

SYSTEM OVERVIEW

- 1 What Raedius Is
- 2 Glossary of Terms
- 3 Supported Devices

DEPLOYMENT · INTEGRATOR

- 4 Plan the Project Hierarchy
- 5 Create Projects
- 6 Users & Roles
- 7 Register Devices
- 8 Device Grouping
- 9 Action Profiles
- 10 Custom Alerts & Schedules
- 11 Commissioning Checklist

HANDOVER

- 12 Handover to Management

DAILY OPERATIONS

- 13 Opening & Logging In
- 14 The Alerts Page
- 15 The Devices Screen
- 16 Resident Sensor How-Tos
- 17 Privacy & Intervention

MAINTENANCE

- 18 Leak Controller Functions & Settings
- 19 Routine Maintenance
- 20 Troubleshooting

Easy User Guide

A start-to-finish operating manual for the Raedius water-leak monitoring platform — from initial server deployment by the Systems Deployment Integrator, through handover, to daily operation and maintenance by concierge and building management staff.

Part 1 · Deployment & Setup

Part 2 · Handover

Part 3 · Daily Operations

Part 4 · Maintenance

PART 1 · SYSTEM OVERVIEW

1. What Raedius Is

The **Raedius Web Console** is a cloud platform for managing Safehous IoT devices (white-labelled from YoSmart under licence) from a web browser. In a residential deployment it connects every leak sensor and automatic water shutoff in the building to a single monitoring dashboard, so that a water event in any suite is visible at the concierge desk within seconds.

Detect

Puck and rope sensors under every water source report leaks, tamper, and battery status.

Act

Valve controllers shut off a suite's water supply automatically when water is detected.

Notify

Residents get Safehous app alerts; staff monitor everything through the Raedius Alerts page.



Who this guide is for. Sections 4–13 are for the Systems Deployment Integrator commissioning a blank server. Sections 14 onward are for concierge and building-management staff operating the system day to day.

PART 1 · SYSTEM OVERVIEW

2. Glossary of Terms

Raedius	The web console used to monitor leak sensors and controllers from the concierge desk. Accessible from any browser.
Safehous	The brand of the sensors, controllers, and resident app. Safehous white-labels the hardware and platform from YoSmart under licence — a few console labels (e.g. the YoLink import button, YS model prefixes) retain the licensor's name.
Safehous App	The phone/tablet app residents use to monitor their own sensors and turn water valves on or off.

Sensor	Battery-powered device placed under or around every water source. On contact with water it beeps and alerts the resident (app) and staff (Raedius), repeating roughly every five minutes until addressed.
Puck sensor	Square sensor resting on a cradle (arrows aligned — no click). Used in accessible spots: behind toilets, under sinks.
Rope sensor	Square sensor with a ~1 m braided cable. Used in hard-to-reach spots: under laundry machines, dishwashers, freezers, shutoffs. Both rope and body detect water; unplugging the rope stops the beeping.
Controller	Motorized shutoff installed in a suite's supply pipes, replacing manual valves. State OPEN = water on, CLOSED = water off. Operated by Smart Fob, Safehaus app, or the Raedius Devices screen. Its detail page reports daily/weekly/monthly flow activity (Section 18).
Smart Fob	One-button wireless fob issued per suite for turning water on/off. AAA battery, resident-supplied.
Project	Raedius's hierarchical container (system → building → suite). Devices, users, roles, groups, automations, and alarm history all bind to a project.
Action Profile	An automation rule: trigger → conditions → actions (notify, invoke devices, create alarm). Defined at device, group, or project level.

PART 1 · SYSTEM OVERVIEW

3. Supported Device Families

Raedius manages the following Safehaus device families (hardware licensed from YoSmart; model numbers retain the licensor's YS prefix). Model numbers are printed on the device label next to the QR code.

Leak Sensor

YS7903 · 7904 · 7906 · 7916

Valve Controller

YS4909 · 5001 · 5002 · 5003

Water Meter Controller

YS5006 · 5007 · 5008

Hub / Speaker Hub

YS1603 · 1604

Siren

YS7103 · 7104 · 7105

Outlet / MultiOutlet

YS6602 · 6604 · 6801 · 6802

Temp & Humidity

YS8003-8006 · 8014 · 8015

Thermostat

YS4002 · 4003

Smoke / CO · Door · Lock

YS7A01 · 7704/7706 · 7606/7607

PART 2 · DEPLOYMENT — INTEGRATOR

4. Plan the Project Hierarchy

A **project** is the container everything else binds to: devices, device groups, users, roles, action profiles, alarm records, and audit logs. Projects nest up to **four levels**, with up to 9,000 sub-projects per layer. Design the hierarchy on paper before touching the server — restructuring later requires device migration and breaks groups and action profiles.

Level 1 King's Landing Water Leak Detection System

└─ **Level 2** Building 1515

| └─ **Level 3** Suite 0101

| └─ Suite 0102 · Suite 0103 · ...

└─ Building 426 · Building 428

└─ Common Areas (lobby · gym · parkade)

! Naming convention matters downstream. Staff search devices as BUILDING#.SUITE# with four-digit suite numbers (e.g. 1515.0101). Name suite-level projects consistently with this format from day one.

4.1 Licensing & quotas

- Base annual fee **\$300** plus **\$5 per device per year**; a 2-month grace buffer applies after expiry.
- SMS, email, and voice-call notifications draw from a basic communication package — purchase an add-on **Communication Package** if alert volume exceeds it.
- Budget notification quota against your action-profile design (Section 10) before go-live.

PART 2 · DEPLOYMENT — INTEGRATOR

5. Create Projects & Sub-Projects

1

Create the primary project

Project Management → PROJECT button → fill in the form → Save. Enter accurate contact details: project contacts are used as action-profile message recipients, and Raedius service reminders (renewals) go to the primary project's contacts by SMS/email.

2

Create second-level projects (buildings)

Select the primary project in the left-hand project tree → SUB-PROJECT button → fill in the form → Save. One per building or wing.

3

Create third-level projects (suites)

Select the building project → SUB-PROJECT → one project per suite, named with the four-digit convention (0101, 0102 ...). Repeat for every suite; the Excel device import can also auto-create these (Section 7).

4

Verify the tree

Click through each level and confirm names, contacts, and structure before importing devices. Editing later is safe (Operation → Edit), but moving devices between projects requires migration and breaks groups/action profiles.

