

Gantner IT Security Assessment - eLoxx365



Document Version 1.2

© Copyright 2026 Gantner Electronic GmbH

Operating instructions, manuals, and software are protected by copyright. All rights are reserved. Copying, duplication, translation, installation in any electronic medium or machine-readable form in whole or in part is prohibited. The sole exception is represented by creation of a back-up copy of software for own use as a safeguard, so far as this is technically possible and recommended by us. Any infringement will render the party committing such infringement liable to compensation payment.

Liability

Any claims against the manufacturer based on the hardware or software products described in this manual shall depend exclusively on the conditions of the guarantee. Any further-reaching claims are excluded, and the manufacturer accepts no liability for the completeness or accuracy of the contents of this manual. The right is reserved to make alterations, and alterations may be made at any time without prior notice being given.

Trademarks

Attention is drawn at this point to markings and registered trademarks used in this manual. All products and company names, which are mentioned in this manual, are only used for identification and explanation purposes. Some of these names may be trademarks or registered trademarks of the corresponding company.

Contact

If you have any questions regarding this product, please contact your local representative or one of the Gantner Electronic GmbH branches directly. The contact addresses can be found using the following link:

www.gantner.com/en/locations.

Contact address of manufacturer

Gantner Electronic GmbH
Bundesstraße 12
6714 Nüziders, Austria

CONTENTS

1	INTRODUCTION	5
1.1	About this manual	5
1.2	Contact & inquiries	5
1.3	Terminology	6
1.4	Networked locking system	7
2	SYSTEM DESCRIPTION	9
2.1	Overview	9
2.1.1	Information and data characteristics	10
2.2	System architecture	11
2.3	Network infrastructure	12
2.4	Hardware components	13
2.4.1	GAT NET.Lock	13
2.4.2	GAT SMART.Lock	13
2.4.3	Sub Controller	14
2.4.4	GC7 Main Controller	14
2.4.5	GT7 Central Locker	14
2.5	Software components	15
2.5.1	Envisio cloud platform	15
2.5.2	G7 device web interface	24
2.5.3	G7 Connect (Gantner Cloud)	25
2.6	Access control data carriers	26
2.6.1	Technology and compatibility	26
2.6.2	UID, CSN, data carrier number	26
3	SECURITY & MANAGEMENT	27
3.1	User management	27
3.2	Role management	28
3.3	Logging	29
3.4	Master cards	30
3.5	Controller offline mode	30
3.6	Essential power circuits / UPS	31
4	SYSTEM ADMINISTRATION	33
4.1	Remote access	33
4.2	Firmware updates	33
4.3	Antivirus software and firewall	33
5	ABOUT GANTNER	35
5.1	Warranty and system support	35
5.2	Client training	36

5.3	Software development standards	37
5.4	Client security assessments	37
6	FREQUENTLY ASKED QUESTIONS	39
6.1	Hardware components	39
6.1.1	Does the system support 802.1x authentication?	39
6.1.2	Are there any hubs or switches included/embedded in the system?	39
6.1.3	Does the system support Gigabit Ethernet connectivity?	39
6.1.4	Is the communication protocol encrypted?	39
6.1.5	Which operating system do the main controllers use?	39
6.1.6	Which operating system do the sub controllers use?	39
6.1.7	Do the main controllers have to use an SD card?	39
6.1.8	What is the NET Bios Name of the main controllers?	39
6.1.9	What are the bandwidth and latency considerations for the main controllers?	39
6.2	Software components	40
6.2.1	How is data in transit protected?	40
6.2.2	Do you encrypt tenant data at rest?	40
6.2.3	Who owns the encryption keys?	40
6.2.4	How are keys provisioned, accessed, rotated, and destroyed?	40
6.2.5	Are database backups encrypted?	40
6.2.6	Are there backup or recovery mechanisms in place to protect the database?	40
6.2.7	What measures does Gantner take to detect vulnerabilities and maintain the security of the application?	40
6.2.8	Do you logically and physically segregate production and non-production environments?	41
6.2.9	Do you protect your cloud services with anti-malware programs?	41
6.2.10	What are the minimum password requirements for eLoxx 365?	41
6.2.11	Does eLoxx 365 support periodical pushed password changes?	41
6.2.12	Are there minimum password requirements for eLoxx 365?	41
6.2.13	Which login methods are possible with eLoxx 365?	41
6.2.14	Is it possible that the eLoxx 365 server becomes temporarily unavailable, e.g., during updates?	
6.2.15	Can I change the ports in eLoxx 365?	41

1 INTRODUCTION

1.1 About this manual

This manual provides additional information for the IT security assessment of the networked locking system from Gantner. The information contained herein is designed to assist IT departments in completing a risk/reward analysis and security vetting in compliance with their approved corporate security policies.

The following documentation is available to download from the Gantner Partner Portal (login required) for the individual products described in this manual that explain all functions associated with the product in greater detail:

1. GAT NET.Lock System
 - o [NET.Lock | Gantner](#)
2. GT7 Terminal
 - o [GT7 | Gantner](#)
3. GC7 Controller
 - o [GC7.2000 | Gantner](#)
 - o [GC7.3000 | Gantner](#)
4. G7 Connect
 - o [G7 Connect | Gantner](#)
5. eLoxx 365 Management Software
 - o [eLoxx 365 | Gantner](#)
6. Envisio Cloud Platform
 - o [Envisio Documentation \(vintia.com\)](#)

1.2 Contact & inquiries

For all inquiries concerning the Gantner networked locking system, please contact your local sales partner or one of the Gantner branch offices directly. The contact details are available via the following link:

www.gantner.com/EN/locations

1.3 Terminology

Several key terms that are used often in this manual are defined below.

Lock

This term refers to the GAT NET.Lock electronic lock from Gantner that is used to lock the lockers.

Locker

This term is used to describe all possible locker applications, e.g., a changing room locker or an office storage locker, which can be locked by the GAT NET.Lock.

User

This term refers to the person responsible for operating the eLoxx 365 management software, e.g., a facility department employee.

Data carrier

This term refers to the employee access control cards, credentials, or fobs that are used with the networked locking system.

RFID (Radio-Frequency Identification)

Identification over short distances (0 – 5 cm, 0 – 2 in) using radio frequency. An RFID data carrier (e.g., employee access card) is used for identification in the networked locking system.

Main controller

This term refers to the control unit that is used for communication with the locker management software, e.g., eLoxx 365.

Sub controller

This term refers to the control unit that the GAT NET.Lock locks connect to. The sub controller receives/sends information from/to the main controller/eLoxx 365 via a serial RS-485 network and controls the electronic locks accordingly. Different variants of the sub controller are available that are described in the GAT NET.Lock manual.

Enviso cloud platform

A cloud-based software provided as Software-as-a-Service (SaaS) for the administration and management of the locker system. The Enviso platform (<https://www.enviso.io/>) is hosted by Amazon Web Services (AWS) in Ireland.

eLoxx 365

The eLoxx 365 area is an app within the Enviso cloud platform that is the interface for managing the lockers, data carriers, and end users of the locker system.

Admin

The “Admin” area is an app within the Enviso cloud platform and provides an interface for administrating the operators, i.e., the employees of the organization, of the locker system.

G7 Connect

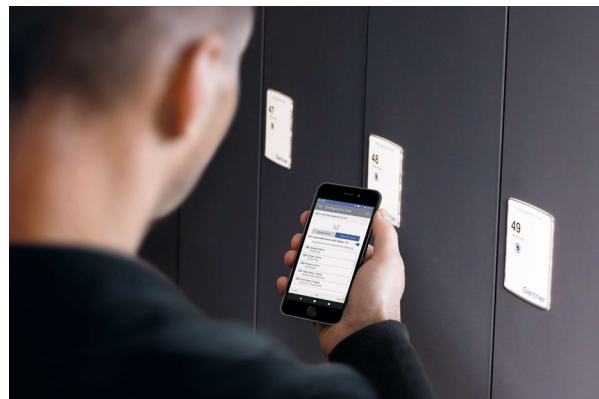
G7 Connect is Gantner’s Cloud service for the configuration and management of projects that contain multiple Gantner devices. G7 Connect is accessible via a web browser following registration and login.

Web interface

The G7 devices are equipped with a web browser accessible interface that allows the device and app settings to be easily viewed and configured.

1.4 Networked locking system

High quantities of storage lockers for company information and/or employees' private belongings must be easy to manage and simple to use to avoid high operating costs in the building operation and security department.



The Gantner networked locking system can use new or existing employee access control cards (provided they are compatible) to lock/unlock a locker and can be managed from any location.

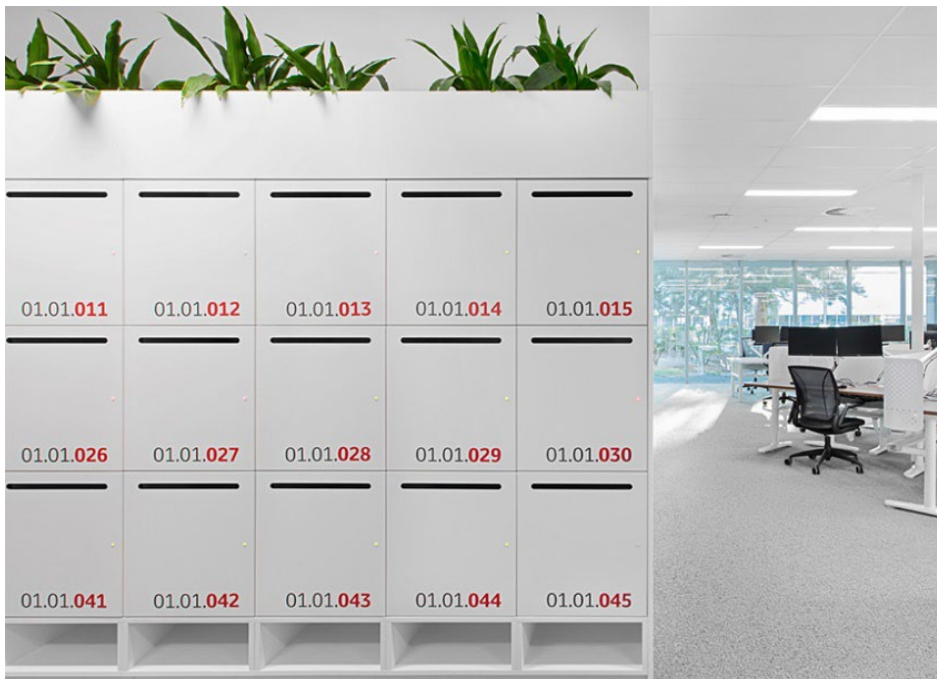
It is a distributed control system with each locker lock providing the same attributes as a door access control system (door lock, door monitor, card reader). The system is a critical business platform that most employees will interact with multiple times each day.



The networked locking system consists of Gantner hardware, and a locker management software, the Enviso cloud platform, which is provided as a software-as-a-service (SaaS). SaaS is a method of remotely delivering software, meaning that you can remotely access the platform from any device with an internet connection. One of the key advantages of SaaS is that costly investments in the hardware and IT services required to troubleshoot and maintain software are eliminated.



Key features of the system include a networked alarm for each locker, a searchable audit trail, full transparency with real-time occupancy monitoring, and the ability to connect to third-party systems via a REST API (e.g., Access Control, Building Management, Human Resources, etc.).



The system connects to the building power supply, does not require any batteries, and contributes to a green IT environment.

