Overview

Welcome to the Core Box Integrator guide. This document serves as a comprehensive guide to using, updating and integrating the Core Box system. It starts with an overview of Core Box and its main functions, followed by detailed descriptions of its key features and variants. You will find explanations of the LED patterns, ignition system interactions, network status, and update instructions. Additionally, the guide includes technical specifications in the datasheet and an overview of the Core Box API, featuring documentation, code examples, and usage guidelines.

Table of contents

Introduction

This guide introduces the Core Box, which is an ECU designed to deliver modular automatic steering solutions for a diverse array of vehicles. Hexagon has tackled the challenges of a fragmented technology landscape, plagued by compatibility and integration issues. The Core Box offers a dependable and precise auto-steering solution seamlessly integrated into the machine's user interface.

Features

Below, you will find the key features of the Core Box. Understanding these features will help you fully utilize the Core Box and maximize its benefits.

- **Versatile Connectivity:** Connects through Wi-Fi and mobile data.
- **Powerful Processing:** Equipped with advanced processing capabilities, custom APIs, and complex algorithms, including automatic driving.

- **Standard Protocol Integration:** Compatible with standard protocols such as ISOBUS for ISOBUS VT.
- **Advanced Sensor Suite:** Includes positioning technologies with integrated GNSS, IMU, and multiple inputs for controlling key functions (valves, motors, etc.).
- **Flexible Display Compatibility:** Supports third-party screens and monitors with an agnostic display design.
- **Enhanced Manufacturing Options:** Allows tractor manufacturers to boost shipping demand with factory-installed automatic driving functionality.

Information: The Core Box is available in two variants: Lite and Full, each of them with optional upgrades. These variants are designed to address a range of user needs and application scenarios, providing flexibility and compatibility with various setups and systems. You can find more information in the Core Box datasheet, which will be discussed in the next section.

Datasheet

There's a document titled Core Box Datasheet that contains technical specifications that outline the product's features and capabilities, including details on dimensions, materials, performance, and electrical requirements. Additionally, it offers guidance on how to use the product correctly, including installation instructions. Click here to access the Core Box datasheet.

Once you have installed the Core Box, you can go ahead and learn how to power it on.

Ignition sense

The Core Box does not have a built-in power on/off button in the ECU itself. Instead, it uses the SNSB, which is a digital input that functions as the sensor for powering the system on and off.

For example, when an operator gets to the tractor and wants to start working, they need to turn the machine's key, which creates a high signal. If the SNSB is connected to this sensor, it will detect the high signal, beep, light up the LED, and turn on the system.

The Core Box is equipped with an ignition sense that, when connected to the outlet, activates standby mode. In this mode, the pin must maintain 12 volts to ensure continuous operation. When the device receives an additional pulse, it begins operation. After initialization, the Core Box's operating system becomes active.

Then, it monitors the pin input to detect if the operator has turned the key to turn off the machine. When this happens, a configurable countdown for shutdown begins, with the default being 10 seconds. When the machine is turned off, the signal drops from 12 volts to 0 volts.

Information: Regarding the time required for a safe shutdown, it is recommended to wait approximately 10 to 12 seconds after power loss.

Now that you know how to power the Core Box, it's time to explore its technical and functional details.

Technical and functional details

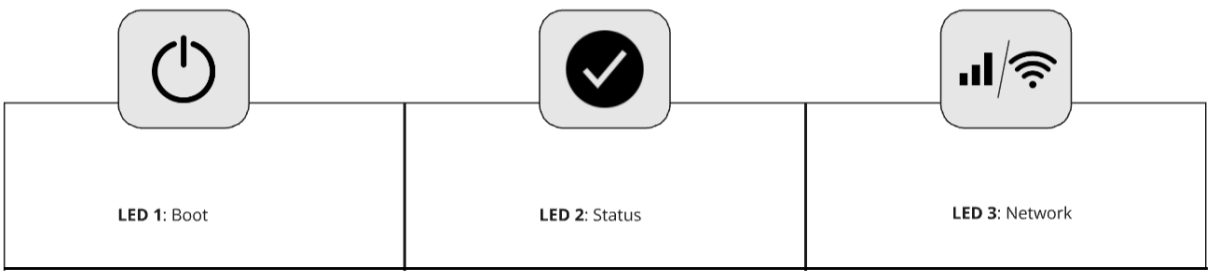
You will now explore how LED patterns function, check network status, and learn how to update and format the Core Box.

