Ecosystems - Privacy and Data Protection Policy

Published date: 26 October 2026
Effective date: 26 October 2026
Version: 1.4

This Privacy Policy explains how the baseworks.tech Ecosystem software handles information. It covers the software that runs on the Compute, the Control Website, the Root Network and apps licensed and deployed as part of a baseworks.tech Ecosystem, as well as the baseworks.tech update and licensing service that any Ecosystem uses. The baseworks.tech Ecosystem is a product of baseworks.tech.

baseworks.tech is the controller of the personal data it processes for its own purposes, as described in this Policy. Information that the Ecosystem stores and processes locally on your hardware remains under your control, as explained in Section 4. Certain providers, such as Home Assistant integrations, device manufacturers and internet services, may act as separate controllers where they independently determine the purposes and means of particular processing. Their own privacy notices govern that processing.

The current version of this policy and other company policies will be available from the baseworks.tech policies page: https://www.baseworks.tech/policies/.

Table of contents:

Section 1: Identity and contact details of the data controller 2
Section 2: Scope 2
Section 3: Summary 3
Section 4: Who controls which information 3
Section 5: Information stored on the Ecosystem 4
5.1 Preparation before delivery 4
5.2 Data stored by the ecosystem 4
Section 6: Information the Ecosystem does not collect 4
Section 7: Update and licensing service 5
Section 8: Internet connectivity checks and other external services 6
Section 9: Home Assistant, sensors and connected devices 7
Section 10: Wi-Fi access point, internet uplink and local network 7
Section 11: Control website sessions and browser storage 8
Section 12: Logs and diagnostics 8
Section 13: Support and correspondence 8
Section 14: Exports, resets and returned hardware 9
Section 15: Retention and deletion 9

baseworks.tech

Section 16: Children 9
Section 17: Your data-protection rights 9
Section 18: Security 10
Section 19: International data transfers 11
Section 20: Changes to this policy 11
Section 21: Governing language 11
Section 22: Contact 11

Section 1: Identity and contact details of the data controller

The data controller (also referred to as the "company") responsible for processing your personal data for its own purposes is:

baseworks.tech, registered in the Netherlands under Chamber of Commerce number (KvK nummer) 98170643, VAT number NL005312934B11, postal address Box E1586, Oder 20, 2491 DC Den Haag, Netherlands.

Questions, requests or complaints about this policy or our data practices may be sent to privacy@baseworks.tech.

Section 2: Scope

This policy applies to the baseworks.tech Ecosystem software:

- the control website;
- the control API, data API and agent that run on the Compute;
- the components that install and manage Home Assistant, the Root Network router and supported sensors;
- the baseworks.tech update and licensing service that the Ecosystem contacts; and
- apps licensed by baseworks.tech update and licensing service, insofar as their components are owned by baseworks.tech

It does not govern the baseworks.tech website, the online shop or the Homebrewed applications. The general policy at https://www.baseworks.tech/policies/#privacy covers orders, payments, deliveries and other shop activity, and it applies to the order information linked to an Ecosystem.

Raspberry Pi OS, Docker, Home Assistant, MikroTik RouterOS, device firmware and third-party integrations operate under their own privacy terms, as explained below.

Section 3: Summary

The Ecosystem is designed to keep your information on the hardware in your possession. Day-to-day operation needs no baseworks.tech account, and none of your personal data is reported to a baseworks.tech cloud service. When interacting with baseworks.tech cloud services, the interaction is only performed based on your explicit agreement (such as toggling on periodic Ecosystem update checks) and the data sent is the minimum necessary to allow your ecosystem to check for updates. baseworks.tech does not receive your sensor readings, Home Assistant data, device lists, network configuration, credentials or logs through the Ecosystem. Before delivery, baseworks.tech generates the initial Ecosystem Password and uses factory default device credentials to prepare your Ecosystem; Section 5.1 explains this. In case you encounter issues with the Ecosystem, you may choose to share some of the logs with the baseworks.tech support, but this process requires your explicit action and doesn't happen automatically.

The Ecosystem software contains no advertising, advertising SDK, general-purpose analytics, usage profiling, telemetry or third-party crash-reporting service. It does not build an advertising or behavioural profile about you.

The Ecosystem communicates with:

- the baseworks.tech update and licensing service, when you check for, download or activate a release, or when you enable automatic update checks;
- connectivity-check and time-synchronization services, to find out whether an internet connection is available and to keep the clock correct;
- software download sources used to install or update Home Assistant and the Root Network router when no offline copy is available;
- your local devices, such as sensors, the Root Network router and devices integrated through Home Assistant; and
- any third-party services that you enable in Home Assistant or on your devices.

