

SIMATIC RTLS

Locating systems SIMATIC RTLS Network Configuration

Application Manual

Introduction

1

Cybersecurity
recommendations

2

Overview

3

Functions in the menu bar

4

Symbols in the tree
topology of the
Locating Manager and the
clients

5

Configuration

6

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Introduction	5
2	Cybersecurity recommendations.....	9
3	Overview.....	13
4	Functions in the menu bar.....	15
5	Symbols in the tree topology of the Locating Manager and the clients	17
6	Configuration.....	19
6.1	Overview of the configuration	19
6.2	Gateways, anchors and transponders	19
6.2.1	Adding a gateway, anchor and transponder manually	20
6.2.2	Gateway and transponder groups.....	20
6.2.3	Firmware update for device classes.....	21
6.2.4	Tolerance of the heartbeats.....	22
6.3	Device configurations.....	22
6.3.1	System information.....	22
6.3.2	Internal and external voltage.....	23
6.3.3	Last heartbeat.....	23
6.3.4	Ping.....	23
6.3.5	Using a device in the network / enabling localization	24
6.3.6	System information and firmware update of individual devices	24
6.3.7	Spatial position of the infrastructure devices	24
6.3.8	IP configuration of the gateways.....	25
6.3.9	Values on node (gateways)	25
6.3.10	LED flashing (gateways and transponders)	25
6.3.11	Readiness to receive (transponder).....	25
6.3.12	Resetting the error memory (gateway and transponder)	26
6.3.13	Importing device data	26
6.4	System	26
6.4.1	Network	27
6.4.2	Enabling/disabling network	27
6.4.3	Exploration	28
6.4.4	Routing information.....	28
6.4.5	Routes	30
6.4.6	Metrics	33
6.4.7	Services	34
6.4.8	Firmware update.....	35
6.4.9	License management.....	36
6.4.10	Protocols.....	37
6.4.11	Scan frequency band	38
6.4.12	System backup.....	39
6.4.13	Service monitoring	39
6.4.14	System parameter	40

Introduction

Purpose of this documentation

The document supported you during the installation and configuration of the "SIMATIC RTLS Network Configuration" client, which is a component of the locating software "SIMATIC RTLS Locating Manager".

Validity of this documentation

This documentation is valid for version 3.1 of the "SIMATIC RTLS Locating Manager".

Additional information

You can find additional information on the SIMATIC RTLS products mentioned in this documentation in the Readme file or on the Siemens support pages.

Link: (<https://support.industry.siemens.com/cs/en/en/ps/25277>)

Trademarks

SIMATIC RTLS® is a registered trademark of Siemens Aktiengesellschaft.

Industry Online Support

In addition to the product documentation, the comprehensive online information platform of Siemens Industry Online Support offers support at the following Internet address: (<https://support.industry.siemens.com/cs/us/en/>)

Apart from news, there you will also find:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option submitting a support query: (<https://support.industry.siemens.com/My/us/en/>)
- Our service offer:
Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact information on the Internet at the following address: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

SITRAIN - Training for Industry

The training offer includes more than 300 courses on basic topics, extended knowledge and special knowledge as well as advanced training for individual sectors - available at more than 130 locations. Courses can also be organized individually and held locally at your location.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address: (<https://www.siemens.com/us/en/products/services/digital-enterprise-services/training-services/sitrain.html>)

RTLS Technology and Practice (ID-RTLS-TP)

Training and certification

After completing the RTLS certification training, you will be able to plan and implement small and medium-sized RTLS projects and provide efficient and multifaceted support in large projects. Your RTLS basics will be strengthened and, building upon them, you will receive new tools of the trade in order to offer customers the optimal solution for them. The complete project sequence is taken as a reference and important steps, resources and work results for each phase are presented. Comprehensive practical exercises in connection with troubleshooting techniques and a great deal of input from industrial projects allow you to internalize a confident approach to working with different types of localization projects. With the training documents, you also receive extensive reference material for your daily work.

Link: (<https://www.sitrain-learning.siemens.com/EN/en/rw35251/Industrielle-Identifikation-RTLS-Technologie-und-Praxis>)

Cybersecurity notes

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines, and networks.

In order to protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions form one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For more information on industrial cybersecurity measures that may be implemented, please visit: (<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends performing product updates as soon as they are available and using only the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under: (<https://new.siemens.com/global/en/products/services/cert.html>)

Note on firmware/software support

Check regularly for new firmware/software versions or security updates and apply them. After the release of a new version, previous versions are no longer supported and are not maintained.

Recycling and disposal

The products are low in harmful substances, can be recycled and meet the requirements of the Directive 2012/19/EU for disposal of waste electrical and electronic equipment (WEEE).

Do not dispose of the products at public disposal sites.

For environmentally compliant recycling and disposal of your electronic waste, please contact a company certified for the disposal of electronic waste or your Siemens representative.

Note the different national regulations.

Cybersecurity recommendations

General

To prevent unauthorized access, note the following cybersecurity recommendations:

- You should make regular checks to ensure that the devices meet these recommendations and/or other cybersecurity guidelines.
- Evaluate your plant as a whole in terms of cybersecurity. Use a cell protection concept with suitable products (<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>).
- Keep the software up to date. Check regularly for security updates for the device. You can find information on this at the Industrial Security (<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>) website.
- Only activate protocols that you require to operate your system.
- Whenever possible, always use the variants of protocols that provide enhanced security (e.g. SNMPv3).
- Connections over unsecured network areas must be secured by security mechanisms such as SSL VPN.
- Always click on the "Log out" button in the submenu of the user profile when you have finished working with the Web app.
- Restrict access to the software and its add-on programs (e.g. database) to qualified personnel.
- Use the user and role administration to configure the rights of the users according to their authorizations.
- Use corresponding certificates including private keys in a local certificate store of the operating system. Also make sure that these are not readable for users who do not have the administrator role.
- Make sure that the databases are updated and managed regularly by means of modern and secure methods.
- Avoid adding security-relevant information, e.g. gateway or transponder names, that can be read by unauthorized persons.

Users, roles and passwords

- Define rules for the use of the software and assignment of passwords. Configure these roles using the "RTLS-LM-IAM" component and Active Directory.
- Regularly update the passwords to increase security.
- Change user names and default passwords of the databases before you use the software. For the SIMATIC RTLS Locating Manager, a changeable user and an editable password is used for each installation. You can change the password via the respective DBMS version. The user data is saved in the RTLS-LM-IAM database. The RTLS-LM-IAM administrator needs to be created during the SIMATIC RTLS Locating Manager installation process.

- Create users and user groups with the "RTLS-LM-IAM" component and assign the available roles, which are tailored to the scope of authorization of each user/user group, to these users. Do not exclusively use the "System administrator" role that is present by default, and disable the "System administrator" user that is present by default after new users with corresponding rights have been created.
- Only use passwords with a high password strength. Avoid weak passwords, for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems or after it has expired.

Physical access

Restrict physical access to the device to qualified personnel.

Automation License Manager

If you do not require the network functions of the Automation License Manager, deny access to its functions in your firewall.

Software (cybersecurity functions)

- Keep the software up to date. Check regularly for security updates for the product. You can find information on this at the website (<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>)
- Only activate the protocols, functions and interfaces that you require to operate your system.
- Restrict access to the device with a firewall or rules in an access control list (ACL - Access Control List).
- The option of VLAN structuring provides good protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Enable the logging functions to record changes and access attempts. Check the logging information regularly. Enable, for example, NTP synchronization of the operating system on the host PC and set up access to an NTP server.

Secure and non-secure protocols

- Check whether the use of SNMPv2c is necessary. SNMPv2c is classified as non-secure. The product provides you with suitable setting options.
- When SNMP is enabled, change the community names. When no unrestricted access is necessary, restrict access with SNMP.

- Use secure protocols when access to the device is not secured by physical protection measures. The following protocols provide a secure alternative:
 - TLSv1.0 → TLSv1.2 or TLSv1.3
 - SNMPv2c → SNMPv3
 - SMTP (simple) → SMTP via SSL
 - LDAP → Kerberos (IAM connection to Active Directory)
- Avoid or disable non-secure protocols. For historical reasons, these protocols are available, however not intended for secure applications. Use non-secure protocols on the device with caution. Instead, use the REST and gRPC protocols over the API interface.
- To prevent unauthorized access to the device or network, take appropriate protective measures against non-secure protocols. In addition, use encrypted hard disks to ensure that sensitive data can only be read after login.

