

SIMATIC NET

Industrial Ethernet Security SCALANCE S615 Web Based Management

Configuration Manual

Preface

Security recommendation

1

Description

2

Technical basics

3

Configuring with Web
Based Management

4

Upkeep and maintenance

5


Appendix A


A


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.

Preface

Scope of the manual

This Configuration Manual covers the following product:

- SCALANCE S615

This Configuration Manual applies to the following software version:

- SCALANCE S615 firmware as of version V6.4

Purpose of the Configuration Manual

This Configuration Manual is intended to provide you with the information you require to install, commission and operate the device. It provides you with the information you require to configure the devices.

New in this edition

- Scheduled restart: Apply configurations from the selected backup prior to restart
- Advanced SNMP configuration
- IPv6 support:
 - LAN interface: SCALANCE M-800/S615
- Configurable password policies
- Dynamic firewall: Time triggered and login to RADIUS server
- Brute Force Prevention: Limit failed login attempts

Orientation in the documentation

Apart from the Configuration Manual you are currently reading, the following documentation is also available on the topic of remote network:

- Configuration Manual: SCALANCE S615 Command Line Interface
This document contains the CLI commands supported by SCALANCE S615 devices.
- Getting Started
Based on examples, this document explains the configuration of the SCALANCE M800/S 615 device.
- Operating Instructions SCALANCE S615
You will find this document on the Internet pages of Siemens Industry Online Support. It contains information on installation, connecting up and approvals of the SCALANCE S615.

- Operating Instructions SINEMA RC Server
You will find this document on the Internet pages of Siemens Industry Online Support. It contains information on the installation, configuration and operation of the application SINEMA Remote Connect Server.
- IP-based remote networks
In this document, the possible configurations of an IP-based remote network are explained in an overview with the requirements and a link to detailed configuration instructions. You will find this document on the Internet under the following entry ID: 26662448 (<https://support.industry.siemens.com/cs/ww/en/view/26662448>)
- Introduction to Industrial Remote Communication
In this entry, you can find an overview - arranged by topic - with links to the most important entries on Industrial Remote Communication in the Siemens Industry Online Support. You can find this entry under the following entry ID: 64721753 (<https://support.industry.siemens.com/cs/ww/en/view/64721753>)

SIMATIC NET manuals

You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

- Using the search function:
Link to Siemens Industry Online Support (<http://support.automation.siemens.com/WW/view/en>)
Enter the entry ID of the relevant manual as the search term.
- In the navigation panel on the left-hand side in the "Industrial Communication" area:
Link to the "Industrial Communication" area (<http://support.automation.siemens.com/WW/view/en/10805878/130000>)
Go to the required product group and make the following settings:
"Entry list" tab, Entry type "Manual"

You will find the documentation for the SIMATIC NET products relevant here on the data storage medium that ships with some products:

- Product CD / product DVD
- SIMATIC NET Manual Collection

Training, Service & Support

You will find information on Training, Service & Support in the multi--language document "DC_support_99.pdf" on the data medium supplied with the documentation.

SIMATIC NET glossary

Explanations of many of the specialist terms used in this documentation can be found in the SIMATIC NET glossary.

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD
The DVD ships with certain SIMATIC NET products.
- On the Internet under the following address:
50305045 (<https://support.industry.siemens.com/cs/ww/en/view/50305045>)

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> (<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/industrialsecurity> (<https://www.siemens.com/industrialsecurity>).

Decommissioning

Shut down the device properly to prevent unauthorized persons from accessing confidential data in the device memory.

To do this, restore the factory settings on the device.

Also restore the factory settings on the storage medium.

Recycling and disposal



The products are low in pollutants, can be recycled and meet the requirements of the WEEE directive 2012/19/EU for the disposal of electrical and electronic equipment.

Do not dispose of the products at public disposal sites.

For environmentally friendly recycling and the disposal of your old device contact a certified disposal company for electronic scrap or your Siemens contact (Product return (<https://support.industry.siemens.com/cs/ww/en/view/109479891>)).

Note the different national regulations.

Device defective

If a fault develops, send the device to your SIEMENS representative for repair. Repairs on-site are not possible.