LEDs pattern

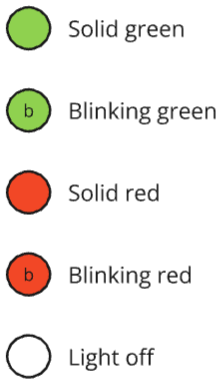
The operation can be checked through the three LEDs and internal monotone buzzer present on the device, as shown below:

In this document, the three LEDs will be referred to as LED 1, LED 2, and LED 3.

LED 1 indicates the Core Box's booting status, LED 2 shows the status of the app, and LED 3 represents the network status.



The three LEDs can display five distinct states, including various colors and flashing patterns (whether solid or blinking).



Combined, the 3 LEDs provide information on the following statuses:

- Power status
- Connectivity status
- Alarms

Tip: LED patterns are useful during manual operation, as they provide visual feedback. In autonomous operation, the LED patterns may not be useful.

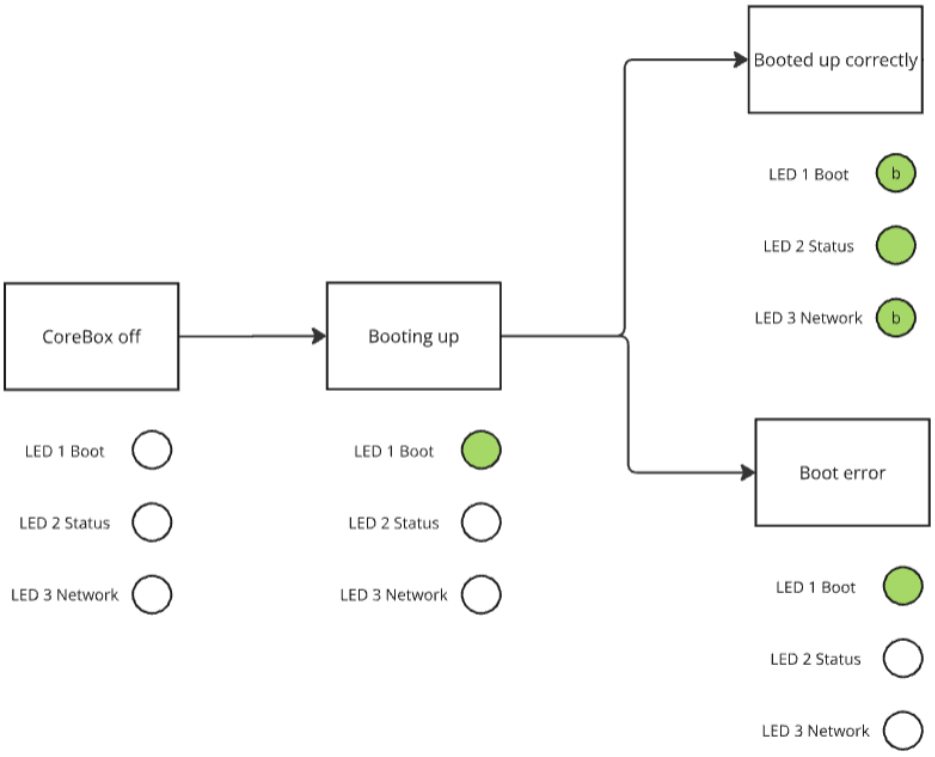
Core Box booting

Now you will learn how to successfully boot the core box. Follow these instructions to ensure a smooth startup process.

1. If the Core Box is powered off, all three LEDs will be off.

2. When you attempt to start it up, LED 1 will light up solid green, while the other two will remain off.
    a. If the Core Box boots successfully, all three LEDs will turn green: LED 1 and LED 3 will blink, and LED 2 will stay solid green.
    b. If there's an error during the boot process, LED 1 will be solid green, and the other two LEDs will stay off.

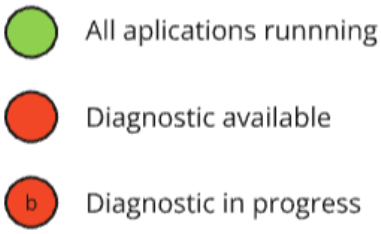
Information: The LED will be solid green when powered through a hardware pull-up and will blink green when the application is active.



App status

The LED signals also indicate the status of the Core Box, whether it's operating correctly, if a diagnostic is in progress, or if it is already available. This applies to any application that fails and generates a diagnostic.