List of available protocols (local access via a local network)

The following is a list of all available protocols and their ports through which the RTLS devices/products can be accessed. Note the list when you configure a firewall.

Explanation for table:

- Service
Specifies the service that the RTLS devices/products support.
- Protocol/port number
Specifies the protocol and the port number that are assigned to the service.
- Default port status
 - Open
The port is open by default.
 - Closed
As default the port is closed.
- Authentication
Specifies whether the communication partner is authenticated.
 - Yes: Authentication takes place.
 - No: Authentication does not take place.
 - Optional: Authentication takes place by default, but can be disabled.

- **Encryption**
Specifies whether the transfer is encrypted.
 - Yes: Transfer is encrypted.
 - No: Transfer is not encrypted.
 - Optional: Transfer is encrypted by default, but can also be configured as unencrypted.
- **Externally available**
Specifies whether the protocol requires external connections.
 - Yes: The functionality requires this port to be accessed. Restrict access to necessary hosts.
 - No: No port within the firewall needs to be open. Access restrictions are recommended.
 - Optional: The functionality depends on your system. Restrict access to necessary hosts if the system requires remote access.

Service	Protocol/ Port number	Default port status	Port configurable	Authentication	Encryption	Externally available
Data export modules	TCP/variable	Closed	Yes	No	No	Optional
Email	TCP/variable	Closed	Yes	Optional	Optional	Yes
TeeRevProxy	TCP/variable	Closed	Yes	No	No	Optional
ReverseProxy	TCP/80	Open	Yes	No	Optional	Yes
ReverseProxy	TCP/443	Open	Yes	No	Optional	Yes
Wireless network	TCP/8000	Open	Yes	No	No	Yes
Heartbeat Monitor	UDP/8000	Closed	No	No	No	Yes
Internal server communication	TCP/8001	Open	No	No	No	No
Heartbeat Monitor	TCP/8080	Closed	Yes	No	No	Yes
gRPC-Gateway	TCP/8081	Open	Yes	No	No	No
IAM Keycloak	TCP/8082	Open	Yes	Yes	Yes	No
ePaper Manager	TCP/8083	Open	Yes	No	Yes	No
Client connection	TCP/9500	Open	Yes	Yes	Yes	Optional
WAMP router	TCP/12344	Open	No	Yes	No	Optional
Prometheus	TCP/40492	Open	Yes	Yes	Yes	No
WindowsExporter (Prometheus)	TCP/40493	Open	Yes	Yes	Yes	No
GatewayPositionIntegrityExporter	TCP/40494	Open	Yes	Yes	Yes	No
gRPC-ClientCommunication	TCP/50051	Open	Yes	Yes	No	No
gRPC-Logging-Service	TCP/50052	Open	Yes	Yes	No	No

Overview

General

This document describes how to use the "Network configuration" client for the Locating Manager.

Note

The client may only be used by experienced and trained users.

Application

With the "Network configuration" client, you can create, manage or delete gateways, anchors and transponders of the RTLS locating system. These devices can also be grouped together. In addition, the "Network configuration" client provides a variety of configuration and management options.

Start client

You start the "Network configuration" client (NWConfig.exe) under "Start > SIMATIC RTLS Locating Manager > Network configuration"

Definition of terms

Term	Description
Gateway	Infrastructure device that uses the Ethernet port
Transponder (TAG)	Mobile device to be localized in RTLS localization network
Infrastructure devices	Gateways with and without using the Ethernet port
Nodes	All gateways and transponders of an RTLS localization network
Locating Manager server	Software that processes the localization data into position data that can be visualized
Client	Software for management and control of the RTLS locating system and the nodes
Localization	Position determination
Ranging	Distance measurement between a transponder and a gateway
Position calculation	Calculation performed by the Locating Manager server of the position coordinates based on the localization data and various filters
Virtualization	Graphical representation of the determined position data
Exploration	Automatic search process to find unknown, for example, newly installed nodes within the wireless range of the RTLS localization network
MHI	Multi-hypothesis initialization Determines the final position from multiple individual positions
TWR	Two-Way Ranging Determines the delays of the signal and calculates the distance between the nodes.

Term	Description
TDOA	Time Difference of Arrival Time-based process to determine the positions of the transponders
UWB	Ultra-wideband Radio technology with wireless transmission

Functions in the menu bar

Connecting and disconnecting

After the client starts, click the "Connect" button to connect to the Locating Manager and log in. As an alternative, you can make a connection using the menu "File > Connect".

The status of the connection is displayed on the left in the status bar.

When a connection has been established, the connection symbol changes to "Disconnect", indicating an existing connection. The red connection symbol "Connect" indicates that there is no connection.

If a connection to the RTLS locating system could not be established, an error message is issued after about 20 seconds. The connection symbol changes to "Connect" and "Disconnected" appears in the status bar.

Changing the language

You can switch between "German" and "English" under "Options > Language".

Search

Under "Options > Search", you can search for any terms, descriptions or even addresses. Any hits found are displayed in the user interface. If there are several search results, the main window switches to the selected hit. Using the F3 key, you can switch from one result to the next.

Search options

Under "Options > Search options", you can restrict the search range to specific node types, transponders, transponder names, antenna positions or types, or specific text boxes. The text boxes for selection for the transponders can be individually assigned. You can also open the "Search options" dialog box by clicking on the "Options" button in the search window.

Automatically look for a better picture and display it

You can find this setting under "Options > Automatically look for a better picture and display it".

When this option is selected, the client automatically tries to switch to the view area that best matches the currently displayed area. This allows you to use detailed images for close zoom levels or overview images.

Clear log

Under "Options > Clear log", you can delete the messages displayed in the output window for logging data. Newly added messages are displayed again.

About (version information)

You can view the following information with "About > About":

- Product name
- Name of the client
- File version of the client
- Log version of the server
- Current ID of the session (if you are logged in)
- Current ID of the user (if you are logged in)
- Copyright

Update picture automatically

You can find this option under "Options > Update picture automatically". This option allows you to specify whether clients automatically check for and use updated maps on the server when they start.

List devices without a license in the tree

If you enable this option, devices that do not have a license at the given time are nevertheless displayed in the tree topology.

Symbols in the tree topology of the Locating Manager and the clients

5

In all clients of the Locating Manager in which anchor, gateways and transponders are displayed, you can determine the operating status of the device using the following symbols:

Anchor	Gateway	Transponder	Description
			Device is offline and does not send a heartbeat
			Device is online and ready for operation
			Device is online and ready for operation, but with low voltage warning Check the supply voltage. Replace the batteries or charge the rechargeable battery.
-	-		Transponder is online, operational and being moved
-	-		Transponder is online, operational and being moved, but with low voltage warning Check the supply voltage. Replace the batteries or charge the rechargeable battery.
-	-	 ... 	Transponder is in "via static configuration" operating mode
-	-	 ... 	Transponder is online and ready for operation, but with low voltage warning Check the supply voltage. Replace the batteries or charge the rechargeable battery.

Configuration

6.1 Overview of the configuration

You can make the following configurations in the "Network configuration" client:

- Create, configure and delete nodes
- Create, configure and delete gateway groups
- Create, configure and delete transponder groups
- Perform firmware updates
- Create and manage routes
- Create and manage metrics
- Start exploration
- Enable or disable localization globally
- Update the status of the Data Export Service
- Run system backup
- Scan for devices in the frequency band
- Configure service monitoring
- Manage license
- Manage logging of localization results
- Export and import device coordinates
- Display system information
- Configuring event management

Most of the configurations of the respective device types are managed in the tree topology under "Gateways" and "Transponder". New anchors can be created manually or localized automatically via exploration ("Tree topology > System > Network > Start"). The exploration procedure is described in more detail in the section "Exploration (Page 28)".

Note

Any changes to the device configurations must be confirmed by clicking the "Save" button.

6.2 Gateways, anchors and transponders

The gateway establishes the connection between the wireless network and the Locating Manager server and is used as a measuring point for the localization and as a collection and transmission point of the gateway data.

6.2 Gateways, anchors and transponders

Transponders are the mobile units of the RTLS locating system. Their positions are determined by the Locating Manager server, e.g. from measurements between the measuring points and the transponders.

Select "Gateway" in the tree topology to add a gateway or anchor as well as a gateway group. Select "Transponder" to add a transponder or a transponder group.

Select a specific device in the tree topology to rename, delete, move it to a group, update its firmware or set and configure the position of gateways and anchors.

