SIEMENS

SIMATIC Ident

RFID systems SIMATIC RF1100

Operating Manual

07/2023
C79000-G8976-C698-01

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 AG. 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.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C698-01
Ⓟ 05/2023 Subject to change

Table of contents

Introduction

1

Purpose of this documentation

This documentation provides you with an overview of the installation and programming of the SIMATIC RF1140R and RF1170R readers. The operating instructions are intended for users and programmers involved in configuration, commissioning and servicing of SIMATIC RF1100 readers.

Basic knowledge required

These operating instructions assume general knowledge of automation engineering and identification systems.

Scope of validity of this documentation

These operating instructions are valid for the SIMATIC RF1140R and RF1170R readers as of product version "01" and delivery state as of 07/2023, as well as firmware version V1.0.

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

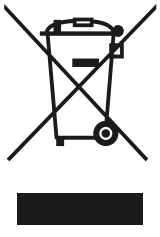
SIMATIC ®, SIMATIC RF ® and MOBY ®

Orientation in the documentation

Detailed information on creating and customizing configurations as well as their transfer to the SIMATIC RF1000 reader is available in the configuration manual "SIMATIC RF1000". You can find all relevant information for XML configuration and programming in the "XML Programming for SIMATIC Ident" manual.

You can find the current versions of the various manuals on the pages of the Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/14970/man).

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.

Adhere to the various country-specific regulations.

Security recommendations

2

To prevent unauthorized access, observe the following security recommendations when working with the reader and WBM (Web Based Management).

General

- Check regularly that the device complies with these recommendations and/or other internal security policies.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Keep the software up to date. Always use the latest firmware/software version of the device. Check regularly for security updates of the products and use them. After the release of a new version, previous versions are no longer supported and are not maintained.
  Information regarding product news and new software versions is available at the following address:
  Link (https://support.industry.siemens.com/cs/ww/en/ps/24224)
- Do not connect the device directly to the Internet. Operate the device within a protected network area. Use a firewall to connect the internal, protected network to external networks and configure it with restrictive rules.
- For data transmission via a non-secure network, use additional security components that provide an encrypted VPN tunnel (IPsec, OpenVPN).
- Terminate connections correctly (e.g. logout in WBM).
- Use the device only for system access control (and not for physical access control).

Physical access

- Restrict physical access to the device to qualified and authorized personnel.

Security functions

- Only enable protocols and functions that you actually need to use the device. Note that, in the factory setting, all protocols/functions can be used and all transponders and card types listed below are recognized. However, while the device has established a connection via a protocol, all other protocols are disabled.
- The XML/Modbus protocols are sent unencrypted. Take suitable measures to ensure that the XML/Modbus communication is tap-proof.
- For optimal security, use SNMPv3 authentication and encryption mechanisms. SNMPv1 is classified as non-secure and should only be used when absolutely necessary.
- Use the latest Web browser version compatible with the product to ensure you are using the most secure encryption methods available.

- Limit access to the device using an external device through a firewall or rules in an access control list (ACL). The firewall and access list can only be configured via an external device.
- The device has protection against brute force attacks to protect the system against trying out different passwords. Restrict the maximum possible number of permitted failed login attempts.
- The device has an automatic disconnect function ("Session Timeout"). Enter the interval after which the connection to the device will be terminated automatically.
- Configuration files can be downloaded from the device. Make sure that the configuration files are adequately protected. You can, for example, digitally sign and encrypt the files, store them at a safe location or transfer configuration files only via secure communication channels.
- The device provides options for backing up and restoring the configuration. For security reasons, neither the IP address of the network interface nor data of the local user administration are backed up. We recommend that you use the network management system "SINEC NMS" to manage this data.

Authentication

Note

Accessibility risk - Risk of data loss

Do not lose the passwords for the device. Access to the device can only be restored by resetting the device to factory settings, which completely removes all configuration data.

- Always use the user management and create new user profiles.
- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for using devices and assigning passwords.
- Define password policies.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. "Password1", "123456789", "abcdefgh") or recurring characters (e.g. "abcabc"). This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Change passwords and keys regularly to improve security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.

Certificates and keys

- There is a preset SSL/TLS certificate for access to the WBM. Replace this certificate with a user-created, high-quality certificate with key.
  Use a certificate signed by a reliable external or internal certification authority.
- Use a certification authority including key revocation and management to sign the certificates.
- Use certificates in the format "PKCS #12".
- Use certificates with a key length of 4096 bits.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.
- If protocols support both certificates and keys, you should favor certificates.
- The following encryption algorithms are supported:

Protocol	Supported encryption algorithms	Supported key and size
Web browser	SHA1 SHA256 with RSA SHA384 with RSA SHA512 with RSA	RSA 2048 bit RSA 4096 bit

- You can find information on the file formats supported by the various certificate types in section "The "Certificates" menu item (Page 58)".
- You can find information on the encryption methods supported by the device in section "Encryption methods (ciphers) (Page 91)".
- Make sure that the data stored on the transponders/cards is encrypted and that decryption/encryption of the data takes place on the connected devices.

Firmware/software

The firmware itself is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device.

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

Decommissioning

Decommission the device properly to prevent unauthorized persons from accessing confidential data in the device memory.
Reset the device to factory settings for this purpose.

2.1 Protocols

Secure/non-secure protocols

- Use only secure protocols, if possible. Avoid or disable non-secure protocols and services. If you need non-secure protocols and services, ensure that the device is operated in a protected network area.
  The following protocols provide secure alternatives:
  - HTTP → HTTPS
    HTTPS is activated at the factory. HTTP is classed as non-secure, but can be activated again at a later time if necessary.
  - SNMPv1 → SNMPv3
    SNMPv1 is enabled in the factory setting in order to facilitate operation of the device in a PROFINET environment. Check whether it is necessary to use SNMPv1. SNMPv1 is classified as non-secure. Make use of the possibility to prevent write access. The product offers corresponding setting options.
    If SNMPv1 is enabled, change the community names. If no unrestricted access is necessary, restrict access over SNMP.
- Only activate services/protocols that you require to use the system, including the built-in interfaces/ports. Unused ports could be used to access the network downstream from the device.
- Restrict the services and protocols available to the outside to a minimum.
- DCP is classified as non-secure. Check whether it is necessary to use DCP. If DCP is required, enable the "Read Only" mode for the DCP function after commissioning.

List of available protocols

All available protocols and their ports that are used with SIMATIC RF1100 readers are listed below.

Table 2-1 List of available protocols

Service/ Protocol	Protocol/ Port number	Preset port status	Port status configurable	Port number configurable	Authentication	Encryption [1)]
DHCP	UDP/68	Open	✓	--	--	--
HTTP	TCP/80	Closed	✓	--	--	--
HTTPS	TCP/443	Open	✓	--	✓	✓
NTP	UDP/123	Closed	✓	--	--	--
SNMP	UDP/161	Closed	✓	--	✓ (when configured)	✓ (when configured)

Service/ Protocol	Protocol/ Port number	Preset port status	Port status configurable	Port number configurable	Authentication	Encryption [1]
Modbus/TCP	TCP/502	Open	✓	✓	--	--
XML	TCP/10001	Open	✓	✓	--	--
Syslog	UDP/ 49152-65535	Closed	✓ [2]	--	--	--

[1] You can find more information on the encryption methods used in the appendix.

[2] Only outgoing, when configured.

Explanation of the table:

- Authentication
  Specifies whether authentication of the communication partner takes place.
- Encryption
  Specifies whether the transfer is encrypted.

2.2 Security information

Siemens provides products and solutions with industrial security 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 security concept. Siemens' products and solutions constitute 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 additional information on industrial security measures that may be implemented, please visit
https://www.siemens.com/industrialsecurity.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
https://www.siemens.com/cert.

2.3 Cell protection concept

The following graphic shows an example of a cell protection concept for the RF1100 readers.

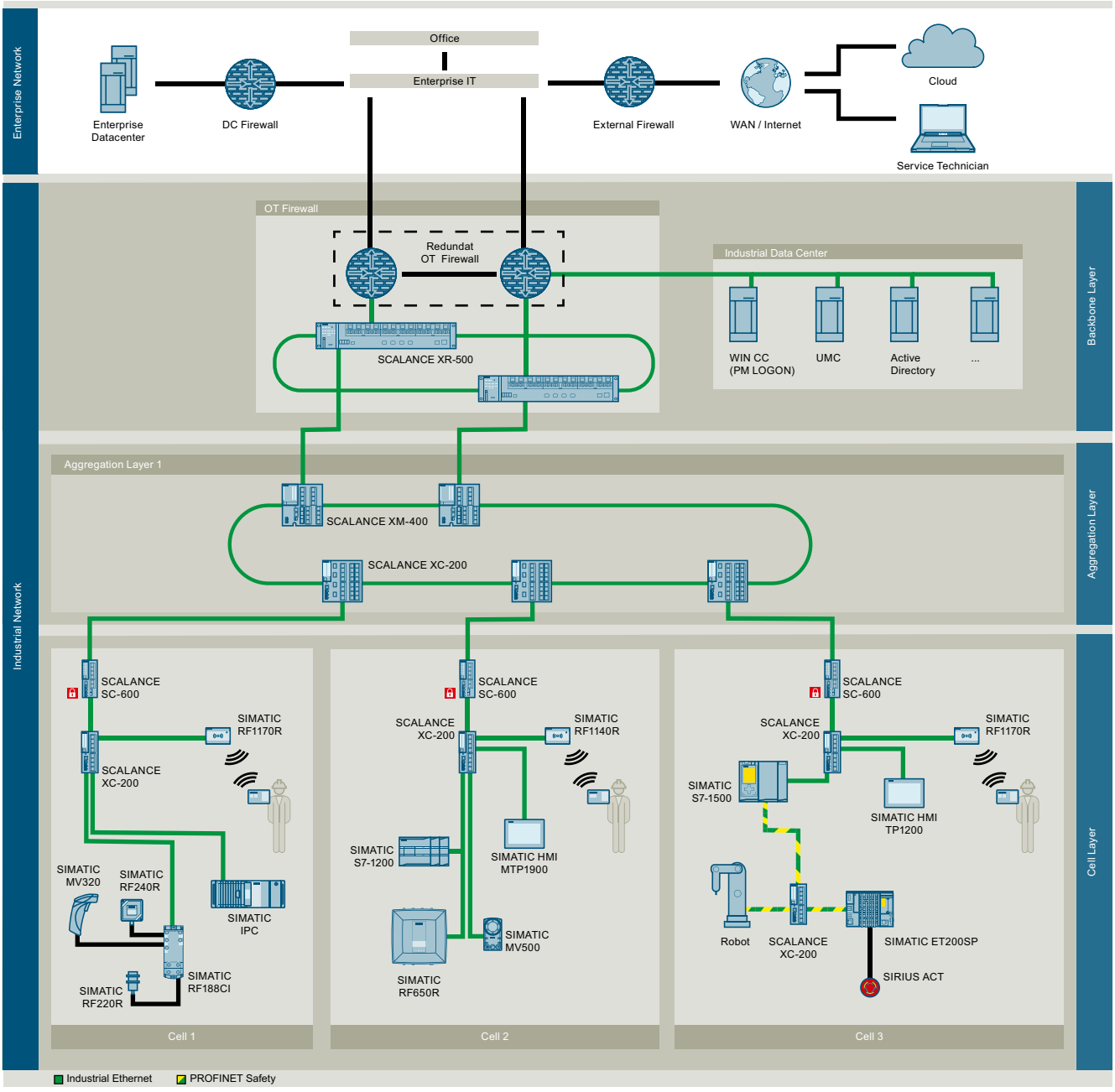


Figure 2-1 Schematic display of a cell protection concept for the RF1100 readers

Description

3

3.1 Properties of the reader

Area of application

Companies have been using RFID-based identification card systems for many years. With the increasing need for security and growing requirements for documentation, solutions are demanded with which access to machines and plants can be controlled on a user-specific basis. You can implement these requirements in access-secured areas by using the SIMATIC RF1140R and RF1170R readers and an employee ID card so that machines and plants must be released with an employee ID before they can be operated. With an appropriate configuration, the data on the transponders/cards can be encrypted and read only by those devices that have the appropriate key. You can adapt the readers to your security requirements as needed. This allows a finely graded access concept to be implemented or user-specific information and instructions to be stored – all with one card.

For security reasons, you should only operate the readers within a protected area. Make sure that the PoE interface is not openly accessible after installation.

Figure 3-1 Product photos of the SIMATIC RF1100 reader

The SIMATIC RF1100 readers are designed for connection to a computer or a Modbus client. Connection is via Ethernet.

Reader-specific differences

In contrast to the RF1170R, the RF1140R reader can read and edit 125 kHz transponders in addition.

Features

The following table provides an overview of the characteristics of the RF1100R readers.

Table 3-1 Features of the communication modules

Features	RF1140R	RF1170R
Operating frequency	125 kHz, 13.56 MHz	13.56 MHz
Transmit power (max.)	125 kHz: < 50 mW, 13.56 MHz: 250 mW	200 mW
Ethernet interface	PoE Transmission speed: 100 Mbps	
Degree of protection	IP67	
Configuration/ diagnostic options	WBM (Web browser)	
Application protocols	XML, Modbus	

Integration

The following graphics show examples of some of the integration options of the readers.

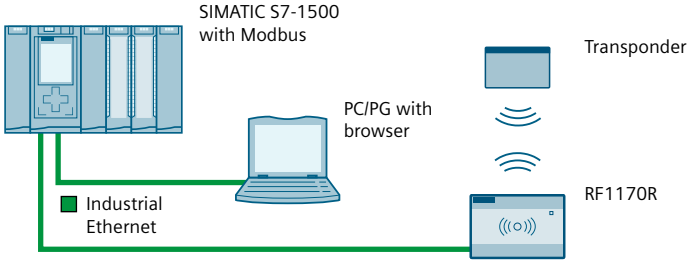


Figure 3-2 Readers in an automation environment with S7 controller

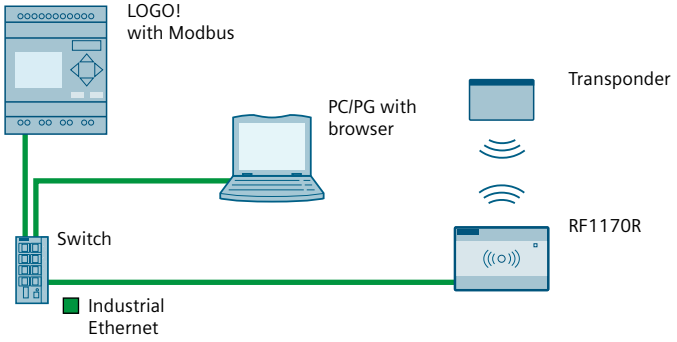


Figure 3-3 Readers in an automation environment with LOGO! controller

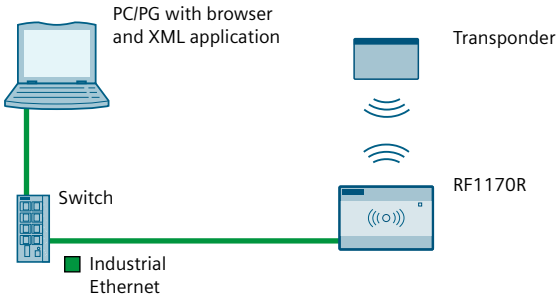


Figure 3-4 Readers in an IT environment

3.2 Supported transponders and protocols

The following table provides an overview of the transponders and protocols supported by the readers.

Table 3-2 Supported transponders

	SIMATIC RF1140R	SIMATIC RF1170R
MDS D100, D124, D126, D324, E600, E611	✓	✓
MDS D200	✓	✓
MDS D400, D424, D426, D524, D526	✓	--

✓: Reading the serial number as well as reading and writing the user memory area

Table 3-3 Supported protocols and card types

	SIMATIC RF1140R	SIMATIC RF1170R
ISO 14443 A/B general	Serial number	Serial number
ISO 15693 general	✓	✓
LEGIC prime	--	✓ 2)
LEGIC advant (ISO 14443 A) 1)	Serial number	✓ 2)
LEGIC advant (ISO 15693) 1)	Serial number	✓ 2)
MIFARE Classic, EV1 1) (1k, 4k, Mini)	✓	✓
MIFARE DESFire, EV1/EV2 1) (2k, 4k, 8k)	✓	✓
MIFARE Plus, EV1 1) (S, X, L1, L2, L3)	✓	Serial number
MIFARE Ultralight / C / EV1	✓	✓
HID iClass, Inside PicoPass	Serial number	Serial number
NXP NTAG21x	Serial number	Serial number
FeliCa	Serial number	Serial number
EM4100/EM4102, Casi-Rusco	Serial number	--

	SIMATIC RF1140R	SIMATIC RF1170R
EM4450/EM4550, EKS	✓ [3]	--
HITAG 1, HITAG S	✓	--
HITAG 2	Serial number	--
Keri [4]	Serial number	--
SecuraKey	Serial number	--
AWID	Serial number	--
ioProxy	Serial number	--

✓: Reading the serial number as well as reading and writing the user memory area

1) Transponder card must be formatted.

2) An identification card is required to access encrypted user memory areas (see section "Commissioning").

3) Only for read access. Write access to the user memory area is not possible.

4) The license must be transferred to the reader with a license card (HID).

In addition to the specified protocols and card types, a variety of transponder cards are generally supported by the readers. If you cannot find the card type that you use in the table, you can ask Siemens Customer Support about the functionality.