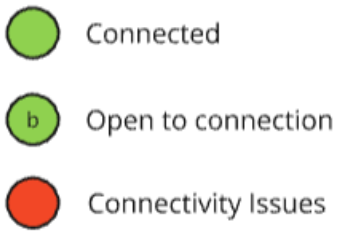
- A solid green LED means that all applications are running smoothly.
- A solid red LED indicates that a diagnostic is available.
- If the LED is blinking red, it signifies that the diagnostic is in progress.



Network status

This LEDs provides a general overview of the network status, indicating issues with Wi-Fi or Ethernet connectivity. Besides network issues, the LED will also turn red if there's an internal problem preventing the API from functioning.

- A solid green light indicates a successful connection.
- A blinking green light means it is open for connection.
- A solid red light signals connectivity issues.



When the Core Box is powered on, the app's status and network connectivity will be signaled by the patterns of the three LEDs.

If the connection is successfully established, the LEDs will display the following behavior:

- LED 1: blinking green
- LED 2: solid green
- LED 3: solid green

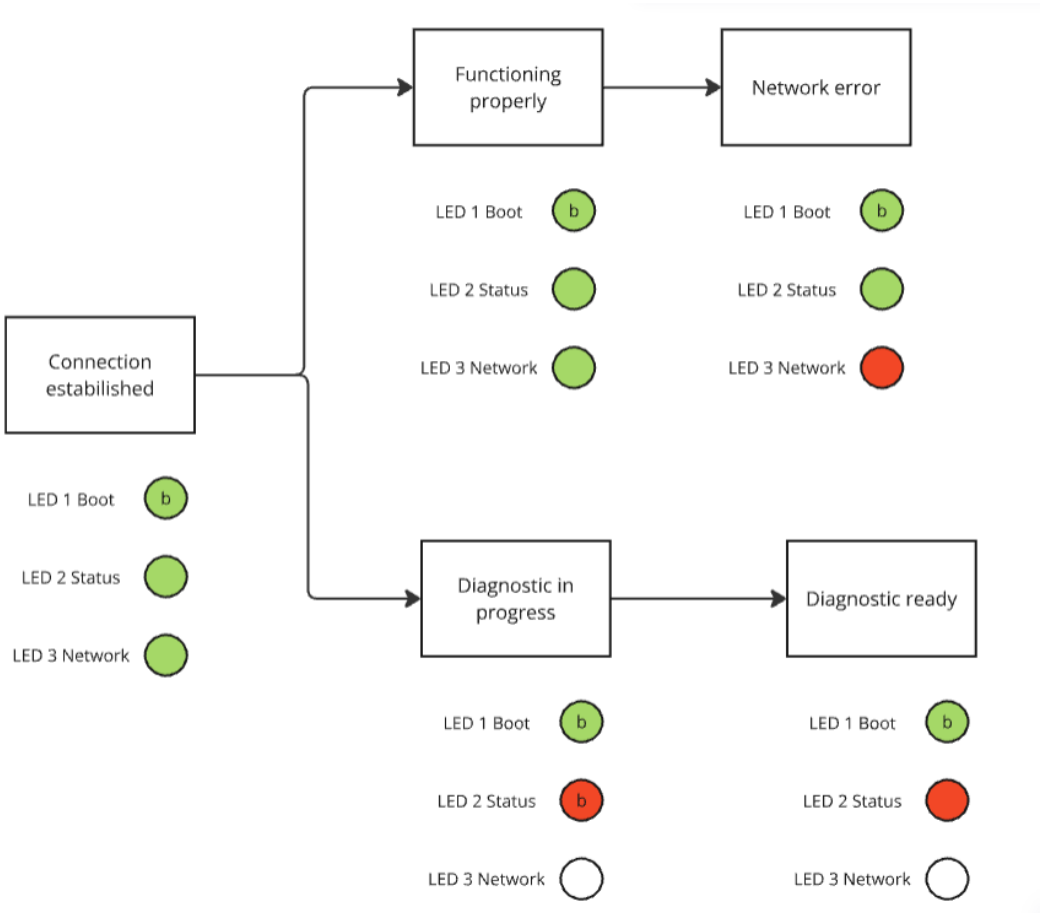
After the connection is established and functioning correctly, the LED behavior remains the same:

- LED 1: blinking green
- LED 2: solid green
- LED 3: solid green

Tip: If a network error occurs after the connection is established, LED 1 will blink green, LED 2 will be solid green, and LED 3 will be solid red.

If the connection is established but does not function correctly, a diagnostic will be initiated to identify the issue.