6.2.1 Adding a gateway, anchor and transponder manually

You can manually add devices to the Locating Manager using the respective buttons "New gateway", "New anchor" and "New transponder". However, gateways are localized automatically by the Locating Manager. You can automatically add anchors using exploration (section "Exploration (Page 28)") and transponders are also added after startup, so that manual addition of devices is only necessary in exceptional situations.

The network address of the device (see nameplate of the respective device), the freely selectable name, the device group to be determined via the drop-down list and the position for gateways and anchors are queried via the text boxes. The IP address and the port within the local network are also required for gateways. Clicking on the "Create" button adds the device to the RTLS locating system.

6.2.2 Gateway and transponder groups

You cannot delete the "DEFAULT" gateway group or "DEFAULT" transponder group created by default, but you can rename them.

Create a new device group

Proceed as follows to create a new device group:

1. Click the "New gateway group" or "New transponder group" button.
2. Enter a name and description for the device group.
3. Click the "Save" button.

Moving devices to other groups

To move devices out of one group into another, follow the steps below:

1. Click the button "Move/Delete Gateways" or "Move/Delete Transponder".
2. In the "Source group" drop-down list, select the group in which the device you want to move is located.
3. In the "Target group" drop-down list, select the group to which you want to move the device.

4. Select the check boxes for the devices you want to move.
 - Use the "All" button to select all devices at once.
 - Use the "None" button to deselect all devices at once.
5. Confirm your selection by clicking "Move".

Note

Alternatively, you can select an individual device in the tree topology to move it to another group. To do this, select the desired group in the "Group" drop-down list and click the "Save" button.

Deleting devices

Proceed as follows to delete a device:

1. Click the button "Move/Delete Gateways" or "Move/Delete Transponder".
2. In the "Source group" drop-down list, select the group that contains the device you want to delete.
3. Select the check boxes for the devices you want to delete.
 - Use the "All" button to select all devices at once.
 - Use the "None" button to deselect all devices at once.
4. Confirm your selection by clicking "Delete".

6.2.3 Firmware update for device classes

In the tree topology under "Gateway", "Anchor" or "Transponder", there is a "Firmwareupdate" section for each device. In this section, you can determine all devices of the respective type and transfer a specific firmware to all devices of the selected type. The firmware update for individual devices is described in the "System information and firmware update of individual devices (Page 24)" section. Under "System > Firmwareupdate", you can perform more differentiated updates with extended selection and sorting options (section "Firmware update (Page 35)").

Only Siemens firmware may be used for the Locating Manager. You can recognize files of the Siemens firmware by the "*.cagl" extension. The installation or storage path for the firmware is the installation folder of the Locating Manager, by default "%ProgramData%\Siemens\SIMATIC RTLS Locating Manager\Firmware".

Clicking "Select firmware" displays all available firmware versions. Select the desired software from the drop-down list and transfer it to all devices of the selected type by clicking the "Transfer..." button. The firmware transfer process may take a few minutes. Do not switch off the devices during the process. Status messages and errors are displayed in the output window for logging data.

6.2.4 Tolerance of the heartbeats

The tolerance (cycles) in the heartbeat configuration determines how many heartbeats of a device in the respective group may fail until the connection to the device is displayed as terminated. The additional tolerance [ms] indicates the waiting time between two heartbeats to compensate for signal propagation delay effects. Click "Save" after a change has been made.

6.3 Device configurations

The network address output in the view of a specific gateway, anchor or transponder represents the wireless address of the device in the Locating Manager. It is indicated on most devices and must be entered when creating devices manually. You can change the name of the device. It is also possible to move a device to another group using the "Group" drop-down list. If you want to move the mouse pointer onto the "Name" info field, device-specific measured values are shown as tooltip. When advanced mode is active, additional data is displayed.

Note

Any changes to the device settings must be confirmed by clicking the "Save" button.

6.3.1 System information

Information about the firmware of the device is displayed in the "System information" section.

The advanced system information is displayed as tooltip when you move the mouse pointer over the system information data. This is additional information for customer support.

System information	
Project:	GANYMED
Subproject:	TY41
Legacy Serial-No.	A08195
Software version:	V 002.002.001
Record version:	GANYMED_TY41_...
Legacy Article Nu...	6021999

If the firmware file of a node does not exist on the Locating Manager server, you cannot configure this device or update it with a new firmware. This is highlighted in red. If you move the mouse pointer over the display, information is displayed about the firmware file.

You can find additional information on the firmware files on the Support pages: (<https://support.industry.siemens.com/cs/search?search=rtls&type=ProductSupport%2CCatalog%2CCertificate%2CCharacteristic%2CDownload%2CDownloadSoftwareArchive%2CExampleOfUse%2CFaq%2CManual%2CProductNote%2CSlk%2CForum&lc=en-US>)

6.3.2 Internal and external voltage

The information fields "Internal voltage" and "External voltage" not only indicate the input voltage currently measured by the device, but also provide information about the received IO signals (input/output). For transponders, the information field additionally indicates whether the transponder is currently moving (Acc: 1) or do not move (Acc: 0).

Example:

```
Voltage 5.8V 0% (IO 0x00 Virt0x01) (Acc: 1)
```

External voltage is the voltage transmitted from outside to a device, for example by a power supply unit. Internal voltage, on the other hand, describes the status of a device-internal power supply, such as batteries or rechargeable batteries built into the device. The voltage value shown in each case depends on the device type being used.

6.3.3 Last heartbeat

The "Last heartbeat" information field indicates when the last heartbeat was received by the device. You manually request a heartbeat by clicking "LS" in the "System information" section.

Example:

```
Last heartbeat 2019-09-27 14:45:38.000
```

This line is missing for devices that have never sent a heartbeat to the server. Transponders are not always ready to receive. This may delay the request for a heartbeat.

6.3.4 Ping

You can send text message to the device using the "Ping" button in the "System information" section. The duration until the response to the request of a ping is output in the output window for logging data. Transponders are not always ready to receive. Requesting a ping may be delayed as a result.

Time	Sender	Message	Level
12.10.2017 18:04:23	Info	[17:85:00:00:00:a6] A 00a6 ping: 1 ms	5

6.3.5 Using a device in the network / enabling localization

The infrastructure devices (gateways and anchors) detected by the exploration are automatically enabled for use. You need to perform this activation manually for transponders. Select the "Localization" option for each transponder that is to be localized.

6.3.6 System information and firmware update of individual devices

The "System Information" dialog box allows you to query the system information and transfer firmware to the device highlighted in the tree topology .

When you click the "Read" button, the firmware version and other information about a gateway, anchor or transponder is updated in the text box below.

You can select the firmware to be transferred in the drop-down list. You confirm the selection by clicking the "Select firmware" button and the firmware is transferred to the device by clicking the "Transmit..." button. Status messages and errors are displayed in the output window for logging data.

Sender	Message	Level
Info	[17:85:00:00:09:4d] A 094d ping: 15 ms	5
Info	[17:85:00:00:01:b6] A 01b6 ping: 36 ms	5
Info	[17:85:00:00:00:a6] A 00a6 ping: 21 ms	5
Info	[17:85:00:00:0b:31] G 0b31 ping: 30 ms	5

6.3.7 Spatial position of the infrastructure devices

The spatial positions of the individual gateways and anchors with the respective x, y and z coordinates must be entered manually if there is no corresponding file in "*.csv" format with this data. The user interface appears for the respective infrastructure devices selected in the tree topology. The position of the infrastructure devices refers to a freely selectable coordinate origin, which represents the reference point for all measurements and for the visualization. Click "Save" after entering the coordinates.

Under "System > Network", you can export all entered position coordinates as a file in "*.csv" format to import them later. The information in the file with "*.csv" format must be structured as follows in order to be read and correctly assigned by the Locating Manager.

```
Name;x;y;z
Gateway 2;-618;-66;0
Gateway 1;96;-43;85
```

The name is the name freely assigned to the device in the Locating Manager (section "Device configurations (Page 22)"). You can create the file in "*.csv" format from the Excel table with the position data of the surveyor.

6.3.8 IP configuration of the gateways

The IP address identifies a gateway in the local Ethernet. This address depends on the device and is provided by the default configuration with "192.168.1.232". If you use "DHCP", then the gateway receives its address automatically from a DHCP server in the local network. The port is 1010.

The Ethernet configuration for gateways is performed using SINEC PNI: (<https://support.industry.siemens.com/cs/ww/en/view/109804190>)

6.3.9 Values on node (gateways)

NOTICE

Qualified personnel

All IP configuration related configurations may only be performed by qualified personnel with expertise in the client "Network configuration".

