection. Please take a look at our data protection policy.

https://www.ourwebsite.com/data-protection-policy

I accept the data privacy

[ ]

[5] Create an account

Please create your account

Username: admin
Password: ********
Confirm: ********
[6] Choose building type
Please select "Functional" for multi-apartment application.
Or select "Residential" for single-house application.

[7] Check the settings
3.4 Login screen

After initial setup, you can access the login screen of "PC management software" using the admin user. The login screen will be different according to the number of admin users.

The number of admin users <6

If the number of users is <6, a name list is displayed on the screen. Enter the password on the right of the user name to continue.

![Login Screen](image)
The number of admin users ≥ 6

If the number of users is ≥ 6, no name list is displayed on the screen. You need to enter the user name and the password to continue.
3.5 **Home screen**

Home screen is displayed if you login successfully.

<table>
<thead>
<tr>
<th>No.</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Message center</strong></td>
</tr>
<tr>
<td></td>
<td>Manage the messages between the indoor stations and &quot;PC management software&quot;.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Emergency unlock</strong></td>
</tr>
<tr>
<td></td>
<td>Click to release all the locks in the event of an emergency.</td>
</tr>
<tr>
<td></td>
<td>see chapter 4.3.3 “Emergency unlock” on page 51.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Searching the devices</strong></td>
</tr>
<tr>
<td></td>
<td>Click to search all devices on the same network automatically.</td>
</tr>
<tr>
<td></td>
<td>see chapter 4.2 “Adding devices” on page 34.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Import building structure</strong></td>
</tr>
<tr>
<td></td>
<td>Click to import the building structure created in the Welcome App.</td>
</tr>
<tr>
<td></td>
<td>see chapter 4.2 “Adding devices” on page 34.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Notification</strong></td>
</tr>
<tr>
<td></td>
<td>View call records, unlock records, alarm records and device fault message.</td>
</tr>
<tr>
<td>6</td>
<td><strong>User management</strong></td>
</tr>
<tr>
<td></td>
<td>Manage the users in the system.</td>
</tr>
<tr>
<td>7</td>
<td><strong>Device management</strong></td>
</tr>
<tr>
<td></td>
<td>Manage the devices in the system.</td>
</tr>
<tr>
<td>8</td>
<td><strong>User account</strong></td>
</tr>
<tr>
<td></td>
<td>Click to change the password of the current user account or log out.</td>
</tr>
<tr>
<td>9</td>
<td><strong>Preferences</strong></td>
</tr>
<tr>
<td></td>
<td>Click to change the settings of the devices.</td>
</tr>
</tbody>
</table>
3.6 Settings

3.6.1 Viewing the version

On the "Preferences" screen, click "System information" to view the firmware information.
3.6.2 Language setting

On the “Preferences” screen, click “Language”, then select the language from the drop-down list.
3.6.3 Third part authority settings

The 3rd party needs to get authority before obtaining the data (e.g. unlock records) from "PC management software".

On the "Preferences" screen, click "3rd party authority" to access the corresponding screen. Please follow the steps below:

1. On the "3rd party authority" screen, click "Add".
2. Click "Browse" to select the certificate sent from the 3rd party.
3. Enter the name for this certificate.
4. Click "Save".
[5] Click "View".
[6] Click "Download the certificate".
[7] Click "Cancel" to go to the previous screen.
[8] Click "Download the root certificate".

[9] Send both certificates to the 3rd party for their next setting.
### 3.6.4 Abnormal devices

On the "Preferences" screen, click "Abnormal devices" to view the error description (e.g. "Device signed failed").

You can check the device when "Device signed failed" appears on the abnormal devices list.

- Has the device been signed before?
- Does the device work in safety mode?
- Does the IP address of the device conflict with other devices?
3.6.5 Onvif IP-Camera settings

On the “Preferences” screen, click “Onvif IPC list” to access the corresponding screen. Please follow the steps below:

[1] On the "Onvif IPC list" screen, click “Search device” to search the cameras used for the public network. The IP addresses of the cameras should be set to the segment 10.x.x.0 before use.

[2] Click "Enter credentials".
[3] Enter the user name and the password of the camera
[4] Click "Pair".
[5] "Paired" is displayed on the screen if successful.

```
<table>
<thead>
<tr>
<th>Preferences</th>
<th>Onvif IPC list</th>
</tr>
</thead>
<tbody>
<tr>
<td>System info</td>
<td>Search device</td>
</tr>
<tr>
<td>Language</td>
<td></td>
</tr>
<tr>
<td>Project Backup</td>
<td></td>
</tr>
<tr>
<td>3rd party auth</td>
<td></td>
</tr>
<tr>
<td>Abnormal devices</td>
<td></td>
</tr>
<tr>
<td>Onvif IPC list</td>
<td></td>
</tr>
<tr>
<td>Misc Settings</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP address</th>
<th>Name</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.19</td>
<td>DCS-2330</td>
<td>Paired</td>
<td>Update credentials</td>
</tr>
</tbody>
</table>
```
You need to download the list onto the indoor station before viewing the camera in the drop-down list. Please see the indoor station product manual for more details.
3.6.6 Time sync setting

**Note**
PC time must be set correctly before use. If PC time is not correct, some devices will not work normally after synchronization. The device to be synchronized needs to enable the "Sync time with PC management software" function before use.

On the "Preferences" screen, click "Misc Settings" to access the corresponding screen. There are 2 options to sync time with the devices on the system.

1. Sync time automatically

Please follow the steps below:

[1] Click to enable "Automatically".

[2] Enter the sync period (1-24). The default is 1 hour.

[3] Click "Apply" to take effect.
2. Sync time manually
Please follow the steps below:
[1] Click to enable "Manual".
[2] Click "Apply" to take effect immediately.
3.6.7  Alarm notification settings

On the "Preferences" screen, click "Misc Settings" to access the corresponding screen. Please follow the steps below:

[1] On the "Misc settings" screen, tick the checkbox to enable the function. "Enable sound notification" function and "Enable popup notification" function are only available when "Alarm when device goes offline" is enabled.

[2] Tick/untick the checkbox to enable/disable the notification function.

[3] Click "Apply". After the function is enabled, "PC management software" will receive an alarm when the device goes offline. see chapter 4.10 "Notification" on page 160.

Note
The alarm is reported via outdoor station 1 (device ID=1) or via gate station 1 (device ID=1). If either of these two devices cannot be detected in the system, the alarm cannot be reported to "PC management software" successfully.

Note
To set the alarm last time, see chapter 3.6.8 "Alarm last time settings" on page 31.
3.6.8  **Alarm last time settings**

On the "Preferences" screen, click "Misc Settings" to access the corresponding screen. Please follow the steps below:

[1] On the "Misc settings" screen, enter the alarm last time (1-30).

[2] Click "Apply".
3.6.9 Agbox settings

Note
Currently, this function is only used in Shanghai, China. This function is disabled by default.

