REDZ
SMART COMMUNICATION

ZRAUTOMATION.CLOUD

User and Administrator Manual

Written for ZRAutomation.Cloud 3.3.5.1 and the mobile app 1.1.0.

Contents

1 Introduction and system overview
2 Installation and updates
3 Licence and support
4 Signing in
5 Devices and channels
6 Dashboards and widgets
7 Cameras
8 Alarms
9 Logic and automations
10 History, analysis and export
11 Users, roles and permissions
12 Remote access and the mobile app
13 System logs, health and settings
14 Troubleshooting
15 Moving from ZR Automation
A Permissions

1 Introduction and system overview

Everyone

ZRAutomation.Cloud runs on a server at the site, on the site's own network. It reads the site's devices every 3 seconds, shows their values, switches their outputs, keeps their history, raises alarms and runs the site's time blocks and scenarios. It keeps doing all of this whether or not anyone is looking at a screen, while its trial or licence runs (see Licence and support).

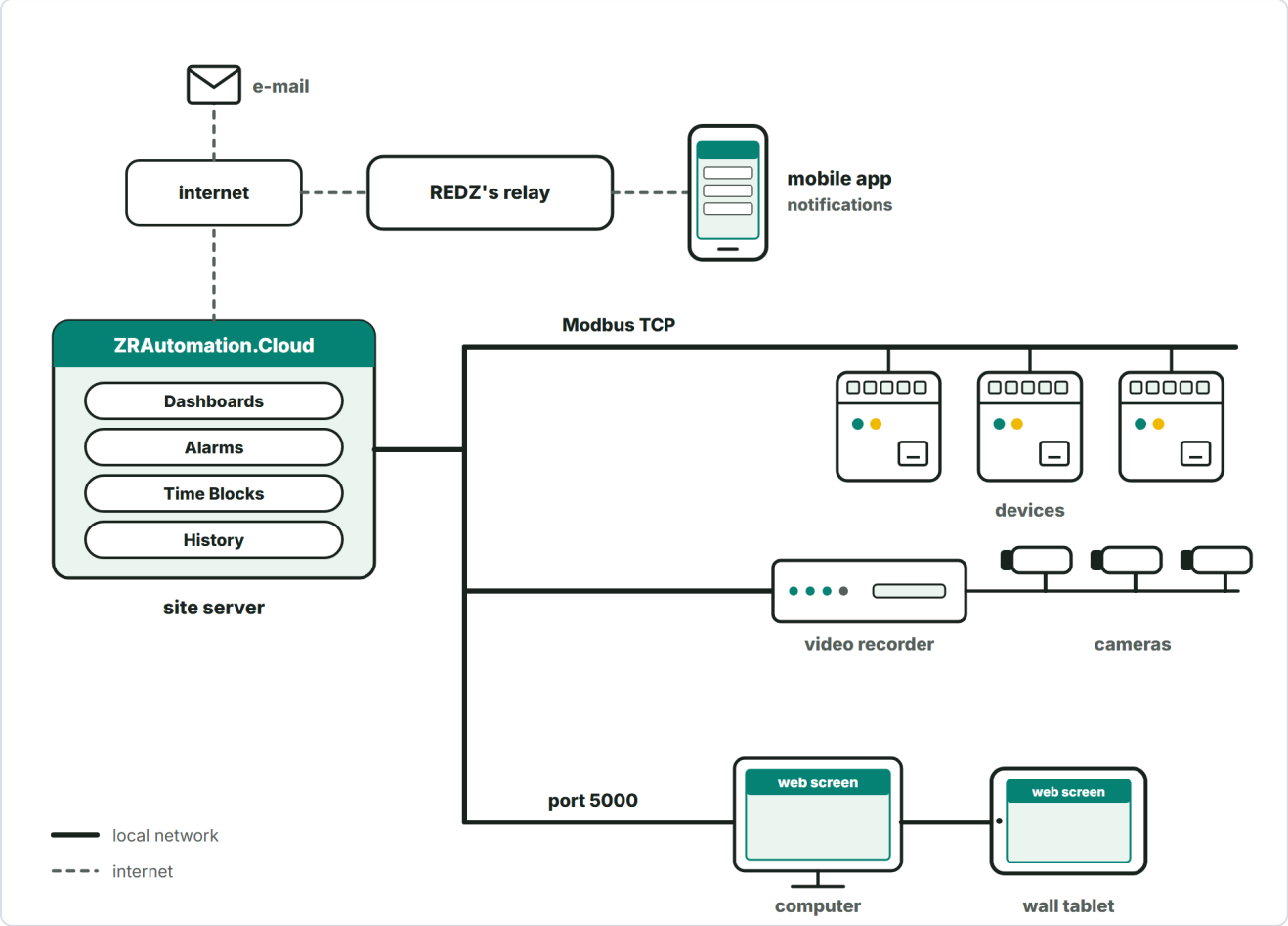


Figure 1.1 The system at a glance: the site server reads the devices and the video recorder on the local network; people use the web screen there, or the mobile app from outside through REDZ's relay.

The parts of the system

- The site server runs the site. Everything the system does happens there.
- The web screen is opened in a browser on the site's local network, on a computer or on a wall tablet. It is where the site is set up and run.
- **Help** at the top right of the web screen opens this manual on redzsoftware.com in a tab of its own, so it needs the internet. The manual there describes the newest version. On a narrow screen only the button's question mark is shown.
- The cameras are shown through the site's video recorder; the pictures come through the site.

- Remote access connects the site to REDZ's relay, so that the mobile app can reach it from outside the local network.
- The mobile app shows the site on a phone, through remote access, and tells the phone about alarms.

Ask ZR

Ask ZR in the top bar, or Ctrl+K anywhere after signing in, opens a box for a short request in English. It finds a page or a tab ("alarm history", "time blocks", "users"), a card of System Settings ("backup", "licence"), a device, a camera or a dashboard page by its name, a chart ("history greenhouse last 7 days"), the offline devices, the errors in the System Logs, and short answers to questions such as "how do I add a device?" It answers as you type; Enter opens the first answer.

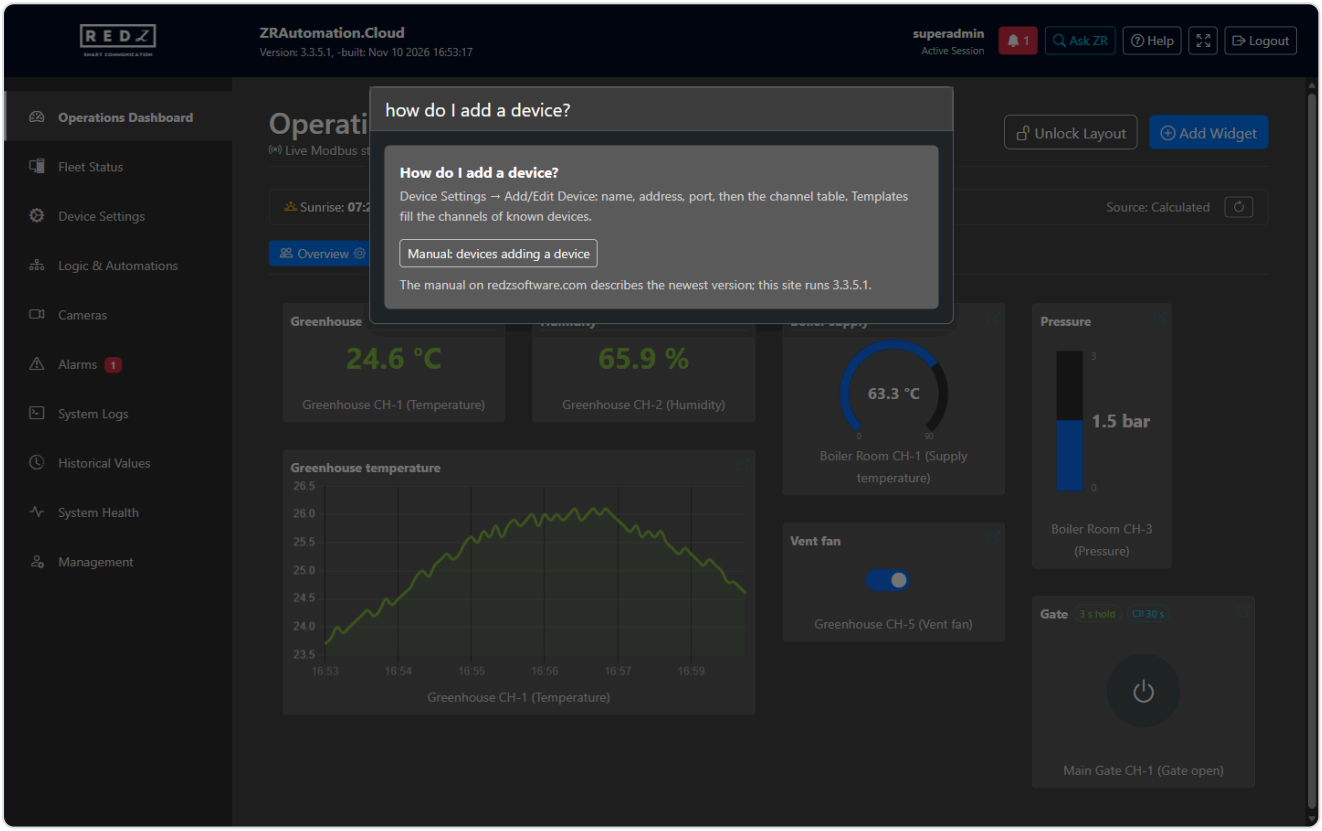


Figure 1.2 Ask ZR over the dashboard with the answer to "how do I add a device?": a short answer and a button that opens this manual's section on redzsoftware.com.

A chart opens with the nearest range the **Historical Values** page offers. A "how do I" answer has a button that opens the section of this manual on redzsoftware.com.

Ask ZR offers only the pages, devices and cameras your role can see, and it changes no setting itself. Asked to send the support package, it opens the **Diagnostics** card after **Confirm**; the package is sent there (see Licence and support).

A request it does not know gets **Not in the list yet** and is kept on the site, with its time but not who asked, so that a later version can learn it. The **Diagnostics** card lists these

requests, newest first.

Accounts and roles

Everybody signs in with an account of their own. The account's role decides which pages and devices it sees and what it may change, on the web screen and in the app alike (see Users, roles and permissions).

What needs the internet

The site, its devices, the web screen on the local network, the cameras and the time blocks, including those that follow sunrise and sunset, work without the internet. Remote access and the mobile app, the notifications on the phones, e-mail and this manual behind **Help** need it.

2 Installation and updates

Administrators

ZRAutomation.Cloud is installed on the site server by REDZ or by a person REDZ has authorised, with its setup program. This chapter says what the server needs, what the setup program sets up, and how an update is done.

What the server needs

- A computer at the site that stays switched on, on the same network as the site's devices and its video recorder. The site works only while this computer is running.
- 64-bit Windows: Windows 11, Windows 10 Enterprise LTSC or IoT Enterprise LTSC, or Windows Server 2016 or later. The setup program stops on 32-bit Windows.
- Nothing else to install: the program brings everything it needs, including the part that decodes the camera pictures.
- The computers and tablets that open the web screen reach the server on port 5000: the web screen's address is the server's address followed by :5000. The setup program opens that port in the Windows firewall for the server's own local network only.
- For remote access, an internet connection from the server. The site connects out to REDZ's relay; no port has to be opened towards the site.

What the setup program sets up

- The setup program runs with an administrator account on the server. It installs the program in C:\Program Files\REDZ\ZRAutomation Cloud and at the end can open the web screen on the server.
- The program runs as a Windows service named ZRAutomation.Cloud, under its own Windows account, NT SERVICE\ZRAutomation.Cloud. It starts with Windows, shortly after the other services, and works without anyone signed in to the server. If it stops by itself, Windows starts it again after a minute, the first two times in a day.
- The setup program starts the service and waits for the site to answer; if it does not, the setup program says so.
- The site keeps its data in C:\ProgramData\REDZ\ZRAutomation Cloud: the database, the licence, the copies of the database and the setup program's record. Only the server's administrators and the service can open that folder. At its first start the site creates its database there.
- It also creates an administrator account named superadmin. Its one-time password is written to a file in that folder, which only the server's administrators can read. The password must be replaced at the first sign-in (see Signing in), and the file is deleted when it is.
- What the setup program did is written to setup.log in the same folder.

Devices, cameras, accounts and roles are then set up on the web screen, as the following chapters describe.

From its first start the site runs as a trial for 30 days; Licence and support says how a licence is activated.

A site that was installed before the setup program existed is taken over by it: the setup program finds the ZRAutomation.Cloud service and updates the site in its own folder.

An earlier version kept the site's data in the program's folder. Such a site moves at its next update: the setup program copies the data to C:\ProgramData\REDZ\ZRAutomation Cloud and gives the service its own account. The old copy stays in the program's folder until the update after that removes it.

Which version is running

The site's version and the date it was built are in the banner at the top of the web screen. A narrow screen leaves that line out. The **System Health** page shows how long the site has been running since it last started.

Updates

An update is installed by running the new version's setup program on the server. It stops the service, copies the site's database into the Backups folder of the data folder, keeps the program files it replaces or no longer has, puts the new ones in place, starts the service and checks that the new version answers. The database, the licence and the site's settings files are never replaced. The last five copies of the database are kept.

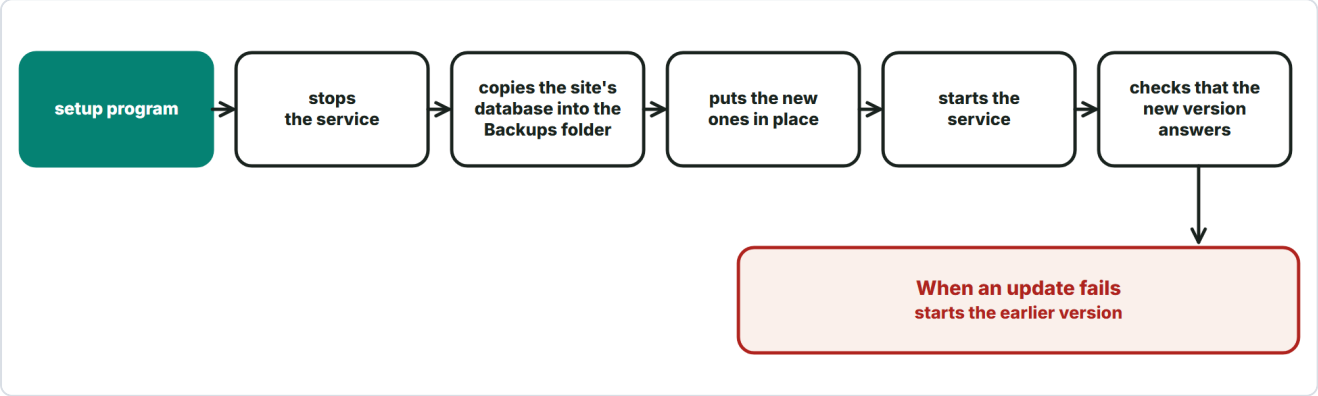


Figure 2.1 An update by the setup program, step by step; when an update fails, the earlier version is started.

While the service is stopped the site does not read its devices or run its time blocks and scenarios. When it starts again, a time block start or end that fell in that time is written late, until the block's other time. The history leaves that time out, as it does any time a device was not read.

The site's data stays: devices, history, alarms, accounts and settings are in the database, which an update does not replace. When a new version needs the database changed, the site does it by itself at its first start and writes an entry about it in the **System Logs**.

A web screen left open during an update keeps trying to connect again for as long as the service is stopped. When the connection comes back with a new version, the screen says so in the banner and reloads itself. If it opens on the sign-in page, sign in again.

When an update fails

If the new version does not start or answer, or one of its files cannot be put in place, the setup program puts the earlier program files, the service's settings and the copy of the database back, starts the earlier version and says that the update failed. The site then runs as it did before the update.

Going back to the earlier version

If an update that went through has to be undone, REDZ puts the earlier version back. The data is kept, so what was entered after the update stays. What the update added is not available until it is installed again.

Removing the program

The program is removed from the list of installed apps in Windows. That removes the service, the firewall rule and the program's files. The data folder stays, with the database, the licence, the copies of the database and setup.log, and a later installation carries on with them.

3 Licence and support

Administrators

A new installation runs as a trial for 30 days, with every part and no limit on the number of devices. The trial begins the first time the site starts without a licence; deleting the site's licence files does not start it again.

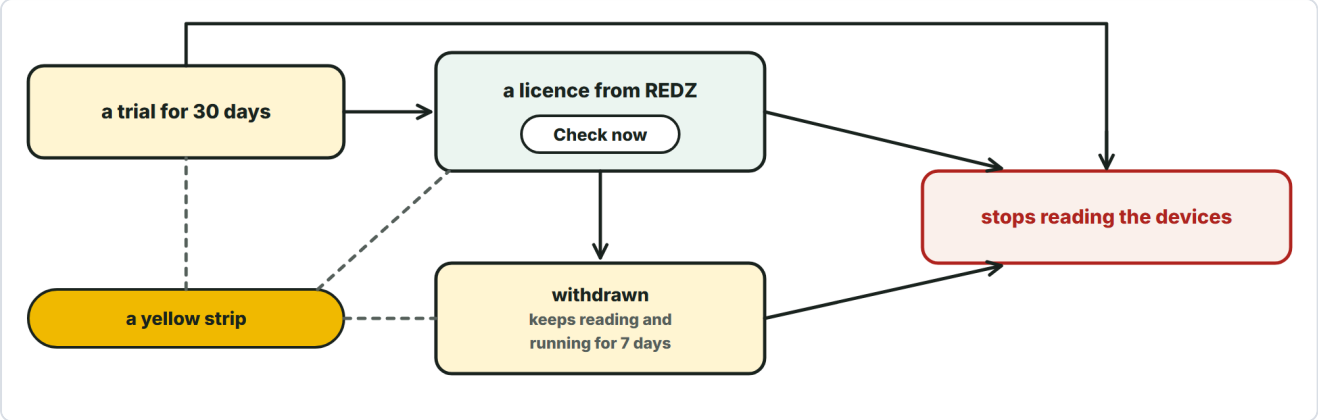


Figure 3.1 The licence over time: a 30-day trial, then a licence from REDZ (Check now); a withdrawn licence keeps the site reading for 7 days, then it stops reading the devices; the yellow strip shows in between.

To keep the site reading and running after the trial, the site needs a licence from REDZ made for this server. A licence names the customer and the number of devices the site may have; it can also have an end date and a maintenance date.

The **License** card is on the **System Settings** tab of the **Management** page, for a role with the **Management** permission and the Edit action. Below it are the cards that get a licence for the site.

Getting a licence online

A server that reaches the internet can get its licence from the REDZ licence server, in one of two ways.

1. In **Request a licence**, fill in **Name**, **Company** and **E-mail**; the phone and the note are optional. Tick the agreement and select **Send request**. The server's machine code goes with the request.
2. The card shows the request number while it waits for REDZ. The page asks every 30 seconds while it is open, and the site asks every 15 minutes. When REDZ approves, the licence loads by itself and the site reads and runs at once.

While a request waits, **Check now** asks at once and **Withdraw the request** takes it back. If REDZ declines it, or it is no longer on the licence server, the card says so; **OK** clears the message and shows the form again.

If REDZ has already given you a licence key, enter it in **Activate with a key** and select **Activate**. The licence server sends back a licence for this server and the site reads and

runs at once.

Activating offline

A server without internet takes a licence file instead. Open **Activate offline**.

1. Copy the **Request code of this PC**, or let REDZ scan the QR code beside it, and send it to REDZ. The code identifies this server and holds no secret.
2. REDZ sends back a licence file (.zrl) made for this server.
3. Under **Licence file**, choose the file and select **Load license file**. The card shows the licence and the site reads and runs at once.

On a virtual machine the card does not offer a file: there the licence is activated online only.

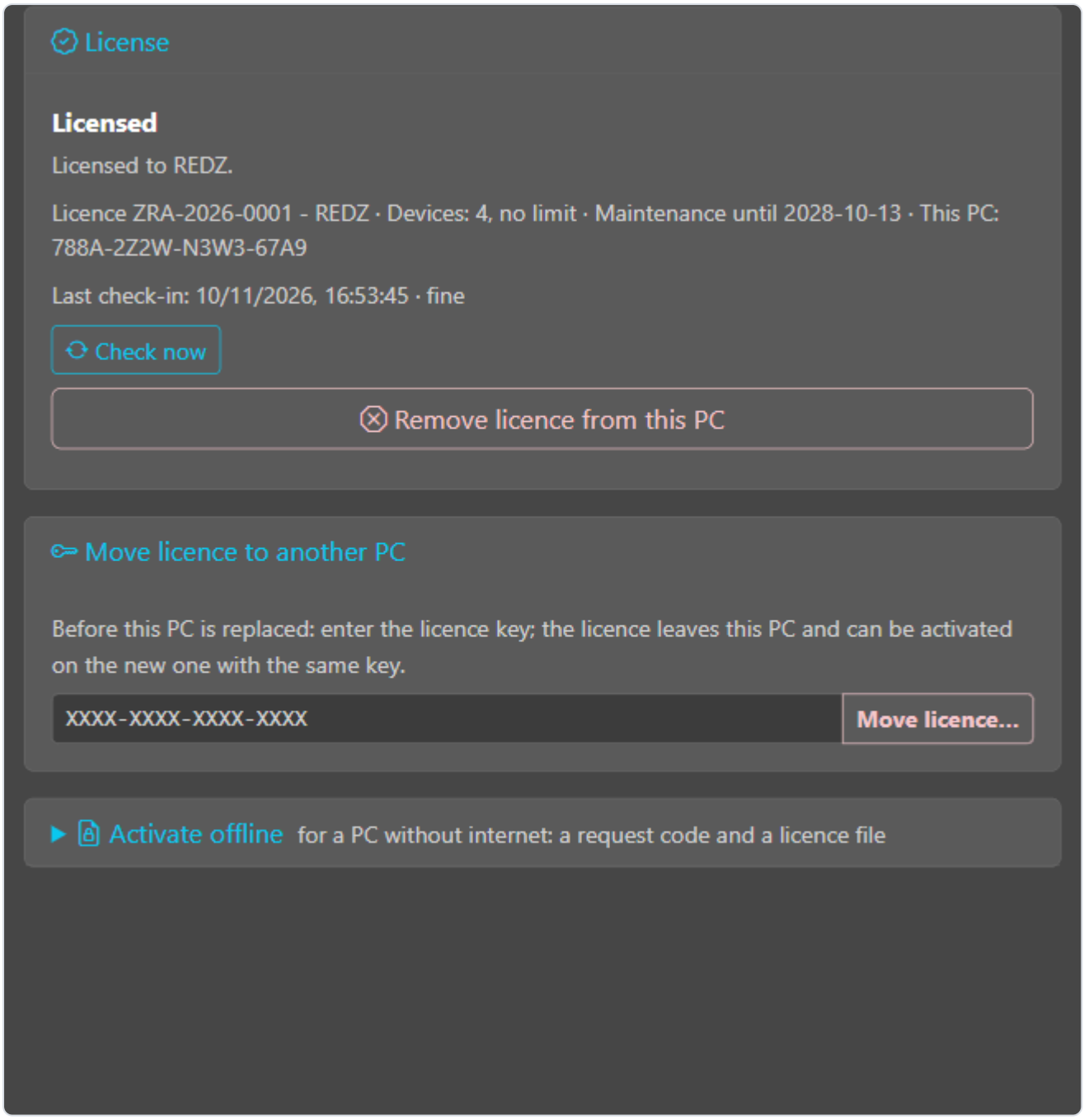


Figure 3.2 The licence cards with a licence activated online: its state and details, the last check-in with Check now, moving the licence to another PC, and Activate offline closed.

A licence works only on the server it was made for. On another server it does not run: ask REDZ for a licence for that server.

Checking in

A licence activated online checks in with the licence server every 7 days. It sends the licence number, the machine code, the version and the number of devices, nothing else. The card shows the last check-in, and **Check now** checks in at once. A licence loaded from a file does not check in.

If the licence server cannot be reached, the site carries on as before. If the server says the licence was withdrawn or moved to another server, the site keeps reading and running for 7 days from that first answer and the card says so; contact REDZ.

On a virtual machine the licence checks in every day and needs the licence server at least once in 7 days; after that the same 7 days begin. If the server sees a copy of the virtual machine, or one put back from a snapshot, that copy stops reading and running at once.

When the site stops reading

When the trial or the licence has ended, or the licence was withdrawn, the site stops reading the devices and stops its automation and alarms, and no output can be switched by hand or started for a time. A timed output that is already on is still turned off at its time. The data, the history and its export and the **License** card stay open: once a licence is activated, the site carries on.

During the trial, and with a licence that has an end date, the site also stops when the server's clock is put back more than 24 hours behind a time it has already seen, until the clock is right again.

The strip at the top

During the trial, in the last 7 days of a licence, in the days after the licence server says the licence was withdrawn, and after its maintenance date, a yellow strip at the top of the web screen and of the app says so. When the site does not read or run, the strip is red and says why. Every account sees it.

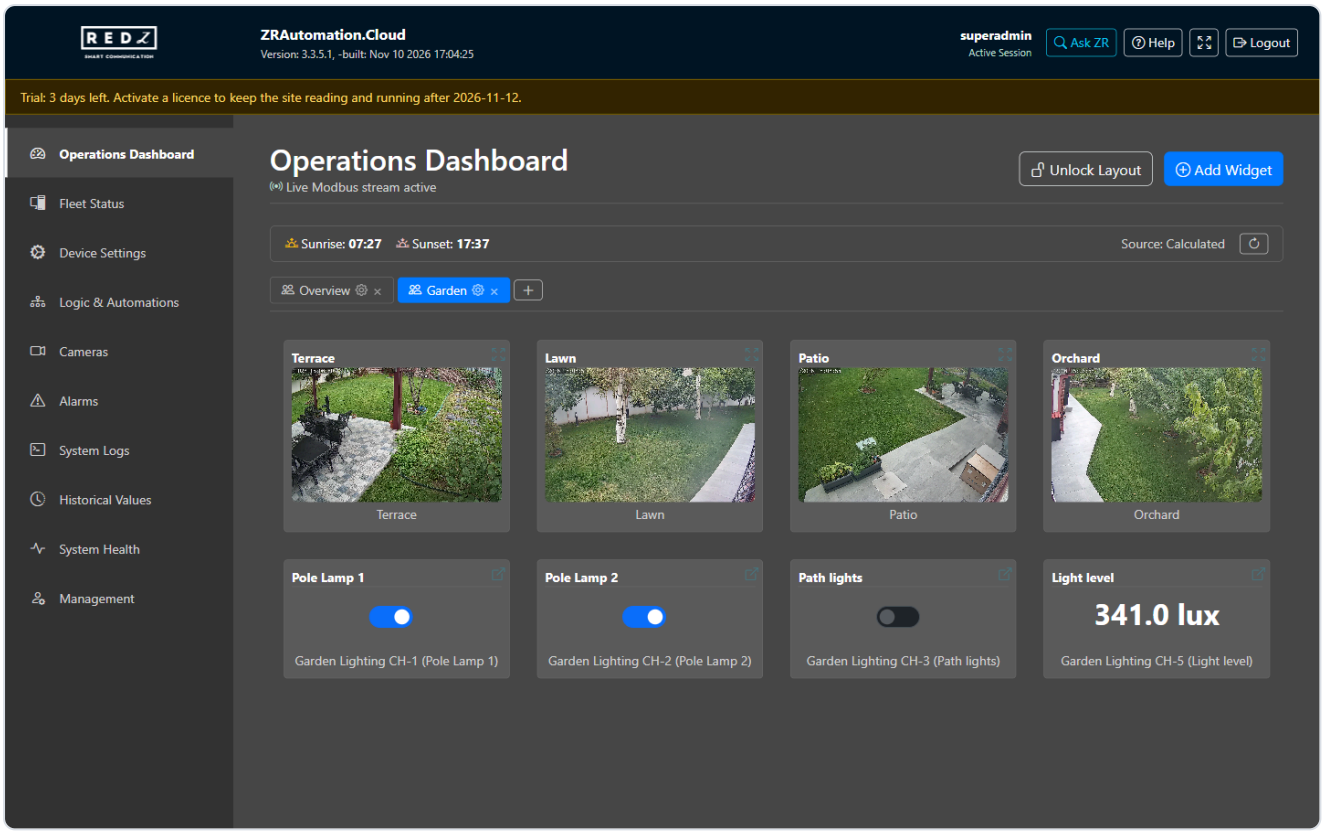


Figure 3.3 The yellow strip at the top of the web screen while the site runs on its trial.