Note that serial numbers (UIDs) of transponders that begin with the byte "0x08" are always newly generated by the transponder. This makes an assignment of serial numbers and transponders impossible. For transponders with a combo-chip (e.g. LEGIC CTC4096), the serial number of the LEGIC Prime chip is always read and not that of the ISO chip 14443/15693. For transponders with two integrated chips (125 kHz / 13.56 MHz), you must ensure which chip is addressed via the reader configuration.

The reader can be addressed and controlled by functions, for example to change the status of the reader or to communicate with a transponder. With the aid of the functions, you can for example control the three-color reader LED. The functions and their calls are described in this manual.

3.3 User-specific procedure

As described above, the readers are designed for different environments and requirements. If you operate the communications modules in an XML or Modbus environment, they are configured and programmed from the perspective of an XML and Modbus user.

If you want to adapt the readers to your requirements, we recommend the following user-specific procedure:

Procedure as XML user

1. Connect the hardware
   You can find information on this in the section "Connecting (Page 25)".
2. Assign the IP address / device name
   You can find information on this in the section "Assigning the IP address / device name with SINEC PNI (Page 29)".

3. Configure reader
   You can find information on this in the section "Configuration via XML (Page 30)" or "Configuring with the WBM (Page 33)".
4. Program reader commands
   You can find information on this in the section "Programming via XML (Page 63)".

Procedure as Modbus user

1. Connect the hardware
   You can find information on this in the section "Connecting (Page 25)".
2. Assign the IP address / device name
   You can find information on this in the section "Assigning the IP address / device name with SINEC PNI (Page 29)".
3. Configure reader
   You can find information on this in the section "Configuring via Modbus (Page 31)" or "Configuring with the WBM (Page 33)".
4. Program reader commands
   You can find information on this in the section "Programming via Modbus (Page 63)".

Orientation in the document

Later in the document, these symbols will help your orientation and will show you whether the section is of interest to you or not. Only the sections with user-specific content, in other words, content that is interface-specific, contain these symbols. Sections without these symbols are general and relevant for all areas of application.

Installation

4

You can install the RF1100 readers in a wall or control cabinet (in-wall/control cabinet mounting). When installing the readers inside or on a wall, you may also want to install a card holder. However, if the readers are to be operated in a cleanroom, you must "seal" the readers using a silicone joint and the cleanroom cover.

Mounting options:

- without accessories
- with card holder "6GT2890-0CA00" or
- with cleanroom cover cabinet installation "6GT2890-0CD00" (relevant for operation in a cleanroom)

NOTICE

Interference due to metallic environments

Electrically conductive materials can interfere with the HF field of the reader to the point that it is completely shielded. Observe the following guidelines to avoid interference:

- Ensure that there is no metal between reader and transponder.
  Coins and other metal parts that are significantly smaller than the transponder antenna, usually do not cause any interference.
- Ensure that there is no metal close to the rear of the transponder.
  Observe a minimum clearance that is at least half the size of the transponder diameter or the card width.
- When installed in metal, note that the read/write range and the detection reliability can be restricted. if the antenna of the transponder is larger than the antenna of the reader (57 x 35 mm).

Note that a short test with a number of example cards is not sufficient to test how large the metal-free area around the reader must be. Even in the event of a positive result, communication failures can occur during operation. This is due to deviations in card antennas, card IC parameters and RFID interface parameters, which can influence both energy transfer and the quality of the data transfer.

NOTICE

Using the reader in a cleanroom

Note that when operating the reader in a cleanroom, the cleanroom cover must be installed and the reader or the table/wall housing must be sealed with a silicone joint.

Recommendations for the silicone joint:

- Silicone recommended for cleanroom: Silirub Cleanroom
- Radius of the joint tool for wiping: 5 mm

NOTICE
Repair and maintenance Do not try to repair the reader in case of a problem. Repair and maintenance work must only be carried out by qualified personnel. Contact Siemens Support in case of repair or maintenance problems. For more information, refer to the section "Service & Support".

Required tools and accessories

The following tool is required:

- Torx screwdriver (T10)
- Slotted screwdriver
- If necessary, caulking gun, silicone cartridge and joint tool (relevant for operation in a cleanroom)

The following accessories are required depending on the mounting options:

- If necessary, card holder "6GT2890-0CA00" or
- If necessary, cleanroom cover cabinet installation "6GT2890-0CD00" (relevant for operation in a cleanroom)

Mounting the reader

NOTICE
Installation conditions • The thickness of the wall on which the reader is mounted must be 2-7 mm. • The installation opening must have the following dimensions: 76.5 (± 0.3) × 48.5 (± 0.3) mm • Protect the reader from mechanical deformation.

Follow the steps below to install the RF1100 reader in a wall or in a control cabinet:

1. Optional: Depending on your requirements, install the card holder or the cleanroom cover.
   - When using a card holder:
     Place the card holder on the side of the reader housing and press it over the reader front so that the card holder locks in place.
     Note that you cannot use the card holder in combination with the cleanroom cover.
   - When using the reader in a cleanroom:
     Place the cleanroom cover on the side of the reader housing and press it over the reader front so that the cover locks in place.
     Note that you cannot use the cleanroom cover in combination with the card holder.
2. Push the reader through the mounting opening intended for this purpose (76.5 [± 0.3] × 48.5 [± 0.3] mm) ①.
3. Slide the screw holder over the back of the reader ②.

4. Attach the reader by tightening the 4x stud screws ③.
   Ensure that the reader housing is flush with the substrate and that the circumferential gap is < 0.5 mm.

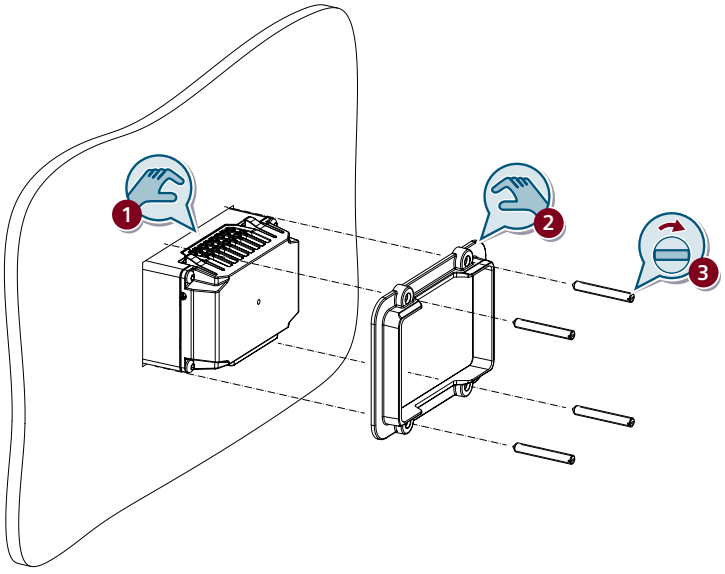


Figure 4-1 Mounting the SIMATIC RF1100 reader

5. Optionally when using the reader in a cleanroom:
   Apply a silicone joint on the front between the reader edge or the cleanroom cover and the surface or the wall.

Connecting

5

⚠ WARNING

Explosion hazard

Note that installation must not be performed and the connecting cable must not be inserted or removed within the hazardous area.

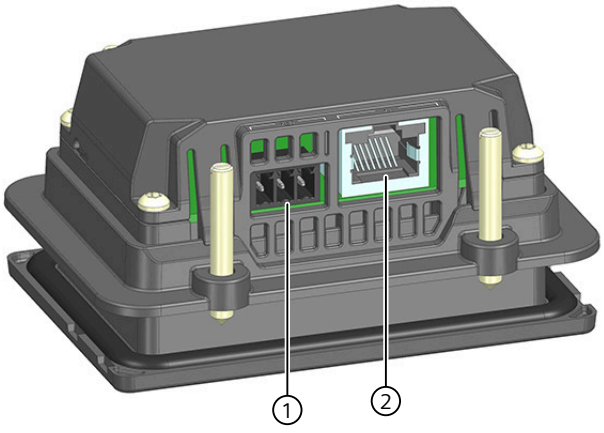
NOTICE

Permissible power supply

The equipment is designed for operation with a Safety Extra-Low Voltage (SELV) system via a Limited Power Source (LPS) and must only be operated with 24 V DC. The power supply must therefore meet at least one of the following conditions:

- Only safety extra low voltage (SELV) with limited power source (LPS) complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 or IEC 62368-1 / EN 62368-1 / VDE 62368-1 can be connected to the power supply terminals.
- The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

The RF1100 readers have the following interfaces:



① Power supply interface (24 V DC)
② Ethernet interface;
Power over Ethernet (PoE)

Figure 5-1 Interfaces of the SIMATIC RF1100 reader

Power supply options

The reader is supplied with voltage via the power supply interface (24 V DC) or the Ethernet interface (PoE), depending on your system configuration. Note that simultaneous/redundant power supply via 24 V DC and PoE is not permitted.

The reader is earthed via one of the pins of the power supply.

5.1 Electrical design of the reader

Electrical isolation

In the electrical design of the reader, electrical isolation is provided between:

- Shield (FE) and all other circuit components
- Communications interfaces (Ethernet) of the RF1100 and all other circuit components

The figure below shows the potential relationships:

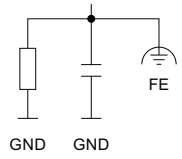
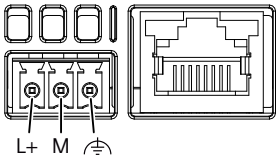


Figure 5-2 Potential ratios of the reader

5.2 24 V DC power supply

The connection of an external power supply (24 V DC) and the connection with functional earth (FE) take place via a connector with 3 pins. The following wiring diagram helps you to allocate the pins of the connector.



L+	+24 V DC (max. 1 A)
M	Reference ground to +24 V DC
FE	Earth connection (FE)

Figure 5-3 Wiring diagram: Socket for the external 24 V DC power supply (view from above)

Connect the respective cables to the corresponding connector pins and then insert the connector into the power supply interface of the reader. If the power supply of the reader is via the Ethernet interface, only the pin ③ can be assigned to functional earth (FE).

NOTICE
Redundant power supply not permissible
Note that simultaneous/redundant power supply via 24 V DC and PoE is not permitted.

Earth connection

You need to connect the SIMATIC RF1100 reader to functional earth (FE). The reader has a pin for earthing to which an earthing cable can be attached.

This connection to functional earth (FE) is also required to discharge any interference currents to earth and for EMI resistance.

Protection against external electrical influences

Below is a description of what you must pay attention to in terms of protection against electrical impacts and/or faults:

- In all plants or systems in which the reader is installed, you must ensure that the plant or the system for dissipating electromagnetic interference is connected to functional earth.
- For supply, signal and bus cables, you must ensure that the cable routing and installation are correct.
- For signal and bus lines, you must ensure that a wire/cable breakage or a cross-circuit does not lead to undefined states of the plant or system.

5.3 Power supply using Power over Ethernet (PoE)

"Power over Ethernet" (PoE) is a power supply technology for network components complying with IEEE 802.3af. The power is supplied over an Ethernet cable used to connect the individual network components (corresponding to IEEE 802.3af) with one another. This makes an additional power cable unnecessary.

SIMATIC RF1100 is a PD (Powered Device), Type 1, Class 2 (max. 6.49 W).

NOTICE
Redundant power supply not permissible
Note that simultaneous/redundant power supply via 24 V DC and PoE is not permitted.

Restriction of the power supply type

The IEEE standard 802.3af specifies two types of power supplies:

- Voltage via wire pairs that are not used for data transmission (redundant wires).
- Voltage via wire pairs that are used for data transmission (phantom power).

The following Siemens switches have PoE connections:

- SCALANCE X108 PoE
- SCALANCE XP208 PoE EEC
- SCALANCE XP216 PoE EEC
- SCALANCE X308-2M PoE
- SCALANCE XR324-4M PoE
- SCALANCE XR324-4M PoE TS
- SCALANCE XM-400 with Port Extender PE408 PoE and
  PoE power supply SCALANCE PS9230 PoE or SCALANCE PS924 PoE
- SCALANCE XR-500M with media module MM992-4PoE or MM992-4PoEC

Addressing and configuring

6

Synchronize device time

Note that the time of the device clock corresponds to UTC time and cannot be adjusted to time zones. It is recommended to synchronize the time with an NTP server to obtain unique time information. The time is reset with a device restart and must be synchronized.

6.1 Assign the IP address / device name

To achieve ideal communication between the PC and reader, you need to assign a unique IP address or device name to each individual reader. If you operate the reader as XML or Modbus user in an IT environment, the unique assignment is based on DHCP or the IP address and can be made using SINEC PNI.

After an IP address has been assigned to the reader, you can also change it later using the WBM.

Note

Support of option "12"

When the address is assigned via DHCP, the option "12" (hostname) is also supported. The hostname can be taken from the SNMP variable "sysName".

The variable can be written using SNMP tools.

6.2 Assigning the IP address / device name with SINEC PNI

Requirements

SINEC PNI is installed and the reader is connected and running. You can find the SINEC PNI on the pages of the "Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/26672/dl)".

Procedure

Follow the steps below to assign a new, unique IP address and a unique device name to the reader:

1. Start SINEC PNI.
2. In the "Settings" menu, select the "Network adapter" via which the reader is connected to the PC.

3. Make sure that the "Scan protocol > PROFINET devices" is selected.
   Note: Note that the function "Fetch additional information" can take some time when the network includes many devices.
4. Click on the "Save" button.
5. Switch to the "Device list" menu.
6. Click on the "Start network scan" button on the toolbar.
   Reaction: The network is scanned for connected devices and all recognized devices are displayed in the device list.
7. Select the desired reader in the device list.
8. Click on the "Configure device" button on the toolbar.
   Reaction: The "Device configuration" window opens.
9. Enter a new, unique IP address for the reader in the "IP address" text box.
   Note: You may have to disable the "DHCP" function beforehand.
10. Enter the subnet mask of your network in the "Subnet mask" input box.
11. Click the "Load all" button to transfer the settings to the reader.

Result: The reader is assigned the new IP address, subnet mask and a new device name.

Device flash test using SINEC PNI

Using the node flash test, you can identify the reader quickly and simply by having the LEDs of the device flash. This function is particularly helpful if multiple devices are connected to the network/PC.

Follow the steps below to identify the relevant reader using the flash test:

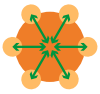
1. Select the desired module from the device list in the "Device list" menu.
2. Click on the "Flash LED" button on the toolbar.
   Reaction: The LED flashes on the selected reader.
3. Click the "Stop" button to stop the flashing.

6.3 Configuration via XML

This section is intended only for XML users.

Configuration of the reader is not necessary for pure XML work. You can continue directly with configuration via WBM and with programming via XML. You can find detailed information on this in the manual "XML programming for SIMATIC Ident (https://support.industry.siemens.com/cs/ww/en/view/109781631)".

6.4 Configuring via Modbus



This section is intended only for Modbus users.

Configuration of the reader is not necessary for pure Modbus work. You can continue directly with configuration via WBM and with programming via Modbus.

Configuring with the WBM

7

The readers are equipped with a Web server that provides Web Based Management (WBM) to the Web client for configuring the readers. The WBM can be called via the Web browser of a PC/ laptop.

The WBM server provides the Web client (PC/laptop) with the parameter data of the reader and accepts parameter changes from the Web client. Note that changed parameter values are not automatically transferred to the reader. You must always manually transfer changes in the configuration to the reader.

Hereafter, the term "WBM" is used to represent the WBM interface displayed in the Web browser.

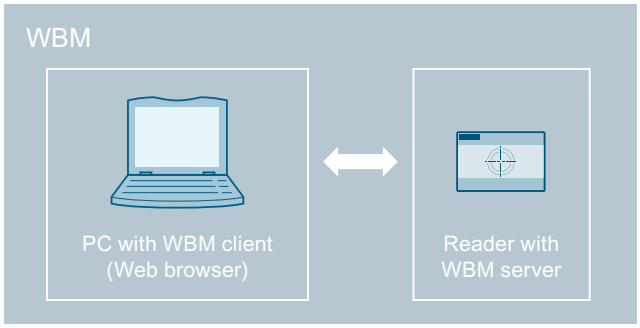


Figure 7-1 Design and function of the WBM

7.1 Starting WBM

Requirement

The reader is connected, turned on and ready for operation and the reader has been assigned an IP address.

To achieve a good workflow with the WBM, we recommend that you use a PC that meets the following minimum requirements:

- CPU: DualCore
- RAM: 2 GB

You can call WBM using the versions of the following Web browsers current at the time of publication of this manual: Microsoft Edge, Mozilla Firefox and Google Chrome. The user interface of the WBM is designed for a screen resolution of at least 1366 x 768 pixels.

Procedure

Proceed as follows to start the WBM:

1. Start your Web browser.
2. Enter the IP address of the reader preceded by "https://" in the address field of your browser.
3. Confirm your entry by pressing the <Enter> key.

Note

Updating HTTPS certificates

The first time you log on, the HTTPS certificate of the reader is shown as not secure. Note that the certificate stored in the reader is only intended to ensure that the initial connection establishment to the reader is encrypted. Confirm that the certificate is secure. Then transfer your own, secure certificate to the reader.

Result: The WBM of the reader opens.