[screenshot placeholder — Project Management page with project tree + SUB-PROJECT button]

✗ **Project deletion is irreversible** and cascades: sub-projects, all associated devices, groups, action configurations, users, and alarm history are destroyed with it. Never delete a project on a live building without a written change order.

PART 2 · DEPLOYMENT — INTEGRATOR

6. Set Up Users & Roles

Users and roles can be created at every project level. Open them via **Project Management** → **Operation** → **User Permissions** on the relevant project. **Create roles before users** — a login account cannot be created without a role.

6.1 Roles (create first)

1. Switch to the **Roles** tab and click the **Roles** button.
2. Enter a name and description, then check the permission boxes the role needs.
3. Click **Save**.

i A role's data access covers **its own level and everything below it**. A role created at Level 1 sees the whole system; a role created on "Building 1515" sees only that building's suites. Create the concierge role at the level matching the staff's monitoring scope. Users of a project cannot use roles created in higher-level projects.

6.2 Creating vs. inviting users

Create (managed account)

Click **Create**, fill in user details. If "allow user login" is selected, also set account name, password, and role. Admin retains full edit/delete control. Use for shared desk accounts (e.g. the concierge station).

Invite (self-owned account)

Click **Invite**, enter email + role, click **Send**; the user accepts via emailed link. Use when one person manages multiple projects. Admin can only change their role or remove them — never edit or delete the account itself.

6.3 Recommended role set for a residential deployment

Integrator Admin	Created at Level 1. Full permissions across the system. Held by the deployment integrator during commissioning; credentials handed to the owner at handover.
Building Manager	Created at Level 1 or building level. Device management, action profiles, alert confirmation, reports. No project deletion.
Concierge Desk	Created at the level matching the monitoring scope. View devices and alerts; operate controller OPEN/CLOSE only under authorization. No configuration permissions.
Auditor / Read-only	View-only role for strata council or insurers: dashboards, alert history, reports.

7. Register Devices

Three registration paths exist. For a building-scale rollout, use **Excel import** or **Safehous app import** — manual entry is a fallback only.

RECOMMENDED A · Excel import

1. Click **Import** → in the popup, click **Download** to get the template.
2. Fill the sheet — one row per device, with its project path. Projects that don't exist yet are auto-created.
3. Upload the sheet and click **Confirm**.

RECOMMENDED B · Safehous app import (Inventory)

1. Click **Inventory** → click the **YoLink** button (the console retains the licensor's label).
2. Log in to the site's Safehous device account on the authorization page; Raedius pulls that account's device list into inventory.
3. Find each device, click **Bind**, select its project, and click **Bind** to confirm.

Inventory devices are inactive: no data is recorded and they don't consume project device quota until bound. Note that QR-code export (Section 7.1) is not supported for devices imported this way.

FALLBACK C · Manual addition

Click **Device**, select the project, enter the device name and its full **32-digit SN code** (obtained by scanning the QR code on the back of the device), then click **Create**.

7.1 Device housekeeping operations

Edit a device	Operation → Edit → change name/details → Update. A device's project cannot be changed here — use Migration.
Migrate a device	Select device(s) → Migration button → choose the new project → Confirm. Warning: migration can break device groupings and action configurations that referenced the device.
Delete a device	Operation → Delete → confirm. Removes the device and stops data collection.
Export history	Select device(s) → export button → choose a range (max 12 months) → Export. Use for insurance claims and incident reports.
Export QR codes	Select device(s) → export-QR button → enter a recipient email → Send. Not available for devices imported via the Safehous app.
Status colors	Table view: red = alarm state · gray = offline · black = normal. Card view: alternating card style indicates offline/alarm.

7.2 Naming devices for operations staff

Name each device so the alert alone tells staff and residents where to go: **Main Bathroom Sink** **Dishwasher 2 Rope Sensor** **Cold 1 Leak Controller**. Controllers should identify their manifold and supply (Cold 1/2, Hot 1/2).

PART 2 · DEPLOYMENT — INTEGRATOR

8. Device Grouping

Groups serve two purposes: pinning **key devices** to the sidebar for quick access, and scoping **group-level action profiles** so one trigger can act on a related set of devices (close valves, sound sirens, notify).

1. Click the **Device Group** button, fill in the group form, click **Create**.
2. In Group Details, click **Device**, select members, click **Confirm**. Remove members via the **Remove** button.
3. Attach automations under the group's **Action Profile** tab (Section 10).

i Typical groups for a residential building: **Common-Area Sensors** (concierge-handled, no resident contact), **All Controllers** per building, and a **Watch List** group for devices under investigation.

PART 2 · DEPLOYMENT — INTEGRATOR

9. Action Profiles (Automation)

Action profiles are the automation engine: **Trigger** → **Preconditions** → **Filters** → **Actions**. They exist at three levels — device (Device Details → Action Profile tab), group (Group Details → Action Profile tab), and project (Action Profile menu). Project-level profiles apply to the project and all subordinate projects.

Triggers (any one fires)

Online/Offline · Low Signal · Low Battery · **Property** · **Status Change**. Optional **Duration** (e.g. fire only if wet ≥ 5 min). Group/project profiles can scope triggers by device type or specific devices.

Actions

Message Notification (SMS / email / voice; recipients: Device Owner, Project Owner, or user list) · **Device Invocation** (e.g. close valves, in profile scope, device scope, or selected devices) · **Create Alarm** (uses a Custom Alert definition, Section 11).

Preconditions & filters

Preconditions (time/date ranges with repeat rules) must **all** pass. Filter conditions block execution if **any** matches. Use filters to suppress non-critical notifications overnight, for example.

Latching

With **LATCH** enabled, a device that fires a trigger won't fire the same trigger again until manually unlatched from the Dashboard. Prevents notification storms; requires an unlock step in daily ops (Section 19).

! Property vs. Status Change — choose deliberately. A leak sensor re-reports water every 5 minutes. A **Property** trigger fires on every report (5-minute repeat alerts — useful for escalation); a **Status Change** trigger fires once per transition (right for valve closure — you

don't want the valve command re-sent forever). The "Personalized" trigger type is deprecated; do not use it.