2 SYSTEM DESCRIPTION

2.1 Overview

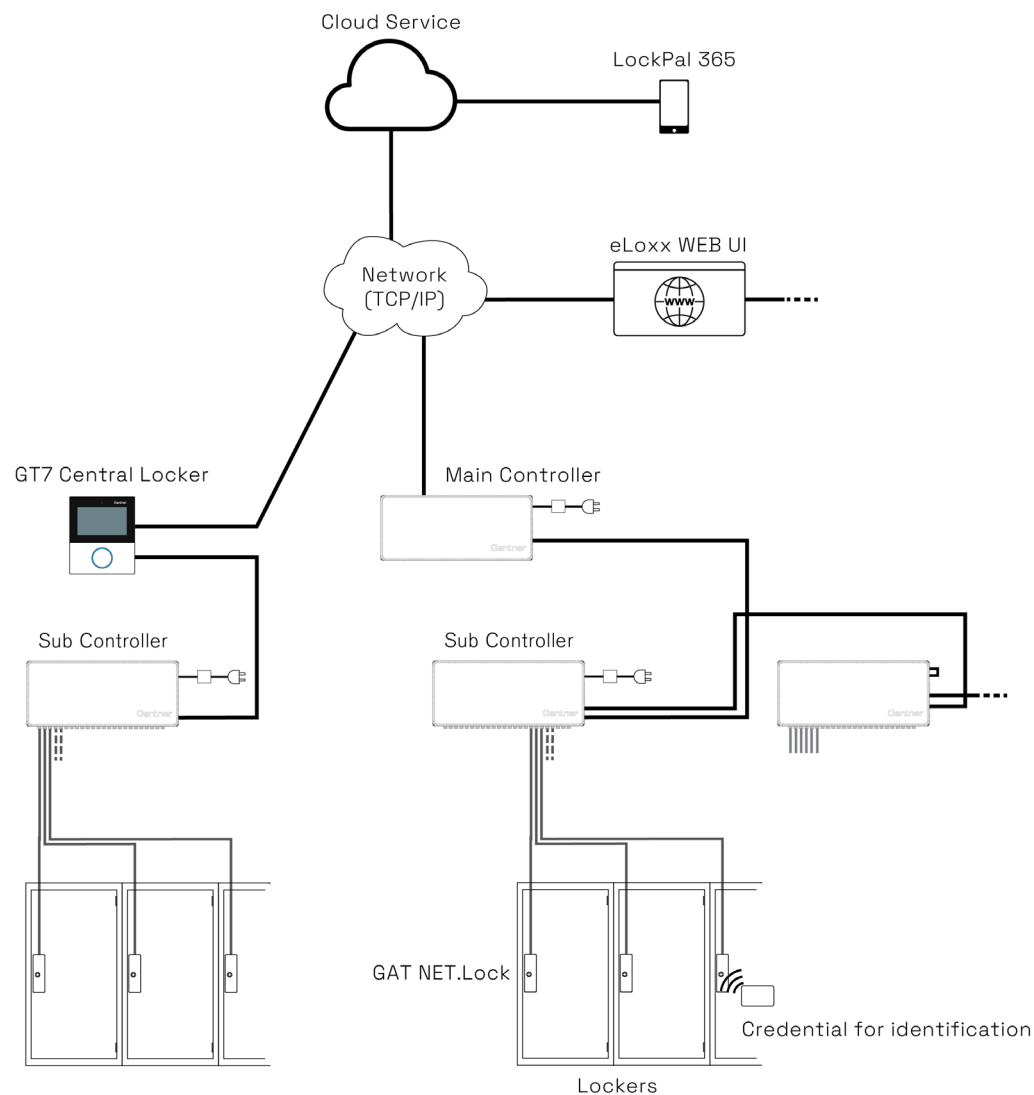


Fig. 2.1 - Structure of the networked locking system

- Each networked locker lock comprises locking mechanics and control circuitry, an integrated RFID data carrier reader, a status LED for user feedback, and a circuit for monitoring the door position (alarm).
- Each GAT NET.Lock is hard coded with a unique serial number and supports live firmware upgrades via its associated sub controller.
- The GAT NET.Lock connects to the sub controller, which can support up to 12 or 24 locks each depending on the model.
- Up to 3 or 8 sub controllers can be interconnected (series link) via an RS-485 network link. Standard network cabling (min. CAT. 5) can be used for these connections.
- Sub controllers are installed in a location near the lockers (max. 5 m cable) and must always be readily accessible for maintenance and inspection. Typical installation locations include suspended ceiling spaces, on top of or beneath the lockers, in a maintenance locker, in raised floor spaces, or in void corners/areas.
- Each sub controller circuit (RS-485) connects to a Gantner main controller, which in turn connects to an Ethernet network.

- When using a GT7 Central Locker device, the sub controller circuit (RS-485) can be connected to the GT7 Central Locker without using a main controller. The GT7 Central Locker is connected to an Ethernet network.
- If main controllers are installed in the nearest secure data communications rack for the floor or area, the client should provide a rack shelf (typically 1 RU) to accommodate the main controllers. Typically, 3 - 4 main controllers can be installed per 1 RU.
- Each main controller requires a network (TCP/IP) connection with internet access.
- The GC7 and GT7 devices communicate with eLoxx 365 via the internet.
- eLoxx 365 is part of Gantner's Enviso cloud platform and is hosted by Amazon Web Services in Ireland.
- Depending on the locker design and layout, Gantner will calculate how many sub and main controllers are required for each project.
- The app LockPal 365 allows locker users to remotely operate their lockers directly via their mobile device, which serves as a key or unique ID for the user.

2.1.1 Information and data characteristics

- Sub controllers store the Unique Identification Number (UID) of each data carrier, e.g., employee credential, which has locked a connected lock plus the UIDs of the master cards.
- Main controllers store locking/unlocking events (log events) and will cache this data in the event of a network or server communication failure.
- Sub controllers communicate authorization requests (lock/unlock) when online and wait for a response from the locker management software sent via the main controller.
- When a sub or main controller is offline and emergency mode is enabled (see "3.5 Controller offline mode"), the controller makes unlocking decisions based on the locally stored data carrier number that locked the locker.
- When a sub controller is offline and emergency mode is enabled (see "3.5 Controller offline mode"), the controller will allow a valid data carrier to lock a locker even though an authorization request is not possible.
- When a sub controller is offline, it will disallow a data carrier from locking a locker only when the same data carrier has already been used to lock another locker connected to the same controller.
- Once communication between the main controllers and eLoxx 365 has been re-established, data from the locker system (log data) is automatically uploaded from the main controllers to the locker management software.

2.2 System architecture

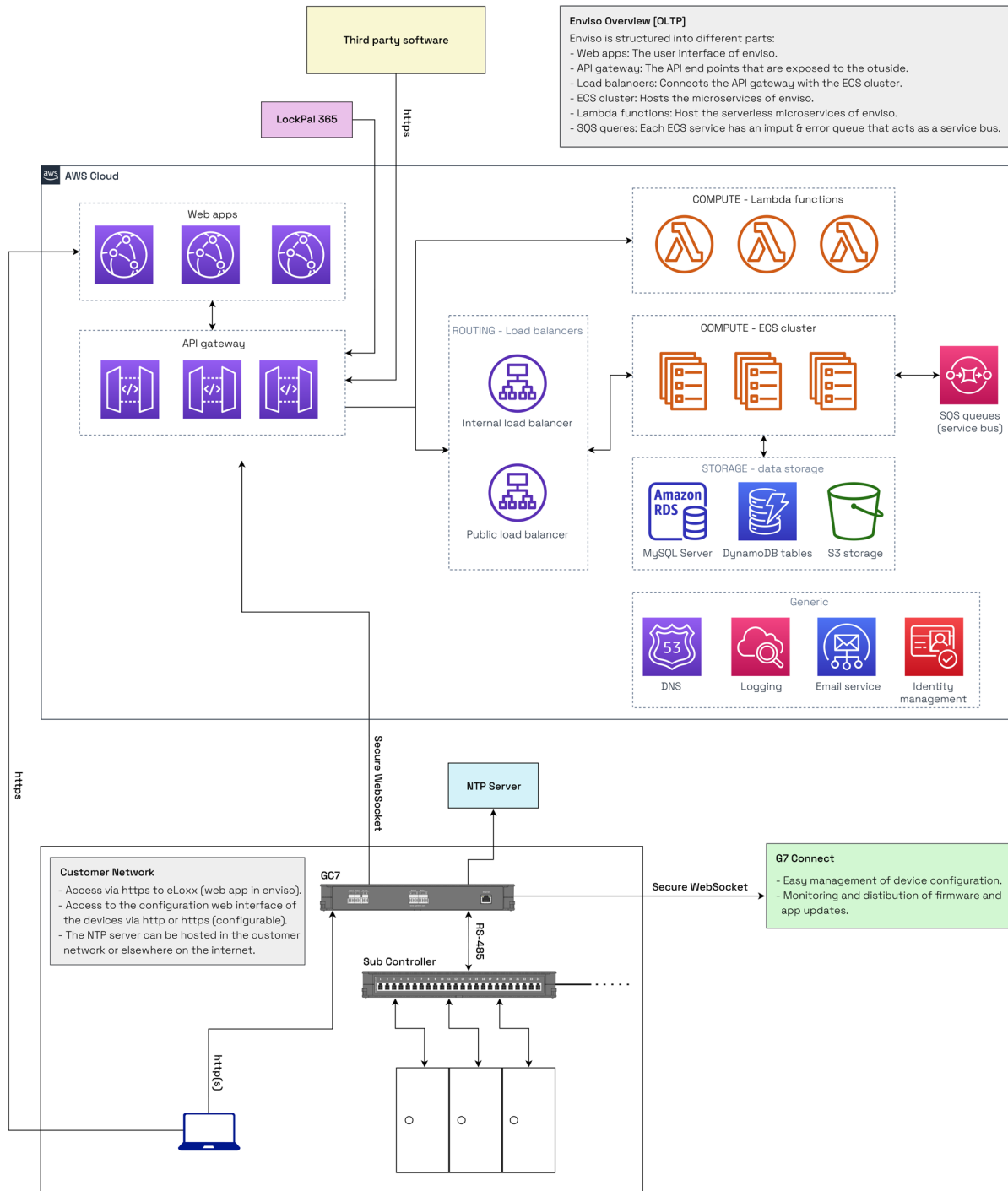


Fig. 2.2 – Architecture of the networked locker system

2.3 Network infrastructure

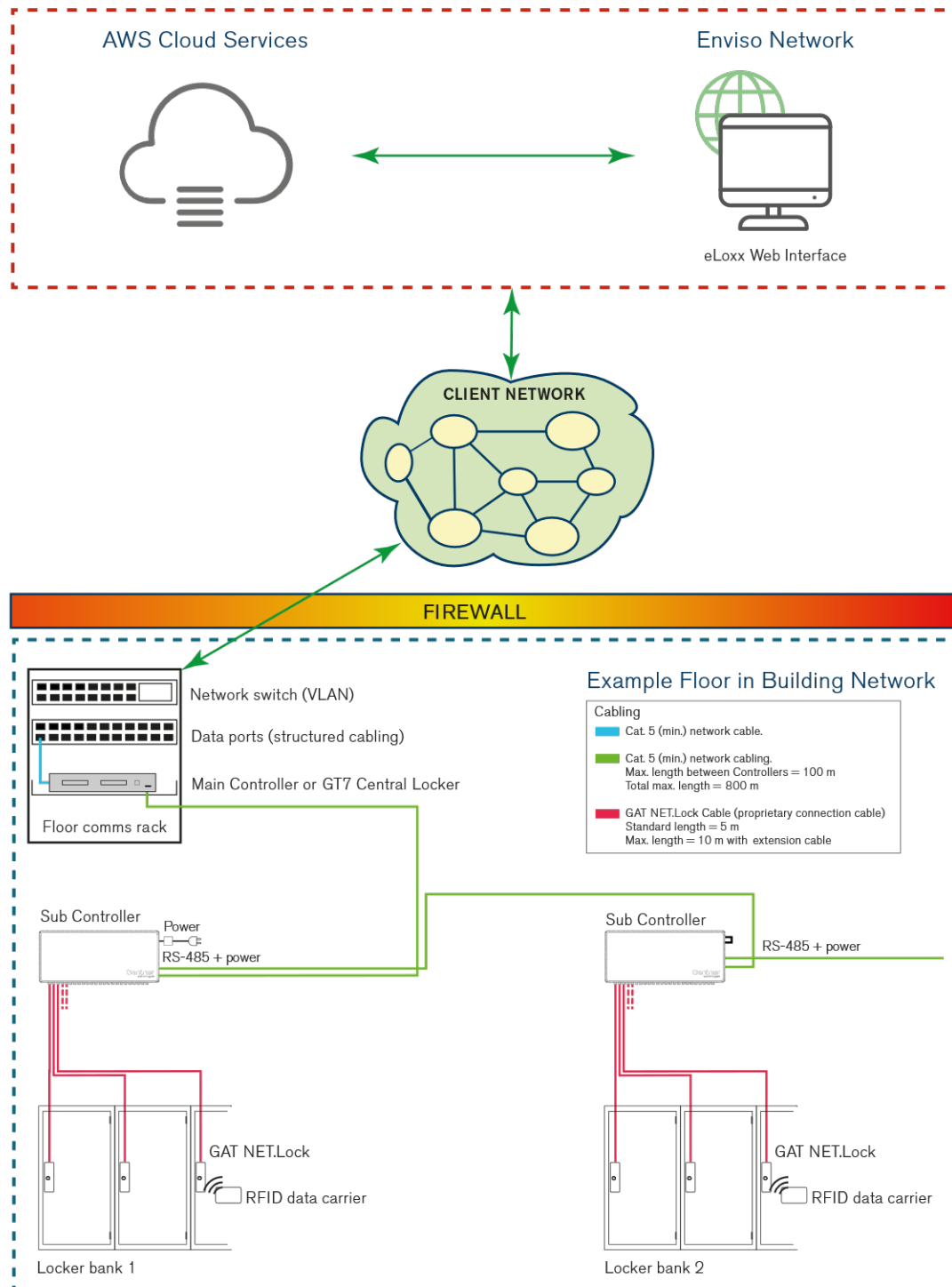


Fig. 2.3 – Example of the networked locker system infrastructure

The Gantner networked locking system is a distributed control system with each lock providing the functions of locking/unlocking of the locker, monitoring of the locker door (alarm/door fault), and reading of the data carriers.

The locks connect to sub controllers, which can support up to 12 or 24 locks each. Sub controllers communicate via an RS-485 serial network meaning that they can be interconnected using standard category 5/6 network cabling. Up to 3 or 8 sub controllers can be interconnected before being connected to a main controller, which converts the RS-485 signal of the sub controllers for communication over a standard Ethernet network.

Sub controllers are installed near the locker banks within the 5 m range (or max. 10 m with extension cable) of the lock cable. To prevent manipulation, the main controllers should be installed in a secure location. Ideally, this is in the nearest data communications rack for the floor or area to which only authorized personnel have access. Structured building cabling is ideally used for the connection between the main controller location and the sub controllers located near the lockers. The main controllers can also be installed near the locker banks depending on the locker layout and client requirements.

Each main controller requires one network connection with internet access. After connecting to the internet, the main controller will then establish a secure WebSocket connection to eLoxx 365 (via the Enviso cloud platform). This connection is encrypted using Transport Layer Security (TLS) 1.2.