Note

The connection to the reader cannot be established

If no connection can be established to the reader, check the following points:

- Make sure that all cables are correctly connected.
- Make sure that the reader has started up.
- Check the IP addresses of the PC and the reader, as well as the subnet mask. Both IP addresses must be located in the same subnet.
- Make sure that the connection is not blocked by a firewall.
- Check the connection between the PC and reader using a ping request.

Logging into the WBM for the first time

When logging into WBM for the first time, a popup window appears prompting you to log in with the default user "admin".

1. Select the required interface language from the drop-down list.
2. Enter the preset default user name "admin" in the "User" text box.
3. Enter the preset default password "admin" in the "Password" text box.

4. Click the "Log in" button.
   Reaction: The popup window is updated and you are prompted to change the default password for the "admin" user.
   Note: Alternatively, you can use the "Disable authentication" button to disable authentication.

NOTICE
Security recommendation: Authentication To ensure that no unauthorized persons can access the reader settings, we recommend that you enable the authentication and create new user profiles. You should also read the information under the "Passwords" heading of the "Security recommendations (Page 9)" section. The authentication can only be enabled/disabled by an administrator. For more information on logging on to WBM and creating/deleting user profiles, refer to the section "The "User management" menu item (Page 54)".

5. If needed, select the primary interface connection over which you are operating the reader from the "Operational environment" drop-down list.
6. Enter your new password for the "admin" user in the "New password" text box.
7. In the "Confirm password" text box, enter the newly selected password again.
8. Click the "Log in" button.

Result: You are logged in to the WBM with the "admin" profile and can now set reader parameters.

Operational environment

Depending on the selected operational environment, the interfaces, communication channels, and associated services that match the mode are enabled beforehand. This restores the parameter values for the mode to the factory default values.

This function increases the security of your device because all other interfaces, communication channels and the associated services are disabled.

Regular login to the WBM

Depending on whether the authentication is enabled or disabled, you may have to log on with your user name and the corresponding password. The WBM homepage opens after logging on, even if authentication is disabled.

Via the "Readme OSS" link, you can open the Readme OSS file with the copyright information and license conditions for the open source software contained in this firmware. Via the "Manual" link, you can open the manual for the reader or WBM.

7.2 The WBM

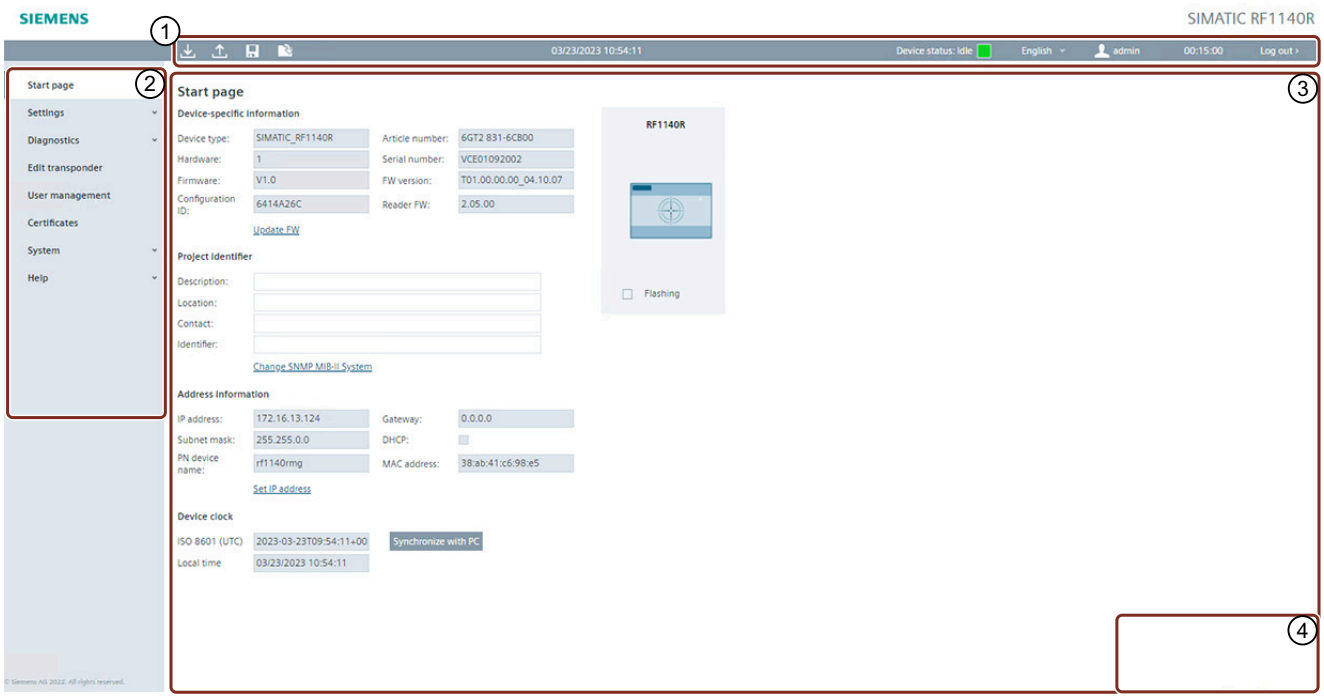
Using the WBM, you can configure the SIMATIC RF1140R/RF1170R readers.

After you have created new user profiles, you need to log on with one of these user profiles when you restart the WBM.

NOTICE
Access to the reader Remember that simultaneous access to a reader using two WBM clients (Web browsers) is possible but not recommended. If changes are made when two WBM clients are accessing a reader at the same time, this can lead to errors in the configuration or an undesired result.

Layout of the WBM

After successful connection establishment to the reader and logon (when authentication is enabled), the start window of the WBM appears:



The WBM start window is divided into the following areas:

① Toolbar / status bar (including logout area)
② Menu tree
③ Main window
④ Message area

Figure 7-2 Start window of the WBM

Toolbar and status bar ①

Toolbar

On the left above the main window, there are four buttons for transferring/loading/ storing the displayed configuration. You can also operate these buttons directly with key combinations.

Table 7-1 The toolbar of the WBM

Icon	Description
	Transfer configuration to reader With this button, you can transfer the configuration data set in the WBM to the reader. Key combination: Ctrl + L **Note** Be aware that transferring a configuration can disrupt running user applications.
	Load configuration from reader Using this button, you can load the configuration data currently set on the reader into the WBM. Key combination: Ctrl + G **Note** You cannot transfer any user profiles and passwords to other readers using the configuration file. After loading the configuration file into a new reader, you may need to enable authentication and create new user profiles and passwords.
	Save configuration as With this button, you can save the configuration data set in the WBM on the PC. Key combination: Ctrl + S
	Load configuration from PC Using this button, you can load the configuration data stored on the PC in the WBM. Remember that this data is only loaded in the WBM. To transfer the data to the reader, you also need to click the "Transfer configuration to reader" button. Key combination: Ctrl + O

Status bar

On the right above the main window there is the status bar with the following information:

- Date/time display of the reader
  Note that the time stamp is generated by the device clock (UTC time). This time is compared with the time format and time zone set on the PC and displayed in the corresponding format.
- Display of the device status
  The following device states are possible:

	Idle The reader is ready for operation.
	Running The reader is running and has established a connection.
	License mode The reader is ready for operation but only reads data from license cards.
	Error (idle) The reader is ready for operation and there is an error.
	Error (running) The reader is running, has established a connection and an error is pending.

- Drop-down list for selecting the user interface language
- Logged-in user (with active authentication)
- Display of the time until the automatic logout as well as a drop-down list for selecting the time interval
- Logout area (with active authentication)

Change notes in the user interface

Deviations between the settings in the user interface of the WBM and the configuration stored on the connected reader are shown with a symbol in the user interface. If a value is changed in the WBM interface, the relevant field is marked by a symbol. In addition, the tab, if applicable, as well as the menu item in which the changed value is located and the "Transfer configuration to reader" button are also marked by a symbol. A distinction is made between the following symbols:

- This symbol indicates that it is a simple change.
- This symbol indicates that a change was made by another application simultaneously to access to the reader via the WBM. To make sure that this change is not lost, you should load the configuration from the reader.
- This symbol indicates that it is a change that leads to a restart of the reader when it is transferred.

Menu tree ②

The menu tree is located in the left margin of the WBM. The currently selected menu item is highlighted in color.

The following table provides an overview of the menu items and the functions they provide.

Table 7-2 The menu structure of the WBM

Menu items		Functions
Homepage		• System overview • View device-specific information • Enter customer-specific plant designation
Settings		
	General	Enable/disable categories of log events
	Reader configuration	Configure reader
	Network settings	Make network settings
Diagnostics		
	Log	Overview of log entries
	Service logbook	Information for service cases
	Syslog logbook	Overview of Syslog messages
Edit transponder		Read out and write transponder data
User management		• Enable/disable authentication • Create and delete user profiles • Change passwords • Configure security settings
Certificates		Import HTTPS certificates
System		
	Device settings:	• Update firmware • Reset reader
Help		Documentation relevant for the reader
	Service and Support	Additional information on the reader
	Manual	Manual of the reader

If you are logged in to the WBM with the "User" role, some menu items can only be used with restrictions. You will find a list of the restrictions in the section "The "User management" menu item (Page 54)".

Main window ③

The main window shows the contents of the selected menu items. Here, you can configure the various menu-dependent parameters.

Message area ④

The message area displays all WBM-related error messages and warnings (e.g. transfer errors).

Operating the WBM via the keyboard

In addition to operating the WBM with the mouse, you can also control the interface objects/text boxes using the keyboard:

- TAB
  Jump to next interface object / text box
- SHIFT + TAB
  Jump to the previous interface object / text box

Apart from manual entry of values, you can also change values in the text boxes with the following buttons:

- Arrow up / down
  The value is increased or decreased by one increment.
- PgUp / PgDn
  The value is increased or decreased by ten increments.
- Home / End
  The value is set to the minimum or maximum value.

7.3 The menu items of the WBM

7.3.1 The "Start page" menu item

The "Start page" menu item is divided into the following areas.

- Device-specific information
- Project ID
- Address information
- Device clock
- Configuration display

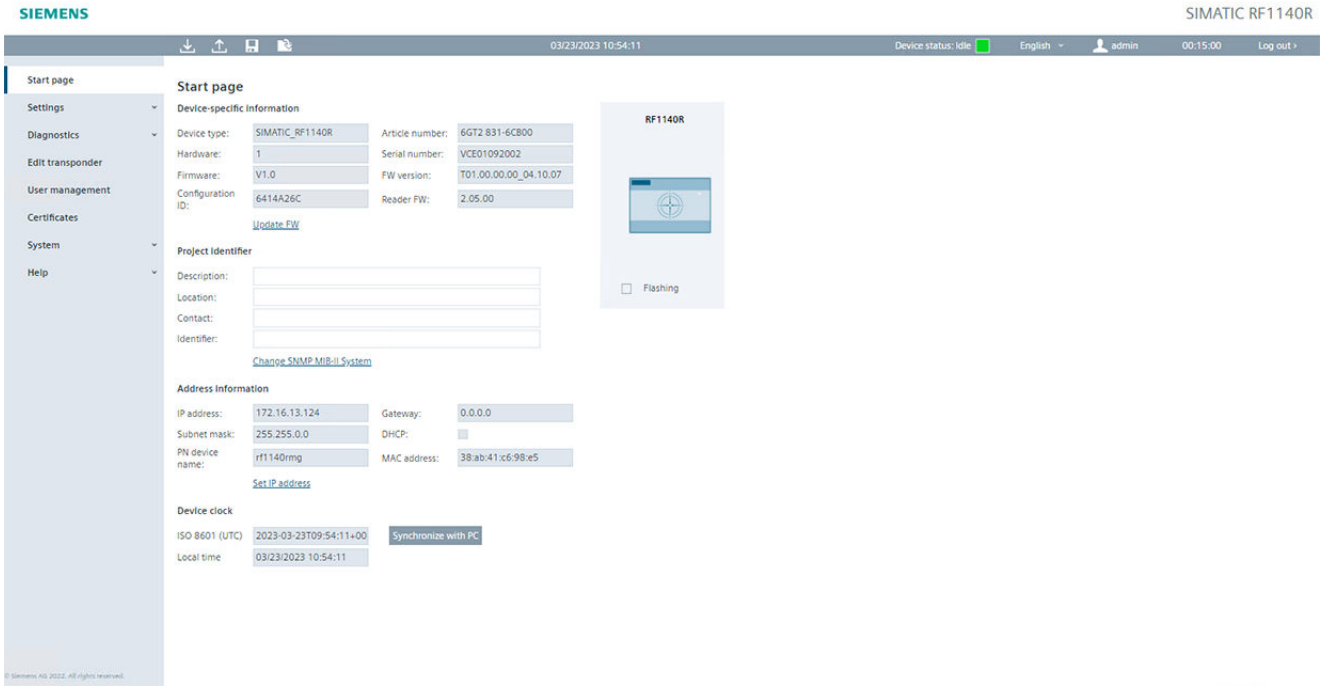


Figure 7-3 The "Homepage" menu item

Device-specific information

The first area contains device-specific information. The "Device type", "Article number", "Hardware" and "Serial number" boxes are specified in the factory. The content of the "Firmware" and "Firmware version" boxes depends on the firmware stored on the reader. Using the "Update firmware" link, you jump to the "System" menu item in which you can update firmware. The "Configuration ID" box contains a unique identifier for the configuration that was last activated on the reader or loaded onto the reader. Click the "Default configuration" button to reset the parameters shown in the user interface to the default values. When you restore the default configuration, address information (IP address, device name) is retained.

Project ID

The second area contains input boxes with which you can store your own device-specific information on the reader. Among other things, this is intended to make it easier to identify the individual readers. Via the link "SNMP MIB-II system", you jump to the "Communication" menu item, where you can view and change the MIB variables.

Address information

The third area contains all the important address information with which the PC can reach the reader. You can assign the IP address and PN device names to the reader using "SINEC PNI". Via the link "IP Address" you jump to the "System" menu item inn which you can also reassign the IP address.

Device clock

The device time according to ISO 8601 (UTC), as well as the calculated local time, is displayed in this area. With the "Synchronize with PC" button, you can synchronize the displayed local time with the time in your operating system.

Note

The device time always corresponds to UTC time (ISO 8601)

Note that the device time always corresponds to UTC time (ISO 8601) and cannot be adapted to time zones. Clicking the button transfers the local time stored in your operating system to the WBM. Because the time synchronized with the PC is lost when the power supply is terminated, we recommend synchronizing the time with an NTP server.

Configuration display

A diagram of the reader is shown to the right of the areas. The schematic diagram contains information on the connected reader type. With the "Flash" check box, you can have the LEDs of the reader flash. This enables you to quickly and easily identify the reader.

7.3.2 The "Settings - General" menu item

The "Settings - General" menu item is divided into the following areas:

- Log settings
- Service logbook settings

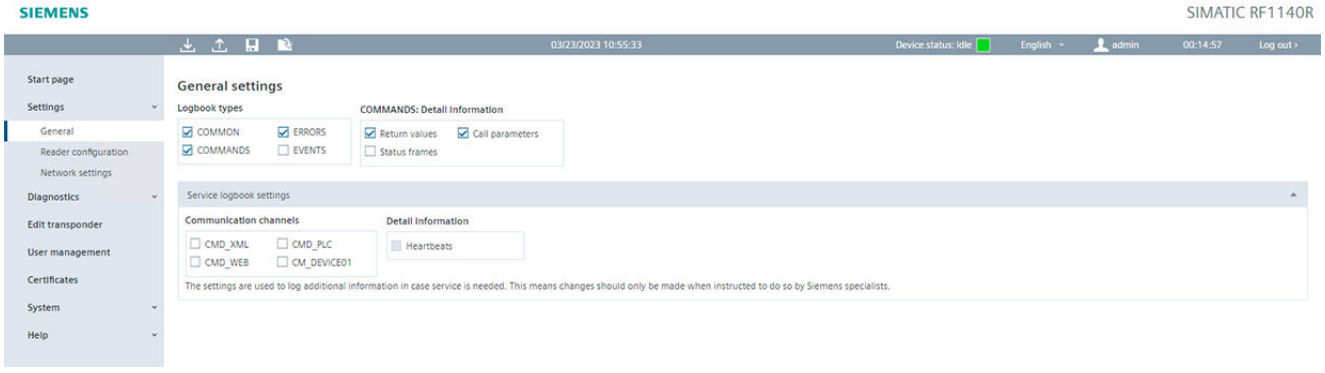


Figure 7-4 The "Settings - General" menu item

Log settings

In the "Log settings" area, you can use the check boxes to decide which events are entered in the log. The log is structured as a ring buffer. Bear in mind that with a high degree of detail

of the data, the ring buffer fills up more quickly, which can have a negative effect on the performance of the device.

Table 7-3 Description of the parameters of the log

Parameter	Description
Logbook types	
COMMON	Messages relating to general events: e.g. reader startup, login to the WBM, ...
ERRORS	Error and alarm messages of the reader
COMMANDS	Commands of the user application
EVENTS	Recording of all tag events
COMMANDS: Detailed information	
Return value	Return values for the commands of the user application and for the written or read transponder data.
Call parameters	Call parameters for the commands of the user application
Status telegrams	Recording of the status frames for Modbus communication. Can be switched off if the status frames are used as line monitoring. In this way, the logbook is kept free for user data.