9.1 Reference profile: suite leak response

TRIGGER	Device type: Leak Sensor · Condition: Status Change → water detected. (Use a parallel Property-trigger profile with Duration 5 min for escalation notifications.)
PRECONDITION	None — leak response runs 24/7.
ACTION 1	Device Invocation: close valve controllers, Invocation Scope = Device Scope (same suite/level as the triggering sensor) — shuts off only the affected suite's water.
ACTION 2	Message Notification → SMS + Email → Recipient: Device Owner (the suite's contact and associated users).
ACTION 3	Message Notification → Email → Recipient: Project Owner (building management / monitoring mailbox).
LATCH	Off for notifications; consider ON for valve invocation to prevent repeated close commands. Latched devices are released from the Dashboard (Unlock).

Recipient semantics: **Device Owner** = contacts + associated users of the triggering device's own project (the suite). **Project Owner** = contacts + associated users of the direct superior projects (the building / system level). Raedius service reminders always go to the primary project's contacts.

PART 2 · DEPLOYMENT — INTEGRATOR

10. Custom Alerts & Schedules

10.1 Custom alerts

Raedius pre-defines basic alarm behaviors per device through **Device Personalization** (Device Details → Personalization). When the defaults aren't enough, define your own types under **Alert Center** → **Custom Alerts**: click **Alert**, fill in the definition, **Save**. Edit or delete via each record's **Operation** menu. Custom alert definitions are what the "Create Alarm" action in an action profile references.

10.2 Scheduler (Beta)

The Scheduler executes timed device calls — e.g. close a common-area valve every night at 23:00. Click **SCHEDULE**, set start time, optionally check **Repeats** with an end time and weekly days, then **Create**. Switch to table view to enable/disable a schedule or delete it via **Operation** → **Delete**. Settings updates and report generation from the Scheduler are planned but not yet available.

PART 2 · DEPLOYMENT — INTEGRATOR

11. Commissioning Checklist

Complete and sign off every line before handover. Test with real water on at least one sensor per suite type.

- ☐ Project hierarchy matches the approved naming plan (four-digit suites, building numbers).
- ☐ All devices bound to the correct suite project; zero devices left in Inventory unbound.
- ☐ Every device reports online (Devices table shows no gray rows).
- ☐ Device names identify their physical location (e.g. 'Main Bathroom Sink', 'Cold 1 Leak Controller').
- ☐ Water test per suite type: sensor wetted → HIGH alert appears in Raedius → valve closes → resident app notified.
- ☐ Valve OPEN/CLOSE verified from Raedius, the Safehous app, and Smart Fob for a sample suite.
- ☐ Flow tracking verified per controller: run a tap and confirm a matching flow event appears on the controller's REPORT tab.
- ☐ Action profiles fire correctly: notifications received by Device Owner and Project Owner test contacts.
- ☐ Roles created and test logins verified for each role; concierge role confirmed unable to modify settings.
- ☐ Communication package quota sufficient for projected alert volume.
- ☐ Historical data export tested; report generation verified in Report Center.
- ☐ Resident handouts (puck/rope one-pagers) delivered to every suite; spares at the desk.
- ☐ Desk shortcut and browser bookmark installed on the concierge workstation, opening to the ALERTS page.

PART 3 · HANDOVER

12. Handover to Building Management

Handover transfers day-to-day custody from the integrator to the concierge / building manager. Deliver the following, walk staff through Sections 13–18 in person, and record the handover date.

- ☐ Admin credentials transferred to the owner in a sealed envelope; integrator account downgraded or removed.
- ☐ Concierge desk account created with the Concierge role; login verified on the desk workstation.
- ☐ This guide (Sections 13–20) walked through live with desk staff, including a simulated HIGH alert.
- ☐ Escalation contact list posted at the desk (who approves controller operation, suite entry, sensor silencing).
- ☐ Commissioning checklist (Section 11) signed and archived with the strata records.
- ☐ Renewal calendar entry created for the annual licence (2-month grace buffer after expiry).

- ☐ Support agreement documented: who to call for device failures, automation issues, and configuration changes.

PART 4 · DAILY OPERATIONS — CONCIERGE

13. Opening & Logging In

1. Click the Raedius shortcut on the taskbar, or the "Raedius" bookmark in Edge/Chrome. Either opens straight to the **ALERTS** page.
2. Raedius normally stays signed in. If the login screen appears, enter the desk credentials, tick **Remember me**, and click **Sign In**.

USERNAME
<desk account name>

PASSWORD
<see credential envelope at desk>

! Desk credentials are held by the Strata President. Do not write them into memos, emails, or shared documents.

13.1 Workstation setup — keep Raedius always visible

1. Drag the Raedius window to one edge of the monitor until the translucent snap outline appears, then release — Raedius fills half the screen.
2. Click any other program in the previews that appear to snap it to the other half.
3. Drag the divider between the windows to size them. Keep the Raedius half wide enough that the **Project** column stays visible.
4. Stack additional apps on the non-Raedius side so Raedius is never covered.

i Raedius columns do not reflow when the window is resized — **refresh the page after any resize** so the layout adjusts. To read every column during an incident, pop the window to full screen, reload, read, then snap it back.

PART 4 · DAILY OPERATIONS — CONCIERGE

14. The Alerts Page

ALERTS is the page staff live on. The icon list on the top-left of every page reaches it; the arrow at the bottom-left expands the icons into a labelled menu. When a new alert arrives, an orange box appears top-right with a pending count — **refresh the page** rather than clicking its "Details" button. Raedius uses a 24-hour clock.

HIGH
Water detected
Repeats every ~5 minutes until the sensor is removed, unplugged, or dried. Monitor closely.

MEDIUM
Sensor removed / unplugged
Usually cleaning or drying. Monitor; no immediate action.

LOW
Sensor reinstalled / plugged in
Confirmation that a device was put back. No action.

14.1 The healthy resolution pattern

HIGH · 17:01 water detected



MEDIUM · 17:07 sensor removed



This progression with no further alarms means the resident handled it — no intervention needed. The opposite pattern — HIGH alerts repeating every 5 minutes with no MEDIUM following — means nobody is responding.

14.2 Response procedure for HIGH alerts

1

Refresh and read the alert

Note the suite, device name, and time. Raedius uses a 24-hour clock. Check whether this is the first alert or a repeat — repeats arrive every 5 minutes while the sensor stays wet.

2

Give the resident time to respond

Most events are splashes the resident handles within minutes. Watch for the MEDIUM (sensor removed) alert that signals someone is dealing with it.