2.4 Hardware components

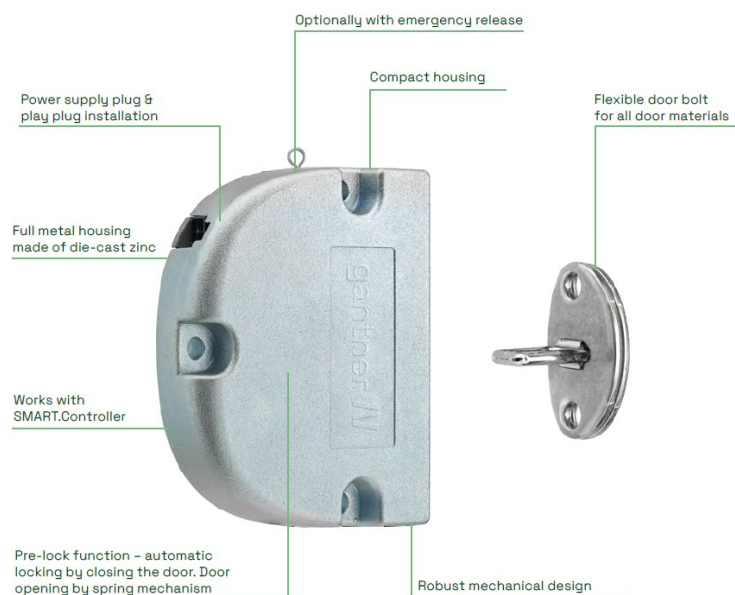
2.4.1 GAT NET.Lock



Dimensions

Width: 100 mm (3.94 in)
Length: 110 mm (4.33 in)
Height: 25 mm (0.98 in)
Weight: 160 g (5.6 oz)

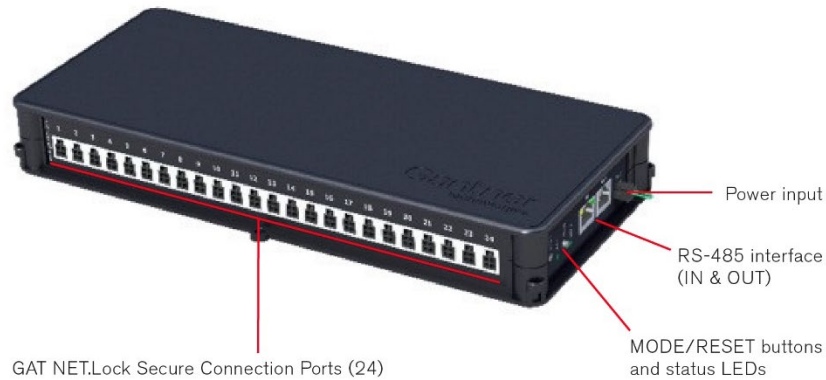
2.4.2 GAT SMART.Lock



Dimensions

Width: 72 mm (2.83 in)
Length: 84 mm (3.3 in)
Height: 18.4 mm (0.72 in)
Weight: 200 g (7.05 oz)

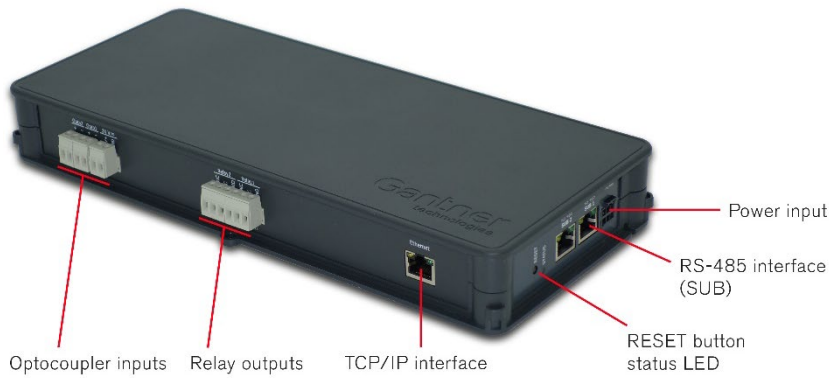
2.4.3 Sub Controller



Dimensions

Width: 133 mm (5.24 in)
Length: 310 mm (12.2 in)
Height: 42 mm (1.65 in)
Weight: 600 g (21.1 oz)

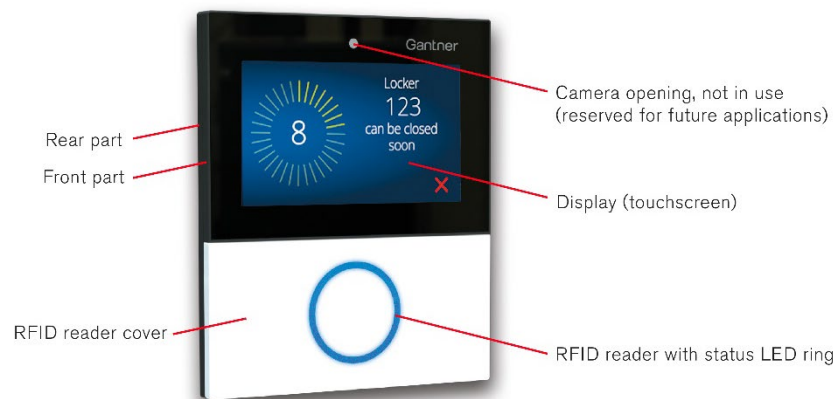
2.4.4 GC7 Main Controller



Dimensions

Width: 133 mm (5.24 in)
Length: 310 mm (12.2 in)
Height: 42 mm (1.65 in)
Weight: 600 g (21.1 oz)

2.4.5 GT7 Central Locker



Dimensions

Width: 127 mm (5 in)
Height: 151 mm (5.95 in)
Depth: 24.7 mm (0.97 in)
Weight: 370 g (13 oz)

2.5 Software components

eLoxx 365 is a locker management software that operates as a SaaS on the Gantner Envisio.io platform. eLoxx 365 provides a user-friendly interface for configuring the hardware components of the locker system, e.g., the locks, controllers, and data carriers, as well as managing the users of the system and assigning lockers. eLoxx 365 can be accessed and operated via all common web browsers. The database for eLoxx 365 is hosted by Amazon Web Services servers located in Ireland.

eLoxx 365 is continually being improved upon with multiple updates per year. Before the update is implemented in the live environment, the staging and production environment is made available for the customer to test the changes.

To begin using the eLoxx 365 application, an account must be created at Envisio.io. The registration process is straightforward, and the customer is advised to create an account themselves to maintain security. Instructions on how to create an account can be found at [Create an eLoxx 365 account | eLoxx 365 Documentation](#). The Gantner Support Team can also assist with this process if required.

After creating an account at Envisio.io, a license for the number of managed locks must be purchased and activated by Gantner. Please contact your Gantner sales representative for more information on the licensing structure of eLoxx 365.

2.5.1 Envisio cloud platform

Once an Envisio account has been created, the Envisio cloud platform can be accessed via any common web browser on a computer or mobile device via the following link: [Envisio Cloud Login](#)

NOTE! Ensure that the latest version of the web browser is used to guarantee optimum performance.

Login is required to access the Envisio cloud platform, and two login methods are supported: using Envisio credentials with two-factor authentication or via single sign-on (SSO) with OpenID Connect (OIDC).

The main operational areas of the Envisio cloud platform can be accessed via the arrow icon at the top of the user interface:

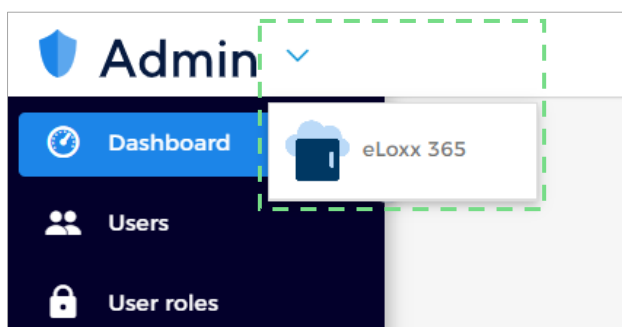


Fig. 2.4 – Envisio cloud platform – Admin

The main operational areas include:

Admin Area

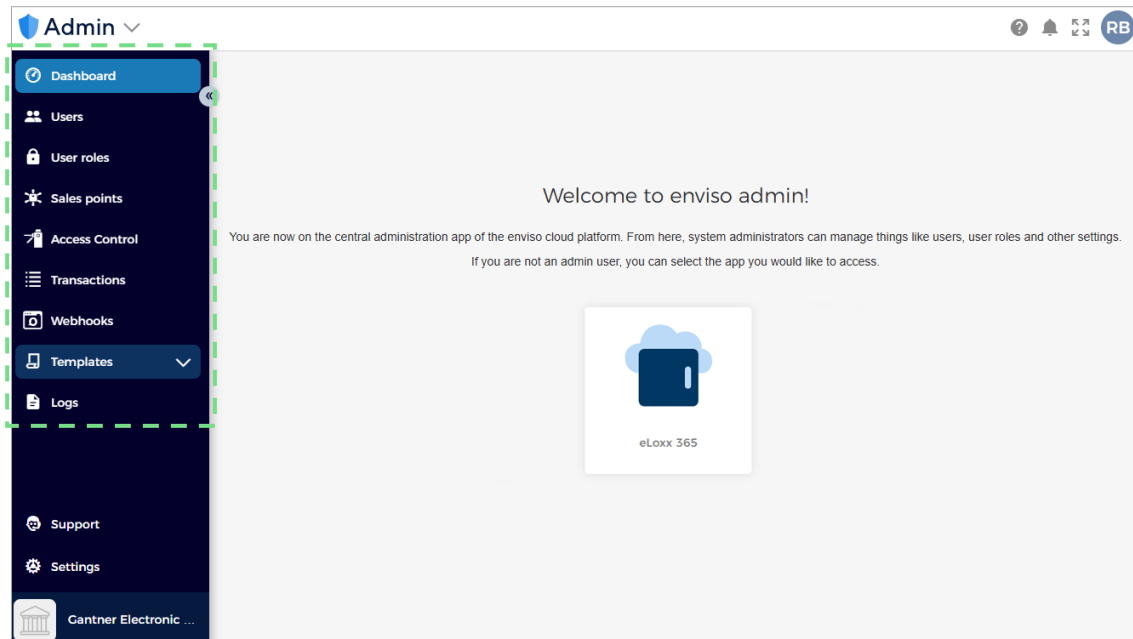


Fig. 2.5 – Enviro cloud platform – Admin area

The various pages of the “Admin” area are displayed via the sidebar to the left, as shown in Fig. 2.5. The apps of the Enviro cloud platform, e.g., “eLoxx 365”, are displayed for selection on the “Dashboard” page.

On the “Users” and “User roles” pages, system administrators can manage the users of the Enviro cloud platform and the user roles that determine the permissions. More information on these topics can be found in chapters “3.1 User management” and “3.2 Role management”.

The “Webhooks” section allows you to configure integrations that listen to system events and send data to external endpoints. You can create, edit, test, and delete webhooks from this interface.

On the “Logs” page, you can consult the activity log of the users using the Enviro apps in your organization. This is for all the tenants - Venues, Resellers, Cities and Locker sites.

The “Settings” page at the bottom of the sidebar allows you to configure various general, regional, and language settings relating to the organization account.

The “Support” page provides legal information as well as contact information in case customer support is required.

eLoxx 365

Similar to the “Admin” area, the different pages of eLoxx 365 are accessed via the sidebar to the left.

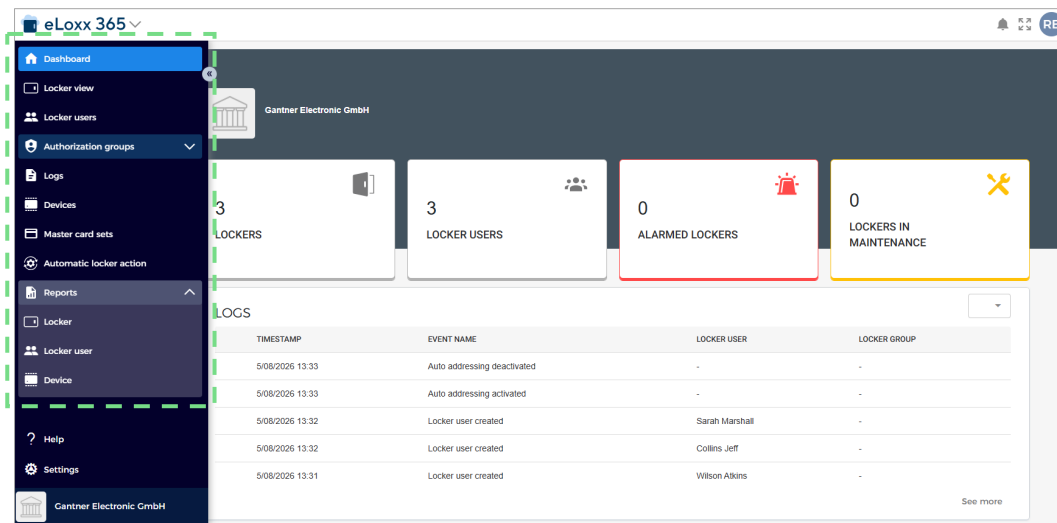


Fig. 2.6 – eLoxx 365 “Dashboard”

On the “Devices” page, all of your organization’s G7 devices and general device information such as the connection status and device IP address, etc., are displayed. New devices can be easily added to the system via the “Add device” button.