On the "Preferences" screen, click "Misc Settings" to access the corresponding screen. Please follow the steps below:

[1] Click to enable the function.
[2] Enter the IP address of the designated Agbox.
[3] Enter the key number of the designated Agbox.
[4] Enter the interval time (1-60).
[5] Click "Save".
4 Operation

4.1 Typical application

"PC management software" can be used to manage all the devices in the building. In this case, "PC management software" should be set to "Functional" on the initial setup. See chapter 3.3 “Initial setup” on page 11.
4.2 Adding devices

4.2.1 Adding devices via scan

**Note**
Only the devices on the same network segment as "PC management software Point" can be auto searched. Please see the devices surrounded by a red box on the diagram below. *Slave indoor station* cannot be added via auto-search.

**Precondition**

- All the devices must be powered on.
- All the devices must be set a different physical address.
- None of the devices should be signed by other "PC management software". If the devices have been signed by others, you will need to clear the signature e.g. changing the physical address of the device.
Adding the devices via auto-search

Please follow the steps below:

[1] On the home screen, click " ".
[2] Click "√" to continue.
[3] Search result is display on the screen, click "√".
[3] The devices are displayed on the screen if successful.
4.2.2 Adding devices manually

**Note**
All the devices can be added on "PC management software" manually. "Slave indoor stations" can be added in this way.

**Precondition**
- All the devices to be added manually must be powered on.
- None of the devices to be added manually should be signed by other "PC management software". If the devices have been signed by other "PC management software", you need to clear the signature e.g. changing the physical address of the device.

**Adding the devices manually**
Please follow the steps below:

[1] On the home screen, click "Device management" to access the corresponding screen.

**Note**
The following operations show you how to add a master indoor station. Please adjust your operations according to the actual devices.

[3] Select a device type from the drop-down list (e.g. "Indoor station").
[8] Enter serial number.
[9] Click “Save” to save.
[10] Click "√".
4.2.3 Importing a building structure via App

"PC management software" can import building structure from Welcome App. It is allowed to import one building or several buildings in batch.

**Importing rule**

Building structure will be overwritten according to the building no.

<table>
<thead>
<tr>
<th>APP buildings</th>
<th>SmartAP original buildings</th>
<th>SmartAP final buildings</th>
</tr>
</thead>
<tbody>
<tr>
<td>B+</td>
<td>A, B, C</td>
<td>A, B+, C</td>
</tr>
<tr>
<td>B+, C+</td>
<td>A, B, C</td>
<td>A, B+, C+</td>
</tr>
<tr>
<td>D, E, F</td>
<td>A, B, C</td>
<td>A, B, C, D, E, F</td>
</tr>
</tbody>
</table>

+ means building structure has been changed.

**Connection**

Welcome App must be in the same network with the router connected to "PC management software".
Operation

On the SmartAP home screen, click "", a pop-up window will appear.
On the "Projects" screen of the APP, swipe the project name to the right, click "  ", select a designated SmartAP and enter the account and password of SmartAP, then click "Log in".

On the configuration screen of SmartAP, a pop-up window shows the importing status.
4.2.4 Removing the devices

Please follow the steps below:

[1] On the home screen, click "Device management".
[2] Click the designate device type (e.g. "Indoor stations").
[3] Click " ".

![Device management screen](image)
[4] Click "Select all" to select all devices or click the designated device one by one to select multiple devices.

[5] Click "Delete".

[6] Click "Confirm".
4.3 Managing the trusted devices

4.3.1 Managing the trusted devices for outdoor station

If you want to release the lock on the outdoor station via the indoor station/guard unit, you need to check:

- If the indoor station/guard unit and the outdoor station have been signed on "PC management software".
- If the indoor station/guard unit has been added to the trusted list of the outdoor station.

Please follow the steps below to add the trusted list:

1. On the "Device management" screen, click "Outdoor stations".
2. Click the designated outdoor station.
[3] Scroll down the list and click "List of trusted devices".
[4] Click "Add trusted devices".
[5] Tick the check boxes to select the devices to be trusted.
[6] Click "✓" to confirm.
[7] The result is displayed on the screen.
[8] Click "Save" to save.
4.3.2 Managing the trusted devices for IP actuator

If you want to release the lock on the IP actuator via the indoor station/guard unit/outdoor station, you need to check:

- If the indoor station/guard unit/outdoor station and the IP actuator have been signed on "PC management software".
- If the indoor station/guard unit/outdoor station has been added to the trusted list of the IP actuator.

Please follow the steps below to add the trusted list:
[1] On the "Device management" screen, click "IP actuator".
[2] Click the designated IP actuator.
[3] Click "List of trusted devices".
[4] Click "Add trusted devices".
[5] Tick the check boxes to select the devices to be trusted.
[6] Click "✓" to confirm.
[7] The result is displayed on the screen.
[8] Click "Save" to save.
4.3.3 **Emergency unlock**

In some emergency cases, you may need to release designated doors. To achieve this, you need to add the designated outdoor stations and the designated public IP actuators to "PC management software".

**Adding the trusted devices**

Please follow the steps below:

1. On the "Device management" screen, click the device type (e.g. "Outdoor stations").
2. Click the designated device.
3. Scroll down the list and click "List of trusted devices".
[4] Click to enable "Trust this management software".
[5] The result is displayed on the list.
[6] Click "√" to save.
Releasing the designated doors

Please follow the steps below:

1. On the configuration screen, click "SOS".
2. Enter the password for current admin user.
3. Click "Unlock all public doors".
4. The result status is displayed on the screen.
Closing the designated doors

Please follow the steps below:

[1] On the configuration screen, click "SOS".
[2] Enter the password for the current admin user.
[3] Click "Lock all public doors".
[4] The result status is displayed on the screen.
4.4 User management

4.4.1 Adding users

1. Adding admin users

Please follow the steps below:

[1] On the "User management" screen, click "Add user".
[2] Select the user role as "Admin".
[3] Enter the user name.
[4] Enter the first name, last name
[5] Enter the password twice.
[6] Click "√" to save.
2. Adding basic users

Please follow the steps below:

[1] On the "User management" screen, click "Add user".
[2] Select the user role as "Basic".
[3] Enter the user name.
[4] Enter the first name, last name
[5] Click "✓" to save.

Note
A maximum of 20,000 users can be added on the system.
4.4.2 **Managing users**

Please follow the steps below to edit user information:

1. On the "User management" screen, click the designated user.
2. Click "Edit user account".
[3] Rename the first name and last name.
[4] Click "✓" to save.
4.4.3 Removing users

On the designated user screen, follow the steps below:

[1] On the "User management" screen, click the designated user.

[2] Click " ".

[3] Click " √ " to confirm.
4.5 Managing permissions

Releasing the locks on the outdoor stations

There are 4 options for you to release the locks on the designated outdoor stations.