3

Contact the resident after ~3 unanswered alarms

Three repeats ≈ fifteen minutes of beeping. Text or call the resident — they may not be home, or may need help.

4

Escalate

Message the Strata President and decide together whether physical intervention is required (e.g. entering the suite if the resident is unreachable). Follow the entry policy in Section 17.

14.3 Common alerts and their causes

WATER DETECTED — laundry rope sensor

Often wet laundry dripping near the machine front — but the braided fill/drain hoses behind the machine can also leak seriously. Always follow up.

WATER DETECTED — kitchen / dish area

Usually splashed water from wet dishes; can also be a genuine leak. Follow up.

Sensor removed / unplugged (MEDIUM)

After a WATER DETECTED alert: normal drying, may stay unplugged for hours. Without a preceding HIGH: likely cleaning — monitor and report if it never comes back.

Sensor plugged in (LOW)

A device was reinstalled. If there's no earlier alert explaining why, check the device's alert history via Devices → Options → Details → Alerts.

Repeat HIGH shortly after LOW

The sensor or rope was reinstalled before it fully dried. Contact the resident and explain drying best practice if it recurs.

Battery low

Sensors and fobs use AAA batteries (~5-year life). Residents supply and replace their own batteries; the alert also reaches their Safehous app.



Acknowledge buttons: alerts can be confirmed with an optional remark once resolved (Alert Center → click record → Confirm). Follow your site's current policy on who acknowledges — if none has been issued, leave acknowledgements alone.

15. The Devices Screen

Open it from the icon list (the icon resembling a Wi-Fi router). Use it for two things only: **checking status** of a suite's devices (online, pending alerts, water OPEN/CLOSED) and — with authorization — **operating controllers or silencing sensors**.

15.1 Searching a suite

BUILDING#.SUITE# → 1515.0101 (4-digit suite, no spaces, press Enter)

- Suite numbers are **always four digits**: suite 101 is entered 0101. Searching 1515.101 returns an error.
- Searching a bare number (e.g. 101) matches every suite containing it across all buildings — always enter the full form.
- Rows highlighted **pink** have unacknowledged pending alerts.
- Pagination defaults to 25 rows (max 100) — check the "1–24 of 24" counter bottom-right so you don't miss devices on a second page. The same pagination pattern appears throughout Raedius.

15.2 Reading a suite listing

Controllers

Listed first — e.g. Cold 1, Cold 2, Hot 1, Hot 2 (two manifolds × hot/cold). State column: OPEN = water on, CLOSED = water off (typical when a resident travels).

Smart Fob

The suite's one-button wireless water on/off fob.

Sensors

Every puck and rope sensor, named by location. Pink highlight = unacknowledged alerts pending on that device.

15.3 Operating a controller (authorized staff only)

Find the controller → **Options** → **Details** → **Settings**. Click **OPEN** to turn water on, **CLOSE** to turn it off. The **Alerts** tab on the same screen shows the device's full alert history.

✗ **DETAILS is the only Options entry staff should use.** Any action beyond viewing — opening/closing valves, changing settings, disabling devices — requires prior approval from the Strata President. Never modify devices on your own initiative.

15.4 Silencing a malfunctioning sensor

Only after speaking with the Strata President: find the sensor → **Options** → **Details** → **Settings** → toggle **Enable** off. Think of Enable as a *silence* switch — it stops the device sending and receiving updates.

! The **Enable toggle does not control water**. Never use it on a CONTROLLER — controllers are operated only with OPEN / CLOSE.

If a resident asks for help turning water on or off, coach them to do it themselves via the Safehous app or their Smart Fob — operate the controller from the desk only during an active water emergency.

When a resident calls about a "Water Detected" notification, walk them through the steps below. Printed copies of both one-pagers are kept at the desk for handout.

Puck sensor — toilets & sinks

1. Find the sensor named in the app notification.
2. Lift the sensor off its cradle — the arrows align, they do not click together.
3. Wipe the sensor's underside and the affected area dry.
4. Check for a genuine leak; report any leak to the concierge.
5. If it was just splash, place the sensor back with the arrows aligned.

Rope sensor — laundry, dishwasher, freezer, shutoffs

1. Find the sensor (white square device) named in the notification.
2. Hold the sensor with one hand and pull the rope plug out with the other. The beeping stops.
3. Set the sensor somewhere dry; leave the rope to air-dry — this can take several hours.
4. Check for a genuine leak; report any leak to the concierge.
5. Only when fully dry, plug the rope back in and replace the sensor. Plugging in a damp rope re-triggers WATER DETECTED.

Turning water back on: once the sensor is removed and any leak resolved, residents restore water via the toggle on each valve in the Safehaus app, or by pressing the top "Home" button on their white fob.

16.1 Printable resident one-pagers

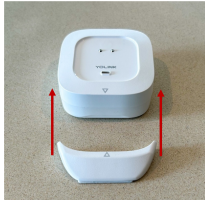
YOLINK SAYS "WATER DETECTED" – WHAT DO I DO?

The YoLink App will notify you of the location of a leak (IE: "Main Bathroom Sink", "Laundry", "Heat Pump", etc.)

PUCK SENSORS can be found near/underneath: **TOILETS and SINKS** (bathrooms, laundry, kitchen, etc.)

Once you find the affected device, remove the sensor from its "cradle."

NOTE: CHECK FOR LEAKS AND REPORT ANY TO THE CONCIERGE

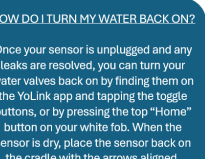
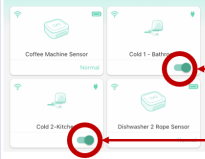


Remove the sensor from the cradle (NOTE: the cradle and sensor rest against one another with the arrows aligned – they do not "click" together)

Once the sensor is removed, wipe off its underside as well as the affected area. If the water was NOT from a leak, you can place the sensor back.

HOW DO I TURN MY WATER BACK ON?

Once your sensor is unplugged and any leaks are resolved, you can turn your water valves back on by finding them on the YoLink app and tapping the toggle buttons, or by pressing the top "Home" button on your white fob. When the sensor is dry, place the sensor back on the cradle with the arrows aligned.



Puck sensor handout

YOLINK SAYS "WATER DETECTED" – WHAT DO I DO?

The YoLink App will notify you of the location of a leak (IE: "Main Bathroom Sink", "Laundry", "Heat Pump", etc.)