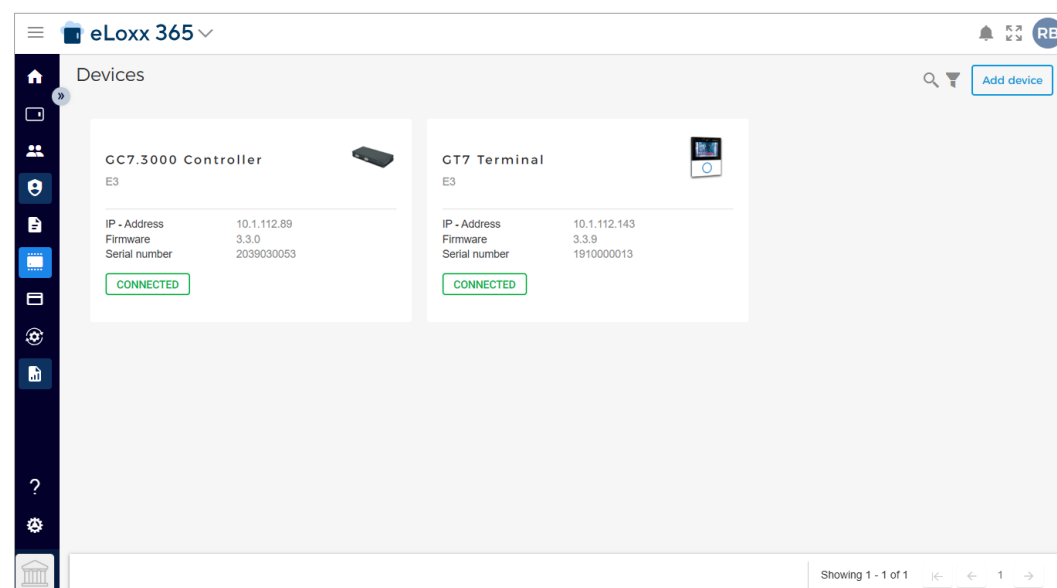


Fig. 2.7 – eLoxx 365 “Devices”

Specific data and settings for each device are displayed after clicking on the device name. Here, you can assign a master card set to the device, see the connected devices, and a link to the device web interface, where all the device settings are available (see “2.5.2 G7 device web interface”), is accessible by clicking on the IP address on the “Device details” page.

Master cards allow the facility manager to access locked lockers in case a user loses their access credential - see chapter “3.4 Master cards” for more information. On the “Master card sets” page, groups of master cards, distinguished by their unique ID number (UID), card can be defined.

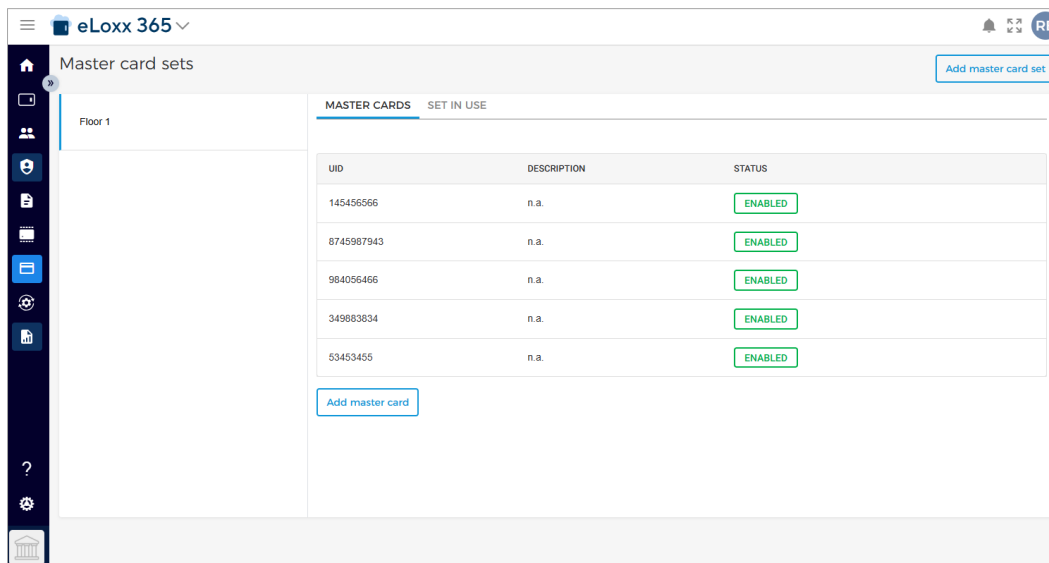


Fig. 2.8 – eLoxx 365 “Master card sets”

A visual overview of each locker is displayed on the “Locker view” page. Thanks to the color-coded backgrounds, here you can see which lockers in the system are currently available or in use at a glance, or where attention is required due to the locker being out of service or where an alarm has been triggered.

The “Locker groups” area on the left displays the structure of the locker system and here you can add new locker groups and assign lockers in a hierarchical way.

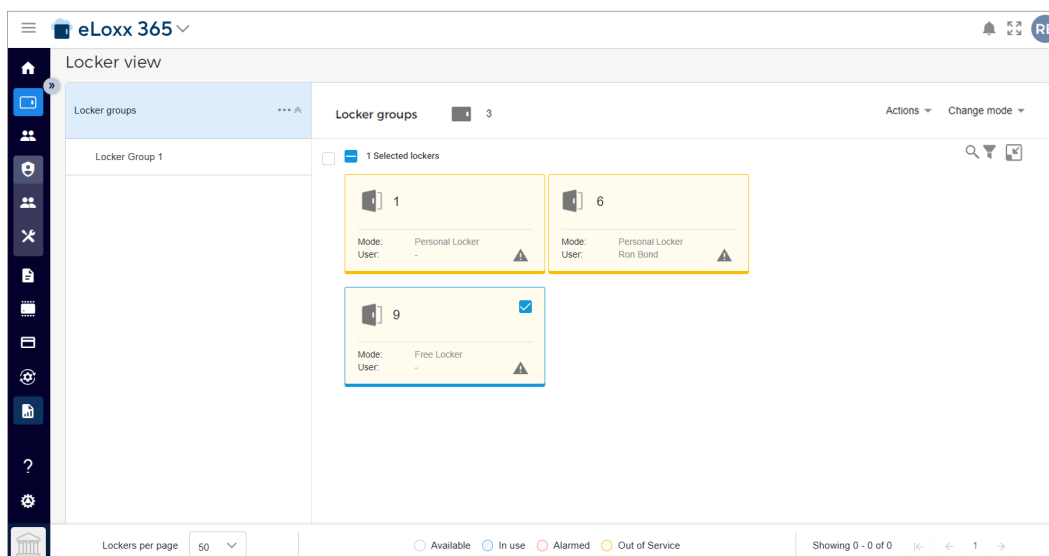


Fig. 2.9 – eLoxx 365 “Locker view”

The locker users in eLoxx 365 refers to the people who are using the lockers to securely store their possessions on a daily basis, e.g., the employees of a company or the members of a fitness club. All current users are displayed on the “Locker users” page in eLoxx 365, and new users can be easily added via the “Add locker users” button.

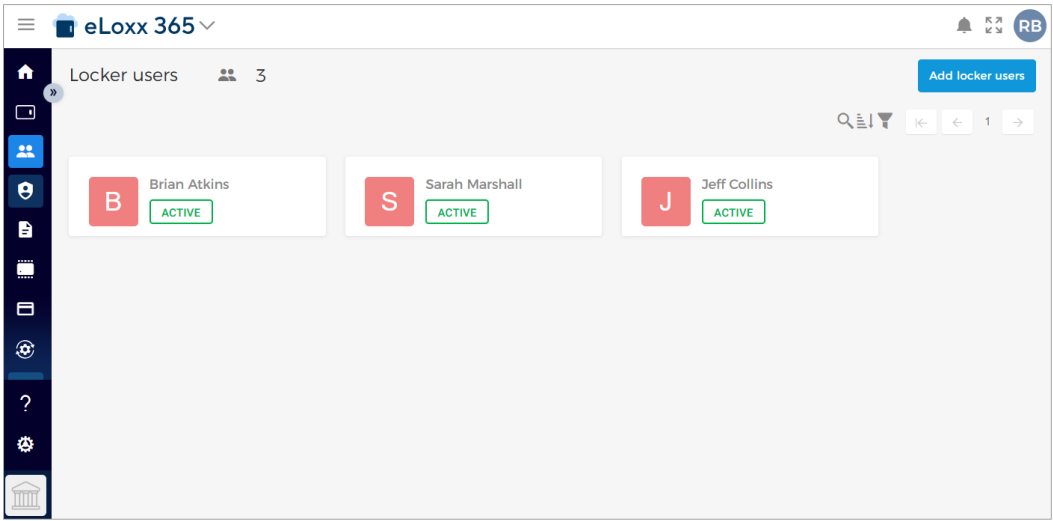


Fig. 2.10 – eLoxx 365 “Locker users”

Additional configuration options and data are shown for each user after clicking on their name. Here, the general data of the user can be edited, and their authorization to use the lockers can be activated and deactivated at the flick of a switch via the “USER STATUS” button. Further key tasks for the user, such as assigning data carriers and lockers as well as assigning the user to authorization groups, are also carried out on this page.

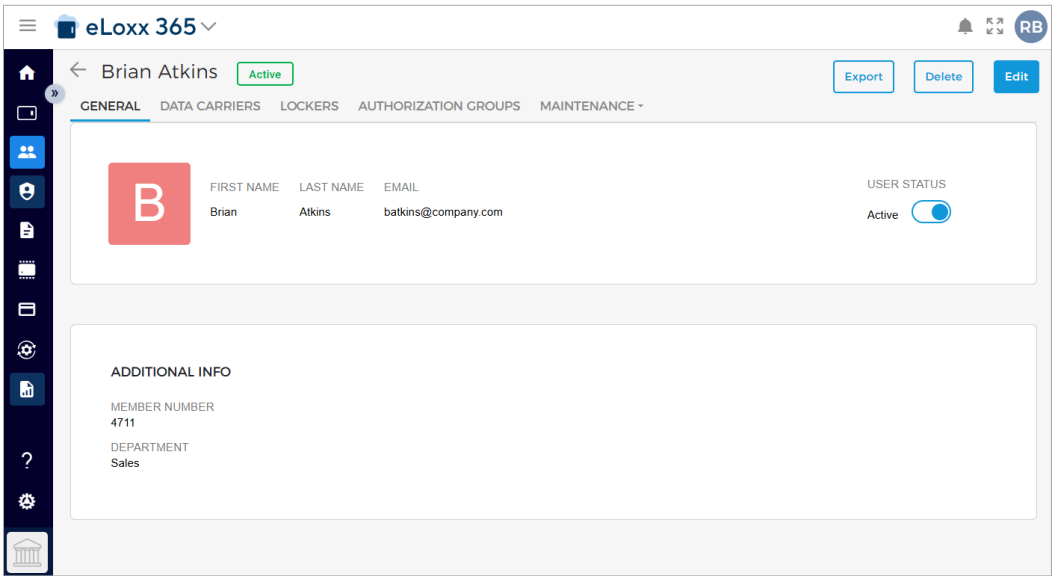


Fig. 2.11 – eLoxx 365 “Locker user”

Authorization groups are used to control how the lockers are used and by whom, and these can be defined on the “Authorization groups” page for locker users and for maintenance purposes.

NAME	NUMBER OF PERSONAL LOCKERS	NUMBER OF DYNAMIC LOCKERS	NUMBER OF FREE LOCKERS	DEFAULT GROUP	SYSTEM-WIDE
Male locker room	1	1	1		
Female locker room	Unlimited	Unlimited	Unlimited		System-wide

Fig. 2.12 – eLoxx 365 “Authorization groups”

For the “Locker user” authorization groups, the key point to note is the difference the three types of operating mode: “free locker” mode, “dynamic locker” mode, and “personal locker” mode. Lockers designated as free lockers can be used by any authorized user provided that the locker is not already in use, which is indicated by a green LED on the lock. After the user has unlocked the locker and is finished using it, it is free to be used by the next person.

Similar to a free locker, any unoccupied dynamic locker can be selected by any authorized user. In contrast however, a dynamic locker remains assigned to the user (via their credential) after they lock the locker for the first time. The locker is then the user’s personal locker from that point on until they decide to release it.

Fig. 2.13 – eLoxx 365 “Edit authorization group”

A locker in personal locker mode can only be locked and unlocked by the locker user assigned to it. You can even assign several locker users to one personal locker. Flexibility is ensured in the creation of authorization groups as all locker modes (free, dynamic, personal) can be used in combination, and the number of lockers that users can occupy in the group can be limited.

A maintenance authorization group can be created and assigned to a locker group or groups to allow maintenance personnel to check and clean the lockers after being used. Different settings are available that define how the lockers behave with the maintenance function.