1. Releasing the locks via the ID authentications
   Please follow the steps below:
   [1] Assigning the ID authentications to a user, see chapter 4.5.2 “Assigning the ID authentications to a user” on page 63.
   [2] Assigning the outdoor station to the user, see chapter 4.5.1 “Assigning the outdoor stations to a user” on page 61.

2. Releasing the locks via the unlock passwords
   Please follow the steps below:
   [1] Assigning the unlock passwords to a user, see chapter 4.5.3 “Assigning the unlock passwords to a user” on page 68.
   [2] Assigning the outdoor station to the user, see chapter 4.5.1 “Assigning the outdoor stations to a user” on page 61.

3. Releasing the locks via the registered faces
   You can assign the designated outdoor stations and all the gate stations to the designated faces when adding them. see chapter 4.5.4 “Assigning the faces to a building” on page 71.

4. Releasing the locks via the QR codes
   Please follow the steps below:
   [1] A user will be created when you create QR code on Welcome App. See the ”Welcome App” product manual for more details.
   [2] Assigning the outdoor station to this user, see chapter 4.5.1 “Assigning the outdoor stations to a user” on page 61.
4.5.1 Assigning the outdoor stations to a user

**Note**  
If the outdoor stations are assigned to a user, the locks of these outdoor stations can be released by this user.

Please follow the steps below:

[1] On the "User management" screen, click the designated user to access the corresponding screen.

[2] Click "Doors".
[3] Click the designated outdoor station on the "Not assigned" section.
[4] Click "√" to confirm.

Repeat steps from 3-4 to assign the outdoor stations one by one.
4.5.2 Assigning the ID authentications to a user

Please follow the steps below:

[1] On the “User management” screen, click the designated user to access the corresponding screen.

[2] Click “User card”.

Please select a category to assign the user to.

Indoor flight, doors, tags and keycards.
[3] Click "Add authentication".
[4] Set card type to "Keycard/Tag".
[5] Set validity period, there are 3 options:
   - Unlimited validity, if this type is selected, you can continue to the next step.
   - Limited validity, if this type is selected, you need to set the start date and end date by clicking "  ".
   - Special period, if this type is selected, you can set the special period (e.g. "Working days", "Non-working days" and festivals). And you can even set the validity period to a certain days of the week.
[7] Set "Registered by" to "Outdoor station" or "Card register".
[8] If "Registered by Outdoor station", select the designated outdoor station from the drop-down list for swiping the ID authentications. If "Registered by Card register", COM part is displayed automatically. If "Encrypt" is enabled, only IC cards with secret key can be supported.

**Note**
For higher security, it is recommended to enable the "Safe mode" function on the designated IP touch 5 outdoor station when registering the ID authentications.

[9] Click "+" to select the floors related to the lift control (optional).
[10] Click "√" to continue.
Operation
[11] Swipe the keycard or tag in front of the outdoor station or the card register.
[12] The outdoor station or the card register will sound a beep if successful.
Repeat steps 11 to register the ID authentications one by one.
IC card specification

<table>
<thead>
<tr>
<th>Operating frequency</th>
<th>13.56 MHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>ISO 14443A</td>
</tr>
<tr>
<td>Support card</td>
<td>Mifare one S50/S70, Mifare desfire EV1/EV2</td>
</tr>
<tr>
<td>Output format</td>
<td>Wiegand 26/34 bit</td>
</tr>
</tbody>
</table>

ID card specification

<table>
<thead>
<tr>
<th>Operating frequency</th>
<th>125 KHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>ISO18000-2</td>
</tr>
<tr>
<td>Support card</td>
<td>EM4100, EM4205, EM4305, EM4450, TK4100, T5567</td>
</tr>
<tr>
<td>Output format</td>
<td>Wiegand 26/34 bit</td>
</tr>
</tbody>
</table>

Note
Up to 500 ID authentications can be assigned to one user.

[13] The registered ID authentications are displayed on the screen.
4.5.3 Assigning the unlock passwords to a user

Please follow the steps below:

[1] On the "User management" screen, click the designated user to access the corresponding screen.

[2] Click "User card".
[3] Click "Add card".
[4] Set card type to "Password".
[5] Enter the name for the password.

Note
This user name cannot be the same as the existing user name on "PC management software".


Note
This password cannot be the same as the existing password on "PC management software".

[7] Set the lock type.
[8] Set validity period, there are 2 options:
  - Unlimited validity, if this type is selected, you can continue to the next step.
  - Limited validity, if this type is selected, you need to set the start date and end date by clicking "  ".

[9] Set unlock times.
[10] Click "+" to select the floors to be controlled by the ID authentications (optional).
[12] The registered password is displayed on the screen.
4.5.4 Assigning the faces to a building

Adding the faces

There are 2 ways to add the faces.

1. Adding the faces one by one

   Please follow the steps below:
   [1] On the "User management" screen, click "Faces" to access the corresponding screen.
   [2] Click "Add face".

![User management screen](image)
[3] Enter the name.
[4] Enter the building number.
[5] Enter the room number.
[6] Enter the telephone number.
[7] Click to select the lock to be released when the face is recognized.
[8] If “All door privilege” is enabled, this face can release all the doors in the system. Otherwise, this face can only release the lock on the designated outdoor station set on step 4.
[9] Click “Browse” to select the designated face.
[10] Set validity period, there are 2 options:
  - Unlimited validity, if this type is selected, you can continue to the next step.
  - Limited validity, if this type is selected, you need to set the start date and end date by clicking “”.
[11] Click “+” to select the floors related to the lift control (optional).
[12] Click “√” to save.

Note
The picture for face registration should be light natural, no overexposure; no occlusion of the face, no makeup, the face area resolution is not less than 200 * 200 image pixels and the face should be as straight as possible.

Note
The faces added via this way can release the locks on the designated outdoor station and all gate stations.
2. Adding the faces in a batch

Please follow the steps below:

[1] On the "Faces" screen, click "Import faces".
[2] Click "Browse" to select the face pictures.
[3] Set validity period, there are 2 options:
   - Unlimited validity, if this type is selected, you can continue to the next step.
   - Limited validity, if this type is selected, you need to set the start date and end date by clicking " „.
[4] Click "√ " to save.

Note

The faces added via this way can release all the locks on the outdoor stations and the gate stations.
3. Editing the faces

Please follow the steps below:

[1] Click to select the criteria from the drop-down list, e.g. "People name".
[2] Enter the search key, e.g. "User1".
[3] Click "Query".
[4] The search result is displayed on the screen, click "Edit". "✓" indicates the picture has been verified. Select the specified units, click "Sync" to sync the face data to other outdoor stations when needed (e.g. replace a new outdoor station).
[5] Edit the data and click "✓" to save the change.
4.5.5 Removing the outdoor stations from a user

Note
If you remove the outdoor station from a user, the ID authentications, the unlock passwords and the QR codes assigned to this user cannot release the lock on this outdoor station any more.

Please follow the steps below:

[1] On the "User management" screen, click the designated user to access the corresponding screen.

