



App user guide

Securitas Direct Pro



TABLE OF CONTENT

Below steps are performed by a technician

3 PROGRAM LOGIN

LOG IN
ADD CENTRAL
TO FIND SID NUMBER

5 PANEL LOGIN

PIN CODE

6 LOGIN

7 OVERVIEW HANDLING

8 MENU

AREAS
Area Modes
Commands
ZONES
Zone status

11 WALK TEST

AREA LIST
WALK TEST PROCESS
WALK TEST REPORT

13 EVENT LOG

14 AUTOMATION

SETTINGS

15 DOOR CONTROL

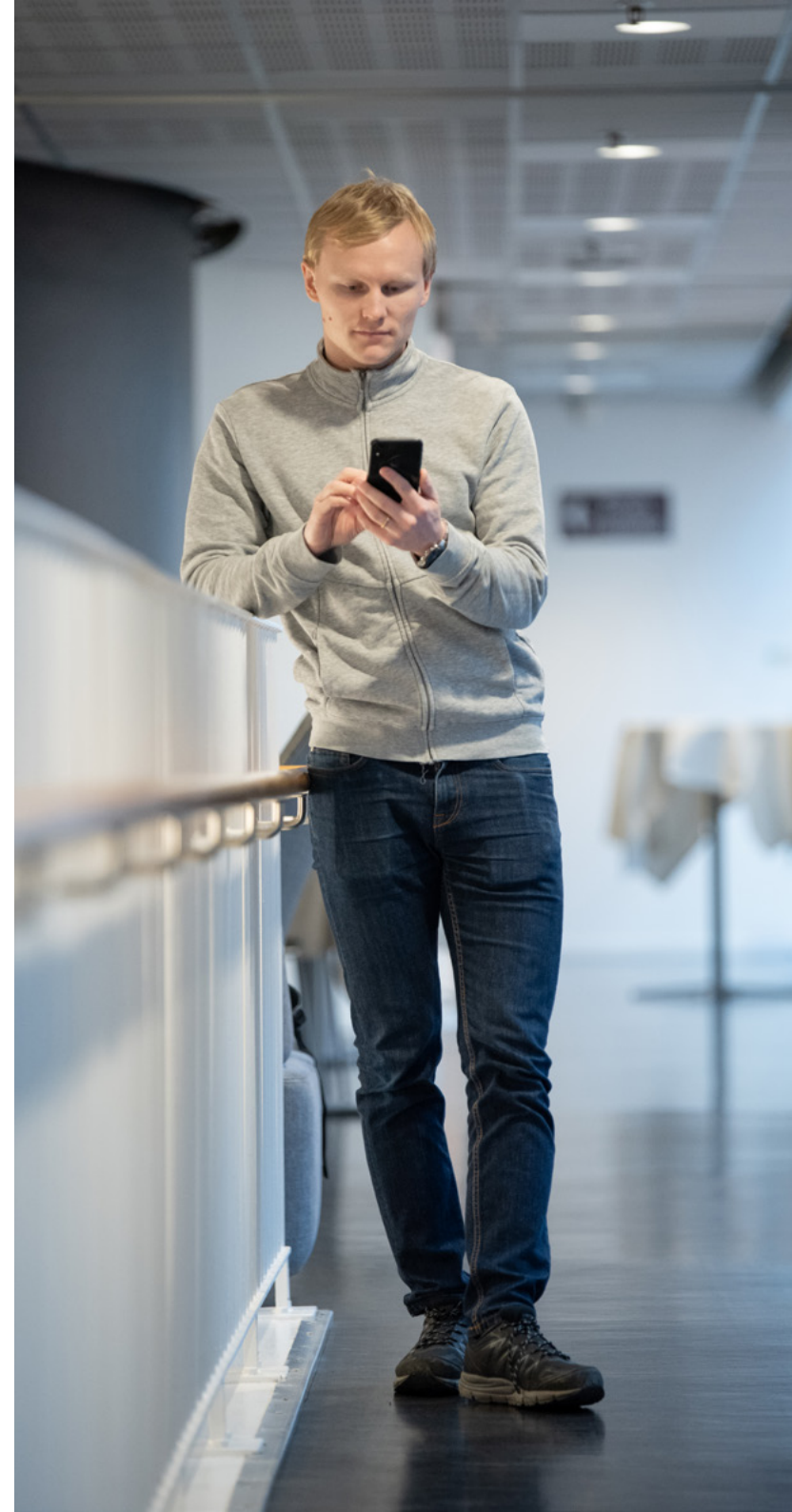
DOOR STATUS
COMMANDS

19 USER MANAGEMENT

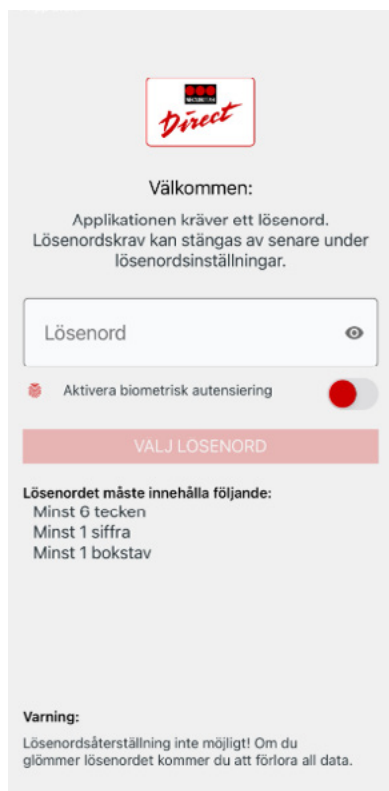
23 PROGRAM SETTINGS

PASSWORD SETTINGS

25 GLOSSARY



PROGRAM LOGIN



The screenshot shows the 'Direct' logo at the top. Below it, the text 'Välkommen:' is followed by a message: 'Applikationen kräver ett lösenord. Lösenordskrav kan stängas av senare under lösenordsinställningar.' A password input field labeled 'Lösenord' with an eye icon is present. Below the field is a toggle switch for 'Aktivera biometrisk autensiering' which is currently off. A red button labeled 'VALJ LÖSENORD' is below the toggle. Underneath, a section titled 'Lösenordet måste innehålla följande:' lists requirements: 'Minst 6 tecken', 'Minst 1 siffra', and 'Minst 1 bokstav'. At the bottom, a 'Varning:' section states: 'Lösenordsåterställning inte möjligt! Om du glömmet lösenordet kommer du att förlora all data.'