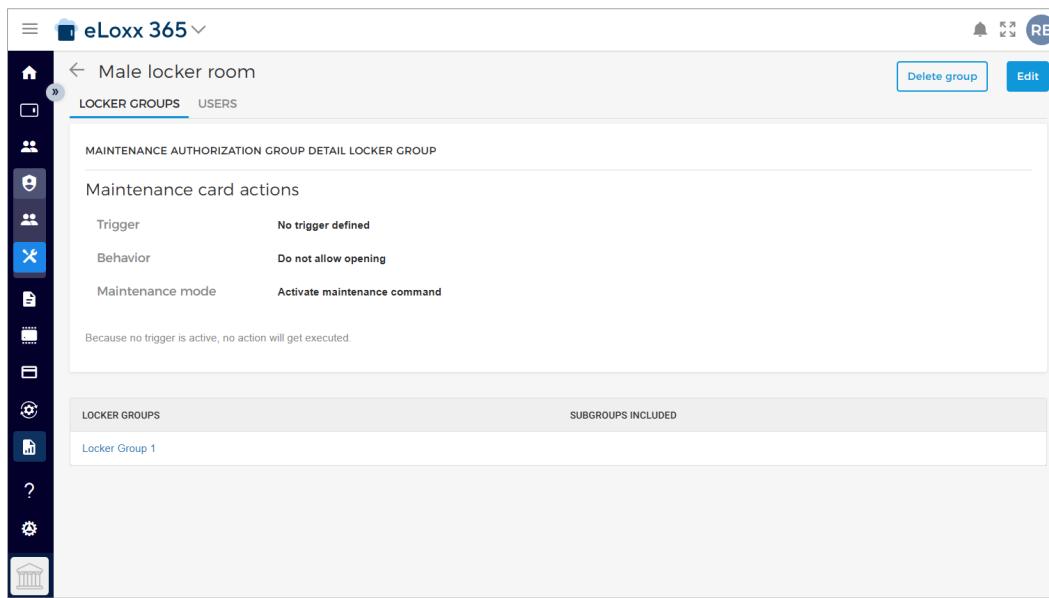


Fig. 2.14 – eLoxx 365 “Maintenance authorization group”

All system activity such as the locking and unlocking of lockers, triggered alarms, and error messages are recorded by eLoxx 365 and available for review on the “Logs” page. More information on this topic is available in chapter “3.3 Logging”. The database can be searched according to specific criteria thereby allowing a specific event, e.g., when an alarm occurred at a locker, to be quickly found.

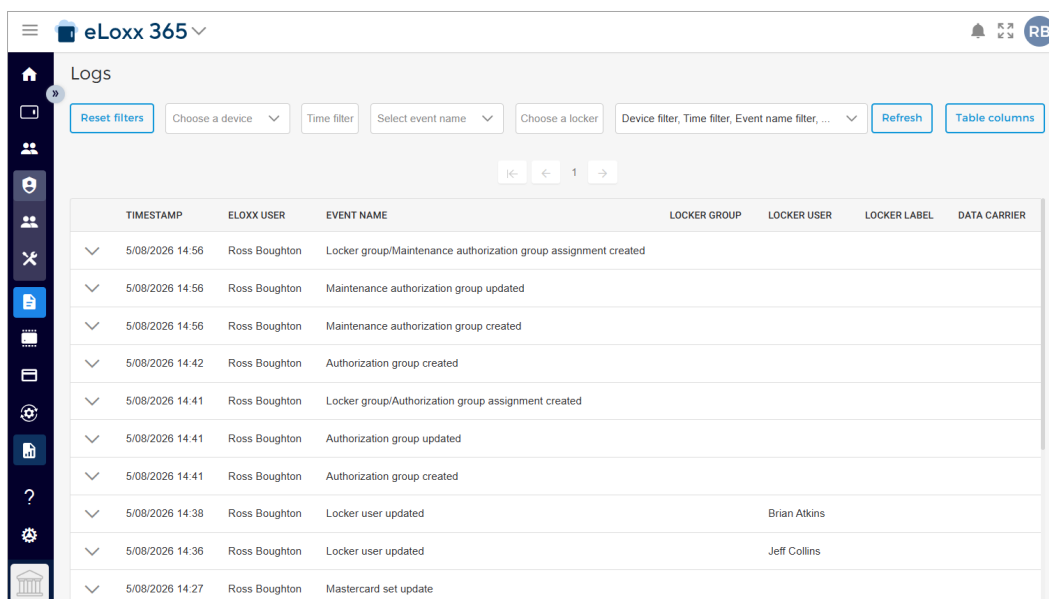


Fig. 2.15 – eLoxx 365 “Logs”

The “Automatic locker action” page in eLoxx 365 allows you to automate locker behavior based on specific triggers and conditions. This helps streamline locker operations and reduces the need for manual management.

The screenshot shows the 'Edit automatic task' page in the eLoxx 365 interface. The page is divided into two main sections. On the left, there is a sidebar with navigation icons and a list of configuration steps, each with a status icon (green checkmark for completed, blue question mark for active). The steps are: Details (Open Locker Task), When action takes place (Usage), With: Select locker group(s) (5 locker group(s) selected), and If: Select locker modes/states (Free Lockers, Only enabled). The right section is titled 'On which condition should an action get started' and contains a table for 'Locker states'.

Locker states*	Yes	No	Both
Locker alarmed	☐	☐	☒
Locker disabled	☐	☒	☐
Locker in use	☒	☐	☐
Locker in maintenance	☐	☐	☒

At the bottom of the page, there are buttons for 'Cancel', 'Previous Step', 'Next Step', and 'Save'.

Fig. 2.16 – eLoxx 365 “Automatic locker action”

Accessible via the “Reports” section in the sidebar are three types of reports that offer detailed visibility into locker infrastructure and user activity. The reports enable you to monitor system performance, identify usage trends, and troubleshoot issues across three key areas:

The screenshot shows the 'Locker Reports' page in the eLoxx 365 interface. The page is divided into two main sections. On the left, there is a sidebar with navigation icons and a list of report types: 'FREE LOCKERS' (selected) and 'PERSONAL/DYNAMIC LOCKERS'. The main content area is titled 'Locker Reports' and contains a section for 'Show reporting data for...'. Below this section, there are three buttons for selecting a time window: '1 Month back', '3 Months back', and '6 Months back'. A note below the buttons states: 'To limit processing time please select a time window below.'

Fig. 2.17 – eLoxx 365 “Locker reports”

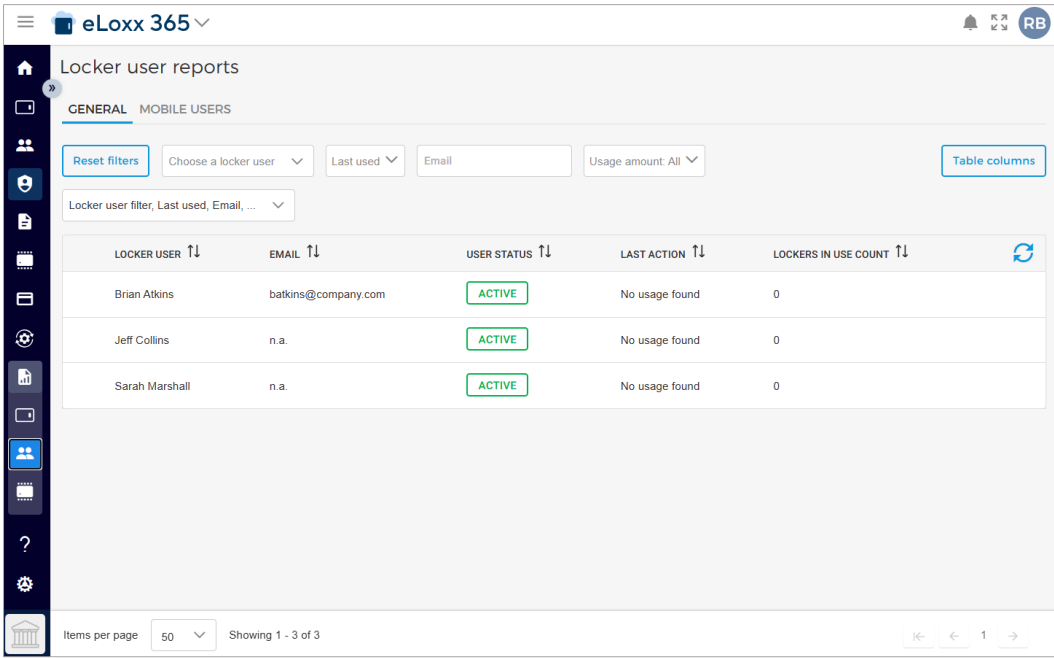


Fig. 2.18 – eLoxx 365 “Locker user reports”

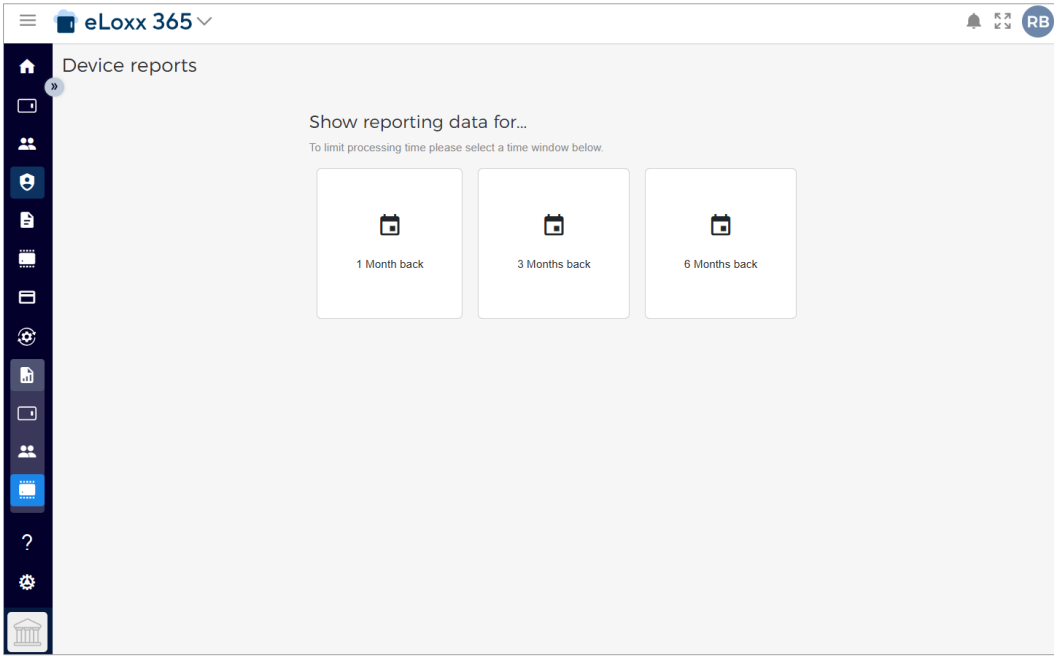


Fig. 2.19 – eLoxx 365 “Device reports”

2.5.2 G7 device web interface

All G7 devices from Gantner include an integrated web interface. Provided that the device is reachable via the network, all settings for the device and the installed apps can be accessed and configured via a web browser. The device web interface is accessed by entering the IP address of the device into the address bar of a web browser.

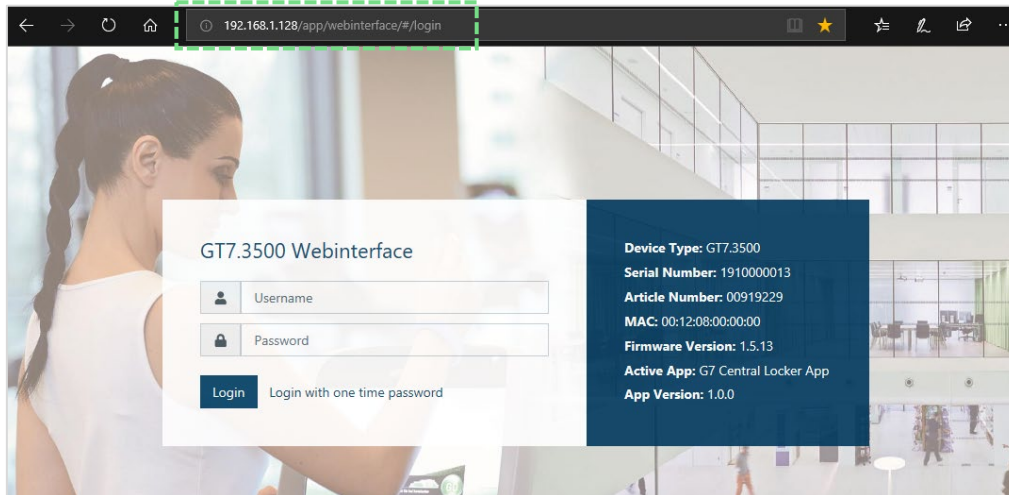


Fig. 2.20 – Login screen of G7 device web interface

After logging in to the Gantner device for the first time using the default login details, the user is prompted to set secure login details to be used for subsequent logins. This step is compulsory and once these details are set, the dashboard of the web interface where all the device settings are available is displayed.