[2] Click "Doors".
[3] Click the designated outdoor station on the "Assigned" section

[4] Click "√" to confirm.

Repeat steps from 3-4 to remove the designated outdoor stations one by one.
4.5.6 Removing ID authentications from a user

Please follow the steps below:

[1] On the "User management" screen, click the designated user to access the corresponding screen.

[2] Click "User card".
[3] Click the designated ID authentication.
[4] Click "Delete card".
[5] Click "√" to confirm.

Repeat steps from 3-5 to remove the designated ID authentications one by one.
### 4.5.7 Removing the unlock passwords from a user

Please follow the steps below:

1. On the "User management" screen, click the designated user to access the corresponding screen.

2. Click "User card".
[3] Click the designated unlock password.
[4] Click "Delete card".
[5] Click "✓" to confirm.

Repeat the steps from 3~5 to remove the unlock passwords one by one.
4.5.8 Removing the QR codes from a user

Welcome App can create QR codes for the user to release the lock on the outdoor station. For creating a QR code, see the product manual for Welcome App. “PC management software” can remove the QR code.

Please follow the steps below:

[1] On the designated user screen, click the QR code.
[3] Click "🗑".
[4] Click "√" to remove the QR code.
4.5.9 Removing the faces from a building

1. Removing a face

Please follow the steps below:

[1] On the "Faces" screen, click to select a criterion from the drop-down list, e.g. "People name".
[2] Enter the search key, e.g. "User1".
[3] Click "Query".
[4] The search result is displayed on the screen, click "Delete", followed by "√".
2. Removing multiple faces in a batch

Please follow the steps below:

[1] On the “Faces” screen, click to select multiple users or using a criterion to filter the users.

4.6 Configuring the devices

4.6.1 Configuring the indoor station

Access the designated indoor station screen

Please follow the steps below:

[1] On the home screen, click "Device management".
[2] Click "Indoor stations".
[3] Click the designated indoor station to access the corresponding screen.
1. Changing the language

Please follow the steps below:

[1] On the designated indoor station screen, click "Language".
[2] Select the language from the drop-down list.
[3] Click "√" to save.
2. Renaming the device

Please follow the steps below:

[1] On the designated indoor station screen, click "Resident(s)/Tenant(s)".
[2] Enter the first name.
[3] Enter the last name or the company name.

**Note**
If the resident has multiple indoor stations in the apartment, it is recommended to use the appropriate name to show the association (e.g. "Master", "Slave 1" etc.).

[4] Click "√" to save.
[5] Click "√" to confirm.
3. Viewing the serial number

Please follow the steps below:

[1] On the "Indoor stations" screen, click the designated indoor station.
[2] The serial number is displayed on the screen. It is recommended to write down the serial number for further use.
4. Managing the physical address

Note
If the master indoor station changes its physical address, the slave indoor stations need to obtain the signature again from "PC management software". Please write down the serial number of the slave indoor stations before changing the physical address.

This function is only available for the master indoor station.

Please follow the steps below:

[1] On the designated indoor station screen, click "Physical addr.".
[2] Change the physical address.
[3] Click "√" to save.
[4] Click "√" to confirm.

If there are no slave indoor stations, the change process is completed at step 4. Otherwise, please continue with the next steps.

[5] Click " " to turn back to "Indoor stations" screen.
[6] Click the slave indoor station.

[7] The slave indoor station failed to access the screen due to the signature is removed automatically. Click "√" to continue.

[8] On the "Indoor stations" screen, click "√".
[9] Click the slave indoor station.
[10] Click "Delete".
[11] Click "Confirm", followed by "√".
[12] On the "Indoor stations" screen, click "Add device".
[13] Set "Device type" to "Indoor station".
[14] Enter the new physical address of the slave indoor station.
[15] Enter the serial number of the slave indoor station.
[16] Click "Save", followed by "√".
[17] Rename the slave indoor station.
5. Managing the logic address

This function is only available for the master indoor station.

Please follow the steps below:
[1] On the designated indoor station screen, click "Logic addr."
[2] Enter the logic address. The address could not be the same to the exist one on "Smart Access Point".
[3] Click "√" to save.
[4] Click "√" to confirm.

Note
The logic address set on the indoor station can be used on the outdoor station.
6. Managing the screensaver

This function is only available for the master indoor station.

Please follow the steps below:

[1] On the designated indoor station screen, click "Screensaver".
[2] Click "Upload screensaver image".
[3] Click "Browse" to select the designated image (only .jpg is supported, maximum resolution of the image is 1024 x 600 pixels).
[4] Click "✓" to confirm.
[5] Click "✓" to upload.
7. Managing the floorplan

This function is only available for the master indoor station.

Please follow the steps below:

[1] On the designated indoor station screen, click "Floor plan".
[2] Click "Upload floorplan".
[3] Click "Browse" to select the designated image (only .jpg is supported, maximum resolution of the image is 1024 x 600 pixels).
[4] Click "√" to confirm.
[5] Click "√" to upload.
8. Duplicating the settings

This function is only available for the master indoor station.

Please follow the steps below:

[2] Click to select the designated indoor station to be duplicated.
[3] Tick the check boxes to select the settings to be duplicated.
[4] Click “√” to confirm.
4.6.2 Configuring the outdoor station

Access the designated outdoor station screen

Please follow the steps below:

[1] On the home screen, click "Device management".
[2] Click "Outdoor stations".
[3] Click the designated outdoor station to access the corresponding screen.
1. Changing the language

Please follow the steps below:

[1] On the designated outdoor station screen, click "Language".
[2] Select the language from the drop-down list.
[3] Click "✓" to save.
2. Viewing the serial number

Please follow the steps below:


[2] The serial number is displayed on the screen. It is recommended to write down the serial number for further use.
3. Managing the physical address

On the designated outdoor station screen, click "Physical address".

There are 3 types devices for selection.

[1] Outdoor station
If the "Device type" is set to "Outdoor station", you need to set the block number and the device number.
[2] Gate station
If the “Device type” is set to “Gate station”, you need to set the block number and the device number.

[3] Second-confirm station
If the “Device type” is set to “Second-confirm station”, you need to set the block number, the floor number, the room number and the device number.

Note
Only an IP pushbutton outdoor station can be set to "Second-confirm station".
4. Unlock setting

Please follow the steps below:

[1] On the designated outdoor station screen, click "Door lock setting".
[2] Set the unlock time for the locks.
[3] Set the lock type for the locks.
[4] Click "√" to save.
5. Time synchronization

Please follow the steps below:

[1] On the designated outdoor station screen, click "Time synchronization".

[2] Tick the check box to enable the function.

[3] Click "√" to save.

[4] Click "√" to confirm.