The accounts whose role has the **Management** permission are told by e-mail and on their phones, once a day in the last 7 days and once when the site stops.

Devices and the licence

When the site has as many devices as its licence allows, adding another is refused; the devices already set up are kept. A restore from a backup adds devices only up to the limit and says how many it left out.

Moving or removing a licence

Before a server with an online licence is replaced, enter the licence key in **Move licence to another PC** and confirm. The licence server frees the licence, the licence leaves this server, and it can be activated on the new server with the same key. The site here then stops reading and running, unless its trial days are still running.

Remove licence from this PC takes the licence off this server without asking the licence server, for example for a licence loaded from a file. The site then stops reading and running until a licence is activated again, unless its trial days are still running; the confirmation says until when. The card shows a removal code: send it to REDZ.

The support package

The **Diagnostics** card, for a role with the **Management** permission and the Edit action, has **Download support package**: a file for REDZ's support with the site's version and licence

state, its settings without passwords, keys or codes, its devices with their addresses, its cameras with their recorder channels, the system log of the last 30 days and the requests Ask ZR did not know. The readings, the history, the database and the backups are not in it. It holds the addresses of the site's equipment: send it only to REDZ.

When the site can reach the REDZ licence server, the card also has **Send to REDZ support**. Write what happened if you like, check the name, e-mail and phone, tick the agreement and select **Send**. The same package goes straight to REDZ support with your note, the contact details, the licence number and the server's machine code, and the card shows a ticket number. Nothing is sent without the agreement, which says what the package holds and how long REDZ keeps it.

4 Signing in

Everyone

On the site's local network, open the site's address in a web browser. Enter your **Username** and **Password** and select **LOGIN**. The pages you see depend on your role.

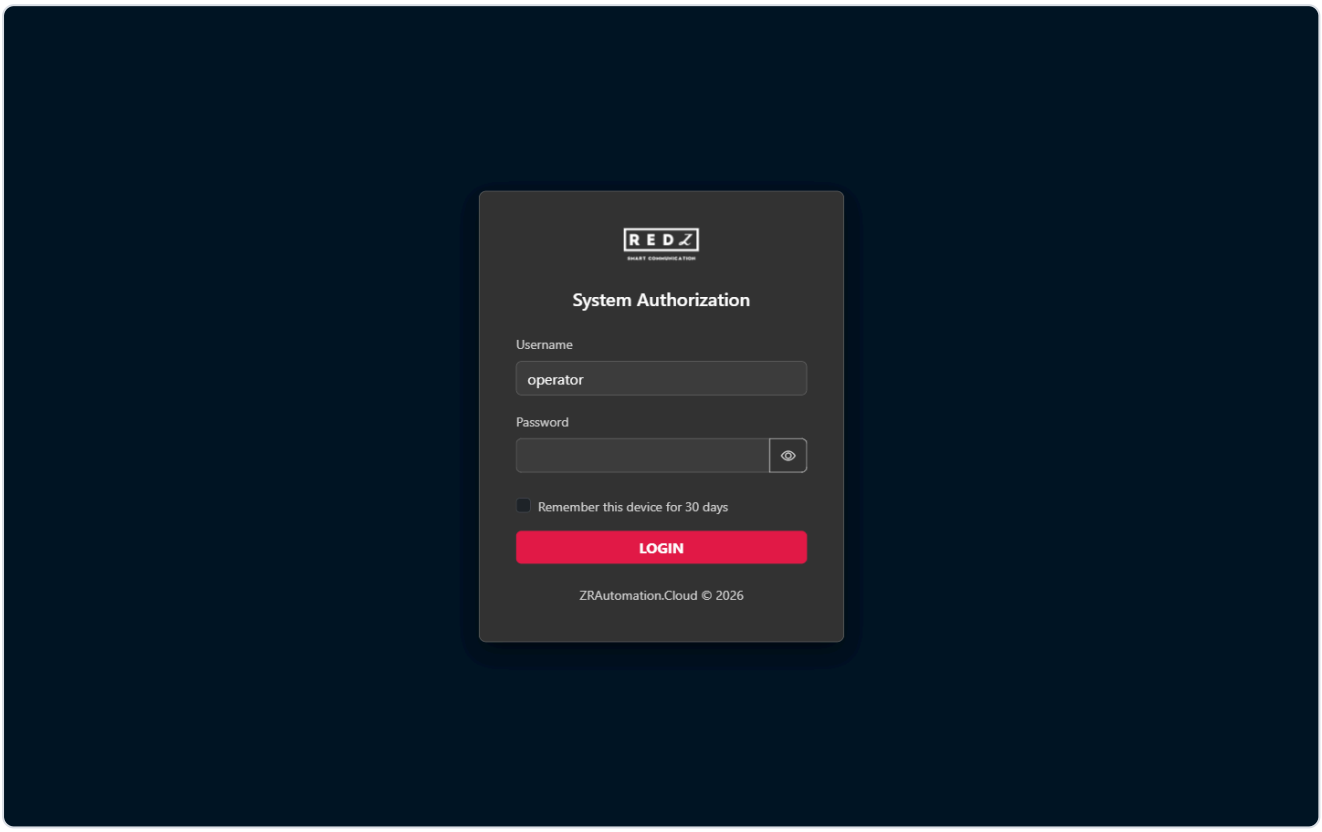


Figure 4.1 The sign-in page of the web screen.

A sign-in lasts 8 hours without use. With **Remember this device** ticked, it lasts 30 days without use instead; an administrator with access to all devices can change the number of days in **Keep signed in for (days)** in System Settings. A screen that stays open, such as a wall tablet, renews its sign-in by itself. When a sign-in ends, the screen returns to the sign-in page.

Wrong passwords

After 5 failed attempts the account is locked for 15 minutes. Wrong sign-in codes count as failed attempts too. A completed sign-in clears the count.

Setting a new password

The administrator account of a new installation must set a new password at its first sign-in. The screen then asks for a **New Password** and for the same password again in **Confirm New Password**. A password has at least 10 characters.

Signing in from outside the site

From outside the local network you sign in with the mobile app, through remote access. Your role needs the **Remote Login** permission. A role with access to all devices has it only when it is ticked.

If an administrator has turned on **Require a mailed code for sign-ins from outside the local network**, the app also asks for a **Sign-in code** of 6 digits, sent to the e-mail address of your account. The code is valid for 10 minutes. **Send a new code** works after 60 seconds. After 5 wrong entries the code can no longer be used.

While codes are required, an account without an e-mail address cannot sign in from outside, and a sign-in is refused when the code cannot be mailed.

With **Remember this device** ticked on the app's **Site setup** screen, that phone is asked for the code once and then not again for the number of days set in **Remember a device for (days)**, 30 unless changed. Changing your password makes every remembered device ask for the code again.

5 Devices and channels

Everyone, with administrator parts

The site reads Modbus TCP devices on its network. Each device has channels: the inputs and outputs the site reads and, for outputs, writes.

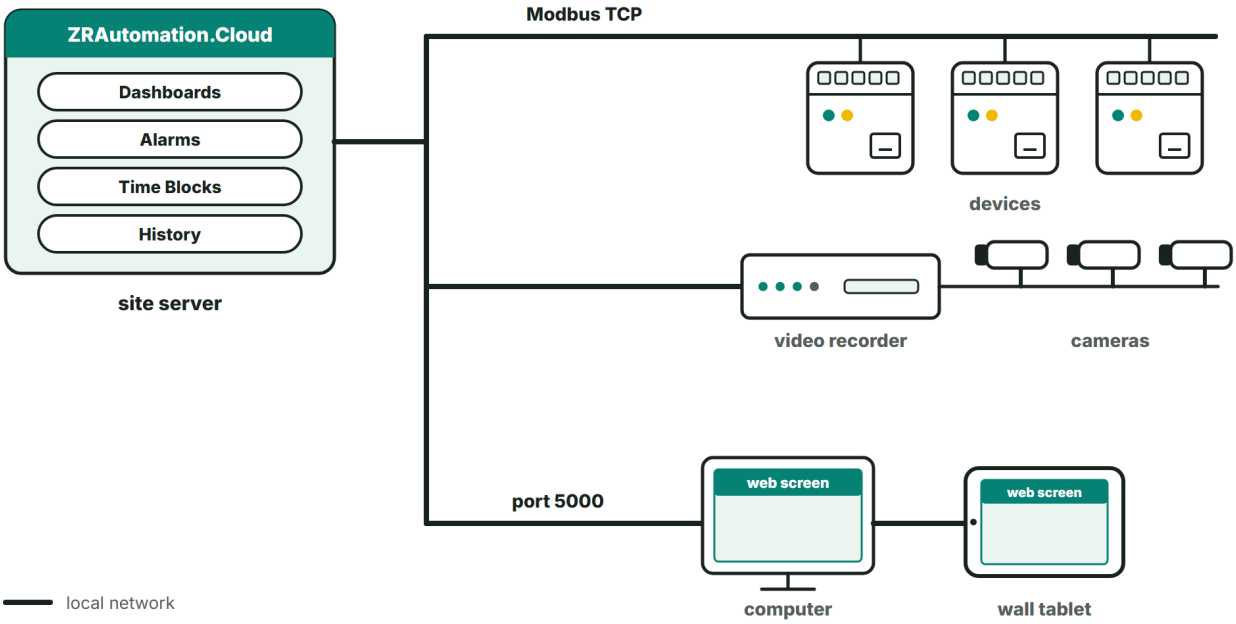


Figure 5.1 On the local network: the site server reads the devices over Modbus TCP and the cameras through the video recorder; computers and a wall tablet open the web screen on port 5000.

Fleet Status

Fleet Status shows the devices your role covers, as cards or as a list. A device the site is reading is ONLINE. An OFFLINE device shows when the site last read it, or that it has not been read since the site last started. Search by name or address, or show **All**, **Online** or **Offline** devices.

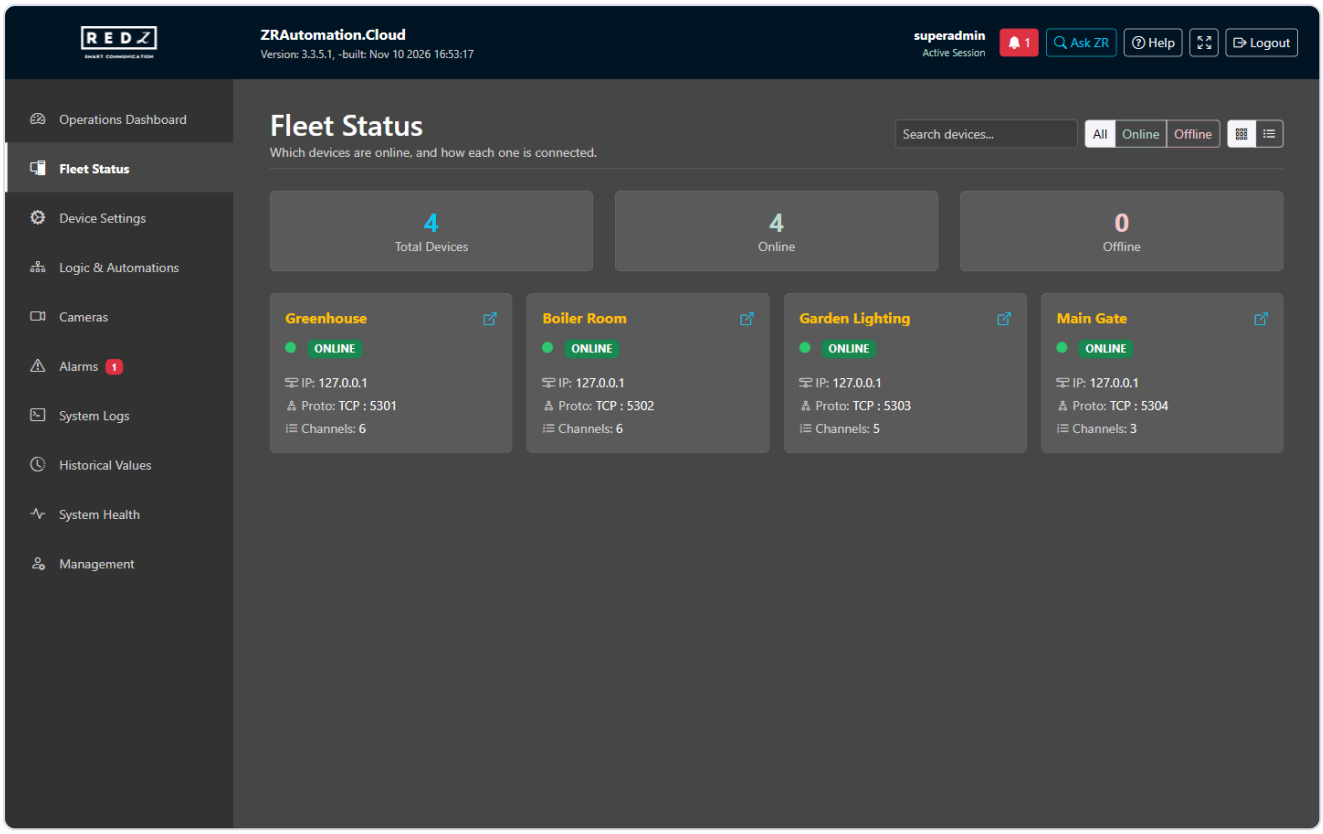


Figure 5.2 Fleet Status as cards: each device with its state, address and channels.

The device page

Open a device from its card in Fleet Status, from the device list, or with the button in a dashboard widget's corner. The page shows the device's address, when it was last read, and each channel with its live value. Show **All** channels, only **Outputs** or only **Inputs**, or search them.

In the Control column a digital output is switched and an analog output is given a value within its range. Changing an output needs the **Edit (Update)** action. While the device is offline the controls are locked.

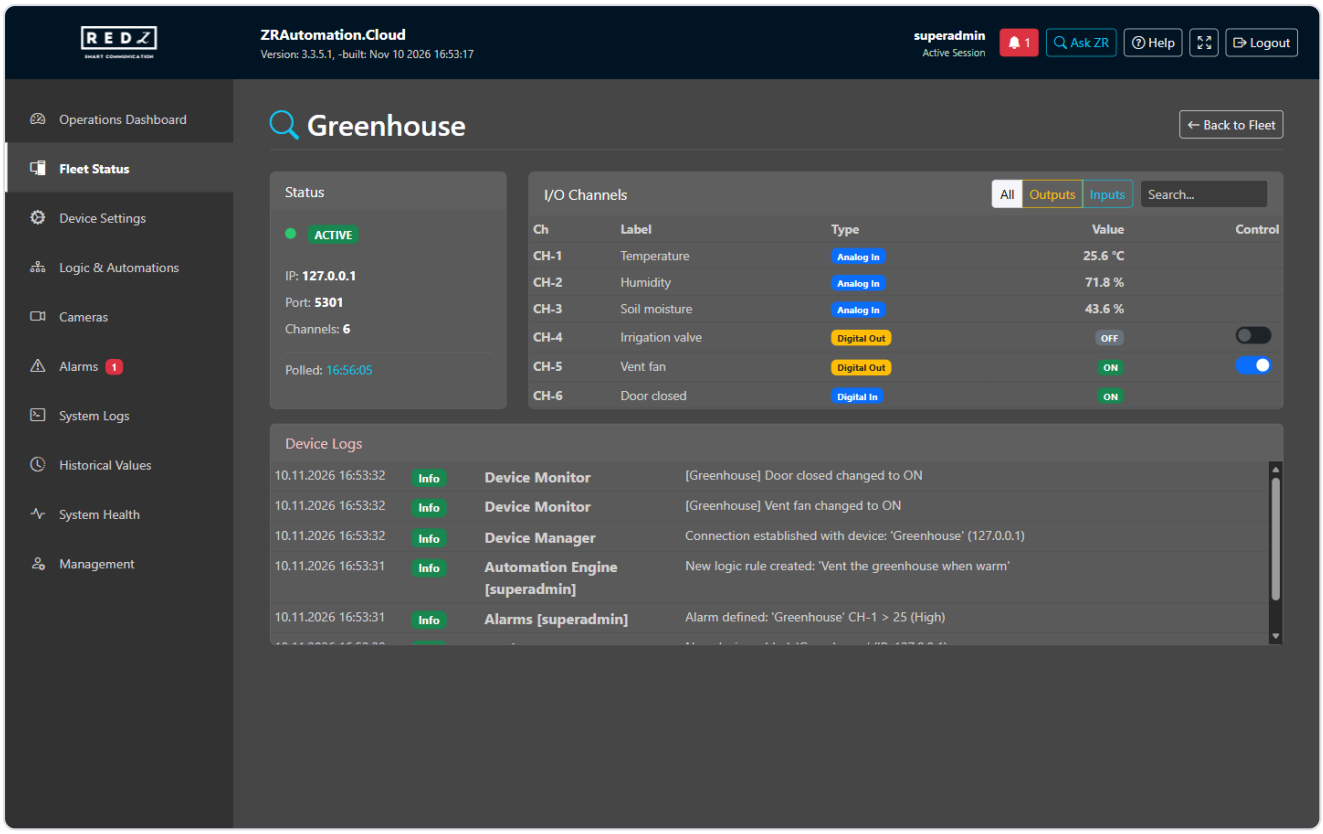


Figure 5.3 The page of one device: its state and each channel with its live value and, for outputs, its control.

A channel's past values are on the **Historical Values** page.

Adding a device

Devices are added and changed on the **Device Settings** page, which lists them on its **Devices** tab. Adding a device needs the **Add (Create)** action; changing one needs **Edit (Update)**.

1. Open the **Add/Edit Device** tab.
2. Under **1. Connection**, enter a **Name**, the device's address in **IP / COM Port** and its **Port** (502 unless the device uses another).
3. In the **Batch IO Configurator**, add a row for each group of channels: how many, the unit id, the signal type, the function code, the data format and the first address. **Generate Channels** fills the channel table; the addresses step by the width of the format.
4. Check the channels in the table and add a label, a unit and, where needed, a scale.
5. Select **Save Device**.

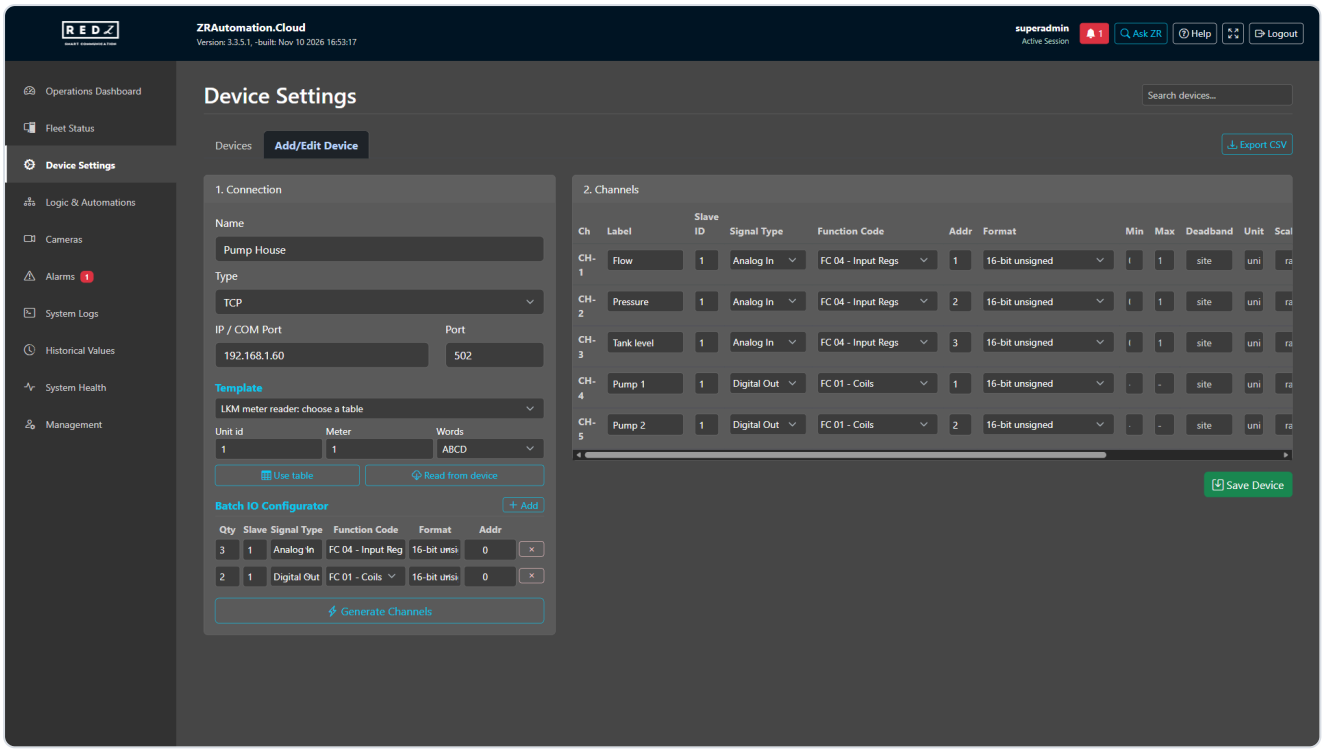


Figure 5.4 A new device on the Add/Edit Device tab: its connection, two rows of the Batch IO Configurator and the channels they generated.

The channel table

COLUMN	WHAT IT HOLDS
Ch	The channel's number on this device, such as CH-1. The site gives it when the channel is created.
Label	A name you choose for the channel. Widgets and lists show it next to the number.
Slave ID	The Modbus unit id the channel is read from, 1 unless the device says otherwise.
Signal Type	Analog or digital, input or output.
Function Code	Which Modbus table the channel is in: coils, discrete inputs, holding registers or input registers.
Addr	The channel's address in that table.
Format	How the register(s) behind this channel are read. A 32-bit channel also occupies the register after its address. Writes always go out as one raw register.
Min	Analog min output limit
Max	Analog max output limit
Deadband	How far a reading has to move before it is kept in the channel history. Empty uses the site default; 0 keeps every change. The live value and the automations always see every reading, and readings never reach the system log at all.
Unit	What the value is counted in - a label only.
Scale (raw → value)	The device's raw span and the span of the quantity it stands for (4-20 mA → 0-10 bar). The site applies it when it reads, so the screen, the history, the automations and the phone all see the scaled number; a write goes back as the raw count. Values recorded before a change keep their old scale.
Counter	A counter only grows - an energy register, a pulse total. Historical Values can then show how much it counted in each interval.

Data formats

A register channel (FC 03 or FC 04) is read in one of these formats. A 32-bit format uses two registers and a 64-bit format four.

FORMAT
16-bit unsigned
16-bit signed
32-bit unsigned (ABCD)
32-bit unsigned (CDAB)
32-bit signed (ABCD)
32-bit signed (CDAB)
32-bit float (ABCD)
32-bit float (CDAB)
64-bit float (ABCD)
64-bit float (GHEFCDAB)

LKM meter readers

For an LKM meter reader the channels can be filled from a table instead. Choose the reader's table under **Template**, set its **Unit id** and which **Meter** it is, then select **Use table**. **Read from device** asks the meter reader which table it uses.

Copying and exporting

The **Clone device** button in the device list makes an inactive copy of a device. **Export CSV** saves the devices your role covers and their channels in one CSV file.

6 Dashboards and widgets

Everyone

The **Operations Dashboard** shows live values from your devices as widgets, arranged on one or more pages. If your role has this page, it is the page that opens after you sign in.

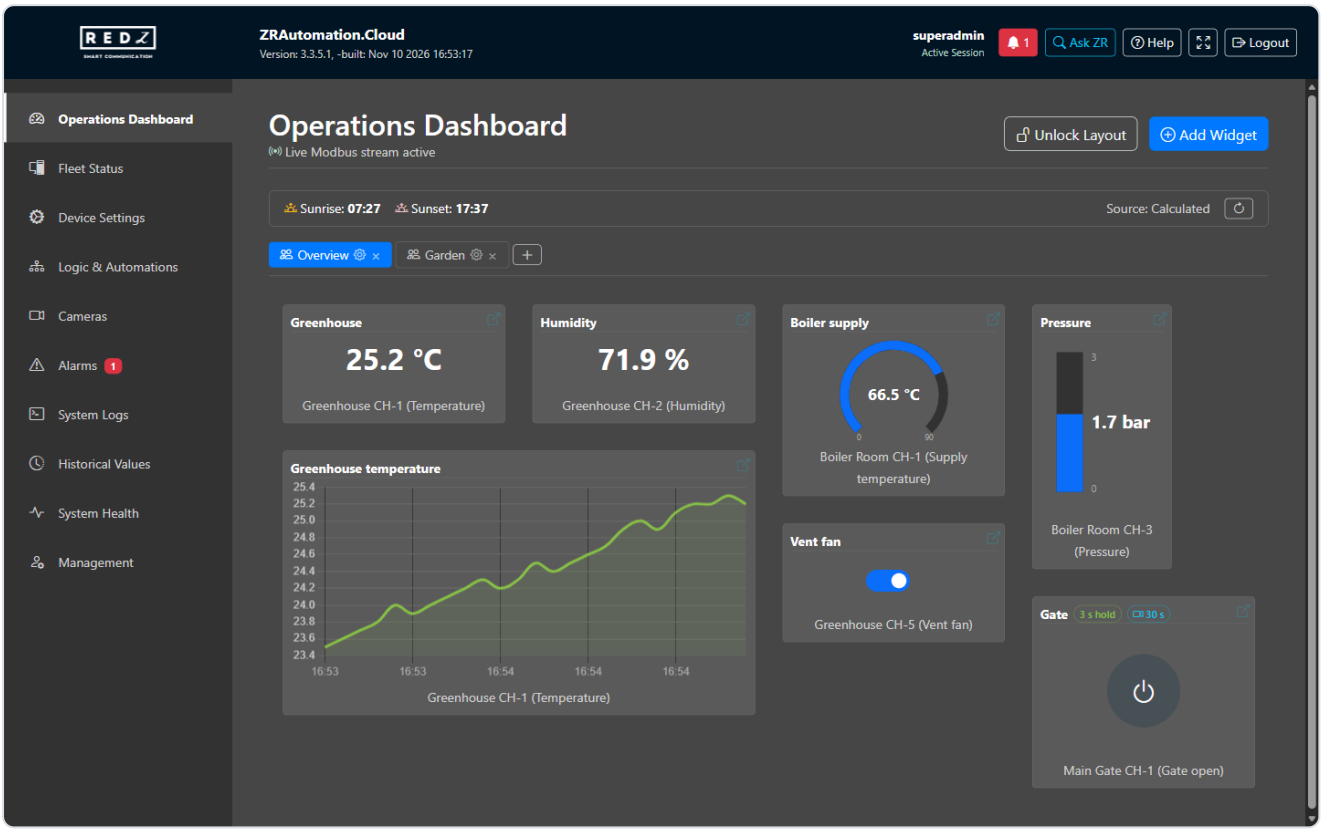


Figure 6.1 A shared page with value, gauge, bar, trend, switch and button widgets. The Gate button holds its output for 3 seconds and opens a camera for 30 seconds when used.