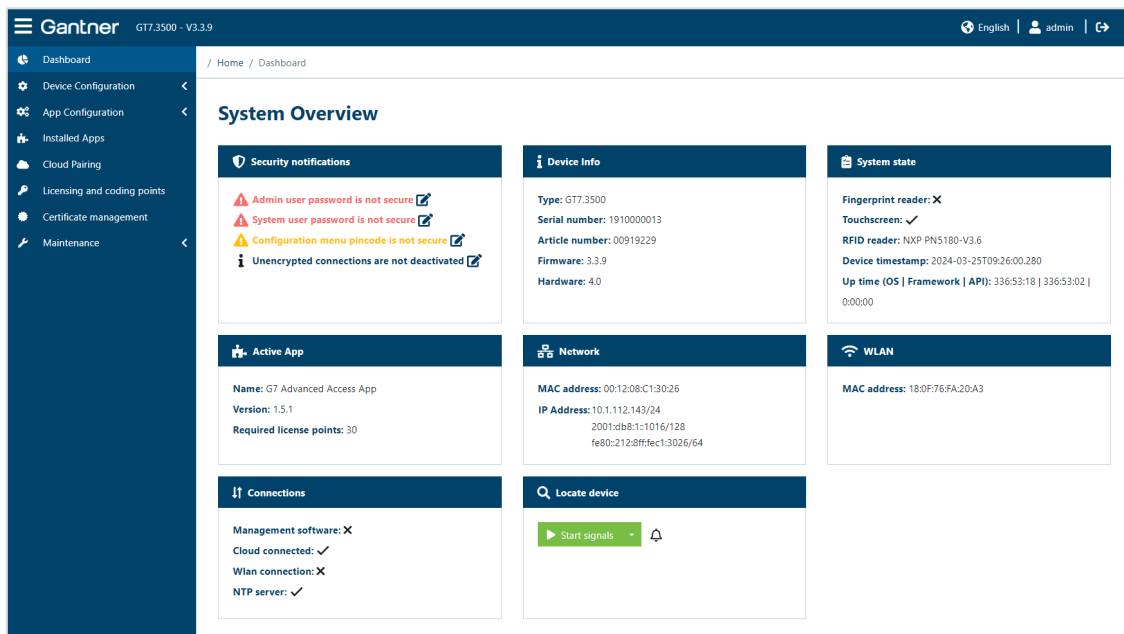


Fig. 2.21 – G7 device web interface

2.5.3 G7 Connect (Gantner Cloud)

G7 Connect is Gantner's cloud platform that provides a clear, user-friendly interface for managing projects that include G7 devices. Similar to the web interface for G7 devices, G7 Connect is accessed via a web browser such as Chrome or Firefox (<https://gantner.cloud>).

The configuration of a G7 device using G7 Connect is also analogous to the configuration via web interface.

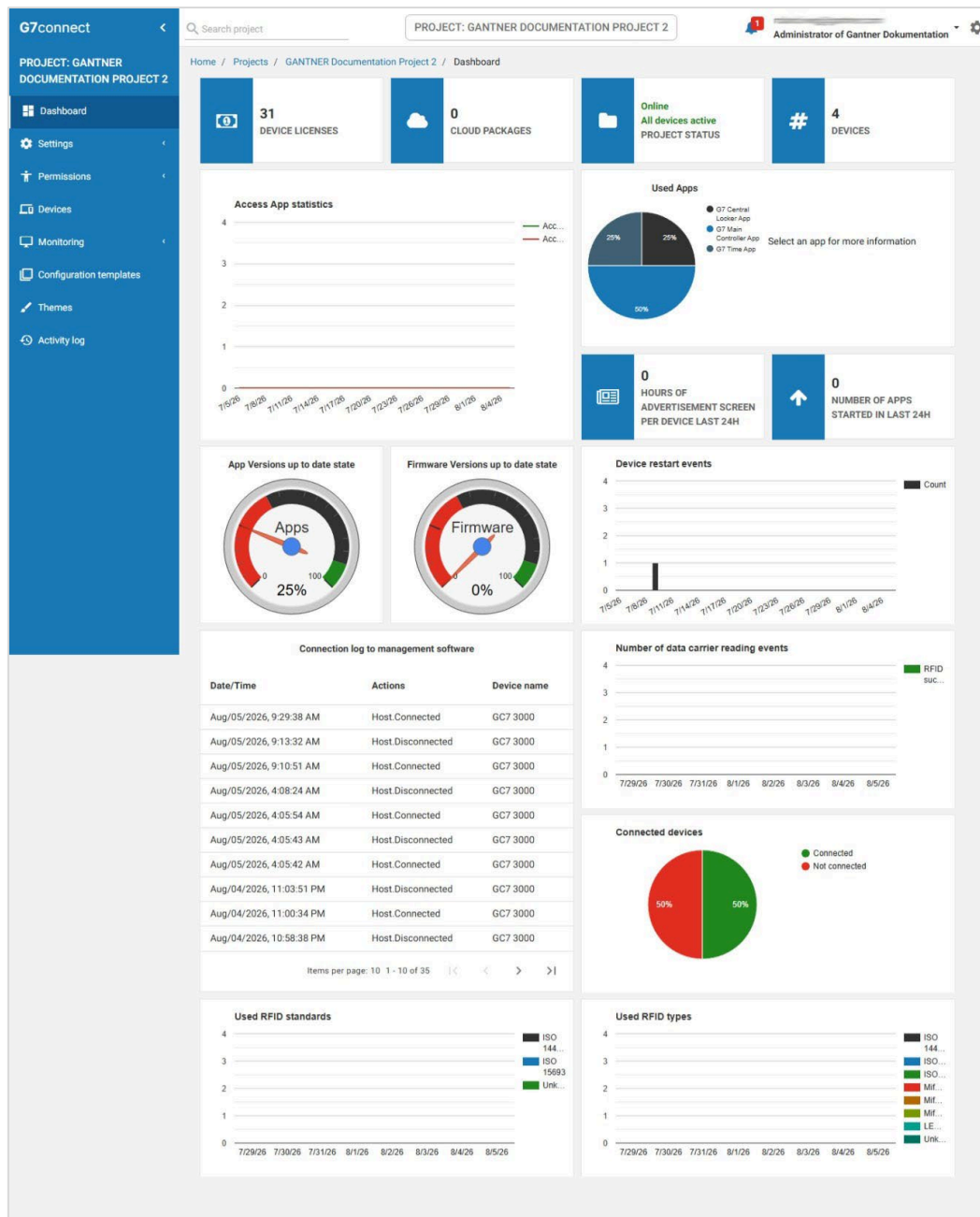


Fig. 2.22 – Project Dashboard of G7 Connect

After opening G7 Connect, the various users, projects, and devices of your organization can be configured and managed. A detailed view is provided on the “Dashboard” page of each project that shows information on the device licenses, cloud packages, used apps, app versions, and also statistics from the current app.

2.6 Access control data carriers

2.6.1 Technology and compatibility

The networked locking system operates using data carriers (employee credentials) based on the 13.56 MHz technology. The following RFID data carrier technologies are compatible with the locking system. For all other technologies, please consult with Gantner.

- MIFARE® (Classic, Ultralight®, and DESFire EV1® / EV2® / EV3®), NFC, ISO 15693
- LEGIC (prime and advant)
- HID (iCLASS, iCLASS Elite, iCLASS Seos)

Compatibility of the client's access control system is subject to analysis and testing. Variables including form factor, multi-cards, different formats, and facility codes can influence the performance of the system. A minimum of three test data carriers (non-assigned) are required to confirm compatibility. Gantner will retain the test data carriers as a reference for the site and for future projects.

For the HID iCLASS Elite program with private keys, the HID Authorization License will be used. The cost of this license is not included in Gantner's scope of supply.

2.6.2 UID, CSN, data carrier number

The system operates using the unique numbers of the data carriers. This number is linked to the locker number in the database in case a locker is locked or assigned to an employee's data carrier.

Many access control data carriers have a pre-programmed number that is usually unique. This number is called the CSN (Card Serial Number) or UID (Unique Identifier). Gantner recommends not to use this pre-programmed number because it may not be unique in rare instances (e.g., the 4-byte ID on current MIFARE Classic cards). But more importantly, this number is not very user friendly, does not link the data carrier to a specific installation, and is most likely not used by the third-party access control system thus making integration difficult.

Gantner recommends to always use the facility code and the programmed data carrier number in the secure memory area. With the facility code configured in the locking system, only data carriers with the correct facility code linked to the installation can be used in the system. Data carriers with other facility codes are ignored.

The term 'facility code' has some equivalents in the access control industry: site code, client code, country code, customer code, etc., are all used to refer to this function.

3 SECURITY & MANAGEMENT

3.1 User management

Each user of eLoxx 365 has their own user account within the Envisio cloud platform, for which there are three login methods available (see “6.2.13 Which login methods are possible with eLoxx 365?”). The login details must be kept private in order to prevent the misuse of the user accounts via invalid login. All users in eLoxx 365 are assigned to one or more roles that define their rights in the system. (see “3.2 Role management” for more information). Each user with full control of the user management can add new users and assign them to an initial role, which is carried out on the “Users” page of the “Admin” area.

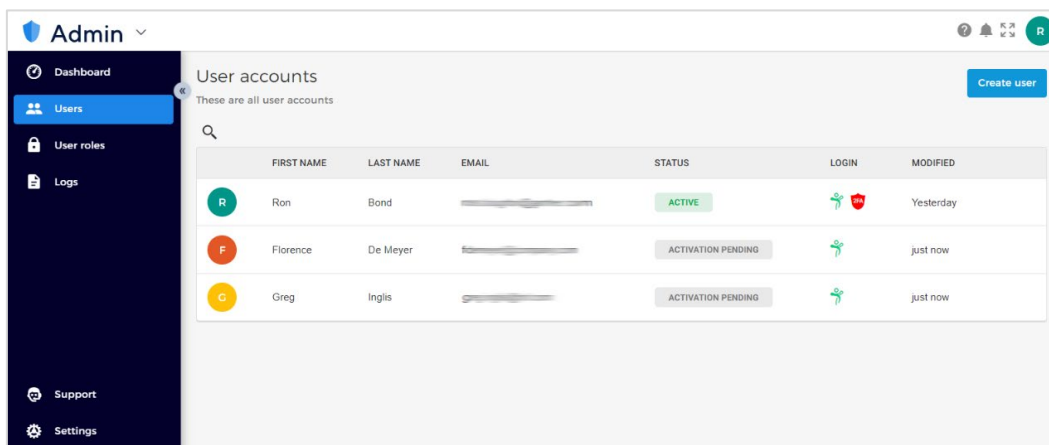


Fig. 3.1 – Envisio Admin - “Users” page

The first user that registers a new organization/tenant in Envisio is automatically assigned to the Envisio Super Admin role, which grants the user full control for all Envisio functions. This user is also the tenant owner and accepts the Terms of Service. It is possible to change the tenant owner. This process can be started either by the tenant owner, by selecting another Super Admin and select “Transfer ownership” in the 3-dot menu, or by the future tenant owner by selecting their own user and clicking on “Take ownership” in the 3-dot menu. In both cases the other affected user will receive in email. In the first case, the new tenant owner can accept the ownership on the next login and by this accepts the Terms of Service. In the second case, the current tenant owner must agree to transfer ownership.

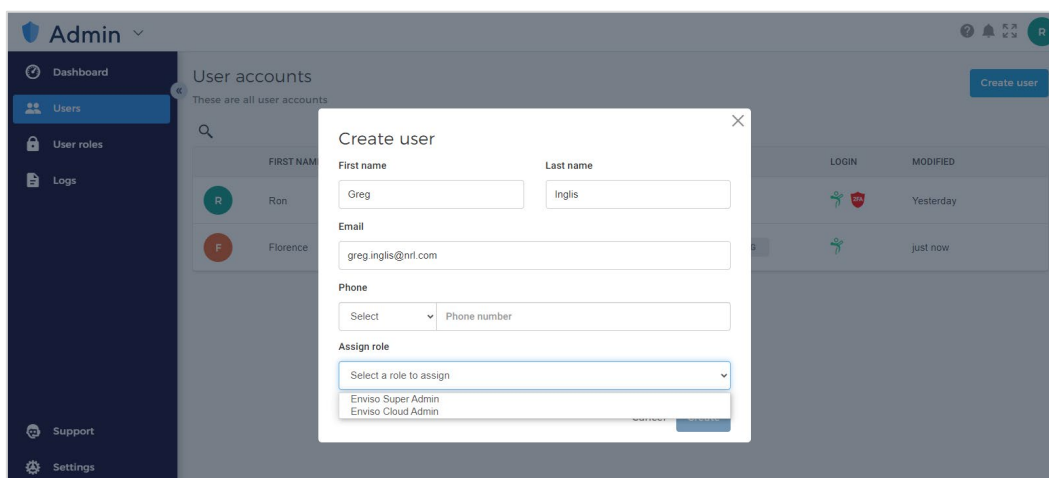


Fig. 3.2 – Envisio Admin – Creating a new user

The new user receives an automatically generated email that they must confirm before defining a password and completing the registration themselves.

3.2 Role management

The Enviro platform offers the possibility to assign individual users with distinct levels of system control, which is done using a role-based system and defined on the “User roles” page of the “Admin” area.