After the setting, the outdoor station can synchronize its time with "PC management software".
6. Managing Lift control

Please follow the steps below:

[1] On the designated outdoor station screen, click "Lift control".
[2] Tick the check box to enable the function.
[3] Enter the floor where the outdoor station is located.
[4] Click "√" to save.
[5] Click "√" to confirm.
7. Initiating a call via physical address

This chapter applies to the IP touch 5 outdoor station and IP keypad outdoor station.

Please follow the steps below:

[1] On the designated outdoor station screen, click "Call type".
[2] Disable the "Name list" (only applied to IP touch 5 outdoor station).
[3] Set "Call type" to "Physical addr.".
[4] Click "√" to save.
8. Initiating a call via logic address

This chapter applies to the IP touch 5 outdoor station and IP keypad outdoor station.

**Adding the logic address**

Please follow the steps below:

[1] On the designated outdoor station screen, click "Call type".
[2] Disable the "Name list" (only applies to the IP touch 5 outdoor station).
[3] Set "Call type" to "Logic addr."
[4] Click "✓" to save.
[5] Click "✓" to confirm.
[6] "Logic addr. list" is displayed on the screen. Click it to continue.
[7] On the "Logic addr. list" screen, click "+".
[8] Click "Select indoor station".
[9] Click to select the designated indoor station.
[10] Click "Confirm".
[11] The indoor station is added to the list.
[12] The logic address is imported to the list.
[13] Click "✓" to save, followed by "✓" to confirm.
Repeat steps 7-13 to add the logic address one by one.
**Importing the logic addresses**

Please follow the steps below:

[1] On the "Logic addr. list" screen, click "Import logic addr. list entries".

**Note**

It is recommended to set the logic address for the indoor station before importing.

[2] Click to select the designated indoor stations.

[3] Click "Import", followed by "√".
[4] The logic addresses are imported to the list.
[5] Enter the key word to filter the search results.
Copying the logic address list to another outdoor station

Please follow the steps below:

[1] On the "Logic addr. list" screen, click "Copy logic addr. list to other OS".
[2] Click to select the designated outdoor stations.
[3] Click "Import", followed by "√".
[4] The logic address list is copied to the other outdoor station.
Removing the logic address

Please follow the steps below:

[1] On the "Logic addr. list" screen, click the designated logic address.

[2] Click "", followed by "√" to confirm.

Note

You can also click "Remove all logic addr. list" to clear all logic addresses.
9. Initiating a call via the name list

This chapter only applies to the IP touch 5 outdoor station.

**Importing the name list**

Please follow the steps below:

[1] On the designated outdoor station screen, click "Call type".

[2] Enable the "Name list".

[3] Click "√" to save.

[4] Click "√" to confirm.
[5] On the designated outdoor station screen, click "Name list".

**Note**
It is recommended to set the name for the indoor stations before importing.

[6] Click "Import name list entries".
[7] Click to select the designated indoor stations.
[8] Click "Import", followed by "√" to confirm.
[9] The names are imported to the list.
[10] Enter the key word to filter the search result.
[11] Click the designated name.
[12] Click "Upload logo image".
[13] Click "Browser" to select a logo image (only .jpg is supported. Maximum resolution is 60 x 60 pixels).
[14] Click "✓" to confirm.
[15] The logo is displayed in the list.
[16] Click "✓" to save.
[17] The logo is displayed on the outdoor station screen.
Copying the name list to other outdoor station

Please follow the steps below:

[1] On the "Name list" screen, click "Copy name list to other OS".

[2] Click to select the designated outdoor stations (only supports the IP touch 5 outdoor station).

[3] Click "Import", followed by "√".
[4] The name list is copied to the other outdoor station.
Removing the logic address

Please follow the steps below:

[1] On the "Logic addr. list" screen, click the designated logic address.

[2] Click "🗑️", followed by "√" to confirm.

Note

You can also click "Remove all entries" to clear the name list.
10. Managing the welcome message

This chapter only applies to the IP touch 5 outdoor station.
Please follow the steps below:

[1] On the designated outdoor station screen, click "Welcome message".
[2] Enter the message (not more than 32 characters).
[3] The result is displayed on the outdoor station screen.
[4] Click "√" to save.
11. Managing the developer information

This chapter only applies to IP touch 5 outdoor station.

Please follow the steps below:

[1] On the designated outdoor station screen, click "Bulletin".
[2] Click "Developer information".
[3] Select "Image" or "Text" from the drop-down list.
[4] Click "Upload image/logo" to select the image (e.g. company logo) or enter the text (pay attention to the content displayed on the screen to avoid abnormal long words).
12. Managing the bulletin

This chapter only applies to the IP touch 5 outdoor station.

Please follow the steps below:
[1] On the designated outdoor station screen, click "Bulletin".
[2] Click "Bulletin".
[3] Click "Add bulletin page" to select the image.
13. Managing the unlock method

This chapter only applies to the IP touch 5 outdoor station.

Please follow the steps below:

[1] On the designated outdoor station screen, click "Unlock mode setting”.
[2] Tick/untick the check boxes to enable/disable the functions.
[3] Click "✓" to save.
14. Cloud settings
This chapter applies to FROS 5 & FROS 10 only.

Please follow the steps below:

[1] On the designated outdoor station screen, click "Cloud settings".
[2] A QR code is displayed.
[3] Scan the QR code in the Maintenance App, bind the community with the outdoor station. Please contact ABB after-sales about the Maintenance App.
[4] Click "Cloud settings" again, the popup window shows "Binded".
4.6.3 Configuring the mini outdoor station

Access "Mini outdoor station" screen

Please follow the steps below:

[1] On the "Main menu" screen, click "Device management".
[2] Click "Outdoor stations".
[3] Click the designated mini outdoor station.
1. Basic information

On the designated mini outdoor station screen,

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Display the device type</td>
</tr>
<tr>
<td>2</td>
<td>Display the physical address</td>
</tr>
<tr>
<td>3</td>
<td>Display the serial number</td>
</tr>
<tr>
<td>4</td>
<td>Display the version</td>
</tr>
</tbody>
</table>
2. Configuring the physical address

On the designated mini outdoor station screen, click "Physical addr."

There are 2 kinds of device types.

[1] Outdoor station

If the "Device type" is set to "Outdoor station", you need to enter the block number and the device number.
[2] Second-confirm station

If the "Device type" is set to "Second-confirm station", you need to enter the block number, floor number, room number and the device number.
3. Card mode setting

Please follow the steps below:

[1] On the designated mini outdoor station screen, click "Card mode setting".

[2] If "Encrypted IC card" is enabled (system default), only the IC cards with secret key can be supported on the outdoor station.

[3] Click "Save".
4. Door lock setting

Please follow the steps below:

[1] On the designated mini outdoor station screen, click "Door lock setting".

[2] Select lock type for the "Default lock" and the "Subsidiary lock". It can be set to "Lock-GND", "NO-NC-COM" or "IPA". If "IPA" is selected, the data e.g. lock type and IPA address is needed.

[3] Set the unlock time.