ROPE SENSORS can be found near/underneath: **laundry machines, dishwashers, freezers and water shutoffs.**

Once you find the affected device, remove the sensor and **UNPLUG THE "ROPE"**

*** NOTE: CHECK FOR LEAKS AND REPORT ANY TO THE CONCIERGE ***

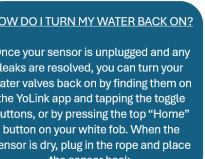
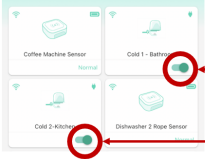


Grab the sensor (white, square-like device) with one hand, and pull out the rope with your other hand.

Once the rope is removed, place the sensor somewhere dry, and leave the rope to air dry (may take several hours)

HOW DO I TURN MY WATER BACK ON?

Once your sensor is unplugged and any leaks are resolved, you can turn your water valves back on by finding them on the YoLink app and tapping the toggle buttons, or by pressing the top "Home" button on your white fob. When the sensor is dry, plug in the rope and place the sensor back.



Rope sensor handout

PART 4 · DAILY OPERATIONS — CONCIERGE

17. Privacy & Intervention Policy

Sensors and controllers sit inside private homes. Raedius exists to mitigate water intrusion — not to observe what happens in a suite. Residents are responsible for their own suites and equipment; support and encourage self-service.

- Do not over-contact residents, especially for LOW and MEDIUM alerts.
- Resident information is always private — including between residents ("is the water from the suite above?") and in daily memos.
- Prolonged HIGH alerts are the priority: leaks travel into neighbouring suites and common property, and sensors don't cover walls, ceilings, or pipe runs.
- If a resident is clearly struggling (e.g. re-plugging a rope too early), wait for them to ask, then explain best practice.

17.1 Entering a suite

1. Contact the Strata President first for assistance or accompaniment — **before responding to any alert**.
2. Unescorted entry is for emergencies only, after all other options are exhausted, or when directed by the Strata President.
3. Document every entry for future reference.

PART 5 • MAINTENANCE

18. Safehaus Leak Controller: Functions & Settings

Every Safehaus Leak Controller (type `LEAK_CONTROLLER · YS5005-UC`) meters the water passing through it and exposes its full function set on its detail page: **Devices** → **Options** → **Details**. The header shows the device name, project path, type, online status, device EUI, and firmware; the large readout is the live valve state and water temperature (e.g. **OPEN / 18.7°C**) with a last-updated timestamp. Eight tabs sit below it.

18.1 The tab bar

REPORT

Flow statistics and history — daily, weekly, or monthly (18.3).

CHARTS

Time-series graphs of the values the device reports (temperature, signal, battery).

PERSONALITY

The built-in alarm conditions — which raise alerts, which latch the device (18.5).

ACTION PROFILES

Device-level automations scoped to this controller (Section 9).

ALERTS

This controller's full alert history with acknowledgement records (18.6).

SETTINGS

Operating configuration — protection mode, sensitivity, usage limits, freeze protection, schedules (18.7).

D2D

Device-to-device pairings that keep working even if the network drops. View only — changes belong to the integrator.

ACTIVITIES

Timestamped log of every state report from the device (18.8).

18.2 Control buttons

OPEN / CLOSE

Operates the valve — water on / water off. Same authorization rules as Section 15.3: emergencies aside, coach residents to use their app or fob.

CALIBRATE

Re-zeroes the controller's flow sensing. Use only when flow tracking is demonstrably wrong (Section 18.4) or after

RESET ALARM

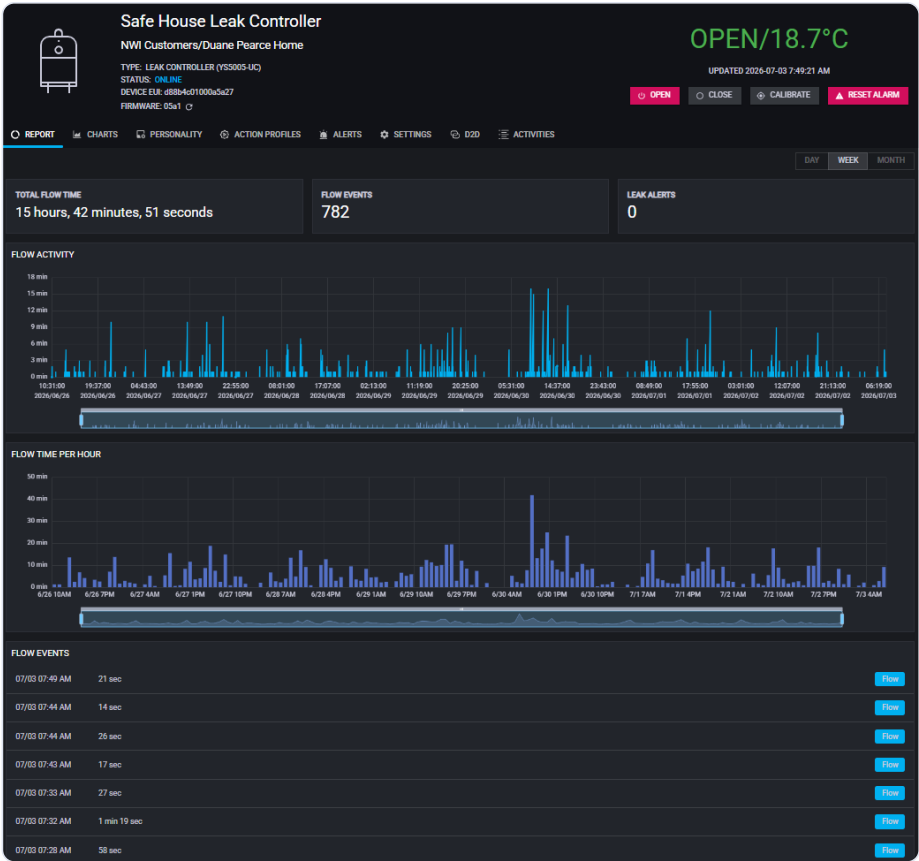
Clears the controller's alarm state after a leak is fully resolved. Confirm the affected area and sensors are dry before resetting.

physical service to the controller.

! Viewing any tab requires no approval — check freely. Changing anything does: CALIBRATE, RESET ALARM, Personality checkboxes, and every Settings change require prior approval from the Strata President (Section 15.3 rules).

