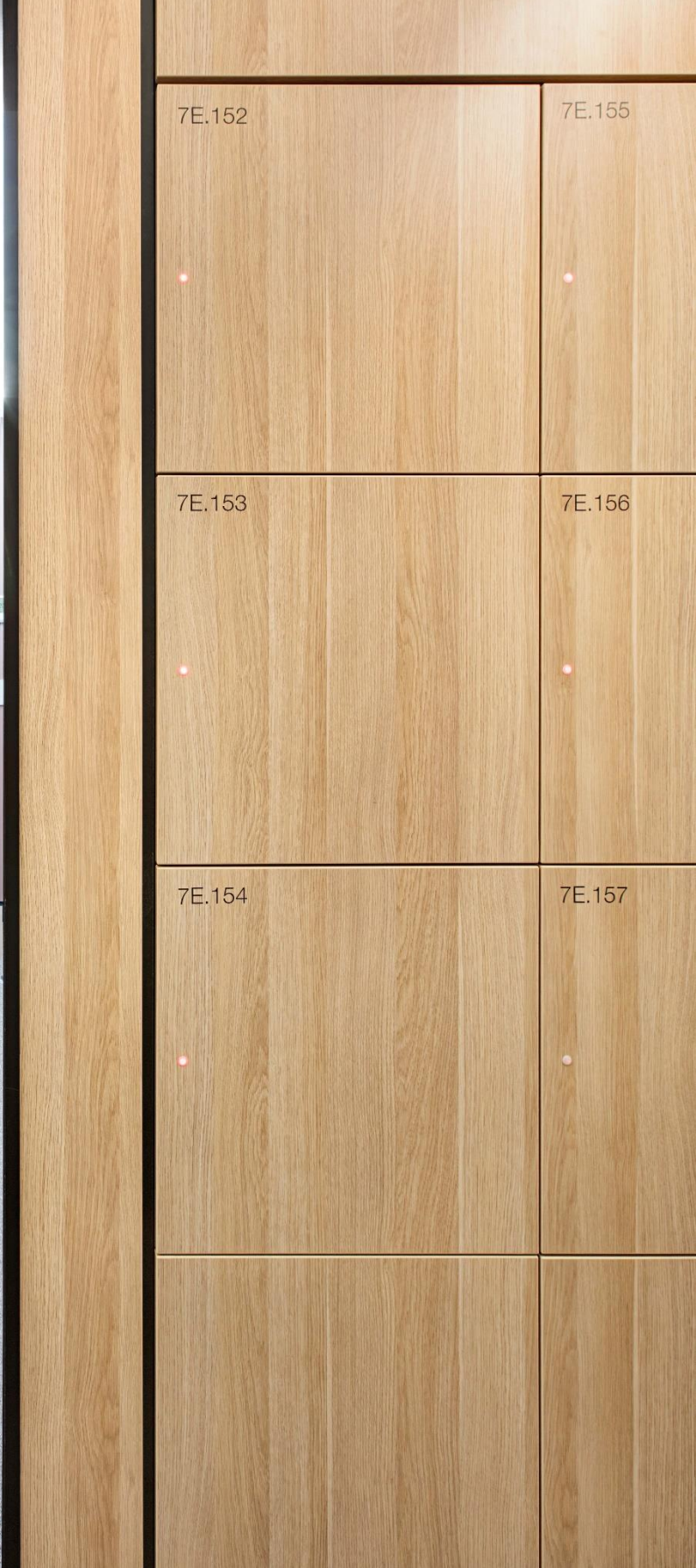




GANTNER IT Security Assessment - Relaxx

System Description of the NET.Lock/Relaxx System for IT Security Assessment

Document Version 2.3

© Copyright 2024 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 in particular 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 product 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

The contact information for questions regarding this manual or for general enquiries is listed below:

Contact address of manufacturer:

GANTNER Electronic GmbH
Bundesstraße 12
6714 Nüziders, Austria
www.gantner.com/locations

CONTENTS

1	INTRODUCTION	5
1.1	About this manual	5
1.2	NET.Lock locker system.....	5
1.3	Terminology	7
1.4	Contact & inquiries	8
2	SYSTEM DESCRIPTION	9
2.1	Overview	9
2.1.1	Information and data characteristics	10
2.2	Hardware components	11
2.2.1	GAT NET.Lock	11
2.2.2	GAT NET.Lock Controller S - Sub Controller.....	11
2.2.3	GAT NET.Lock Controller M - Main Controller.....	11
2.2.4	GC7 - Main Controller	12
2.2.5	GT7 Central Locker	12
2.3	Software components	13
2.3.1	Software requirements	13
2.3.2	Relaxx client	14
2.3.3	Supported operating systems.....	14
2.3.4	Optional component: Relaxx WEB UI 2.....	15
2.3.5	Optional component: LockPal and REST API.....	16
2.4	Relaxx database	17
2.4.1	Database requirements	17
2.4.2	Microsoft .NET Framework.....	18
2.4.3	Microsoft .NET Core Runtime	18
2.4.4	Database storage	18
2.4.5	Database size	18
2.4.6	Data protection / GDPR guidelines.....	19
2.5	Access control data carriers	21
2.5.1	Technology and compatibility.....	21
2.5.2	UID, CSN, Data carrier number.....	21
2.6	Network infrastructure	22
3	SECURITY & MANAGEMENT.....	25
3.1	Role management.....	25
3.2	User management / Active Directory	26
3.3	Logging	27
3.4	Relaxx database backup	28
3.5	TLS communication	29
3.6	Master cards	30
3.7	Controller offline mode	30
3.8	Essential power circuits / UPS.....	31
4	SYSTEM ADMINISTRATION	33
4.1	Remote access	33
4.2	Software and 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	35
5.3	Software development standards	36
5.4	Customer security assessments.....	36
6	FREQUENTLY ASKED QUESTIONS	37
6.1	Hardware components	37
6.1.1	Does the system support 802.1x authentication?.....	37
6.1.2	Are there any hubs or switches included/embedded in the system?.....	37
6.1.3	Does the system support Gigabit Ethernet (GbE) connectivity?	37
6.1.4	Is the communication protocol encrypted?.....	37
6.1.5	Which operating system do the main controllers use?.....	37

6.1.6 Which operating system do the sub controllers use? 37

6.1.7 Do the main controllers have to use an SD card? 37

6.1.8 What is the NETBios name of the main controllers? 37

6.1.9 What are the bandwidth and latency considerations for the main controllers? 38

6.2 Software components.....38

6.2.1 Does Relaxx support periodical pushed password changes? 38

6.2.2 Are there minimum password requirements for Relaxx? 38

6.2.3 Can the Relaxx server be redundant for availability during, e.g., software updates? 38

6.2.4 Can Relaxx run in the cloud? 38

6.2.5 Can Relaxx be deployed using MSI packages? 38

6.2.6 Can two Relaxx databases be merged together into one? 38

6.2.7 What options are there for importing data into the Relaxx database?.....39

6.2.8 How many locker groups can be configured in Relaxx? 39

6.2.9 How do I plan Relaxx with high availability and site resilience?.....39

6.2.10 Can I change the ports in Relaxx? 39

6.2.11 Can Microsoft Windows® and SQL Server® updates be made regularly and automatically or only when GANTNER communicates the release of an update to its customers? 39

6.2.12 Is there support for running applications on a virtual server with Hyper-V?.....39

6.2.13 Can Relaxx WEB UI run on multiple IIS instances behind a load balancer? 39

7 APPENDIX 41

7.1 Component model.....41

7.2 Target interfaces.....42

1 INTRODUCTION

1.1 About this manual

This manual provides additional information for the IT security assessment of GANTNER's GAT NET.Lock system. The information provided herein is intended to assist IT departments in performing a risk/benefit analysis and security review in accordance with their approved corporate security policies.

The following manuals are available for the individual products described in this document that explain all functions associated with the product in greater detail.

- GAT NET.Lock System
 - o Manual for installation, configuration, and operation.
- G7 Central Locker System
 - o Manual for installation, configuration, and operation.
- Relaxx Management Software
 - o Manual for the installation and configuration of the Relaxx software.
 - o Manual for the operation of the Relaxx software.
 - o Manual for the installation, configuration, and operation of the Relaxx WEB User Interface.
- LockPal App
 - o Manual for installation, configuration, and operation.

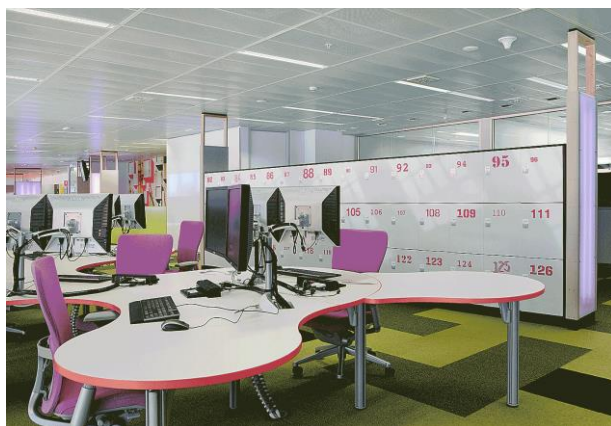
1.2 NET.Lock locker system

Large numbers of lockers for storing company information and/or employees' personal belongings must be easy to manage and use in order to avoid high operating costs in the building operations and security department.



The NET.Lock 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 PC in the client's network via the Relaxx management software.

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 the majority of employees will interact with multiple times each day.



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 JSON interface (e.g., access control, building management, human resources, etc.).

The system connects to the building's power supply, requires no batteries, and contributes to a green IT environment. A mobile app (LockPal) is available for mobile devices with Android or iOS operating systems, providing remote access to lockers in the facility for secure locking and unlocking of available lockers.

The NET.Lock system consists of GANTNER hardware and software connected to the client's network. GANTNER does not provide ongoing IT infrastructure services.