[4] Click "Save".
5. Time synchronization

Please follow the steps below:

[1] On the designated mini outdoor station screen, click "Time synchronization".

[2] Tick/untick the check box to enable/disable the function. If the function is enabled, the mini outdoor station will sync its time with the time of PC management system.

[3] Click "Save".
6. Language

Please follow the steps below:

[1] On the designated mini outdoor station screen, click "Language".
[2] Select the language from the drop-down list.
[3] Click "Save".
7. Local firmware update

Please follow the steps below:

[1] On the designated mini outdoor station screen, click "Local firmware update".
[4] Click "Firmware update".
8. Online firmware update

Please follow the steps below:

[1] On the designated mini outdoor station screen, click "Online firmware update".
[3] Click "Firmware update".
9. List of trusted devices

If you want the indoor station to release the lock on the mini outdoor station, you need to add the indoor unit to the trusted list of the mini outdoor station.

Please follow the steps below:

[1] On the designated mini outdoor station screen, click "List of trusted devices".

[2] Click "Add trusted devices".
[3] Select the designated indoor station.
[4] Click "√".
[5] If “Trust this management software” is enabled, the lock on this outdoor station will be released in an emergency case (optional).
[6] Click "Save".
4.6.4 Configuring the guard unit

Access the designated guard unit screen

Please follow the steps below:

[1] On the home screen, click "Device management".
[2] Click "Guard units".
[3] Click the designated guard unit to access the corresponding screen.
1. Setting the device number

Please follow the steps below:

[1] On the designated guard unit screen, enter a new device number.
[2] Click "√" to save.
[3] Click "√" to confirm.
2. Viewing the serial number

Please follow the steps below:

[1] On the designated guard unit screen, the serial number is displayed on the screen. It is recommended to write down the serial number for further use.
4.6.5 Configuring the IP actuator

Accessing the designated IP actuator screen

Please follow the steps below:

[1] On the home screen, click "Device management".
[2] Click "IP actuators".
[3] Click the designated IP actuator to access the corresponding screen.
1. Viewing the serial number

Please follow the steps below:

[1] On the designated IP actuator screen, the serial number is displayed on the screen. It is recommended to write down the serial number for further use.
2. Managing the physical address

There are 3 types devices for selection.

[1] Network IPA

If the "Device type" is set to "Network IPA", you need to set the device number (1-32).

[2] Building IPA

If the "Device type" is set to "Building IPA", you need to set the block number (1-999) and the device number (1-32).
[3] Private IPA

If the "Device type" is set to "Private IPA", you need to set the block number (1-999), floor number (1-63), room number (1-32), and the device number (1-32).
3. Unlock setting

Please follow the steps below:

[1] On the designated IP actuator screen, click "Unlock setting".
[2] Set the output mode for "Lock-GND" from among "AC output", "DC output (NC)" and "DC output (NO)".
[3] Set the unlock time for "Lock-GND".
[4] Set the output mode for "Relay lock" between "Unlock" and "Light".
[5] Set the unlock time for "Relay lock".
[6] Click "√" to save.
4.7 Managing the backup

4.7.1 Creating the backup

Note
It is strongly recommended to create a backup and store in a proper catalogue when the devices used on the system are signed successfully.

Please follow the steps below:

[1] On the home screen, click "Preferences".
[2] Click "Project backup".
[3] Click "+".
[4] Enter the name.
[5] Enter the recovery password.
[6] Tick the check box to export the logs/records.
[7] Click "Save".
[8] The result is displayed on the screen.

**Note**

It is not recommended to backup logs (step 6). Logs contain a lot of snapshots and it will take a long time to backup due to the large size. If you want to backup the logs without the snapshots, see chapter 4.10 "Notification" on page 160.
4.7.2 Restoring the backup

Please follow the steps below:

[1] On the backup screen, click the designated backup.
[2] Click "Restore project backup".
[3] Enter the recovery password.
[4] Click "OK".

**Notice**

The backup notifications are valid for half a year. If more than half a year, the data such as "alarm record", "device failure", "call record", "unlock record" and "system log" will be automatically removed when the backup is restored.
4.7.3 Removing the backup

Please follow the steps below:

[1] On the backup screen, click the designated backup.
[2] Click "Delete".
[3] Click "Confirm".
4.7.4 Exporting the backup

Please follow the steps below:

[1] On the backup screen, click the designated backup.
[2] Click "Export".
4.7.5 Importing the backup

Please follow the steps below:

1. On the backup screen, click "Upload".
2. Click "Browse" to select the designated backup file from the PC.
3. Enter the recovery password.
4. Click "OK".
5. When the backup file is more than 2 GB, a pop-up window will appear (optional).
6. Copy the backup file to the software installation folder\file\binaries (optional).
7. Click "√" to confirm.
Click "✓" to restore the backup file.
4.8 Updating the firmware

There are 3 options to update the firmware of the device in the system.
1. Local firmware update

Local firmware update one by one

Note
Please access the website "https://new.abb.com/low-voltage/products/building-automation/product-range/abb-welcome" to download the latest firmware of the designated device before use.

Please follow the steps below:
[1] On the designated device (e.g. "Indoor station") screen, click "Local firmware update".
[4] Click "√" to confirm.
Local firmware update in a batch

Note
Please access the website "https://new.abb.com/low-voltage/products/building-automation/product-range/abb-welcome" to download the latest firmware of the designated device before use.

Please follow the steps below:
[1] On the home screen, click "Device management".
[2] Click the designated device (e.g. "Indoor stations").
[3] Click "  ".

![User interface diagram]
[4] Click "Select all" to select all devices or click the designated device one by one to select multiple devices.

[5] Click "Next".

[6] Click "Local firmware update".

---

Operation
[8] Upload the signature.
[9] Click "√" to confirm.
2. Online firmware update

**Note**
Please make sure your PC can connect to the internet before use. You can ask your IT engineer for help.

Please follow the steps below:

[1] On the designated device (e.g. "Indoor station") screen, click "Online firmware update".


[3] "Current firmware is up to date" will be displayed on the screen if the current version is the latest one. Otherwise click "√" to update the new firmware.
3. Updating the firmware on a pop-up window

**Note**
Please make sure your PC can connect to the internet before use. You can ask your IT engineer for help.

Please follow the steps below:

[1] On the home screen, click "Appears and flashes only when the device have a new firmware to update).

[2] The devices to be updated are displayed on the screen.

[3] Click "Update all" to update all the devices in a batch. Or you can click "Ask me next time" to skip the update.
4.9  **Restoring to factory default**

Please follow the steps below:

1. On the home screen, click "Preferences" to access the corresponding screen.
2. On the "Preferences" screen, click "System information".
3. Click "System reset".
4. Enter the current admin password to restore all the settings of the "PC management software" to factory default settings except "3rd party authority".
4.10 Notification

4.10.1 Call list

1. Viewing the records

Please follow the steps below:

[1] On the "Notification" screen, click "Call list".
[2] Click "Filter".
[3] Enter the criterias (e.g. date, call type, unlock type, device type and device number).
[4] Click "Inquire" to view the results.
[5] Click the designated record.