Service logbook settings

In the "Service logbook settings" area, you can use the check boxes to decide which events are entered in the Service logbook. The Service logbook is structured as a ring buffer. Bear in mind that with a high degree of detail of the data, the ring buffer fills up more quickly, which can have a negative effect on the performance of the device.

Table 7-4 Description of service logbook parameters

Parameter	Description
Communication channels	
CMD_XML	Frames on the XML interface
CMD_PLC	Internal frames on the Modbus interface
CMD_WEB	Internal frames to the Web server
CM_DEVICE01	Frames on the internal interface
Detailed information	
Line monitoring	Recording of the line monitoring frames (CMD_XML and CMD_PLC) for service information. Can be switched off to keep the logbook free for payload data.

7.3.3 The "Settings - Reader configuration" menu item

In the "Settings - Reader configuration" menu item, you can create and edit tag fields as well as enable/disable and configure the Modbus and XML interface.

This page is divided into the following areas:

- Basic settings
- Tag fields

- Tag field properties
- Modbus settings
- XML settings
- Advanced
- License mode

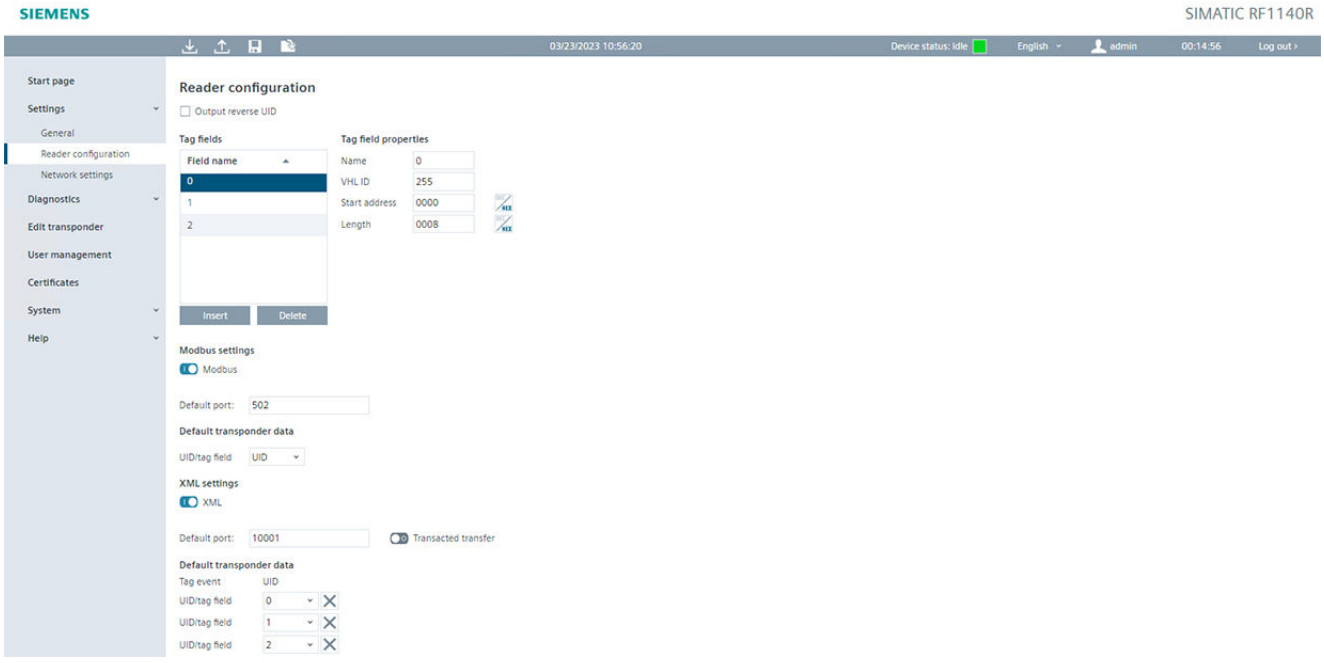


Figure 7-5 The "Settings - Reader configuration" menu item

Basic settings

Select the "Output reverse UID" check box if you want to reverse the byte order when the UID is output.

Tag fields

In this area, you can create and edit up to ten tag fields. Tag fields are user-defined memory areas on a transponder. Specific transponder data can be read with tag fields. To edit a tag field, select the required field in the list. The selected tag field is highlighted in color. Click the "Insert" button to create a new tag field. Click the "Delete" button to delete the selected tag field.

Tag field properties

In the "Tag field properties" area, you can adapt the parameters of the individual tag fields.

Table 7-5 Description of the parameters of the tag fields

Parameter	Description
Name	Input box for assigning a logical name/descriptive title to the tag field. Possible characters: 0 ... 9
VHL File ID	Input box for entering the number of the VHL file ID. With the ID, you can define which memory area should be accessed.
Start address	Input box for entering the start address within the memory area from which you want to read, change or write the data of the target transponder. You can use the button to change the input/output format (decimal or hexadecimal). Range of values: 0 ... 65535 bytes
Length	Input box for entering the length within the memory area and starting from the start address within which you want to read, change or write the data of the target transponder. You can use the button to change the input/output format (decimal or hexadecimal). Range of values: 1 ... 1024 bytes

Modbus settings

In the "Modbus settings" area, you can enable/disable the Modbus communication and change the port number of the interface. Via the "UID/tag field" drop-down list, you can determine which transponder data the reader should read out. The data selected here can be retrieved via the Modbus interface.

XML settings

In the "XML basic settings" area, you can enable/disable the XML communication via the XML interface of the reader and change the port number of the interface. In addition, you can define which events are sent to the user application via all XML channels.

Table 7-6 Description of the XML basic parameters

Parameter	Description
Transaction-secured transmission	If the check box is selected, each frame (XML report) received from the user application of the reader is confirmed with a response frame. If no response frame is received by the reader within 10 seconds, it sends the report to the application again. Reports that are not transmitted are buffered in the reader. With this function, you can make sure that no frames from the reader are lost even if the connection is unstable (e.g. WLAN connection aborts occasionally). This function also allows batch operation of the reader when there is only a connection to the user application at certain times. The reader collects the frames and these can, when necessary, be called up using a PC application.
Transponder data presettings	
Tag event	Specification of which tag field data a tag event should contain.
Tag field	
Read point properties	

Parameter	Description
Autoread	If the check box is selected, tag events are created automatically as soon as transponders enter the antenna field of the reader. Use of the XML command "triggerSource" is not necessary.
Tag events	If the check box is selected, a tag event frame (Observed) is generated each time a transponder is reliably detected. When a transponder leaves the antenna field, an additional tag event frame (LOST) is generated.
Presence events	If the check box is selected, information about presence states or changes is transferred as events.
Log events	If the check box is selected, all logbook entries are transferred as events.

Advanced

In this area, you can load a configuration created with the Config Editor into the reader. These configurations are required if the VHL File ID ≠ 255 (e.g. with encrypted transponders). You can find detailed information on the Config Editor and configurations in the configuration manual "SIMATIC RF1000/RF1100 (https://support.industry.siemens.com/cs/ww/en/ps/24223/man)".

Note that Autoread configurations created with the Config Editor are not supported by the readers.

License mode

You can enable/disable the license mode in this area. If the license mode is enabled, the device status of the reader changes. In this mode, you can transfer a license to the reader using a license card by holding the license card in front of the reader. Note that only data from license cards is read in this mode. The installed license is displayed in the output box. After the desired license has been transferred, the license mode is automatically disabled again and the reader returns to the original device status.

Note

Licenses cannot be transferred

Note that licenses can only be transferred once. A license cannot be transferred to multiple readers or from one reader to another.

7.3.4 The "Settings - Network interface" menu item

In the "Settings - Network Settings" menu item, you can enable/disable the network port and SNMP protocols and configure them.

This page is divided into the following areas:

- Network basic settings
- SNMP

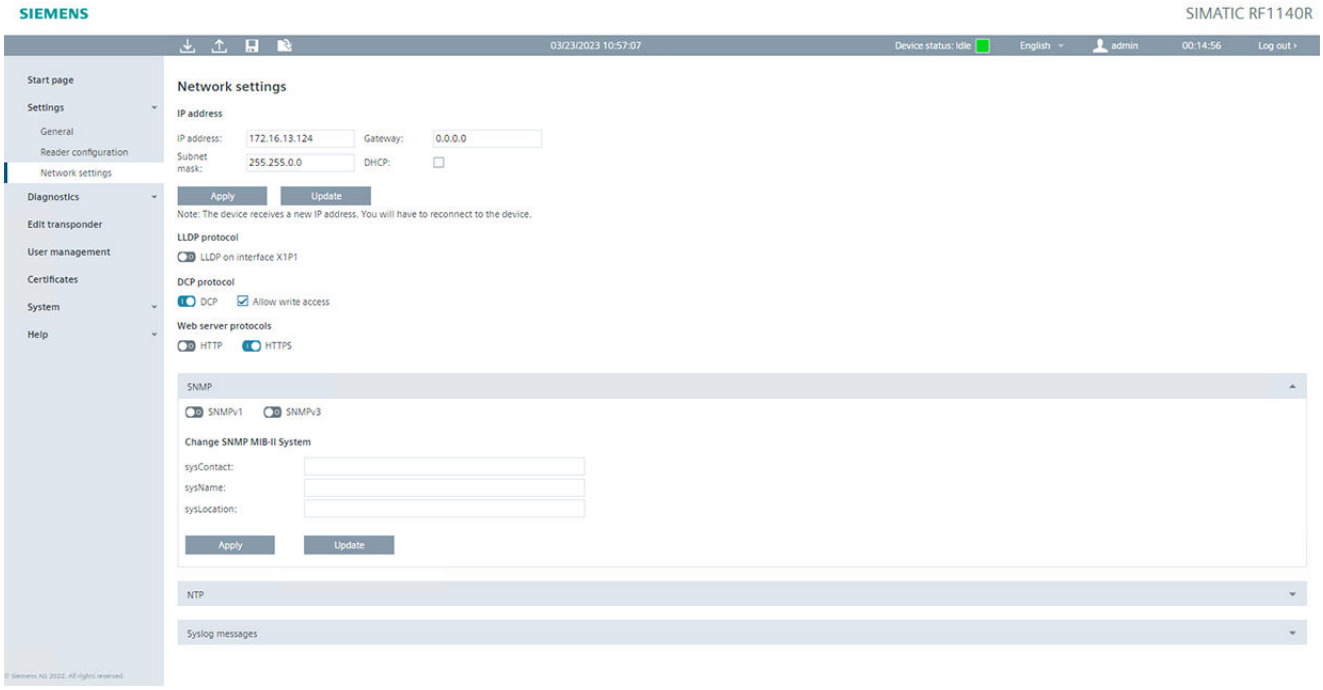


Figure 7-6 The "Settings -- Network settings" menu item

Network basic settings

In the "Network basic settings" area, you can enable/disable the network ports of the reader, allow/prohibit access via DCP protocols, and specify the Web server protocols via which communication with the WBM is allowed.

Table 7-7 Description of the network basic parameters

Parameter	Description
IP address	In this area, you can change the IP address, subnet mask and gateway of the reader. As an alternative, the configuration of the IP data can be obtained from a DHCP server. Using the "Apply" button, you can transfer the address data changed in the WBM to the reader. You can use the "Update" button to update the address data displayed in the WBM or reload it from the reader. **Note** When the address is assigned via DHCP, the option "12" (hostname) is also supported. The hostname can be taken from the SNMP variable "sysName". The variable can be written using SNMP tools.
LLDP protocol	In this area, you can enable/disable the LLDP communication protocol for the Ethernet interface. LLDP is a protocol for monitoring the neighborhood.
DCP protocol	In this area, you can enable/disable communication via DCP protocols. You can define here whether the access to the reader via the DCP protocols is write only or read and write. Depending on the decision made here, the factory settings may or may not be restored to the reader via SINEC PNI, for example.
Web server protocols	In this area, you can specify which web server protocols can be used to access the WBM of the reader. For security reasons, it is recommended that you do not enable the "HTTP" function, since this protocol does not encrypt the data.

Disable the "Allow write access" function if you want to ensure that no access to the reader takes place via DCP. This setting prevents the reader from being reset to factory settings via SINEC PNI, for example.

Note

Requirement for port statistics

You can read out port statistics via SNMP.

SNMP

In the "SNMP" area, you can enable/disable the network protocol. "SNMP" is a protocol for monitoring network components.

SNMP is deactivated at the factory. Check whether it is necessary to use SNMPv1. SNMPv1 is classified as non-secure. If possible, only use SNMPv3. If you do not use the protocol, we recommend that you disable the setting for security reasons.

Table 7-8 Description of the SNMP parameters

Parameter	Description
SNMPv1 settings	
Read community string	Input box for specifying the user name for read access to SNMP variables. This property is typically assigned the value "public".
Write community string	Input box for specifying the user name for write access to SNMP variables. This property is typically assigned the value "private". In this box, changes can only be made if write access was permitted. Write access is only possible for the SNMP variables "sysName", "sysLocation" and "sysContact" of the "system" group of MIB-II.
Allow write access	Check box to enable/disable write protection for SNMP variables.
SNMPv3 settings	
Users	List of the created SNMP users. Using the "Add user" button, you can create new user profiles and add them. You can delete selected user profiles using the "Delete" button.
User properties	Input box and drop-down list Enter the name of the newly created user profile in the input box and assign read or read/write permissions to the user.
Authentication	Drop-down list and input boxes Specify whether users need to authenticate themselves and, if so, with which protocol. If necessary, enter the authentication password of the newly created user profile in the input boxes.
Encryption	Drop-down list and input boxes Specify whether SNMP communication of the user needs to be encrypted and, if so, with which protocol. If necessary, enter the encryption password of the newly created user profile in the input boxes.
Save	You can use the button to save changes made to existing user profiles.
SNMP MIB-II system	

Parameter	Description
sysName	Fields for reading out ("Update") and changing ("Apply") the MIB-II system information. These are usually assigned via network management systems (e.g. SINEC PNI). Changes made here are displayed accordingly in the network management system and vice versa. This information is only required when using network management systems.
sysLocation	
sysContact	

7.3.5 The "Diagnostics - Log" menu item

The log of the reader is displayed in the "Diagnostics - Log" menu item.

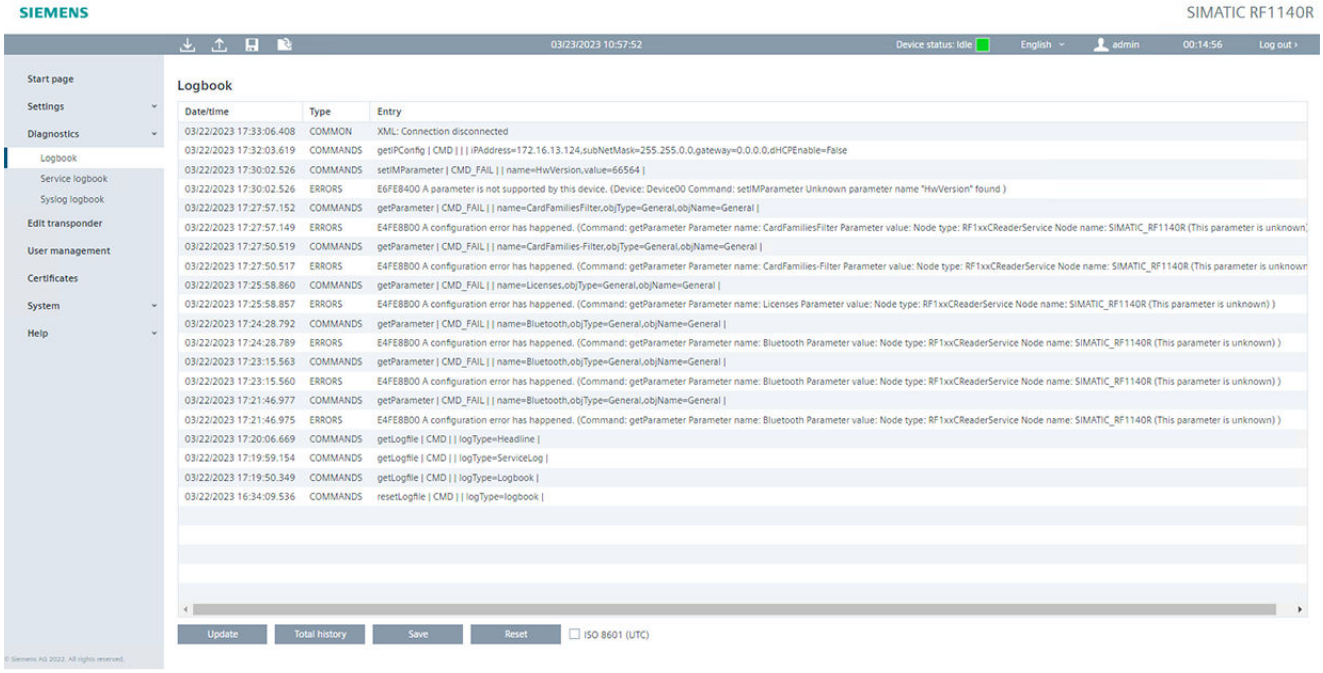


Figure 7-7 The "Diagnostics - Log" menu item

The menu item "Log" shows all message types that were selected in the menu item "Settings - General" in the "Log settings" area. This menu item documents the actions performed by the reader.