Pages

The pages are shown as tabs above the widgets. A shared page, marked with a people icon, is seen by every user. A personal page, marked with a person icon, is seen only by you.

To add a page, select + at the end of the tabs. In **Page Settings**, enter a **Name** and turn on **Shared page** if every user should see it. Anyone can add personal pages; adding or changing shared pages needs the **Shared Dashboards** permission.

On a page you may change, the gear on its tab opens its settings and the x deletes it. The last shared page cannot be deleted or made personal.

If your role cannot change a shared page, **Copy to My Dashboards** makes a personal copy of it that you can change.

Each browser remembers the last page you chose and opens it the next time. When that page is not there for you, the first page opens, and the page you chose stays remembered.

Widget types

TYPE	WHAT IT SHOWS
Value	The channel's latest value with its unit.
Switch	An on and off switch. Turning it on writes 1 to the channel; turning it off writes 0.
Trend	A line chart of the channel's recent values, updated as new values arrive.
Gauge	A dial showing where the value stands within a range you set. For a role with the Alarms permission, the channel's limit alarms that are on are marked on it. Not available for digital channels.
Bar	The same as a gauge, drawn as a bar.
Camera	A camera picture. Selecting it opens the camera full screen.
Button	For digital outputs only. Without a duration, the output is on while you hold the button and off when you let go. With a duration, one tap turns the output on and the site turns it off after that time, even if the browser tab is closed.

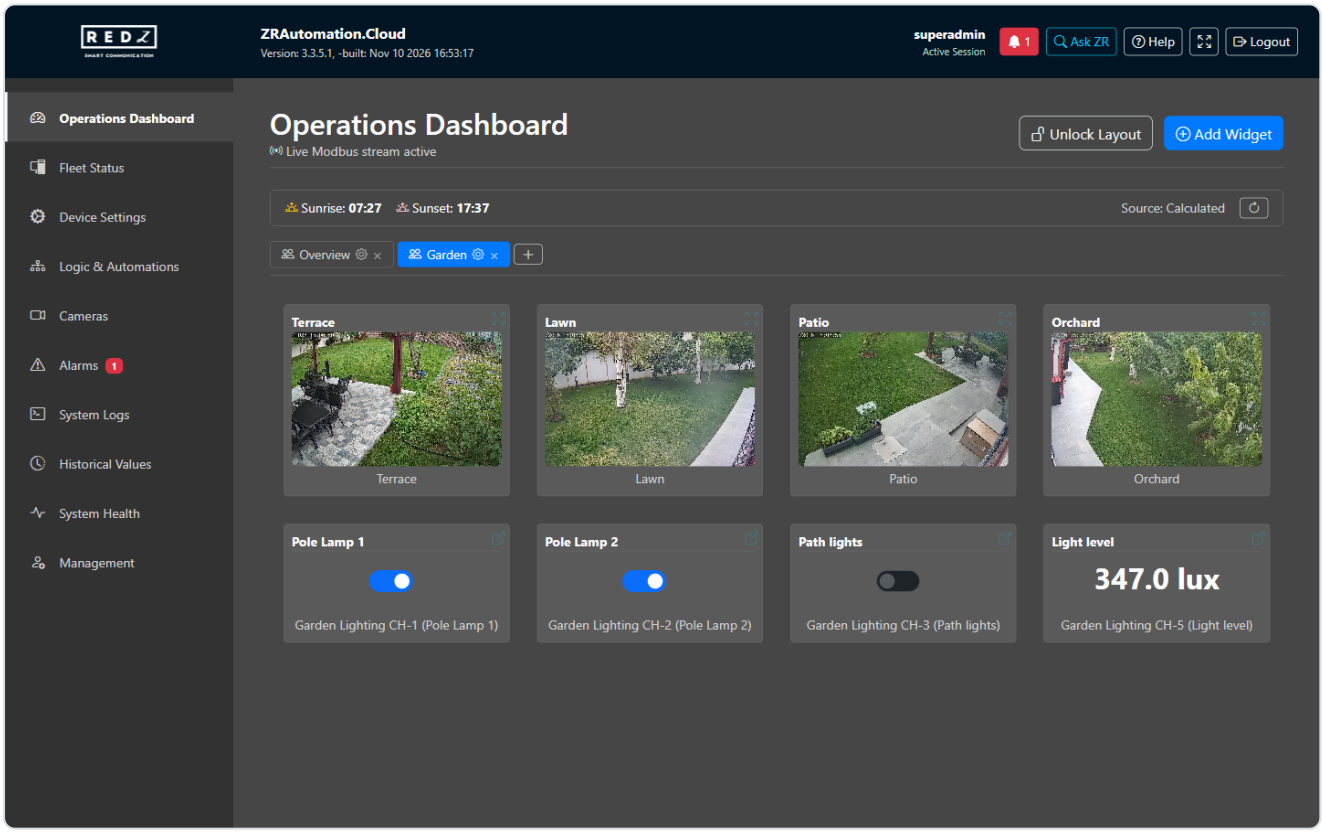


Figure 6.2 A shared page with four camera widgets and the garden lighting.

Adding a widget

1. Select **Add Widget**.

2. In **New Widget**, enter a title and choose the device, the channel and the widget type. A button can be chosen only for a digital output, and a gauge or a bar not for a digital channel.
3. For a gauge or a bar, set the range in the channel's units. For a button, set a duration in seconds, or leave it blank to press and hold.
4. For a switch or a button, you can choose a camera under **Show a camera when used**: using the widget then opens that camera on the screen for the number of seconds you set.
5. Select **Add Widget** at the bottom of the window.

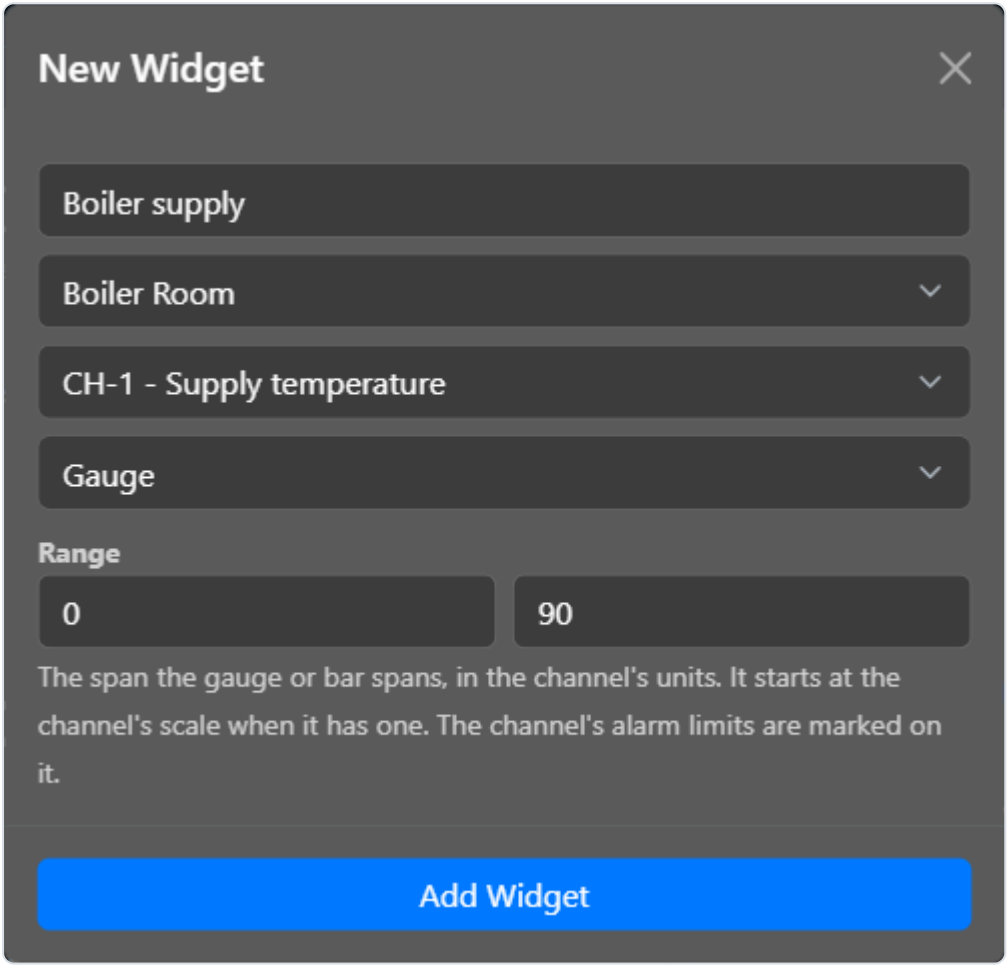
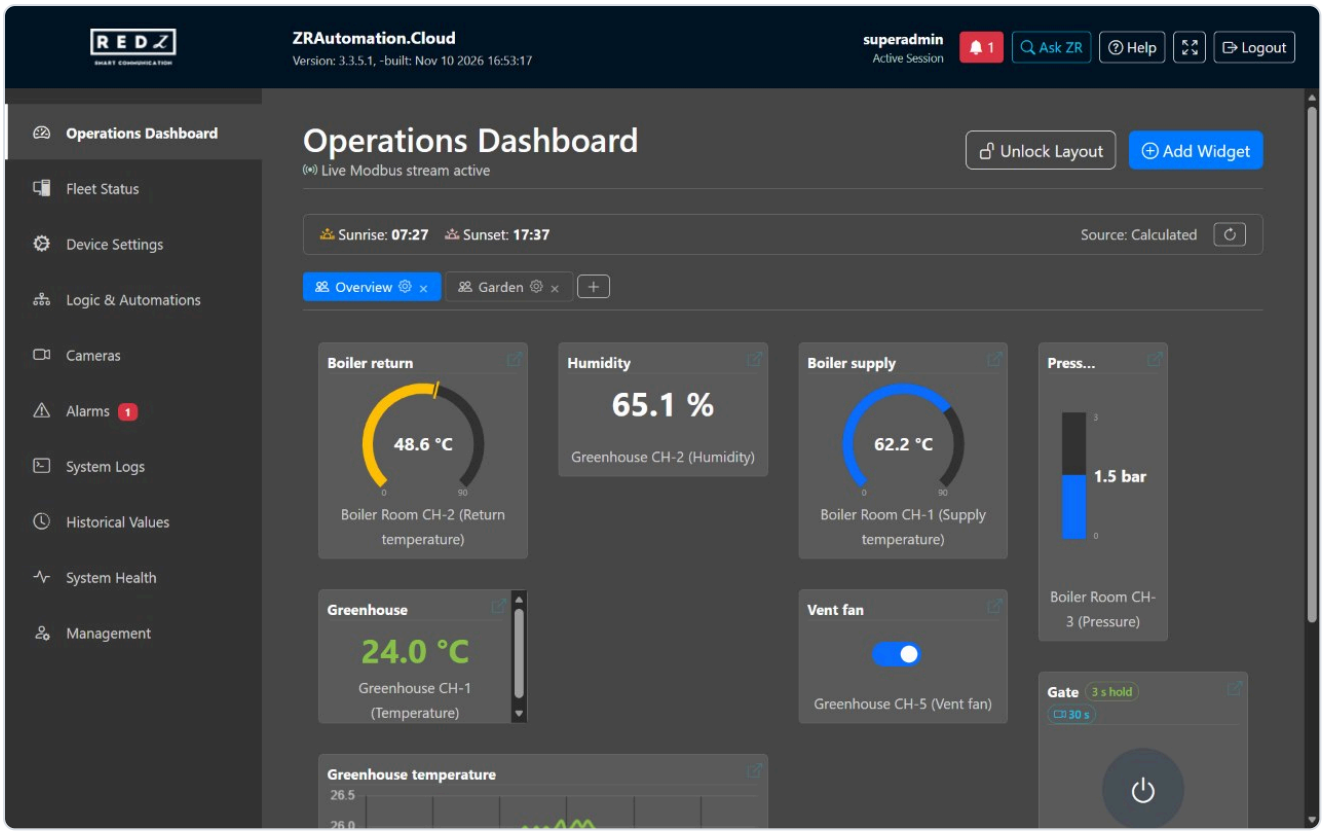


Figure 6.3 The New Widget window filled in for a gauge with a range of 0 to 90.



Video 6.1 Adding a widget: the New Widget window is filled for a gauge, Add Widget places it on the page. The video is in the online manual.

Arranging the page

Select **Unlock Layout** to move and resize widgets, delete them, or move them to another page. Select **Lock Layout** to save the arrangement.

When the dashboard is too narrow for its columns, for example on a phone or a tablet held upright, the widgets are shown in one column and the page cannot be arranged.

What your role allows

- A widget of a device your role does not cover is not shown. It keeps its place on the page for the users who can see it.
- A shared page whose widgets all belong to such devices is not shown at all.
- Without the **Edit (Update)** action, switches and buttons are marked view only: you can watch the channel but not change it.
- Without the **Cameras** permission, a switch or button linked to a camera still works, but no camera picture opens.
- On a shared page you cannot change, **Unlock Layout** and **Add Widget** are not shown.

7 Cameras

Everyone

The site shows the cameras of its video recorder. The pictures come through the site, so a browser or a phone never connects to the recorder itself. Seeing cameras needs the **Cameras** permission.

The Cameras page

The **Cameras** page shows the cameras grouped by zone, each picture renewed every 4 seconds. Cameras without a zone are listed last, under Other. A camera that gives no picture shows **No picture**.

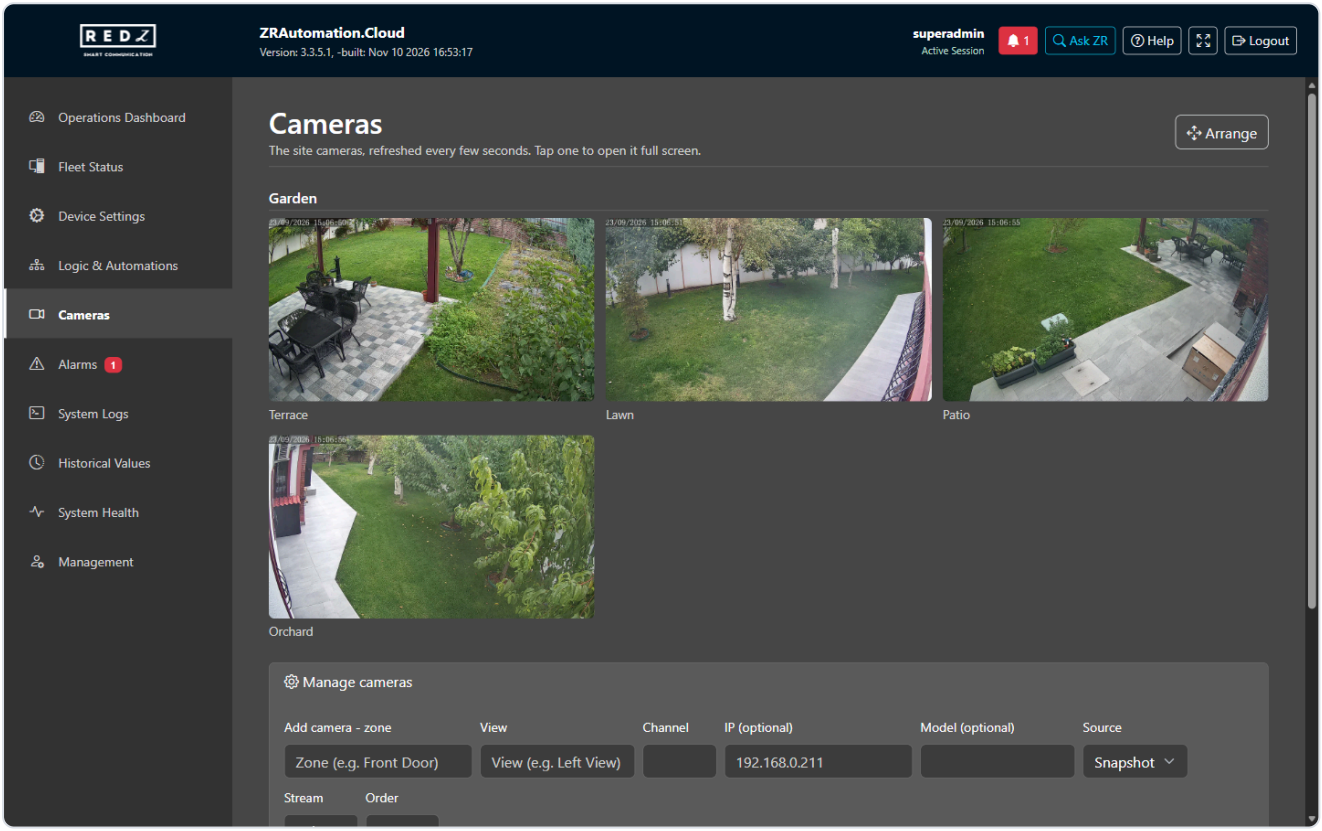


Figure 7.1 The Cameras page: the garden cameras in their zone.

Select a camera to open it full screen. Full screen shows the camera's main stream as video. The site sends up to 2 videos at a time, and a camera shown at two sizes on different screens counts twice; past that, or when a camera cannot send video, the picture is shown as a quick series of still pictures from the smaller stream instead. A video, and then a quick series, each run for 10 minutes; a full screen left open longer goes on with a still picture every 4 seconds.

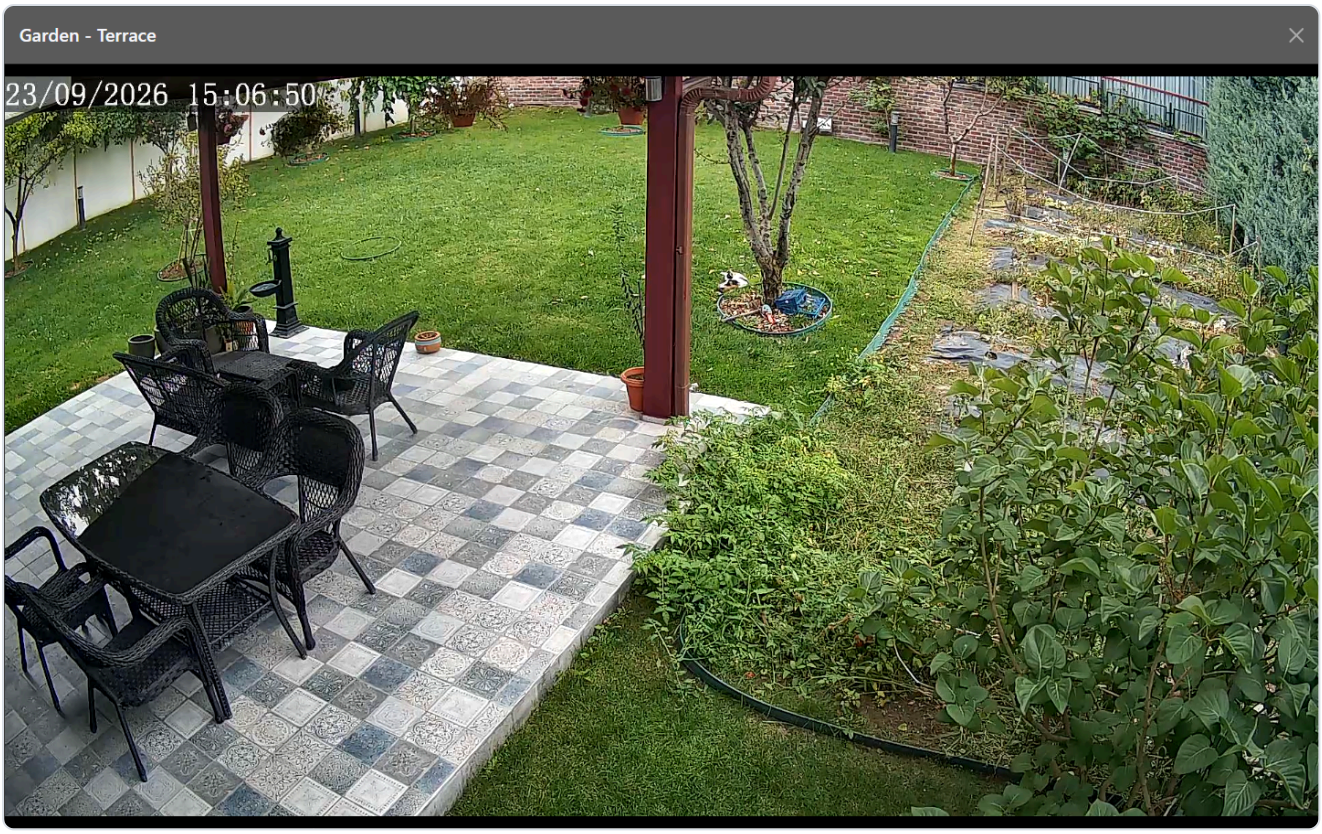


Figure 7.2 A camera full screen, playing its main stream as video.

A camera widget on a dashboard opens the same full screen view.

Arranging the cameras

With the **Edit (Update)** action, **Arrange** puts arrows on each camera to move it within its zone, and on each named zone to move it up or down; Other stays last. Each move is saved at once. Select **Done** to leave.

A camera when a control is used

A switch or button widget can open cameras when it is used, for example the gate camera when the gate button is pressed. Setting this needs the **Cameras** permission.

1. On the dashboard, select **Unlock Layout**.
2. Select the camera symbol on the switch or button.
3. In **Camera on use**, choose up to 4 cameras and the number of **Seconds** they stay open, from 5 to 600; 30 unless changed. A number outside that range is not saved, and the window says so.
4. Select **Save**, then **Lock Layout**. **Remove** takes the cameras off the widget.

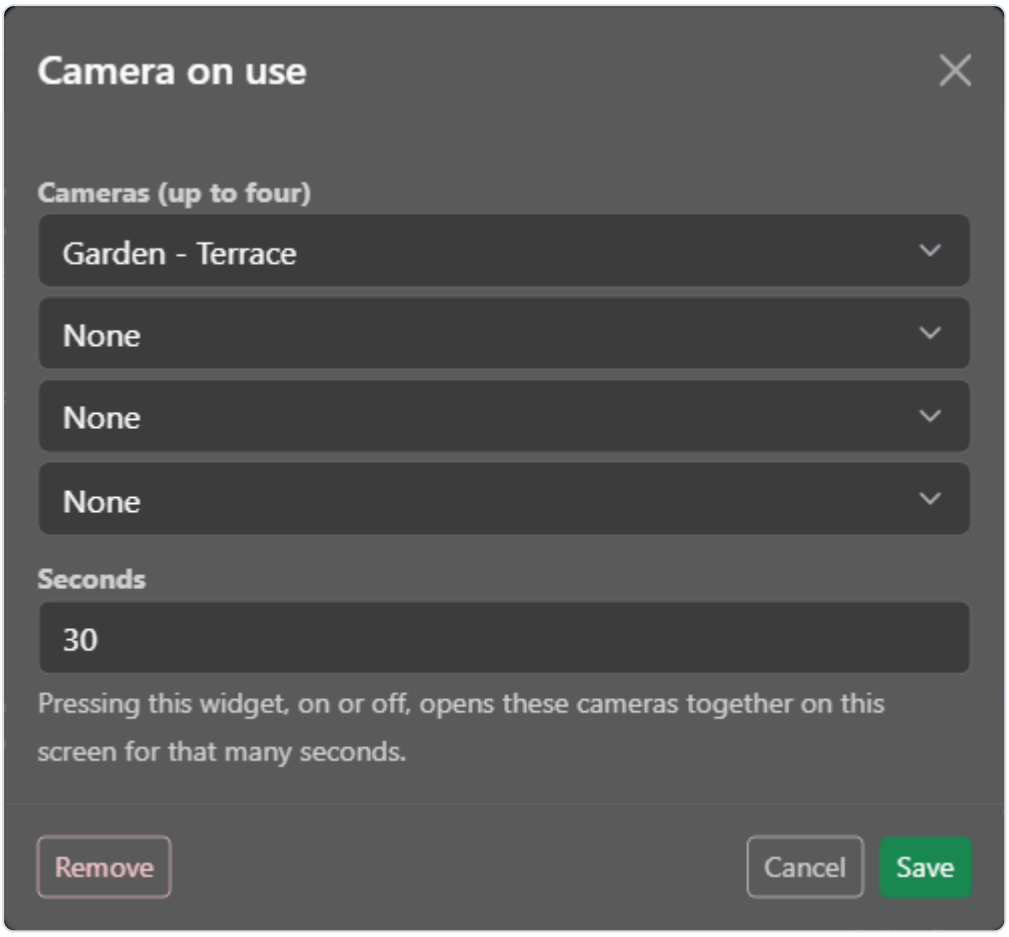


Figure 7.3 Camera on use for the Gate button: one camera, open for 30 seconds.

Using the widget, on or off, then opens those cameras together on the same screen, with the seconds counting down; the window closes by itself. The widget shows a camera symbol and the seconds. Without the Cameras permission the widget still works, but no camera opens.