- During the diagnostic process, LED 1 will blink green, LED 2 will blink red, and LED 3 will be off.
- Once the diagnostic is complete, LED 1 will continue to blink green, LED 2 will display a solid red, and LED 3 will remain off.

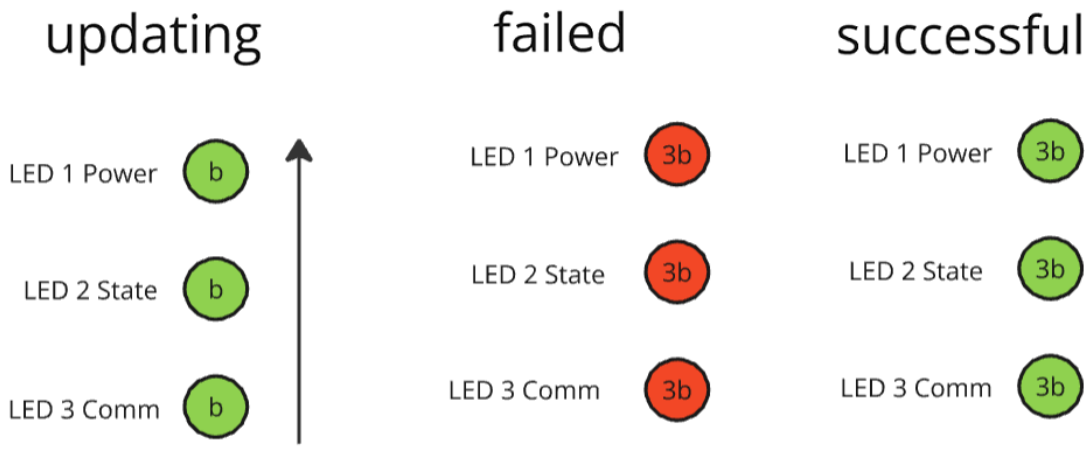


Having learned how to interpret the LED patterns and their meanings, you're now ready to learn how to update and format the Core Box.

Updating and formatting the Core Box

During updates or formatting, the LEDs serve as the primary user interface. They are used to indicate that progress is being made and to signal when the process is complete.

- When updating, it blinks in succession to create a wave effect and resemble a loading bar.
- When the update fails, it blinks three times, like other hardware components. The Core Box will continue to function without interruption and will be ready for another attempt or usage without needing a new update.
- When the update is successful, it blinks three times.



Information: The device beeps when an update is finished, regardless of success or failure, and when formatting is completed. Click here if you want to learn how to update the Core Box.

Static IP

To connect and configure the Core Box, it's important to note that the Core Box board includes up to 5 internal network interfaces:

- Ethernet 100BASE-TX (Linux interface: eth1)
- Ethernet 100BASE-T1 (automotive Ethernet) (Linux interface: eth0)
- Internal WiFi (Linux interface: wifi0)
- Mobile network module (M2 interface)
- Mobile network module (PCIe interface)

When it comes to static IPs, by default, the Core Box has the following static IPs:

- Static IP **192.168.1.150** on the ethernet interface **eth0**
- Static IP **192.168.1.151** on the ethernet interface **eth1**

Information: You can also use the external connector to attach additional devices such as external WiFi dongles (Linux interface: wifi1) or Ethernet adapters. The connector type to use is M12 Female – 4-pin key D, indicated as connector number four in the image below.

Now that you have explored the Core Box functionalities and specificities, you will learn more about the Core Box external communication API.

Core Box external communication API

The Core Box offers a user-friendly and flexible API that allows users to input the desired path and adjust all necessary system settings. It is designed to enable seamless interaction between the Core Box system and external systems or applications. It provides a structured way to execute commands, transmit data and discover interfaces. Overall, this API allows for efficient management and integration of the Core Box system with other systems or applications, enhancing its functionality and flexibility.

Click here to learn more about the Core Box external communication API.

Integrating the Core Box with your system

Automatic Steering enables the vehicle to follow a predefined path by identifying the closest point and maintaining the intended trajectory. The system relies on proper path configuration to avoid ambiguity and ensure smooth operation.

The Core Box automatically steers vehicles using paths sent via API. For this, we provide the Point Feed interface, which allows the defining and dynamically updating the path to be followed by the Core Box. Below, you will find important information to guide the integration.

Managing paths with the Point Feed in Core Box's Automatic Steering

While Automatic Steering is disengaged, any received path completely replaces the current path.