Section 4: Who controls which information

Information stored and processed on your Ecosystem hardware is under your control. baseworks.tech cannot inspect it remotely and does not process it on its own behalf. Where that information relates to other people, you decide how the Ecosystem is used and may be responsible for complying with data-protection law. Examples are household members, guests, tenants or employees whose presence or activity a sensor could reveal. In a private household, the household exemption of the General Data Protection Regulation (GDPR) may apply. In a workplace or other non-household setting, you may need to inform people, consult them, or carry out an assessment before monitoring a shared space.

baseworks.tech is the controller for the limited information described in Section 7, which the Ecosystem exchanges with the baseworks.tech update and licensing service. It is also the controller for correspondence you send us (Section 13).

Section 5: Information stored on the Ecosystem

5.1 Preparation before delivery

When baseworks.tech prepares an Ecosystem, it generates the initial Ecosystem Password, configures devices using their factory default credentials, and prints these on setup cards and QR codes packed with the Ecosystem. baseworks.tech keeps no copy of them after dispatch. Replace the initial password during the first setup.

5.2 Data stored by the ecosystem

The Ecosystem stores the following information on the Compute's storage medium:

- the Ecosystem password and recovery code. These are encrypted with AES-256-GCM, and a separate one-way verifier is used to check sign-in attempts;
- whether sign-in to the control website is required;
- host settings, such as the Ecosystem's name and the name of the space in which it is installed;
- the configuration of installed components. This includes addresses and access tokens used to manage Home Assistant, which are encrypted;
- installation and maintenance task history, and Ecosystem preferences such as notification and automatic update check settings;
- the progress of the guided welcome tour;
- the name, identifier and password of a Wi-Fi network you select as the internet uplink (only when you explicitly choose so), stored in the operating system's network configuration;
- application logs and diagnostic records, as described in Section 12;
- licensing information: a random Ecosystem identifier, a device key pair generated for the Ecosystem, and the Activation Codes installed on it;
- If you install Remote Access: the device name and remote address, which services and devices you made reachable, and the key that identifies the Compute on your Tailscale network. The key is kept only in Remote Access's own folder, readable only by its own system user, and is never included in exports or in any API answer. Remote Access also records each connection that reaches the Ecosystem through it, allowed or refused. A record names the Tailscale account (usually an email address), the device name and the network address of whoever connected, what they tried to reach, and the time. The latest 100 records are kept in memory and shown in the control website. The same details are written to the application log, at most once a minute for each person and target, and are rotated as described in Section 12; and
- the data that Home Assistant, the Root Network router and connected sensors record in their own storage. This can include sensor measurements, device states, history, automations and network client lists.

The Remote Access connection records can describe other people who use your Tailscale network, such as members of your household, colleagues or employees. If you install Remote Access in a workplace or another shared space, you are responsible for informing those people and for any legal basis that their monitoring requires.

baseworks.tech

The Root Network router stores its own configuration, including the Wi-Fi network name and password and the list of connected devices. Sensors store their own Wi-Fi configuration.

Measurements such as CO2 levels, temperature, humidity or occupancy can reveal information about the routines and presence of people in a space. The Ecosystem treats this information as local content under the control of the Ecosystem's owner.

Section 6: Information the Ecosystem does not collect

The Ecosystem does not transmit any of the following outside your local environment on behalf of baseworks.tech:

- a baseworks.tech user account. The Ecosystem has no baseworks.tech account system;
- your Ecosystem Password, recovery code, Wi-Fi passwords or Home Assistant tokens;
- sensor measurements, Home Assistant history, device lists or automations;
- your location. The Ecosystem does not determine the physical location of the hardware; any time zone and country you enter are stored locally for Home Assistant;
- advertising identifiers or information for advertising or cross-app tracking;
- analytics, usage statistics, crash reports or behavioural telemetry;
- your Tailscale account details or Remote Access connection records. They stay on the Compute, and Tailscale receives only what Section 8 describes; or
- payment details. The online shop and its payment providers process these under the general Privacy and Data Protection Policy at https://www.baseworks.tech/policies/#privacy.

When Home Assistant is set up, the Ecosystem does not enable Home Assistant's optional analytics reporting. You can change that setting in Home Assistant yourself. You may also choose to enable Home Assistant cloud services, which is governed by their own terms and privacy policies.

Section 7: Update and licensing service

The Ecosystem uses the baseworks.tech update and licensing service at https://www.baseworks.tech to check for new releases, download Update Bundles and verify Activation Codes. The Ecosystem contacts the service only when you start one of these actions in the control website, or when you have enabled automatic update checks. Automatic checks are off by default.