1.3 Terminology

The following terms are used frequently in the manual:

Lock

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

Main controller

This term refers to the control unit that is used for communication with the locker system software, e.g., Relaxx. Different variants of the main controller are available that are described in the GAT NET.Lock manual.

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/Relaxx server via the 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.

Relaxx

Microsoft Windows® management software that consists of two components: Relaxx server and Relaxx client. The term Relaxx is used in this manual to refer to the management software in general. When information is only applicable for one component of Relaxx, e.g., server or client, this will be noted.

Relaxx server

A component of the Relaxx management software. Relaxx Server is a Windows® service that operates in the background to handle communication with the controllers/locks.

Relaxx client

A component of the Relaxx management software. The Relaxx client is a user software that layers over the top of the Relaxx server for the purpose of configuring system components, controlling locks/controllers, monitoring system activity, and writing/retrieving information to/from the Relaxx database.

Relaxx database

A version of Microsoft® SQL Server® is used to store data from Relaxx and the NET.Lock system. The term Relaxx database is used in this manual to refer to this database.

Relaxx WEB UI

Relaxx WEB UI is an optional component included with Relaxx that provides a visualization of the locker system and basic control options via a web browser (desktop or mobile).

Data carrier

This term refers to the employee access control cards, armbands, or fobs that are used with the NET.Lock system.

User

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

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 control card) is used for identification in the NET.Lock system.

LockPal

Users of the electronic lockers can install the LockPal app on their mobile devices and connect to the Relaxx software in order to lock and open available lockers and check the lock status.

1.4 Contact & inquiries

If you have any questions concerning the NET.Lock 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/locations

2 SYSTEM DESCRIPTION

2.1 Overview

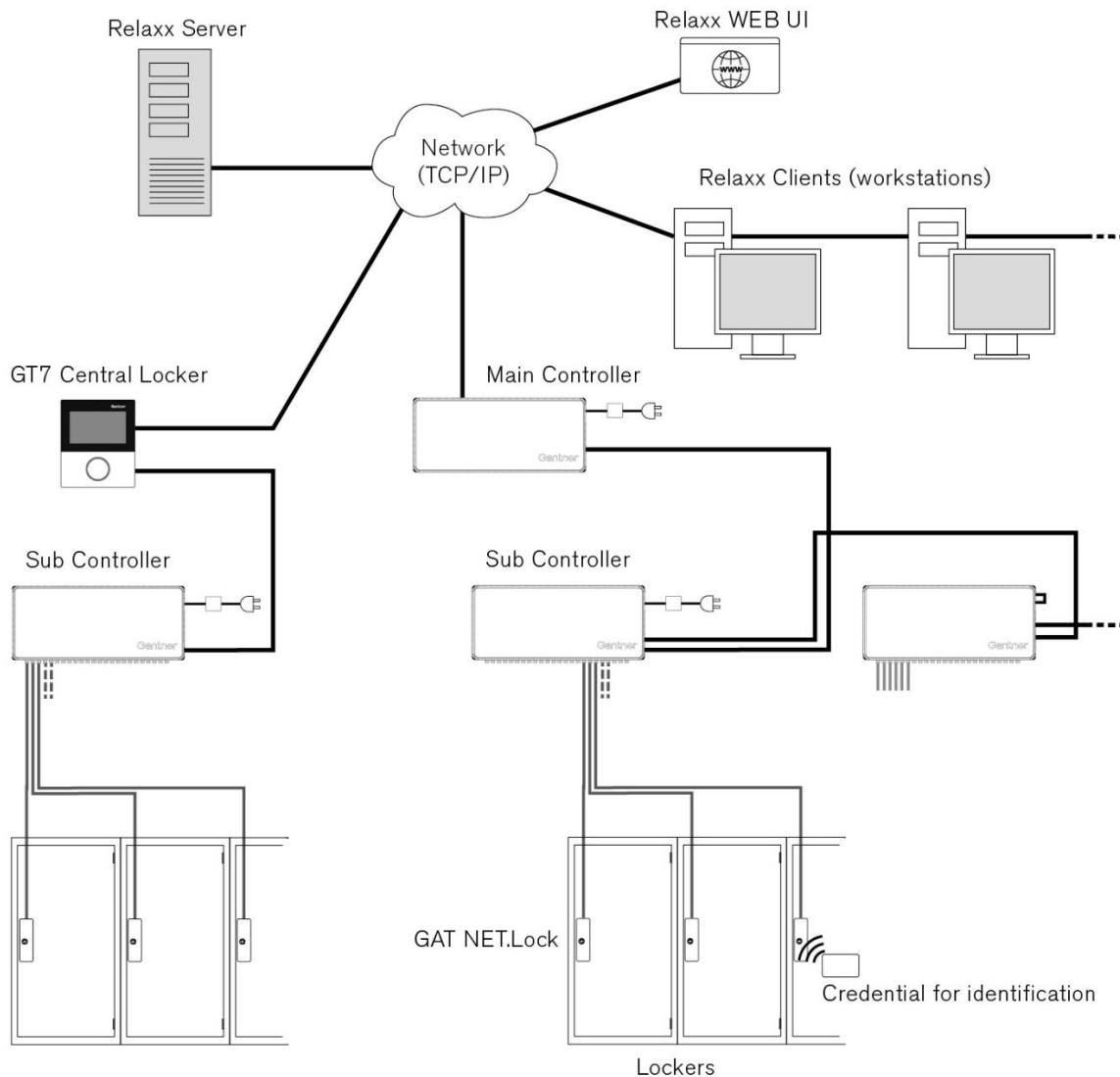


Figure 2.1 - Hardware structure of the NET.Lock system

- Each NET.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 category 5/6 network cabling can be used for these connections.

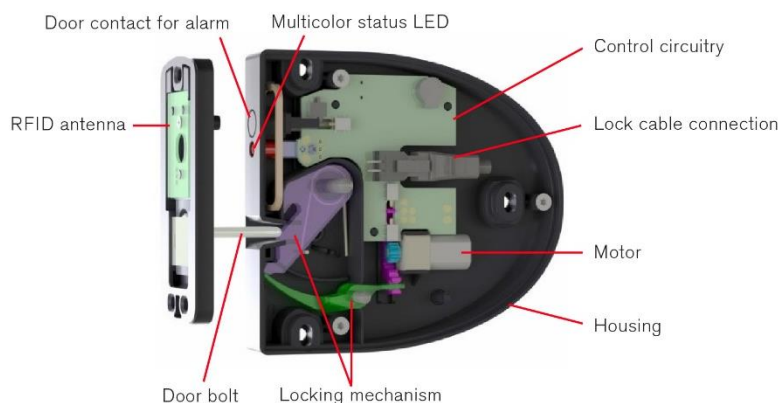
- Sub controllers are installed in a location near the locker locks (max. 5 m cable) and must always be readily accessible for maintenance and inspection. Typical installation locations include suspended ceiling spaces, on top of or beneath the lockers, in a maintenance locker, in raised floor spaces, 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 one network (TCP/IP) connection to the client/building network. The network connection can be a spare port on a building services or security network or can be a port within a dedicated VLAN for larger projects.
- The Relaxx server (Windows Service) communicates through the network to the main controllers.
- The Relaxx server communicates with the Relaxx database for the purposes of checking user authorizations as well as writing all system events and statuses to the database.
- The Relaxx client is a user software that layers over the top of the Relaxx server for the purpose of configuring system components, controlling locks/controllers, monitoring system activity, and writing/retrieving information to/from the Relaxx database.
- The Relaxx client, usually installed on the server for configuring hardware or on a PC for administrative work (multiple client installations possible), is an instance of Relaxx minus the Relaxx server component. The Relaxx client connects to the server instance of the Relaxx server via TCP port 8236.
- The Relaxx WEB UI application provides a clear, user-friendly interface for monitoring and controlling GANTNER electronic locker locks and for the authorization assignment of data carriers.
- Relaxx WEB UI is a website that is installed on an Internet Server (Microsoft Windows® IIS = Internet Information Services). Users can access the Relaxx WEB UI via an internet browser such as Chrome or Firefox.
- LockPal is a mobile app that allows users to access the locking system to lock and unlock their lockers and check the locking status via their mobile device. The connection to Relaxx is via the REST API, which runs on the Internet Server IIS.
- Depending on the locker design and layout, GANTNER will calculate how many sub and main controllers are required for each project.

2.1.1 Information and data characteristics

- Sub controllers store the Unique Identification Number (UID) of each data carrier, e.g., employee data carrier, which has locked a connected lock plus the UIDs of the master cards.
- Main controllers store lock/unlock 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 Relaxx server via the main controller.
- When a sub or main controller is offline and emergency mode is enabled (see “3.7 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 “3.7 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 if the same data carrier has already been used to lock another locker connected to the same controller.
- Once communication between the main controllers and the Relaxx server is re-established, data from the locker system (log data) is automatically uploaded from the main controllers to the Relaxx server.