Information: Only one path is kept in memory, which is identified by a token.

If Automatic Steering is operating, only commands related to the current path (identified by the token) will be accepted, with the purpose of merging them into the current path.

Tip: If the token does not match the current path's token, the command will be rejected.

To extend the current path with new path points, include at least five repeated points from the end of the existing path. If no repeated points are provided or they are too far from the last known point, the command will be rejected, returning code 4 from the Point Feed call.

Warning: After merging a path, already traversed points will be deleted from the memory.

You must ensure that the path is navigable, as the system does not perform any checks based on mechanical or performance constraints. A minimum of four path points is required to create a path.

Information: The Core Box may apply filters to the path in an attempt to smooth it, slightly altering its geometry.

The distance between path points must allow a trajectory reconstruction. In straight segments, a long distance between points is acceptable, while in curves, the tighter the radius, the shorter the distance between points.

Refer to parameter code 2 in the SetParameters method of the Guidance interface. Below are the minimum recommended distances between path points:

- **Straight line:** 2 points, one at the beginning and one at the end
- **Curve with a 15m radius:** 1 point per meter
- **Curve with a 5m radius:** 1 point every 0.25 m

Automatic Steering behavior

When Automatic Steering is engaged, the system determines the trajectory as follows:

- It identifies the closest point on the path relative to the vehicle's current position. This point serves as the starting reference for trajectory tracking, with the direction depending on the vehicle's orientation.

Warning: Avoid sending a path that could create ambiguity in the intended direction.

- With Automatic Steering engaged, the vehicle follows the path in the order of the points, starting from the previously identified point. If Automatic Steering is turned off while on the path and then reactivated, this process will repeat.

Information: Automatic Steering will be disengaged if the end of the path is reached or if the deviation from the path or the angle exceeds the configured values.

Suggested usage

Once the system has been properly calibrated and the GNSS is synchronized, follow the steps below:

1. Avoid sending an initial segment of the path that contains:
    - Joints, nodes, or similar elements;
    - Nearby trajectories that are closer to the vehicle’s current position than the intended start of the path;
    - A starting point that is too close to the vehicle’s current position.

Tip: Automatic Steering will not engage if the distance and angle relative to the guide exceed the safety parameters configured in the Steering interface (SET/GET parameters method, parameters with ID 10 and 11).

2. Monitor the Guidance signal updates.
3. As the vehicle approaches the end of the path, send new points for the current path using the same token.

Information: The higher the vehicle's speed, the earlier the points should be sent. To ensure smooth processing and error handling, maintain a 30-second buffer before reaching the end of the path.

4. Now that Automatic Steering is already operating, a longer path can be sent, including nodes and joints, and other elements.
5. If Automatic Steering disengages, repeat the process.

This is all you need to know to start the integration of the Core Box with your system. Next, you will learn how to update the Core Box.

How do I update the Core Box?

To update the Core box software version, you will need a USB flash drive and a .uti file.

Follow the step-by-step instructions:

1. To download the .uti file for the desired version, access the **Release Notes**, where you can download the desired version.
2. Insert the downloaded file into the root directory of a USB flash drive.

Warning: The USB flash drive needs to be formatted in FAT32 for the update to work.

Note: Different files can be downloaded for updates, such as configuration (.cti) and firmware (.ati) updates. It is recommended to insert only one file onto the USB flash drive at a time. If multiple files are present on the drive, the .uti file will be processed before the .cti and .ati files. If there are multiple .uti files, the most recent one will be executed first.

Tip: The Hexagon support team will recommend and share .cti and .ati files with customers as needed.

3. Insert the USB flash drive into the Core Box while it is powered off.
4. Now, power the Core Box on and the update will start automatically.
5. Wait for the update to complete. Use the LED feedback to understand the status of the update process.
6. Once the update is finished, the Core Box will automatically restart.

Network configuration and privacy transparency

This section covers the device's network exposure and how users are informed about changes to data processing, security, and privacy. It details the key network interfaces and services in the factory default state, along with the procedures for notifying users about updates that affect their personal data.

Exposed network interfaces and services in factory default state

In the factory default state, the equipment exposes several network interfaces and services, which are essential for its operation and connectivity.

The available network interfaces include a Wi-Fi access point, a Wi-Fi client, Ethernet, and mobile connections. These interfaces enable various communication methods, ensuring flexibility in how the device connects to other systems or networks.

