



YOUR PRODUCT. YOUR GUIDE.

Smart Home Device Manual

Install, connect, control, and recover your device

5 PAGES / FILLABLE FIELDS / COMPLIANCE REVIEW



Make this document yours

Product / system name

Name used on the product or release

Model / version / configuration

Exact models and versions covered

Document ID and revision

Controlled reference and revision number

Issue date and market

Date, language and countries covered

Responsible manufacturer / organization

Your organization's legal name and address

Author and support contact

Document owner, support email / phone / URL

Inside this template

- 02 Identify the device and prerequisites
- 03 Install and connect the device
- 04 Use automations and manage privacy
- 05 Smart device safety and compliance review

Authoring draft: fill the labeled fields, replace bracketed prompts, and add verified procedures and diagrams. Complete product and market review before release. This template does not certify a product.

CHECK MODEL, APP, AND ECOSYSTEM

Identify the device and prerequisites

Connected devices depend on hardware, app, network, region, and cloud availability. State the supported combinations and explain how to locate device identifiers.

Document control and owner**Responsible manufacturer or organization**

[Legal name], [address], [support phone], [support email or website]

Device and covered variants

[Product name], [model], [region / radio / hardware version]

Guide revision

[Document ID], [revision], [issue date], [language]

Audience and markets

[Intended user / installer], [countries or regions]

Required environment

List supported app versions, mobile operating systems, network bands or topology, account types, hubs, ecosystems, and subscription needs from the released compatibility matrix. Explain how to find the firmware version and device ID without exposing credentials or private setup codes.

Prepare for pairing

- ☐ Install the app from the approved distribution channel.
- ☐ Confirm the phone, network, and hub meet this model's requirements.
- ☐ Use a private network and account intended for the device owner.
- ☐ Keep setup codes and account recovery details away from public view.
- ☐ Place the device where its documented radio and sensor conditions are met.

Template status

Manual Tools by Manuals+ publishes this template at <https://manual.tools>. It is not verified smart home instructions. The responsible organization must validate pairing, ecosystem support, security, privacy, hazards, and regional claims.

SET UP A TRUSTED CONNECTION

Install and connect the device

Separate physical installation from app enrollment. Explain required permissions and data sharing at the moment they matter, and identify installer-only work.

Placement and mounting

Provide verified mounting direction, surface, clearance, environmental limits, sensor orientation, and utility conditions. Name work that requires a qualified installer. Explain how physical placement affects signal, sensing, or coverage using tested guidance. Never publish guessed range or load values.

Enrollment sequence

1. Power or install the device using the model-specific instructions.
2. Open the approved app and sign in to the intended household or workspace.
3. Start adding a device and select the exact model or scan its approved setup code.
4. Grant only the permissions required for the stated feature and account role.
5. Wait for a verified connected state, then test the intended local control.

If enrollment fails

Tell the user how to check the device's status indicator, app version, network selection, and account ownership. Specify any reset action and what it erases before asking the user to reset. Provide a direct support route when ownership, access, or repeated pairing failure blocks setup.

Connection support record**App and firmware versions**

[Version numbers and supported range]

Network and ecosystem requirements

[Verified requirements and source]

Device ID location

[Label or app path; redact secret pairing codes]

UNDERSTAND WHAT CONNECTED ACTIONS DO

Use automations and manage privacy

Explain device controls, automation triggers, and failure behavior. Make the physical product's local behavior clear when network, power, or cloud service is unavailable.

Create a simple automation

1. Choose the device, trigger, and action supported by this release.
2. Review timing, household scope, and any people or device data involved.
3. Set a clear manual override or stop action where the product supports it.
4. Save and test the automation while observing the physical device.
5. Disable it and use the documented recovery path if behavior is unexpected.

Privacy and account ownership

Describe what device and household data the feature collects or sends, when it is shared, and how the user changes available controls. Link to the current privacy notice and explain account transfer, household removal, and deletion behavior only as implemented. Do not say data is local or encrypted unless the product team has verified that claim.

Operating state map

State	What the user can observe	Safe next action
Connected	[Verified indication]	[Action]
Network unavailable	[Local behavior]	[Action]
Power interrupted	[Physical behavior]	[Action]
Account access lost	[Observed state]	[Recovery route]

Secure everyday use

- ☐ Use unique account credentials and approved recovery options.
- ☐ Review household members and remove access when no longer needed.
- ☐ Install updates through the supported channel.
- ☐ Avoid sharing setup codes or screenshots that expose them.

CONNECTED-PRODUCT RELEASE REVIEW

Smart device safety and compliance review

Connected products can combine installation, radio, privacy, cybersecurity, safety, and lifecycle obligations. Determine what applies to each market and keep the proof with the release record.

Safe connected behavior

Document what the physical device does during loss of power, network, cloud service, account access, or update. Add product-specific warnings for locks, alarms, heating, access control, or other consequential functions where applicable. Explain local override and emergency access using verified behavior.

Product-specific compliance author prompts

- ☐ Identify applicable radio, electrical, product safety, privacy, cybersecurity, consumer, labeling, language, and disposal requirements by market.
- ☐ Insert verified radio IDs, warnings, security support period, privacy notices, and regional declarations where required.
- ☐ List RF, security, privacy, safety, usability, and software release evidence by controlled file ID.
- ☐ Route review to qualified product safety, security, privacy, legal, and market owners.

Evidence and sign-off**Responsible organization and support contact**

[Legal name, address, support phone, support email or website]

Markets, models, and guide revision

[Markets], [device / app variants], [document ID], [revision / date]

Evidence and approved notices

[Evidence IDs, notice / label / declaration references]

Review record

[Reviewer, role, date, decision, approval record]

Publication decision

The template from Manual Tools by Manuals+ at <https://manual.tools> is not a product assessment or compliance proof. The responsible organization must verify physical and connected behavior and approve all market statements.

Official reference starting points - applicability must be determined for your product and market.

European Commission: GDPR applicability

Your Europe: electrical waste (WEEE)