The entries contain the following properties:

Table 7-9 Displayed properties of the log messages

Property	Description
Date/time	Time stamp when the entry was made by the reader. Note that the time stamp is generated by the device clock (UTC time). This time is compared with the time format and time zone set on the PC and displayed in the corresponding format.
Type	Type of message Which message types are signaled depends on the check boxes enabled in the menu item "Settings - General" in the "Log settings" area.
Entry	Text of the message

You can use the buttons to control the entries:

- Update
  The log is read in again from the reader and the list updated. The log entries displayed include the most current data (200 KB).
- Total history
  The complete stored log of the reader is read in. The log entries displayed include all saved data (10 MB).
- Save as
  The log read by the reader is saved as a *.csv file on the PC.
  Note that the time stamp is generated by the device clock according to ISO 8601 (UTC time).
- Reset
  The log is deleted on the reader.

With the "ISO 8601 (UTC)" check box, you can convert the data display in the "Date/Time" column to UTC time, identical to the output in the exported logbook.

With a large number of log entries in the history, it may take several minutes before these are displayed.

7.3.6 The "Diagnostics - Service Log" menu item

The service log of the reader is displayed in the "Diagnostics - Service Log" menu item. The log records internal processes of the reader and is required for service support by SIEMENS specialists. Only make settings on this page if you are instructed to do so by SIEMENS personnel. The log entries are also evaluated by SIEMENS personnel.

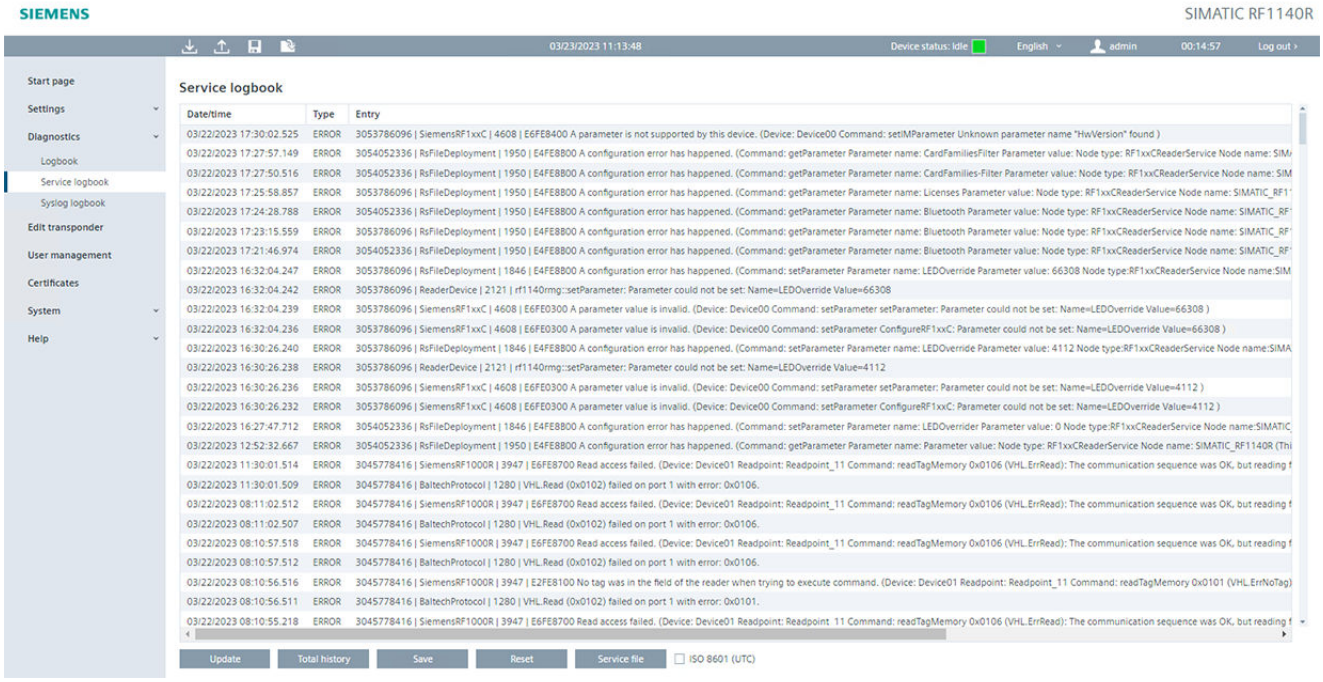


Figure 7-8 The "Diagnostics - Service Log" menu item

This page displays all the message types that have been defined in the "Settings - General > Service logbook settings" menu.

The entries contain the following properties:

Table 7-10 Displayed properties of the log messages

Property	Description
Date/time	Time stamp when the entry was made by the reader. Note that the time stamp is generated by the device clock (UTC time). This time is compared with the time format and time zone set on the PC and displayed accordingly.
Type	Type of message Which message types are signaled depends on the check boxes enabled in the menu item "Settings - General" in the "Log settings" area.
Entry	Text of the message

With the "Update", "Save as" and "Reset" buttons, you can control the entries:

- Update
  The log is read in again from the reader and the list updated. The log entries displayed include the most current data (200 KB).
- Save as
  The log read out by the reader is saved as a *.csv file.
- Reset
  The log is deleted on the reader.
- Service file
  All reader data relevant for diagnostics are stored as a *.slf file. The file only contains information relevant for Siemens service personnel and can only be evaluated by them.

With the "ISO 8601 (UTC)" check box, you can convert the data display in the "Date/Time" column to UTC time, identical to the output in the exported logbook.

With a large number of log entries in the history, it may take several minutes before these are displayed.

7.3.7 The "Diagnostics - Syslog logbook" menu item

The menu item "Diagnostics - Syslog logbook" displays the logbook of the Syslog messages when the Syslog function is enabled. This page can only be called by users with administrator rights.

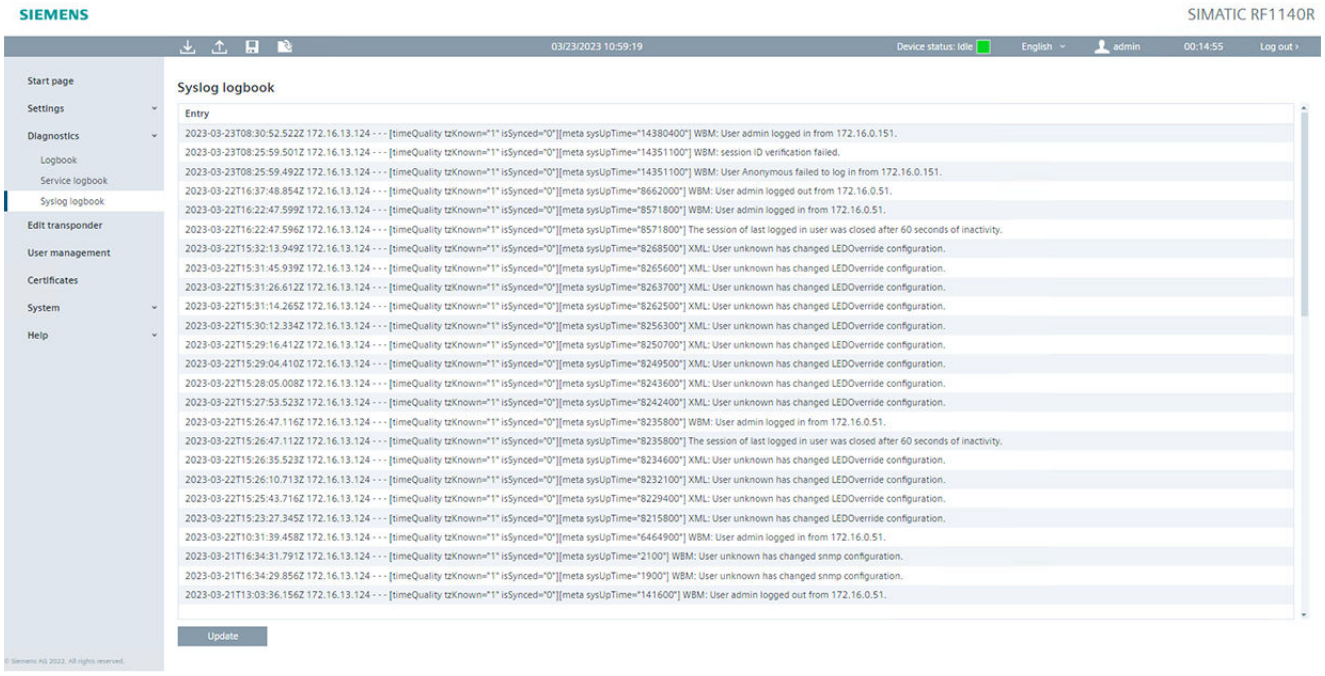


Figure 7-9 The "Diagnostics - Syslog logbook" menu item

All Syslog messages are displayed in the "Syslog logbook" menu item. This menu item documents all safety-related access operations to the reader and performed actions. You

can find detailed information on the Syslog messages, their structure and contents in the section "Syslog messages".

With the "Update" button, you can read in the entries from the reader again and update the list. The displayed log entries contain 128 KB of data.

7.3.8 The "Edit transponder" menu item

You can read out and write transponder data with the "Edit transponder" menu item.

This page is divided into the following areas:

- Read UID
- Read/write

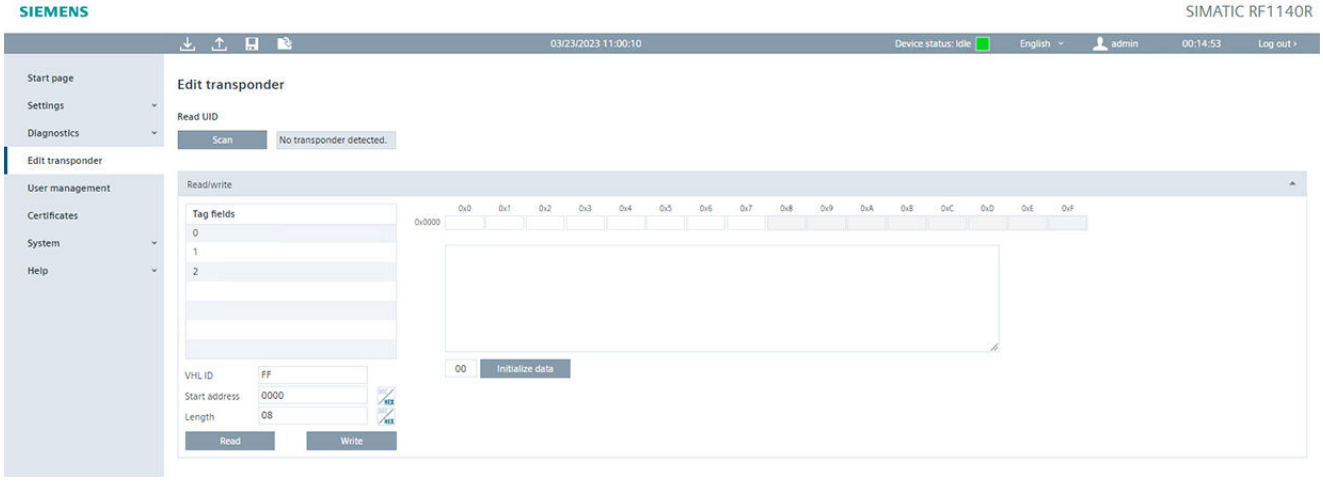


Figure 7-10 The "Edit transponder" menu item

Read UID

You can read out the UID (Unique Identifier) of the transponder in the "Read UID" area.

Read/write

In the "Read/write" area, you can read out and overwrite the memory areas. You can access pre-defined addresses (tag fields). Using the parameters, you can adapt the memory area manually.

Table 7-11 Description of the parameters of the tag fields

Parameter	Description
Tag fields	List with predefined addresses.
VHL ID	ID of the configuration stored in the reader.
Start address	Input box for entering the address within the selected tag field from which you want to read, change or write the data of the target transponder. You can use the button to change the input/output format (decimal or hexadecimal). Range of values: 0 ... 65535

Parameter	Description
Length	Input box for entering the length within the selected tag field and starting from the start address within which you want to read, change or write the data of the target transponder. You can use the button to change the input/output format (decimal or hexadecimal). Range of values: 1 ... 1024 bytes
Data	Input/output boxes for the values (decimal or hexadecimal). Possible characters: 0 ... 9, A ... F
ASCII	In the ASCII field, the data is shown additionally in ASCII notation. You can edit the data both in the data field and in the ASCII field.
Initialize data	Button for initializing the data. Using the initialization function, you can preset the data fields.

Next to the list of tag fields, the data of the selected memory area is displayed (decimal or hexadecimal and in ASCII).

With the "Read" button, the data is read from the transponder. The data read from the transponder is highlighted in red to distinguish it from the data entered manually. If no values are displayed, this means that no values have yet been read from the transponder.

Click the "Write" button to transfer the changed data to the transponder.

NOTICE
Read/write transponder data To enable transponder data to be read/written via the WBM, the reader must have been correctly initialized beforehand. Depending on the transponder/card types used, the reader may need to be configured using the Config Editor first. You can find information on this in the configuration manual "SIMATIC RF1000".

7.3.9 The "User management" menu item

In the "User management" menu item, you can enable/disable authentication, create, delete and edit user profiles and change passwords.

This page is divided into the following areas:

- User profiles
- User properties
- Password
- Roles
- Auto logoff
- Authentication
- Security settings

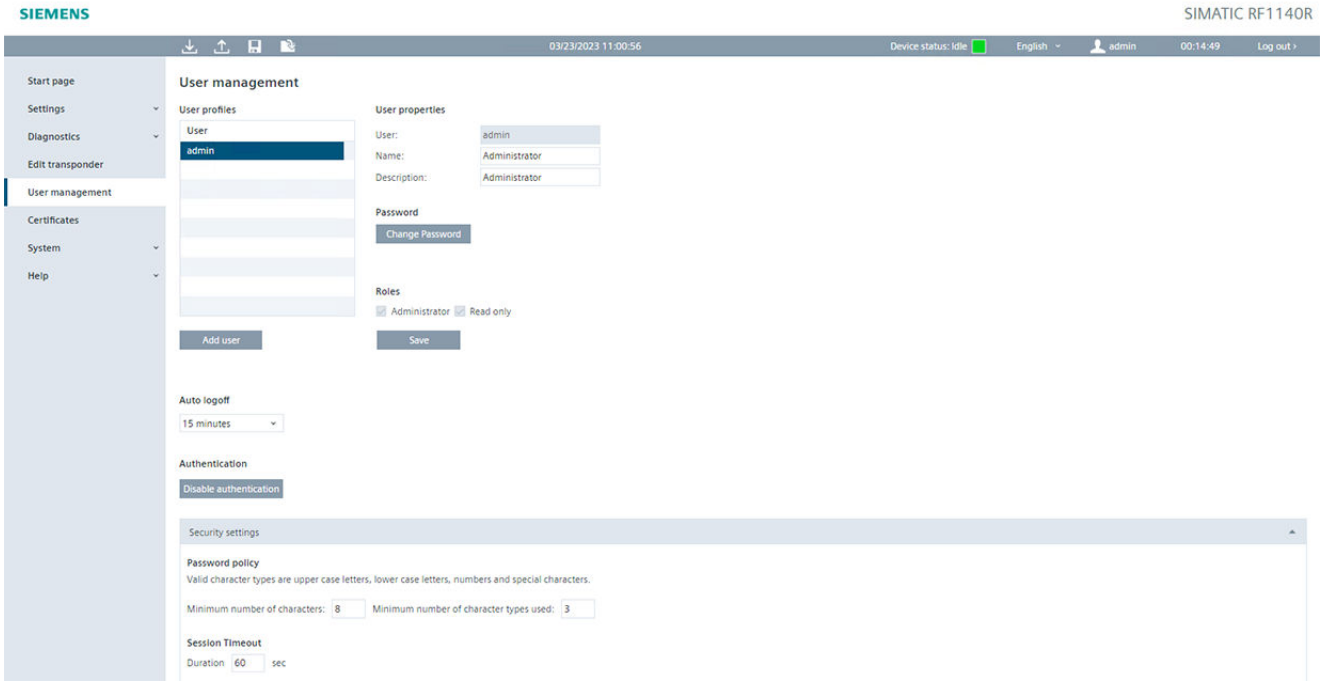


Figure 7-11 The "User management" menu item

User profiles

The "User profiles" area contains a list of all existing user profiles. Up to a maximum of 30 user profiles can be created. To edit a user profile, select the required user name in the list. The selected user name is highlighted in color.

Click the "Add new users" button to create a new user. Click the "Delete" button to delete a selected user profile.

User properties

In the "User" input box, enter the name of the newly created user profile. You require the user name and the password to log in to the WBM. The user name cannot be edited later.

In the "Name" input box, you can enter the name of the person or the name of the group that works with the user profile. In the "Description" input box, you can enter further information about the user profile.

Password

Enter the password of the user profile in the "Password" and "Repeat password" input boxes. You require the user name and the password to log in to the WBM. User passwords can be changed by the users themselves or an administrator. The strength of your password is indicated by color and text.

NOTICE
Security recommendation: Passwords You should also read the information under the "Passwords" heading of the "Security recommendations (Page 9)" section.

If you lose your administrator password, you must reset the reader to the factory settings as described in the section "Restoring the factory settings for the hardware (Page 79)".