Firmware

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

License conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product.

You will find license conditions in the following documents on the supplied data medium:

- OSS_Scalance-M-800-S615_86.pdf

Trademarks

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

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

Table of contents

| | | |
|----------|---|-----------|
| | Preface | 3 |
| 1 | Security recommendation | 13 |
| 2 | Description..... | 19 |
| 2.1 | Function | 19 |
| 2.2 | Configuration examples | 20 |
| 2.2.1 | TeleControl with SINEMA RC..... | 20 |
| 2.2.2 | Secure access with S615 | 22 |
| 2.3 | Requirements for operation..... | 22 |
| 2.3.1 | Use in a PROFINET environment | 23 |
| 2.3.2 | TIA Portal Cloud Connector | 24 |
| 2.4 | System functions | 24 |
| 2.5 | Configuration limits for WBM and CLI..... | 26 |
| 2.6 | Configuration limits for SINEMA RC..... | 27 |
| 2.7 | PLUG | 28 |
| 2.7.1 | C-PLUG and KEY-PLUG | 28 |
| 2.7.2 | PRESET PLUG..... | 30 |
| 3 | Technical basics | 31 |
| 3.1 | IP addresses | 31 |
| 3.1.1 | IPv4 / IPv6 | 31 |
| 3.1.2 | IPv4 address..... | 32 |
| 3.1.2.1 | Structure of an IPv4 address | 32 |
| 3.1.2.2 | Initial assignment of an IPv4 address | 34 |
| 3.1.2.3 | Address assignment via DHCPv4..... | 34 |
| 3.1.2.4 | Address assignment with SINEC PNI..... | 35 |
| 3.1.2.5 | Address assignment with STEP 7 | 35 |
| 3.1.3 | IPv6 address..... | 36 |
| 3.1.3.1 | IPv6 terms | 36 |
| 3.1.3.2 | Structure of an IPv6 address | 37 |
| 3.2 | ICMP..... | 38 |
| 3.3 | VLAN | 40 |
| 3.3.1 | VLAN | 40 |
| 3.3.2 | VLAN tagging | 41 |
| 3.4 | SNMP | 43 |
| 3.5 | Security functions | 45 |
| 3.5.1 | User management | 45 |
| 3.5.2 | Firewall..... | 47 |
| 3.5.2.1 | Firewall..... | 47 |
| 3.5.3 | NAT | 51 |
| 3.5.4 | NAT and firewall..... | 52 |

| | | |
|----------|---|-----------|
| 3.5.5 | Certificates..... | 54 |
| 3.5.6 | VPN | 54 |
| 3.5.6.1 | IPsec VPN..... | 54 |
| 3.5.6.2 | OpenVPN..... | 58 |
| 3.5.6.3 | VPN connection establishment..... | 59 |
| 3.6 | Redundancy..... | 63 |
| 3.6.1 | Spanning Tree..... | 63 |
| 3.6.1.1 | RSTP | 64 |
| 3.6.2 | VRRPv3 | 64 |
| 4 | Configuring with Web Based Management..... | 67 |
| 4.1 | Web Based Management..... | 67 |
| 4.2 | Starting and logging in | 68 |
| 4.3 | "Wizard" menu | 72 |
| 4.3.1 | Basic Wizard..... | 72 |
| 4.3.2 | IP..... | 73 |
| 4.3.3 | Device | 75 |
| 4.3.4 | Time Settings..... | 76 |
| 4.3.5 | DDNS..... | 78 |
| 4.3.6 | SINEMA RC..... | 79 |
| 4.3.7 | Cloud Connector | 82 |
| 4.3.8 | Summary..... | 83 |
| 4.4 | "Information" menu | 85 |
| 4.4.1 | Start Page | 85 |
| 4.4.2 | Versions..... | 91 |
| 4.4.3 | Identification & Maintenance..... | 92 |
| 4.4.4 | ARP / neighbors..... | 93 |
| 4.4.4.1 | ARP-Table | 93 |
| 4.4.4.2 | IPv6 Neighbor Table | 94 |
| 4.4.5 | Log Tables | 95 |
| 4.4.5.1 | Event log | 95 |
| 4.4.5.2 | Security Log..... | 97 |
| 4.4.5.3 | Firewall Log | 99 |
| 4.4.6 | Faults | 100 |
| 4.4.7 | DHCP Server | 101 |
| 4.4.8 | SNMP | 103 |
| 4.4.9 | LLDP | 103 |
| 4.4.10 | IPv4 Routing | 104 |
| 4.4.11 | IPv6 Routing | 105 |
| 4.4.12 | IPsec VPN..... | 106 |
| 4.4.13 | SINEMA RC..... | 107 |
| 4.4.14 | OpenVPN client..... | 109 |
| 4.4.15 | Redundancy..... | 110 |
| 4.4.15.1 | Overview | 110 |
| 4.4.15.2 | Spanning Tree..... | 112 |
| 4.4.16 | VRRPv3 Statistics..... | 115 |
| 4.4.17 | Security | 117 |
| 4.4.17.1 | Overview | 117 |
| 4.4.17.2 | Supported Function Rights | 120 |
| 4.4.17.3 | Roles | 121 |