In the "Values on node" section, you can read the values set on the device relating to its network operation, set new values or the default value by clicking the respective button. After each change, click "Reset" to enable the new values for the device.

The values to edit are Duplex mode, DHCP mode, Device IP, Server IP, Subnet mask, and Gateway IP. It may be necessary to change these values, for example, during the commissioning of the Locating Manager to adapt to the local IT network or to change your local network infrastructure.

6.3.10 LED flashing (gateways and transponders)

For gateways and transponders that have an LED and support the functionality to make it flash, you can start the flashing of the LED via a button in their device configuration. To do this, click the "Flash LED" button. This sends a command to the device that causes the LED to flash for 15 seconds with a specific pattern. The log window will then show you a message about whether or not the command was successfully delivered.

6.3.11 Readiness to receive (transponder)

The "Readiness to receive" function is only available in advanced mode.

You can configure the following parameters:

Parameter	Example value	Description
After direct messages [ms]	30	After the transponder has received a direct message, it remains available for this time period in milliseconds.
After messages to the server [ms]	130	After the transponder has received a direct message, it waits for messages from the server for this time period in milliseconds.

After broadcasts [ms]	130	After the transponder has received an indirect message, it waits for messages from the server for this time period in milliseconds.
After service messages [ms]	130	After the transponder has received a service message, it remains available for this time period in milliseconds.

The higher the time periods are configured, the lower the expected battery life of the transponders.

If the time periods are configured too low, it is possible that the transponders can no longer be reached.

6.3.12 Resetting the error memory (gateway and transponder)

The "Reset error memory" function is only available in advanced mode.

Every gateway and every transponder has an internal error memory for collecting independently detected error situations (see the corresponding operating instructions for details). Clicking the "Ers Reset" button resets all error memory entries on the device. If all values of the error memories are already at 0, this has no effects.

6.3.13 Importing device data

The "Import devices" function is only available in advanced mode.

When device data is imported, you can create devices or configure values, such as names or positions of devices, via a csv file. Click the "Devices" button for "Configured import" under "System > Network". When this function is executed for the first time, you are informed that the required section does not yet exist in the ini file and the section with default values needs to be created. When you click "OK", the section is entered in the ini file. The parameters are set via the configuration file. Observe the notes in this configuration file. Then select a corresponding csv file with the devices to be imported. If the structure of the csv file is correct, the devices are imported or updated.

6.4 System

You can perform the following actions under "System" in the tree topology:

- Network-specific actions, such as exploration
- Enable and disable localization service
- Run system backup
- Scan for devices in the frequency band
- Update of the firmware of the devices
- Back up database settings

- Manage licenses
- Make configurations for logging

You can also see information about the current server version and the scope of licenses.

6.4.1 Network

You can control the wireless network and its functionalities under "System > Network" in the tree topology.

You can perform the following actions:

- Enable or disable the wireless network
- Start exploration
- Import pre-configured device coordinates or save existing coordinates
- Import saved coordinates
- Query and display routing information

The "TDOA time master" sub-item enables the definition of the time master for the "Time-Difference-Of-Arrival" (TDOA) technology. The cyclically transmitted signals of the transponders are received in a time-synchronous network and the propagation time difference of the signals is measured. The Locating Manager server uses the propagation time difference to determine the position.

6.4.2 Enabling/disabling network

Click "Stop tasks" or "Start tasks" to disable or enable the Locating Manager's communication services that are relevant for localization. This is displayed in the output window for logging data. You can only perform localization when the network is enabled.

6.4.3 Exploration

If at least one gateway has been configured, you can automatically search the topology of the RTLS localization network via the exploration in the tree topology under "System > Network". Starting from this gateway, exploration searches the wireless network for additional infrastructure devices. All wireless receivers are located within range, integrated into the network via static routes, automatically assigned to the respective "DEFAULT" group in the tree topology and configured. Based on the resulting network, a search is conducted for further wireless systems which could not be reached in the first step. If no further gateways or anchors have been located, the exploration is complete. Exploration may take several minutes depending on the size of the RTLS localization network. The "Start" button below the exploration configuration is disabled during this time. The exploration progress is recorded in the output window for logging data.

Note

If gateways with Ethernet are used, you need to perform an exploration. At the end of the exploration, enable the gateways to connect to the transponders.

When you integrate new gateways into an existing production system, this setting is not active to avoid affecting the existing production system.

Transponders are not localized with exploration. Instead, they are automatically added and included in the tree topology if the RTLS localization network has been set up correctly. If you have enabled the "Localization" option in the transponder display screen (section "Using a device in the network / enabling localization (Page 24)"), the transponders can be located. If you have enabled "Partial exploration", you can select individual nodes which serve as new starting points for partial exploration.

6.4.4 Routing information

Define the device positions so that the functions offered under "Routing information" can be meaningfully used. You can get a better visualization if you have created and scaled a location view in "Localization Configuration" client beforehand. You can find details on the procedure in the "Location view" section of the "Localization Configuration" client documentation. The "Routing information" section includes the routes and metrics. The routes describe which path the data take from the transponders to the server and vice versa, i.e. the communication relationships between the devices. The metrics show which devices are accessible to each via wireless and how good this wireless connection is. Routes and metrics are generated automatically with each exploration and are selected accordingly in the drop-down list. Move the mouse pointer over the route / metric selected in the drop-down list to get a complete display of the route or metric name.

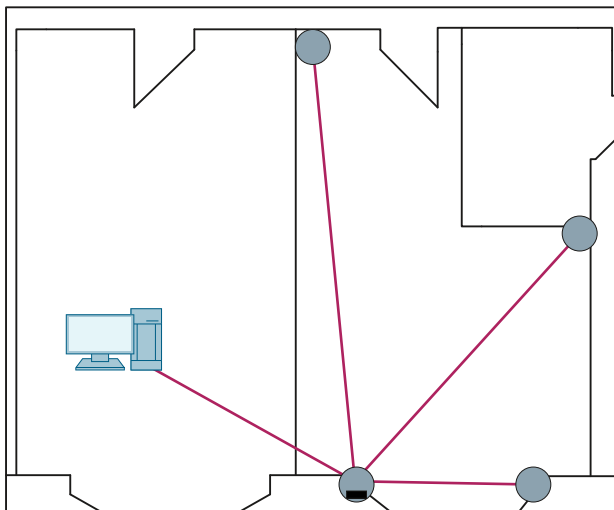
Displaying routes or metrics

The operation for routes and metrics is identical. Clicking "List" displays all existing route or metric data records as a drop-down list. Select the desired data record and then click "Select". The graphic representation of the data record then appears immediately.

You can use the "Create" button to manually generate route or metric data records. A view without any routes or metrics is displayed. Use the "Delete" button to permanently delete the selected route or metric record.

With the "Stop" button, you can cancel activation of route records or reading out of metric data. Note that this can lead to error messages.

The infrastructure devices are represented by gray dots, with gateways having a small black bar in their circle symbol.



Note**Navigation in the map**

You can use the scroll wheel of the mouse to navigate faster through the routing or metric map. Rolling the wheel shifts the display range vertically and holding down the shift key moves it horizontally. By using the scroll wheel and the control button at the same time, you can zoom in and out of the map.

Note**Determining the distance between two points on the map**

Follow these steps to determine the distance between two points on the map:

1. Left-click in the map on the starting point of the distance measurement.
2. Then hold the Shift key down and left-click on the destination point of the distance measurement.

The distance is shown in the message box at the bottom. In advanced mode, the angle is shown in addition.

6.4.5 Routes

Basically, it is recommended to use the routes automatically generated during the exploration. In individual cases, such as with variable wireless accessibility of the device infrastructure (e.g. an occasionally high bus or pallet stack covering devices), it is recommended to create additional routes. This ensures permanent accessibility of the Locating Manager server by the infrastructure devices. Routes with the highest priority are shown in red, routes with lower priority in blue.

Show Locating Manager server

You can show or hide the Locating Manager server by selecting the "Server" option and setting any position. Displaying the Locating Manager server is usually not helpful in large RTLS localization networks, since each individual connection to a gateway is displayed and the display quickly becomes confusing.

Selecting routes

If you enable the arrow symbol  to the right of the graphic, you can select routes or individual devices in the graphic. If you select a device or the Locating Manager server, the devices for which there is a direct route are displayed. The selection displays the route information of the selected route.