Notice

The call records are valid for half a year. If more than half a year, the data will be removed automatically.
2. Exporting the records

*Note*
The snapshots will not be exported when this operation is carried out.

Please follow the steps below:

[1] On the "Notification" screen, click "Export".
[2] Click to select "Call list".
[3] Click "√".
4.10.2 Unlock list

1. Viewing the records

Please follow the steps below:

[1] On the "Notification" screen, click "Unlock list".

[2] Click "Filter".

[3] Enter the criteria (e.g. date, unlock type, device type and device number).

[4] Click "Inquire" to view the results.

[5] Click the designated record.


Notice

The unlock records are valid for half a year. If more than half a year, the data will be removed automatically.
2. Exporting the records

Please follow the steps below:

[1] On the "Notification" screen, click "Export".
[2] Click to select "Call list".
[3] Click "√".
4.10.3 **Alarm list**

1. **Alarm notification**

A pop-up window will be displayed when there is an alarm. You can set the status (e.g. "Processed" and "False alarm") and enter the comment for the alarm.
2. Viewing the records

Please follow the steps below:

[1] On the "Notification" screen, click "Alarm list".
[2] Click "Filter".
[3] Enter the criteria (e.g. date, alarm type, alarm status, event times, device type and device number).
[4] Click "Inquire" to view the results.
[5] Click the designated record. " ● " on the title highlights unhandled status.
[6] If the alarm is not handled, click to set the handle status and enter the comment, otherwise view the details of the alarm.

Notice

The alarm records are valid for half a year. If more than half a year, the data will be removed automatically.
3. Exporting the records

Please follow the steps below:

[1] On the "Notification" screen, click "Export".
[2] Click to select "Alarm list".
[3] Click "√".
4.10.4 Device fault

Please enable the “Alarm when device goes offline” function before use. See chapter 3.6.7 “Alarm notification settings” on page 30.

1. Alarm notification - the device is disconnected

A pop-up window will be displayed when there is an offline device. You can set the status (e.g. “Processed” and “False alarm”) and enter the comment for the alarm.

![Image of pop-up window for device fault notification]
2. Viewing the records

Please follow the steps below:

[1] On the "Notification" screen, click "Device fault".
[2] Click "Filter".
[3] Enter the criteria (e.g. date, alarm status, device type and device number).
[4] Click "Inquire" to view the results.
[5] Click the designated record. " ● " on the title highlights unhandled status.
[6] If the alarm is not handled, click to set the handle status and enter the comment, otherwise view the details of the alarm.

Notice

The device fault records are valid for half a year. If more than half a year, the data will be removed automatically.
3. **Alarm notification - the device is reconnected**

A pop-up window will be displayed when the connection is recovered. You can set the status (e.g. "Processed" and "False alarm") and enter the comment for the alarm.
4. Exporting the records

Please follow the steps below:

[1] On the "Notification" screen, click "Export".
[2] Click to select "Device fault".
[3] Click "√".

![Exporting the records screenshot]
### 4.10.5 System log

1. Viewing the records

Please follow the steps below:

1. On the "Notification" screen, click "System log".
2. Click "Filter".
3. Enter the criteria (e.g. date).
4. Click "Inquire" to view the results.
5. Click the designated record.
6. The detail is displayed on the screen.

<table>
<thead>
<tr>
<th>Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 5, 2021</td>
<td>Feb 5, 2021</td>
</tr>
</tbody>
</table>

**Notice**

The system logs are valid for half a year. If more than half a year, the data will be removed automatically.
2. Exporting the records

Please follow the steps below:

[1] On the "Notification" screen, click "Export".
[2] Click to select "System log".
[3] Click "√".
4.11 Message center

4.11.1 Creating a message

On the "Message center" screen, click "+" to set a recipient, then enter the subject and the message, click "✓" to create and send the message.
4.11.2 Replying to a message

On the "Message center" screen, click "Inbox" to view the message received from the indoor stations. You can click on a message and reply to it directly.

A maximum of 1000 messages is supported.

Your reply messages can be viewed in the "Outbox".

A maximum of 10000 messages can be supported.
4.12 Cloud setting

4.12.1 Log in the cloud

Please follow the steps below:

[1] On the "Main menu" screen, click "Preference".
[2] Click "Cloud settings".
[3] Paste the cloud setting key which can be obtained from ABB after-sales.
[4] Click "Enable".
4.12.2 Log out the cloud

Please follow the steps below:

[1] On the "Main menu" screen, click "Preference".
[2] Click "Cloud settings".
[3] Click "Disable", "√".

![Preferences screen with Cloud Settings highlighted](image)

**Note**

ABB i-HD management system cannot review the owners and manage the residents if it logged out the cloud. It needs to log in the cloud again.
4.12.3 Exporting topology

To use the cloud functions (e.g. cloud intercom), you need to export the community topology and provide it to ABB after-sales. They will create a community on the cloud and give you back the cloud setting key for binding. Please follow the seteps below:

[1] On the "Main menu" screen, click "Preference".
[2] Click "Cloud settings".
[3] Click "Export topology".
[4] A .csv file will be created automatically.

Note
Once the topology is exported, it is hard to modify again. The only solution is to create a new topology. Please ensure that the topology to export contains the complete building and room information.
4.12.4 Cloud backup or restore

Precondition
ABB i-HD management software has been logged in the cloud.

Access the "Cloud backup" screen
Please follow the steps below:
[1] On the "Main menu" screen, click "Preference".
[2] Click "Cloud backup or restore".

![Image of the "Cloud backup" screen showing steps 1 and 2]
**Backup automatically**
- i-HD PC management system backup the data in recently 3 days.
- i-HD PC management system backup the data every morning.
- The backup data contains the device list, user list, card information, PIN code, QR code and face information.
- The backup data doesn’t contain the logs (e.g. calling records, unlock records and alarms).

**Backup manually**
- Only one manual backup can be supported and the new backup will overwrite the old one.
- The backup data contains the device list, user list, card information, PIN code, QR code and face information.
- The backup data contains the logs (e.g. calling records, unlock records and alarms).
- The backup has large size and it will take longer time.

On the "Cloud backup/restore" screen, click "Backup by manual", "√".

### Cloud backups/restore

<table>
<thead>
<tr>
<th>Date</th>
<th>Type</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021-12-29 02:00:00</td>
<td>AUTO</td>
<td>Remove the backup</td>
</tr>
<tr>
<td>2021-12-27 02:21:13</td>
<td>AUTO</td>
<td>Remove the backup</td>
</tr>
<tr>
<td>2021-12-26 02:25:18</td>
<td>AUTO</td>
<td>Remove the backup</td>
</tr>
<tr>
<td>2021-12-09 06:37:04</td>
<td>MANUAL</td>
<td>Remove the backup</td>
</tr>
</tbody>
</table>

**Note**

It is not recommended to carry on any other operations on ABB i-HD management system before the backup is completed.
Recover the backup

On the "Cloud backup/restore" screen, click "Recover the backup", "√".