| | | |
|----------|------------------------------------|-----|
| 4.4.17.4 | Groups | 121 |
| 4.5 | "System" menu | 122 |
| 4.5.1 | Configuration..... | 122 |
| 4.5.2 | General | 129 |
| 4.5.2.1 | Device | 129 |
| 4.5.2.2 | Coordinates | 130 |
| 4.5.3 | Restart..... | 132 |
| 4.5.4 | Load&Save..... | 134 |
| 4.5.4.1 | File list..... | 134 |
| 4.5.4.2 | HTTP | 136 |
| 4.5.4.3 | TFTP | 139 |
| 4.5.4.4 | SFTP | 143 |
| 4.5.4.5 | Passwords..... | 147 |
| 4.5.5 | Events | 148 |
| 4.5.5.1 | Event Configuration | 148 |
| 4.5.5.2 | Severity Filters | 152 |
| 4.5.6 | SMTP client..... | 153 |
| 4.5.6.1 | General | 153 |
| 4.5.6.2 | Recipient | 156 |
| 4.5.7 | SNMP | 157 |
| 4.5.7.1 | General | 157 |
| 4.5.7.2 | SNMPv3 Users..... | 160 |
| 4.5.7.3 | SNMPv3 User to Group mapping | 162 |
| 4.5.7.4 | SNMPv3 Access..... | 163 |
| 4.5.7.5 | SNMPv3 Views | 165 |
| 4.5.7.6 | Notifications | 167 |
| 4.5.8 | System Time | 169 |
| 4.5.8.1 | Manual Setting | 169 |
| 4.5.8.2 | DST Overview | 171 |
| 4.5.8.3 | DST Configuration | 173 |
| 4.5.8.4 | SNTP Client..... | 176 |
| 4.5.8.5 | NTP Client..... | 179 |
| 4.5.8.6 | SIMATIC Time Client | 183 |
| 4.5.8.7 | NTP Server | 184 |
| 4.5.9 | Auto Logout..... | 186 |
| 4.5.10 | Button | 187 |
| 4.5.11 | Syslog Client..... | 188 |
| 4.5.12 | Fault Monitoring | 190 |
| 4.5.12.1 | Link Change..... | 190 |
| 4.5.13 | PLUG | 192 |
| 4.5.13.1 | Configuration..... | 192 |
| 4.5.13.2 | License | 195 |
| 4.5.14 | Ping..... | 197 |
| 4.5.15 | DCP Discovery..... | 198 |
| 4.5.16 | DNS..... | 200 |
| 4.5.16.1 | DNS Client | 200 |
| 4.5.16.2 | DNS Proxy..... | 201 |
| 4.5.16.3 | DDNS Client..... | 202 |
| 4.5.16.4 | DNS record | 203 |
| 4.5.17 | DHCP..... | 204 |
| 4.5.17.1 | DHCP Client | 204 |
| 4.5.17.2 | DHCP Server | 206 |