Roles

In the "Roles" area, you can assign roles to the user profile. Click the relevant check box to assign the required roles to the user profile. The "Administrator" role has all read/write rights

- Administrator
  User profile with all read/write rights
- Read only
  Restricted user profile with read rights. With the "User" role, you cannot create new user profiles or edit other user profiles. Neither can you write to the reader.

Click the "Save" button to save the changes and to create the new user profile.

Auto logoff

In this area, you can define the time period after which you are automatically logged off of the WBM. This time period expires due to inactivity and is automatically reset to the value you have set. As soon as the configured time period has expired, the connection to the reader is automatically disconnected. This ensures that the connection to the reader is not blocked by an inactive user and is shared with other users.

Authentication

In this area, you can enable/disable authentication. Note that any user has all read/write privileges (administrator rights) when authentication is disabled.

NOTICE
Security recommendation: Authentication To ensure that no unauthorized persons can access the reader settings, we recommend that you enable the authentication and create new user profiles. Note that authentication can only be enabled/disabled by an administrator.

Security settings

You can define the conditions for the password policies, Session Timeout and Brute Force Prevention (BFP) in the "Security settings" area.

A brute force attack is an attack method in which password-protected access is decrypted by repeated and systematic entry of user/password variants and combinations based on powerful computer systems and automated software. With this attack method, an extremely large number of user/password variants/combinations can be processed with high performance.

This process is slowed down by Brute Force Prevention (BFP) by limiting the number of invalid login attempts, whereby the prospects of success of brute force attacks are reduced significantly. With the SIMATIC Ident devices, the leaky bucket algorithm is used. This means that the BFP level is increased by the set value on an invalid login attempt. If the BFP level

exceeds the defined BFP threshold value, all further login attempts are ignored. At the same time, the BFP level is reduced by the set value per second.

Table 7-12 Description of the security settings

Parameter	Description
Password policy	
Minimum number of characters	In this input box, you can define the minimum number of characters that the passwords of the user profiles need to contain. Range of values: 1 ... 32 Default setting: 12
Minimum number of character types used	In this input box, you can define the minimum number of character types that the passwords of the user profiles need to contain. Range of values: 1 ... 4 Default setting: 3
Session Timeout	
Period	In this input box, you can define the period of time after which the connection to the reader is terminated automatically (e.g. due to a terminated Ethernet connection). Range of values: 30 ... 3 600 s Default setting: 60 s
Brute Force Prevention (BFP)	
BFP level increase (per invalid login attempt)	In this input box, you can define the value by which the BFP level is increased on every incorrect password entry or every invalid login attempt. Range of values: 1 ... 10 000 Default setting: 200
BFP threshold value	In this input box, you can define the BFP threshold value. As soon as the BFP threshold is exceeded due to multiple incorrect password entries or invalid login attempts, all further login attempts are ignored. Successful login attempts are only possible again when the current BFP level falls below the BFP threshold value. Range of values: 1 ... 10 000 Default setting: 4 000
Maximum value of the BFP level	In this input box, you can define the maximum value of the BFP value. The BFP level is increased up until the value specified here, at most. Range of values: 1 ... 10 000 Default setting: 10000
BFP level reduction (per second)	In this input box, you can define the value by which the current BFP level is reduced every second. The BFP level is reduced every second until the BFP level is reduced to "0". Range of values: 1 ... 10 000 s Default setting: 50 s

Parameter	Description
Number of invalid login attempts	Output box/display of the number of invalid login attempts that can be made within x seconds until the BFP threshold value is reached and, consequently, all further login attempts are ignored. The values in these fields are calculated based on the input boxes "BFP level increase (per invalid login attempt)" and "BFP threshold value" or "BFP level increase (per invalid login attempt)" and "BFP level reduction (per second)".
Maximum wait time	Output box/display of the maximum wait time that elapses - after the maximum value of the BFP level has been reached - until successful login attempts are possible again, provided that no further invalid login attempts take place in the meantime. The value in this field is calculated based on the input boxes "Maximum value of the BFP level", "BFP threshold value" and "BFP level reduction (per second)".

Using the "Save" button, you can transfer the changed BFP values to the communications module. You can use the "Update" button to update the BFP values displayed in the WBM or reload them from the reader.

7.3.10 The "Certificates" menu item

In the "Certificates" menu item, you can view existing certificates, import new certificates, as well as create certificate signing requests and transfer certificate files and certificate key files to the reader.

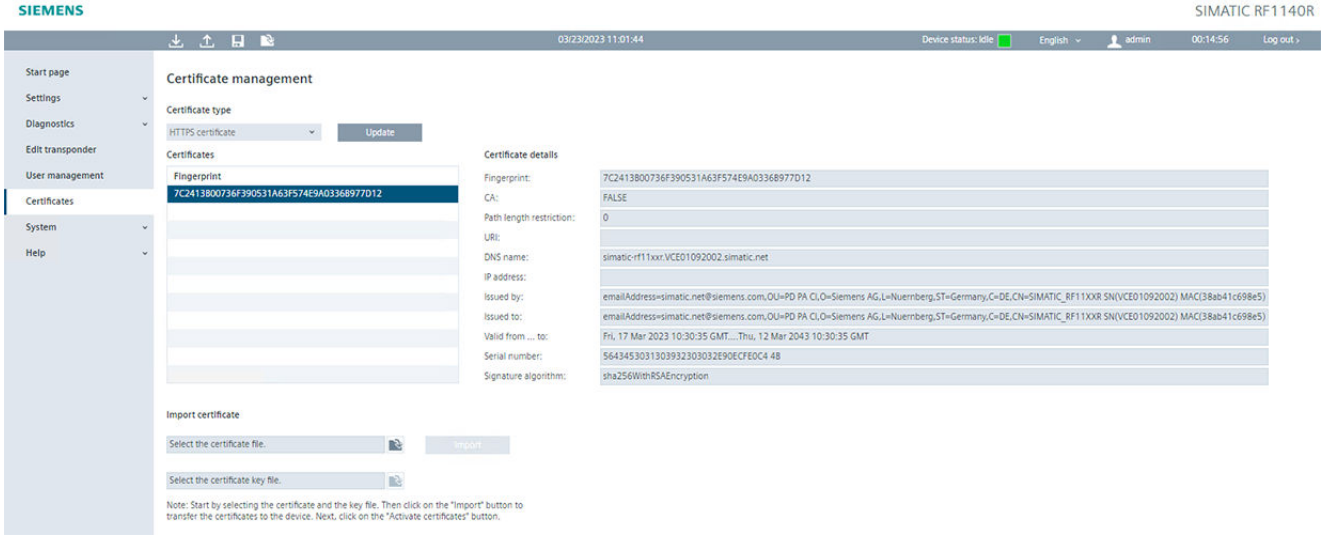


Figure 7-12 The "Certificates" menu item

Using certificates, you can integrate the reader in your specific security infrastructure. Certificates are used to check the identity of a person or a device, to authenticate a service or to encrypt files. You can create your own certificates or use official certificates created by a certification authority. You can import certificates that contain a certificate as well as a private key (PKCS#12). When you import certificates and the associated private keys in separate files, then both files must be coded either in "ASN.1" or "Base64".

Certificates always consist of a certificate file and a certificate key file that you must transfer to the reader. Remember that you first need to import the data into the reader before you can enable it.

Contact your administrative IT department for more information on the topic.

Parameter overview

Note that the parameters listed below depend on the selected certificate type and not all parameters are displayed for all certificate types.

Table 7-13 Description of the parameters

Parameter	Description
Certificate type	Selection of the certificate type Select the required certificate type from the drop-down list and click on the "Update" button to display the certificates matching the selected certificate type. • HTTPS certificate HTTPS certificate of the reader. Note that the selection of the certificate type has an effect on the display of the subsequent parameters.
Update	Button for refreshing the certificates displayed in the list Updating loads and displays all certificates currently stored in the reader.
Certificates	List of all existing certificates The certificates included in this list with a black background are considered as trustworthy by the reader. To display details of a certificate, select the required certificate in the list. The selected certificate field is highlighted in color. Certificates displayed in red have not yet been classified as trustworthy. A client using such a certificate cannot yet establish a connection to the OPC UA partner. These certificates must still be accepted and permitted by an administrator with the "Accept" button. Certificates displayed in black have already been accepted and are classified as trustworthy. Depending on the selected certificate type, you can delete existing certificates. To do so, select the desired certificate in the list and click on the "Delete" button.
Certificate details	List with detail information on the selected certificate Detailed information about the certificate details is available in the X.509 specifications.
Blacklists	List of all blacklists This area is only displayed when the certificate types "CA certificates" or "Issuer certificates" were selected. A blacklist is issued by a certificate authority. A blacklist must be stored for each CA certificate and issuer certificate. Blacklists give certification authorities the option to lock client certificates again that they have issued and signed. The certificates listed in a blacklist are locked for communication with the reader. To display the details of a blacklist, select the required blacklist in the list. The selected blacklist is highlighted in color. To delete blacklists from the list again, select the desired blacklist in the list and click on the "Delete" button.

Parameter	Description
Blacklist details	List with detail information on the selected blacklist Detailed information about the blacklist details is available in the X.509 specifications.
Importing a certificate	In this area, you can transfer the certificate files to the reader. Valid formats: • *.p12, *.pfx Binary file format, in which the certificate file and the certificate key file are stored in a single file. This file is usually protected by a password. Enter the password in the text box at the bottom. Note that this format can only be used for server certificates. • *.cer, *.crt, *.der, *.pem Binary or text coded file format, in which the certificate file and the certificate key file are stored in separate files. Note that the server certificates necessarily require a separate certificate key file. Once you have imported a server certificate, you still need to enable it.

Supported file formats

The following table provides an overview of the file formats supported by the various certificate types.

Table 7-14 Supported file formats of the various certificate types

Certificate types	Supported file formats
HTTPS	*.p12 *.pfx *.pem [1)] *.cer *.der

[1)] May contain a private key.

7.3.11 The "System - Device settings" menu item

In the "System - Device settings" menu item, you can update firmware, reset the reader to the factory settings, change the IP address of the reader, load certificates onto the reader and transfer control files to the PC. This page is divided into the following areas:

- Firmware update
- Reset

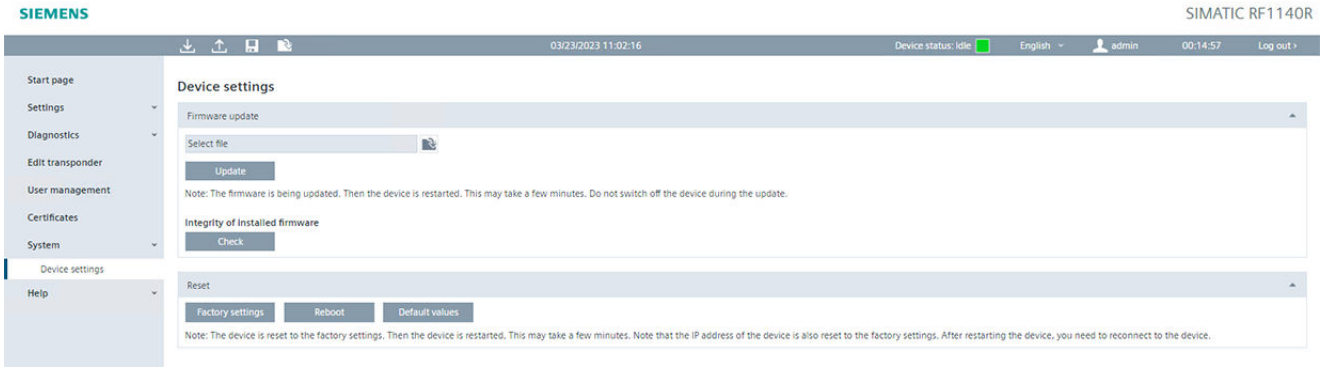


Figure 7-13 The "System - Device settings" menu item

Firmware update

- Firmware update
  With the "Firmware update" button, you can update the firmware of the communications module. For a detailed description of firmware updates, refer to the section Updating the firmware via WBM (Page 77).
- Check
  You can use the "Check" button to check the integrity of the firmware. You can use this function to check whether the firmware matches the firmware published by Siemens or whether it has possibly been maliciously modified.

Factory setting

In the "Factory settings" area, you can restore the reader's factory settings or preset default values or restart it.

- Factory setting
  Using the "Factory settings" button, you can restore the factory configuration settings on the reader. When you restore the factory settings of the reader, all set configuration data, settings of the user management and address information are lost. After the reset, the reader is automatically restarted. Note that you then need to assign new IP addresses to the reader. If you lose your administrator password, you must reset the reader to the factory settings as described in the section "Restoring the factory settings for the hardware (Page 79)".
- Restart
  You can use the "Reboot" button to restart the reader.
- Default values
  You can use the "Default values" button to reset the parameter values of the reader to the factory configuration settings. When resetting to the default values, all set configuration data is lost, but user management settings and address information are retained.

7.3.12 The "Help" menu item

Service & Support

The "Help - Service and Support" menu item includes additional information on the RF1140R/ RF1170R reader, as well as links to the relevant documents and the Siemens Industry Online Support pages. Via a link, you can also open the Readme OSS file with the copyright information and license conditions for the open source software contained in this firmware.

Manual

With the "Help - Manual" menu item, you can find the corresponding "SIMATIC RF1100" manual for the reader or WBM.

Programming

8

8.1 Programming via XML

This section is intended only for XML users.

Requirement: The XML interface has been activated in WBM.

You can program the reader via the XML interface using XML commands. You can find detailed information on this in the manual "XML programming for SIMATIC Ident (https://support.industry.siemens.com/cs/ww/en/view/109781631)".

8.2 Programming via Modbus

This section is intended only for Modbus users.

Requirement: The Modbus interface has been activated in WBM.

Specific function blocks for programming the Modbus interface are available to you depending on the controller used. When connected to S7-1200/1500, the reader is programmed using the "MB_CLIENT" function block. This function block supports a wide variety of Modbus functions. The basic functions for reading the UID and tag fields are already implemented in the WBM of the reader and the data can easily be requested in this way. Via the WBM, you can easily create tag fields and determine which transponder data can be read out via the Modbus interface. You can find more information on this in the section "The "Settings - Reader configuration" menu item (Page 43)".

You can find a detailed description of the "MB_CLIENT" function block on the Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/62830463) pages.

NOTICE
Access to the reader Remember that simultaneous access to a reader using multiple Modbus clients is possible but not recommended. If changes are made when two Modbus clients are accessing a reader at the same time, this can lead to errors in the configuration or to an undesired result.

Reader-specific Modbus functions

You can perform the following functions via the Modbus interface:

- Read UID/tag fields
- Detect the presence of a transponder
- Read/write user data via preset tag fields
- Read/write user data via address and length
- Program reader LEDs

These functions are described below.

8.2.1 Register overview

The Modbus interface of the reader consists of Input and Holding registers (see table). You can access these registers using the following Modbus functions:

- Read Holding Registers 3
- Write Single Register 6
- Write Multiple Registers 16

The registers need to be addressed accordingly depending on the function to be executed. The following table provides an overview of the specific Modbus registers of the reader.

Table 8-1 Register overview

Register address	Register quantity	Register name	Data type	Access
0	1	Status	Word	R
1	11	reserved	Word	--
12	1	Tag field name	Word	R/W
13	1	VHL File ID	Word	R/W
14	1	Address Hi	Word	R/W
15	1	Address Lo	Word	R/W
16	1	Length	Word	R/W
17	1	Command	Word	R/(W)
18	1	reserved	Word	--
19	1	Result	Word	R
20	100	Data	Word Data[0..99]	R/W
120	1	LED Control	Word	R/W

8.2.2 RFID functions

8.2.2.1 Read UID/tag fields

This function allows you to read out the UID or a tag field from a transponder. Tag fields are user-defined memory areas on a transponder. Specific transponder data can be read with tag fields. So that the data can be displayed in the "Data" register, the parameters need to be selected accordingly in the WBM.

For the "UID" use case, it is only necessary to select the "UID" parameter in the WBM. For the "Tag fields" use case, the length and address of the user memory must be specified in the WBM. Using the UID or the tag field selection, you can read out the data without changing the read or write parameters in the Modbus client program.

UID

The "Command" register is preset with the "Read UID" command. The UID is output in the "Data" registers. The "Length" register shows the length of the UID. The result output in the "Data" register is valid if the register shows "Result = Done".

Tag fields

The "Tag field name" register contains the name of the tag field as it is configured in the WBM. The "Command" register is preset with the "Read tag field" command. Note that the command can be changed or a different tag field can be selected by the client during runtime. If a different tag field is selected in the WBM, the "Command" and "Length" registers are automatically changed accordingly.

Table 8-2 Relevant registers

Register address	Register name
16	Length
17	Command
19	Result
20 ... 119	Data

8.2.2.2 Detecting the presence of a transponder

This register reports the presence of a transponder.

Table 8-3 Relevant registers

Register address	Register name
0	Status

8.2.2.3 Reading/writing user data via tag fields

With this function, you can read out data from a symbolically addressed memory area of a transponder or write data to it. The address of the data area is stored in the tag field. Access takes place via the name of a tag field. You can create tag fields in the WBM.

Read (Command = 2)

With "Tag field name", a tag field (memory area) created in the WBM is selected. The data is provided from the "Data" registers, if the register shows "Result = Done".

Write (Command = 3)

With "Tag field name", a tag field (memory area) created in the WBM is selected. The data in the "Data" registers was written to the transponder, if the register shows "Result = Done".