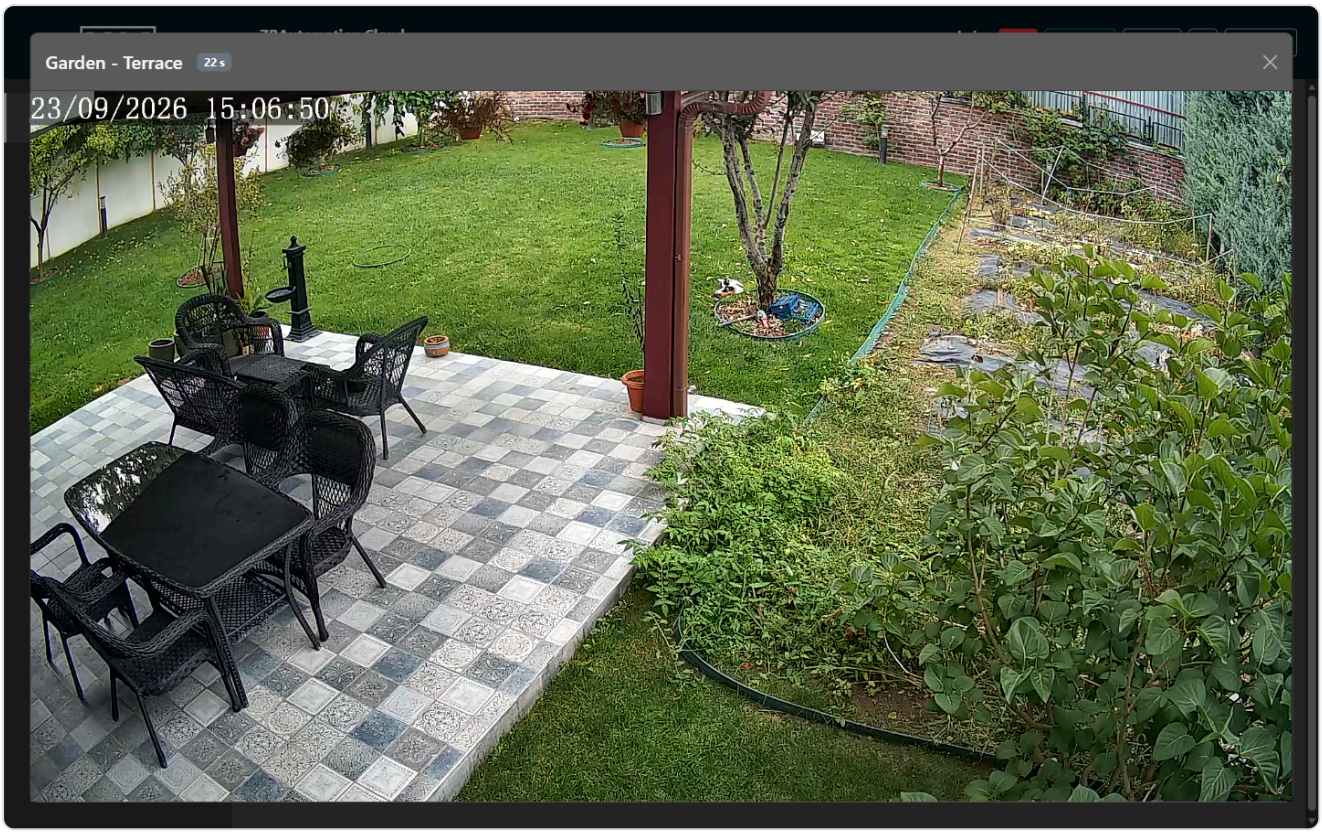
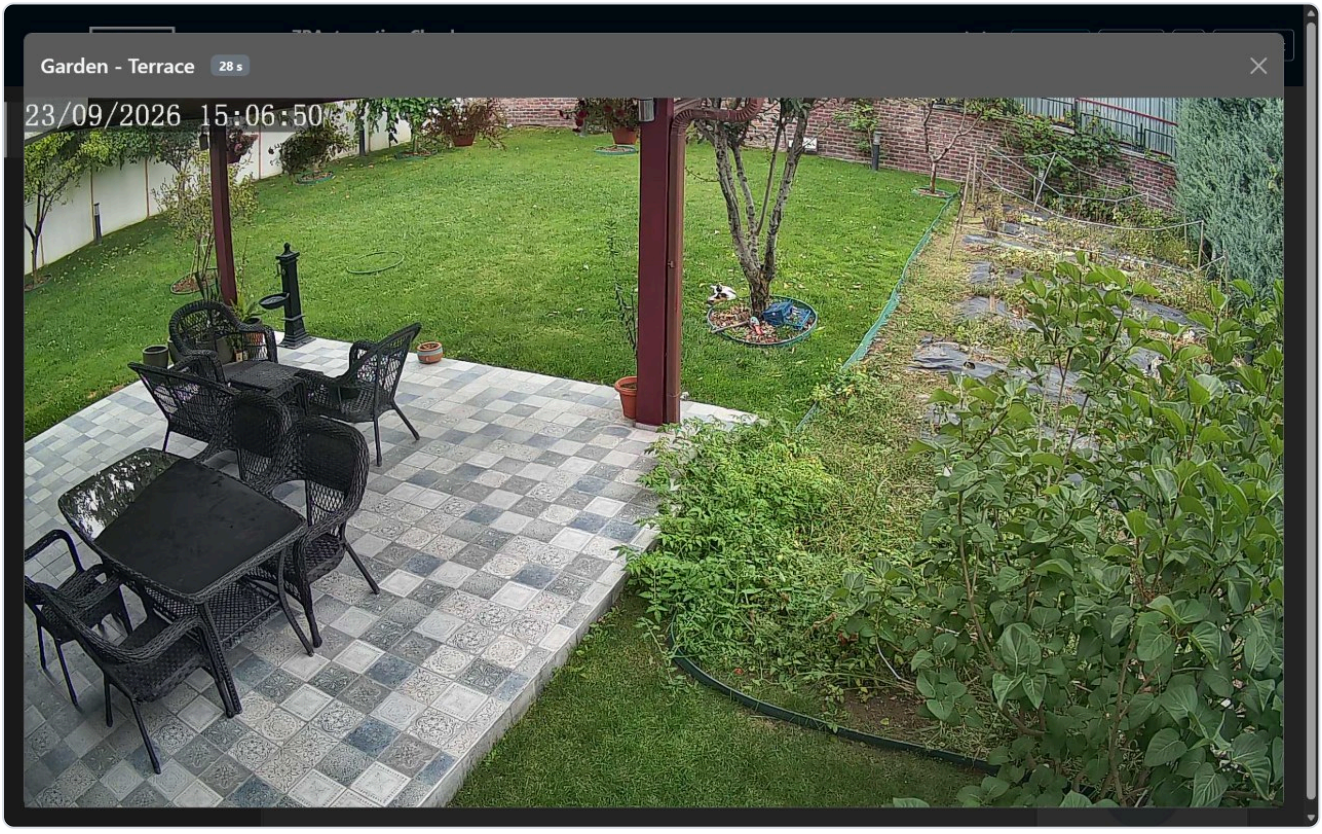


Figure 7.4 The window a control opens when it is used, counting down its seconds.



Video 7.1 Using the Gate button opens its camera in a window for 30 seconds; the seconds count down in its title. The video is in the online manual.

Adding cameras

Cameras are added under **Manage cameras** at the bottom of the Cameras page. Besides the Cameras permission, adding a camera needs the **Add (Create)** action, changing one **Edit (Update)** and removing one **Delete**.

1. Under **Add camera - zone**, enter the zone, such as the area the camera watches, and under **View** the camera's own name. Screens show the two together.
2. Enter the recorder's **Channel** for this camera, 1 to 64. Each channel can be used by one camera only.
3. **IP (optional)** and **Model (optional)** are notes for you; the site does not use them.
4. Under **Source**, choose **Snapshot** if the recorder gives a still picture for the channel, or **RTSP** to take the picture from the channel's video stream. Use RTSP for a camera that shows No picture with Snapshot.
5. Under **Stream**, choose which stream the page uses for its picture: **Sub** is smaller and faster, **Main** is sharper. Full screen video always uses the main stream.
6. **Order** sets the camera's place. A camera that is not **Active** stays in the list but is not shown.
7. Select **Save**.

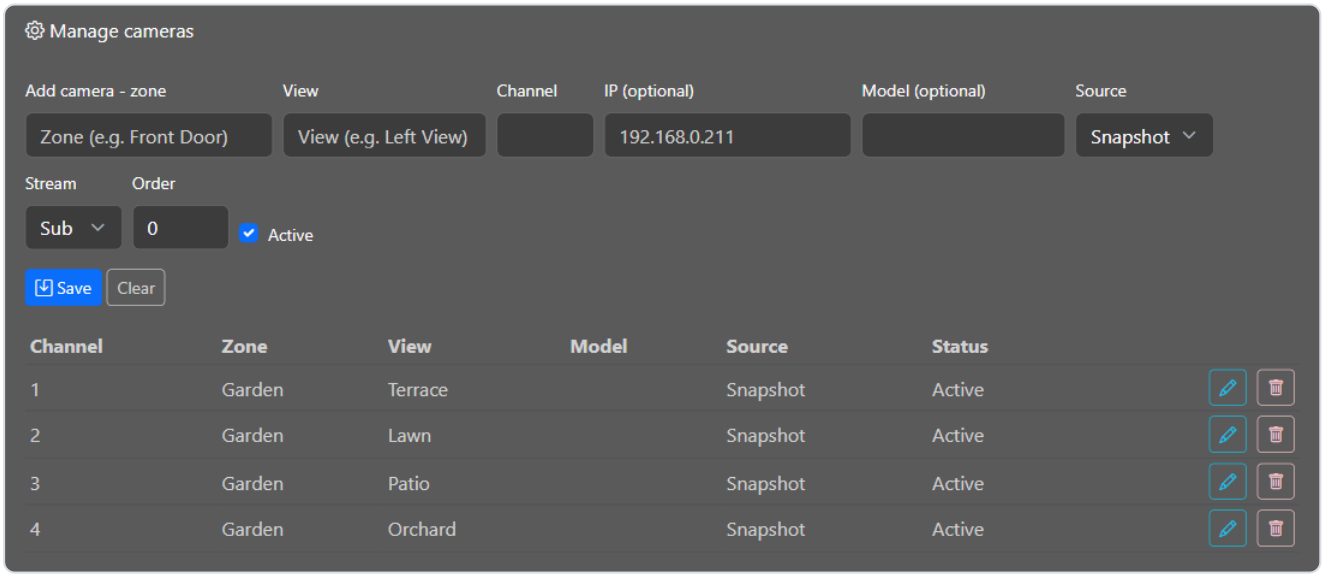


Figure 7.5 Manage cameras: the form for a camera and the cameras already set.

The recorder

The site's connection to the recorder is set on the **Management** page, **System Settings** tab, in **Camera Recorder**: the **Recorder address**, its **HTTP port** and **RTSP port**, and the recorder's **Account** and **Password**. Changing it needs the **Management** permission and the **Edit (Update)** action.

Leave the password blank to keep the stored one. The password is kept sealed with the site server's own key: after the site moves to another server, it has to be entered again. It

is never sent to a browser.

If the recorder refuses the password, the site stops asking it for pictures, so that the recorder does not lock its account, and every camera shows No picture. Pictures come back after the right password is saved.

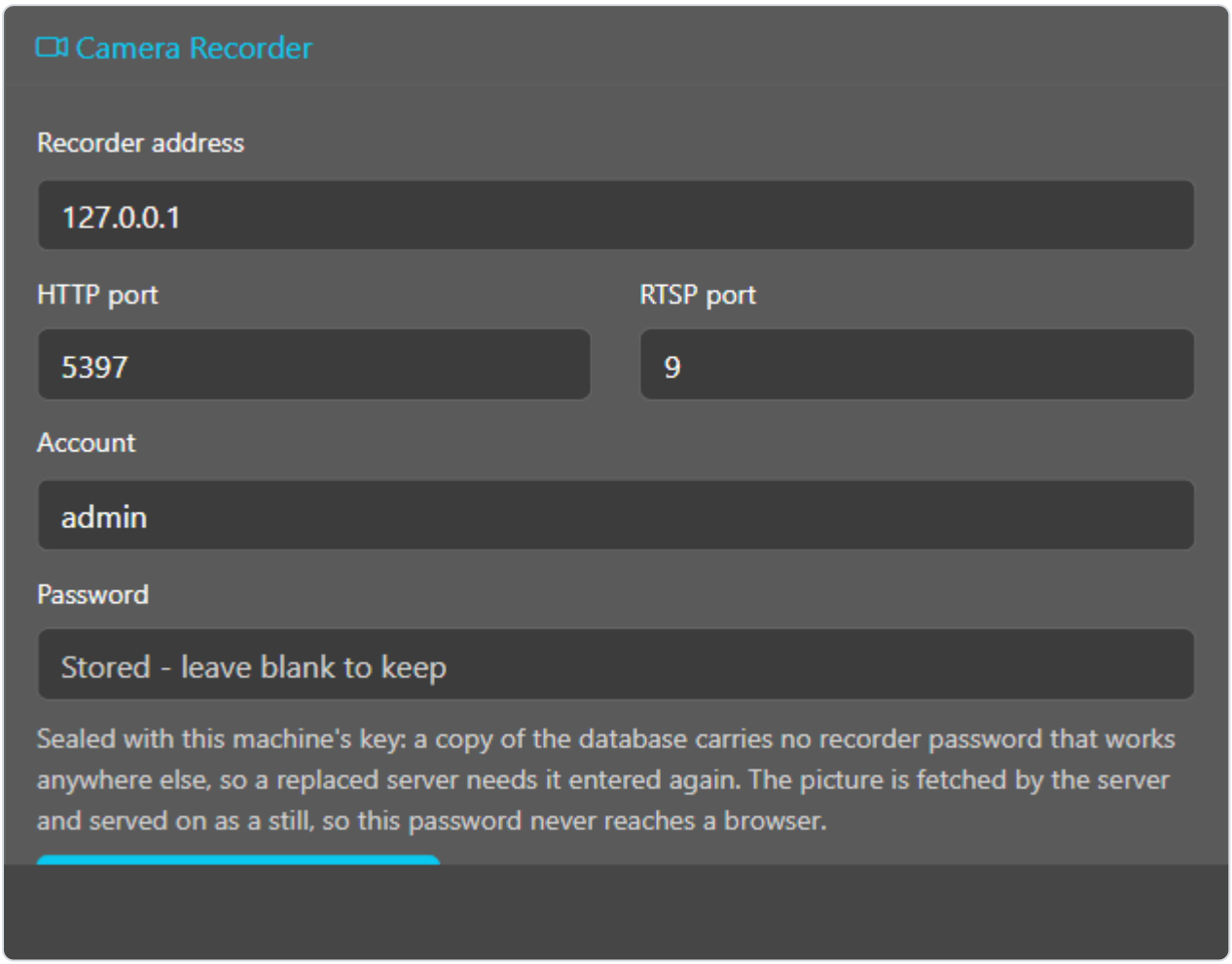


Figure 7.6 The Camera Recorder card on the System Settings tab.

8 Alarms

Everyone

The **Alarms** page lists what is in alarm now and what was. An alarm is raised when a value crosses a limit, when a digital channel is in a given state, or when a device stops answering.

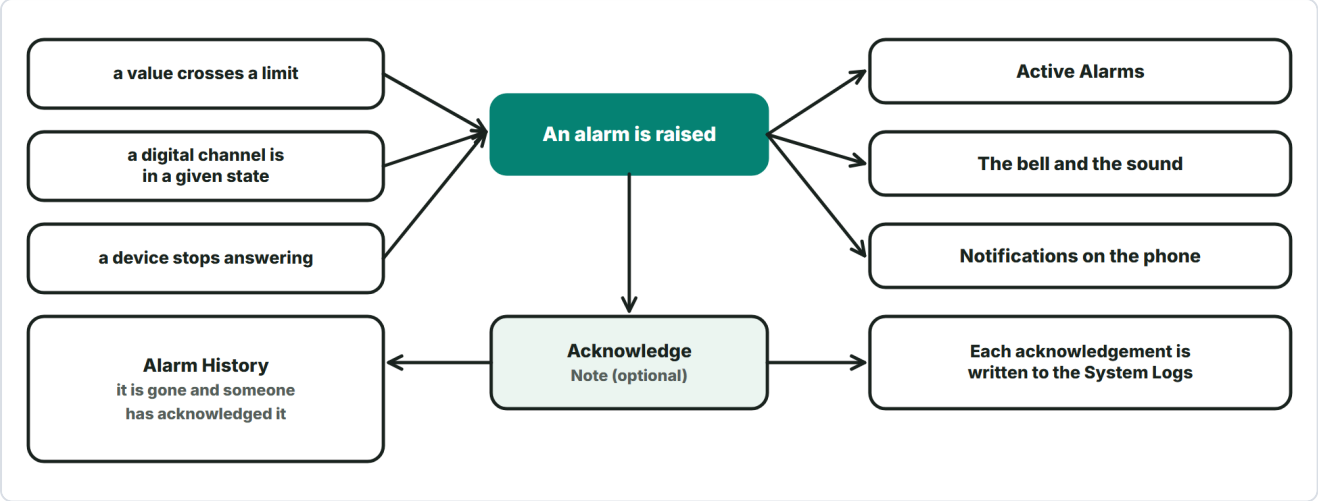


Figure 8.1 The life of an alarm: raised by a limit, a digital state or a device that stops answering; seen in Active Alarms, the bell and the sound and on the phone; acknowledged with an optional note; kept in Alarm History once it is gone and acknowledged.

You see the alarms of the devices your role covers. The page, the bell and the alarm sound need the **Alarms** permission.

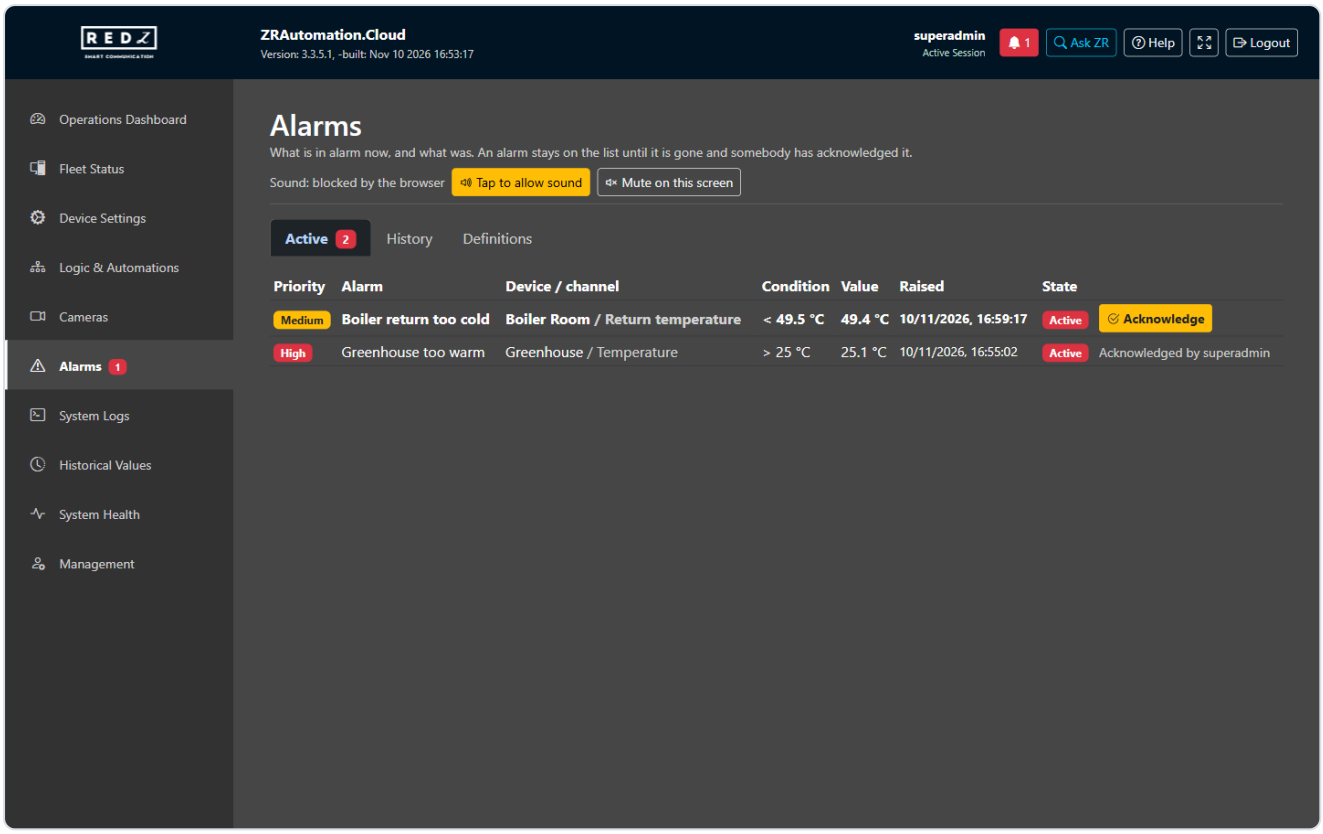


Figure 8.2 The Active tab. An alarm that is on and not yet acknowledged is shown in bold with its Acknowledge button.

Active alarms

The **Active** tab shows each alarm with its priority, its text, the device and channel, the condition, the value when it was raised and the time. An alarm stays on this list until it is gone and someone has acknowledged it, so an alarm that came and went while nobody was watching is not missed.

Alarms nobody has acknowledged come first, then by priority (High, Medium, Low), newest first. An alarm that is still on and not acknowledged is shown in bold. When an alarm is over, its state shows the time it went.

1. Select **Acknowledge** on the alarm's row.
2. In **Acknowledge alarm**, add a note if you wish under **Note (optional)**, such as what you checked. A note can be up to 200 characters.
3. Select **Acknowledge** in the window.

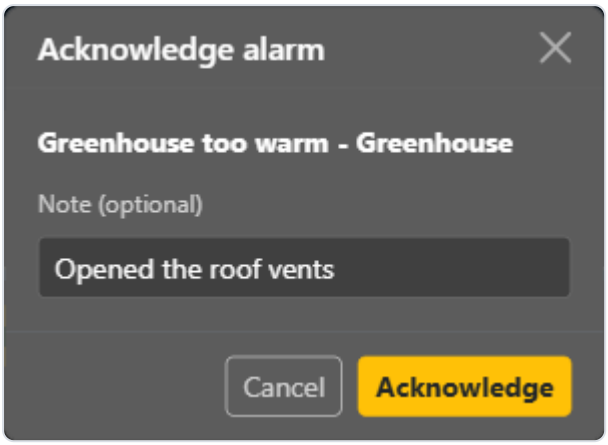
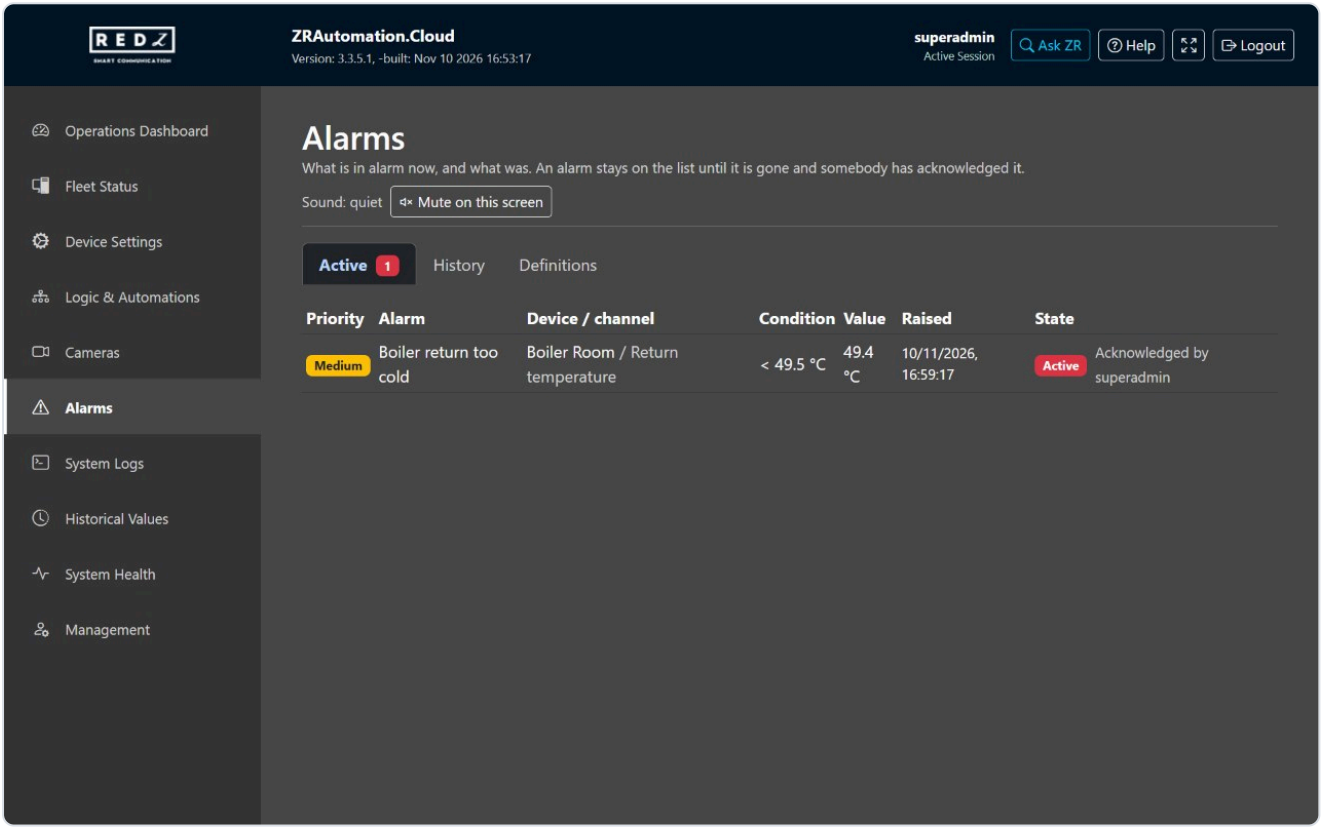


Figure 8.3 Acknowledging an alarm, with a note.



Video 8.1 Acknowledging an alarm with a note; it stays on the list as acknowledged until it is gone. The video is in the online manual.

The row then shows who acknowledged the alarm; an alarm that was already gone leaves the list and stays in the history. Each acknowledgement is written to the **System Logs** with its note. If two people acknowledge the same alarm, the first one counts.

The bell and the sound

While an alarm waits to be acknowledged, a bell with the number of such alarms is shown at the top of the screen, and the Alarms entry in the sidebar shows the same number. Selecting the bell opens the Alarms page.

The screen plays an alarm sound while an alarm is still on and nobody has acknowledged it. The sound stops when the last such alarm is acknowledged or gone.

Mute on this screen silences only the browser you are using, for example a wall tablet, and not the other screens. **Sound on this screen** turns it back on.

A browser may refuse to play sound until someone has touched the page. The page then says so and shows **Tap to allow sound**; selecting the bell does the same.

On a gauge or bar widget the channel's alarm limits are marked, and while one of them is in alarm the widget takes the colour of its priority.

Alarm history

The **History** tab lists the alarms raised in the window you choose, from **Last 24 hours** to **Last 90 days**, newest first, with when each one went and who acknowledged it, when and with what note.

Alarms that are gone and acknowledged are kept for the number of days set in **Alarms (days)** in System Settings, counted from when they were raised, 90 unless changed. An alarm nobody has acknowledged is kept however old it is.

Defining alarms

Alarms are defined on the **Definitions** tab. Besides the Alarms permission, adding an alarm needs the **Add (Create)** action, changing one needs **Edit (Update)** and deleting one needs **Delete**. The form for a new alarm is shown only to a role that may add alarms.

1. Choose the **Device** and the **Kind** of alarm.
2. For **Limit (a value)**, choose a register channel, the comparison under **When** and the **Limit** in the channel's units. **Hysteresis** is how far back past the limit the value has to come before the alarm counts as gone; with 0 it is gone as soon as the condition no longer holds.
3. For **State (on / off)**, choose a digital channel and the **State** that raises the alarm.
4. For **Device not answering** no channel is needed: the alarm is raised when the device has not answered for the seconds in **After (s)**, at least 10.
5. **Delay (s)** is how long the condition has to hold before the alarm is raised; 0 raises it at once.
6. Choose the **Priority** and write the **Alarm text** people will see. Without a text, the site writes one from the channel and the condition, or for a device that does not answer, the device's name and "is not answering".
7. Leave **Tell the phones** ticked to notify the mobile app, and **On** ticked for the alarm to be watched.
8. Select **Save alarm**.

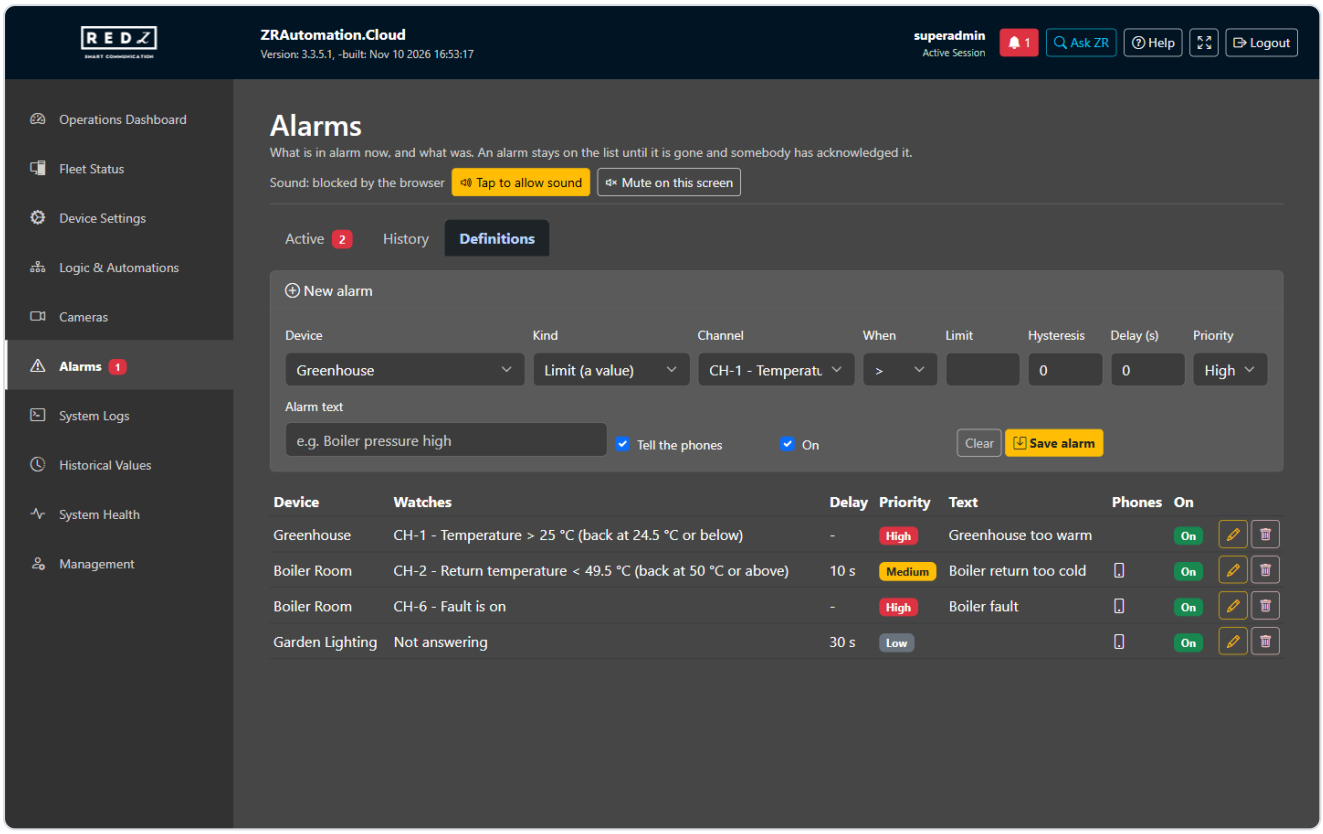


Figure 8.4 The Definitions tab: the form for a new alarm and the alarms already set.