When you start up for the first time, the program requires you to create a password.

The password must contain at least 6 characters, including letters and numbers.



The screenshot shows the 'Direct' logo at the top. Below it, the text 'Var god slå in lösenord och logga in.' is underlined. A password input field labeled 'Lösenord' with an eye icon is present. Below the field is a link 'Glömt lösenord?'. At the bottom is a red button labeled 'LOGGA IN'.

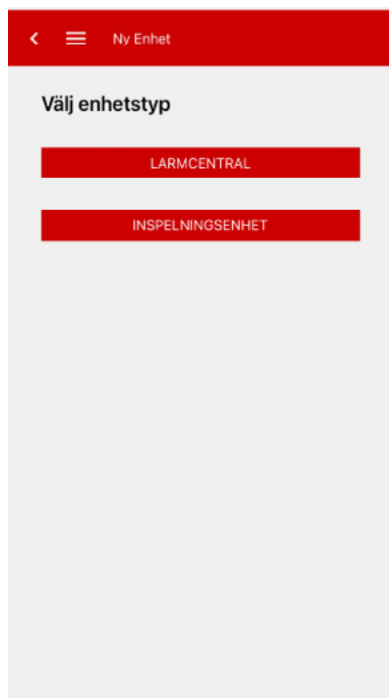
If required by the program settings, you must authenticate with this password every time you enter the program.

Password authentication can be disabled in [Password Settings](#) > Enable Password.

! If the password requirement is disabled, security is lost as the code is not required for arming/disarming.

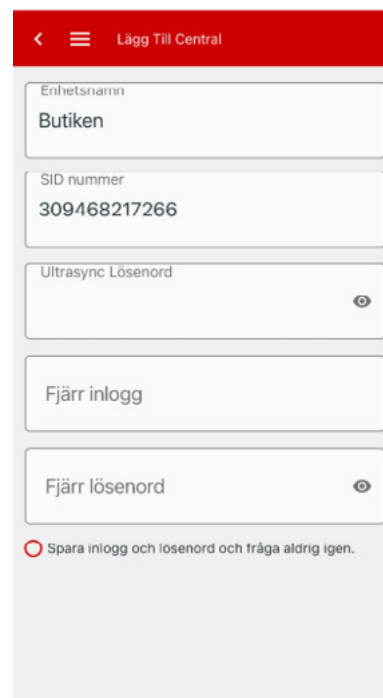
ADD CENTRAL

During installation, or the first time you log into the app, a central unit must be added to connect to the alarm system.



ADD NEW DEVICE

Select **ALARM CENTRAL** as the device type.



CONNECT VIA ULTRASYNC

This can be done in two different ways, via UltraSync or via IP. We only use UltraSync.

Via UltraSync

Device name, SID number, and password must be entered.

To find SID number

- Enter with supervisor code in the control panel
- Go to 8 – Service
- Go to 5 – Communication
- Then go to 4 – Ultrasync
- Then go to 1 – SID

To find Ultrasync password

- Enter with supervisor code in the control panel
- Go to 8 – Service
- Go to 5 – Communication
- Then go to 4 – Ultrasync
- Then go to 2 – Password

To connect

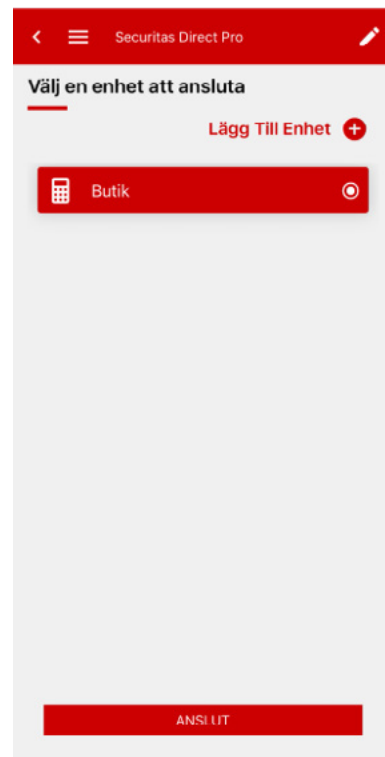
Press **Detect burglary alarm** and enter Remote login and Remote password. (**Remote login and password are assigned by the installer.**)

Confirm with **CONNECT VIA ULTRASYNC**

If the characters ",+%&<>/@" or spaces are used in the remote login or password, it is not possible to activate notifications in the app. It is still possible to log into the app and operate the alarm.



PANEL LOGIN




CONNECT TO PANEL

Select an alarm system to connect.

Press **CONNECT** to connect to the panel.

Enter **PIN code** (see **PIN code** on the right).

Press the Edit icon  to edit or remove the selected alarm system. If there is no configured system, you will be guided to add a new central (see **Add New Central**).

Press **Add Device**  to create a new central.

NOTE: When you open the app for the first time, you will be prompted to add a new central (see **Add New Central**).

Approved login will lead you to Areas. See [Areas](#).

LOGIN



LOGIN

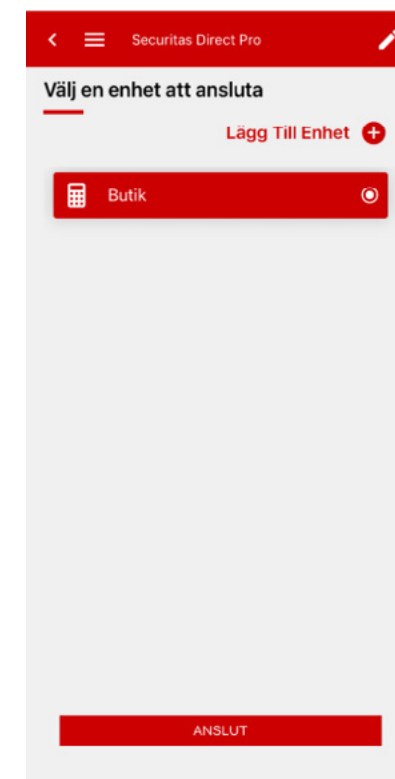
Log in with the password created for the app.



Press Forgot Password if you have lost your password. You will be prompted to create a new password after you have completed the reset process.

Once you have approved the data reset, you will be taken to the password settings screen.

WARNING! This will erase all data. The entire configuration will be permanently lost.