You can delete all routes of the selected device with the "Remove routes" button. With this option, make sure that new routes are created if required so that the device remains accessible. If a device does not have a route to the Locating Manager server, it no longer participates in the communication. It can still be used for locating if it was configured as last active for locating.

Creating routes

It is generally recommended to use the automatically generated routes and only create additional alternative routes. Proceed as follows to create a route:

1. Click  to create a route.
2. Select the target device by clicking the mouse while pressing the Shift key.
3. Now select the device or devices through which the target device is to communicate with the server, up to the server if it is shown.
If the Locating Manager server is hidden, double-click the last device before the server (i.e. a gateway) so that the route is extended to the Locating Manager server.
4. Click the  button if you want to create several routes in order to remain in creation mode after creating a route.

- Click the  button if the routes are to be created in both directions, i.e. from the device to the Locating Manager server and in the opposite direction.
The route for the respective opposite direction is created automatically when the first route direction is created.

Note

When you select the "Server warning" check box, a warning appears in the output window for log data to indicate that a created route does not extend to the server.

- Enable the crosshairs  and click on the desired position on the map. The x and y coordinates of the position are displayed in the output window for logging data.
It may be helpful to query positions (in each case to the reference point/coordinate origin) in the map.
- Click "Save" to save all the changes you have made. Click "Enable" to apply the changes and transfer them to the node.

You can find more options for creating routes in the "Routing" section.

Button	Description
Restore	This button allows you to restore deleted routes. This only works if the deletion has not yet been saved.
Delete	The button deletes the entire routing set.
Copy	Use the button to create a new routing set that corresponds to the one currently displayed. This enables you, for example, to add additional routes based on the automatically generated routing data record without changing the old data record. This allows you to reactivate the old routing set at any time.
Validate	You can test the routing set using the button. Any errors such as the missing server connection of individual devices are displayed in the output window for logging data. You can use the "Only routes" check box below to check devices for which there are routes.
Clear	Use the button to delete all routes in the routing set. The "Gate <-> Server" button is then the first action to be performed. This creates routes from Locating Manager server to all gateways.
List	The button triggers the output of all routes in the output window for log data. The devices are identified by their network address and the priority ("weight") of the respective route is also displayed.
From metrics	Click the button to create new routes from the last available metric set if a metric set has been loaded in the client.
Check device	Use the button to check whether the routes in the user interface match those saved on the devices. The result of the check is displayed in the output window for logging data.

Display routing information (list)

When you click the "List (all)" button, a table is created in a dialog box for the infrastructure device selected in the map. It lists all routes communicated through this device. The table created by clicking the "List (from/to)" button shows only the routes between the selected device and the Locating Manager server.

Read the routing table from left to right.

Columns	Description
Column 1	Describes the costs of a route For the routes automatically created with exploration, this information indicates how good and fast a route is (internal calculation from the number of hops to the server and the corresponding reception field strengths on the route). As a rule, the most effective routes are always used.
Column 2	Describes the message source The device whose data is to be transmitted to the Locating Manager server or the Locating Manager server in the reverse direction.
Column 3 to n-1	Intermediate routers that transfer messages from the message source in column 2 to the message sink (Locating Manager server or reception node) in column n.
Column n	Message sink

Priority of the route

Additionally created routes get the value "Hops + 1", so they are not used preferentially. You can change the sequence in which routes are used manually by entering a different number in the "Costs" column of the corresponding cell. The lower number always has priority. As soon as a cost field has been changed, the "Weights > Cost" button appears at the bottom of the table. Click this button to transfer the changes made to the nodes. From this point on, the newly defined priority will be used when selecting routes. Note that there are two entries for each route, one for the route from the device to the server and one for the route from the server to the device. The costs must be changed for both directions. Accordingly, the route that is primarily used is displayed in red.

Selection bar and menu in the table

The selection bar enables more settings to be made.

Setting	Description
Remove both ways	Select this check box to delete routes for both directions if the corresponding action is executed via "Right-click > Menu".
Highlight node	Select this check box to highlight the corresponding route and device by highlighting the table cell on the map.
On top	You can use this check box to keep the displayed table in the foreground. If this check box is cleared, the table is moved to the background of the user interface.

The shortcut menu in the table allows you to make further settings.

Setting	Description
Remove route	Click this button to delete the route selected in the table. Note here whether "Remove both ways" was enabled beforehand.
Remove route highlight	Click this button to show all routes and devices displayed on the map in the same way.

6.4.6 Metrics

The metrics are relevant when routes are optimized or created manually. You can also use the metric to run error diagnostics, especially to determine whether an infrastructure device is wirelessly accessible. A metric data record shows which devices can reach each other wirelessly and how well at the respective time they were set up. A metric set is created with each exploration. All potential wireless connections or metrics between the individual devices are displayed.

Click the  button to select objects in the map. You can decide whether you want to display the selection of infrastructure devices and/or metrics by selecting the corresponding  and/or  buttons.

As soon as you select an infrastructure device, a section for this device appears. The device type, the network address and the name are displayed.

Button	Description
Readout	Clicking the button measures the current reception field strength and stability of the wireless connections.
Remove metrics	The button allows you to delete the metrics of the selected device or metric.
Relocate in map	You can reposition a device by clicking the button. To do this, select the device. Click "Relocate in map" and then on a new position within the map.
Save	This button becomes active when you have selected a new position for a device. Click the button to save the position.
Restore	This button becomes active when you have selected a new position for a device. Click the button to undo the change.

After selecting a single metric, the associated metric data appears. The network and device names of the two devices involved are displayed as source (Src - Source) and destination (Dst - Destination). If you click the "Src <-> Dst" button, you can swap the direction of the data transfer. The  button allows you to edit or create metrics simultaneously in both directions.

RSSI is an indicator for the quality of the reception field strength, where 127 is the maximum. If you click the "Range" button, a distance measurement between the two devices is triggered and the result is displayed in the "Dist cm" text box.

"Stability" shows the stability of the radio connection between the devices on this router. The value range is from the value "0" to the value "100".

You can use the metrics to create alternative routes. To do this, read the metrics of the device to be connected via a route several times in succession at short intervals. This quickly analyzes which other device is the most stable for the route.

If the metric data record contains nodes that no longer exist (e.g. because the device has been replaced), an error message appears. If the affected node served as an intermediate point of a route, it is recommended that you manually create a new route to the destination device or perform a new exploration.

6.4.7 Services

Enabling/ disabling localization

You can enable or disable localization via "System > Services". If localization is disabled, no position data is calculated. Once the localization is enabled, the wireless network starts measuring distances and sends the results to the Locating Manager server, which converts them into position data.

WAMP router

The port of the WAMP router can be enabled for incoming connections from other PCs when the programming interface "ExportEpaperAPI" is to be reachable from other PCs. After changing this configuration, the Locating Manager server must be restarted for the change to become effective.

TCP port for gateway connections

The TCP port of the Locating Manager server for the gateway connections can be configured, for example, when the "TeeRevProxy" service is used. After changing this configuration, the Locating Manager server must be restarted for the change to become effective.

Data Export Service state

You can operate the "Data Export Service" with one and with multiple interfaces. An example is the use of different depot management systems at different locations within a transport company. The localization data from the Locating Manager is transferred to the depot management systems and the data from the different locations is compared via several modules of the "Data Export Service".

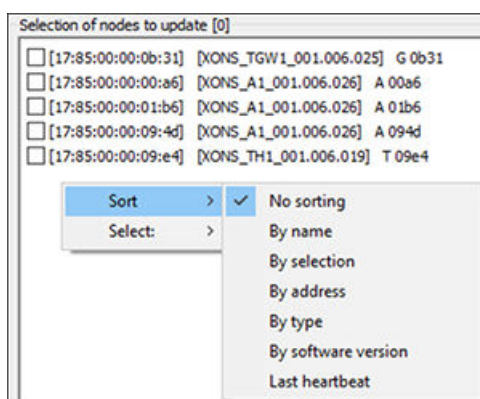
Click "Update" in the "DataExportService state" section to display a list of all configured modules of the "Data Export Service". Modules operating error-free are displayed green, modules that not operating error-free are displayed red and modules that are not connected are displayed orange. The list contains buttons for enabling and disabling the individual modules. You can find more information on error messages in the documentation for the "Log Viewer" client.

You can use the "Logging" check box to determine whether the data transfer of a module to a file should be logged. You can find additional information in the "Data Export Service" documentation. You can configure the modules during the module runtime.