The list shows what each alarm watches. The pencil changes an alarm and the bin deletes it. An alarm that is on when its definition is deleted or switched off is closed, and the history keeps it.

A limit or state alarm is judged on fresh readings only: while a device does not answer, its alarms neither rise nor clear, and a **Device not answering** alarm, if one is defined, tells you about that time. Switching a device off or removing it, or removing the channel, closes its alarms that are on.

Notifications on the phone

When an alarm with **Tell the phones** is raised, the mobile app is notified on the phones of the accounts whose role has the Alarms permission and covers the device. The notification names the device and shows the alarm text.

Notifications travel through remote access. While remote access is off or not connected, no notification is sent, and none is sent later; the app still lists the alarm among its notices the next time it connects.

9 Logic and automations

Administrators

The **Logic & Automations** page sets what the site does by itself: **Time Blocks** switch outputs at set times, **Scenarios** act when a channel reaches a value, and **Holidays** are the days time blocks can skip. The site checks them every 3 seconds, whether or not a screen is open, while its trial or licence runs (see Licence and support). The page needs the **Logic & Automations** permission.

You see the time blocks and scenarios whose devices your role covers. Adding one needs the **Add (Create)** action, changing one **Edit (Update)** and deleting one **Delete**, and your role has to cover every device it uses.

Time blocks

A time block writes one value to an output at its start time and another at its end time, on the days you choose. In between, the site does not hold the output: if someone switches it, it stays so until the block's next time.

The start and the end are written in their own minute. If that minute is missed, because the device did not answer or the site was not running, the site writes it as soon as the device answers, until the block's other time comes, and the System Logs say it was late. When both a start and an end were missed, only the later of the two is written.

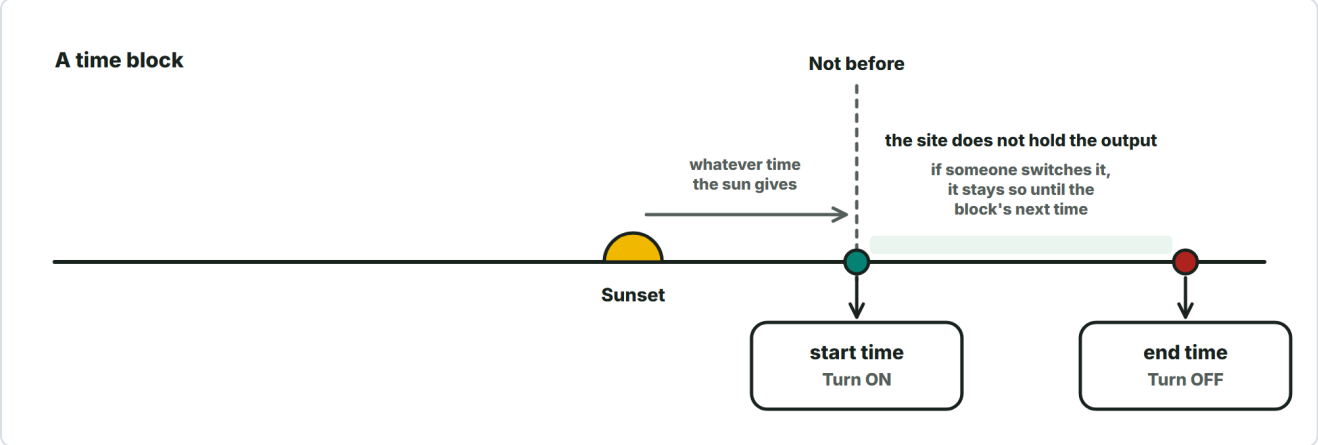


Figure 9.1 One day of a time block that starts at sunset with Not before: when the sun's time is earlier, the start comes at Not before; the end writes the other value, and in between the site does not hold the output.

1. Enter a **Routine Name** and choose the **Device** and the **Channel**. Only outputs are offered.
2. Tick the **Active Days**.
3. Leave **Do not run on Holidays** ticked for the block not to run on the days on the Holidays tab.
4. Under **Start Action**, choose **Fixed Time** and a time, or Sunrise or Sunset and the minutes after it (with a minus sign, the minutes before it). Then choose the value: **Turn ON** or **Turn OFF** for a digital output, a number for an analog one.

5. With Sunrise or Sunset you can also fill in **Not before**: the time then comes no earlier than this, whatever time the sun gives. Leave it empty for no limit.
6. Set the **End Action** the same way.
7. Select **Save Routine**.

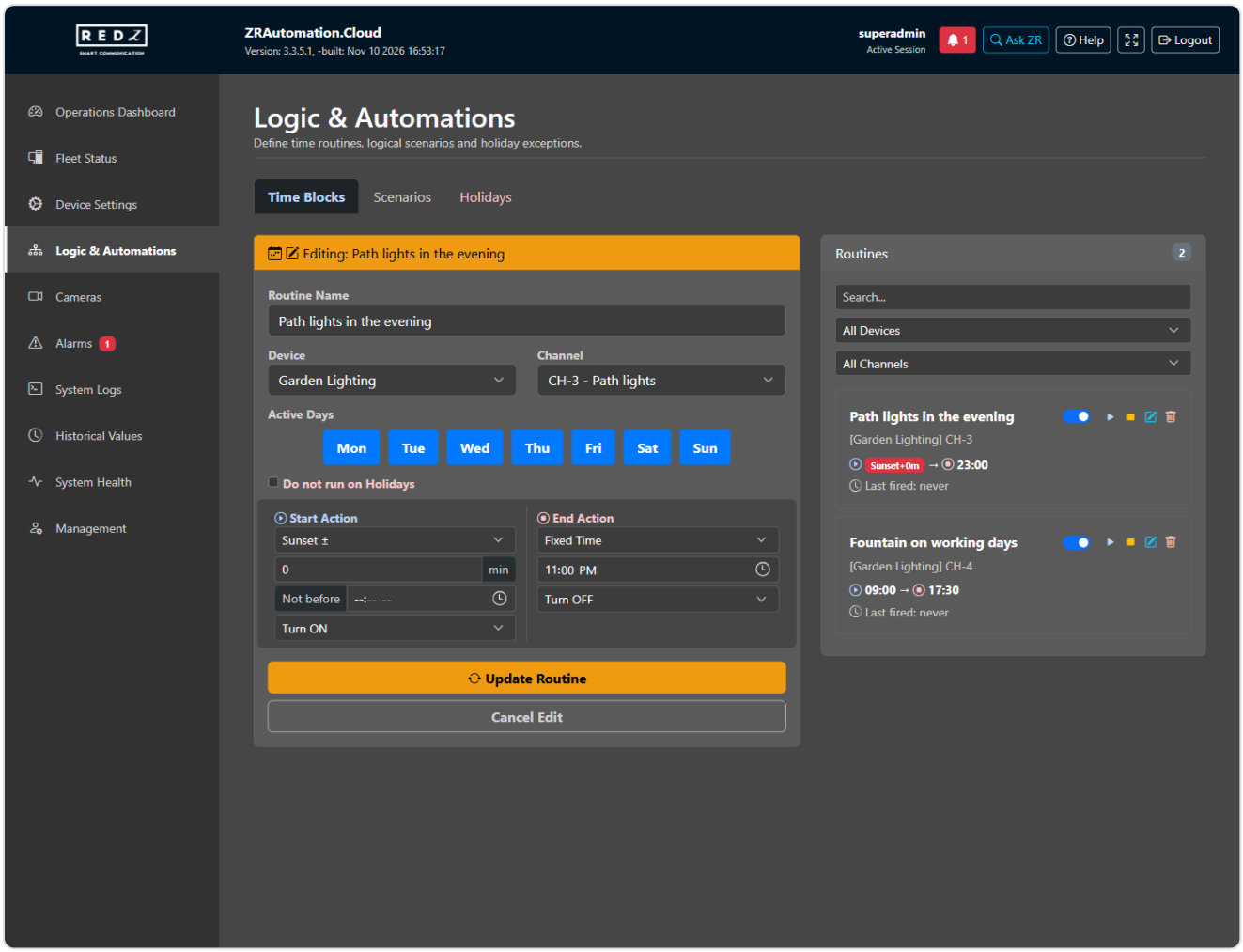


Figure 9.2 A time block opened for changing: the path lights come on at sunset and go off at 23:00 every day. The list shows the demo's two blocks.

The list shows each block's device and channel, its start and end, and when it last started. With the **Edit (Update)** action, the play and stop buttons write the block's start or end value now, after you confirm; the block's own times are not changed.

The switch beside each block turns it off and on without deleting it; nothing else of the block changes. A block that is off is marked **Disabled** and writes nothing. Switched back on, it carries on at its own next time: what fell while it was off is not written late. Changing the switch needs the **Edit (Update)** action.

Sunrise and sunset are the times the site uses for the day (see Location and sun times in System logs, health and settings). When it has none, a block that follows them does nothing.

Scenarios

A scenario watches one channel and writes a value to an output when a condition holds: if a channel is above, below or equal to a value, then set an output.

1. Enter a **Name**.
2. Under IF, choose the device, the channel, the comparison and the value; for a digital channel the comparison is equal and the value ON or OFF.
3. Under THEN, choose the device and the output, the **Set Value** and, if the output should wait, a **Delay (s)**.
4. To limit the scenario to some days and hours, turn on **Active Hours & Days Restriction** and set the days, the start and the end. The end can be after midnight, for example from sunset to sunrise.
5. To be told on the phone, turn on **Notify phones when this fires** and write the message, up to 160 characters.
6. Select **Save Scenario**, or **Update Scenario** when changing one.

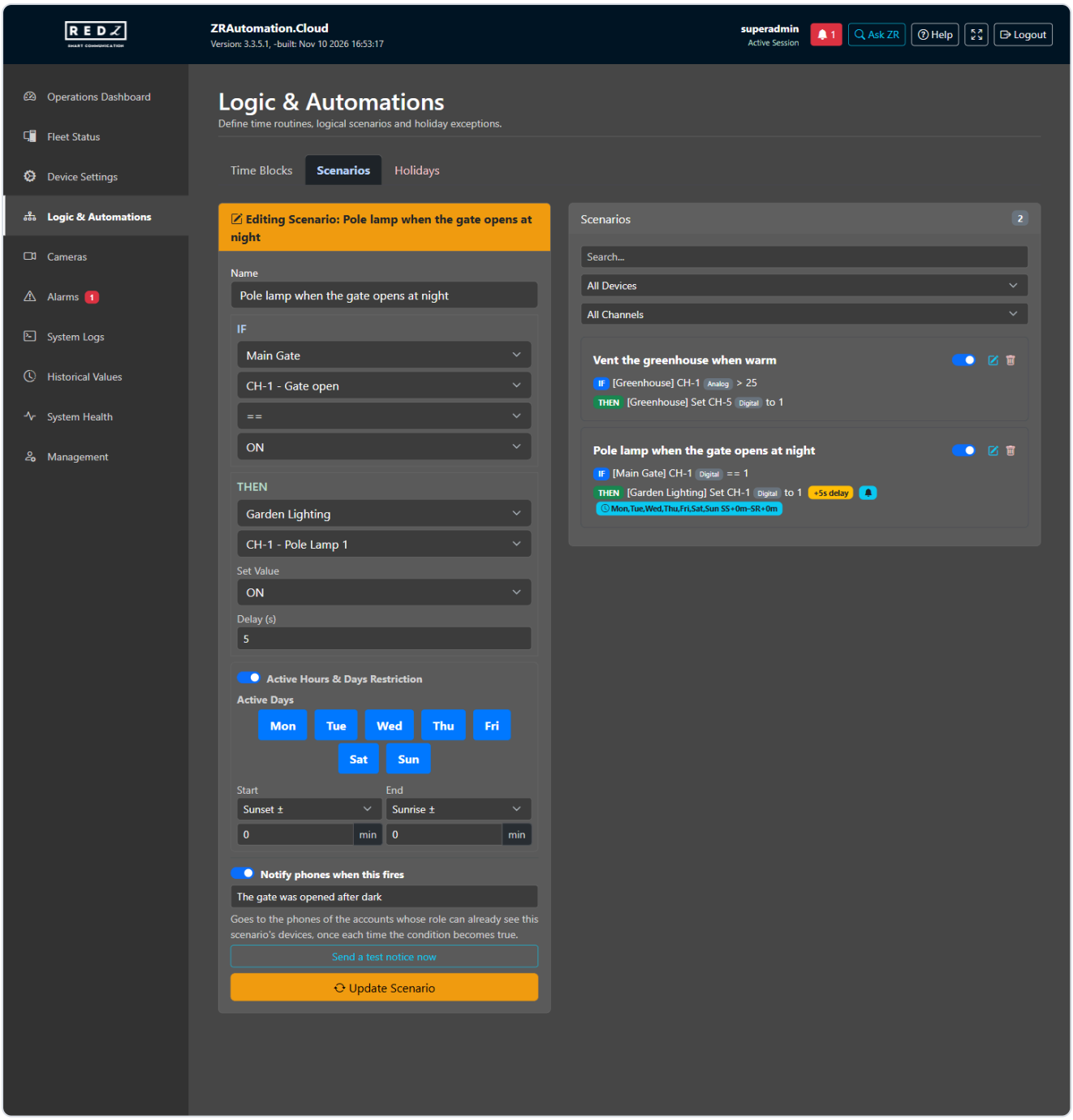


Figure 9.3 A scenario opened for changing: after dark, a pole lamp comes on 5 seconds after the gate opens, and the phones are told.

Without a delay, the site keeps the output at the value for as long as the condition holds: if someone changes the output, the site sets it back at its next check. When the condition ends, the output is left as it is. To switch it back, add a second scenario with the opposite condition.

With a delay, the value is written once, the given number of seconds after the condition became true, even if the condition has ended by then; if it becomes true again in the meantime, the count starts again. A delayed write that falls outside the scenario's days and hours is not made, and the System Logs say so.

A button press on the dashboard counts even when it is over before the site's next check.

Outside its days and hours a scenario does nothing. A button press that it ignores for that reason is written to the System Logs.

A channel that gives no value is not compared with anything; the scenario waits.

The list shows each scenario's IF and THEN, its delay, a bell when it notifies phones and its days and hours. Each scenario has an on and off switch, the same one the mobile app shows; a scenario switched off does nothing, keeps its settings and is marked Disabled. Switching it needs the **Edit (Update)** action.

Notifications from a scenario

A scenario that notifies phones does so once each time its condition becomes true within its days and hours. A restart of the site does not repeat it; a scenario added or switched on while its condition already holds notifies once. The notice goes to the phones of the accounts whose role covers the scenario's devices, with your message, or without one with the scenario's name.

Send a test notice now sends the notice of a saved scenario at once, so you can see that it arrives; it needs the **Edit (Update)** action. Like the alarm notifications, these travel through remote access.

Holidays

The **Holidays** tab lists the days on which time blocks with Do not run on Holidays do not run. Holidays do not affect scenarios.

1. Enter the name and the date.
2. Leave **Recurring** ticked for a day that comes back every year on the same date.
3. Select **Add**.

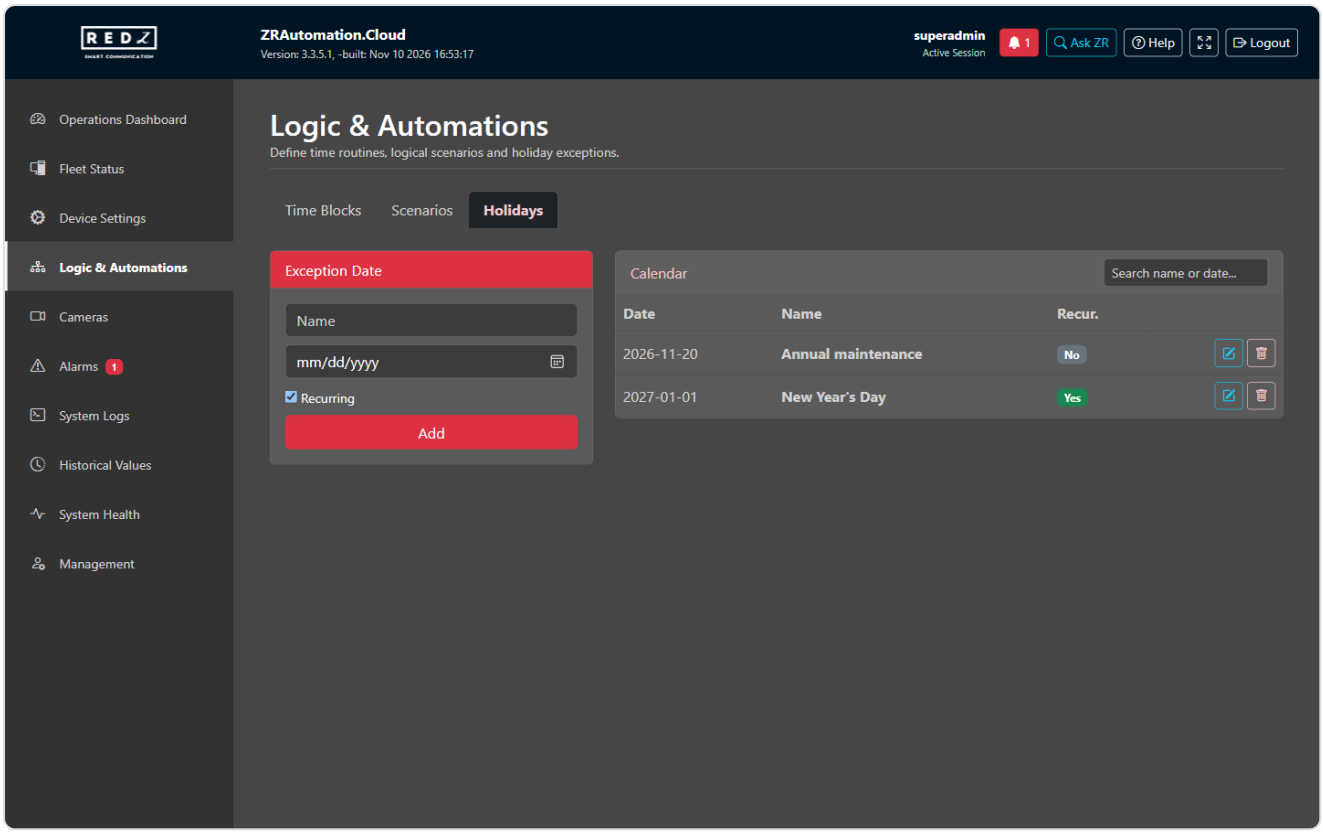


Figure 9.4 The holiday calendar: a day that comes back every year and a one-off day.

10 History, analysis and export

Everyone

The **Historical Values** page shows how channels changed over time, as a chart, a summary and a table, and saves the same analysis as an Excel workbook. It needs the **Historical Values** permission, and it offers the devices your role covers.

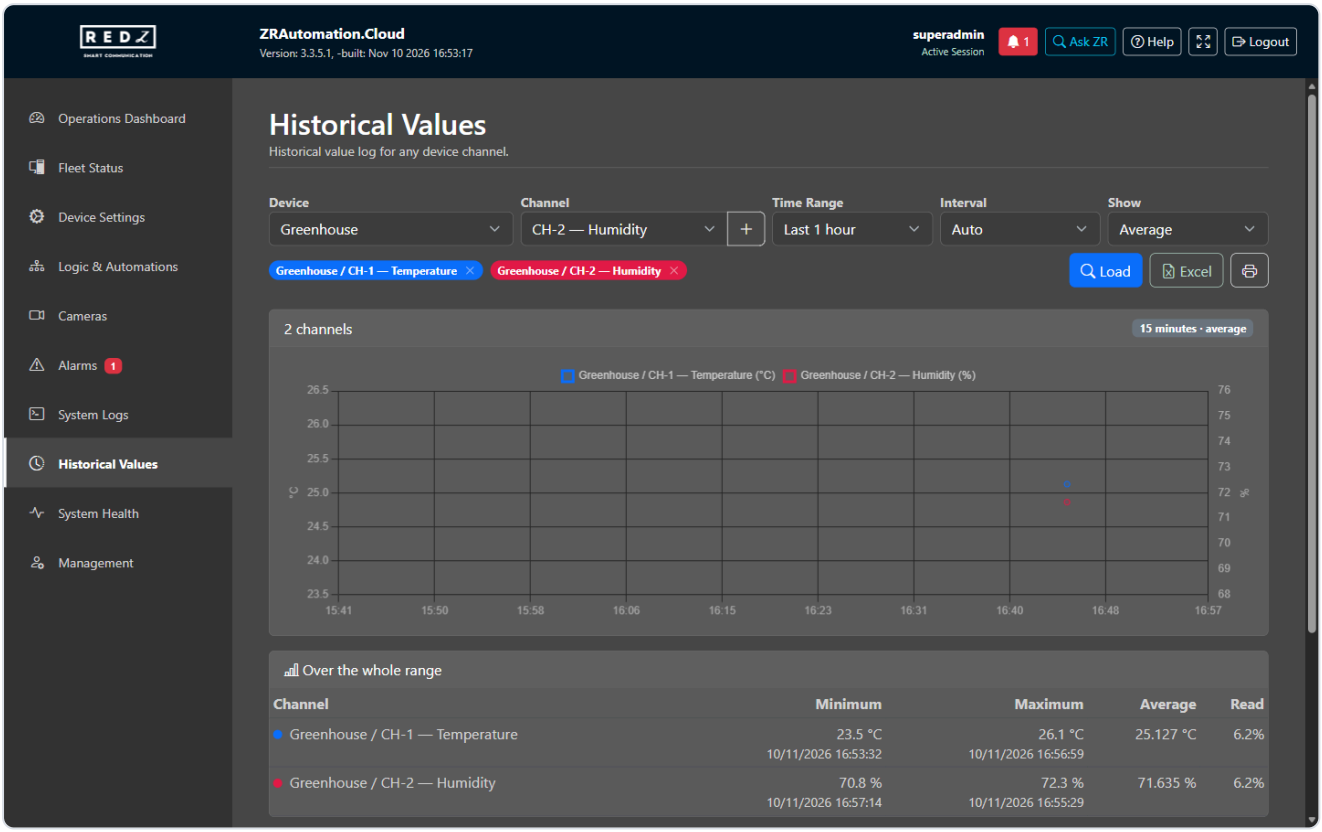


Figure 10.1 Two channels of the greenhouse over the last hour: temperature on the left scale, humidity on the right.

Choosing what to show

1. Choose a **Device** and a **Channel**. To compare channels, select + after each one; up to 8 channels, from any of your devices. Without +, the channel chosen is the one shown.
2. Choose the **Time Range**, from **Last 1 hour** to **Last 90 days**.
3. Choose the **Interval**. **Auto** uses 15 minutes up to 48 hours, 1 hour up to 7 days and 1 day beyond. **Raw** shows every recorded change instead of intervals.
4. Under **Show**, choose what each interval shows: its **Average**, **Minimum** or **Maximum**.
5. Select **Load**.

The channels added are listed under the controls, each in its colour on the chart; the x on one removes it.

Reading the chart

The site records a channel when its value changes, and a value holds until the next change. The averages are therefore taken over time: a busy ten minutes does not

outweigh ten quiet hours. Time in which a device was not being read is left out, and the chart shows a gap there.

Channels with different units get their own scale, the first on the left and the second on the right. One chart takes at most 2 units.

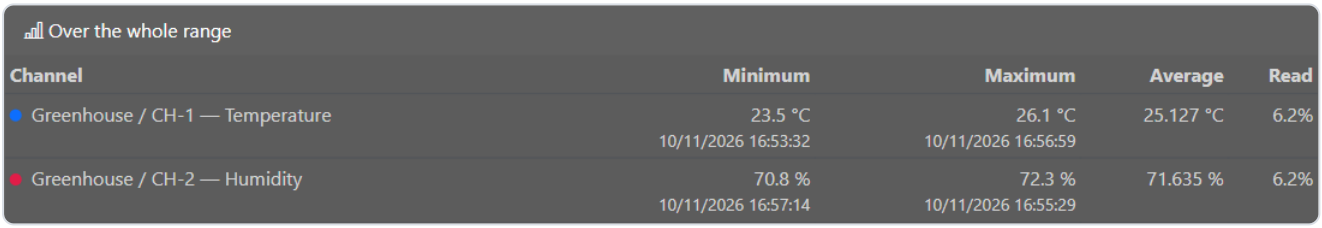
A change smaller than the channel's deadband is not recorded, so the lowest and highest values can differ from the real ones by up to that amount.

Raw shows at most 10,000 changes of a channel; for more, choose an interval or a shorter range.

The summary and the table

Over the whole range, the summary gives each channel's **Minimum** and **Maximum** with the time they were reached, its **Average**, and **Read**: how much of the range the device was being read.

The table below lists every interval, or for Raw every recorded change, newest first. The page shows the newest 2,000 rows; the Excel workbook has them all.


Over the whole range

Channel	Minimum	Maximum	Average	Read
Greenhouse / CH-1 — Temperature	23.5 °C 10/11/2026 16:53:32	26.1 °C 10/11/2026 16:56:59	25.127 °C	6.2%
Greenhouse / CH-2 — Humidity	70.8 % 10/11/2026 16:57:14	72.3 % 10/11/2026 16:55:29	71.635 %	6.2%

Figure 10.2 Over the whole range: each channel's lowest and highest value with its time, its average, and how much of the range it was read.

Consumption of a counter

When every chosen channel is a counter, such as an energy meter, **Show** also offers **Consumption**: how much the counter counted in each interval, drawn as bars. An interval in which the counter went back, or whose start or end was not read, has no consumption. The summary adds a total of the intervals that have one and says how many they are.

A channel is a counter when Counter is ticked for it in the channel table (see Devices and channels).

Excel and printing

Excel saves the analysis of the current choices as a workbook: the channels side by side, one row per interval, or for Raw one per recorded change, with the lowest, highest and average above the table.

The printer button prints the chart and the tables, or saves them as PDF from the browser's print window.

11 Users, roles and permissions

Administrators

Accounts and roles are managed on the **Management** page, which needs the **Management** permission. Each account has one role; the role decides which pages, actions and devices the account has. What each permission allows is listed in Appendix A.