Request	Information included in the request	Legal Basis for Processing
Check for a release	Ecosystem identifier, time of the request, cryptographic signature of the request	Your consent (Article 6(1)(a)). Tell you whether a newer release is available for your licensed applications

Download a release (ecosystem update, application bundle).	Ecosystem identifier, time, signature, requested application and version	Your consent (Article 6(1)(a)). Confirm the licence and deliver the Update Bundle through a short-lived download link
Activate or refresh licences	Ecosystem identifier, time, signature, the Activation Code or licence tokens being verified	Your consent (Article 6(1)(a)). Verify and record the licences for the Ecosystem
Tailscale coordination service or the coordination server that you configure	When Remote Access is set up or signs in, and while it runs	The Compute's Tailscale public key, its device name, operating system and version, its network addresses (including the public IP address of your internet connection), and the Tailscale account it joins
Tailscale relay servers	When your devices cannot connect to the Compute directly	Encrypted traffic that the relays cannot read, and ordinary connection information

Remote Access is optional and contacts these services only after you install it and sign in. Tailscale Inc. processes this information under the account that you hold with it, as an independent controller, under its own privacy policy, available on their website. baseworks.tech does not receive it. Connections through Remote Access are encrypted end to end between your devices with WireGuard. Remote Access switches off the Tailscale client's upload of logs and diagnostics, so no client logs are sent to Tailscale.

The requests do not deliberately include your name, contact details, credentials, sensor data or network configuration.

When an Ecosystem is licensed, baseworks.tech records the following in the service:

- the Ecosystem identifier;
- the Ecosystem's public key;
- for each licensed application, the licence grant with its status and issue date; and
- the order reference.

Through the order reference, this information can be linked to the order and customer information held under the general Privacy and Data Protection Policy at https://www.baseworks.tech/policies/#privacy.

Like any internet service, the update service and its hosting and content-delivery infrastructure receive ordinary connection information. This includes the requesting IP address, time, requested address and user-agent information. It is used to deliver the response, protect the service against abuse and investigate faults.

baseworks.tech

We process this information to perform the contract under which you licensed the Ecosystem Software, including supplying updates and verifying licences (Article 6(1)(b) GDPR). Where a legal obligation applies, such as supplying conformity and security updates, we rely on compliance with that obligation (Article 6(1)(c)). For protecting the service and investigating misuse, we rely on our legitimate interest in operating a secure update service (Article 6(1)(f)).

The service is hosted on Amazon Web Services (AWS) in the EU region. Downloads are delivered through the AWS content-delivery network. AWS acts as our processor.

If you install releases offline, you need no connection to the update service.

Section 8: Internet connectivity checks and other external services

To find out whether an internet connection is available, and to perform the actions you request, the Ecosystem can contact the following independent services. Note that any of these requests can go through and reach their intended Service only when an internet connection on the Compute Ethernet, Wifi Uplink or Root Network Ethernet/Wifi is available. The act to connect to the internet is considered an intentional action by the user. baseworks.tech does not have any internet connectivity out of the box:

Service	**When**	**Information intentionally included**
GNOME connectivity check (nmcheck.gnome.org)	About every 30 seconds while the Compute is connected to a network through the Wi-Fi uplink or cable	None beyond an ordinary web request
Google connectivity check (connectivitycheck.gstatic.com)	When the Ecosystem checks the cable connection or detects a captive portal	None beyond an ordinary web request
NTP Pool Project (pool.ntp.org)	Periodically, to synchronize the Root Network router's clock	None beyond an ordinary time request
GitHub Container Registry (ghcr.io)	When Home Assistant is installed or updated without an offline copy	The requested Home Assistant version
MikroTik downloads (download.mikrotik.com)	When RouterOS is installed or updated without an offline copy	The requested RouterOS version and architecture

These services receive ordinary connection information needed to answer the request, such as the public IP address of your internet connection, the time and the requested address. They determine how they log and retain that information under their own privacy terms. baseworks.tech does not receive their logs.

baseworks.tech

Raspberry Pi OS, Docker and other Third-Party Software can make their own network requests, for example to check for or install software packages.

Section 9: Home Assistant, sensors and connected devices

The Ecosystem installs and configures Home Assistant on the Compute. It also sets up supported sensors, such as CO2 monitors, so that they connect to the Ecosystem's network, as well as other apps where requested by the user or required to allow correct functioning of the Ecosystem. Home Assistant and the sensors store their data locally. When the Ecosystem sets up Home Assistant, it provides the country and time zone that you select, so that units, formats and schedules are correct.