In addition to the network interfaces, the device also exposes a range of services. Below is an overview of each service and its purpose:

- The SSH server provides secure remote access to a system over a network, allowing support to log in and manage the file system with encrypted communication.
- The Software Update service manages software and firmware updates, ensuring the system remains current by downloading and applying necessary patches.
- Cloud sync uploads files to Hexagon's cloud platform, enabling Remote Access and backup.
- The MQTT client enables low-bandwidth communication between devices in applications using the MQTT protocol.
- The FTP client facilitates file transfers between local systems and remote servers over a network.
- Remote Access allows users to control a system remotely via the internet.
- The NTRIP client manages network routing information, optimizing data routing within a network.
- The NTP client synchronizes the system clock with a remote time server to maintain accurate time logs and coordination.

What conditions or risks can impact the network's performance or security?

The display device supports four types of network connectivity: Wi-Fi in client mode, Wi-Fi in access point mode, mobile network (via SIM card), and Ethernet. These interfaces enable communication with cloud services, local devices, or both, depending on the configuration. Regardless of the network type, the display maintains a dedicated CAN bus connection to machine controllers, ensuring real-time communication with the equipment it operates.

Network connectivity	Risks
Wi-Fi in client mode: The display device connects to the internet and cloud services via a Wi-Fi router using WPA2 security. The user is required to manually input the Wi-Fi credentials into the display. Network access is managed by a designated network administrator ensuring that only authorized devices can join the network.	• Unauthorized access: If Wi-Fi credentials are weak or reused, attackers could gain access to the network. • Credential exposure: Manual entry of credentials into the display may be intercepted if not securely handled. • Network misconfiguration: Incorrect router settings (e.g., open ports, weak firewall rules) can expose the device. • Shared network risks: Other devices on the same network may be compromised and used to attack the display.
Wi-Fi in access point mode: The display device can be configured by the user to operate as a Wi-Fi access point under WPA2 security. In this mode, the display does not share internet access but allows local devices to connect for local services only. The user is responsible for managing access to the AP, including password configuration and device authorization.	• Unauthorized local access: If WPA2 password is weak or shared, unauthorized users may connect to the AP. • Local attack surface: Devices connected to the AP may attempt to exploit local services on the display. • User mismanagement: Improper configuration of access control by the user may expose the network. • Connected device re-shares network access without access control: Devices connected to the AP may create their own access points or bridges, unintentionally exposing the local network to unauthorized users.
Mobile network: The display device supports mobile network connectivity via a SIM card. The user must configure the network credentials (e.g., APN, PIN) to enable direct access to internet and cloud services. The network manager is responsible for overseeing access control and data usage. This setup provides independent connectivity, bypassing local network infrastructure.	• Data plan exhaustion: Uncontrolled data usage may lead to service disruption or unexpected costs. • Weak APN configuration: Incorrect or insecure APN settings may expose the device to external threats. • Limited Monitoring: Mobile networks may lack the visibility and control of enterprise-managed networks.
Ethernet: The device connects to the network using a physical Ethernet cable, offering a more secure and stable connection compared to wireless. Like the Wi-Fi client mode, the user must configure network addresses, and access is managed by a network administrator.	• Physical access: If the Ethernet port is accessible, attackers can plug in and gain network access. • Shared LAN exposure: Devices on the same LAN may attempt lateral movement to exploit the display.

- Static IP misconfiguration: Incorrect IP settings may lead to conflicts or exposure to untrusted segments.
- Lack of encryption: Ethernet does not inherently encrypt traffic—data may be intercepted on the LAN.

User notifications for changes in data processing and security

To keep users fully informed about changes that may impact the processing, security, and privacy of their personal data, notifications will be provided in advance through Release Notes. These notes will include detailed information about the changes and their potential effects on user data, ensuring transparency and maintaining trust. Click here to view our Release Notes page.

These notifications will cover the collection and processing of new personal data categories, explaining what data is being collected, its purpose, and how it will be processed. Additionally, any changes to processing operations, security controls, or logging settings will be clearly outlined, including the reasons for the changes and their impact on privacy and data security. Users will also be informed of any modifications to the types or parameters of data processing that could affect the level of privacy protection, ensuring they are fully aware of how their data is being handled and any actions they may need to take.

Document history

Version	Date	Who	Comments
0.1	27 Sep 2024	Amanda Arrais	First Release.

0.2	12 Feb 2025	Amanda Arrais	Added the section “Integrating the Core Box with your system” and its subsections.
0.3	26 May 2025	Amanda Arrais	Added the section “Network configuration and privacy transparency”