| | | |
|----------|-----------------------------|-----|
| 4.5.17.3 | DHCP Options | 208 |
| 4.5.17.4 | Static Leases | 211 |
| 4.5.18 | cRSP / SRS | 213 |
| 4.5.19 | Proxy Server..... | 214 |
| 4.5.20 | SINEMA RC..... | 215 |
| 4.5.21 | Cloud Connector | 219 |
| 4.5.22 | Configuration Backup..... | 220 |
| 4.5.23 | Connection Check..... | 222 |
| 4.5.23.1 | Connection Fallback..... | 224 |
| 4.6 | "Interfaces" menu | 225 |
| 4.6.1 | Ethernet | 225 |
| 4.6.1.1 | Overview | 225 |
| 4.6.1.2 | Configuration..... | 226 |
| 4.6.2 | PPP | 228 |
| 4.6.2.1 | Overview | 228 |
| 4.6.2.2 | Configuration..... | 229 |
| 4.7 | "Layer 2" menu | 231 |
| 4.7.1 | Layer 2 configuration | 231 |
| 4.7.2 | VLAN..... | 232 |
| 4.7.2.1 | General | 232 |
| 4.7.2.2 | Port Based VLAN | 236 |
| 4.7.3 | Dynamic MAC Aging | 238 |
| 4.7.4 | Spanning Tree..... | 239 |
| 4.7.4.1 | General | 239 |
| 4.7.4.2 | ST general | 240 |
| 4.7.4.3 | ST port | 241 |
| 4.7.5 | LLDP..... | 244 |
| 4.8 | Menu "Layer 3 (IPv4)" | 246 |
| 4.8.1 | Static routes..... | 246 |
| 4.8.2 | Subnets | 248 |
| 4.8.2.1 | Overview | 248 |
| 4.8.2.2 | Configuration..... | 251 |
| 4.8.3 | NAT | 252 |
| 4.8.3.1 | NAT General | 252 |
| 4.8.3.2 | Masquerading..... | 253 |
| 4.8.3.3 | NAPT | 253 |
| 4.8.3.4 | Source NAT | 255 |
| 4.8.3.5 | NETMAP | 257 |
| 4.8.4 | VRRPv3 | 260 |
| 4.8.4.1 | Router | 260 |
| 4.8.4.2 | Configuration..... | 262 |
| 4.8.4.3 | Address overview..... | 264 |
| 4.8.4.4 | Address Configuration..... | 265 |
| 4.8.4.5 | Interface Tracking | 266 |
| 4.8.4.6 | Address monitoring..... | 267 |
| 4.9 | Menu "Layer 3 (IPv6)" | 269 |
| 4.9.1 | Subnets | 269 |
| 4.9.2 | NAT | 272 |
| 4.9.2.1 | Masquerading..... | 272 |
| 4.10 | "Security" menu | 273 |

| | | |
|----------|--|------------|
| 4.10.1 | Users | 273 |
| 4.10.1.1 | Local users..... | 273 |
| 4.10.1.2 | Roles | 276 |
| 4.10.1.3 | Groups | 278 |
| 4.10.2 | Passwords..... | 280 |
| 4.10.2.1 | Passwords..... | 280 |
| 4.10.2.2 | Options | 281 |
| 4.10.3 | AAA..... | 282 |
| 4.10.3.1 | General | 282 |
| 4.10.3.2 | RADIUS client..... | 283 |
| 4.10.4 | Certificates..... | 286 |
| 4.10.4.1 | Overview | 286 |
| 4.10.4.2 | Certificates..... | 288 |
| 4.10.5 | Firewall..... | 291 |
| 4.10.5.1 | General | 291 |
| 4.10.5.2 | Predefined | 292 |
| 4.10.5.3 | Dynamic Rules | 294 |
| 4.10.5.4 | IP services..... | 298 |
| 4.10.5.5 | ICMP services..... | 299 |
| 4.10.5.6 | IP protocols..... | 300 |
| 4.10.5.7 | IP rules | 301 |
| 4.10.6 | IPsec VPN..... | 304 |
| 4.10.6.1 | General | 304 |
| 4.10.6.2 | Remote End | 305 |
| 4.10.6.3 | Connections | 307 |
| 4.10.6.4 | Authentication..... | 310 |
| 4.10.6.5 | Phase 1..... | 311 |
| 4.10.6.6 | Phase 2..... | 313 |
| 4.10.7 | OpenVPN client..... | 316 |
| 4.10.7.1 | General | 316 |
| 4.10.7.2 | Connections | 317 |
| 4.10.7.3 | Remote..... | 319 |
| 4.10.7.4 | Authentication..... | 320 |
| 4.10.8 | Brute Force Prevention | 321 |
| 5 | Upkeep and maintenance..... | 325 |
| 5.1 | Device configuration with PRESET-PLUG..... | 325 |
| 5.2 | Firmware update - via WBM..... | 327 |
| 5.3 | Firmware update via WBM and CLI not possible | 328 |
| 5.4 | Restoring the factory settings..... | 330 |
| A | Appendix A | 331 |
| A.1 | Format of the syslog messages..... | 331 |
| A.2 | Parameters in Syslog messages | 332 |
| A.3 | Syslog messages | 333 |
| | Index..... | 343 |