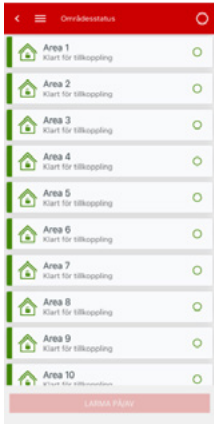
CONNECT

Connect to the system by selecting it and pressing **CONNECT**.

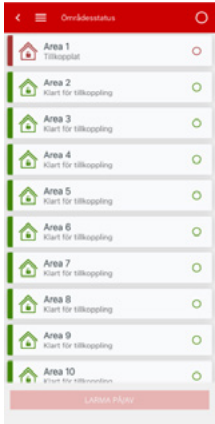
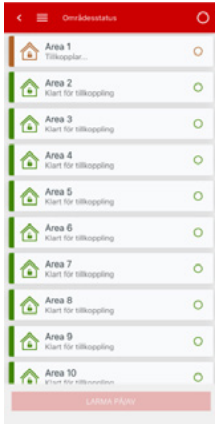
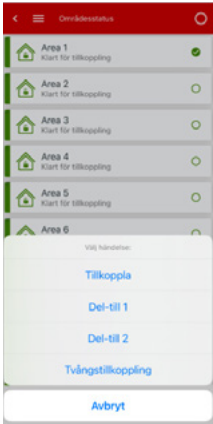
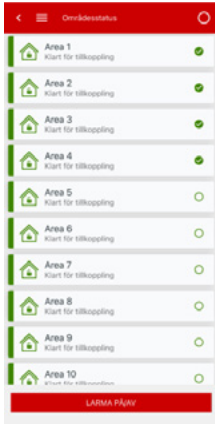
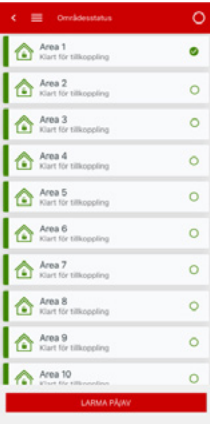
If you have multiple systems, you will choose which one you want to connect to here.

OVERVIEW HANDLING

HOME PAGE



ARM



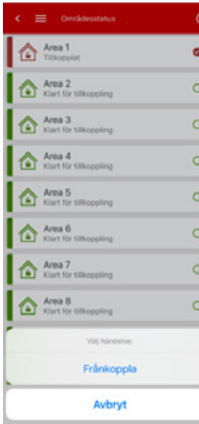
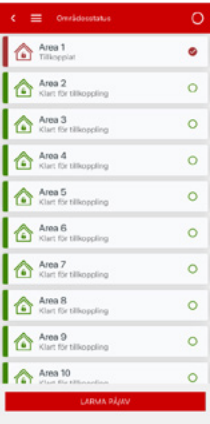
Select which area(s) you want to arm and press **ARM/DISARM**.

Confirm the type of arming.

Arming in progress.

All areas armed.

DISARM



Select which area(s) you want to disarm and press **ARM/DISARM**.
Confirm disarming in the next step.

AREA STATUS

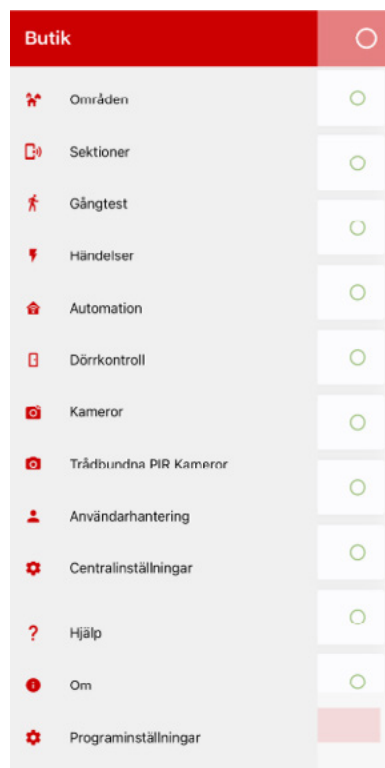
ARM

- Select the area(s) you want to connect
- Press the alarm ON/OFF
- Press Arm

DISARM

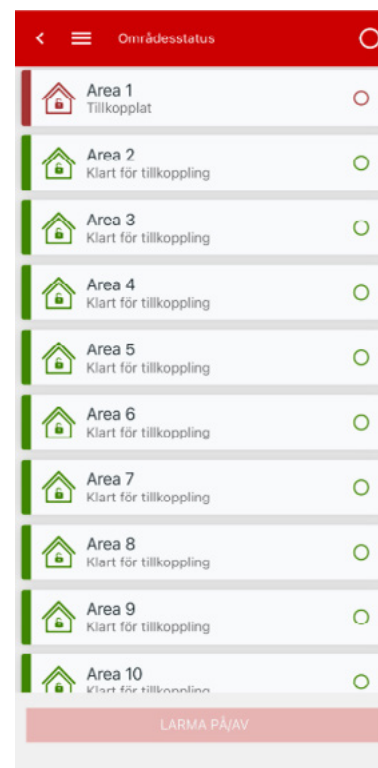
- Select the area(s) you want to arm
- Press the alarm ON/OFF
- Press Disarm

MENU



MENU

Descriptions of all the app's menu options. Below is a review of the current settings.



AREAS

On the home page, the status of each area is displayed. From here, you can arm and disarm one or more areas.

Area Modes

The following area modes are possible:

Ready to arm: The area is disarmed, and all zones are in normal mode.

Armed: The area is armed.

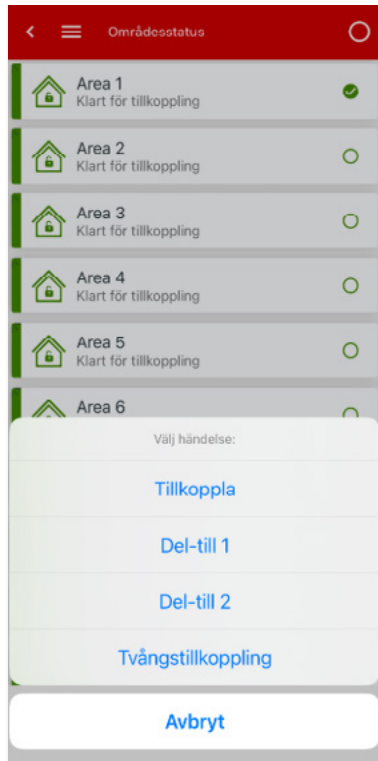
Arming: The area is in the process of arming. The exit timer is running.

Alarm: The area is in alarm mode.