18.3 REPORT tab — flow statistics

Flow activity can be viewed **daily, weekly, or monthly** per controller — the primary tool for verifying the sensor is tracking flow correctly and for spotting abnormal or excessive usage.



REPORT tab — WEEK view

DAY / WEEK / MONTH

Toggle (top-right) that sets the reporting window for every tile and chart below. Use DAY for incident review, WEEK for routine checks, MONTH for baseline comparison.

Total Flow Time

Cumulative time water flowed through the controller in the selected window (e.g. 15 h 42 m over a week).

Flow Events

Count of distinct flow occurrences — every tap run, toilet flush, or appliance cycle registers as an event.

Leak Alerts

Number of leak alarms raised by this controller in the window. Should normally read 0; cross-check any count against the Alerts page.

Flow Activity chart

Each bar is one flow event, plotted by time with its duration on the vertical axis. Long or clustered bars at unusual hours stand out immediately.

Flow Time Per Hour

Total minutes of flow in each hour. A healthy suite shows quiet overnight hours; flow in every hour around the clock suggests a running fixture.

Flow Events log

Timestamped list of every event with its duration (e.g. 07:44 AM — 26 sec). Use it to match a reported incident to exact times.

18.4 Using flow data for troubleshooting

- Verify the controller is tracking flow**

With the resident's cooperation, run a tap in the suite for about one minute, then refresh the REPORT tab. A matching flow event (~1 min) should appear in the log. No event while water is clearly running = flow sensing fault — calibrate (with approval) or escalate to the integrator.
- Spot abnormal or excessive usage**

Flow events in every hour — including overnight — usually mean a running toilet, dripping fixture, or slow leak. The Flow Time Per Hour chart makes this obvious at a glance. Contact the resident before it becomes a damage claim.
- Compare against baseline**

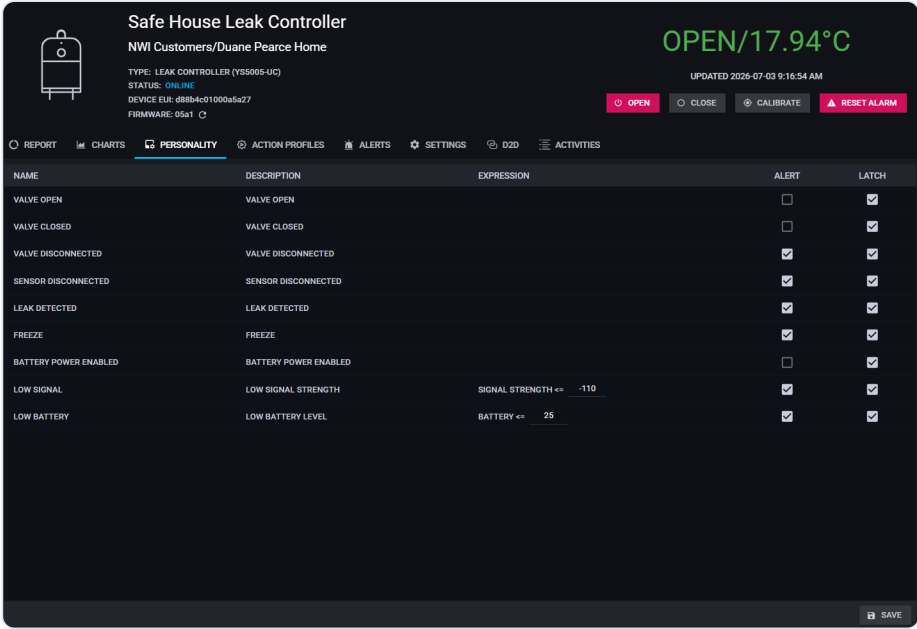
Switch between WEEK and MONTH views to learn a suite's normal Total Flow Time and event count. A sudden jump with no lifestyle explanation warrants a closer look.
- Check vacant suites**

A suite whose water is left ON while the resident travels should show zero flow events. Any activity in an unoccupied suite is a red flag — investigate and escalate.
- Reconcile leak alerts**

The Leak Alerts tile counts alarms raised by this controller in the window. Confirm each one has a corresponding, resolved entry in the Alerts page history before clearing alarm states.

18.5 PERSONALITY tab — built-in alarm conditions

This is the controller's copy of Device Personalization (Section 10.1): the pre-defined conditions the device watches for, and what each one does when it fires.



PERSONALITY tab — condition list with ALERT and LATCH checkboxes

Conditions list

VALVE OPEN · VALVE CLOSED · VALVE DISCONNECTED · SENSOR DISCONNECTED · LEAK DETECTED · FREEZE · BATTERY POWER ENABLED · LOW SIGNAL · LOW BATTERY. These are the controller's pre-defined alarm behaviors.

EXPRESSION

Threshold for measured conditions, editable inline — e.g. LOW SIGNAL fires at signal strength ≤ -110, LOW BATTERY at

battery ≤ 25.

ALERT checkbox

Ticked = the condition raises an alert on the Alerts page.
Routine states (VALVE OPEN, VALVE CLOSED, BATTERY POWER ENABLED) ship unticked so normal operation stays quiet — leave them that way unless investigating a specific problem.

LATCH checkbox

Ticked = the condition locks the device when it fires; it will not re-trigger until manually unlocked from the Dashboard (Section 19).

Saving changes

Tick/untick boxes or edit a threshold, then click SAVE at the bottom-right — nothing applies until saved. Changes require approval from the Strata President.