Security recommendation

To prevent unauthorized access, note the following security recommendations.

A checklist supports you in setting up your device. You can find the checklist at the following address: (<https://support.industry.siemens.com/cs/ww/en/view/109745536>)

General

- You should make regular checks to make sure that the device meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products:
Link: (<https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx>)
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network use an encrypted VPN tunnel (IPsec, Open VPN).
- Separate connections correctly (WBM, Telnet, SSH etc.).

Physical / remote access

- Operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Limit physical access to the device exclusively to trusted personnel.
The memory card or the PLUG (C-PLUG, KEY-PLUG, CLP) contains sensitive data such as certificates, keys, etc. that can be read out and modified.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device. For more information, see the configuration manuals, section "Brute Force Prevention".
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communication.
- When you establish a secure connection to a server (for example for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTP, HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning".

Software (security functions)

- Keep the software up to date. Check regularly for security updates of the product. You will find information on this on the Internet pages "Industrial Security (<https://www.siemens.com/industrialsecurity>)".
- Inform yourself regularly about security advisories and bulletins published by Siemens ProductCERT (<https://www.siemens.com/cert/en/cert-security-advisories.htm>).
- Only activate protocols that you really require to use the device.
- Restrict access to the management of the device with firewall rules.
- The option of VLAN structuring provides good protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment. When you adapt the default VLAN configuration, ensure clear VLAN separation.
- Use a central logging server to log changes and accesses. Operate your logging server within the protected network area and check the logging information regularly.
- We recommend formatting a PLUG that is not being used.

Passwords and 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.

- Define rules for the assignment of passwords.
- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Use passwords with a high password strength.
- Regularly change your passwords to increase security.
- Make sure that all passwords are protected and inaccessible to unauthorized persons.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- Do not use the same password for different users and systems.
- Store the passwords at a safe location (not online) to have them available when needed.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.

Keys and certificates

This section deals with the security keys and certificates you require to set up TLS, VPN (IPsec, OpenVPN) and SINEMA RC.

- The device contains a pre-installed X.509 certificate with key. Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed by a reliable external or internal certification authority.
- Use the certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- 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.
- It is recommended that you use password-protected certificates in the PKCS#12 format.
- It is recommended that you use certificates with a key length of at least 2048 bits.
- Change keys and certificates immediately, if there is a suspicion of compromise.

Secure/non-secure protocols

- Avoid or disable non-secure protocols, for example Telnet and TFTP. For historical reasons, these protocols are still available, however not intended for secure applications. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).
- Avoid or disable non-secure protocols. Check whether use of the following protocols is necessary:
 - Telnet
 - HTTP
 - Broadcast pings
 - Non authenticated and unencrypted interfaces
 - ICMP (redirect)
 - LLDP
 - Syslog
 - DHCP Options 66/67
 - SNTP
 - NTP
 - TFTP
 - TIA Portal Cloud Connector