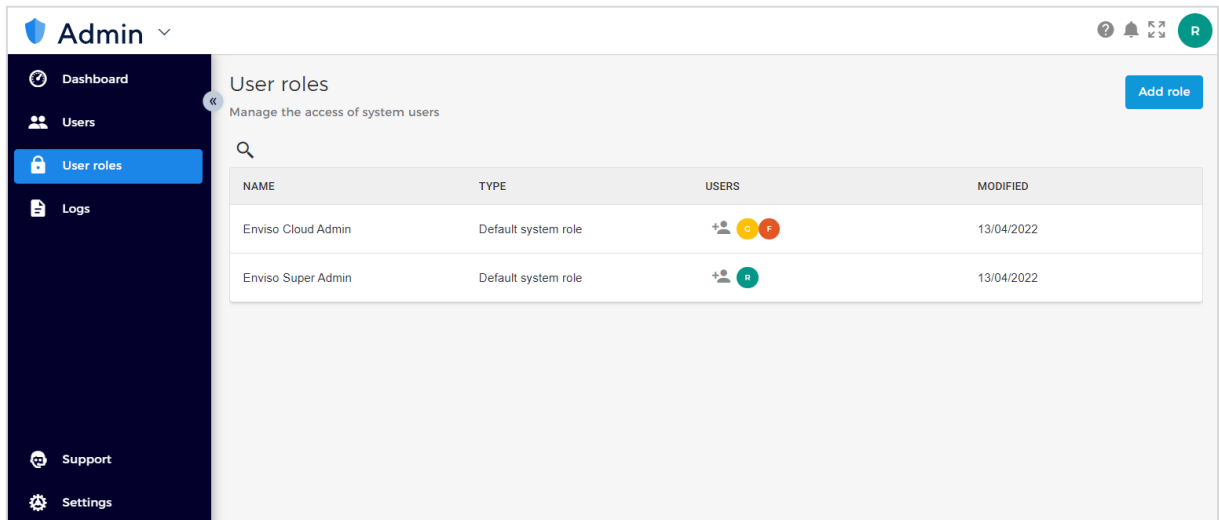


Fig. 3.3 – Admin area – User roles

Each user is assigned to one or more roles with the user's system control being inherited from their role. A role represents a collection of rights to complete certain functions within the locker system and for user administration, i.e., in the “eLoxx 365” and “Admin” areas of Enviro. There are two default roles for Enviro users:

1. Enviro Super Admin
2. Enviro Cloud Admin

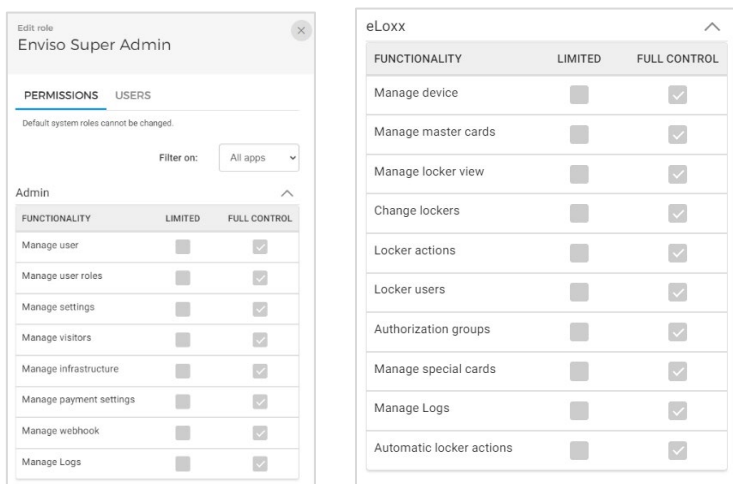
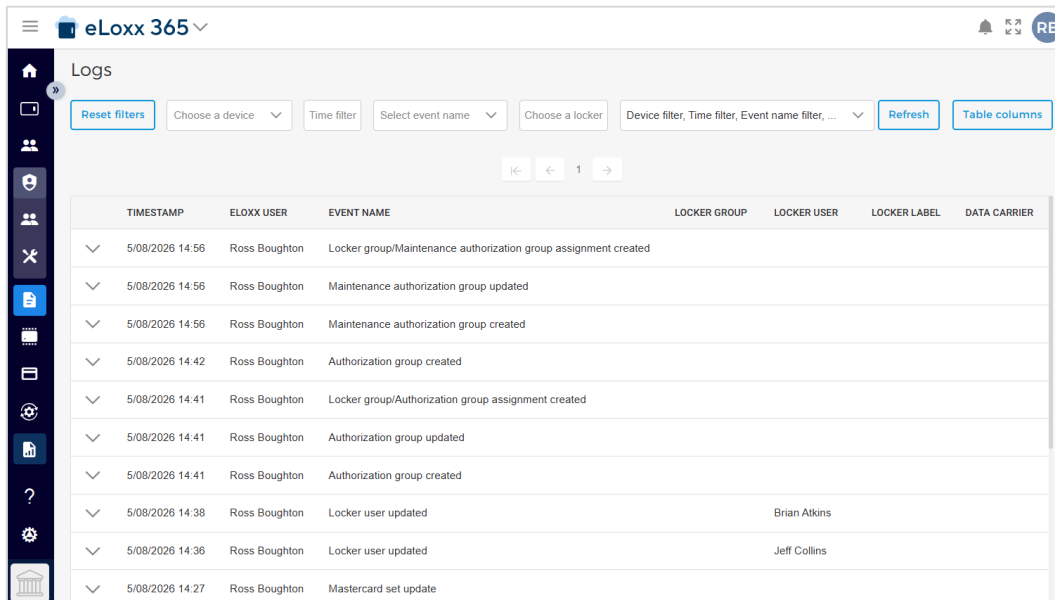


Fig. 3.4 – Settings for “Enviro Super Admin” role

For each functionality, a role can be assigned to full control, limited control, or no control. Roles that are assigned full control for the “Manage user roles” option are allowed to manage roles. In addition to the three default system roles, Enviro allows the creation of client-specific user roles, which are displayed as the type “User created role” on the “User roles” page.

3.3 Logging

Each locker event and user action, such as the locking and unlocking of lockers and the reading of user credentials, is logged in eLoxx 365. The logged events can be analyzed in eLoxx 365 via the “Logs” page. The logging system creates a complete audit trail that allows all changes and activity in the locker system to be tracked.

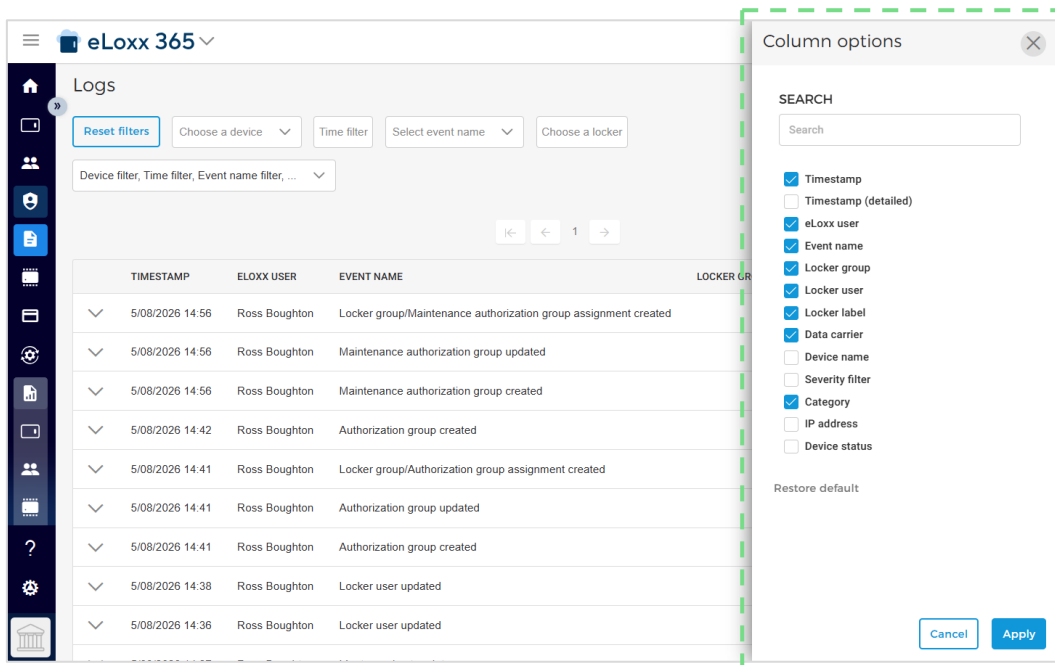


The screenshot shows the 'Logs' page in the eLoxx 365 interface. It features a sidebar with navigation icons, a top navigation bar with the eLoxx 365 logo and user profile, and a main content area. The main area has a 'Logs' title, a 'Reset filters' button, and several filter dropdowns: 'Choose a device', 'Time filter', 'Select event name', 'Choose a locker', and a combined 'Device filter, Time filter, Event name filter, ...'. There are also 'Refresh' and 'Table columns' buttons. Below the filters is a table with the following columns: TIMESTAMP, ELOXX USER, EVENT NAME, LOCKER GROUP, LOCKER USER, LOCKER LABEL, and DATA CARRIER. The table contains 10 rows of log entries.

TIMESTAMP	ELOXX USER	EVENT NAME	LOCKER GROUP	LOCKER USER	LOCKER LABEL	DATA CARRIER
5/08/2026 14:56	Ross Boughton	Locker group/Maintenance authorization group assignment created				
5/08/2026 14:56	Ross Boughton	Maintenance authorization group updated				
5/08/2026 14:56	Ross Boughton	Maintenance authorization group created				
5/08/2026 14:42	Ross Boughton	Authorization group created				
5/08/2026 14:41	Ross Boughton	Locker group/Authorization group assignment created				
5/08/2026 14:41	Ross Boughton	Authorization group updated				
5/08/2026 14:41	Ross Boughton	Authorization group created				
5/08/2026 14:38	Ross Boughton	Locker user updated		Brian Atkins		
5/08/2026 14:36	Ross Boughton	Locker user updated		Jeff Collins		
5/08/2026 14:27	Ross Boughton	Mastercard set update				

Fig. 3.5 – eLoxx 365 “Logs” page

The data displayed in the table can be configured by selecting or deselecting the column options.



The screenshot shows the 'Logs' page with the 'Column options' dialog box open. The dialog has a 'SEARCH' field and a list of checkboxes for selecting or deselecting columns. The columns listed are: Timestamp, Timestamp (detailed), eLoxx user, Event name, Locker group, Locker user, Locker label, Data carrier, Device name, Severity filter, Category, IP address, and Device status. The 'Timestamp', 'eLoxx user', 'Event name', 'Locker group', 'Locker user', 'Locker label', and 'Data carrier' checkboxes are checked. The 'Timestamp (detailed)', 'Device name', 'Severity filter', 'Category', 'IP address', and 'Device status' checkboxes are unchecked. There is a 'Restore default' link and 'Cancel' and 'Apply' buttons at the bottom of the dialog.

TIMESTAMP	ELOXX USER	EVENT NAME	LOCKER GROUP	LOCKER USER	LOCKER LABEL	DATA CARRIER
5/08/2026 14:56	Ross Boughton	Locker group/Maintenance authorization group assignment created				
5/08/2026 14:56	Ross Boughton	Maintenance authorization group updated				
5/08/2026 14:56	Ross Boughton	Maintenance authorization group created				
5/08/2026 14:42	Ross Boughton	Authorization group created				
5/08/2026 14:41	Ross Boughton	Locker group/Authorization group assignment created				
5/08/2026 14:41	Ross Boughton	Authorization group updated				
5/08/2026 14:41	Ross Boughton	Authorization group created				
5/08/2026 14:38	Ross Boughton	Locker user updated		Brian Atkins		
5/08/2026 14:36	Ross Boughton	Locker user updated		Jeff Collins		
5/08/2026 14:27	Ross Boughton	Mastercard set update				

Fig. 3.6 – Configuring the data displayed on the “Logs” page

3.4 Master cards

Master cards allow the facility operations and security departments to access locked lockers if an employee loses their access credential. A master card must also be used to acknowledge an alarm at the locker thus ensuring that the operations/security team investigates the cause of the alarm at the locker.

Master cards share the same technology as the standard data carriers but have special rights assigned to them. They are stored on each main and sub controller and can lock and unlock any locker controlled by the main controller without limitations, even when eLoxx 365 is not reachable. It is therefore paramount to store the master cards in a secure place. The use of master cards is recorded in the log database, and this data can be searched for and analyzed in eLoxx 365.

NOTE! The system operator is responsible for ensuring that the master cards are stored in a secure location and are not misused.

Each main controller is assigned a set of max. 10 master cards. For larger systems, several master card sets can be defined and assigned to the corresponding main controllers (e.g., one set per floor or building). The UID of the master cards are stored in the eLoxx 365 management software, the main controllers, and the sub controllers, thereby allowing their use during system shutdown or network failures.

3.5 Controller offline mode

The networked locking system is designed for fail-safe operation. This means that if the connection to the server is not available, the main controller will assume responsibility for authorization checks and logging. If the main controller fails, the sub controller will assume responsibility for authorization checks and logging. This automatic hierarchical assignment of control ensures that the locker users (e.g., an employee) do not notice any failures in the network and the locker operation continues as normal. Different settings can be configured to determine how the controllers manage requests while in offline mode.

The controllers will attempt to re-establish communication at configurable intervals, e.g., every 30 seconds. As soon as communication is re-established, the main controllers switch back to normal mode and send all log data that was logged during offline mode to the eLoxx 365 management software.

NOTE! In this manual, Controller Offline Mode does not refer to Controller Offline Application, which is a function available for locker systems that use MIFARE or LEGIC technology.

3.6 Essential power circuits / UPS

The networked locking system uses instantaneous power to lock and instantaneous power to unlock, which is provided by the sub controller. Should a mains power failure occur in the building, the locks remain in their last state and resume normal operation once power returns.

We recommend connecting the system to essential power circuits, so lockers can be used during a mains power failure. For installations where a generator-backed essential power supply is not available, we recommend that dedicated power circuits suitable for the inclusion of, or connection to, a battery-backed uninterruptible power supply (UPS) be installed for locker controllers.

Calculate the total power consumption allowing 5 VA per controller with all 24 locks connected. Gantner suggests selecting a UPS with a battery backup time of at least 60 minutes for the calculated total power consumption.