Not ready to arm: There are active zones in the area.

Disarming: The area is in the process of disarming. The entry timer is running.

WARNING: Area status is only updated when the alarm system is online and connected.



COMMANDS

Click on an area to select or deselect it. You can also click on **Select All**  to select or deselect all areas.

Click on **ARM/DISARM**.

Then choose a command according to the options below.

The following commands may be available depending on the area mode:

Arm: Arm the area.

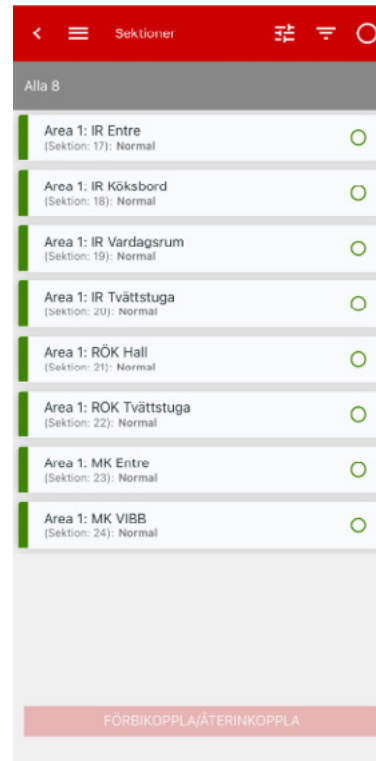
Partial Arm 1: Partially arm part 1 of the area.

Partial Arm 2: Partially arm part 2 of the area.

Disarm: Disarm the area.


Force Arm: Arm the area, temporarily bypass faults or open zones.


Confirm & Disarm: Confirm the alarm and disarm the area.




ZONES

The status of the zones is displayed, and from here you can bypass and re-enable them.

Press **Filter**  to filter zones by status.

Press **Sort**  to sort zones by status or zone number.

Click on a zone to select or deselect it, or click on **Select All**  to select or deselect all zones.

Click on **BYPASS/RE-ENABLE** to inhibit the selected zones.

INHIBIT ZONE

- Menu
- Zones
- Select Zone
- Press bypass
- A box will appear with the text:
"Do you want to inhibit?"
- Press YES

The Zone will be disconnected until it is manually reconnected or until someone disarms the alarm.

ZONE STATUS

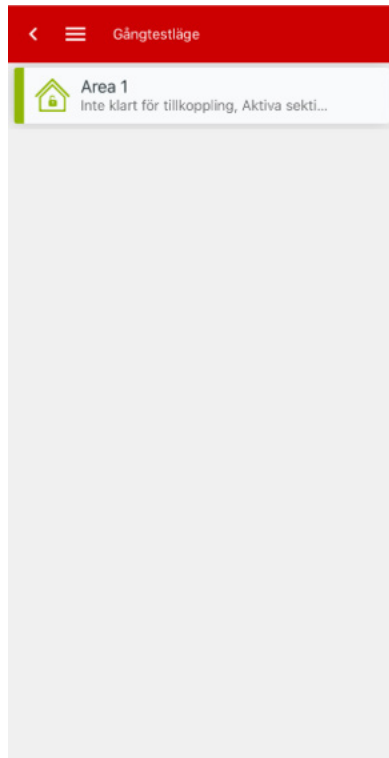
COMMANDS

The zones can have the following statuses, which are illustrated with appropriate text and color:

- **Normal (green):** The zone is NOT activated when the area is disarmed. For example, emergency exit closed.
- **Set (purple):** The zone is normal when the area is armed.
- **Active (blue):** The zone is activated when the area is disarmed. For example, emergency exit open.
- **Alarm (red):** The zone is activated when the area is armed.
- **Tamper (red):** The zone is open or short-circuited. Someone may have tried to tamper with the detector or device.
- **Inhibited (gray):** The zone has been bypassed and does not indicate normal or active status. It is excluded from functioning as part of the system for a certain period. Tamper is still monitored.
- **Isolated (black):** The zone has been bypassed and does not indicate normal or active status. It is permanently excluded from functioning as part of the system. *(This is done only in consultation with Securitas Direct.)*
- **Masked or Fault (yellow):** The detector is masked or the zone is false alarming.
- **Switched (orange):** The zone has been inhibited for a certain period.



WALK TEST




WALK TEST

A function where you can perform a walk test that will check all zones in the selected areas.

Area List

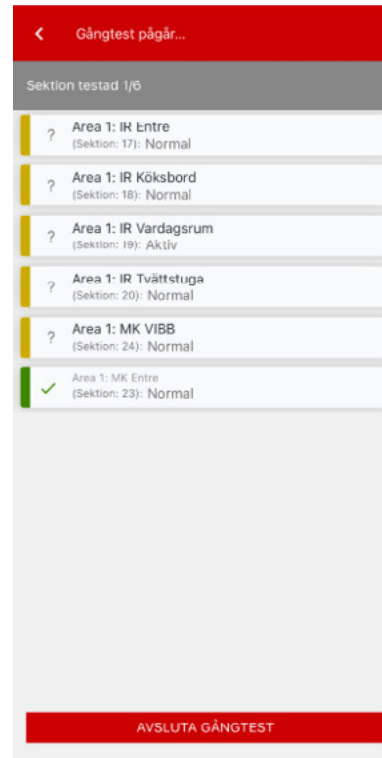
NOTE: Only areas with the status Ready to arm can be selected for the walk test, i.e., a disarmed area.

Click on an area to select or deselect it. You can also click **Select All**  to select or deselect all areas.

Then click **START WALK TEST** to start the walk test in the selected areas.

START WALK TEST

- Menu
- Walk Test
- Select the area to be tested
- Start walk test
- The walk test ends when all zones are tested, or the user manually ends it with the **END WALK TEST** button.



WALK TEST PROCESS

During the walk test, the zones are sorted into the following groups:

Not tested (upper part)

Tested (lower part)

The walk test ends when all zones are tested, or the user manually ends it with the **END WALK TEST** button.