- The following protocols provide secure alternatives:
 - SNMPv1/v2 → SNMPv3
Check whether use of SNMPv1 is necessary. SNMPv1 is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options. If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
 - HTTP → HTTPS
 - Telnet → SSH
 - NTP → Secure NTP
 - SNTP → Secure NTP
 - TFTP → SFTP
 - TIA Portal Cloud Connector using a secure connection.
Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector" to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server").
- Use secure protocols when access to the device is not prevented by physical protection measures.
- To prevent unauthorized access to the device or network, take suitable protective measures against non-secure protocols.
- If you require non-secure protocols and services, activate these at interfaces that are located within a protected network area.
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- For the DCP function, enable the "DCP read-only" mode after commissioning.

List of available protocols

The following is a list of all available services and their ports through which the device can be accessed.

The table includes the following columns:

- **Service**
The services that the device supports.
- **Protocol/port number**
Port number assigned to the protocol
- **Default port status**
The port status on delivery (factory setting) distinguishes between local and external access.
 - Local access: The port is accessed via a local connection (vlan1).
 - External access: The port is accessed via an external connection (vlan2).
- **Configurable port/service**
Indicates whether the port number or the service can be configured via WBM / CLI.

- **Authentication**
Specifies whether the communication partner is authenticated.
If optional, the authentication can be configured as required.
- **Encryption**
Specifies whether the transfer is encrypted.
If optional, the encryption can be configured as required.

| Layer3 services | Protocol/ Port number | Default port status | | Configurable | | Authenti- cation | Encryp- tion |
|-----------------------------------|--------------------------|----------------------|-------------------------------|--------------|---------|---------------------|-----------------|
| | | Local access | External access ¹⁾ | Port | Service | | |
| DHCPv4 client | UDP/68 | Closed ²⁾ | Closed | -- | ✓ | -- | -- |
| DHCPv6 client | UDP/546 | Open | Open | -- | -- | -- | -- |
| DHCPv4 server | UDP/67 | Closed | Closed | -- | ✓ | -- | -- |
| DNS client | TCP/53 UDP/53 | Outgoing only | Outgoing only | -- | ✓ | -- | -- |
| DNS server | TCP/53 UDP/53 | Open ⁴⁾ | Closed | -- | ✓ | -- | -- |
| DynDNS | TCP/80 | Outgoing only | Outgoing only | -- | ✓ | ✓ | -- |
| HTTP | TCP/80 | Open | Closed | ✓ | ✓ | ✓ | -- |
| HTTP Proxy | TCP/80 TCP/443 | Outgoing only | Outgoing only | ✓ | ✓ | Optional | -- |
| HTTPS | TCP/443 | Open | Closed | ✓ | ✓ | ✓ | ✓ |
| IPsec/IKE | UDP/500 UDP/4500 | Closed | Closed | -- | ✓ | ✓ | ✓ |
| NTP client | UDP/123 | Outgoing only | Outgoing only | ✓ | ✓ | -- | -- |
| NTP client | UDP/123 | Outgoing only | Outgoing only | ✓ | ✓ | ✓ | -- |
| NTP server | UDP/123 | Closed | Closed | ✓ | ✓ | -- | -- |
| NTP server (secure) | UDP/123 | Closed | Closed | ✓ | ✓ | ✓ | -- |
| OpenVPN | UDP/1194 TCP/1194 | Outgoing only | Outgoing only | ✓ | ✓ | ✓ | ✓ |
| Ping | ICMP | Open | Closed | -- | ✓ | ✓ | -- |
| PROFINET | UDP/34964 | Closed | Closed | -- | -- | -- | -- |
| RADIUS | UDP/1812 UDP/1813 | Closed | Closed | ✓ | ✓ | -- | -- |
| SFTP | TCP/22 | Outgoing only | Outgoing only | ✓ | ✓ | ✓ | ✓ |
| Siemens Remote Service (cRSP/SRS) | TCP/443 | Outgoing only | Outgoing only | -- | ✓ | Optional | ✓ |