Accounts

The **Users** tab lists the accounts with their role and status. Their e-mail addresses are shown only to a role with the **Management** permission and the **Edit (Update)** action.

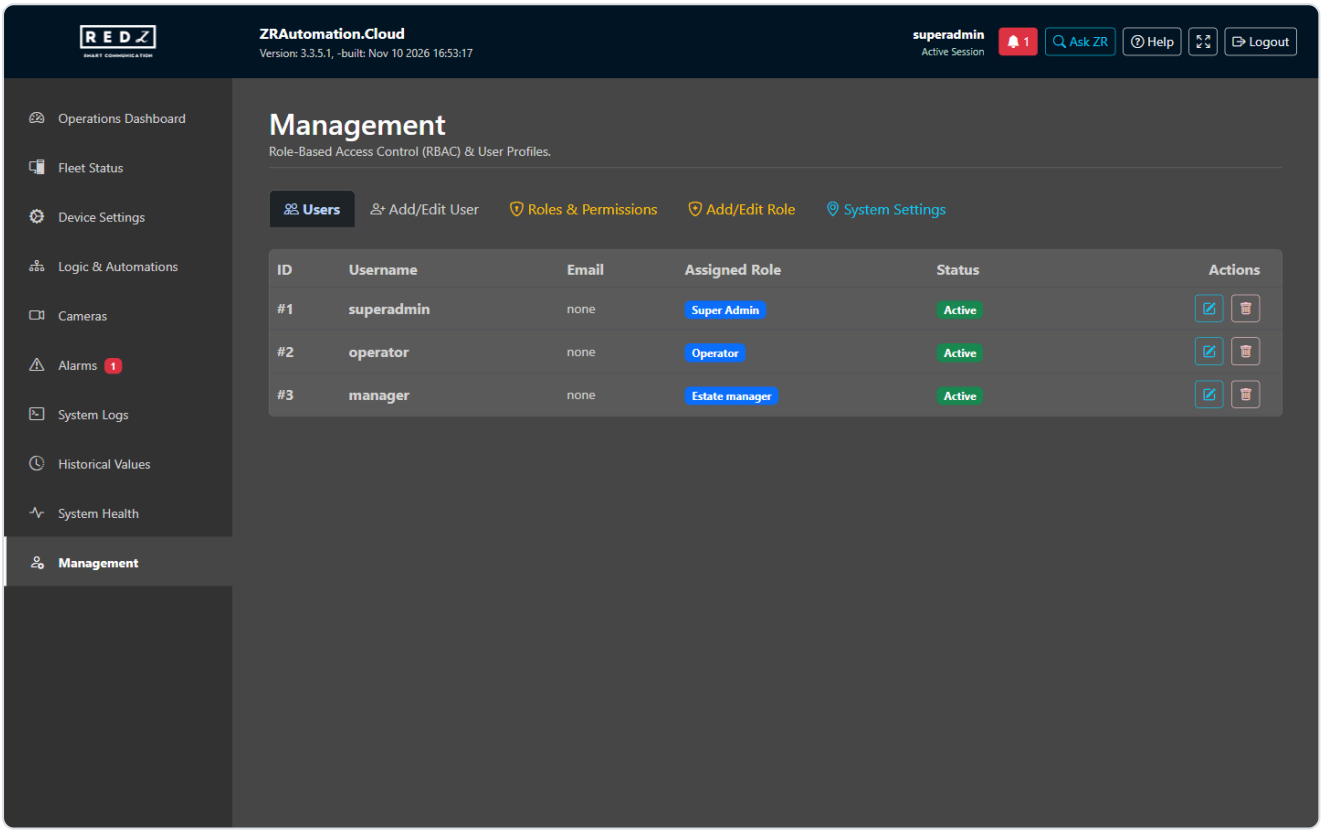


Figure 11.1 The Users tab: each account with its role and status.

1. Open the **Add/Edit User** tab, or the pencil of an account in the list to change it.
2. Enter the **Username** and a **Password** of at least 10 characters. When changing an account, leave the password blank to keep it.
3. **Email** is optional. It is where sign-in codes are sent when they are required for sign-ins from outside the local network; without it, the account cannot sign in from outside then.
4. Choose the role under **Assign Role**. Turn off **Account is Active** to stop the account signing in without deleting it.
5. Select **Save User**, or **Update User** when changing an account.

Adding an account needs the **Add (Create)** action, changing one **Edit (Update)** and deleting one **Delete**.

A new password or a disabled account takes effect at once: that account is signed out everywhere, and its remembered phones are asked for a sign-in code again.

Deleting an account also deletes its personal dashboard pages.

Roles

The **Roles & Permissions** tab lists the roles with the number of their pages and devices and the names of their actions. A role is set on the **Add/Edit Role** tab.

1. Enter the **Role Name**.
2. Under **2. Menu Access Permissions**, tick the pages the role may open.
3. Under **3. Action Permissions**, tick what the role may change. A role without actions cannot add, change or delete devices, rules, settings or accounts, and without **Edit (Update)** it cannot switch outputs; it can still acknowledge alarms and arrange its own dashboard pages.
4. Under **4. Device Permissions**, tick the devices the role covers. **Select All** turns on the Full access switch, which covers every device, including devices added later, and every page and action.
5. Select **Save Role**, or **Update Role** when changing a role.

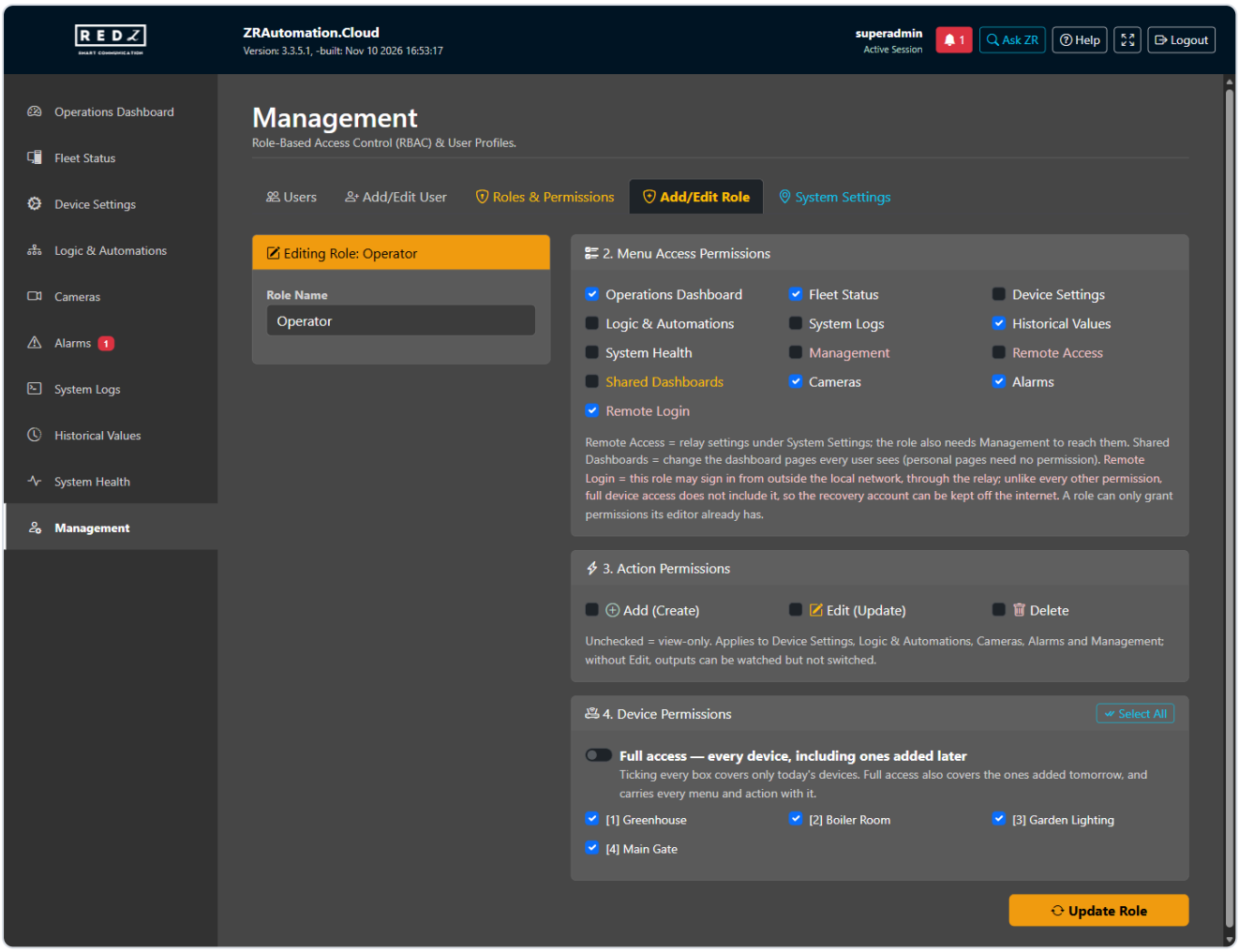


Figure 11.2 The demo's Operator role opened on the Add/Edit Role tab: its pages, no actions, and its devices.

Remote Login is never included in full access: it has to be ticked for every role that may sign in from outside the local network.

What an administrator can change

- Nobody can give a role a permission their own role does not have. A role with full access can give every permission, Remote Login included.
- Nobody can change a role, or an account of a role, that has permissions their own role does not have.
- Nobody can change their own role, or disable or delete their own account.
- A role that still has accounts cannot be deleted: move the accounts to another role first.
- A changed role applies at once to every account that has it.

12 Remote access and the mobile app

Everyone, with administrator parts

Remote access lets the mobile app reach the site from outside its local network, through REDZ's relay. The site connects out to the relay, so no port has to be opened on the site's router. On the local network the web screen works as before.

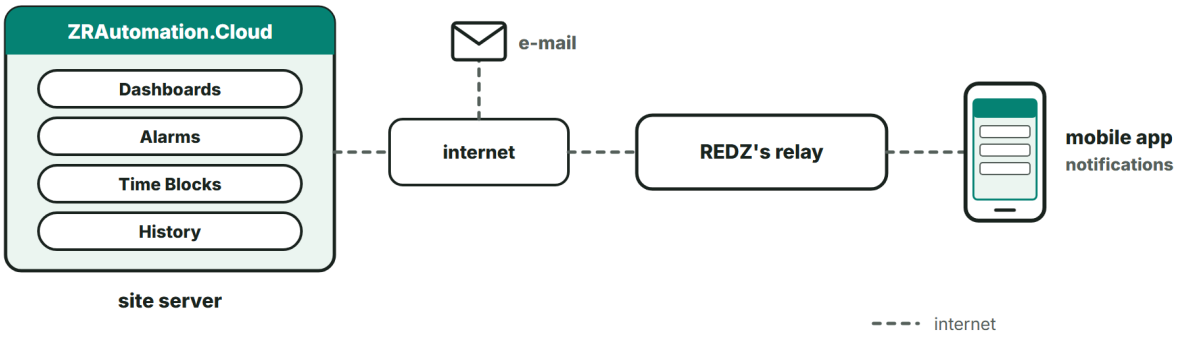


Figure 12.1 From outside: the mobile app reaches the site through REDZ's relay over the internet; notifications and e-mail come from the site.

Turning remote access on

Remote access is set in **Remote Access** on the **System Settings** tab of the **Management** page. The card is shown to a role with access to all devices, or to a role with both the **Management** and the **Remote Access** permissions.

1. Ask REDZ for the relay address, the site name and the site key of your site.
2. Turn on **Enable remote access** and enter the **Relay URL**, the **Site Slug** and the **Site Key**.
3. Select **Save Remote Access**. The site applies the settings within 15 seconds.

The badge on the card shows the connection: Connected, with the time since when, or Connecting, Reconnecting, Disconnected, Incomplete (switched on but the settings are not complete) or Disabled. While it is not connected and not disabled, the reason is shown under the fields when the site has one.

The site key is never shown again once saved. Leave the field blank to keep it.

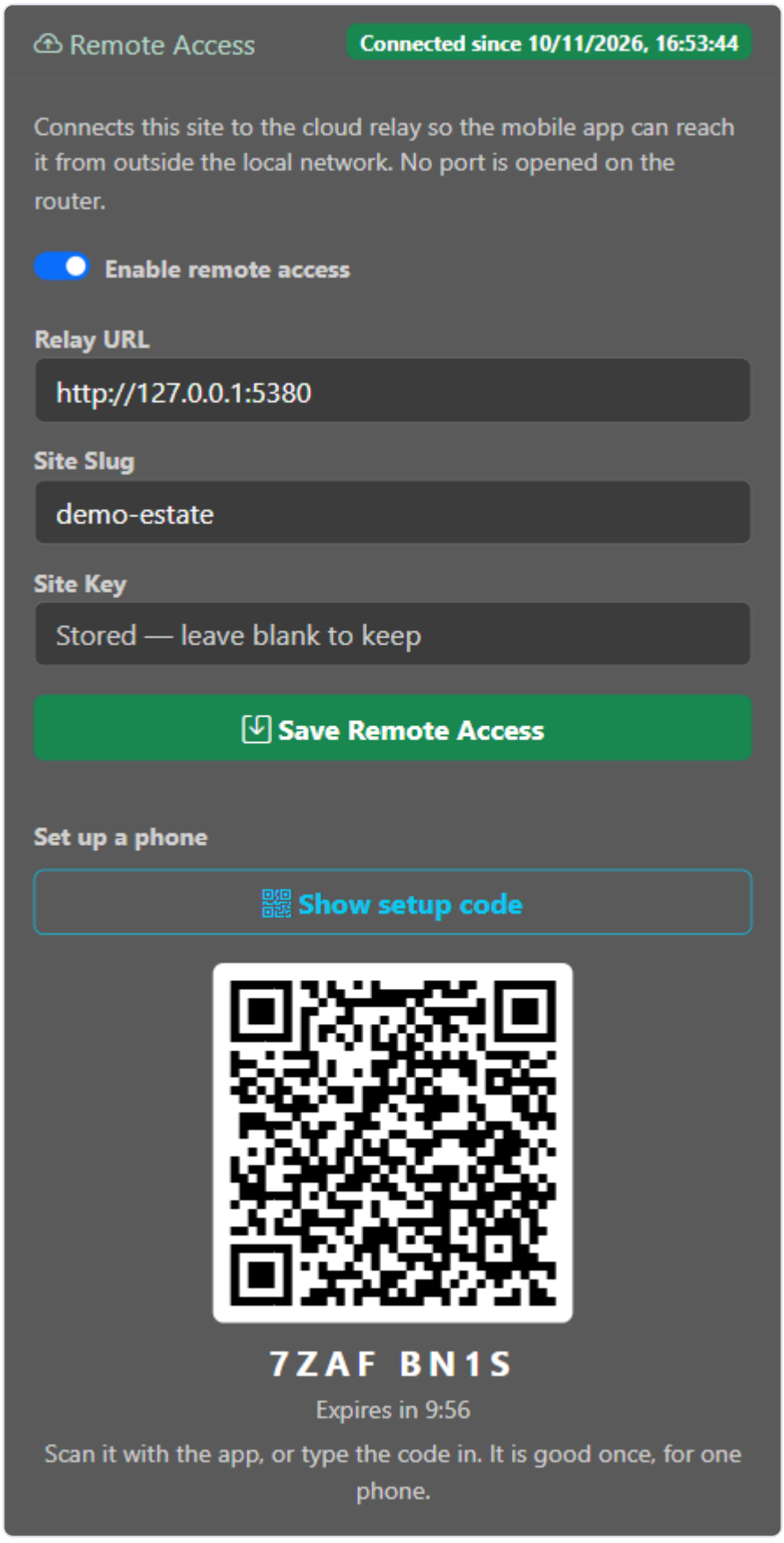


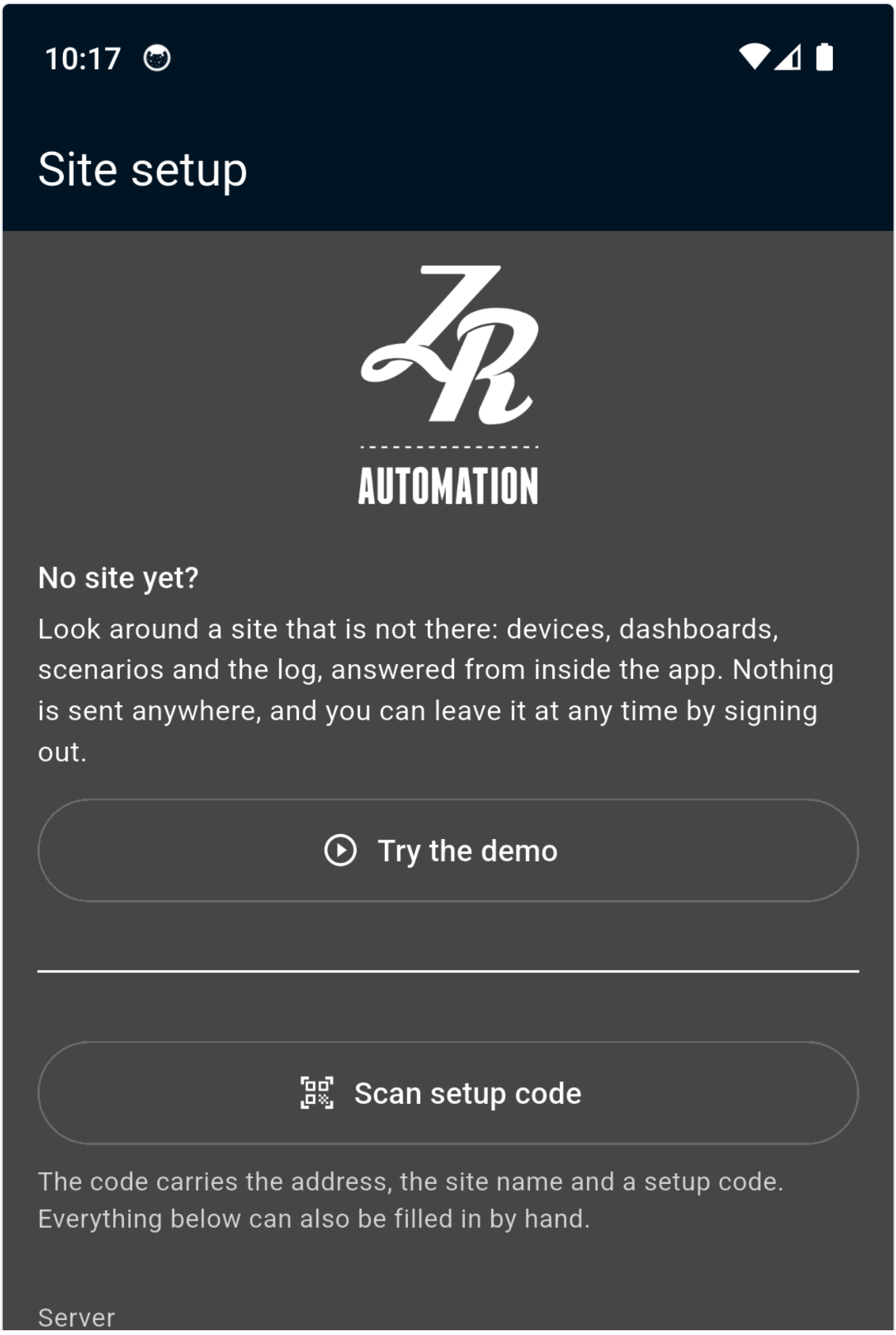
Figure 12.2 Remote access connected, with a setup code for a phone: the QR code, the same code to type, and the time it is good for.

Setting up a phone

Show setup code on the same card shows a QR code and the same code as 8 characters. A code is good for 10 minutes and for one phone, and disappears from the screen when it expires. The site key itself goes only to the relay and never to a browser or a phone: each phone receives a key of its own.

1. Install the ZRAutomation app from Google Play and open it.
2. On **Site setup**, select **Scan setup code** and point the camera at the QR code. The app fills in the site and exchanges the code at once.
3. Check the site name and select **Save**.

Without a camera, choose the relay under **Server** (or **Other address...**), enter the **Site name** and type the code into **Client key or setup code**, then select **Save**. **Remember this device** is ticked to begin with: when the site requires sign-in codes, the phone is asked for one at its first sign-in and then not again for the site's number of days (see Signing in).


10:17
Site setup
AUTOMATION
No site yet?
Look around a site that is not there: devices, dashboards, scenarios and the log, answered from inside the app. Nothing is sent anywhere, and you can leave it at any time by signing out.
Try the demo
Scan setup code
The code carries the address, the site name and a setup code. Everything below can also be filled in by hand.
Server

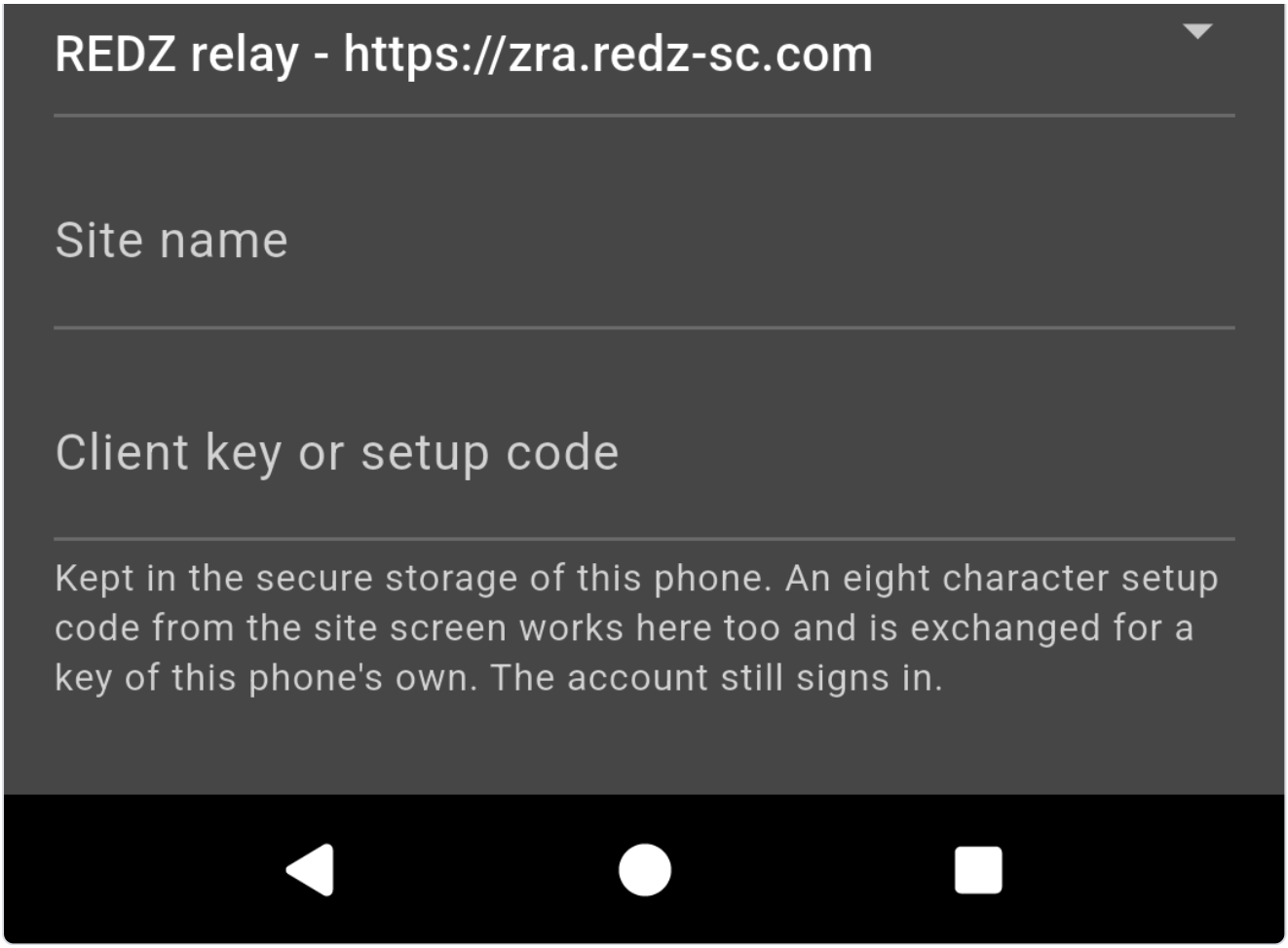


Figure 12.3 The app's first screen: the demo, a setup code to scan, or the site typed in.

Try the demo opens an example site inside the app, to look around before a site is set up. Nothing is sent anywhere; the screens are marked DEMO. Signing out leaves the demo and goes back to the setup screen.

Signing in on the phone

The **Sign in** screen shows the site's name and address. Sign in with your account's **User name** and **Password**; your role needs the **Remote Login** permission. When the site requires sign-in codes, the app asks for one unless that phone passed a code for the account within the site's number of days and the password has not changed since. Below the password, a box that names the site's number of days keeps the sign-in on that phone for the days set in **Keep signed in for (days)** (30 unless changed) instead of 8 hours, as on the web; it is off until you tick it.

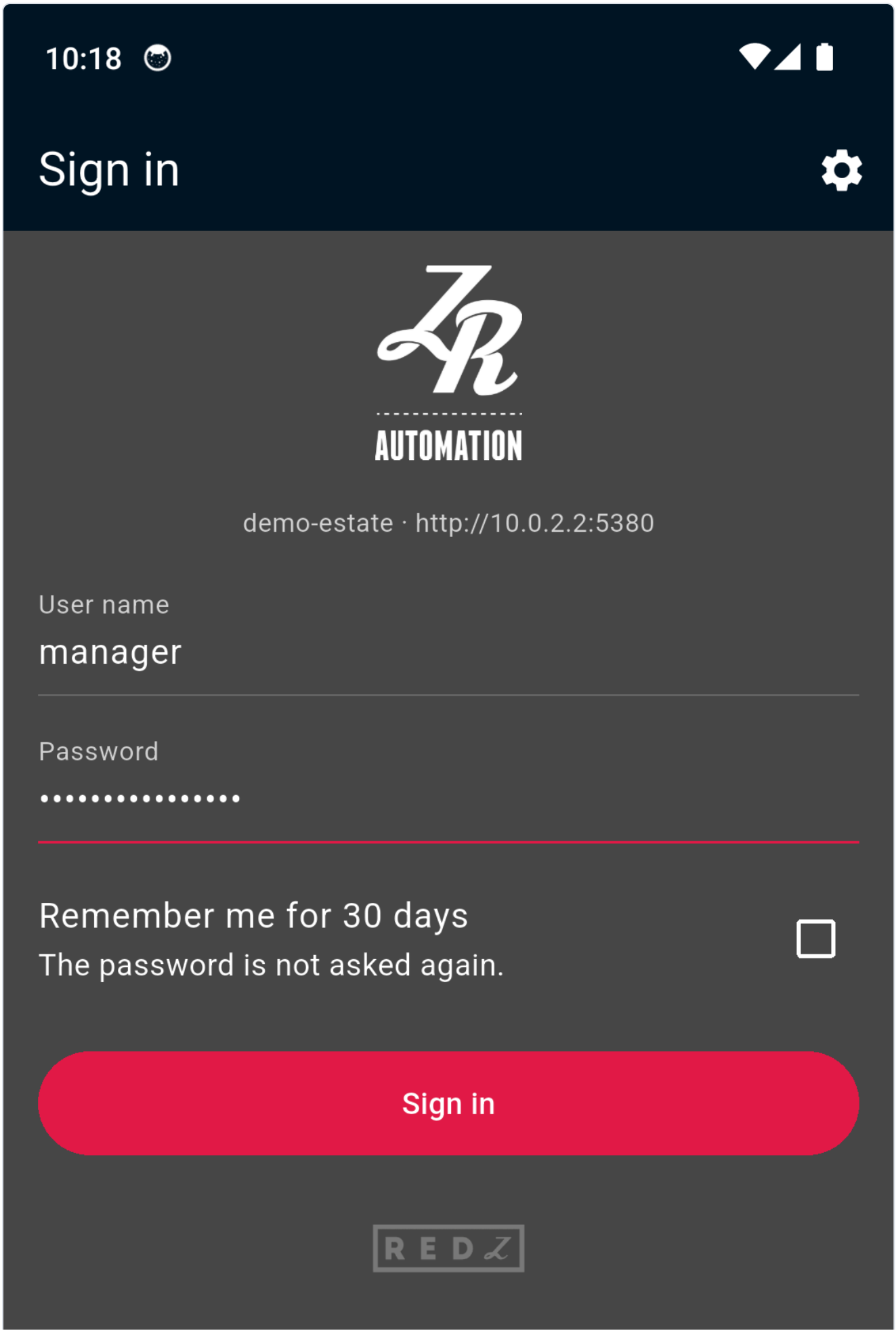

10:18
Sign in
AUTOMATION
demo-estate · http://10.0.2.2:5380
User name
manager
Password
Remember me for 30 days
The password is not asked again.
Sign in
REDZ



Figure 12.4 Signing in to the demo site through remote access; the site's name and address are shown above the form.