Home Assistant supports many integrations. Some connect to cloud services operated by device manufacturers or other providers, for example smart-plug, camera, voice-assistant or remote-access services. If you enable such an integration, information such as device states, commands, camera images or account identifiers may be exchanged with that provider. The provider acts as an independent controller under its own privacy terms, and your choice to enable the integration determines that processing.

Cameras, microphones and presence sensors can record information about other people. Section 4 explains your responsibilities when using them.

Section 10: Wi-Fi access point, internet uplink and local network

The Compute can broadcast a Wi-Fi access point for setup and management. The control website can display a QR code containing the access point's name and password. Anyone who scans or photographs that code can join the network.

When you set up a Wi-Fi uplink, the Compute scans for nearby Wi-Fi networks so that you can choose one. The names, signal strengths and security types of nearby networks are displayed to you. They are not sent to baseworks.tech. The credentials of the network you select are stored on the Compute, as described in Section 5.

The Root Network router and the Compute keep lists of connected devices, including device names, hardware (MAC) addresses and IP addresses, so that they can route traffic and display network status. This information stays on your hardware.

If you choose to make the Ecosystem's local services reachable from your local network (which, by default, is not possible, and requires your explicit action to enable), other devices on that network can reach them. Section 18 describes the related security considerations.

baseworks.tech

Section 11: Control website sessions and browser storage

When you sign in to the control website, the Compute issues session tokens. Your browser keeps them in its local storage so that you stay signed in. The control website also stores display preferences, setup progress and similar technical state in your browser's local and session storage.

The control website uses no cookies or storage for analytics or advertising, and loads no third-party trackers. You can remove the stored information by signing out or by clearing the site data for the control website in your browser.

Section 12: Logs and diagnostics

The Ecosystem applications keep technical logs on the Compute to help diagnose failures. Logs are rotated hourly and old files are removed automatically; each application normally keeps about the last 24 hours. Records contain timestamps, events, error descriptions and technical values such as device addresses, component names and network state. Passwords, tokens and similar secrets are designed to be redacted.

By default, the operating system journal is kept in memory only and is cleared when the Compute restarts. You can enable persistent system logging in the control website, for example to investigate a problem across restarts. Persistent logs then remain on the storage medium until they are rotated or you disable persistent logging.

The control website can display a live diagnostics stream. Logs and diagnostics are not transmitted to baseworks.tech or to a crash-reporting provider. You decide whether to include them in a support request.

Section 13: Support and correspondence

If you contact baseworks.tech for support or privacy assistance, we process the message and contact details you provide, together with any screenshots, logs or exports you choose to attach, so that we can respond. We rely on the performance of our contract with you (Article 6(1)(b)) or our legitimate interest in answering enquiries (Article 6(1)(f)). The general baseworks.tech Privacy and Data Protection Policy applies to that correspondence, including its retention periods.

Before sending logs or exports, review them and remove information you do not want to share.

Section 14: Exports, resets and returned hardware

The control website can prepare a downloadable export of the Ecosystem's data and recent logs. Passwords, recovery codes and tokens are replaced with a redaction placeholder. The export is prepared on the Compute and downloaded directly to your browser. Once you save or share it, you control that copy. Protect it accordingly.

baseworks.tech

Resetting the Ecosystem removes the configuration of the selected components. A reset keeps the licensing information described in Section 5, so that licensed applications can be reinstalled.

Due to the flash nature of the storage devices, certain information may still be recoverable after removing it. Always contact an authorized company if you want to achieve irreversible data deletion.

If you return hardware to baseworks.tech, remove or back up your data first. Storage media returned to baseworks.tech may be erased and re-imaged. We do not inspect or keep personal data left on returned media, except where that is necessary to diagnose a reported defect you asked us to investigate.

We do our best to irrecoverably delete the data from your storage device upon permanent return from you by erasing it and overwriting it with zero and random bytes. As of baseworks.tech knowledge, no software removal process on the baseworks.tech side guarantees 100% irrecoverability.

A full reset removes Remote Access, signs the Ecosystem out of your Tailscale network and deletes its Remote Access identity and the component's folders. A reset that keeps components deletes the Remote Access identity and keeps the component. Remote Access connection records are not included in exports, except as part of the application logs if you choose to export them.