| Layer3 services | Protocol/ Port number | Default port status | | Configurable | | Authentification | Encryption |
|--|---|---------------------|-------------------------------|--------------|---------|------------------|------------|
| | | Local access | External access ¹⁾ | Port | Service | | |
| SINEMA RC | HTTPS/443 and TCP/UDP depending on the server configuration | Outgoing only | Outgoing only | ✓ | ✓ | ✓ | ✓ |
| SMTP | TCP/25 | Outgoing only | Outgoing only | ✓ | ✓ | -- | -- |
| SMTP (Secure) | TCP/465 TCP/587 | Outgoing only | Outgoing only | ✓ | ✓ | Optional | ✓ |
| SNMPv1 | UDP/161 | Open | Closed | ✓ | ✓ | -- | -- |
| SNMPv3 | UDP/161 | Open | Closed | ✓ | ✓ | Optional | Optional |
| SNTP | UDP/123 | Closed | Closed | -- | ✓ | -- | -- |
| SSH | TCP/22 | Open | Closed | ✓ | ✓ | ✓ | ✓ |
| Syslog | UDP/514 | Outgoing only | Outgoing only | ✓ | ✓ | -- | -- |
| Syslog over TLS | TCP/6514 | Outgoing only | Outgoing only | ✓ | ✓ | -- | ✓ |
| Telnet | TCP/23 | Closed | Closed | ✓ | ✓ | ✓ | -- |
| TFTP | UDP/69 | Outgoing only | Outgoing only | ✓ | ✓ | -- | -- |
| TIA Portal Cloud Connector ⁵⁾ | TCP/9023 | Closed | Closed | ✓ | ✓ | -- | -- |

- 1) With SCALANCE M826 and M804PB, only access via vlan1 is possible in the delivery state (factory setting).
- 2) Only open with SCALANCE M826
- 3) Only open with SCALANCE S615
- 4) Only closed with SCALANCE S615
- 5) Not available for SCALANCE MUM856-1

| Layer 2 service | Default status | Configurable | | Authentication | Encryption |
|-----------------|------------------------|--------------|---------|----------------|------------|
| | | Port | Service | | |
| DCP | Open (when configured) | -- | ✓ | -- | -- |
| LLDP | Open (when configured) | -- | ✓ | -- | -- |
| SimaticTime | Open (when configured) | -- | ✓ | -- | -- |
| VLAN | Open (when configured) | -- | ✓ | -- | -- |

Description

2.1 Function

Configuration

Configuration of all parameters using the

- Web Based Management (WBM) via HTTP and HTTPS.
- Command Line Interface (CLI) via Telnet and SSH.

Security functions

- Router with NAT function
 - IP masquerading
 - NAT
 - SourceNAT
 - NETMAP
- Password protection
- Firewall function
 - Port forwarding
 - IP firewall with stateful packet inspection (layer 3 and 4)
 - Global and user-defined firewall rules
- VPN functions
To establish a VPN (Virtual Private Network), the following functions are available
 - IPsec VPN
 - OpenVPN client
- SINEMA RC client
- Proxy server
- Siemens Remote Service (SRS)
- Brute Force Prevention

Monitoring / diagnostics / maintenance

- LEDs
Display of operating statuses via the LED display. You will find further information on this in the Operating Instructions of the device.
- Logging
For monitoring have the events logged.
- SNMP
For monitoring and controlling network components such as routers or switches from a central station.

Other functions

- Time-of-day synchronization
 - NTP client and NTP server
 - Secure NTP server
 - SIMATIC Time Client
 - SNTP Client
- DHCP
 - DHCP server (local network)
 - DHCP client
- Virtual networks (VLAN)
To structure Industrial Ethernet networks with a fast growing number of devices, a physical network can be divided into several virtual subnets
- Digital input/digital output
- Dynamic DNS client
- DNS client, DNS proxy and DNS records
- SMTP client
- TIA Portal Cloud Connector