Table 8-4 Relevant registers

Register address	Register name
12	Tag field name
16	Length
17	Command
19	Result
20 ... 119	Data

8.2.2.4 Reading/writing user data via address and length

With this function, you can read out data from a memory area of a transponder or write data to it. The appropriate VHL File ID must be specified depending on the configuration used. When unencrypted MDS D transponders are used, "VHL File ID = 255".

Read (Command = 4)

The memory area is defined by the "VHL File ID", "Address" and "Length" registers. With "VHL File ID = 255", "Address" and "Length" are absolute values. If "VHL File ID ≠ 255", the configuration is a user-created configuration that was loaded. In this case, "Address" and "Length" relate to the element defined by the VHL File ID. The data is provided from the "Data" registers, if the register shows "Result = Done".

Write (Command = 5)

The memory area is defined by the "VHL File ID", "Address" and "Length" registers. With "VHL File ID = 255", "Address" and "Length" are absolute values. If "VHL File ID ≠ 255", the configuration is a user-created configuration that was loaded. In this case, "Address" and "Length" relate to the element defined by the VHL File ID. The data in the "Data" registers was written to the transponder, if the register shows "Result = Done".

Table 8-5 Relevant registers

Register address	Register name
13	VHL File ID
14	Address Hi
15	Address Lo
16	Length
17	Command
19	Result
20 ... 119	Data

8.2.2.5 Define LED behavior

With this function, you can define the behavior of the reader LEDs or overwrite the LED behavior.

Table 8-6 Relevant registers

Register address	Register name
120	LED Control

8.2.3 Register

8.2.3.1 Status

You can view the presence of transponders with this register.

Table 8-7 Register structure

	Bit	
	15...1	**0**
Name	Reserved	Presence
Access	Read only	Read only
Default value	0	1 = Transponder in antenna field

8.2.3.2 Tag field name

With this register, you define tag fields for the commands "Read tag field" and "Write tag field". The address of the data area is specified by the name of a tag field. The tag field and the name of the field are specified using the WBM.

Table 8-8 Register structure

	Bit
	15...0
Name	Tag field name
Access	Read and write
Default value	0

8.2.3.3 VHL File ID

With this register, you define VHL File IDs for the commands "Read tag field" and "Write tag field" which are used when accessing the user memory of the transponder.

The value is ignored during the UID read operation.

Table 8-9 Register structure

	Bit	
	15...8	**7...0**
Name	Reserved	VHL File ID
Access	Read only	Read and write
Default value	0	0xFF

8.2.3.4 Address Hi

This register contains the most significant bits of the start address of the command (i.e. the first data retrieved from the transponder). These are relevant for executing the "Read" and "Write" commands.

The value must be set by the client.

The value is ignored for the UID/tag field access.

Table 8-10 Register structure

	Bit
	15...0
Name	Address 31...16
Access	Read and write
Default value	0

8.2.3.5 Address Lo

This register contains the least significant bits of the start address of the command (i.e. the first data retrieved from the transponder). These are relevant for executing the "Read" and "Write" commands.

The value must be set by the client.

The value is ignored for the UID/tag field access.

Table 8-11 Register structure

	Bit
	15...0
Name	Address 15...0
Access	Read and write
Default value	0

8.2.3.6 Length

With this register, you can define the length of the data to be read from the transponder or written to the transponder. When the UID or a tag field is read, the length is set to the length of the UID data or tag field data.

Note that the data length cannot exceed 200. If more data is specified, the command fails and an error code is generated in the "Result" register.

Table 8-12 Register structure

	Bit
	15...0
Name	Length
Access	Read and write
Default value	0

8.2.3.7 Command

With this register, you define the type of access of the reader to the transponder.

If one of the registers between VHL File ID and Data[99] is written while the reader processes commands, the error message "4 – Application error" is returned. To support the client with the continuous query, no error message is returned if exactly the same data is written while the reader is busy. Instead, the write operations are ignored.

To support the client, repeated write commands with identical data contents are only performed when the "Done" bit in the "Result" register is not set. This bit is automatically reset as soon as a new transponder is detected or the current transponder leaves the antenna field of the reader. An error is never reported when the "Data" register is read. A new read command is only started when neither the "Done" nor the "Busy" bit is set.

Command processing modes

- Normal case
  The "Done" bit is reset as soon as a new transponder is detected.
- Force
  Transponder access operations with the same data are only performed once per transponder. If the client wants to repeat the same access operation for the same transponder, the "Force" bit needs to be set to perform the access operation again.
- Wait
  When this bit is set, read access to the "Result" register is delayed until the current operation is complete ("Busy = 0"). In this way, the client can avoid querying the "Result" register. After an operation is started, the client can start reading of the "Result" register, which only ends after the operation has been completed.

Possible commands

- 0: No command
  Read commands return the values last written to the "Data" registers. If a switch takes place from one of the following commands (1...5) to this command, this deletes the entries in the "Data" tab.
- 1: Read UID
  Write access to the "Data" registers is ignored, while read access starts retrieving the UID of the transponder. The length of the UID is in the "Length" register. The UID data is saved in the "Data" registers. When the command is started, the "Data" registers are deleted or reset to 0. While the command is being executed, further read operations to the "Data" registers return the value "0". This command is automatically preset if the "UID" tag field is selected in the WBM.
- 2: Read tag field
  In contrast, read access starts retrieving the tag field data. Length, Address and VHL File ID are provided by the tag field definition in the WBM. When the command is started, the "Data" registers are deleted or reset to 0. While the command is being executed, further read operations to the "Data" registers return the value "0". This command is automatically preset if one of the tag fields "0...9" is selected in the WBM.
- 3: Write tag field
  Read access to the "Data" registers return the previously written values. Write access starts a write operation to the address area of the user memory of the transponder. The address area is provided by the tag field definition in the WBM.
- 4: Read
  In contrast, read access retrieves the user memory values designated by the "Offset" and "Length" register in the "Data" register. When the command is started, the "Data" registers are deleted or reset to 0. While the command is being executed, further read operations to the "Data" registers return the value "0".
- 5: Write
  Read access to the "Data" registers return the previously written values. Write access starts a write operation to the user memory of the transponder with consideration of "Address" and "Address + Length".

Table 8-13 Register structure

	Bit			
	15	**14**	**13...5**	**4...0**
Name	Force	Wait	Reserved	Command
Access	Write only	Read and write	Read only	Read and write
Default value	0	0	0	0

8.2.3.8 Result

This register contains the result of the last command. It is reset as soon as a new command is started.

Depending on the configured command, reading via Modbus is delayed until the current command is completed (OK or Error).

- Busy
  Set to "1" when a command is active but not yet completed.
- Done
  Set to "1" when the last command has been completed (OK or Error). This bit is reset as soon as a new transponder is detected. When this bit is set, repeated commands (e.g. same command, same data) are ignored. Writing different values into the setup registers (VHL File ID, Command, Length, Address) deletes the "Done" bit.
- Status
  If the last command was executed, this bit receives the value "0". If the command was not executed, the error code is displayed in the bit. The error codes from the Ident profile are used.

Table 8-14 Register structure

	Bit		
	15	**14**	**13...0**
Name	Busy	Done	Status
Access	Read only	Read only	Read only
Default value	0	0	0

8.2.3.9 Data

Either these registers contain the result of a read command, or the client writes the data for a write command into these registers.

If these registers are read while a read command is pending at the same time, the value "0" is returned. If these registers are read while a write command is pending at the same time, the written values are returned.

Table 8-15 Register structure

	Bit	
	15...8	**7...0**
Name	Data [2*n]	Data [2*n+1]
Access	Read and write	Read and write
Default value	0	0

8.2.3.10 LED Control

You can use this register to assign parameters to the LEDs and the acoustic signal of the reader.

Table 8-16 Register structure

	Bit		
	15...8	**7**	**6...0**
Name	Flash frequency of LED	Acustic signal	LED color
Access	Read and write	Read and write	Read and write
Default value	0	0	0
Possible values	• 0: • 1: 1 Hz • 2: 2 Hz • 3: Reserved • 4: 4 Hz • 5...255: Reserved	• 0: Off • 1: On	• 0: Transparent (the reader controls the LED) • 1: Off • 2: Red • 3: Orange • 4: Green • 5...255: Reserved

Error messages

9

You have the following options for error analysis of the modules:

- Using WBM
- Via XML error messages

These alternative methods are described below.

9.1 Reading out error messages using the WBM

All the diagnostic messages of the reader are entered in the "Log" if a check mark was set for "ERRORS" in the WBM configuration in "Settings - General". You will find further information on the "Log" in the section "The "Diagnostics - Log" menu item (Page 49)".

9.2 XML/Modbus error messages

A list of the possible XML/Modbus error codes can be found in the "XML programming for SIMATIC Ident (https://support.industry.siemens.com/cs/ww/en/view/109781631)" manual.

The XML error messages are identical to the Modbus error messages. The error codes in the "Result code" column are relevant for Modbus.

Maintenance and service 10

10.1 Diagnostics

You have the following diagnostics options available for the readers:

- Via the LED display
- Via SNMP
- Using WBM
- Via XML

These alternative methods are described below.

10.1.1 Diagnostics via the LED display

The "R/S" LED indicates the reader's operating states. The LED can be green, orange or red and have the states off, on, flashes:

Table 10-1 Display of the operating states via the LEDs

R/S	Meaning
	The reader is turned off.
	The power supply was switched off and the reader is starting up.
	There is a transponder in the antenna field.
	The reader is starting up. The reader is being initialized and/or the connection to the user application is terminated.
	The reader is switched on and ready for operation. The connection to the user application has been established.
	The reader is in license mode.
	The flash test is performed for reader identification.
	A firmware update is in progress.
	There is an error. You can find detailed information on the error in the "Logbook (Page 49)".

10.1.2 Diagnostics via SNMP

Using SNMP, you have extensive diagnostics options for the network functions of the reader. The following diagnostics options (MIBs) are supported by the readers:

- RFC 2863: IF-MIB
- RFC 3418: SNMPv2-MIB

- RFC 4022: TCP-MIB
- RFC 4113: UDP-MIB
- RFC 4292: IP-MIB
- SIEMENS:
  - AUTOMATION-SN-SYSTEM-MIB
  - AUTOMATION-SYSTEM-MIB
  - IEEE 802.1AB 2005 LLDP-MIB
  - LLDP-EXT-DOT1-MIB
  - LLDP-EXT-DOT3-MIB
  - LLDP-EXT-PNO-MIB

You can find the MIB files corresponding to the readers on the pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/67637278), and you can find information on the MIB files under "PROFINET user organization (https://www.profibus.com/download/profinet-specification/)".

The readers support the SNMPv3 and SNMPv1 protocol. SNMPv1 is classified as non-secure. Deactivate SNMP if it is not required or use SNMPv3. You can find information on SNMP in the section "The "Settings - Network interface" menu item (Page 46)".
You can find detailed information on using SNMP and, in particular, on the structure of the automation.mib in the diagnostics manual "Network management diagnostics and configuration with SNMP (https://support.industry.siemens.com/cs/ww/en/view/103949062)".

10.1.3 Diagnostics using the WBM

A wide variety of diagnostics options are available via the WBM. These are described below.

In the "Log" menu, you can find all the diagnostics messages of the communication module that have occurred. The "Service log" helps SIEMENS specialists to analyze errors. You can read out the syslog messages of the reader from the "Syslog logbook".

You will find further information on the "Log" in the section "The "Diagnostics - Log" menu item (Page 49)".

10.1.4 Diagnostics via XML

This section is intended only for XML users.

Comprehensive diagnostics options are available to you via XML. You can find detailed information on the diagnostic options in the "XML programming for SIMATIC Ident (https://support.industry.siemens.com/cs/ww/en/view/109781631)" manual.

10.2 Updating the firmware via WBM

You can perform a firmware update using the WBM.

Requirements

- The reader is connected to the PC via Industrial Ethernet.
- The reader has been disconnected from running operation.
- The required update file (*.sfw) is stored locally.

Procedure

Proceed as follows to run a firmware update using the WBM:

1. Start your Web browser.
2. Enter the IP address of the reader in the address field of your browser.
3. If not logged in, log in to the WBM.
   Please note that as a "Read only" user, you cannot perform a firmware update.
4. Click on the "System - Device settings" menu item.
5. In the "Firmware update" area, click the "Select firmware file" icon .
6. Select the update file (*.sfw).
7. Click on the "Open" button.
8. Click the "Update" button.

Result: The firmware is updated. The update process is indicated in the information bar.

After the update has completed, the reader is restarted. The reader is ready for operation when the "R/S" LED is lit green. Note that the startup process takes approx. 1 minute after a firmware update.

The updated firmware is active following the restart.

10.3 Factory settings

You can restore the configuration of the communication modules to the factory settings at any time. To reset to the factory settings, you have the following options available:

- Using WBM
- Via SINEC PNI
- Via XML
- On the hardware side using the Reset button

These alternative methods are described below.

10.3.1 Restoring the factory settings via WBM

Requirement

The reader is connected to the PC via Industrial Ethernet.

Procedure

Proceed as follows to reset all settings to the factory settings using the WBM:

1. Start your Web browser.
2. Enter the IP address of the reader in the address field of your browser.
3. If not logged in, log in to the WBM.
4. Click on the "System" menu item.
5. In the "Reset" area, click on the "Reset" button.

Result: The reader is reset to the original factory settings. The restore process is indicated in the information bar.

Note that restoring the factory settings also resets the IP address of the reader. With the factory settings, the IP address is obtained via a DHCP server. You can only recognize when the reset is finished based on the "R/S" LED. After the reset, the reader is restarted. The reader is ready for operation when the "R/S" LED is lit green.

After restarting the reader, you may need to assign a new IP address or a new device name to the reader.

10.3.2 Reset the factory setting with SINEC PNI

Requirement

The reader is connected to the PC via Industrial Ethernet.

Procedure

Proceed as follows to reset all settings to the factory settings using SINEC PNI:

1. Start SINEC PNI.
2. Click on the "Start network scan" button on the toolbar.
   Reaction: The network is scanned for connected devices and all recognized devices are displayed in the device list.
3. Select the desired reader in the device list.
4. Click on the "Reset device" button on the toolbar.

Result: The reader is reset to the original factory settings.

Note that restoring the factory settings also resets the IP address of the reader. With the factory settings, the IP address is obtained via a DHCP server. You can only recognize when

the reset is finished based on the "R/S" LED. After the reset, the reader is restarted. The reader is ready for operation when the "R/S" LED is lit green.

After restarting the reader, you may need to assign a new IP address or a new device name to the reader.

10.3.3 Restoring the factory settings via XML

Via the XML interface, you can use the command "resetDevice" to reset all settings to the factory settings.

Note that restoring the factory settings also resets the IP address of the reader. With the factory settings, the IP address is obtained via a DHCP server. You can only recognize when the reset is finished based on the "R/S" LED. After the reset, the reader is restarted. The reader is ready for operation when the "R/S" LED is lit green.

After restarting the reader, you may need to assign a new IP address or a new device name to the reader.

10.3.4 Restoring the factory settings for the hardware

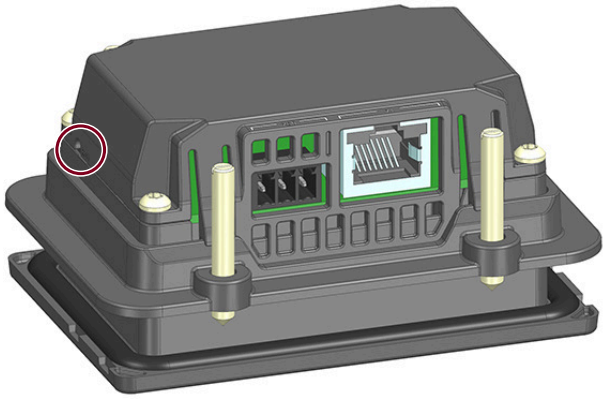
Requirement

The reader has been disconnected from the power supply.

Procedure

Follow the steps below to reset all settings to the factory settings using the Reset button:

1. Press and hold the Reset button using a pointed object.



2. With the Reset button pressed, connect the reader to the power supply (24 V DC or PoE).
3. Wait for 30 seconds.

4. Release the Reset button.
5. Wait until the "R/S" LED is continuously lit in green.

Result: The reader was reset to its original factory settings.

Note that restoring the factory settings also resets the IP address of the reader. With the factory settings, the IP address is obtained via a DHCP server.

After restarting the reader, you may need to assign a new IP address or a new device name to the reader.

10.4 Module replacement

NOTICE
Backing up the configuration Prior to replacing the module, make sure that you back up the configuration stored on the reader so that you can transfer this to the newly connected reader following module replacement.

NOTICE
Loading a configuration Note that you cannot transfer any user profiles and passwords to other readers using the configuration file. After loading the configuration file into a new reader, you may need to enable authentication and create new user profiles and passwords.

With the WBM, you can back up the current configuration of the reader and restore it on the newly connected reader following module replacement.

10.4.1 Backup configuration data

Table 10-2 Properties and requirements

Backup option	Properties
Backup via the WBM (as *.xml file)	• Configuration data is saved regardless of the project and controller ⇒ The download to the communication module can be performed manually using the WBM user application. • You can copy additional communication modules of the same type • Older configuration versions can be saved (versioning) ⇒ The updating and versioning of the configuration versions needs to be started and managed manually by you yourself.