2.2 Hardware components

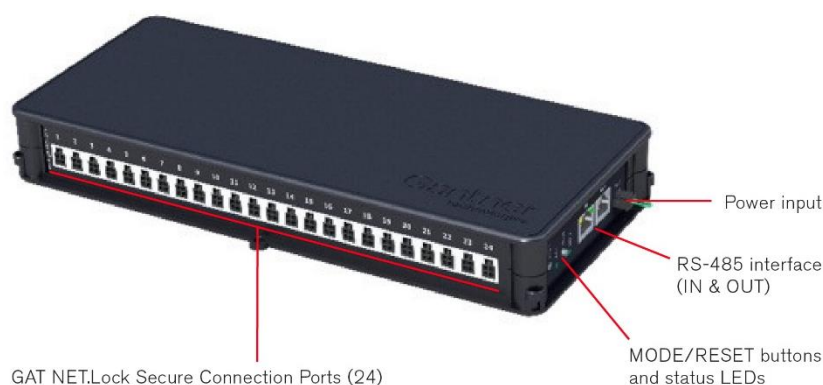
2.2.1 GAT NET.Lock



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)

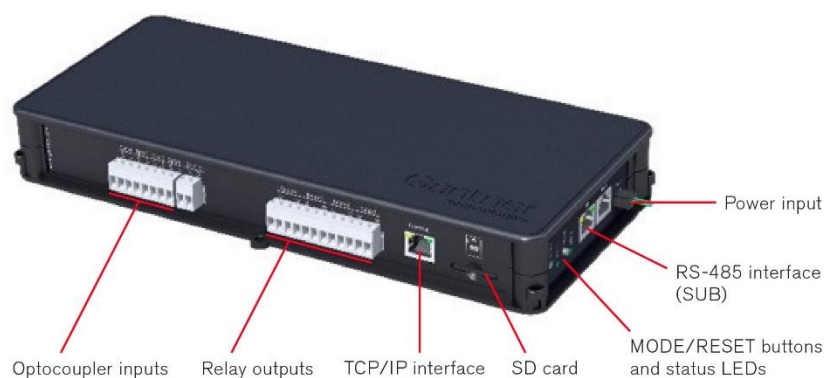
2.2.2 GAT NET.Lock Controller S - Sub Controller



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)

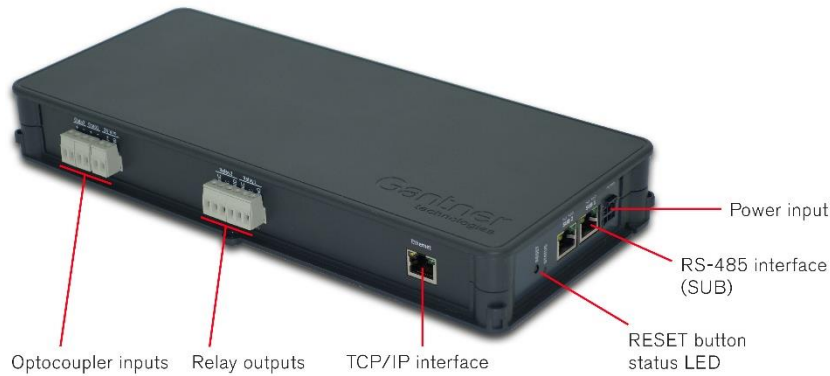
2.2.3 GAT NET.Lock Controller M - Main Controller



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)

2.2.4 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)

2.2.5 GT7 Central Locker



Dimensions

Width: 127 mm (5 in)
Height: 151 mm (59.5 in)
Depth: 24.7 mm (0.97 in)
Weight: 370 g (13 oz)

2.3 Software components

Relaxx runs on computers with a Microsoft Windows® operating system and provides a platform for configuring, controlling, and visualizing the NET.Lock system. Relaxx consists of two components: a Windows® service, called Relaxx server, which runs in the background and handles communication with the controllers/locks, and a user interface, called Relaxx client, which is used to configure the locking system hardware and display the occupancy status of the lockers. The Relaxx server should be installed on a server/PC (physical or virtual) provided by the client and designed for 24/7 operation.

2.3.1 Software requirements

The following minimum requirements are recommended for the Relaxx server and Relaxx client.

Project size: < 1000 lockers

Relaxx server

- Windows® Server 2016 or later version
- Min. 4 CPU cores
- Min. 8 GB RAM (free)
- Min. 30 GB HDD space

Relaxx client

- Windows® 8 or later
- Min. 4 CPU cores
- Min. 4 GB RAM (free)
- Min. 20 GB HDD space

Project size: > 1000 lockers

Relaxx server

- Windows® Server 2016 or later version
- Min. 8 CPU cores
- Min. 8 GB RAM (free)
- Min. 30 GB HDD space (applications)
- Min. 30 GB HDD space (data)

Relaxx client

- Windows® 8 or later
- Min. 4 CPU cores
- Min. 4 GB RAM (free)
- Min. 20 GB HDD space

The “free” RAM value refers to the required RAM that must be available for Relaxx server and Relaxx client to use exclusively. If other applications are running on the same computer, the required RAM increases correspondingly.

Other requirements

These items are to be provided by the client unless specified otherwise.

- Microsoft® Windows® Server 2016 or later – (Full Install).
- GANTNER engineers must be provided with the server user account(s) that include local administrator rights.
- Microsoft .NET Framework min. V 6.0.10 (included in the Relaxx installation package).
- Network connection for Relaxx clients: TCP/IP
- Network connection for main controllers: TCP/IP, latency below 60 ms (recommended for a smooth user experience), bandwidth 1.5 Mbit/s (see “6.1.9 What are the bandwidth and latency considerations for the main controllers?).
- Permanent 24/7 remote access for commissioning, support, and important maintenance via RDP with a secure channel / VPN link (e.g., Citrix, etc.).
- Possibility to install the Relaxx management software.

Once a system is installed on an organization’s network, the IT Administrator has the option to connect to the Relaxx server with a PC/laptop to run an instance of the Relaxx client.

2.3.2 Relaxx client

The license module and the user management system allow the installation of multiple Relaxx clients on different computers, which all share access to a single Relaxx server installation via the network. Each Relaxx client logs in to the shared Relaxx server and Relaxx database using their own username and password.

For simple systems, it is possible to run a single Relaxx client installed on the same PC as the Relaxx server and Relaxx database.

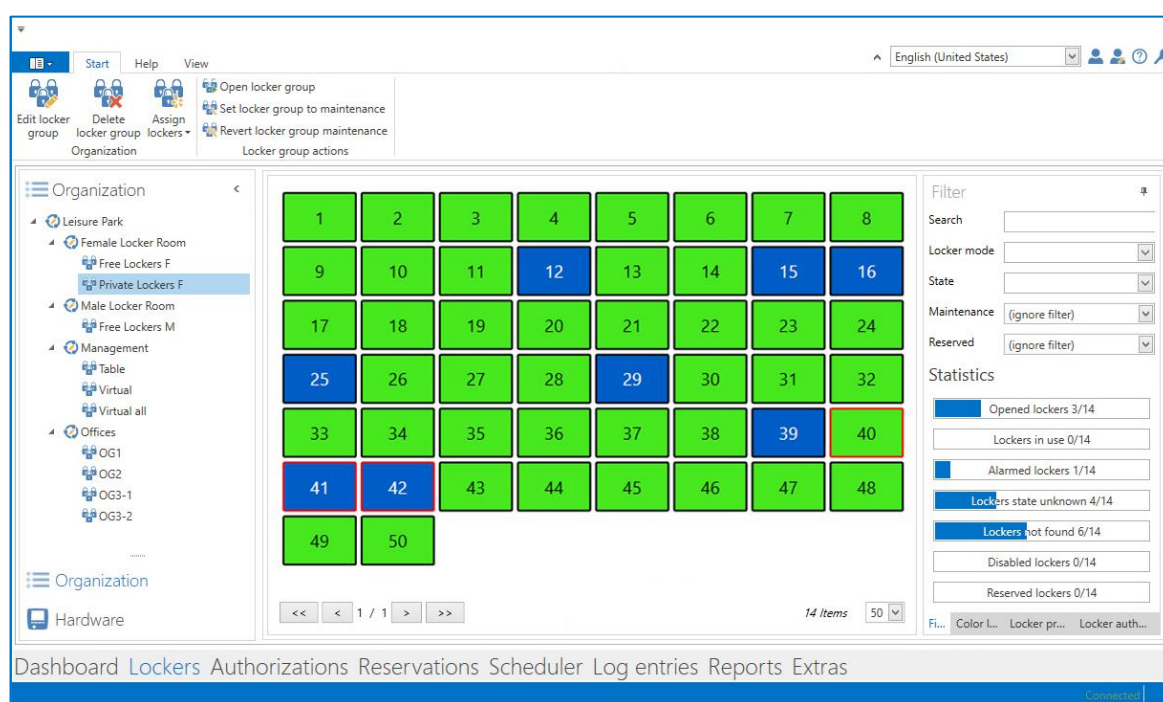


Figure 2.2 – Relaxx user interface

2.3.3 Supported operating systems

- Microsoft® Windows® 11 – Editions: Pro and Enterprise (32 and 64-bit)
- Microsoft® Windows® 10 – Editions: Pro and Enterprise (32 and 64-bit)
- Microsoft® Windows® 8.1 – Editions: Pro and Enterprise (32 and 64-bit)
- Microsoft® Windows® 8 – Editions: Pro and Enterprise (32 and 64-bit)
- Microsoft® Windows Server® 2022 - Editions: Standard and Datacenter (64-bit)
- Microsoft® Windows Server® 2019 - Editions: Standard and Datacenter (64-bit)
- Microsoft® Windows Server® 2016 - Editions: Standard, Essentials and Datacenter (64-bit)

NOTE! Editions not listed here, such as Home, Starter, Web, RT, etc., are not supported by Relaxx. Furthermore, Relaxx does not support the Server Core installation option of Windows Server® 2016, Windows Server® 2019 and Windows Server® 2022.

NOTE! Please note that the GANTNER Support Team can only assist when Relaxx is installed on a German or English version of Windows. In addition, support can only be given when the customer provides all access authorizations required by the Support Team, e.g., access to the Windows account under which Relaxx runs or access to the SQL database, etc.

NOTE! The client is responsible for providing any additional licenses required, e.g., for the operating system or database.

2.3.4 Optional component: Relaxx WEB UI 2

Relaxx WEB UI 2 is an optional component included with Relaxx (at no additional cost) that provides visualization of the locker system and basic control options via a web browser (desktop or mobile). It is licensed and configured through the Relaxx client but is not required to operate the locking system. The decision to install Relaxx WEB UI 2 must be made by the customer based on their locker management procedures and locker management devices (operating system).

The website for Relaxx WEB UI 2 is installed on a Microsoft Windows® IIS Internet server. The user must log in to access the website. The user management system is connected to and configured through the Relaxx client.