6.4.8 Firmware update

This functionality is especially intended for updating a larger number of similar devices. You can update the firmware of individual devices by selecting the device in the tree topology and then going to the "System Information" subsection (section "System information and firmware update of individual devices (Page 24)"). To perform a firmware update, you need the corresponding firmware file in "*.cagl" format. By default, these files must be located in the directory "%ProgramData%\Siemens\SIMATIC RTLS Locating Manager\Firmware" on the Locating Manager server.

In the tree topology under "Firmware update", the "Selection of nodes to update" section contains a list of all devices of the RTLS locating network, including devices currently inactive or switched-off. The firmware update is performed with a time delay as soon as the device is active again or can be reached via the RTLS localization network. For smaller networks, you can select the desired nodes by selecting the check box of the device. To make the update function practical for larger networks, there is a shortcut menu. This provides self-explanatory sorting options for the node list.



The "Select" command in the shortcut menu offers options according to which the devices are automatically selected in the list. The option representing the best solution in the specific case depends on the respective project status. Note that the selections are added together. This means, for example, that if you first select "Transponder" and then "Anchor", all transponders and all anchors are selected.

In the "AddNode" section, all available firmware files are displayed in the shortcut menu. You can use the "R" button to update this list after you have copied a new file into the firmware directory, for example. Select the firmware to be transferred to the previously selected devices. Select the "List only matching" check box to improve the clarity of this list. After you click the "R" button, firmware files that do not match the selected devices are hidden.

If you select the "Show idle nodes" check box, devices whose firmware update has been completed will continue to be displayed in the list. If the check box remains cleared, these devices will be hidden after a certain period of time. The update process starts as soon as you have selected the "Add" button.

If you select the "Force-Flash Mode" check box, various security checks on the compatibility of the selected file are skipped. The device could become permanently unusable as a result. The use of this function is at your own risk and Siemens does not accept any liability for correct functioning of the device to be updated.

The check box is always cleared when the firmware update page is selected. If you enable this option, a warning is displayed.

The "State counter" section shows the number of devices updated via the selection made, as well as the status the devices have.

All devices to be updated are listed individually below. If you move the mouse pointer over the displayed data, a tooltip shows which device is in "Force-Flash Mode".

Address	Description	Current	Target	State	StateId	Counter
17:b4:10:00:78:bd	T 78bd	TAURI_TAW2_002.000.002	TAURI_TAW2_002.000.004	WaitStartCond	2	0
17:b4:10:00:78:c0	T 78c0	TAURI_TAW2_002.000.002	TAURI_TAW2_002.000.004	WaitStartCond	2	0
17:b4:10:00:78:c1	T 78c1	TAURI_TAW2_002.000.002	TAURI_TAW2_002.000.004	WaitStartCond	2	0
17:b4:10:00:78:c2	T 78c2	TAURI_TAW2_002.000.002	TAURI_TAW2_002.000.004	WaitStartCond	2	0

Name	Description
Address	Shows the network address of the device
Description	Shows the name of the device
Current	Shows the current firmware version
Target	Shows the firmware version after the update
State	Shows the current status of the update
StateId	Shows the corresponding status number
Counter	Shows the number of attempts of the update

If you select a firmware version that does not match, the update is not performed for the corresponding device. Instead, a warning is issued.

6.4.9 License management

In addition to checking the sufficient size of the license, license management enables assignment of licenses to individual devices. You can open the license management by clicking the button  in the menu bar once.

Select "System" in the tree topology to see how many transponders the license is valid for. License management provides a much more detailed view of the licensing scope.

No license

If no license is available, a message indicates that there is no license for mobile nodes.

Localization is disabled. Devices are no longer displayed in the "Localization Configuration" client. In this case, you can add or renew the license via the "Read license" button. As an alternative to reading in the license using the button, you can wait about one minute for the system to automatically read the license.

Allocating licensing capacity

Each sub-item of the license management in the tree topology enables the assignment of the license quota to the respective device types or functionalities. You can temporarily make the assignment to a device without a license by selecting the respective option and automatically release it by deleting the device.

"Allocate temporarily" means that free (unused) licenses are automatically, but only temporarily, assigned to devices without a license.

"Deallocate licenses when deleting" causes manually assigned licenses to be automatically released as soon as the node is deleted from the system.

Manual assignment

If one or more devices have no license and licenses are not assigned automatically, this is displayed in the overview of the respective device group. A warning appears in the view of the affected device itself.

Select the corresponding sub-item in License Management to assign a license from the quota to the device. Select the affected device in the "Transponder known to the system" section and click the arrow button to move it to the "Mobile nodes with license" section. As soon as you click the "Save" button, the device is available for localization. You can use the "Restore" button to undo the changes you have made.

Note

In general, it can be assumed that the license is sufficiently large for the number of devices. Therefore, it is recommended to use the automatic (temporary) assignment as described above. Manual, individual assignment of licenses only makes sense in exceptional cases.

6.4.10

Protocols

With "System > Protocols", you can configure whether and for how long the localization data of the transponders should be stored and whether old log entries should be deleted automatically.

Note

If there are more than one million entries in one of the logs, the older entries are deleted. With the "System" log, all entries of all levels of severity are added together. This deletion also takes place if deletion is disabled after the time of the log.

NOTICE

Note the following in relation to changes to the configuration!

Only make changes to this configuration in consultation with Siemens Aktiengesellschaft or if you are a very experienced user.

Setting	Description
"Restore" button	This button is enabled when you change this configuration. Click the button to undo the change.
"Save" button	Clicking this button saves the changed configuration.
Eventlog	The log saves all event management events.
Measurement	The log saves all sensor data (raw measured values) for localization and the heartbeat.

Setting	Description
System 0 to 9	These logs save system messages in different urgency levels.
TrackDist	The log stores the distance debug data of the transponders to the nodes.
TrackPos	The log stores the calculated position data of the transponders.
Save	You can configure whether or not the log is to be saved in this column. Double-clicking on the column name selects or clears all check boxes below.
Duration	You can configure the storage duration of the logs in hours in this column. If you move the mouse pointer over the "Duration" text box, the duration is displayed in days. You can also enter days or weeks in the text box. To do so, enter "2d" for "2 days" or "3w" for "3 weeks", for example. This input is automatically converted into hours.
Delete	You can configure whether or not the old logs are to be deleted in this column. Double-clicking on the column name selects or clears all the check boxes below.

6.4.11 Scan frequency band

The "Scan frequency band" function is only available in advanced mode.

During localization with the "PHASE" wireless technology, you can use blacklisting and whitelisting to select specific channels that are not yet under a heavy load in the used environment and can or cannot be used. However, the quality of localization is highest when all channels remain activated. You can make changes to the existing configuration according to your needs.

To configure blacklisting and whitelisting, follow these steps:

1. Enable all affected devices under "Devices" and click the "Read out" button.
2. A scan takes place for the duration configured under "Scan duration". The scan result is then displayed graphically.

Color of line or bar	Description
Blue	The blue line shows the currently measured signal.
Gray	The gray line shows the level between the blacklisted and whitelisted signal.
Orange	The orange bar represents the data communication channel.
Green	The green line shows your configuration that you made on the graph.

3. Click on the graph with the left and right mouse button to add a corresponding channel at the position of the mouse pointer to the blacklist or whitelist. The configured behavior is now shown as whitelist in the graph with the green line.
4. Click the "Apply" button when you have performed the configuration for the blacklisting and whitelisting.
5. Click "Set whitelist in network" to activate the updated configuration for the network.

Note**Recommendations for the configuration**

- The usage rate must be > 10% and should be as high as possible.
 - If possible, use contiguous frequency blocks for Black and White.
 - Do not enable the "Used communication channel" option when scanning, because data traffic always takes place in this case.
-

6.4.12 System backup

The "System backup" function is only available in advanced mode.

You can create a system backup on this page. The data of the Locating Manager is stored as .zip file. This .zip file contains the configuration files, log files in the default paths and executable files. A backup of the database tables is created in addition if the database is installed on the same PC as the Locating Manager. It may not be possible to copy files being used at the time. This includes logs that are being written at this moment or some of the runtime data from the "%ProgramData%\Siemens\SIMATIC RTLS Locating Manager\" directory. If the database is not on the same PC as the Locating Manager, backup of the database is skipped.