Note
It is not recommended to carry on any other operations on ABB i-HD management system before the restore is completed.
4.12.5 Reviewing the owners

Precondition
ABB i-HD management software has been logged in the cloud.

Review the owner
Please follow the steps below:
[2] On the "Main menu" screen,  will flash when a new user needs approval. Click  .
[3] The user to be approved is listed on the screen.
[4] Click "Approve".
[5] Select the resident type, it can be set to "Owner" or "Tenement".
[6] Click "√".

![Image of operation steps]
4.12.6 Managing the residents

Precondition
ABB i-HD management software has been logged in the cloud.

Search the resident
Please follow the steps below:

[2] User list is displayed.
[3] Enter the user name or the phone.
[4] Select the resident type.
[5] Click "Search".
View the resident

Please follow the steps below:

[1] On the “Resident center” screen, select the designated user.

[2] Click “View”.

[3] Resident details are displayed on the pop-up window.
**Edit the resident**

Please follow the steps below:

1. On the "Resident center" screen, select the designated user.
2. Click "Edit".
3. Select access authority from the drop-down list. It can be set to "Authorized" or "Unauthorized". Only authorized user can use the app (e.g. face, QR code and password) to release the lock.
4. Enter the start date and time.
5. Enter the end date and time.
6. Click "√".
Delete the resident

Please follow the steps below:

[1] On the "Resident center" screen, select the designated user.
[2] Click "Delete".
[3] Click "✓".
5 Cyber security

5.1 Disclaimer

This product is designed to be connected and to communicate information and data via a network interface, which should be connected to a secure network. It is customer's sole responsibility to provide and continuously ensure a secure connection between the product and customer's network or any other network (as the case may be) and to establish and maintain appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the product, the network, its system and interfaces against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB Ltd and its affiliates are not liable for damages and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Although ABB provides functionality testing on the products and updates that we release, you should institute your own testing program for any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third party software updates or patches, hardware change out, etc.) to ensure that the security measures that you have implemented have not been compromised and system functionality in your environment is as expected.

5.2 Performance and service and network performance

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>100 Mbps (148,800 packets/s)</td>
</tr>
<tr>
<td>ARP</td>
<td>20 Mbps (29,760 packets/s)</td>
</tr>
<tr>
<td>ICMP</td>
<td>100 Mbps (148,800 packets/s)</td>
</tr>
<tr>
<td>IP</td>
<td>60 Mbps (89,280 packets/sec)</td>
</tr>
</tbody>
</table>
## Port and service

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP web service for the &quot;PC management software&quot; (end user UI interface)</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS web service for the &quot;PC management software&quot; (end user UI interface)</td>
</tr>
<tr>
<td>3333</td>
<td>UDP</td>
<td>Multicast UDP service for device</td>
</tr>
<tr>
<td>5222</td>
<td>TCP</td>
<td>Service for XMPP client</td>
</tr>
<tr>
<td>5223</td>
<td>TCP</td>
<td>Service for XMPP client with secure connection</td>
</tr>
<tr>
<td>7000</td>
<td>TCP</td>
<td>RPC service for device</td>
</tr>
<tr>
<td>7070</td>
<td>TCP</td>
<td>HTTP service for XMPP Client</td>
</tr>
<tr>
<td>7443</td>
<td>TCP</td>
<td>HTTPS service for XMPP Client</td>
</tr>
<tr>
<td>7777</td>
<td>UDP</td>
<td>Service for device with UDP</td>
</tr>
<tr>
<td>8832</td>
<td>TCP</td>
<td>RPC service for UI (TLS)</td>
</tr>
<tr>
<td>8884</td>
<td>TCP</td>
<td>MQTT Service(with TLS)</td>
</tr>
<tr>
<td>8887</td>
<td>TCP</td>
<td>RPC service for device for firmware update</td>
</tr>
<tr>
<td>8888</td>
<td>TCP</td>
<td>Service for HTTP Proxy Server for firmware update</td>
</tr>
<tr>
<td>9090</td>
<td>TCP</td>
<td>HTTP service for XMPP administrator</td>
</tr>
<tr>
<td>9091</td>
<td>TCP</td>
<td>HTTPS service for XMPP administrator</td>
</tr>
<tr>
<td>10700</td>
<td>TCP</td>
<td>RPC service for device (under TLS)</td>
</tr>
<tr>
<td>17700</td>
<td>TCP</td>
<td>RPC service (Low priority) for device(TLS)</td>
</tr>
</tbody>
</table>
5.3 Deployment guideline

Please do not install in a public place and ensure that physical access to the devices is granted only to trusted personnel.

The device needs to be installed in secure locations to prevent theft and avoid offline attacks.

When this product is installed on a home network, make sure there is no public export service to the internet via any Dynamic DNS services.

If the user decides to remove the device from system, the user shall reset the device to the factory settings to remove all the configuration data and sensitive data on the device. This will prevent sensitive data leaks.

You should use a TPM and BitLocker enabled computer to host this product to provide sufficient data security.

You should use two independent network interfaces in the host computer to implement communication segregation. One for internet-facing communication, one for other communication.

You should install this product on the computer which support secure boot to protect your system.

5.4 Upgrading

If new firmware is available, the system will prompt the user to perform a remote update and the user can choose the version to update in "Preferences" on "PC management software".
5.5 Backup/restore

Users can create a data backup (project backup) which is saved in "PC management software". For data security, it is suggested to export the data backup to other external storage devices. Users are recommended to create a backup version after completing the first initialization operation. Thereafter, create a backup every time any major changes are made, such as adding or deleting devices. Backup data can be imported to "PC management software" system for use by the admin user.

5.6 Malware prevention solution

The device is not susceptible to malware, because custom code cannot be executed on the system. The only way to update the software is via firmware upgrade. Only firmware signed by ABB can be accepted.
6 Notice

We reserve the right to at all times make technical changes as well as changes to the contents of this document without prior notice.

The detailed specifications agreed to at the time of ordering apply to all orders. ABB accepts no responsibility for possible errors or incompleteness in this document.

We reserve all rights to this document and the topics and illustrations contained therein. The document and its contents, or excerpts thereof, must not be reproduced, transmitted or reused by third parties without prior written consent by ABB.
Notice
We reserve the right to at all times make technical changes as well as changes to the contents of this document without prior notice. The detailed specifications agreed upon apply for orders. ABB accepts no responsibility for possible errors or incompleteness in this document.

We reserve all rights to this document and the topics and illustrations contained therein. The document and its contents, or extracts thereof, must not be reproduced, transmitted or reused by third parties without prior written consent by ABB.
错误！使用“开始”选项卡将 Überschrift 1 应用于要在此处显示的文字。