The following requirements apply for operating Relaxx WEB UI 2:

- Supported web browsers:
 - NOTE!** Always use the latest version of the web browser to ensure optimum performance.
 - Microsoft Edge
 - Google Chrome
 - Mozilla Firefox
- IIS server components must be activated in Windows (automatically performed during software installation).
- The IIS extension "URL Rewrite" must be installed (can be installed from within the Relaxx setup).
- A TLS certificate for an encrypted connection between the web browser and IIS is recommended (a TLS certificate is not supplied by GANTNER). See "3.5. TLS communication" for more information.

NOTE! Additional information regarding the system requirements is provided in the Relaxx WEB UI 2 manual.

Relaxx WEB UI 2 allows the operator to access the locker system remotely via a web browser. The functions available to the user in Relaxx WEB UI 2 depend upon their assigned role in Relaxx client, and their correspondingly assigned permissions in Relaxx WEB UI 2.

A user with full permissions is able to access all areas of Relaxx WEB UI 2, which includes:

- Dashboard: An overview of the locker system, e.g., locker usage, alarms, etc., is displayed here.
- Lockers: A list of all lockers defined in the system, divided into locker groups, is displayed here.
- Authorizations: The data carriers and lockers are authorized and assigned to the end users here.
- Reservations: Lockers can be assigned to users for a certain time period. The users can then use the lockers within this time period.
- Scheduler: Planning automatic actions, e.g., database backups, service openings of lockers, or data imports.
- Log entries: All locker system data is displayed here.
- Reports: Different reports that provide information on system use are available to view and export here.
- Master card sets: Master card sets (as defined in Relaxx client) are displayed and can be activated or deactivated.
- Permissions: In the permissions area, operators can be granted the right to view/edit the different areas of the user interface based upon their assigned role.

2.3.5 Optional component: LockPal and REST API

The **LockPal** software application is an app for use on mobile devices with Android or iOS operating systems. It can be downloaded free of charge from the Google Play Store or the Apple App Store. With the LockPal app, users can select and lock or open their wardrobe lockers, office lockers, etc., which are equipped with a GAT NET.Lock 70x0. To control the locker, e.g., lock or unlock, the user presses the desired button in LockPal on their mobile device, which serves as a key or unique ID for the user. The control command is then sent from LockPal to the Relaxx server for execution.

LockPal must be linked to the relevant system so that the lockers within the system can be used. The user then defines a personal password to protect against the unauthorized use of their app. For LockPal to communicate with the locker locks, the software Relaxx (min. version 7.x) must be installed on a server/PC in the system. Following this, LockPal communicates via WLAN and the Relaxx REST API with the Relaxx software, which forwards the requests via the LAN network to the relevant controllers and GAT NET.Lock 70x0 locks.

The Relaxx REST API is included in the Relaxx Enterprise installation package, but it is not essential for the operation of the locking system. The decision to install the REST API must be made by the customer based on their lock management procedures and lock management devices (operating system).

The Relaxx REST API is installed on a Microsoft Windows® IIS Internet server.

The following requirements apply for the REST API:

- Min. Relaxx 7.x (see requirements for Relaxx in the Relaxx Installation manual).
- Microsoft .NET Core Runtime min. V 6.0.10. The .NET Core Runtime can be installed via the "Hosting Bundle for Windows" option in the installation wizard of Relaxx.
- IIS server components must be activated in Windows (automatically performed during software installation).
- For LockPal, min. Android V 6.0 or iOS V 14 and a mobile device with Bluetooth are required.

NOTE! For more information on system requirements, please refer to the Relaxx Installation manual and the LockPal manual.

The following functions are available for the users of LockPal:

- My lockers: Overview of personal lockers that are assigned and used by the user.
- Locker groups: A list of all locker groups where all available free lockers are shown. The user can select and use a locker from that list.
- Favorite lockers: Mark lockers as favorites for a quick overview.
- Change organization: Connect to a different locker installation. Authorization from Relaxx is required.
- Change password: Changing the password that is required to log in to LockPal.
- Help: Integrated assistance.

2.4 Relaxx database

2.4.1 Database requirements

Supported databases:

- Microsoft® SQL Server® 2014 – Editions: Standard, Express, Enterprise
- Microsoft® SQL Server® 2016 – Editions: Standard, Express, Enterprise
- Microsoft® SQL Server® 2017 – Editions: Standard, Express, Enterprise
- Microsoft® SQL Server® 2019 – Editions: Standard, Express, Enterprise
- Microsoft® SQL Server® 2022 – Editions: Standard, Express, Enterprise

NOTE! Editions not listed here are not supported.

The Microsoft SQL Server® 2022 Express is included in the Relaxx installation package. Information on the system requirements for Microsoft SQL Server® 2022 is available via the following link:

<https://learn.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-2019>

It is recommended to also install Microsoft SQL Server Management Studio Express. This application is included in the Relaxx installation package.

Regarding the directory where the database is installed, please observe the following points:

- Anti-virus software is not permitted to scan the directory (see also “4.3 Antivirus software and firewall”). Please read the following security considerations from Microsoft: (<https://technet.microsoft.com/en-us/library/ms144228.aspx>).
- Automatic backups of the database should only be completed using the backup function in Relaxx or a special SQL backup tool provided by the client. A typical file backup of the database folder is not allowed.

Important Information for Express Editions!

- Please note that the Relaxx installation package only contains the free Express version of Microsoft SQL Server® 2022. If a full version of Microsoft SQL Server® including license is required, this must be provided by the client IT system administrator.
- When using the Express version of Microsoft SQL Server®, ensure the database maintenance function is enabled to keep the database size to a minimum. This function is configured in the Scheduler section of Relaxx. Further information is available in the Relaxx Operation manual.
- Observe the limitations of the Express editions:
 - Database size is limited to 10 GB.
 - Only one CPU (but several cores) is supported.
 - No SQL Server Agent.

Information for database administrators:

In case the database of the Microsoft SQL Server is provided by the customer or a service company, the following information may be helpful:

- Recommended collation: Latin1_General_CI_AS
- Additional features of the Microsoft SQL Server, e.g., Full-Text Search, Reporting Services, etc., are not required.

- The standard values of the Microsoft SQL Server for the automatic expansion of the database (1 MB and 10% for data or logs) must be set accordingly. The values depend on the size of the system, however; the setting 500 MB for data and logs is a good average value.
- Relaxx server and GANTNER Support require the privileges for the "DB_OWNER" SQL database role.

Important information for a client supplied SQL database!

- If the client IT department is providing a separate server for the Relaxx database (separate to the server for Relaxx server), scheduled database backups via the Relaxx client may not be possible due to permissions.
- In this case, it is the responsibility of the client IT department to schedule backups via the Relaxx database. In addition, GANTNER requires the contact details of the responsible person in case we need to conduct a database restoration.

2.4.2 Microsoft .NET Framework

- Min. V 6.0.10 (included in the Relaxx installation package).

2.4.3 Microsoft .NET Core Runtime

- Min. V 6.0.10

The .NET Core Runtime is only required if the Relaxx REST API is to be used (included in the Relaxx installation package).

2.4.4 Database storage

All data is stored in the Relaxx database and is owned by the client. Access to the database is protected by SQL user login authentication. The physical location of the Relaxx database and all security, backup, and maintenance requirements relating to the database server are the client's responsibility.

2.4.5 Database size

The database size depends mainly on the number of locks connected to the system and the retention duration of all the log entries produced during normal operation.

Assuming that log entries are retained for a 30-day period and the lockers are used four times a day on average, the following database sizes can be expected.

1000 locks:	0.85 GB
2000 locks:	1.70 GB
3000 locks:	2.50 GB
4000 locks:	3.40 GB
etc.	

2.4.6 Data protection / GDPR guidelines

This section provides a brief overview of the roles and responsibilities under the General Data Protection Regulation (GDPR) in relation to data processing activities when using the Relaxx software. The terms personal data, controller and processor have the meaning as defined in the GDPR. Personal data of the customer refers to the personal data that may be processed by a third party on behalf of the customer, in the course of the provision of certain services.

Disclaimer

The GDPR guidelines are based on GANTNER's interpretation of the GDPR at the time of publication of this information and are intended to help GANTNER sales partners and customers to better understand the GDPR requirements when using the Relaxx software. The information provided and the obligations described are not exhaustive and do not constitute or replace legal advice.

It should be noted that the measures required to ensure compliance with the GDPR will always depend on the specific context. Customers are therefore strongly advised to seek legal advice on the measures to be taken to comply with the obligations under the GDPR when using Relaxx.

a) Personal data stored in Relaxx

To manage lockers with Relaxx, personal data is stored in the Relaxx database.

In order to operate the system, Relaxx processes the data carrier UID of the end user. During the use of the locker system, Relaxx records operational data (i.e., a log of accesses and access attempts by individuals to lockers and access devices), which is linked to the data carrier UID. Additional personal information that may be stored in Relaxx includes, for example, first name, last name, email address, department, position. User-defined fields allow customers to store any other information in Relaxx that is deemed necessary for the operation of the system.

b) Data controllership and associated responsibilities

The customer typically acts as the controller of the personal data stored and processed in Relaxx, since the purpose and means of the processing of personal data is determined by the client.

GANTNER does not process or access any personal data stored and processed in Relaxx by the client during the normal operation of the Relaxx software. GANTNER therefore does not act as a data processor in the day-to-day operation of Relaxx. However, when providing support services, GANTNER may have access to personal data (see section d)).

As a data controller, the client shall comply with the obligations set out in the GDPR. For example, the client shall ensure that personal data is lawfully processed in accordance with the conditions set out in Art. 5 GDPR, to obtain the consent of the data subject (i.e. the end user) for the processing of their personal data, if applicable, and to provide the data subject with transparent information (Art. 13, 14 GDPR) about the data processing activity as well as their rights, etc.

Relaxx can either be installed on a server owned by the customer (on-premises) or hosted by an external party, e.g., cloud service, Software as a Service (SaaS). For any solution in which Relaxx is hosted by an external party, it is the responsibility of the controller (client) and the processor (service provider) to enter into a data processing agreement pursuant to Art. 28. GDPR. Whether the GANTNER sales partner or a third party acts as the processor depends on the specific structure of the contractual relationship. GANTNER does not offer hosting solutions for Relaxx.

c) When does GANTNER's sales partner act as a data processor?