Clicking the "Start Backup" button creates the data backup of the database in the "%ProgramData%\Siemens\SIMATIC RTLS Locating Manager\Backup\" directory. It allows the "Database configuration" section to change the database name if there are different databases at different locations within a system, for example. The progress of the system backup is shown in the log window. If you want to use a backup, contact your Siemens representative and/or Customer Support.

The following files or folders are not secured in the system backup because they are in use:

- Keycloak-DB %ProgramData%\Siemens\SIMATIC_RTLS_LM\Config\IAM\keycloakdb.*
- Keycloak-Logs %ProgramData%\Siemens\SIMATIC_RTLS_LM\Logs\IAM\RTLS_LM_IAM_Service.err.log
- Keycloak-Logs %ProgramData%\Siemens\SIMATIC_RTLS_LM\Logs\IAM\RTLS_LM_IAM_Service.out.log
- Apache Logs %ProgramData%\Siemens\SIMATIC_RTLS_LM\Logs\ReverseProxy*
- Prometheus-DB %ProgramData%\Siemens\SIMATIC_RTLS_LM\OperationalData\Prometheus*
- EPaperManager %ProgramData%\Siemens\SIMATIC_RTLS_LM\Logs\lePaper Manager*

6.4.13 Service monitoring

The "Service monitoring" function is only available in advanced mode.

Service monitoring can monitor the listed services of the Locating Manager and start them in specific error situations. Monitoring takes place via the database. If the database cannot be reached then this function cannot be used.

With service monitoring, you can configure which services should be ended or started. Restarting is performed by an automatically determined master of the involved service monitoring services. The available system parameters are described in section "System parameter (Page 40)".

If you use the "HeartbeatMonitor" service in your configuration, starting of this service monitoring must be disabled.

Note

Only make changes to this configuration in consultation with Siemens Aktiengesellschaft or if you are a very experienced user.

Behavior of the service monitoring

The monitored services report that they are in operation regularly via heartbeats in the database. If this last state message of a service is older than the configured timeout, this service is considered "stuck" and is then automatically restarted.

After a service is started and as soon as the configured time in the "ServiceMonitor.MonitoringStartDelay" system parameter ends:

- The service checks whether it can communicate with the configured database and may end independently.
- A service start event is created.
- The service reports its heartbeat cyclically.

After the additional delay time of the system parameter "ServiceMonitor.TimeoutDetectionStartDelay" has elapsed, the service monitoring master begins monitoring the timeouts of other services. If the master detects a timeout:

- A log message is created. The first message for the corresponding timeout is sent with the urgency "Emergency". All repeat messages have the "Verbose" urgency.
- With the initial message, an event is created in which it is configured whether the corresponding service can be started or not.

6.4.14 System parameter

The "System parameter" function is only available in advanced mode.

The mode of operation of the Locating Manager can be configured or changed by configuring system parameters. Configuration takes place via the menu item "System > System parameters". All system parameters are listed in a table with their name, the current value and the default value. A change to the respective value can be configured in the corresponding cell of the current value. Click "Save" to activate the configuration of the parameters that you have made. You can activate multiple previously changed parameters at the same time. The changes are saved in the database. The parameters whose current

values differ from their respective default value are marked in bold in the respective cell of the current value.

If you move the mouse pointer over the respective parameter row in the table, additional information about the parameter is displayed as tooltip. You can sort the table in alphabetical order by clicking on the top column of the parameter name. Clicking on the column of the parameter name again undoes the sorting. You can reset unsaved changes to parameters with the "Restore" button.

For an optimized overview, you can use the text filter via the table. This text filter performs a sub-string search within the parameter name. When you select a row in the table, you can copy the contents to the clipboard using the shortcut [CTRL]+[C]. You can then configure the current value outside of the "Network Configuration" client and paste it again from the clipboard using the shortcut [CTRL]+[V].

The following system parameters are available:

Context	Parameter	Description
Sensor data logging	LoggingServer.SDSFileWriter.enable	Enables saving of SDS (sensor data structure) data in files. This can be used for later simulation or evaluation. Possible values: 0: not active 1: active Default value: 0 Data type: Integer
	LoggingServer.SDSFileWriter.path	Absolute or relative file path used to save SDS data. The file path must end with the "\" character; otherwise, the string after the last "\" is used as prefix to the file name. The placeholder "%programdata%" is replaced with the environment variable "%programData%" plus "\\Siemens\\SIMATIC RTLS Locating Manager". Default value: %programdata%\\Data\\sdsData\\ Data type: String
	LoggingServer.SDSFileWriter.maxfilesize	Maximum size of the file. A new file is generated when this value is reached. Default value: 200 MB Data type: Integer
	LoggingServer.SDSFileWriter.maxfileage	Maximum age of the file. A new file is generated when this value is reached. Default value: 86 400 s = 24 hours Data type: Integer
	LoggingServer.SDSFilePurger.enable	Enables deletion of SDS data according to age and size. In this case, the system parameters with the name part "SDSFilePurger" are included. Possible values: 0: not active 1: active Default value: 1 Data type: Integer
	LoggingServer.SDSFilePurger.minfileage	Storage time for SDS files. As soon as this time is exceeded, the file is deleted. Default value: 86 400 s = 24 hours Special value: 0 = Deactivated Data type: Integer
	LoggingServer.SDSFilePurger.maxfilesize	Maximum size of the folder. As soon as the limit is exceeded by the total of all files in the folder, the oldest file is deleted automatically. Default value: 200 MB Special value: 0 = Deactivated Data type: Integer

Context	Parameter	Description
Database	Database.dwMaxDurationWarningMS	Maximum duration of a database operation. If an operation exceeds this duration, a log entry and a log event are created. Default value: 3000 ms (milliseconds) Special value: 0 = Deactivated Data type: Integer
Firmware update	FirmwareManagement.bMaxNumberOfCurrentlyFlashedNodes	Maximum number of devices (transponders or gateways) for which the firmware update can be performed at the same time. This is the load control in the firmware update. Firmware updates that exceed this maximum number of devices are performed as soon as fewer firmware updates are active. Default value: 5 Special value: 0 = Firmware update deactivated Data type: Integer
	FirmwareManagement.sParamAfterWriteFileName	When the firmware update for a device is complete, parameters can be written automatically to the device. The file is in csv format and must be in the "%ProgramData%\Siemens\SIMATIC RTLS Locating Manager\Firmware" directory and have the following format with respect to columns: [Address;Variable;Value] If the file does not exist, no parameters are written automatically. Default value: "" Data type: String

Context	Parameter	Description
Service monitoring	ServiceMonitor.MonitoringStartDelay	Monitors the background services of the Locating Manager that use a database connection. All services involved automatically negotiate a master which causes the respective other service to restart if no heartbeat messages are received. Initial delays of monitoring after the Windows service starts. Default value: 20 000 ms Data type: Integer
	ServiceMonitor.TimeoutDetectionStartDelay	Additional delay time from which the master monitors the timeouts of other services. Default value: 60 000 ms Data type: Integer
	ServiceMonitor.ProcessRestartDelay	Maximum duration available to a restarting service for reporting. Default value: 60 000 ms Data type: Integer
	ServiceMonitor.ManagerLifeSignTimeout	If a heartbeat message of a service is older than the configured seconds, this service is restarted. Default value: 60 s Special value: 0 = No master is determined Data type: Integer
	ServiceMonitor.ManagerLifeSignCycle	Cycle time in which the heartbeat message of the service is written. Within this time, the master service is also determined. Default value: 20 000 ms Data type: Integer
	ServiceMonitor.boServiceRestartEnabled	Enabling the service restart. If this parameter is active, the respective service is restarted in the event of a heartbeat timeout. If the parameter is disabled, logging only takes place once and further monitoring of the respective service is ended. Possible values: 0: not active 1: active Default value: 1 Data type: Integer
	ServiceMonitor.stopServiceOnError	Activation of independent termination. When this parameter is enabled, a service terminates automatically as soon as it detects critical and untreated errors. Possible values: 0: not active 1: active Default value: 1 Data type: Integer
	ServiceMonitor.disableServiceHostname-CheckAtRuntime	Deactivation of host name check of the host on which the respective service is currently running. This disa-

Context	Parameter	Description
		bles the basic protection function that only one Locating Manager instance can be active on a database instance. If the "HeartbeatMonitor" service is used with a "Fail-Over" when the same database is used at the same time, you need to set this parameter to the value "1". Then set the cells in the database column "service-host" in the "ServiceMonitorManager" table to the value "0". Possible values: • 0: Monitoring enabled • 1: Monitoring disabled Default value: 0 Data type: Integer