18.6 ALERTS tab — this controller's alert history



Safe House Leak Controller

NWI Customers/Duane Pearce Home

TYPE: LEAK CONTROLLER (Y33005-UC)

STATUS: ONLINE

DEVICE EUR: d8854cd1000a6a27

FIRMWARE: 05a1

OPEN/17.94°C

UPDATED 2025-07-03 9:16:54 AM

OPEN CLOSE CALIBRATE RESET ALARM

REPORTCHARTSPERSONALITYACTION PROFILESALERTSSETTINGSD2DACTIVITIES

ALERT NAME

SEARCH

CLEAR ALERTS

NAME	LEVEL	REMARKS	CREATED TIME	COMPLETE ACCOUNT	COMPLETE TIME	OPERATIONS
☐ LEAK DETECTED	HIGH		2025-06-25 12:24:38 AM	nwlicustomers	2025-06-25 5:33:45 AM	ACKNOWLEDGED
☐ LOW BATTERY	HIGH		2024-12-23 10:13:31 PM	nwlicustomers	2025-06-24 7:33:23 PM	ACKNOWLEDGED
☐ VALVE DISCONNECTED	HIGH		2024-12-18 9:57:55 PM	nwlicustomers	2025-06-24 7:33:23 PM	ACKNOWLEDGED
☐ VALVE DISCONNECTED	HIGH	test alarms	2024-12-14 11:54:28 AM	nwlicustomers	2024-12-18 3:53:29 PM	ACKNOWLEDGED
☐ LEAK DETECTED	HIGH	test alarms	2024-12-14 11:49:22 AM	nwlicustomers	2024-12-18 3:53:29 PM	ACKNOWLEDGED

ROWS PER PAGE: 251 of 5

ALERTS tab — history with acknowledgement account and time

Search

Filter by alert name and/or a date range, then click SEARCH.
Standard pagination applies (default 25 rows).

Columns

Name · level (leak-related conditions report HIGH) · remarks · created time · completing account · completion time.

ACKNOWLEDGED

Green = confirmed by a staff account; Raedius records who acknowledged and when. Acknowledge resolved alerts per your site's policy, adding a remark where useful.

CLEAR ALERTS

Bulk-removes selected alert records — this deletes history used for incident review. Use only with approval from the Strata President.

18.7 SETTINGS tab — operating configuration

Settings are grouped into collapsible panels. Adjust values within a panel, then click that panel's **SAVE / SAVE PROPERTIES** button — changes do not apply until saved.

Safe House Leak Controller
NWI Customers/Duane Pearce Home
TYPE: LEAK CONTROLLER (Y5005-UC)
STATUS: ONLINE
SERVICE EUI: c88a4cd01000a3a27
FIRMWARE: 02a1

UPDATED 2025-07-03 9:18:45 AM

OPEN CLOSE CALIBRATE RESET ALARM

REPORT CHARTS PERSONALITY ACTION PROFILES ALERTS **SETTINGS** D2D ACTIVITIES

GENERAL

ENABLE ☒

TIMEZONE (GMT-07:00 America/Vancouver) SYNC TIMEZONE

PROPERTIES

COLD/HOT WATER: COLD

LEAK PROTECTION MODE: LEAK SCHEDULE

SENSITIVITY: 5

Shut off valve when frozen: DISABLE

Set sensitivity on APP: ENABLE

MAXIMUM CONTINUOUS WATER USAGE DURATION

ENABLE ☒

LEAK DURATION BEFORE ALARM: 120 MIN

CLOSE VALVE: DISABLE

DRY PIPE AND FREEZE PROTECTION

DRY PIPE DEGREES: 230°F

FREEZE TEMPERATURE: 39.9°F

SAVE PROPERTIES

VALVE SCHEDULE

LEAK SCHEDULE

START TIME	END TIME	LEAK DURATION BEFORE ALARM	CLOSE VALVE	REPEAT	ENABLE	DISABLE	EDIT	DELETE
12:00 AM	11:59 PM	60 MIN	DISABLE	SUN, MON, TUES, WED, THUR, FRI, SAT	ENABLE	DISABLE	EDIT	DELETE

CREATE LEAK SCHEDULE

LEAK SCHEDULE (AWAY)

SETTINGS tab — properties, usage-duration guard, freeze protection, and leak schedules

GENERAL

ENABLE toggle (the device silence switch — see warning below) and TIMEZONE with a SYNC TIMEZONE button. Keep the timezone correct, or every schedule below runs at the wrong hour.

PROPERTIES

COLD/HOT WATER designation · LEAK PROTECTION MODE (how the controller decides to act, e.g. LEAK SCHEDULE) · SENSITIVITY stepper (higher flags smaller flows; set too high it produces false leak alarms) · SHUT OFF VALVE WHEN FROZEN enable/disable · SET SENSITIVITY ON APP (lets the resident adjust sensitivity from the Safehous app). Click SAVE PROPERTIES after changes.

MAXIMUM CONTINUOUS WATER USAGE DURATION

The 'water running too long' guard. Enable it, set LEAK DURATION BEFORE ALARM (e.g. 120 minutes of continuous flow), and choose whether CLOSE VALVE fires automatically or the event only raises an alarm.

DRY PIPE & FREEZE PROTECTION

Two temperature sliders: DRY PIPE DEGREES (over-temperature threshold, e.g. 230°F) and FREEZE TEMPERATURE (e.g. 39.9°F — below this the FREEZE condition fires, and the valve closes if shut-off-when-frozen is enabled).

VALVE SCHEDULE

Timed valve OPEN/CLOSE local to this controller — same idea as the Project Scheduler (Section 10.2).

LEAK SCHEDULE / LEAK SCHEDULE (AWAY)

Time-windowed leak rules: start/end time, LEAK DURATION BEFORE ALARM (e.g. 60 min), CLOSE VALVE on/off, and repeat days. Create with CREATE LEAK SCHEDULE; manage with ENABLE / DISABLE / EDIT / DELETE. The AWAY variant applies stricter rules while the suite is unoccupied — typically a shorter duration with automatic valve closure.

! The GENERAL panel's **ENABLE toggle is the silence switch** (Section 15.4) — it stops the device sending/receiving updates. It does not control water, and disabling a controller removes the suite's leak protection. Approval required, always.