GANTNER's sales partners are expected to offer first-level technical support to clients while refraining from accessing any client personal data.

However, if a resolution cannot be reached otherwise, the GANTNER sales partner may need to connect to the client's network on which Relaxx is installed or request a copy of the Relaxx database. In certain cases, GANTNER's sales partner may handle client personal data on behalf of the controller while providing support services.

In such situations, the sales partner acts as a processor. Consequently, the client must enter into a data processing agreement with the GANTNER sales partner as per Art. 28 GDPR. It should be noted that GANTNER sales partners are separate entities from GANTNER. Thus, it is solely the responsibility of the client and GANTNER's sales partner to ensure that a data processing agreement is signed before processing any client personal data. Access to client personal data shall only occur upon the client's request and consent. After the specific support service is completed, all client personal data shall be deleted and not processed for any further purpose.

d) When does GANTNER act as a data processor?

GANTNER offers technical support services to clients if they cannot resolve a specific issue through the GANTNER sales partner's technical support or if they have purchased the product directly from GANTNER.

GANTNER is tasked with providing technical support services without accessing any client personal data.

If the issue cannot be resolved by alternative means, it may be necessary for GANTNER to access or connect to the client's network on which Relaxx is installed or obtain a copy of the Relaxx database. In these specific situations, GANTNER may process personal data of the client on behalf of the controller while providing support services.

In such cases, GANTNER acts as a processor. Therefore, the client must enter into a data processing agreement according to Art. 28 GDPR with GANTNER. Any access to the client's personal data will only take place with the client's request and consent. Personal data will be deleted and not processed for any other purpose upon completion of the specific support service.

GANTNER agrees to sign a data processing agreement before processing any of the client's personal data on the client's behalf. For this purpose, GANTNER has developed a template agreement for data processing that clients can sign upon their request before receiving technical support services. The data processing contract template is available upon request via privacy@gantner.com.

2.5 Access control data carriers

2.5.1 Technology and compatibility

The NET.Lock 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 contact GANTNER.

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

Compatibility of the client's access control system is dependent on analysis and testing. Variables such as 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.

2.5.2 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 in rare cases it might not be unique (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 therefore 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.

2.6 Network infrastructure

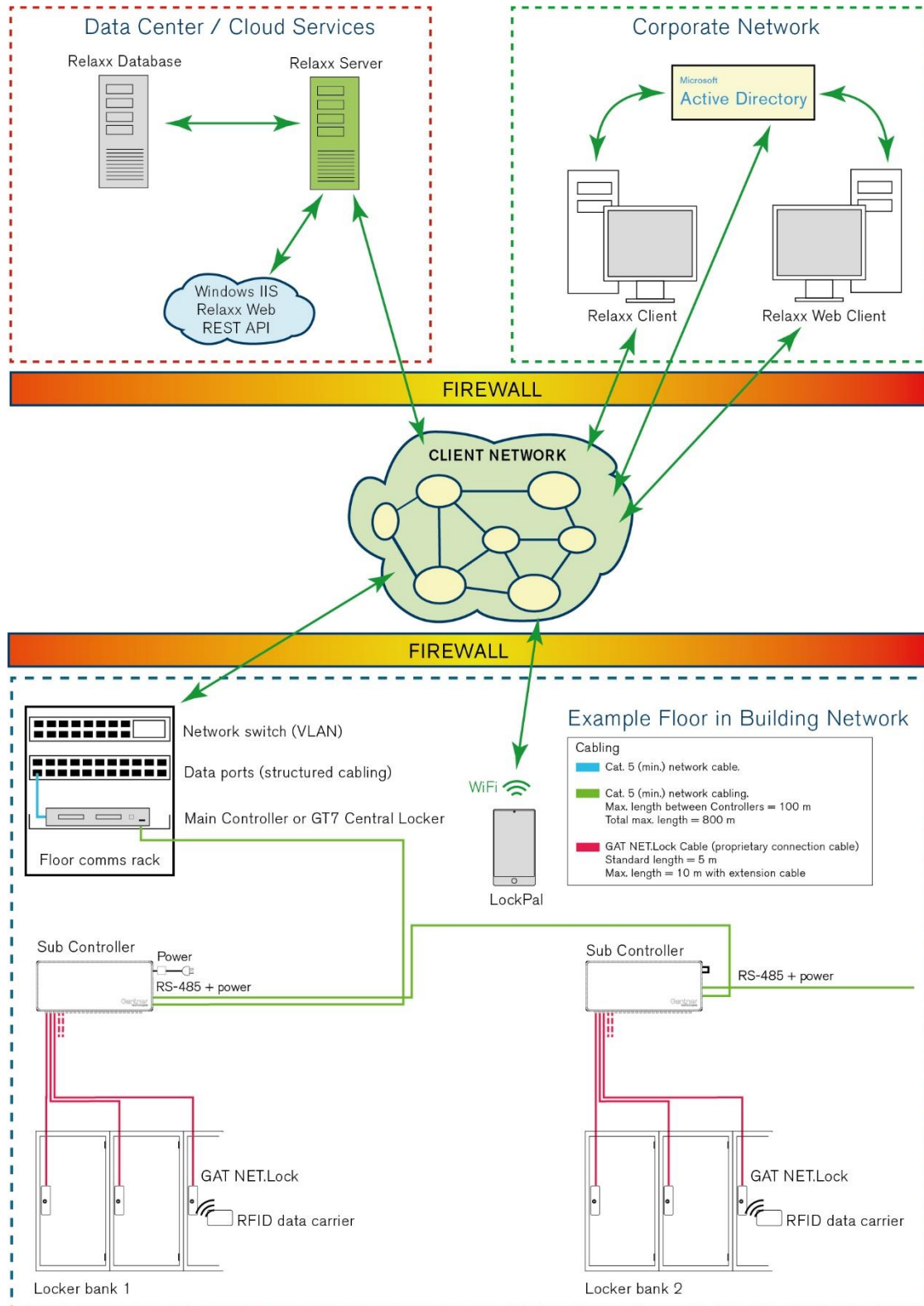


Figure 2.3 – Example of the NET.Lock system infrastructure

The NET.Lock system is a networked control system with each locker lock providing the function of locker locking, locker door monitoring (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 cabled/patched together before being connected to a main controller that converts all the sub controller communication into a standard Ethernet network.

Sub controllers are installed near the locker banks within the 5 m (or max. 10 m with extension cable) lock cable length. 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 rack location and the sub controllers located at the locker banks. The main controllers can also be installed at the locker banks depending on the locker layout and client requirements.

Each main controller requires one network connection on the client's/building network. This network connection can be a spare port on a building services or security network or for larger projects may be a port within a dedicated VLAN. A list of IP addresses for the main controllers must be provided by the client before commissioning of the system.

The communication between the Relaxx server and the Relaxx client can optionally be encrypted using the TLS protocol. The Relaxx server can use a certificate provided by the customer or create a self-signed certificate by itself. The first option is strongly recommended. TLS can also be used for communication between the Relaxx service and the G7 devices (GC7.xxxx main controller, GT7 Access or GT7 Info).

Relaxx can be installed locally on a server in the facility, or it can also be installed in a cloud hosting environment. Furthermore, there is the possibility to use a local database such as Microsoft SQL or a database cloud service such as RDS.

3 SECURITY & MANAGEMENT

3.1 Role management

The Relaxx management software offers the possibility to assign individual users with different levels of system control. This is done using a hierarchical “role” based access system. Each user is assigned to one role with the user’s system control being inherited from this role. A role represents a collection of permissions to modify certain functions within the locker system, e.g., reconfigure a locker.

The screenshot displays the 'Define the rights for Relaxx users' interface. On the left is a blue sidebar with navigation links: General, Alarm, Devices, Card Readers, Database, Authorizations, Maintenance, Reservations, Notifications, Users (highlighted), and Advanced. The main content area has a title 'Define the rights for Relaxx users' and two sections: 'Roles' and 'Users'.

Roles Section: Includes icons for 'Add role', 'Edit role', and 'Delete role', along with 'Active Directory' and 'SAML Configuration' links. Below is a table of roles:

Role Id	Role name	Role description	Parent role	Level
1	SYSTEM	SYSTEM		0
2	Administrator	Administrator	SYSTEM	1
3	System Manager	System Manager	Administrator	2
4	Power User	Power User	System Manager	3
5	User	User	Power User	4

Users Section: Includes icons for 'Add user', 'Edit user', and 'Delete user'. Below is a table of users:

User Id	Display name	User name	Role	Last login	Special rights
1	SYSTEM User	SYSTEM	SYSTEM	3/29/2023	☐
2	Administrator	Administrator	Administrator	4/1/2019	☒
3	System Manager	System Manager	System Manager		☐
4	Power User	Power User	Power User		☐
5	User	User	User		☐

Figure 3.1 – Role and user overview in Relaxx

There are pre-defined roles (Administrator, System manager, Power User, User), however, the system allows the overriding of permissions at user level and the creation of client-specific roles.

Relaxx starts with one superior role called the SYSTEM role. The SYSTEM role contains exactly one user who is able to do everything within the application including creating other roles. Each subsequent role created in Relaxx is a descendant of the SYSTEM role.

Name	C	R	U	D	E	G
Application settings management					☒	☒
Start/stop service					☒	☒
Role management	☒	☒	☒	☒		☒
User management	☒	☒	☒	☒		☒
Web UI permission management	☒	☒	☒	☒		☒
Manage hardware	☒	☒	☒	☒		☒
Scan devices					☒	☒
Debug view					☒	☒
Organization view	☒	☒	☒	☒		☒
Open lockers					☒	☒
Open locker groups					☒	☒
Login for locker commands					☒	☒
Send locker command					☒	☒
Send locker commands to locker groups					☒	☒
Diagnostics view					☒	☒
Authorization management	☒	☒	☒	☒		☒
Reservation view	☒	☒	☒	☒		☒
Scheduler view	☒	☒	☒	☒		☒
Log view	☒	☒	☒	☒		☒
Reports					☒	☒
Extras					☒	☒

Figure 3.2 – Role settings in Relaxx (for “Administrator” user)

The hierarchical structure defines who is allowed to manage which roles and therefore which users. For example, users assigned to the “System Manager” role can only manage descendant roles and the users assigned to these roles (provided the “System Manager” role has been assigned "User Management" and "Role Management" permission).