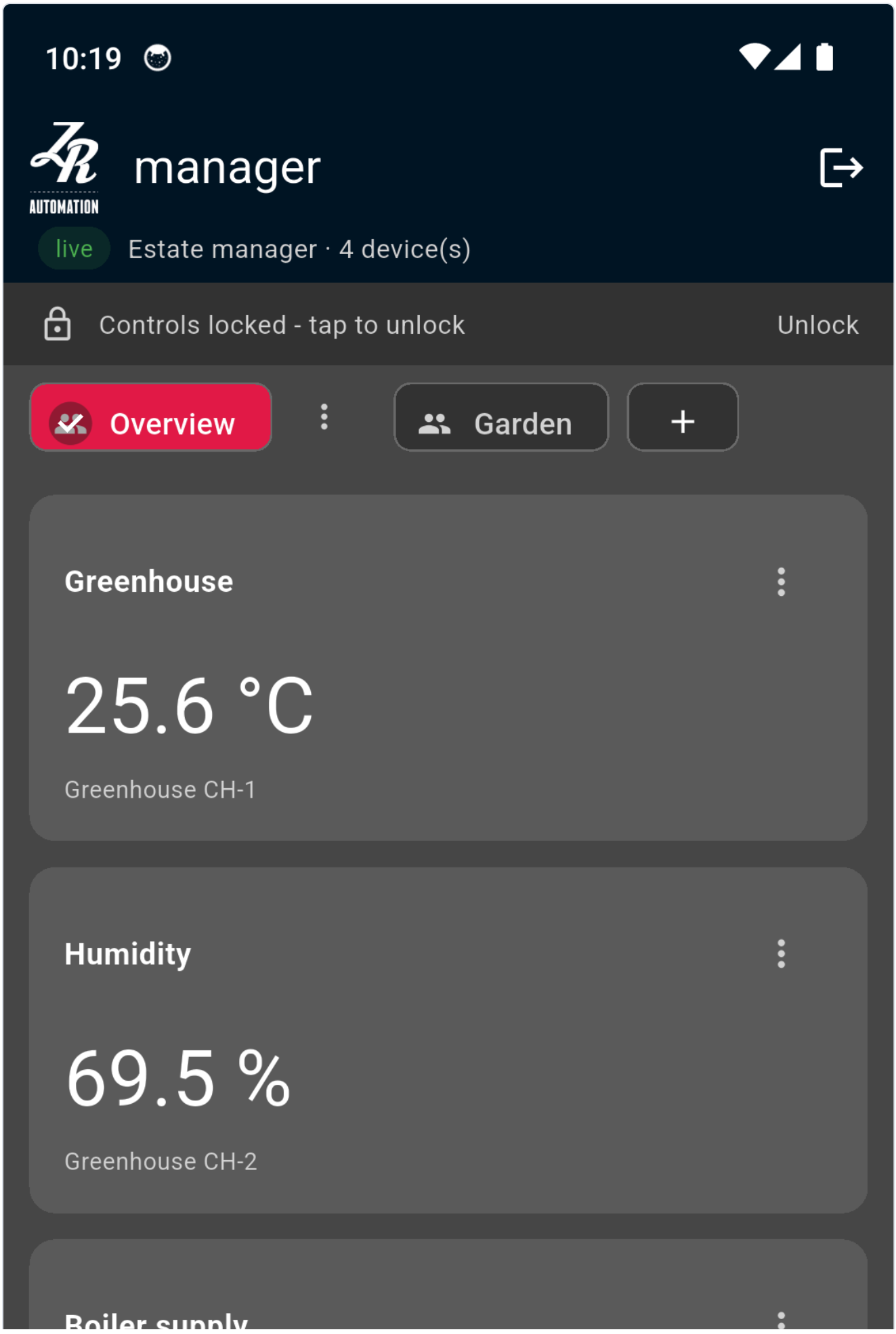
On Android 13 and later the phone asks once whether the app may send notifications. Allow it, or alarms cannot reach you when the app is closed.

The app's tabs

- **Dashboard**: the dashboard pages, as on the web, for a role with the Operations Dashboard permission.
- **Fleet**: the devices with their state, and each device's channels, for a role with the Fleet Status or the Device Settings permission.
- **Cameras**: the cameras, for a role with the Cameras permission.
- **Notifications**: the notices from the site, and for a role with the Alarms permission the active alarms. Every account has it.
- **System**: the web's other pages, as far as your role has them: **Logic & Automations**, **Users & roles**, **Historical Values**, **System Logs**, **System Health** and **System Settings**.

In **Logic & Automations**, each time block has the same switch as on the web screen: with the **Edit (Update)** action it turns the block off and on, without it the switch only shows the state. A time that follows the sun shows its Not before time too.

The top of every tab shows your account, whether the app is connected (live), your role and the number of devices it covers. The sign-out button offers **Sign out** and **Sign out and forget this device**; after the second one, the next sign-in from that phone asks for a code again when codes are required.


10:19
manager
AUTOMATION
live
Estate manager · 4 device(s)
Controls locked - tap to unlock
Unlock
Overview
Garden
Greenhouse
25.6 °C
Greenhouse CH-1
Humidity
69.5 %
Greenhouse CH-2

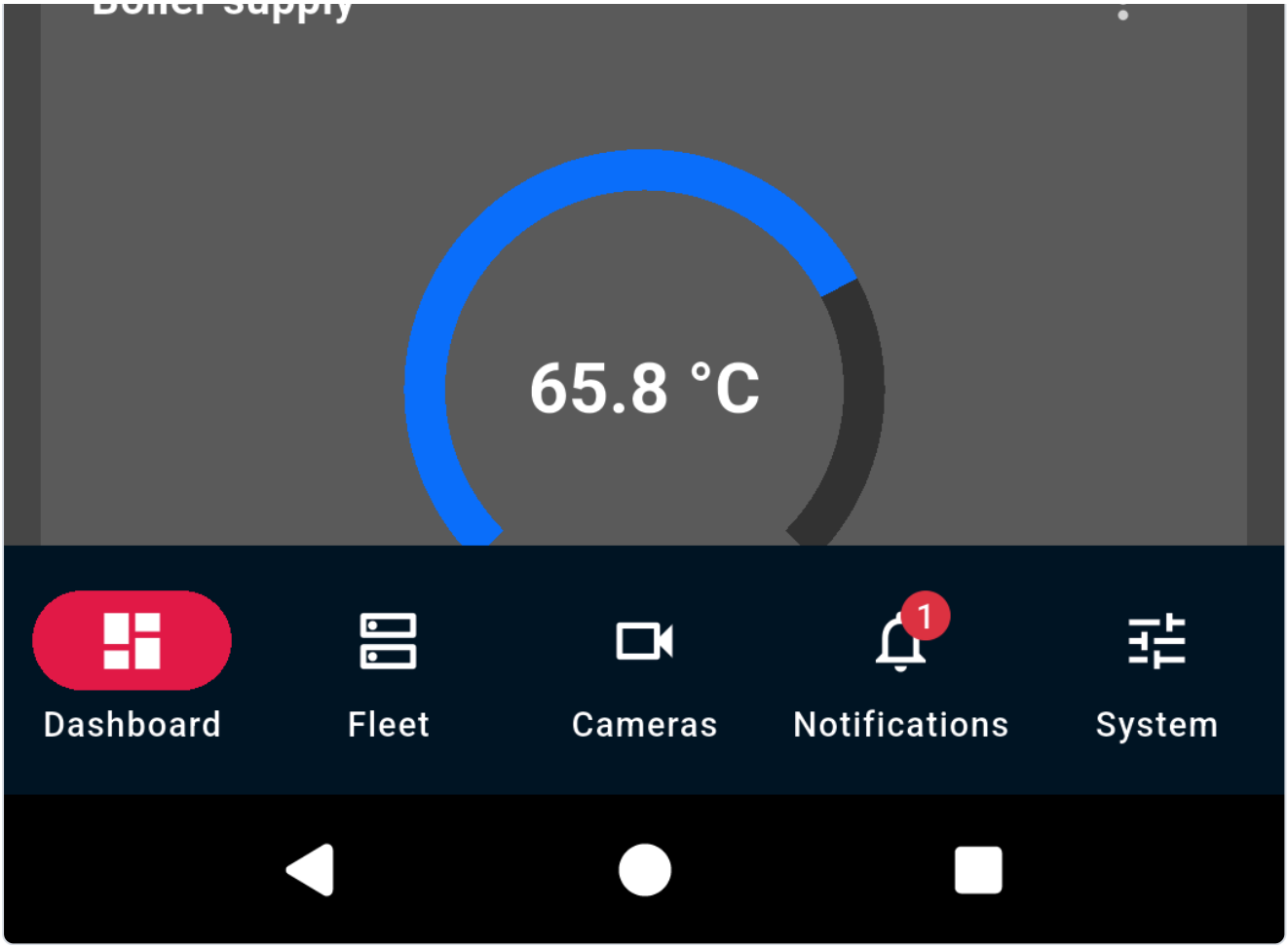


Figure 12.5 The Dashboard tab with the control lock above the widgets.

The control lock

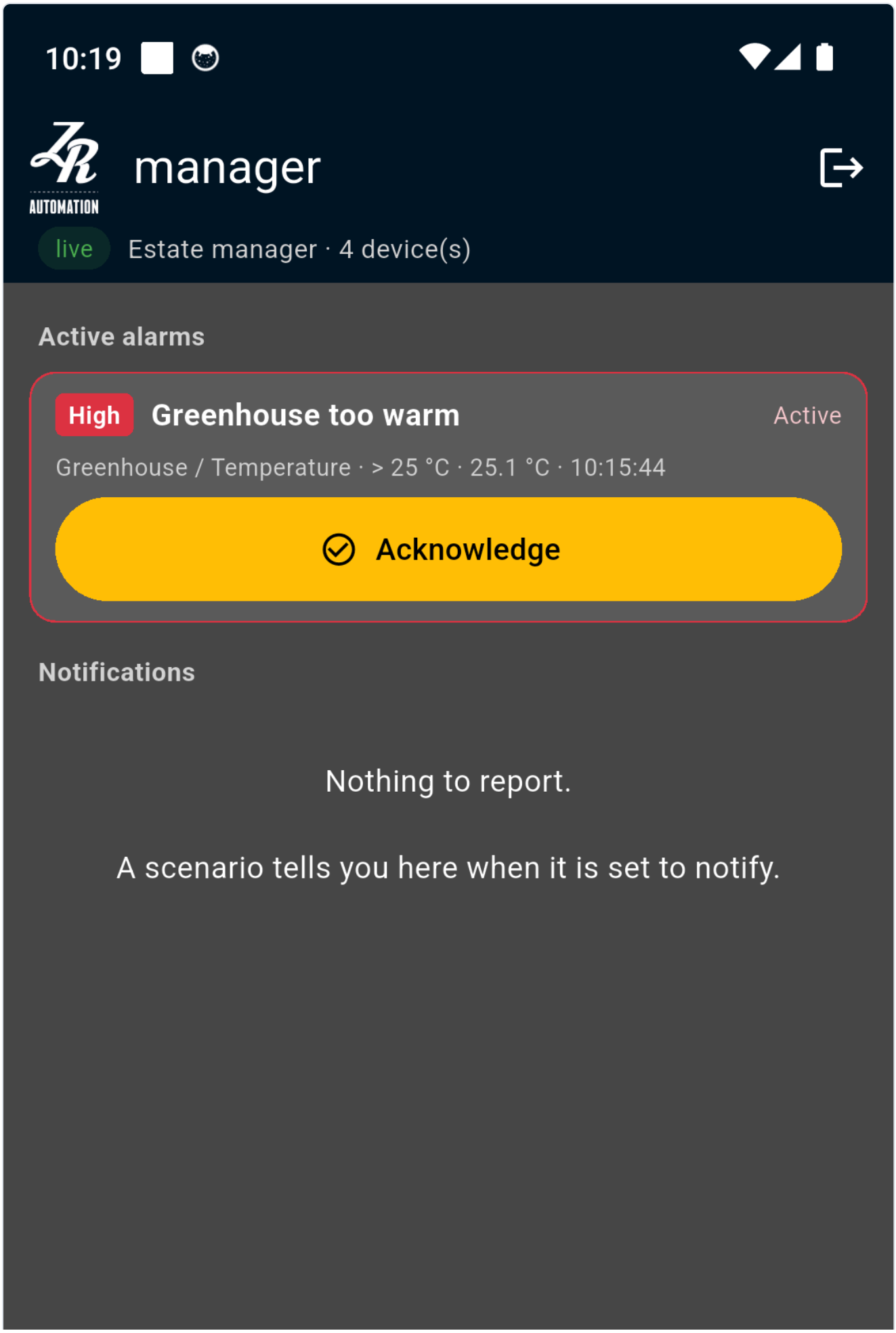
In the app, switches, buttons and outputs are locked so that a phone in a pocket cannot switch anything. Tap **Controls locked - tap to unlock** to unlock them for 2 minutes; they lock again by themselves, or at once with **Lock now**. One lock covers the dashboard and the device pages.

The lock is shown only when there is something to unlock: a role without the **Edit (Update)** action can watch but not switch, and sees the lock only on a dashboard page it may remove. Removing a dashboard page also needs the controls unlocked.

Notifications

For a role with the Alarms permission, the **Notifications** tab lists the active alarms as on the web's Active tab, each waiting one with **Acknowledge** and an optional note, and then the notices, newest first. The tab's badge shows how many alarms are waiting, or when none is, how many notices are new. Tapping a notification on the phone opens this tab.

An alarm notification plays the same alarm sound as the web screen. The words of a notification are read from the site when it arrives, so a phone that was switched off finds what it missed in this list.


10:19
manager
AUTOMATION
live
Estate manager · 4 device(s)
Active alarms
High
Greenhouse too warm
Active
Greenhouse / Temperature · > 25 °C · 25.1 °C · 10:15:44
Acknowledge
Notifications
Nothing to report.
A scenario tells you here when it is set to notify.

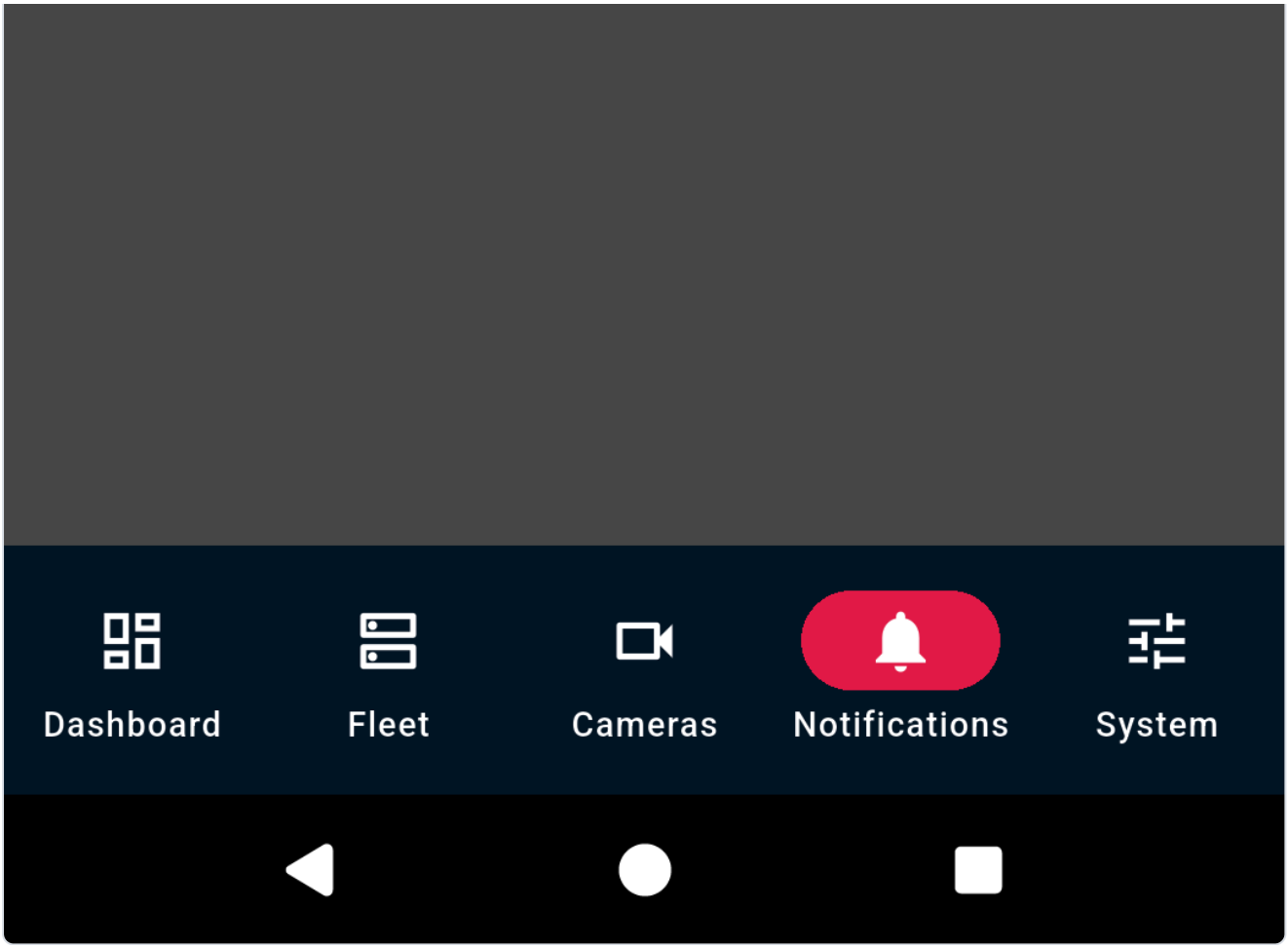
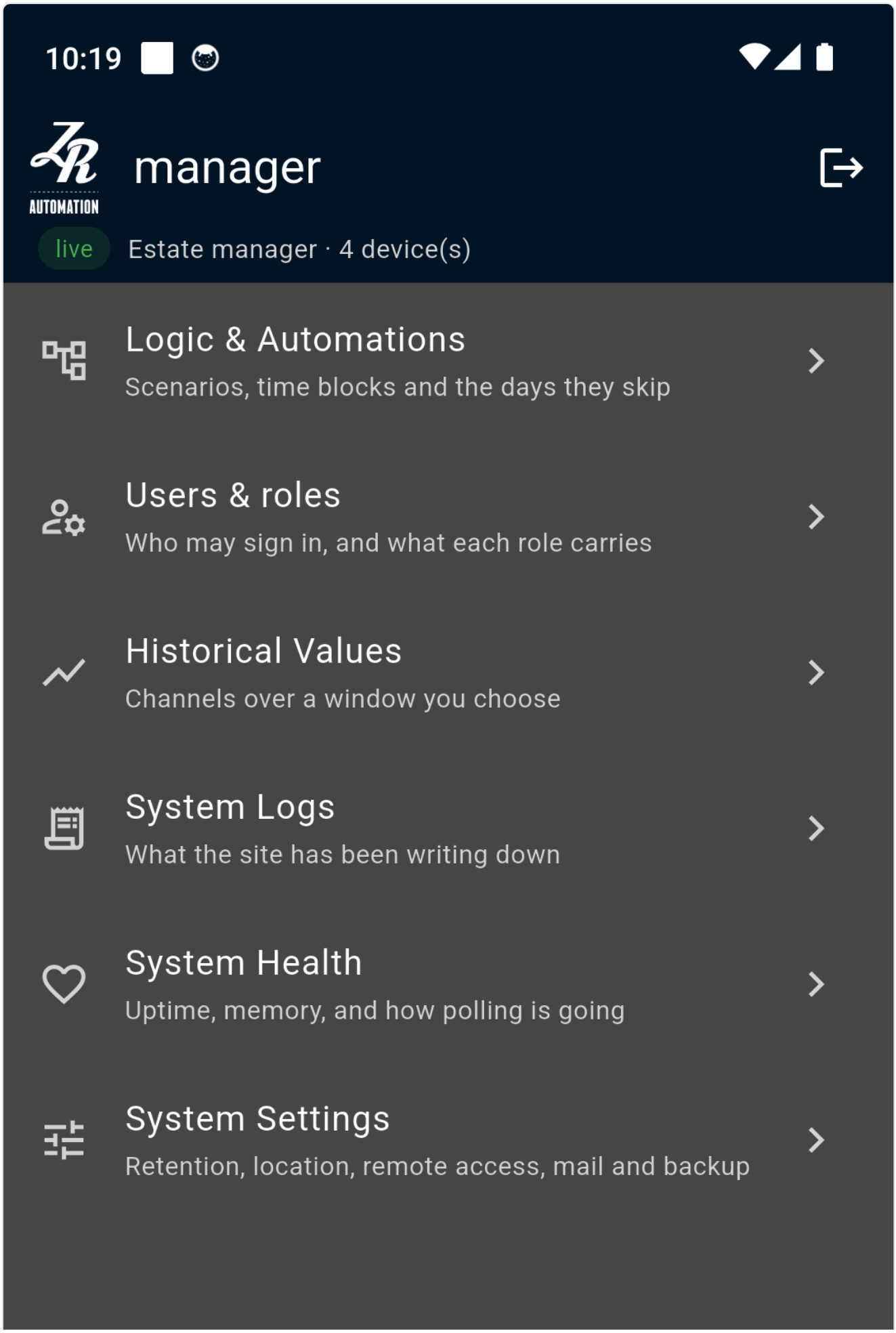


Figure 12.6 The Notifications tab: the alarms waiting to be acknowledged, then the notices.

Alarm definitions and the alarm history are on the web screen only.


10:19
manager
AUTOMATION
live
Estate manager · 4 device(s)
Logic & Automations
Scenarios, time blocks and the days they skip
Users & roles
Who may sign in, and what each role carries
Historical Values
Channels over a window you choose
System Logs
What the site has been writing down
System Health
Uptime, memory, and how polling is going
System Settings
Retention, location, remote access, mail and backup

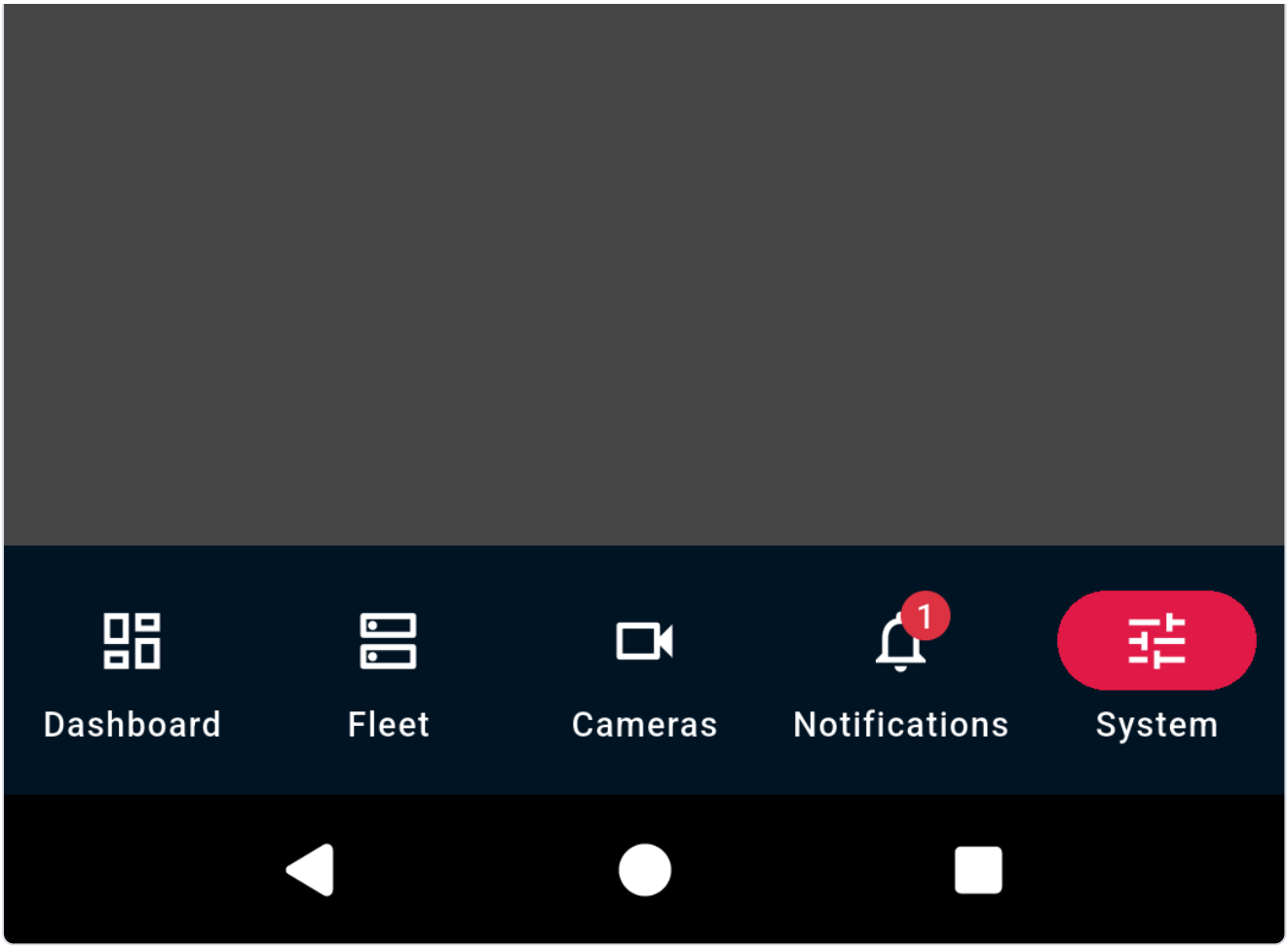


Figure 12.7 The System tab: the web's other pages, as far as the role has them.

13 System logs, health and settings

Administrators

Three places look after the site itself: the **System Logs** page, the **System Health** page and the **System Settings** tab of the **Management** page.

System logs

The **System Logs** page is the site's record of what was done, by a person, by a scenario or by the site itself: sign-ins, changes to devices, settings and accounts, acknowledged alarms, a device that stopped answering, a digital input or output that turned on or off. The values of analog channels are not written there; they are in the channel history. The page needs the **System Logs** permission.

Each entry has its time, its level (**Info**, **Warning** or **Error**), its source and its message. When a person did it, the source ends with that person's account name in brackets.

The page lists the newest 500 entries, newest first, and adds new entries as they happen.

All or one level shows the entries of that level. The **Search source / message...** box keeps the entries whose source or message contains what you type.