18.8 ACTIVITIES tab — the device's diary



Safe House Leak Controller

NWI Customers/Duane Pearce Home

TYPE: LEAK CONTROLLER (Y5005-UC)

STATUS: ONLINE

DEVICE EUI: c8b8-4a2f1000a5a27

FIRMWARE: 05a1

OPEN/18.13°C

UPDATED 2025-07-03 9:18:45 AM

OPEN

CLOSE

CALIBRATE

RESET ALARM

REPORT

CHARTS

PERSONALITY

ACTION PROFILES

ALERTS

SETTINGS

D2D

ACTIVITIES

DESCRIPTION

2025-07-04 00:00:00 - 2026-07-03 23:59:59

SEARCH

DATE	ACTIVITY
2026-06-09 9:53:45 PM	clear alarms
2026-05-28 12:56:51 PM	valve status: open, temperature: 60.3°F(15.72°C), leak detected, maximum water usage duration alarm
2026-05-19 12:44:27 PM	clear alarms
2026-05-16 8:22:58 AM	valve status: open, temperature: 53.9°F(12.18°C), leak detected, maximum water usage duration alarm
2026-05-16 6:22:52 AM	valve status: open
2026-05-16 6:22:41 AM	clear alarms
2026-05-16 12:00:20 AM	valve status: close, temperature: 52.3°F(11.20°C), leak detected, maximum water usage duration alarm
2026-05-15 7:02:32 PM	valve status: open, temperature: 52.1°F(11.19°C), leak detected, maximum water usage duration alarm
2026-05-11 9:00:08 AM	valve status: open, temperature: 52.6°F(11.47°C), leak detected
2026-05-08 7:50:01 PM	valve status: open
2026-05-08 7:49:50 PM	valve status: close
2026-02-11 6:10:47 AM	clear alarms
2026-01-23 8:09:33 PM	valve status: open, leak detected, maximum water usage duration alarm
2026-01-22 5:55:15 AM	clear alarms
2026-01-08 5:21:10 PM	valve status: open, leak detected, maximum water usage duration alarm
2026-01-08 3:20:39 PM	valve status: open, temperature: 54.1°F(12.28°C)
2025-12-29 8:59:28 PM	online
2025-12-29 8:22:25 PM	offline
2025-12-02 1:39:37 PM	valve status: open, leak detected, maximum water usage duration alarm
2025-11-25 11:09:34 PM	clear alarms
2025-11-25 11:08:24 PM	valve status: open, leak detected, maximum water usage duration alarm
2025-11-25 11:08:19 PM	valve status: open, leak detected, valve/sensor disconnected, maximum water usage duration alarm
2025-11-25 4:55:32 PM	valve status: open, leak detected, maximum water usage duration alarm
2025-11-25 4:55:10 PM	valve status: open, leak detected, valve/sensor disconnected, maximum water usage duration alarm
2025-11-25 4:55:01 PM	valve status: open, leak detected, maximum water usage duration alarm

ROWS PER PAGE: 25

1-25 OF 204

ACTIVITIES tab — timestamped device log

What's logged

Every report from the device: valve status (open/close), temperature readings, leak detected, maximum-water-usage-duration alarms, clear-alarms actions, and online/offline transitions.

Search

Filter by description keyword and a date range, then SEARCH. Logs run to hundreds of rows — narrow the date range first, and mind the pagination counter.

When to use it

Building a minute-by-minute incident timeline; confirming exactly when a valve closed or an alarm cleared; spotting repeated offline/online cycles that suggest a power or connectivity problem.

PART 5 • MAINTENANCE

19. Routine Maintenance

Daily — Dashboard sweep

Check online/offline counts, current alarms, and locked devices. Investigate any gray (offline) devices — usually a battery or hub issue.

Per incident — Confirm alarms	Once a device's alarm state is genuinely resolved, clear it: Dashboard → Confirm Alarm (or Alert Center → record → Confirm, with an optional remark).
Per incident — Unlock devices	Devices latched by personalization or an action profile stay locked until manually unlocked from the Dashboard. A locked device will not re-trigger the same condition — unlock promptly after resolution.
Monthly — Reports	Generate an activity report from Report Center; export device history (up to 12 months) for any suite with recurring events.
Every ~5 years — Batteries	Sensors and fobs run on resident-supplied AAA batteries. Battery-low alerts reach both Raedius and the resident's app; chase suites that ignore them.
Annually — Licence renewal	\$300 base + \$5/device/year. A 2-month grace buffer applies after expiry; renew before it lapses. Top up the Communication Package if SMS/voice quota ran short.

PART 5 · MAINTENANCE

20. Troubleshooting

Columns are cut off / layout looks wrong

Raadius doesn't reflow on window resize. Refresh the page after resizing; for a full read, maximize the window, reload, then snap it back into split screen.

Suite search returns an error

Use the exact format BUILDING#.SUITE# with a four-digit suite: 1515.0101, not 1515.101. No spaces.

Search shows devices from many suites

You searched a bare number. Any suite containing that number matches (101 → 0101, 1101, 2101 ...). Enter the full building.suite form.

Devices seem to be missing from a suite

Check the pagination counter bottom-right. Default is 25 rows per page — click the arrows or raise 'Rows per page' (max 100).

Sensor keeps re-arming after cleanup

The rope or sensor was reinstalled damp. Unplug again and allow several hours of air-drying before reinstalling.

A sensor is malfunctioning (false alarms)

With approval from the Strata President only: Devices → Options → Details → Settings → toggle Enable off to silence it. Never use Enable on a controller.

An automation/action profile stopped firing for a device

The device is probably latched. Check the Dashboard's locked devices and unlock it. Latching is per-profile — other profiles still run.

Notifications (SMS/voice) stopped sending

Communication package quota may be exhausted — check with the account owner and purchase a top-up package.

Controller doesn't seem to be tracking flow

Open the controller's REPORT tab (Section 18), run a tap in the suite for about a minute, and watch for a matching flow event. If nothing registers, the flow sensing is faulty — CALIBRATE only with approval from the Strata President, or escalate to the integrator.

Flow report shows abnormal or excessive usage

Frequent flow events around the clock — especially overnight — usually mean a running toilet, dripping fixture, or slow leak. Compare the WEEK and MONTH views against the suite's normal baseline, then contact the resident.

Frequent false leak alarms from one controller

Sensitivity may be set too high, or a leak schedule's duration too short. Review Settings → PROPERTIES (sensitivity stepper) and the LEAK SCHEDULE panels (Section 18.7); adjust and SAVE PROPERTIES only with approval from the Strata President.

'Maximum water usage duration' alarms during normal use

The continuous-usage guard's LEAK DURATION BEFORE ALARM is shorter than the household's real usage (long showers, irrigation). Raise the duration in Settings → MAXIMUM CONTINUOUS WATER USAGE DURATION — with approval — rather than disabling the guard.

Controller stuck in alarm after a leak is resolved

Confirm the affected area and sensors are dry, then use RESET ALARM on the controller's detail page — with approval from the Strata President.

Device shows offline (gray)

Check its battery, then the suite's hub power/connection. If it stays offline, open Device Details → Activities to see when it dropped and escalate to the integrator.

Still stuck?

Escalate to the Strata President · Integrator support per your service agreement · System description & training: www.safehous.com/chubb-training