A role cannot have more permissions than the permissions of its parent role. Removing a permission from a parent role will also delete the permission from all descendant roles.

3.2 User management / Active Directory

Each user of the Relaxx management software has their own user account. With this account, a user is identified by a unique username and password that is used to prevent other people from logging in under this user account. Every user in the software must be assigned to exactly one role and will inherit the system permissions from that role.

Alternatively, an Active Directory (AD) domain controller authenticates and authorizes all users and computers in a Windows domain type network. When a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted login details to confirm the validity. The Relaxx management software allows users to log in to the application using their Windows login details (username and password).

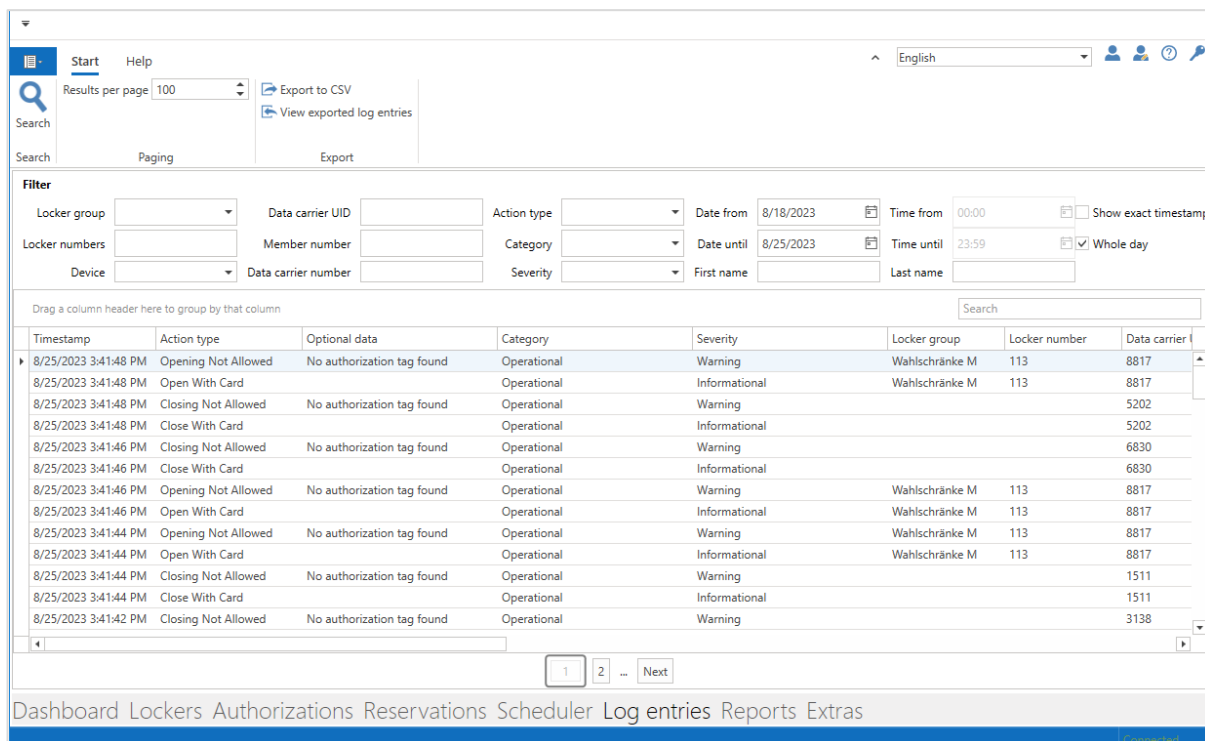
Relaxx supports the single sign-on (SSO) function. This means that a user who is authorized in Active Directory (AD) must only log in once in the domain or in Windows. This user authorization can be used for automatic login when Relaxx is started, i.e., after starting Relaxx, the user is automatically logged in and the main screen is displayed. For more information see the Relaxx Installation manual.

Login without single sign-on (i.e., with a Relaxx username and password) is done via port 8236. Login with single sign-on is done using the Kerberos or NTLM protocol via port 8242 (the Kerberos protocol is recommended for optimum security).

3.3 Logging

System activity, e.g., the locking/unlocking of lockers, activated alarms, and error messages, is logged by the main controllers. The type of log data that is logged can be configured, or the data logging function disabled, in the controller settings. The system also stores the dynamic data of the locker usage. This data can be viewed on the "Log Entries" page of the Relaxx client.

The Relaxx database can be searched according to specific criteria in Relaxx client and Relaxx WEB UI via the "Log Entries" page. Email notifications can be sent for selected log entries, e.g., daily master card usage. The log data should be exported as a CSV file and archived regularly (at least monthly is recommended) in order to free space in the Relaxx database.



Timestamp	Action type	Optional data	Category	Severity	Locker group	Locker number	Data carrier
8/25/2023 3:41:48 PM	Opening Not Allowed	No authorization tag found	Operational	Warning	Wahlschranke M	113	8817
8/25/2023 3:41:48 PM	Open With Card		Operational	Informational	Wahlschranke M	113	8817
8/25/2023 3:41:48 PM	Closing Not Allowed	No authorization tag found	Operational	Warning			5202
8/25/2023 3:41:48 PM	Close With Card		Operational	Informational			5202
8/25/2023 3:41:46 PM	Closing Not Allowed	No authorization tag found	Operational	Warning			6830
8/25/2023 3:41:46 PM	Close With Card		Operational	Informational			6830
8/25/2023 3:41:46 PM	Opening Not Allowed	No authorization tag found	Operational	Warning	Wahlschranke M	113	8817
8/25/2023 3:41:46 PM	Open With Card		Operational	Informational	Wahlschranke M	113	8817
8/25/2023 3:41:44 PM	Opening Not Allowed	No authorization tag found	Operational	Warning	Wahlschranke M	113	8817
8/25/2023 3:41:44 PM	Open With Card		Operational	Informational	Wahlschranke M	113	8817
8/25/2023 3:41:44 PM	Closing Not Allowed	No authorization tag found	Operational	Warning			1511
8/25/2023 3:41:44 PM	Close With Card		Operational	Informational			1511
8/25/2023 3:41:42 PM	Closing Not Allowed	No authorization tag found	Operational	Warning			3138

Figure 3.3 – Log entries page in Relaxx client

3.4 Relaxx database backup

The Relaxx database contains all the data, e.g., hardware configuration data, log data, and the authorization list settings, used to operate the locker system. The scheduler function in Relaxx client allows backups of the database to be carried out automatically at regular intervals.

Figure 3.4 – Scheduling an automatic backup of the Relaxx database

A new file is created for each database backup with the date and time of the backup included in the file name. This allows a previous database file to be easily imported into Relaxx, e.g., after an error event occurs. Operation of the system can then continue on using the data as of the time of the backup.

NOTE!

- When the client IT department is providing a separate server for the Relaxx database (separate to the server for Relaxx server), scheduled database backups via Relaxx client may not be possible due to permissions.
- In this case, it is the responsibility of the client IT department to schedule backups of the Relaxx database directly via Microsoft SQL Server. In addition, GANTNER requires the contact details of the responsible person in case we need to conduct a database restoration.

3.5 TLS communication

The communication between the Relaxx server and the Relaxx client and between the Relaxx server and a G7 device (GT7 or GC7 main controller) can be optionally encrypted using the TLS protocol. The Relaxx server can use a certificate provided by the customer or create a self-signed certificate by itself. The first option is strongly recommended.