Example:

1 x main controller	1 x 5 VA = 5 VA
6 x sub controllers (144 locks)	6 x 5 VA = 30 VA
Total power consumption	35 VA

Select a UPS that can deliver the 35 VA power for at least 60 minutes during a mains power failure.

NOTE! Some UPS providers offer online selection tools. A sample selection tool is available via the following link.

http://www.apc.com/tools/ups_selector/psor/rslr/by_load.cfm?location_type=home

4 SYSTEM ADMINISTRATION

4.1 Remote access

Remote access to the G7 devices is provided via the device web interface (see "2.5.2 G7 device web interface"), which can be accessed via a web browser using the device's IP address. Access to the network on which the devices are connected is required.

For remote access to the eLoxx 365 software to be possible, e.g., for support or remote configuration, access to the Envisio website (<https://cloud.enviso.io>) must not be blocked, e.g., by a firewall, etc.

This requirement for remote access also applies for accessing the project(s) of your organization in G7 Connect, i.e., access to the G7 Connect website (<https://gantner.cloud>) must not be blocked.

4.2 Firmware updates

Gantner releases updates for the firmware and apps of the G7 devices several times per year. The updates can be loaded to the devices via the web interface of the G7 device (see "2.5.2 G7 device web interface") or via G7 Connect (see "2.5.3 G7 Connect (Gantner Cloud)").

Refer to the respective device manual for instructions on updating the firmware.

4.3 Antivirus software and firewall

The following ports are used for communication and must not be blocked by a firewall.

- 123 (TCP/UDP, Outbound): NTP time server that the G7 devices use to synchronize the time.
- 443 (TCP, Outbound): Communication between the G7 devices and the eLoxx 365 software.

The following URLs must be connectable for outbound connections.

- Gantner devices used in the system should be able to connect to: <https://socketapi.enviso.io/>
- eLoxx 365 users should be able to open: <https://eloxx365.enviso.io>

5 ABOUT GANTNER

Gantner is the inventor of the most widely used networked locking system for the corporate office industry around the world. With over 35 years' experience in the design, development, and manufacturing of electronic locking systems, Gantner offers its clients not only cutting-edge technology, but also global partnerships with locker and furniture manufacturers with whom we collaborate to produce custom-made solutions. Gantner is part of the Salto WECOSYSTEM group of companies.

Made to meet the highest European environmental and quality standards, the entire production of the networked locking system is environmentally friendly and completed within the European Union. All components are developed and manufactured under **ISO 14001 / ISO 9001** Environmental and Quality Management conditions. The networked locking system is produced according to Green IT standards, which translates to requiring minimum to no maintenance during utilization and ultra-low energy consumption.

ISO 27001 is the leading international standard focused on information security and comprises a set of requirements for defining, implementing, operating, and improving an Information Security Management System (ISMS). On a yearly basis, Gantner has successfully completed the ISO 27001 certification carried out by external auditors from TÜV Rheinland. Our Cybersecurity Policy Framework defines the mandatory controls that protect our information, systems, products, and operations worldwide. Built on ISO 27001:2022 and ETSI IoT standards, it ensures that security is embedded into how we work, design, and operate every day.

5.1 Warranty and system support

The networked locking system is covered by a standard one-year warranty with the option to extend the warranty for up to 5 years. The warranty includes all hardware components, software updates, bug fixes, and patches.

In addition to the documentation (manuals, datasheets, etc.) available for each device or software application, Gantner will supply a project-specific operations and maintenance manual in electronic format that includes all project-specific drawings, information, datasheets, and manuals.

Support for the system is provided by the Gantner Support Team. The Support Team's competence is ensured by the combined 25+ years of knowledge on the intricate workings of Gantner's hardware and software products. System support is provided during standard business hours in English and German with an 8-hour response time guaranteed. A customer specific support contract is available upon request.

Opt-in Support

The Envisio platform also offers opt-in support for 24/7 assistance with the Envisio apps including eLoxx 365. Opt-in support is enabled and configured in the "Admin" area.

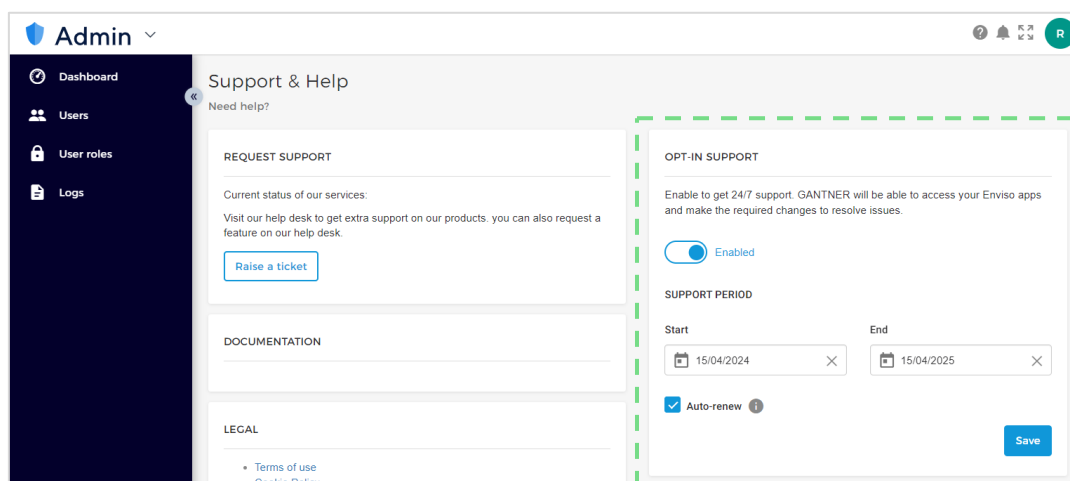


Fig. 5.7 – Envisio "Support & Help"

Based on your specific needs, you can define the support period for a minimum of 2 hours to a maximum of 1 year. By default, the end date is set to one year from the start date, and the option to auto-renew is enabled. This means, by default, the support period will auto-renew each year.

You can disable auto-renew if you do not wish the support period to be renewed automatically. The Admin user will receive two reminder emails shortly before the support period is due for renewal.

5.2 Client training

Gantner Electronic GmbH offers the Gantner Academy, an educational department responsible for client training and knowledge expansion through a series of courses, interactive workshops, and online webinars.

The Gantner Academy draws upon the expertise of sales, product management, research and development, and industry partners to deliver courses that educate clients on our latest products, projects, and other important developments, all aiming to strengthen organizations and individuals.

Each training course is designed to provide attendees with the confidence and knowledge to make informed decisions on behalf of their organization. For each project, Gantner provides project-specific training courses either as remote training or training on-site.

5.3 Software development standards

Gantner's Software Research & Development Department uses the latest technologies and tools to achieve optimal security standards for software applications. The security principles have been taken from the previous edition of the OWASP Development Guide and normalized with the security principles outlined in "*Writing Secure Code*" by Howard and LeBlanc.

Agile development

Our software development process is agile. In an agile development, the development team is careful to ensure that security issues are not ignored in an effort to meet deadlines.

Source code protection

Obfuscation technologies are used to prevent the source code of our applications from being read. This technology is well proven, especially for .NET applications. Therefore, we use external tools from a well-known software producer.

Manipulation protection

To prevent components of the application from manipulation, we use signed components. This means that our components and libraries are signed using a unique key. If a component of the application is exchanged with a foreign component, it is detected and not trusted.

External interface protection

To prevent attacks to external interfaces, we use the latest technologies such as challenge-response authentication and approved encryption.

Software testing

Gantner's Quality Assurance Department is responsible for testing our applications during development before software updates are released. This not only ensures that the functionality is performing as described but also that our stringent security requirements are met.

5.4 Client security assessments

Gantner places a high value on client security and the security of our systems generally. Should you require specific information in addition to that supplied in this manual, or if you need our assistance in completing a security risk assessment relating to the networked locking system, Gantner has resources in place ready to meet these needs. We are experienced and motivated in cooperating with clients to fulfill individual risk analysis requirements.

6 FREQUENTLY ASKED QUESTIONS

6.1 Hardware components

6.1.1 Does the system support 802.1x authentication?

Yes, the GC7.xxxx main controllers support 802.1x authentication.

6.1.2 Are there any hubs or switches included/embedded in the system?

No, standard network equipment is not included in our system or offer.

6.1.3 Does the system support Gigabit Ethernet connectivity?

No, currently only 10/100 Mbit connectivity is supported.

6.1.4 Is the communication protocol encrypted?

Yes, please refer to section "2.3 Network infrastructure".

6.1.5 Which operating system do the main controllers use?

The GC7 main controllers use a Linux-based operating system.

6.1.6 Which operating system do the sub controllers use?

Keil RTX Real-Time Operating System.

6.1.7 Do the main controllers have to use an SD card?

The GC7 controllers and GT7 terminals always need to operate with their SD card.

6.1.8 What is the NET Bios Name of the main controllers?

The default NET Bios Name (Host Name) of the GC7 main controllers is "GC7_S0000000000". The last 10 digits is the serial number of the main controller that is printed on the controller label. The NET Bios Name of the main controllers can be changed.

6.1.9 What are the bandwidth and latency considerations for the main controllers?

It is recommended to keep latency below 60 ms to guarantee a smooth user experience at the locker door. A stable network connection, in which no data packets are lost, is also important. The client is responsible for ensuring that the response time caused by latency in the network is acceptable for the controllers and locker users. The bandwidth requirements can be calculated at around 15 MB per G7 device per day (= 450 MB per month).

6.2 Software components

6.2.1 How is data in transit protected?

All network traffic between the Envisio cloud platform and the database instance is transparently encrypted using TLS 1.2. Data sent between the main controller and the Envisio cloud platform is encrypted using TLS 1.2. More information on data in transit can be found here:
<https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/protecting-data-in-transit.html>

6.2.2 Do you encrypt tenant data at rest?

Yes, all data of the eLoxx 365 application is stored in DynamoDB by AWS, which is always encrypted at rest using 256-bit AES-GCM. More information on data at rest can be found here:
<https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/protecting-data-at-rest.html>

6.2.3 Who owns the encryption keys?

The encryption keys are managed by the AWS KMS service.

6.2.4 How are keys provisioned, accessed, rotated, and destroyed?

The encryption keys are provisioned/destroyed automatically by AWS and rotated every year via the AWS KMS service.

6.2.5 Are database backups encrypted?

Yes, they are encrypted using an encryption key managed by KMS.

6.2.6 Are there backup or recovery mechanisms in place to protect the database?

Yes, a backup of all databases is conducted every night, and the backups are stored for 30 days.

6.2.7 What measures does Gantner take to detect vulnerabilities and maintain the security of the application?

We continuously monitor our application using a combination of AWS native tools & Datadog (centralized monitoring).

- AWS GuardDuty (see <https://aws.amazon.com/guardduty/>)
 - Continuously analyses network traffic, AWS CloudTrail events, etc., to detect suspicious or anomalous behavior. When unusual activity is identified, GuardDuty generates alerts.
- AWS CloudTrail (see <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html>)
 - Logs all API activity carried out on our AWS accounts, providing full visibility into access and configuration changes.
- AWS ECR (see [Scan images for software vulnerabilities in Amazon ECR - Amazon ECR](#))
 - The docker images are scanned using AWS ECR integration.
- Datadog
 - Datadog is our primary monitoring solution and is closely integrated with our application providing detailed insights into tenant-specific traffic.
 - Our microservice containers are scanned at runtime using Datadog Runtime SCA. The Datadog software notifies us about open-source vulnerabilities (see [Datadog Software Composition Analysis](#)).
 - Datadog is integrated with our other tools and serves as the central alerting platform, directing notifications to the relevant teams.

6.2.8 Do you logically and physically segregate production and non-production environments?

Yes, each environment uses a different AWS account. This means the production environment is separated from the non-production environments.

6.2.9 Do you protect your cloud services with anti-malware programs?

Yes, Amazon Web Application Firewall and Amazon Guard Duty are enabled to protect the Enviso environment.

6.2.10 What are the minimum password requirements for eLoxx 365?

Passwords must be at least 12 characters and include an uppercase letter, a lowercase letter, a number, and a special character. The password cannot be the same as the previous 12 passwords.

6.2.11 Does eLoxx 365 support periodical pushed password changes?

No, eLoxx 365 does not force the users to periodically change their password.

6.2.12 Are there minimum password requirements for eLoxx 365?

The minimum requirements are: eight characters including at least two different types of characters, e.g., uppercase letters, lowercase letters, numeric digits, and punctuation marks.

6.2.13 Which login methods are possible with eLoxx 365?

1. Via Enviso credentials with two-factor authentication: Additional authentication using a verification code.
2. Via single sign-on (SSO): OpenID Connect (OIDC) is supported, which enables a user to log in using their Facebook or Google account for example rather than entering user credentials.

6.2.14 Is it possible that the eLoxx 365 server becomes temporarily unavailable, e.g., during updates?

There are multiple updates throughout the year that mostly take place without any downtime; however, short periods of downtime can occur.

6.2.15 Can I change the ports in eLoxx 365?

No, the ports cannot be changed.



gantner 
INSPIRED ACCESS

SALTO  **WECOSYSTEM**

© 2026 Gantner
Gantner reserves the right to change technical specifications,
designs and services without prior notice.
Photos: Salto WECOSYSTEM / Shutterstock

SCAN FOR CONTACT