The chart above the list shows how many entries each of the last 7 days holds, today included. The site counts them, among the entries your role may see; the level buttons and the search box do not change it. New entries are added as they happen.

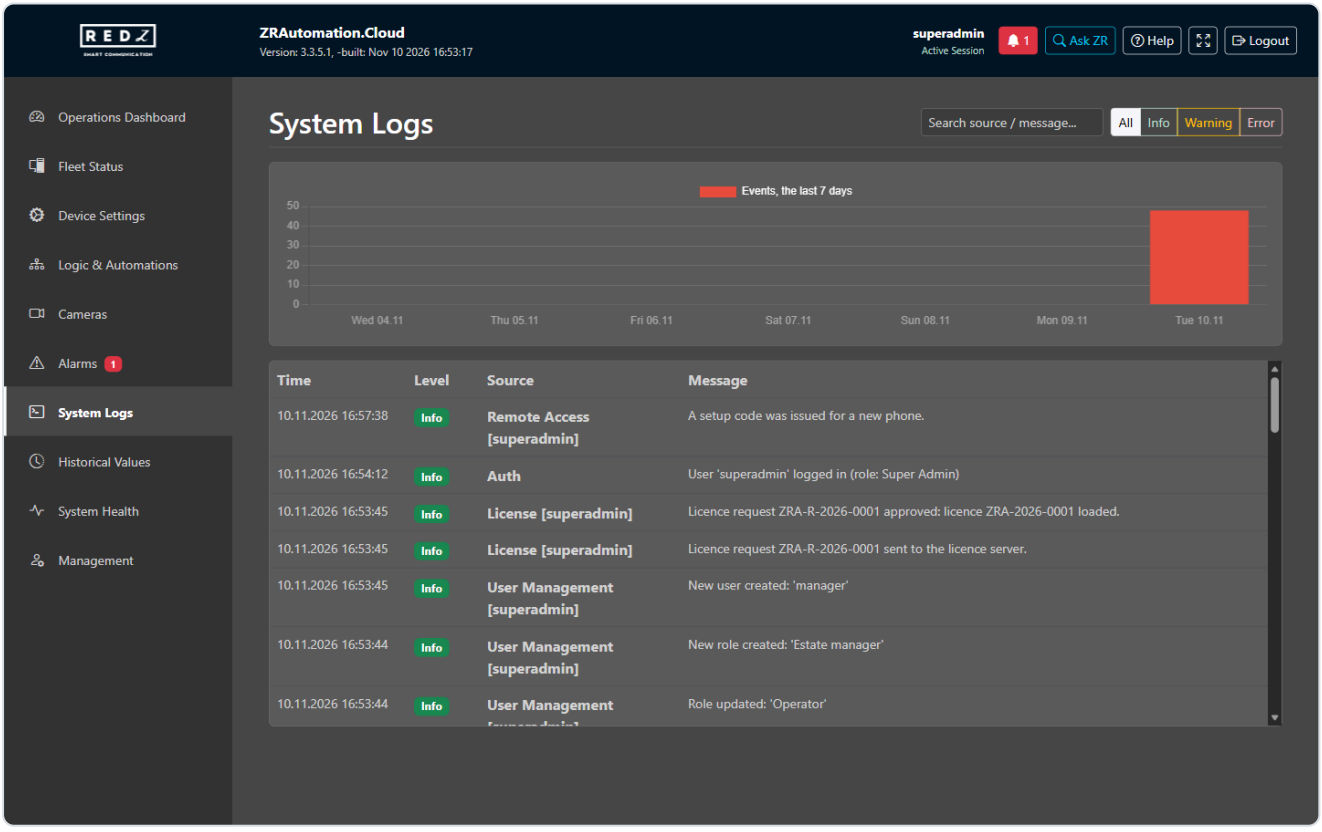


Figure 13.1 The system log as an administrator sees it, newest first, with the number of entries per day of the week above it.

The entries about the devices' connections, their settings, digital channels turning on or off and writes that failed are shown only to a role with access to all devices. An entry about an output switched by a person, a scenario, a time block or a timed output is shown to a role that covers its device, and for a scenario both of its devices; such entries written before this version are shown only to a role with access to all devices. In the mobile app a role without access to all devices finds these entries in the list, but they are not added as they happen.

Entries are kept for the number of days in **System Log (days)** in System Settings, 30 unless changed.

System health

The **System Health** page shows how the site is running. It needs the **System Health** permission. It is read when the page opens; **Refresh** reads it again.

- **Uptime**: how long the site has been running since it last started.
- **Memory (RAM)**: the memory the site is using.
- **Database Size**: the size of the site's database file.

Device Poll Statistics lists each active device your role covers with its successful and failed reads since the site last started, and the success rate: green from 95%, yellow from 70%, red below.

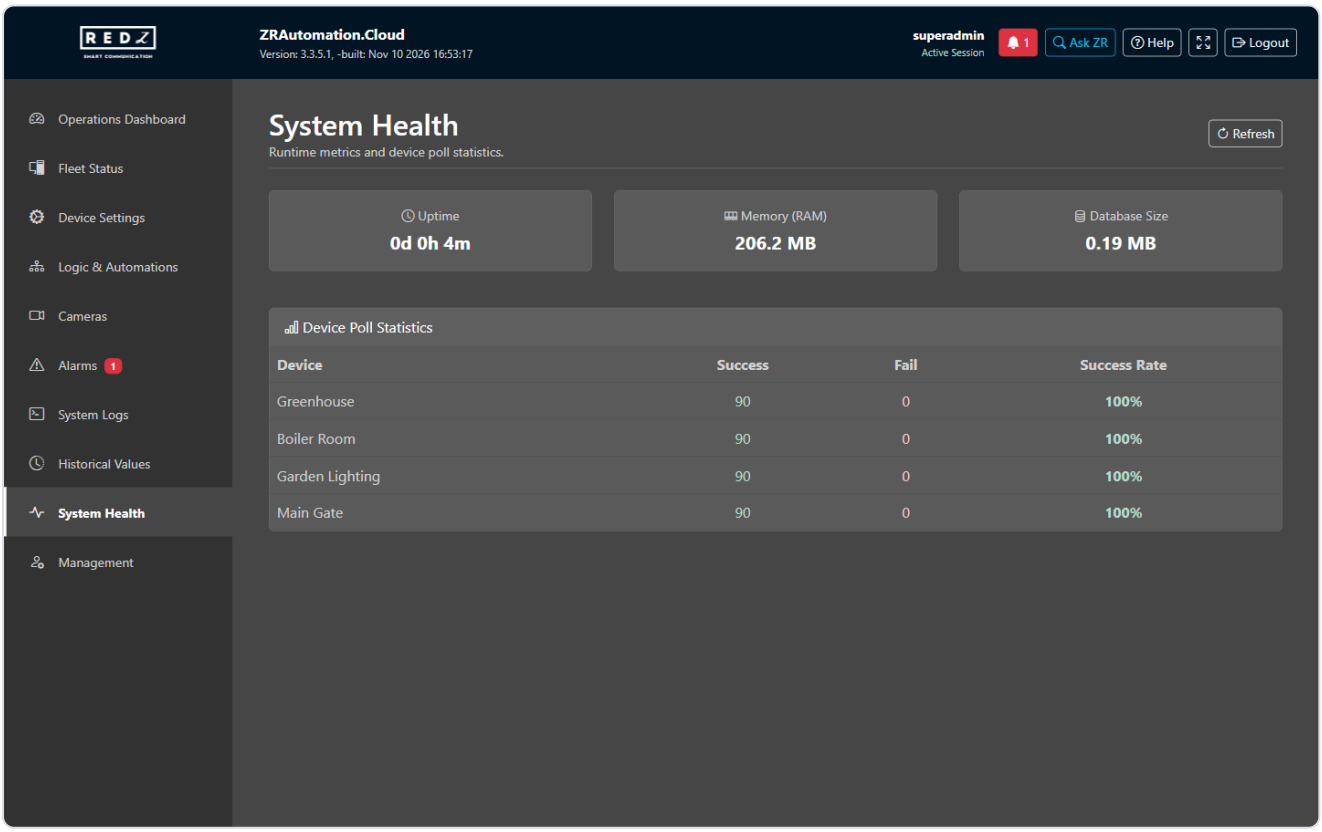


Figure 13.2 How long the site has been running, its memory and database size, and each device's reads since it started.

System settings

The **System Settings** tab is on the **Management** page, which needs the **Management** permission. Changing a setting there also needs the **Edit (Update)** action. **Backup & Restore**, the e-mail settings and **Keep signed in for (days)** are shown only to a role with access to all devices. The **Remote Access** settings have their own permission and are described in Remote access and the mobile app, and the **Camera Recorder** in Cameras.

How long records are kept

Under **Data Retention**, old records are deleted by the site itself: log entries and channel history when the site starts and then once a day, alarms every hour:

- **System Log (days)**: system log entries, 30 days unless changed.
- **Channel History (days)**: the recorded values of the channels, 90 days unless changed. A channel's last value from before that time is kept, so a channel that has not changed since still shows its value.
- **Alarms (days)**: alarms that are gone and acknowledged, 90 days unless changed. An alarm nobody has acknowledged is kept.

Default channel deadband is how far a reading has to move before it is recorded in the channel history, for every channel that does not set its own. 0 records every change. Select **Save Retention**.

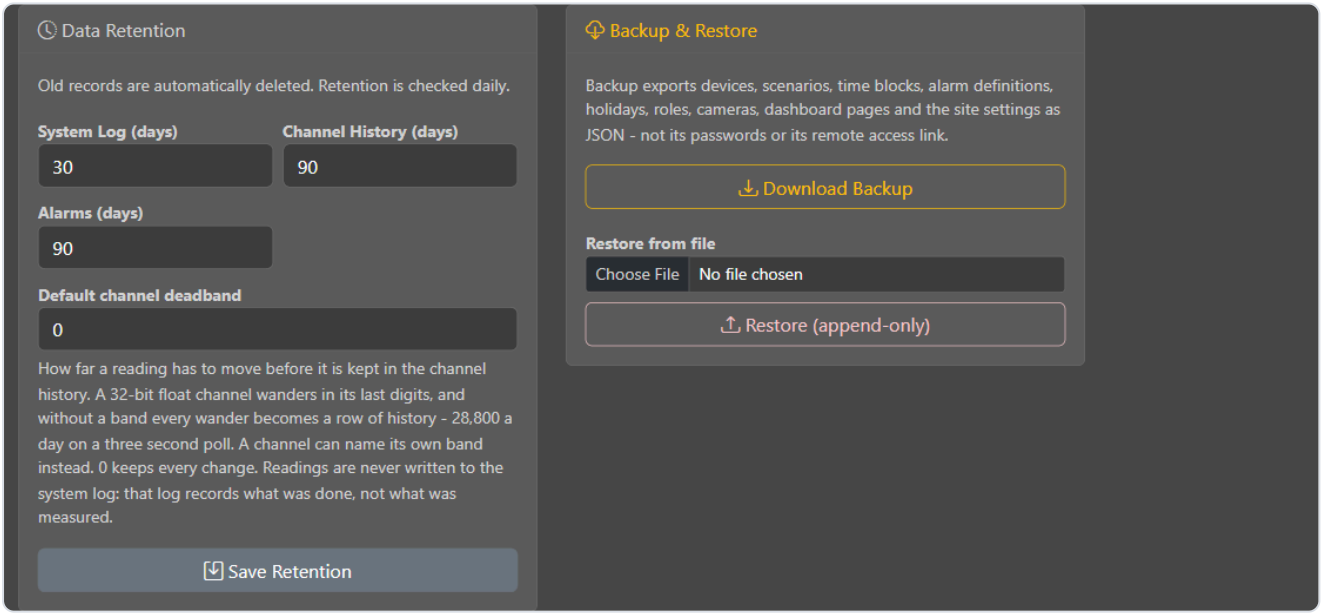


Figure 13.3 How long records are kept, and backup and restore, which only a role with access to all devices sees.

Location and sun times

Time blocks can follow sunrise and sunset. Enter the site's **Latitude** and **Longitude** under **Location & Sun Time**; the site works out each day's sunrise and sunset from them by itself,

without the internet. A site with no location uses the **Fallback Sunrise** and **Fallback Sunset** times. Select **Save & Refresh**; **Today's Sun Times** shows the times in use.

Backup and restore

Download Backup saves a file with the devices and their channels, the scenarios and time blocks, the alarm definitions, the holidays, the roles, the shared dashboard pages, the cameras and the settings someone has set up.

Accounts, personal dashboard pages, passwords and the remote access settings are not in a backup, and neither is the switch that requires sign-in codes.

1. Under **Restore from file**, choose a backup file.
2. Select **Restore (append-only)** and confirm.

A restore only adds: what the site already has, by its name, is left as it is, and a setting is restored only where the site has none. A scenario, time block or alarm definition whose device is not on the site is not restored, and neither is a camera whose name or recorder channel the site already uses. The widgets of a restored page are matched to this site's devices and cameras by name; a widget whose device or camera is not on the site shows nothing. The devices of a restored role are matched by name too: a device that is not on the site is left out of the role, and a role with access to all devices keeps it. When it is done, the restore says what it added and what it left out. A file in which a new device has two channels with the same number is refused as a whole.

E-mail and the sign-in code

The site sends e-mail for two things: the codes for signing in from outside the local network, when they are required, and notices to an account's own address when its password is changed, when it is locked after failed sign-ins and when a new device is remembered for it.

1. Turn on **Enable sending email** and enter the mail server's **SMTP Host** and **Port**. Keep **Use TLS** on: with it off, the password travels unencrypted.
2. Enter the mail account's **Username** and **Password**. Leave the password blank to keep the stored one. It is kept sealed with the site server's own key: after the site moves to another server, the page says so and it has to be entered again.
3. Enter the **From Address** and, if you wish, a **From Name**, and select **Save Email Settings**.
4. Enter your address next to **Send Test**, select it, and check that the message arrives. The test uses the saved settings: with changes not yet saved, the page asks you to save first.
5. Once the test message has arrived, turn on **Require a mailed code for sign-ins from outside the local network** to require codes, set **Remember a device for (days)**, from 1 to 365; 30 unless changed, and select **Save Email Settings** again.

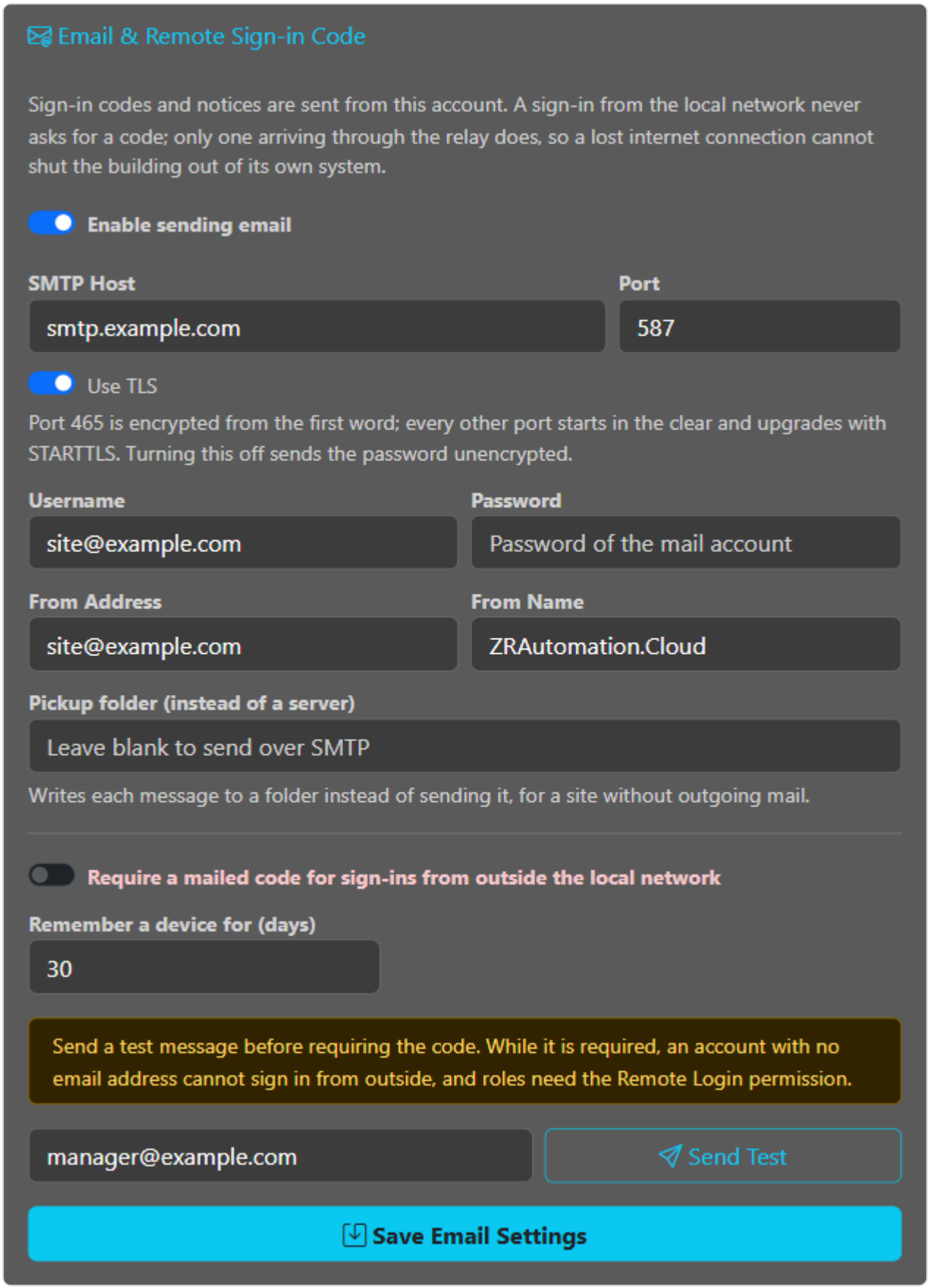


Figure 13.4 The mail account that sends sign-in codes and account notices, filled with example values (not saved).

Codes can be required only while e-mail is on with a **From Address** and a mail server or a pickup folder. A sign-in from the local network never asks for a code. While codes are required, an account without an e-mail address cannot sign in from outside. Signing in from outside always needs the **Remote Login** permission, codes or not (see Signing in).

Pickup folder (instead of a server) writes each message to a folder on the site server instead of sending it, for a site without outgoing mail.

14 Troubleshooting

Everyone

Each part below starts from what you see. The **System Logs** page usually says why; the entries about the devices' connections and readings are shown only to a role with access to all devices.

The web screen does not open

- Check the address: it is the server's address followed by :5000.
- Check that the server is switched on and that the Windows service ZRAutomation.Cloud is running on it. The service starts with Windows, a little after the other services, and Windows starts it again after a minute if it stops by itself; otherwise the server's administrator can start it again in Windows.
- Check that the computer or tablet is on the site's local network and that nothing between it and the server blocks the port. The setup program opens the port for the server's own local network only: a computer on another network needs the server's administrator to allow it.

The screen says the live stream is not connected

Live stream reconnecting... means the screen has lost its live connection to the site and is trying again by itself, every 30 seconds for as long as it takes. **Live stream not connected - values may be stale** means the screen could not connect and is not trying again: the values on the screen may be old. Check the site as in the part above, then reload the page.

No device is read and the strip at the top is red

The site does not read or run without a licence that runs: the trial or the licence has ended, the licence is for another server, or the server's clock was put back. The red strip says which. See Licence and support.

A device is OFFLINE

A device is OFFLINE when the site cannot read it. **Fleet Status** shows when the site last read it, and **System Health** counts its failed reads.

- In the device list of **Device Settings**, check that the device is **Enabled**. A **Disabled** device is not read. A copy made with **Clone device** starts disabled.
- Check that the device is powered and on the network, and that its **IP / COM Port** and **Port** are right.
- When the connection is lost, the System Logs get an entry with the device's name, its address and the reason.
- While a device does not answer, its limit and state alarms neither rise nor clear and the history leaves the time out; a disabled device's alarms are closed. A **Device not answering** alarm, if one is defined for the device, tells you about it (see Alarms).

A value shows a dash or looks wrong

- A dash means the channel read no number. The dash stays until it reads one again, and the System Logs note both moments.
- A value that is far off can come from its **Format**: a 32-bit value read in the wrong word order (ABCD or CDAB), or as the wrong kind of number, gives a very different value. Check the format against the device's documentation, then the scale.
- A value that changes on the screen but not in the history is moving less than the channel's deadband, or the site's default deadband when the channel has none (see Devices and channels).

A camera shows No picture

- If every camera shows **No picture**, check **Camera Recorder** in System Settings: the recorder's address, ports, account and password. When the recorder refuses the password, the site stops asking it for pictures, so that the recorder does not lock its account, and the System Logs say so. Pictures come back when the right password is saved.
- After the site has moved to another server, the recorder password has to be entered again.
- If one camera shows No picture, check its **Channel**. For a camera that gives no still picture, choose **RTSP** under **Source**.

The phone cannot be set up

- A setup code is good for 10 minutes and for one phone. If the app says the code is not valid any more, show a new one on the web screen.
- If the app says **This relay does not know that site name.**, check the site name against the **Site Slug** on the Remote Access card.

The phone cannot sign in

- **The site is not reachable through the relay right now.** The site is not connected to the relay. Check the badge on the **Remote Access** card; while it is not Connected, the reason is shown under the fields. The site also needs its internet connection.
- **This account may not sign in from outside the local network.** The account's role needs the **Remote Login** permission.
- If the app says the account has no e-mail address, an administrator adds one on the local network: while sign-in codes are required, an account needs one to sign in from outside.
- **A one-time password is still in place. It has to be changed on the local network.** Sign in once on the web screen and set a new password.
- **The site could not send the code. Its email settings need attention.** Check the e-mail settings with **Send Test** (see System logs, health and settings).

- **The relay refused the client key, or does not know this site name.** Set the phone up again with a new setup code.

Notifications do not arrive

- Notifications travel through remote access: while it is not connected, none are sent, and none are sent later. The app still lists the alarm among its notices the next time it connects.
- On Android 13 and later the app needs the phone's permission to send notifications.
- An alarm notifies only when **Tell the phones** is ticked, and only the accounts whose role has the **Alarms** permission and covers the device.
- **Send a test notice now** on a saved scenario shows whether notices reach the phones.

No alarm sound

A browser may refuse to play sound until someone has touched the page; select **Tap to allow sound**. Check also that the screen has not been muted with **Mute on this screen**.

A time block did not switch

A start or an end missed in its own minute is written late, as soon as the device answers, but only until the block's other time; the System Logs show the late write, and the failed attempts when the device did not answer. A block that follows sunrise or sunset does nothing on a day the site has no sun times for, and a block with **Do not run on Holidays** skips the days on the Holidays tab (see Logic and automations). A block marked **Disabled** has its switch off and writes nothing; a sun time with **Not before** does not come earlier than the time set there.

Nobody can sign in

- After 5 failed attempts, wrong passwords and wrong sign-in codes together, an account is locked for 15 minutes. It can sign in again after that time.
- If no administrator can sign in, REDZ or the server's administrator can run ZRAutomation.Cloud.exe --reset-admin-password from an administrator command prompt on the server. It gives the superadmin account a one-time password and shows it in the window, unlocks and switches on the account, gives it full access again and creates it again if it was deleted. It signs the account out everywhere and makes its remembered phones ask for a sign-in code again. The one-time password must be replaced at the first sign-in.

15 Moving from ZR Automation

Everyone

ZR Automation was a Windows program made of five modules. ZRAutomation.Cloud does the same work on a server at the site, with a web screen and a mobile app. This chapter takes each module of ZR Automation and says where its work is now, and what this version does not have.

Device Registration and Configuration

Devices are registered on the **Device Settings** page, with their channels (see Devices and channels). The site reads Modbus TCP devices on its network, from any maker. How a value is shown is chosen on the dashboard, as a widget (see Dashboards and widgets).

Read Data and Instantaneous Data Monitoring

There is no reading to start or schedule: the site reads every enabled device, 3 seconds after each read, all the time. The values are followed on the **Operations Dashboard** and on each device's page, on the web screen and in the mobile app; **Fleet Status** shows which devices are online. Outputs are switched there too, by a role with the **Edit (Update)** action that covers the device.

Detailed Data Analysis

The **Historical Values** page shows the recorded values as a chart, a summary and a table, over the range and interval you choose, and saves them as an Excel workbook. For a PDF, print the page and save it as PDF from the browser's print window (see History, analysis and export).

Alarm Management

The **Alarms** page holds the alarms: limits on a value, the state of a digital channel, and a device that stops answering, each with its own text. Alarms are acknowledged, with a note if you wish, and the screen shows a bell and plays a sound while one waits (see Alarms).

Instead of an SMS, an alarm with **Tell the phones** ticked is sent as a notification to the mobile app, on the phones of the accounts that may see it. A scenario can send a notice of its own (see Logic and automations).

Settings

The site's settings are on the **Management** page, with the accounts and roles (see System logs, health and settings, and Users, roles and permissions). The version is shown in the banner at the top of the web screen.

Not in this version

- Serial connections and the GPRS, 3G, 4G and radio (RF) modems: the site reads devices over its network only.

- SMS messages. Alarms are not sent by e-mail either; e-mail is used for sign-in codes, account notices and licence notices.
- A Turkish interface: the web screen and the app are in English.
- Licences by part: every installation has every part, and each person's role decides what they see. A licence sets the number of devices (see Licence and support).
- Windows XP, 7 and 8, and 32-bit Windows. The server needs a Windows version listed in Installation and updates.

Moving a site

ZR Automation's devices and readings are not carried over. The devices are added again on the **Device Settings** page, where the **Batch IO Configurator** fills many channels at once; the history starts when the site first reads them.

A Appendix A. Permissions

Generated from the product

A role is a set of page permissions, action permissions and devices. A role with access to all devices has every page and every action, except Remote Login, which must be ticked.

Pages

PERMISSION	WHAT IT ALLOWS	WEB SIDEBAR	MOBILE APP
Operations Dashboard	Shows the Operations Dashboard page.	Operations Dashboard	Dashboard
Fleet Status	Shows the Fleet Status page.	Fleet Status	Fleet
Device Settings	Shows the Device Settings page.	Device Settings	Fleet
Logic & Automations	Shows the Logic & Automations page.	Logic & Automations	System: Logic & Automations
System Logs	Shows the System Logs page, including new entries as they arrive.	System Logs	System: System Logs
Historical Values	Shows the Historical Values page.	Historical Values	System: Historical Values
System Health	Shows the System Health page.	System Health	System: System Health
Cameras	Shows the cameras. Adding, changing or removing a camera also needs the matching action. Without it, a control linked to a camera still works but shows no picture.	Cameras	Cameras
Alarms	Shows the alarms of the role's devices and allows acknowledging them. Adding, changing or deleting an alarm also needs the matching action.	Alarms	-
Management	Shows the Management page. Changing System Settings also needs the Edit action; the e-mail, sign-in and backup settings need access to all devices.	Management	System: Users & roles, System: System Settings
Remote Access	Shows and changes the remote access settings, and creates the	-	-

PERMISSION	WHAT IT ALLOWS	WEB SIDEBAR	MOBILE APP
	setup code for a phone. On the web they are on the Management page, so the role also needs Management.		
Shared Dashboards	Allows changing the shared dashboard pages that every user sees.	-	-
Remote Login	Allows signing in from outside the site through remote access. Full access does not include it: it must be ticked.	-	-

The app's Notifications tab is shown to every account. Its System tab is shown when at least one of its rows is.

Actions

PERMISSION	WHAT IT ALLOWS
Add (Create)	Creating devices, alarms, cameras, automations, users and roles.
Edit (Update)	Changing devices, alarms, cameras, automations, users and roles, switching outputs, and changing System Settings together with the Management permission.
Delete	Deleting devices, alarms, cameras, automations, users and roles.