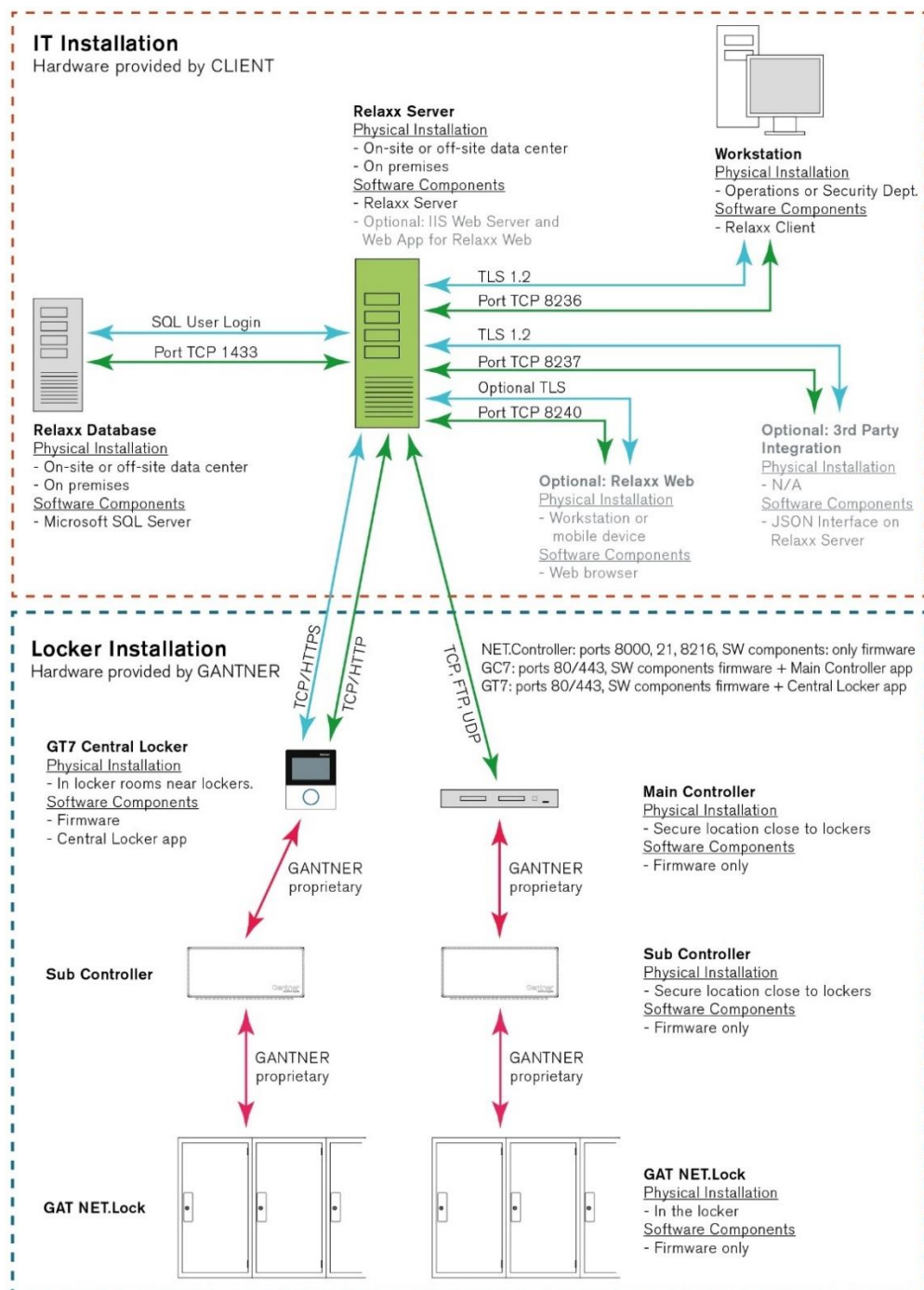


Figure 3.5 - Encryption and authentication

3.6 Master cards

Master cards allow the facility's operations or security team to access locked lockers in the event that an employee loses their access control key card. A master card must also be used to acknowledge an alarm at the locker, ensuring that the operations or security team can investigate the cause of the alarm at the locker.

Master cards use the same technology as the standard data carrier but are assigned special rights. Master cards loaded into the main controllers can lock/unlock any locker controlled by the main controller without restriction, even if Relaxx is unreachable. It is therefore essential to keep the master cards in a secure place. The use of master cards is recorded in the log database and this data can be searched/displayed in the locker management software.

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

Each master controller is assigned a set of up to 10 master cards. For larger systems, several sets of master cards can be defined and assigned to the corresponding main controllers (e.g., one set per floor or building). The UIDs of the master cards are stored in the Relaxx management software, the main controllers and the sub controllers, allowing them to be used in the event of a system shutdown or network failure.

3.7 Controller offline mode

The NET.Lock system is designed for fail-safe operation. This means that if the Relaxx 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) are unaware of any failures in the network and that locker operations continue as normal. Different settings can be configured to determine how the controllers handle requests while in offline mode.

The Relaxx server will attempt to re-establish communication with the controllers 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 Relaxx server.

NOTE! In this manual, **controller offline mode** does not refer to **controller offline application**, which is a function available for locker systems using MIFARE or LEGIC technology.

3.8 Essential power circuits / UPS

The NET.Lock system uses instantaneous power for locking and instantaneous power for unlocking provided by the sub controller. If the building loses power, the locks will remain in their last state and resume normal operation when power is restored.

It is recommended that the system be connected to essential power circuits so that the lockers can be used during a power outage. For installations where generator-backed essential power is not available, we recommend installing dedicated power circuits for locker controllers that are suitable for containing or connecting to a battery backed uninterruptible power supply (UPS).

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

Example

1 main controller	1 x 5 VA = 5 VA
6 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

The GANTNER Support Team strongly recommends 24/7 remote access for commissioning, support, and important maintenance via RDP with a secure channel/VPN link (e.g., Citrix, etc.).

4.2 Software and firmware updates

Software and firmware updates can be managed manually by an authorized user of Relaxx to ensure that the system meets the constantly evolving security requirements throughout the system lifecycle. Any software and firmware update in an operational system must be carefully planned!

In the event of a critical security update or major release for the software or firmware, GANTNER will inform all sales partners via the partner portal and our email newsletter. The GANTNER sales partner will then inform their clients immediately regarding the update.

4.3 Antivirus software and firewall

If an antivirus scanner is used, please observe the recommendations regarding antivirus software for the Microsoft® SQL Server® used for the Relaxx database.

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

- 21 (TCP/FTP, Outbound): Only required for firmware updates of the GAT NET.Lock controller (via FTP).
- 80 (TCP, Outbound): Default communication port between Relaxx and G7 devices.
- 389 (TCP, Outbound): LDAP plain text.
- 443 (TCP, Outbound): Communication port between Relaxx and G7 devices when TLS is enabled.
- 636 (TCP, Outbound): LDAP SSL connection.
- 1433 (TCP, Outbound): Relaxx database (SQL Server) interface. Note that a customer-specific port can be selected for the database connection if the default port cannot be used.
- 3268 (TCP, Outbound): LDAP connection to Global Catalog (GC) server.
- 3269 (TCP, Outbound): LDAP connection to Global Catalog (GC) server via SSL.
- 8000 (TCP, Outbound): For communication with the main controller.
- 8216 (UDP, Outbound): Time synchronization for connected GANTNER devices.
- 8236 (TCP, Inbound): Communication between the Relaxx server and Relaxx client(s).
- 8236 (TCP, Inbound): Communication between the Relaxx server and Relaxx WEB UI.
- 8237 (TCP, Inbound): RelaxxBasicServerInterface (used by third-party systems for requests and notifications).
- 8340 (TCP, Inbound): Communication between the web browser and Relaxx WEB UI 2 (if used).
- 8241 (TCP, Inbound): Communication via the REST API (lock remote control) with the LockPal app.
- 8242 (TCP, Inbound): For Single-Sign-On function for the AD protocols NTLM / Kerberos

5 ABOUT GANTNER

GANTNER is the inventor of the world's most widely used networked locking system for the corporate office industry. With over 35 years of experience in the design, development, and manufacture of electronic locking systems, GANTNER offers its customers not only state-of-the-art technology, but also global partnerships with locker and furniture manufacturers with whom we collaborate to produce tailor-made solutions.

In accordance with the highest European environmental and quality standards, the entire production of the NET.Lock system is environmentally friendly and carried out within the European Union. It is designed and manufactured under ISO 14001 / ISO 9001 environmental and quality management conditions. The NET.Lock system is manufactured in accordance with Green IT standards, requiring minimum or no maintenance during use and extremely low energy consumption. GANTNER is part of the SALTO Group.

5.1 Warranty and system support

The NET.Lock system comes with a standard one-year warranty, with the option to extend the warranty up to five 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 provides a project-specific operation and maintenance manual in electronic format containing all project-specific drawings, information, datasheets and manuals.

The system is supported by the GANTNER Support Team. The competence of the support team is ensured by the combined knowledge of more than 25 years in the intricate workings of GANTNER hardware and software products. System support is provided during normal business hours in English and German with an 8-hour response time. Customized support contracts are available upon request.

5.2 Client training

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

The GANTNER Academy draws on the expertise of sales, product management, R&D and industry partners to deliver courses that educate customers on our latest products, projects and other important developments, all aimed at empowering organizations and individuals.

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

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 intended but also that our stringent security requirements are met.

5.4 Customer security assessments

GANTNER takes the security of our customers and our systems in general very seriously. If you require specific information in addition to that provided in this manual, or if you require our assistance in carrying out a security risk assessment in relation to the NET.Lock system, GANTNER has resources available to meet these needs. We are experienced and motivated in working with customers to meet their individual risk analysis requirements.

6 FREQUENTLY ASKED QUESTIONS

6.1 Hardware components

6.1.1 Does the system support 802.1x authentication?

Yes, the latest GANTNER main controllers (GC7.xxxx series) support 802.1x authentication. The GAT NET.Controller M 7020 main controllers do not 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 (GbE) connectivity?

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

6.1.4 Is the communication protocol encrypted?

Yes, please refer to section “3.5 TLS communication” for more information.

6.1.5 Which operating system do the main controllers use?

The main controllers of the GAT NET.Controller M 70x0 and S 70x0 series use a Keil RTX Real-Time Operating System. The latest GC7.xxxx 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 GAT NET.Controller 70x0 main controllers can operate without an SD card. However, removing the SD card means that certain functions, e.g., diagnostic logs and firmware updates, become unavailable. The GC7 series controllers and GT7 series terminals always need to operate with an SD card.

6.1.8 What is the NETBios name of the main controllers?

The default NETBios name (host name) of the GAT NET.Controller M 70x0 main controllers is “LC7xS0000000000” and of the GC7.xxxx “GC7_S0000000000”. The last 10 digits is the serial number of the main controller that is printed on the controller label. The NETBios 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.

6.2 Software components

6.2.1 Does Relaxx support periodical pushed password changes?

Yes, when Active Directory is used (recommended) for user authentication. Relaxx itself does not force the operator to periodically change their password.

6.2.2 Are there minimum password requirements for Relaxx?

When using Active Directory as recommended, the password policy from Active Directory is adopted to avoid policy conflicts. When not using Active Directory, the minimum length of a password is 7 characters, and it must contain 1 number, 1 upper-case letter, and 1 lower-case letter.

6.2.3 Can the Relaxx server be redundant for availability during, e.g., software updates?

A virtual installation (warm instance) could be switched manually but this needs to follow a clear procedure. The JSON connection especially must be properly closed on both ends and properly started after manually switching the installation.

6.2.4 Can Relaxx run in the cloud?

Yes, it can run on a virtual machine in the cloud. A secure connection to the main controllers is required, e.g., a VPN connection or similar set up by the customer's IT department. GANTNER recommends testing to ensure that the Relaxx VM / cloud system meets the customer's individual performance, latency and reliability expectations.

The Relaxx database can also be hosted in the cloud, e.g., with Amazon RDS.