! Important for Smoke Detectors and Panic Alarms

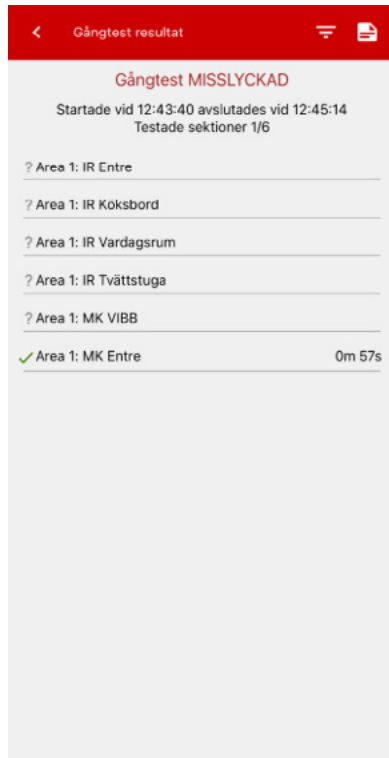
A smoke detector and a panic alarm cannot be walk tested without the siren starting and a real alarm being sent to the alarm center.

Therefore, these should not be tested on your own.

In the list of zones, these products will be placed under not tested, but the results for the remaining zones will be displayed.


When the walk test ends, **Walk Test Failed** will be displayed, which is because not all zones are tested. As long as green status is displayed on the zone, the walk test is successful.


WALK TEST Continued




WALK TEST REPORT

When the walk test is completed, a report of the results is displayed. This report includes the time and a list of tested and untested zones with a relative test time for the zones that have been tested.

Click **Filter / Select Order**  to sort the list by time or zone number.

Click **Export**  to export the report as an HTML file, and then use the standard Android or iOS functions to share the file.


EVENT LOG



Händelselogg		
Alla 63		
Area 1 Rapport OK Larmcentral 1: Securitas Direct	2025-02-13 12:45	
Area 1 Rapport OK Larmcentral 1: Securitas Direct	2025-02-13 12:45	
Area 1 Test klar ANVÄNDARE 2: Supervisor	2025-02-13 12:45	
Area 1 Sektion ej testad Sektion 17: IR Entre	2025-02-13 12:45	
Area 1 Sektion ej testad Sektion 19: IR Köksbord	2025-02-13 12:45	
Area 1 Sektion ej testad Sektion 19: IR Vardagsrum	2025-02-13 12:45	
Area 1 Sektion ej testad Sektion 20: IR Tvättstuga	2025-02-13 12:45	
Area 1 Sektion ej testad Sektion 24: MK VIBB	2025-02-13 12:45	
Area 1 Sektion ej testad	2025-02-13 12:45	

EVENT LOG

You can download and review events for the control panel. Events are sorted by time (from newest to oldest).

Press **Filter**  to filter events/type.

The following event types are available:

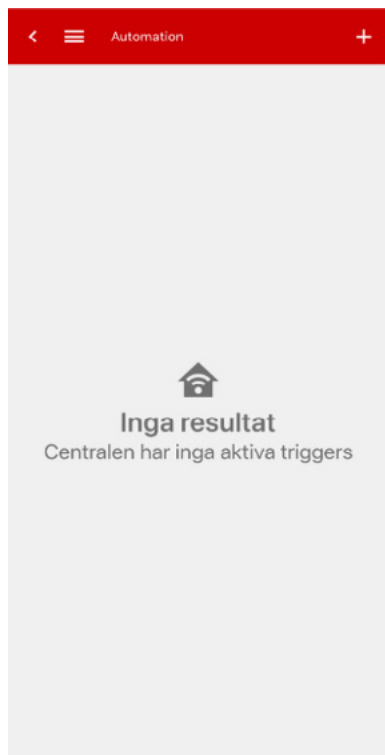
- All
- Alarm
- Image
- Arm/Partial Arm
- Disarm
- Passage
- Problem
- Reset
- Information

Press an event to see more details.

- ! Only the Supervisor (Alarm Manager/Master User) can read the event log in the app.

Other users can only read the event log on My Pages.

AUTOMATION



AUTOMATION

Via automation, you can control external devices.


NOTE: The devices must be configured and programmed in the control panel.


Contact your installer to configure the control panel according to its output.

The device's status is indicated by the color of the power button:

 Red: The device is **OFF**

 Green: The device is **ON**

 Grey: The user does not have access rights to the device

The switch  adjusts the status of triggers.

NOTE: The exclamation mark next to the device's status indicates that the status is unknown due to an error (e.g., a communication error).

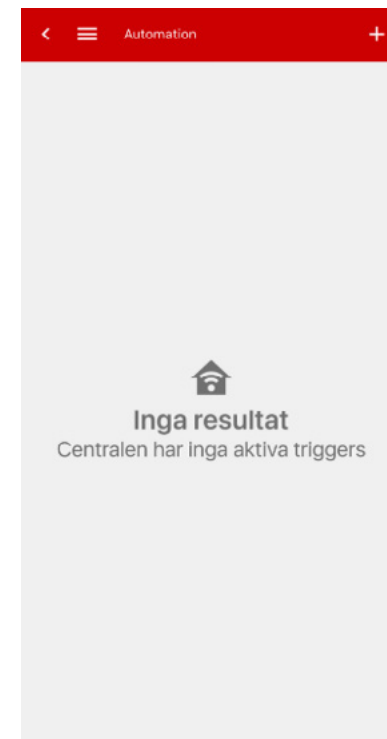
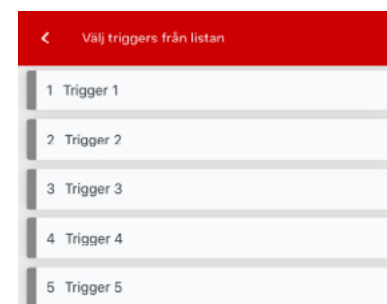
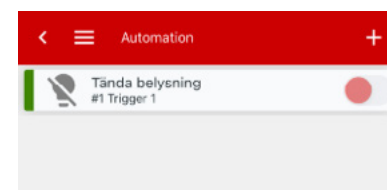
Click on **a trigger description** to change or remove it.

Click on **a configured device** to toggle its mode. Press **+** to add and edit a trigger.

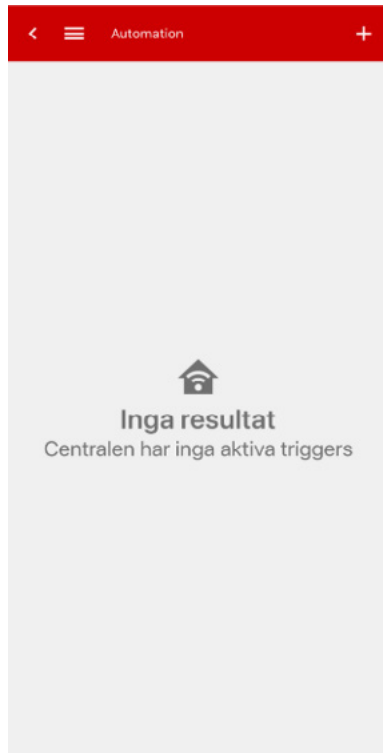
SETTINGS

To add a device, follow these steps::

1. Select a trigger from the available trigger list.
2. Describe the device under **Function Name**.
3. Choose a color for the device's control button.
4. Select an output from the list on the control panel.
5. Press **Save**.