Backup via the WBM

On the upper toolbar of the WBM, there are two buttons for loading and saving configurations. Using these buttons, you can back up configurations, re-load them and transfer them to other readers. You will find further information on saving and loading the configuration on or from the PC in the section "The WBM (Page 35)".

10.4.2 Replacing a module

Requirements

The reader is installed. A new reader of the same type is ready.

Before replacing a module

NOTICE
Backing up the configuration Prior to replacing the module, make sure that you back up the configuration stored on the reader so that you can transfer this to the newly connected reader following module replacement.

NOTICE
Installation/removal with the power off Wire the readers to be connected only when the power is off. Make sure that the power supply is turned off when installing/uninstalling the devices.

Procedure

Follow the steps below to replace a reader:

1. Make sure that the reader is disconnected from the power supply.
2. Pull the cable from the reader.
3. Unmount the reader.
4. Mount the new reader.
5. Connect the reader to the PC using the supplied Ethernet cable.
6. Connect the reader to the power supply using the connecting cable, if necessary.
   Wait until the reader has started up and is ready for operation ("R/S" LED is lit green).
7. If necessary, assign the reader a unique IP address and a unique device name.
8. Load the configuration(s) (WBM and possibly Config Editor) to the reader.
9. Configure the user management according to the requirements of your application.

Technical specifications 11

11.1 Technical specifications of SIMATIC RF1100

Table 11-1 Technical specifications of the SIMATIC RF1100 reader

	6GT2831-6xB00
Product type designation	SIMATIC RF1140R SIMATIC RF1170R
Radio frequency	
Operating frequency	
• RFID	• RF1140R: 125 kHz; 13.56 MHz • RF1170R: 13.56 MHz
• BLE	• 2.402 ... 2.48 GHz
Protocol for wireless transmission	RF1140R, RF1170R: ISO 14443 A/B, ISO 15693, LEGIC advant, MIFARE Classic, MIFARE DESFire, MIFARE Plus, MIFARE Ultralight, HID iClass, NXP NTAG21x, FeliCa BLE for wireless communication RF1140R (in addition): EM4100/EM4102, EM4450/EM4550, HITAG 1, HITAG S, HITAG 2, Keri, SecuraKey, AWID, ioProxy RF1170R (in addition): LEGIC prime
Electrical data	
Maximum transmission power	• RF1140R: – 13.56 MHz: 250 mW – 125 kHz: < 50 mW • RF1170R: 200 mW
Maximum range	30 mm
Mechanical specifications	
Housing	
• Material	• Lexan EXL5689
• Color	• TI-Gray
Interfaces	
RFID	Integrated antenna
BLE	Integrated antenna (default: deactivated)

	6GT2831-6xB00
Ethernet interface	
Type of connection	XML, Modbus TCP
Physical medium	Ethernet over 4-wire cable
Operating mode	100BaseX full duplex
Transmission speed	100 Mbps
Connector	RJ45
Max. cable length	100 m
Cable type	STP Cat 5
Autonegotation	Yes
Autocrossing	Yes
Switch function	No
Vendor ID	0x002A
Device ID	0x0C0A
Supply voltage, current consumption, power loss	
Power supply	
• Power over Ethernet (PoE)	• 3.5 W
• 24 V DC	• 20 to 30 V DC
• Supply interruption (max.)	• 1 ms
Current consumption (at 24 V DC)	
• Typical	• 100 mA
• Maximum	• 130 mA
Permitted ambient conditions	
Ambient temperature	
• During operation	• -25 ... +55 °C
• During transportation and storage	• -25 ... +55 °C
Minimum distance between two readers	15 cm [1]
Degree of protection according to EN 60529 (in installed state)	• Front: IP65 [2] • Rear: IP20
Shock-resistant to IEC 61131-2	150 m/s²
Vibration-resistant acc. to IEC 61131-2	10 m/s²
Design, dimensions and weights	
Dimensions (W × H × D)	
• Reader excl. card holder	• 90 × 62 × 45.5 mm
• Mounting opening	• 76.5 (± 0.3) × 48.5 (± 0.3) mm
Weight	Approx. 170 g
Type of mounting	• 4 x stud screws (slotted screws) M4 x 20 • Installation wall thickness 2-7 mm

	6GT2831-6xB00
Approvals	CE / FCC / IC
MTBF	103 years

1) The minimum distance can be lowered if, from an application point of view, it is permissible that a transponder can also be read by an adjacent reader.

2) IP67 in connection with the cleanroom cover

11.2 Technical specifications of the license card

Table 11-2 Technical specifications of the license card

	6GT2300-0CC00-0AX1
Product type designation	HID license card for SIMATIC RF1000 and RF1100
Mechanical specifications	
Housing	
• Material	• PVC
• Color	• White
Printing	Writeable handwritten
Permitted ambient conditions	
Ambient temperature	
• During write/read access	• -25 ... +60 °C
• Outside the read/write field	• -25 ... +60 °C
• During storage	• -25 ... +60 °C
Degree of protection according to EN 60529	IP67
Design, dimensions and weights	
Dimensions (D × W × H)	86 × 54 × 0.8 mm
Weight	6 g

Dimension drawings

12

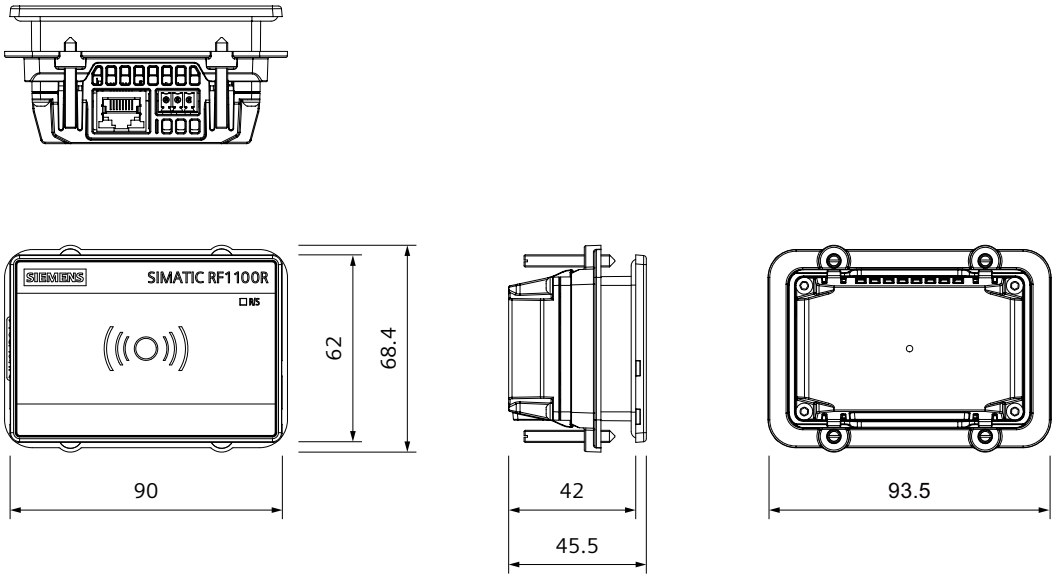


Figure 12-1 Dimension drawing of a SIMATIC RF1170R

All dimensions in [mm].

Appendix

A

A.1 Certificates & approvals

Note

Granted approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

Current approvals

SIMATIC NET/SIMATIC Ident products are regularly submitted to the authorities and approval centers for approvals relating to certain markets and applications.

Contact your Siemens representative if you need a list of the current approvals for the individual devices or check the Internet pages of Siemens Industry Online Support:

Current approvals (https://support.industry.siemens.com/cs/ww/en/ps/15728/cert)

Go to the relevant product there and select the "Certificates" entry type from the "Entry list" tab.

Overview of the approvals and standards

The RF1140R/RF1070R readers have the following approvals and meet the following standards:

- EC directives and standards
  - EU directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive) according to the following standards:
    EN 61000-6-1, EN 61000-6-2, EN 61000-6-3, EN 61000-6-4, EN 55032, EN 55024
  - EU Directive 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS)
- cULus LISTED IND. CONT. EQ.
- FCC

EU Declaration of Conformity

CE

The RF1140R/RF1070R readers meet the general and safety-related requirements of the following EU directives and conform to the harmonized European standards (EN) for programmable controllers published in the official gazettes of the European Union and here:

- EU directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive)
  - Immunity
    EN 61000-6-2: Industrial area
  - Noise emission
    EN 55032: Electromagnetic Compatibility of Multimedia Devices and Equipment - Requirements for emissions
- EU Directive 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS)

The CE Declaration of Conformity is available for the responsible authorities at the following address:

Siemens AG
D-76181 Karlsruhe
Germany

You will find the CE Declaration of Conformity for this product on the Internet at the following address:

CE declaration of conformity (https://support.industry.siemens.com/cs/ww/en/ps/15105/cert)

Country-specific approvals

Safety

If the device has one of the following markings, the corresponding approval has been obtained.

Marking	Description
CE	CE according to RED directive 2014/53/EU CE according to RoHS directive 2011/65/EU
FC Federal Communications Commission	This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. **Caution** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. **Note** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Marking	Description
Industry Canada Radio Standards Specifications	This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. Le présent appareil est conforme aux CNR d`Industrie Canada applicables aux appareils radio exempts de licence. L`exploitation est autorisée aux deux conditions suivantes : (1) L`appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l`appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d`en compromettre le fonctionnement.
UK CA	Importer UK: Siemens plc, Sir William Siemens House, Princess Road, Manchester M20 2UR

A.2 Encryption methods (ciphers)

The following tables list the encryption methods (ciphers) that the device uses.

SSL

Table A-1 Supported encryption methods (cipher suites) for HTTPS WBM servers

Category	Method	Value (hex)	Enabled by default
Cipher suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC02F	✓
Cipher suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC030	✓
Cipher suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Cipher suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Cipher suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Cipher suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Protocol version	TLSv1.2	--	✓
Protocol version	TLSv1.3	--	✓

SNMP

Table A-2 Supported encryption methods (cipher suites) for SNMP servers

Category	Method	Value (hex)	Enabled by default
Authentication	HMAC-MD5-96	--	--
Authentication	HMAC-SHA-96	--	--
Encryption	aes128-cbc	--	--
Encryption	des-cbc	--	--

A.3 Ordering data

Table A-3 Ordering data

Product	Article number
SIMATIC RF1140R	6GT2831-6CB00
SIMATIC RF1170R	6GT2831-6BB00

Table A-4 Ordering data accessories

Product	Article number
Card holder for RF1100	6GT2890-0CA00
Cleanroom cover surface installation for RF1100	6GT2890-0CC00
HID license card for SIMATIC RF1000 and RF1100	6GT2300-0CC00-0AX1

Syslog messages

B

B.1 Structure of the Syslog messages

The Syslog server collects all logbook information of the devices and informs you about specific events. The Syslog messages are received from the Syslog server over the configured UDP port (default: 514) and sent according to RFC 5424 or RFC 5426.

Syslog messages log information during access to the device. Information can be status information, such as the origin of the message or a time stamp. The Syslog protocol prescribes a specified order and structure of the possible parameters. Syslog messages are structured as follows in accordance with RFC 5424:

Table B-1 Structure of the Syslog messages

Parameter	Explanation
HEADER	
PRI	Within PRI, the priority of the Syslog message is coded into Severity (severity of the message) and Facility (origin of the message).
VERSION	Version number of the Syslog specification.
TIMESTAMP	The device sends the time stamp in the format "2010-01-01T02:03:15.0003+02:00" as local time including time zone and adjustment for daylight saving time/standard time, if necessary.
HOSTNAME	References the source device with its name or IP address. IPv4 address according to RFC1035: Bytes in decimal form: XXX.XXX.XXX.XXX If there is no information, "-" is output.
APP-NAME	Device or application from which the message originates. This parameter is not used by the device and "-" is always output.
PROCID	The process ID is used to clearly identify the individual processes, for example, during analysis and troubleshooting. This parameter is not used by the device and "-" is always output.
MSGID	ID for identification of the message. This parameter is not used by the device and "-" is always output.
STRUCTURED-DATA	
timeQuality	The structured data element "timeQuality" provides information on the system time. The "tzKnown" parameter specifies whether the sender knows its time zone (value "1" = known; value "0" = unknown). The "isSynced" parameter specifies whether the sender is synchronized with a reliable external time source, e.g. via NTP (value "1" = synchronized; value "0" = not synchronized).
sysUpTime	The "sysUpTime" parameter is metainformation about the message. It specifies the time (in hundredths of a second) since the last reinitialization of the network management part of the system.
MSG	
MESSAGE	Message as ASCII string (English)

Note

Additional information

You can find additional information on the structure of Syslog messages and the meaning of the parameters in the RFCs:

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

B.2 Variables in Syslog messages

The variables are displayed in the "Syslog messages" section in the "Message text" field with curly brackets {variable}.

The output messages can contain the following variables:

Table B-2 Possible variables in Syslog messages

Variable	Description	Format	Possible values or example
{Ip address}	IPv4 address to RFC1035	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105
{Protocol}	Protocol used or service that has generated the event.	%s	TCP | WBM | PNIO | PB | OPC | EIP
{User name}	Character string (without spaces) that identifies the authenticated user based on the name.	%s	<name>
{Action user name} or {Destination user name}	Identifies the user based on his/her name This is not the authenticated user.	%s	<First name>.<Name>
{Role}	Symbolic name for the group role.	%s	Administrator | User | OPC UA
{Time second}	Number of seconds	%d	44
{Max sessions}	Maximum number of sessions	%d	10
{Url}	URL of the Web server that was accessed.	%s	/Engineering/Reset2Factory?r=0.6856445562508033
{Config detail}	Character string (with spaces) for the configuration.	%s	Power

B.3 List of Syslog messages

Message text	{protocol}: User {user name} logged in from {ip address}.
Example	WBM: User admin logged in from 192.168.0.1.
Explanation	Valid logon information that is provided during logon.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {user name} failed to log in from {ip address}.
Example	WBM: User admin failed to log in from 192.168.0.1.
Explanation	Incorrect user name or incorrect password specified during logon.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {user name} logged out from {ip address}.
Example	WBM: User admin logged out from 192.168.0.1.
Explanation	User session completed - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: Default user {user name} logged in from {ip address}.
Example	PNIO: Default user admin logged in from 192.168.0.1.
Explanation	Default user is logged on via the IP address.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

Message text	Authentication was enabled.
Example	Authentication was enabled.
Explanation	Authentication was enabled.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	Authentication was disabled.
Example	Authentication was disabled.
Explanation	Authentication was disabled.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} has changed the password.
Example	WBM: User admin has changed the password.
Explanation	User has changed the password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} has changed the password of user {Destination user name}.
Example	WBM: User admin has changed the password of user user1.
Explanation	User has changed the password of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} created user-account {Destination user name} with role {Role}.
Example	WBM: User admin created user-account admin2 with role Administrator.
Explanation	The administrator has created an account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} deleted user-account {Destination user name}.
Example	WBM: User admin deleted user-account admin2.
Explanation	The administrator has deleted an existing account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User}: Access to url {url} denied.
Example	WBM: User admin: Access to url /Engineering/Reset2Factory?r=0.6856445562508033 denied.
Explanation	Access to Web resource was denied.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Message text	• Brute force protection activated. • Brute force protection deactivated.
Example	Brute force protection activated.
Explanation	With too many failed logon attempts, the corresponding user account is locked for a specific time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Message text	{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.
Example	WBM: The session of user admin was closed after 310 seconds of inactivity.
Explanation	The current session was locked due to inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Example	WBM: The maximum number of 10 concurrent login sessions exceeded.
Explanation	The maximum number of simultaneous sessions has been exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Message text	{Protocol}: User {User name} has changed configuration.
Example	OPC: User unknown has changed configuration.
Explanation	User has changed the entire configuration. User could not be found. The "unknown" user is always output.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	{Protocol}: User {User name} has changed {Config detail} configuration.
Example	OPC: User admin has changed Power configuration.
Explanation	User has changed specific configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	{Protocol}: User {User name} has initiated a reset to factory defaults.
Example	WBM: User admin has initiated a reset to factory defaults.
Explanation	User has initiated a reset to factory settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	Configuration integrity verification failed.
Example	Configuration integrity verification failed.
Explanation	Configuration integrity verification failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Message text	{Protocol}: Session ID verification failed.
Example	WBM: Session ID verification failed.

Explanation	Session ID is invalid.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

Message text	{Protocol}: Firmware {Version} was activated.
Example	WBM: Firmware V2 was activated.
Explanation	Firmware successfully activated.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{Protocol}: Firmware activation failed.
Example	WBM: Firmware activation failed.
Explanation	Firmware activation failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Service & Support

C

Industry Online Support

In addition to the product documentation, you are supported by the comprehensive online information platform of Siemens Industry Online Support at the following Internet address:
Link: (https://support.industry.siemens.com/cs/de/en/)

Apart from news, you will also find the following there:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option to submit a support request:
  Link: (https://support.industry.siemens.com/My/ww/en/requests)
- 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 data on the Internet at the following address:
Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

"Industrial Identification" homepage

You can find the latest general information about our identification systems on the Internet at our Homepage (www.siemens.com/ident).

Online catalog and ordering system

The online catalog and the online ordering system can also be found on the Industry Mall home page (https://mall.industry.siemens.com).

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:

Link: (https://new.siemens.com/global/en/products/services/industry/sitrain.html)