6.2.5 Can Relaxx be deployed using MSI packages?

It is possible to deploy the Relaxx server and/or Relaxx client to multiple computers in your company or organization by using an MSI package. More information is available in the Relaxx Installation manual.

6.2.6 Can two Relaxx databases be merged together into one?

Currently, there is no automated mechanism to merge the databases of multiple Relaxx instances into a single database.

6.2.7 What options are there for importing data into the Relaxx database?

The options are:

- File-based importation (e.g., CSV file).
- Via JSON or REST interface.
- Manual importation (least efficient method).

6.2.8 How many locker groups can be configured in Relaxx?

2000 locker groups can be configured and the locker numbering within each group must be unique.

6.2.9 How do I plan Relaxx with high availability and site resilience?

It is possible to provide a passive fail-safe instance ("warm standby") on another server.

6.2.10 Can I change the ports in Relaxx?

Yes, the ports of the software components can be changed in the configuration file. These include the API interfaces and the Relaxx clients. The port to connect the Relaxx client to an SQL Server can be changed, e.g., in the configuration window of the database connection (during the initial startup).

6.2.11 Can Microsoft Windows® and SQL Server® updates be made regularly and automatically or only when GANTNER communicates the release of an update to its customers?

Updates (but not hotfixes) of supported operating systems and databases can be installed in principle provided that certain updates are not explicitly rated as "incompatible" by GANTNER.

6.2.12 Is there support for running applications on a virtual server with Hyper-V?

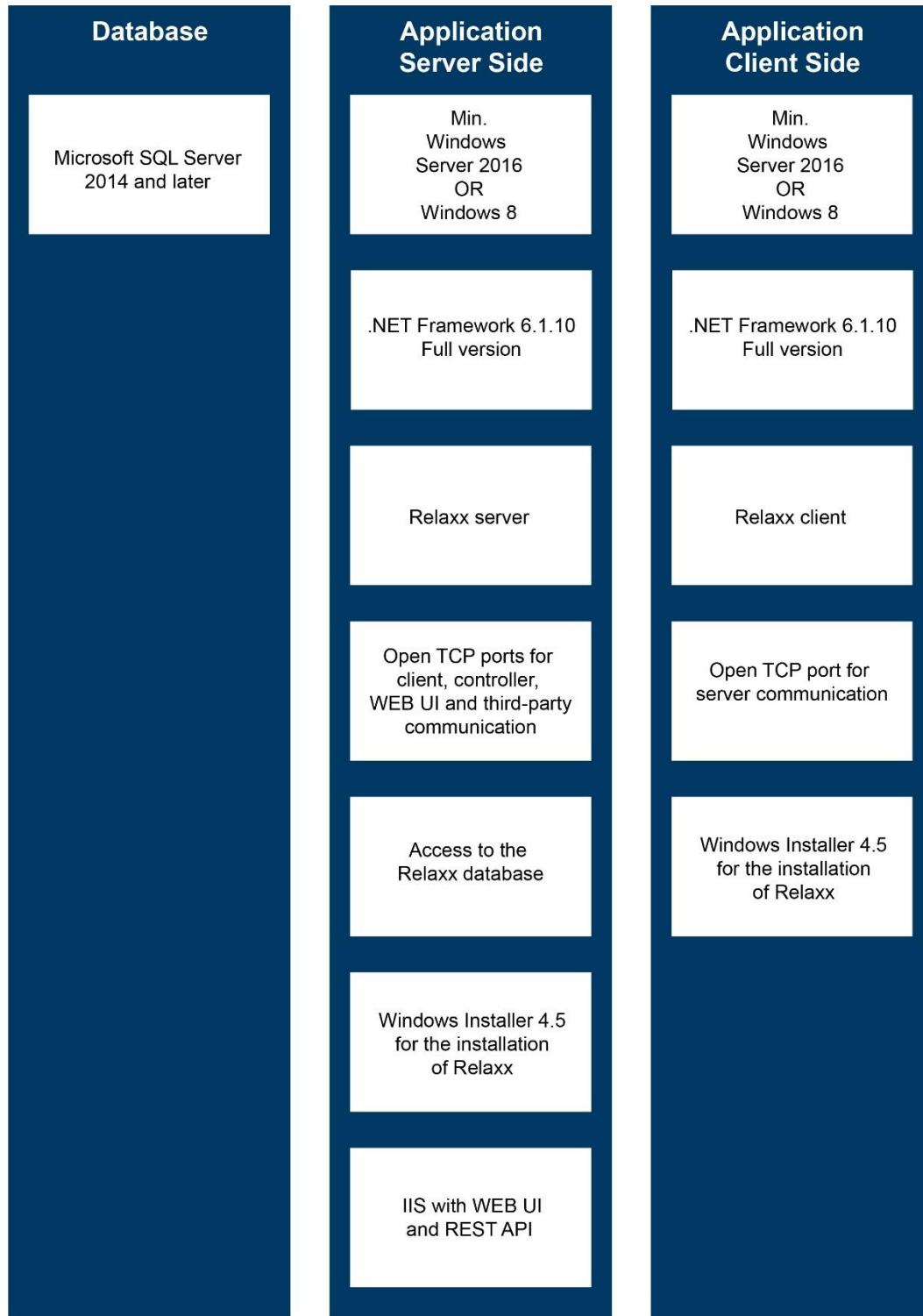
Yes, core applications, including Microsoft® SQL Server®, are able to operate in virtualized Hyper-V Windows environments.

6.2.13 Can Relaxx WEB UI run on multiple IIS instances behind a load balancer?

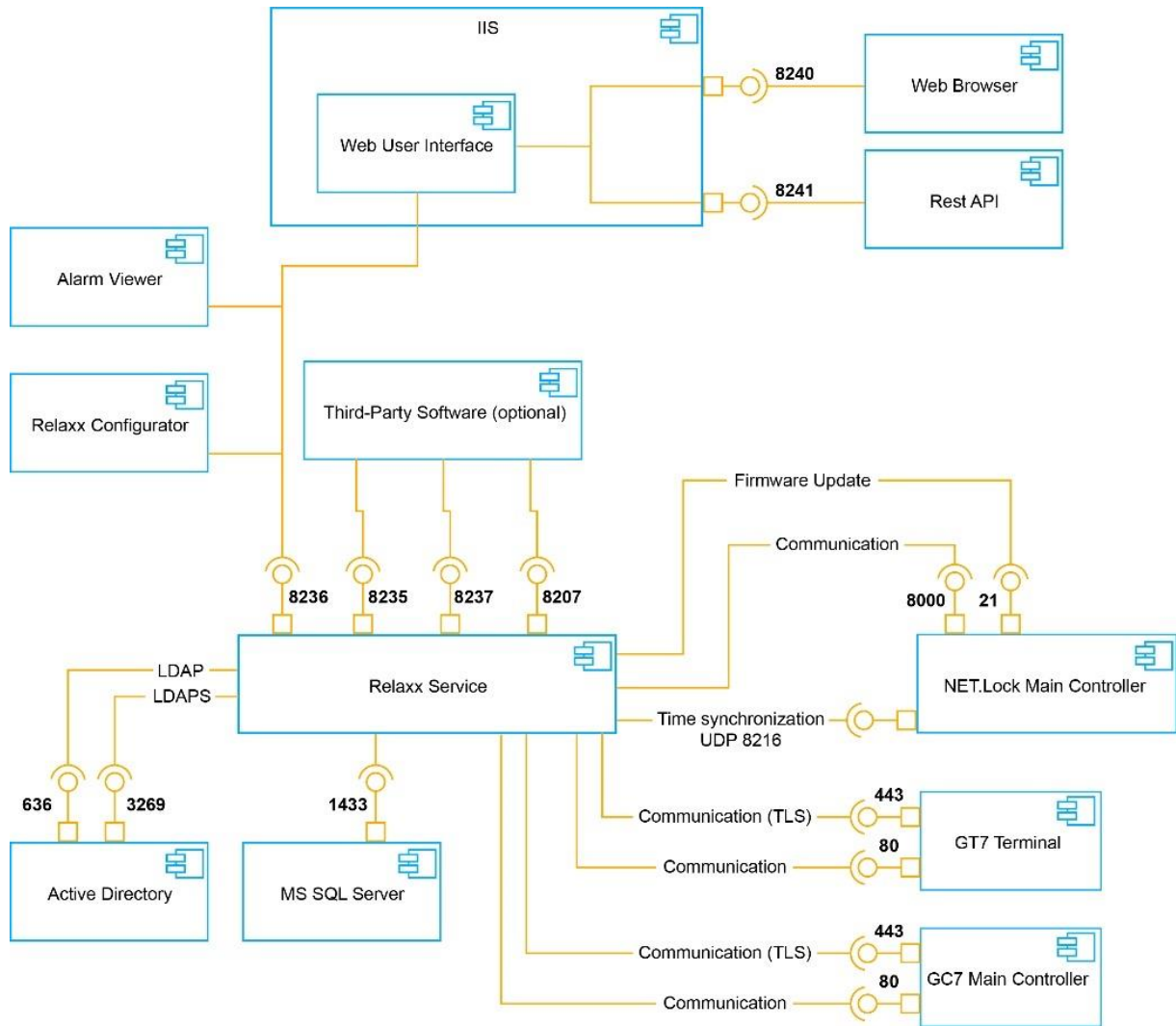
No, this is not possible as some security information cannot be shared across multiple IIS instances.

7 APPENDIX

7.1 Component model



7.2 Target interfaces



NOTE:

This manual is valid as of June 3, 2024. It is subject to change.
Amendments can be made without prior notice at any time.



GLOBAL
PARTNER NETWORK



40+
OFFICES



40,000+
PROJECTS WORLDWIDE



40+ MILLION
USERS DAILY

Gantner

A SALTO GROUP COMPANY

www.gantner.com

© 2024 GANTNER ®

GANTNER reserves the right to change technical specifications,
designs and services without prior notice.

Photos: GANTNER, shutterstock, IMSinteriors, SALTO Systems

SCAN FOR CONTACT