Section 15: Retention and deletion

Information stored on the Ecosystem remains there until you delete it, reset the relevant component, or erase or replace the storage medium. Application logs are rotated automatically, as described in Section 12.

baseworks.tech keeps the update and licensing records described in Section 7 for as long as the Ecosystem's licences exist. After that, we keep them only for as long as needed to comply with legal obligations or to establish, exercise or defend legal claims. Short-lived records used to prevent replay of signed requests expire automatically after about ten minutes. Service logs are kept for up to one month.

The general Privacy and Data Protection Policy at https://www.baseworks.tech/policies/#privacy sets out the retention periods for order information linked to an Ecosystem.

Section 16: Children

The Ecosystem is not directed at children, and baseworks.tech does not knowingly collect children's personal data through it. Where the Ecosystem is used in a space that children occupy, a parent, guardian or responsible organization should decide how measurements and connected devices are used.

Section 17: Your data-protection rights

Where baseworks.tech acts as a controller of your personal data, applicable data-protection law may give you the following rights:

- information and access;
- rectification and erasure;

- restriction and portability;
- objection; and
- rights concerning consent and automated decision-making.

In practice, the information described in Sections 5 and 9 to 12 stays in your possession. You can inspect, correct, export and delete it using the control website and the components it manages, without asking baseworks.tech. The Ecosystem does not make decisions about you that produce legal or similarly significant effects.

For the update and licensing records described in Section 7, and for information you provide when contacting us, send a request to privacy@baseworks.tech. We may need enough information to understand the request and to verify that we are responding to the correct person, for example the Ecosystem identifier shown in the control website. We will handle the request within the period required by applicable law.

You may complain to the supervisory authority in the country where you live or work, or where you believe an infringement occurred. In the Netherlands, the authority is the Autoriteit Persoonsgegevens (https://autoriteitpersoonsgegevens.nl/).

Section 18: Security

The Ecosystem uses the following safeguards:

- Credentials and management tokens are encrypted at rest;
- Sign-in attempts are checked against a one-way verifier;
- Update Bundles and Activation Codes are verified with digital signatures before they are used;
- Requests to the update service are signed with a key generated for the Ecosystem, and are sent over encrypted HTTPS connections;
- The setup cards contain the initial Ecosystem Password. You are asked to change the Ecosystem Password to a secure password during first setup and store or destroy the cards securely;
- Remote Access publishes nothing on the public internet. Only devices signed in to your Tailscale network can connect, and only to the services and devices that you switched on. Any other connection is refused and recorded;
- Requests to the control website through Remote Access still require the Ecosystem Password when sign-in is switched on; and
- The Remote Access identity key is stored on the storage medium. A person who can read the storage medium may be able to use it. Remove the device from your Tailscale network if the Compute or its storage medium is lost.

The encryption key for stored credentials is kept on the same storage medium as the data it protects. The protection therefore depends on the physical security of the Compute and its storage medium. A person who can remove and read the storage medium may be able to recover stored credentials. The same Ecosystem Password protects the control website, the Compute access point, Home Assistant and the Root Network, so keep it confidential and choose a strong one.

baseworks.tech

If you disable sign-in for the control website, or make local services reachable on a network you do not fully trust, other people on that network may be able to access or change the Ecosystem. No storage or transmission method can be guaranteed completely secure.

Section 19: International data transfers

The update and licensing service stores its records in the EU. Downloads and requests pass through AWS's content distribution service (CloudFront), a global content-delivery network, so connection information may be processed at the network location closest to you, including outside the European Economic Area. Where personal data is transferred outside the EEA, we rely on an applicable transfer mechanism, such as an adequacy decision or the European Commission's Standard Contractual Clauses in the AWS data-processing terms.

The external services listed in Section 8, and third-party services you enable in Home Assistant, may process connection information in other countries under their own terms.

If you use Remote Access, Tailscale Inc. may process the information described in Section 8 in other countries, including the United States, under its own terms and transfer mechanisms.

Section 20: Changes to this policy

We may update this policy when the Ecosystem's features, legal obligations or third-party services change.

The latest version will be published on the baseworks.tech policies page, with a version number and effective date. Each Ecosystem release includes the current policy version when the release was built, and shows it in the control website. Where required, we will also identify material changes to how the Ecosystem handles information through release notes, the control website or another appropriate method.

Section 21: Governing language

The authoritative version of this policy is English. A translation may be supplied for convenience. If a translation differs from the English version, the English version prevails to the extent permitted by applicable law. Mandatory language requirements remain unaffected.

Section 22: Contact

Privacy questions, requests or complaints:

privacy@baseworks.tech

General Ecosystem support:

support@baseworks.tech

baseworks.tech

Postal correspondence:

baseworks.tech, Box E1586, Oder 20, 2491 DC Den Haag, Netherlands

baseworks.tech