Context	Parameter	Description
Raw data logging	ProtocolFile.boEnable	Enabling logging of all incoming and outgoing messages to devices. Possible values: • 0: not active • 1: active Default value: 0 Data type: Integer
	ProtocolFile.sFilename	Part of the file name of the log file automatically generated by logging. The resulting file name is: ([sFilePath]/TIMESTAMP_[sFileName]) Default value: Protocol.csv Data type: String
	ProtocolFile.sFilePath	Absolute or relative file path for saving device messages. The file path must end with the "\" character; otherwise, the string after the last "\" is used as prefix to the file name. The placeholder "%programdata%" is replaced with the environment variable "%programData%" plus "\\Siemens\\SIMATIC RTLS Locating Manager". Default value: %programdata%\Data\rawData\ Data type: String
	ProtocolFile.dwMaxFileSize	Threshold value for the size of a log file. If this size is exceeded, a new log file with the respective time stamp is created. Default value: 100 MB Special value: 0 = Deactivated Data type: Integer
	ProtocolFile.dwMaxFileAge	Maximum age of the file. A new file is generated when this value is reached. Default value: 7200 s = 2 hours Special value: 0 = Deactivated Data type: Integer
	ProtocolFile.dwMinFreeDiskSpace	If the value drops below this, logging is disabled for at least 10 seconds. Log entries that occur are not saved. After the 10 seconds have elapsed, the available hard disk size is checked. If the free memory space is larger than this value, logging starts again automatically with a new file (see "sFilename"). Default value: 500 MB Special value: 0 = Deactivated Data type: Integer

Context	Parameter	Description
Write positions to file	TrackposToFileWriter.Enable	Enabling writing of transponder positions to log files on the file system. This is independent logging in addition to the database. These files can be displayed with the "TrackViewer" client. The format/column definition of the csv file is as follows: [INSTIME;MODULETIME;NODEKEY;LOCAREAID;LOCAREATYPE;RETTYTYPE;CONDITION;CONDCHANGE;XPOS;YPOS;ZPOS;DISTANCE;DEBUGINFO] Possible values: • 0: not active • 1: active Default value: 0 Data type: Integer
	TrackposToFileWriter.FilePath	Absolute or relative file path for saving TrackPos data. The file path must end with the "\" character; otherwise, the string after the last "\" is used as prefix to the file name. The placeholder "%programdata%" is replaced with the environment variable "%programData%" plus "Siemens\SIMATIC RTLS Locating Manager". Default value: %programdata%\Data\trackposData\ Data type: String
	TrackposToFileWriter.MaxFileSize	Threshold value for the size of a log file. If this size is exceeded, a new log file with the respective time stamp is created. Default value: 100 MB Special value "0": Disabled Data type: Integer
	TrackposToFileWriter.MaxFileAge	Maximum age of the file. A new file is generated when this value is reached. Default value: 7200 s = 2 hours Special value "0": Disabled Data type: Integer
	TrackposToFileWriter.MinFreeDiskSpace	If the value drops below this, logging is disabled for at least 10 seconds. Log entries that occur are not saved. After the 10 seconds have elapsed, the available hard disk size is checked. If the free memory space is larger than this value, logging starts again automatically with a new file (see "sFilename"). Default value: 500 MB Special value "0": Disabled Data type: Integer

Context	Parameter	Description
GLOBAL	DEBUG_DATLET_DEBUG_MSG	Enabling of additional text messages in the output window for logging data of the client applications which is received during communication of the Locating Manager with gateways and transponders. This function is only released for Siemens Support. Possible values: • 0: Disabled • 1: Unknown • 2: All • 3: Only heartbeat Default value: 0 Data type: Integer
	RefPointGPS	Client applications and the data export service expand their internal structure by this reference point. Default value: "" Data type: String

Context	Parameter	Description
Device time monitoring	LocServer.MessageShortPastMS	If device messages are received whose module time stamp is older than the configured time period of the calculated or managed current module time in the Locating Manager server, these messages are discarded with an error entry. Default value: 10 000 ms Data type: Integer
	LocServer.MessageShortPastAcceptMS	If device messages are received whose module time stamp is within this configured time period of the calculated or managed current module time in the Locating Manager server, these messages are accepted and used for localization calculation. If the messages are older and younger than "LocServer.MessageShortPastMS" at the same time, they are discarded without an error message. Possible values: • 0: not active • 1: active Default value: 400 ms Data type: Integer
	NodeTimeManager.ContinuousTimeSync	The Locating Manager calculates the module time of transponders and gateways based on the messages received from these devices (e.g. heartbeats). Synchronization of the module times between the Locating Manager server and the module times contained in the messages only takes place once by default. The module time on the server side is required primarily to make the module time missing in TDOA messages (blinks) available for localization calculation. In the event of long periods without synchronization, a significant offset between the device module time and server module time can occur (clock drift). This can result in unwanted reinitialization of the localization calculation. When this parameter is enabled, synchronization takes place regularly with the receipt of these messages with module times.

Context	Parameter	Description
TDOA	TDOA.TWR.Enabled	The Locating Manager can measure the distance between two gateways via TWR. In this way, the actual runtime of the time synchronization messages can be determined. This message runtime can be used to improve time synchronization. This parameter is used to enable or disable the basic TWR measurement function which is used in different scenarios in the Locating Manager. If you change this system parameter, you must restart the Locating Manager server afterwards. Possible values: 0: not active 1: active Default value: 1 Data type: Integer
	TDOA.HyperbelGenerator.MaxTDOAsPerBlink	Limit to the number of generated TDOA hyperbolas per transponder and TDOA blink. If this limit is reached or exceeded, no more hyperbolas are formed for the transponder until the next TDOA blink. Default value: 153 Special value: 0 = Not active, no limit Data type: Integer
Device parameter assignment	parameterisation.Enabled	Enables reading and writing of parameter changes from and to the physical devices (transponders and gateways). If the system parameter is disabled, read/write operations are saved in the database and not performed. Possible values: 0: not active 1: active Default value: 1 Data type: Integer
	parameterisation.boChecksumCheckActive	Enables the consistency check between the system parameters saved on the devices and the parameter values saved in the database using checksums. If devices support this and differences are detected, the current parameter values are requested automatically by the devices. Default value: 1 Data type: Integer

Context	Parameter	Description
Device/network communication	Comm.RoutingTable.MismatchLogIntervall-Sec	Minimum time difference between two consecutive log messages of the form "Incoming Packet does not match to current Server-RoutingTable". This parameter has the effect that the warning is output less frequently in the event of invalid route data. Default value: 0 s (seconds) Data type: Integer
	Comm.MsgQueue.ResendDetection.time	Time during which incoming data packets are compared to one another and binary equal data packets are discarded. If the value is "0", no comparison is performed (e.g. for simulations). The maximum value for this parameter is 65535 ms. Data packets greater than 1024 bytes are not entered in the buffer. These data packets are therefore not detected as duplicates. The maximum memory that is allocated in total by this buffer is 8 MB (65536 entries with typical packet length of 128 bytes) Default value: 30 ms (milliseconds) Special value: 0 = Not active, no comparison of data packets is performed Data type: Integer
	Nodes.LifeSign.boAckLifeSigns	Enables sending of confirmation messages for the receipt of heartbeat messages from transponders and gateways. When a passive Locating Manager is operated, you need to disable this parameter. Possible values: • 0: not active • 1: active Default value: 1 Data type: Integer

Context	Parameter	Description
Virtual Heartbeat Generator	VirtualHeartbeatGenerator.interval	Interval in ms (the low limit at which virtual heartbeats are generated for infrastructure; for transponders, each received TWR/blink results in a virtual heartbeat) Default value: 10 000 ms (milliseconds) Data type: Integer
	VirtualHeartbeatGenerator.timeout	When this value is exceeded, a VirtualHeartbeatTimeout message is created for transponders for which localization data is missing. If this value is changed, this value is only applied after expiry of the old timeout value. If this takes too long, Siemens recommends a restart of the Locating Manager server. Default value: 0 ms (milliseconds) Special value: 0 = Not active Data type: Integer
Health Monitoring	GWPositionIntegrity.distance.sampling.interval_min	The interval of Health Monitoring with which distance measurements between the gateways are performed. The "scrape interval" of "PrometheusExporter" must have a lower value than this system parameter value. The value "0" disables the processing of distance measurement values. Default value: 15 min (minutes) Special value: 0 = Not active Data type: Integer