DOOR CONTROL



DOOR CONTROL

With the door control function, you can control defined doors in the control panel. The list includes doors assigned to a door group that you have access to.

NOTE! The following door types are supported:

- **Standard doors**
(where we have a magnetic contact/vibration detector)
- **Intelligent doors**
(controlled by an ATS125x door controller)

Intelligent doors controlled by a CDC4(-EN) door controller are not supported.

Door Status

NOTE! The door status is only updated when the system is online and connected.

POSSIBLE DOOR STATES

Locked – Closed: The door is locked, and its associated zone indicates that the door is closed.

Locked – Open: The door is locked and opened. The possible cause is forced opening.

Unlocked – Closed: The door is unlocked and closed. The electronic lock allows it to be opened.

Unlocked – Open: The door is unlocked and opened.

Disabled: The door cannot be operated except to change it to enabled.

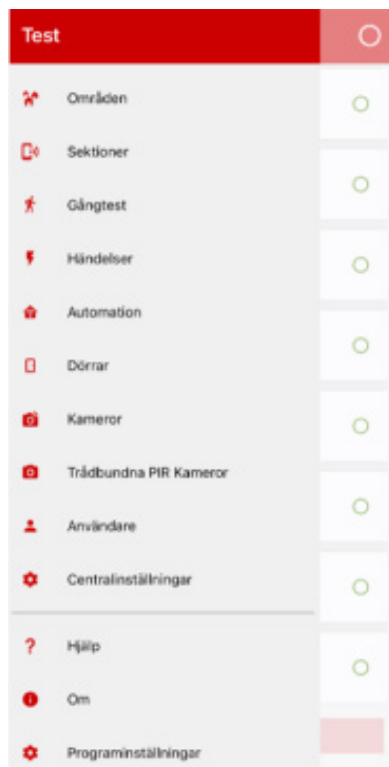
Commands

Press a door to display the list of commands available for the selected door. This list depends on the current state of the selected door.

The following functions may be available:

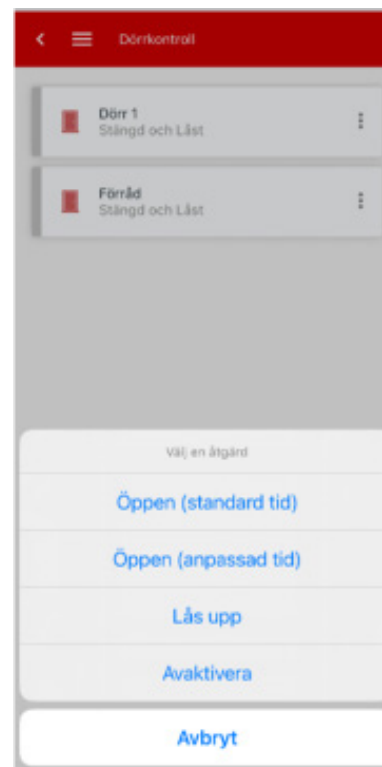
- | | |
|-----------------|--|
| Unlock: | Unlock the door and keep it unlocked until the lock command is executed. |
| Lock: | Lock the door. |
| Open: | This command allows you to unlock the selected door for a time (standard time) configured in the control panel. |
| Open: | Unlock the door for a custom time. After this (custom time) command is selected, the user is prompted to enter a time (valid interval 1 to 255 seconds). |
| Disable: | Set the door to disabled mode. |
| Enable: | Remove a disabled status from the selected door. |

DOOR CONTROL



OPEN A DOOR VIA THE MOBILE APP

- Menu
- Doors



- Then tap the door you want to access
- If you have full access rights to the selected door, you will see four options:

Open (Standard Time)

Opens the door for the preset, programmed duration

Open (Custom Time)

Allows you to choose how long the door should remain open

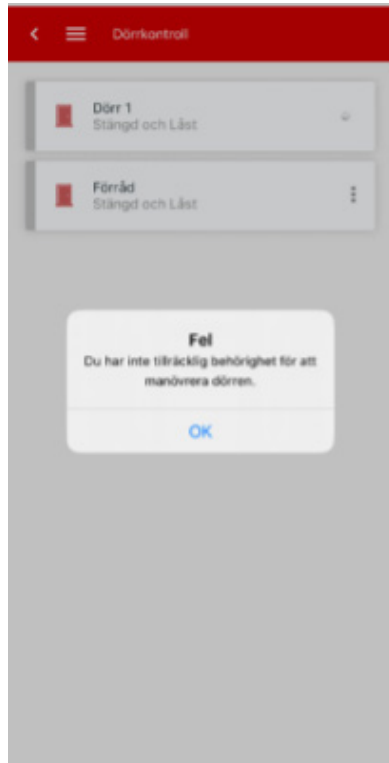
Unlock

Unlocks the door permanently until it is manually locked again

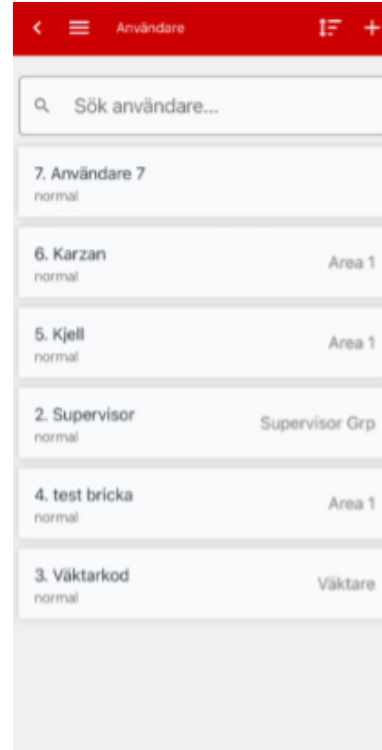
Deactivate

Disables the card reader until it is reactivated

DOOR CONTROL



If you do not have permission for the selected door, an information message will appear.



ADD A USER IN THE APP

- Menu
- Users
- Tap + to add a new user

DOOR CONTROL

- Enter the **username**
- Choose a **PIN code**
- Enter remote **login / password** if the user should have access to the mobile app

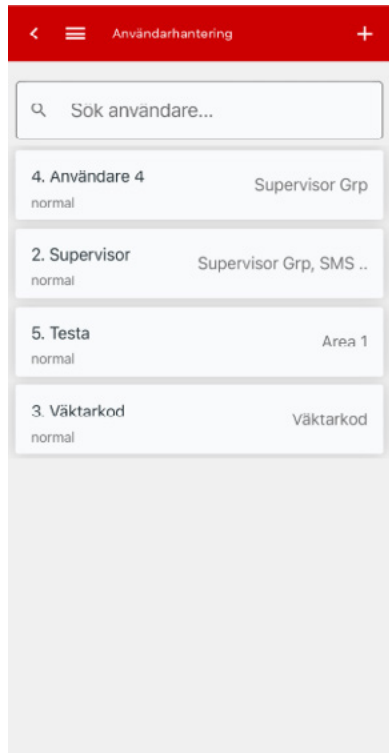
Card Number

- Tap **LEARN (LÄR)**, then present the tag to the main card reader / panel.

If a number appears under Card Number, the process was successful.

- Select **User Group** (defines which permissions the user will have)
- Then select the **Door Group** (defines which doors the user will be able to control)

USER MANAGEMENT



USER MANAGEMENT

With user management, you can manage the control panel's users: add, change, and remove. User management is only available for the Master user / Supervisor user configured in the control panel at position 2.


NOTE! The option **Allow remote access to configuration for Master** must be approved with **YES** in the installation menu.

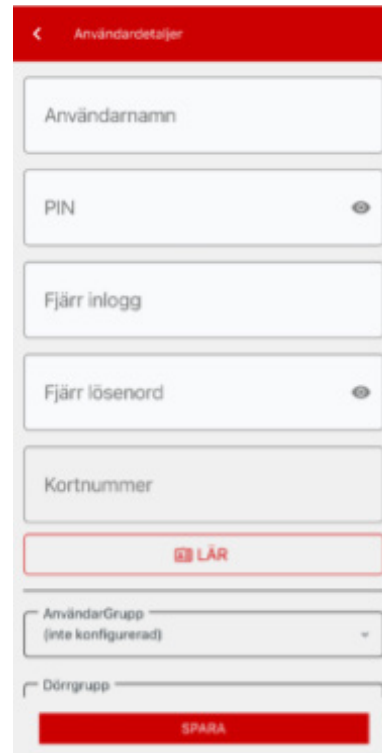
User List

The list includes all users defined in the control panel (except the installer). The installer user is not visible in the list and cannot be changed. The current user (master) is the first in the list. Other users are listed in alphabetical order.

Commands

The following commands are available:

- Add new users via **Add +**
- Remove a user via **Remove** 
- Start typing a username in the search field **Search to filter the user list.**
- Press a user to view user details.



USER DETAILS


NOTE! User details for the currently logged-in user (master) only contain two fields: **Name** and **PIN**.

This window contains two tabs:

- **Details**
- **User Group** (see User Groups page 18.)

A user can have the following attributes:

- **Name**
- **Language**
- **PIN code**
- **Card number** (see **Learn Card** page 18)
- **User type**
- **Door group**
- **Floor group**

Press the delete icon **Remove**  to remove a user. Note that the master user cannot be deleted.

USER DETAILS Continued

EXAMPLE OF USER TASKS TO ADMINISTER

ADD CODE

**Only the Supervisor (alarm manager)
can administer this!**

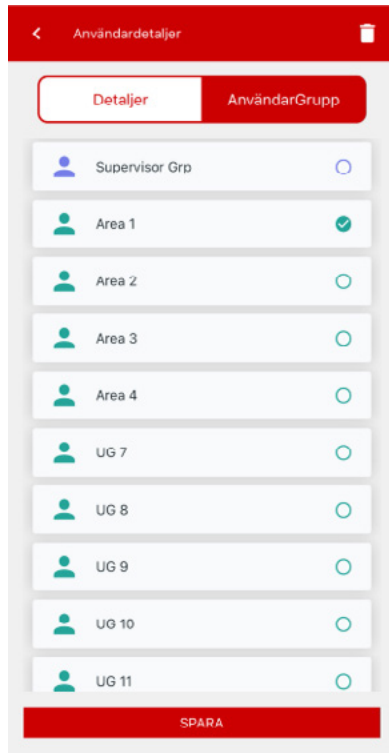
- Menu
- User Management
- Press + in the top right corner
- Add name + PIN
- Permission type = Normal
- Press on User Group
- Select at least one user group/area
for the selected user
- Go back to Details
- Press Save

ADD APP USER

**Only the Supervisor (alarm manager)
can administer this!**

- Menu
- User Management
- Press + in the top right corner
- Add name + PIN
- Permission type = Normal
- Enter any remote login + remote password
for the user (you cannot have the same
remote login for multiple users)
- Press on User Group
- Select at least one user group/area for
the selected user.
- Go back to Details
- Press Save

USER DETAILS Continued

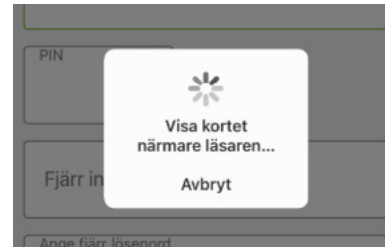


USER GROUPS

Select at least one user group/area for the selected user.

- **Supervisor group:** Full access in the app
 - An unlimited number of users can have this user group
 - Does not grant access to the event log or user administration
- **Area, 1, 2, etc.:** Users are only authorized for the respective area
- **Custom groups:** Technicians can, during installation, add multiple areas to a group and name it. The user will then have access to only this group.

NOTE! Username, PIN, user type, and at least one assigned user group are required for the user.





ACCESS CARD

This function allows you to activate the **access card mode** on the control panel.

Show the card to the reader so that the card number is linked to the selected user.

CENTRAL SETTINGS

  Timeout För Anslutning

Appen kopplas automatiskt ifrån centralen om den inte använts efter:

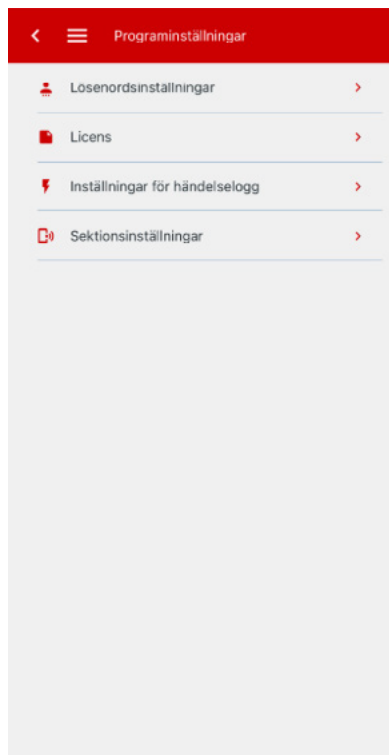
- ☐ 1 min
- ☐ 2 min
- ☐ 3 min
- ☐ 4 min
- ☒ 5 min

TIMEOUT FOR CONNECTION

When the app is not in use, it disconnects from the control panel. Select here after what time it should disconnect.



PROGRAM SETTINGS



PROGRAM SETTINGS

The settings allow you to configure your app.



PASSWORD SETTINGS

The menu allows you to enable or disable password authentication and change the password you created when you first opened the app.

Enable Password

Enable or disable password authentication for the program.

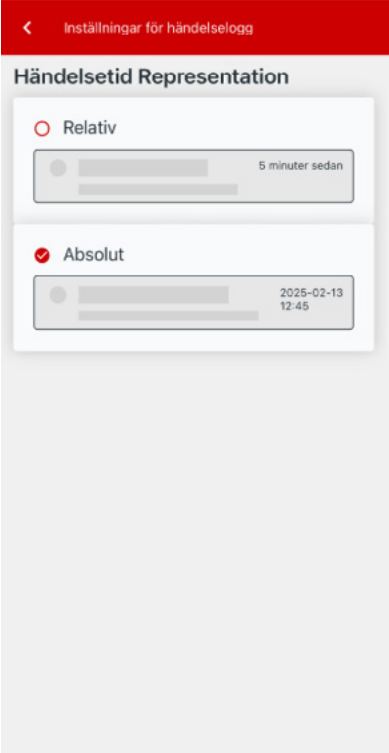
See also [Program Login](#).

! If the password requirement is disabled, security is lost as a code is not required for arming/disarming.

Change Password

If you want to change the password for the program, enter the old password and then enter and repeat the new password. Then click **SAVE**.

See also [Program Login](#).

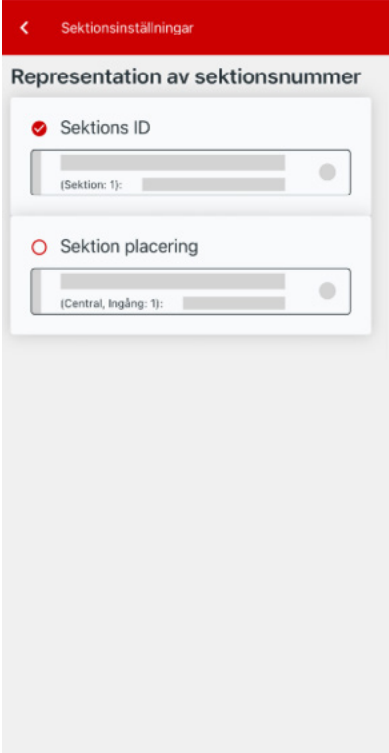


EVENT LOG SETTINGS

Here you choose how the event log is presented.

RELATIVE – shows how long ago the event occurred

ABSOLUTE – shows the detailed time



ZONE SETTINGS

Here you choose how the zones are presented

ZONE ID – shows zone number

ZONE LOCATION – shows location

GLOSSARY

SUPERVISOR

Supervisor code: Main code (code slot 2 by default)

Supervisor user: Alarm manager/Master user

- View event log
- Manage codes and users
- There can only be one Supervisor user

USER GROUPS

- **Supervisor group:** Full access in the app, access to all areas
 - An unlimited number of users can have this user group
 - Exception: Cannot view event log, manage users
- **Area, 1, 2 etc:** Users are only authorized for the respective area
- **Custom groups:** Technicians can, during installation, add multiple areas to a group and name it. The user will then have access to only this group.

REMOTE LOGIN AND REMOTE PASSWORD:

These are the user's login credentials for the control unit.

INHIBIT:

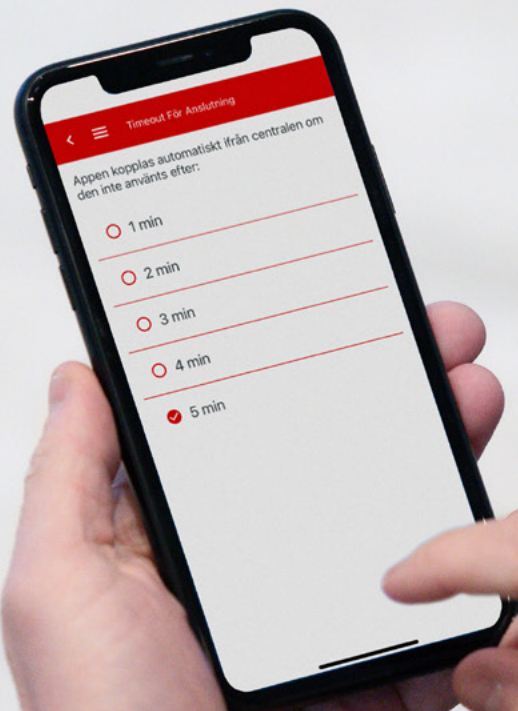
Temporarily disconnect the zone; no alarms will be triggered from the zone while it is inhibited, and you will not be able to see the status of the zone. The tamper alarm will still be active. Inhibited zones are automatically reconnected when the area they belong to is disconnected.

EXAMPLE: A detector that should not trigger a burglary alarm one night because it is broken or there is activity in the premises while other detectors in the area are active at night. The zone is reconnected when the area is disconnected.

ISOLATE:

The zone is completely disconnected until it is manually reconnected again. Both alarm and tamper are disconnected.

EXAMPLE: A detector has been hit by a truck in the warehouse, and the service technician cannot come and fix it until next week. Note that this is only done in consultation with Securitas Direct.



Timeout För Anslutning

< ☰

Appen kopplas automatiskt från centralen om den inte använts efter:

- ☐ 1 min
- ☐ 2 min
- ☐ 3 min
- ☐ 4 min
- ☒ 5 min



Securitas Direct Pro is a free app available in App Store and Google Play.
For facilities with requirements according to SSF130:9, the function can be deactivated.