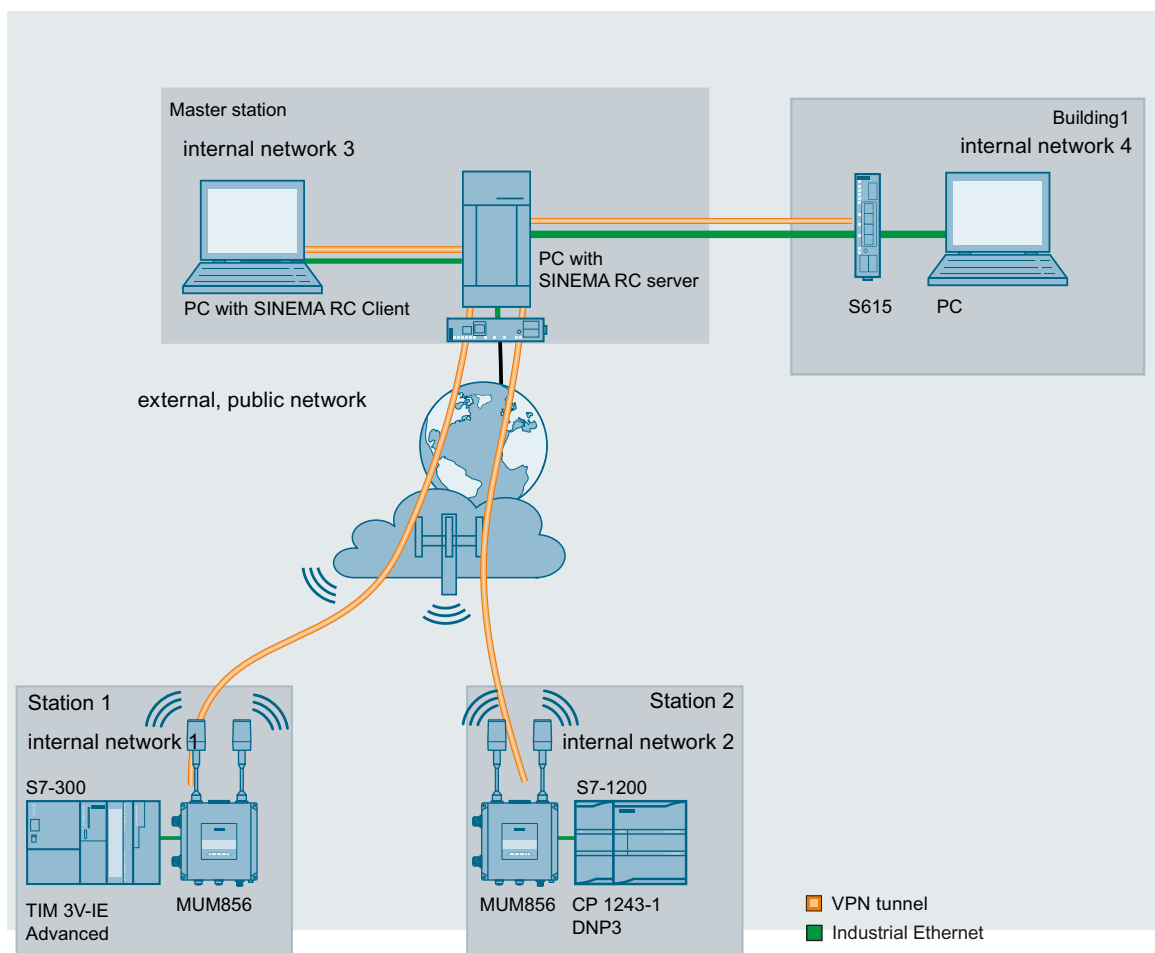
2.2 Configuration examples

2.2.1 TeleControl with SINEMA RC

In this configuration, the remote maintenance master station is connected to the Internet/ intranet via the SINEMA Remote Connect Server. The stations communicate via SCALANCE MUM856 or SCALANCE S615 that establish a VPN tunnel to the SINEMA RC server. In the master station, the SINEMA RC client establishes a VPN tunnel to the SINEMA RC server.

The devices must log on to the SINEMA RC server. The VPN tunnel between the device and the SINEMA RC Server is established only after successful authentication. Depending on the

configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.



Procedure

To be able to access a plant via a remote maintenance master station, follow the steps below:

1. Establish the Ethernet connection between the S615 and the connected Admin PC.
2. Create the devices and node groups on the SINEMA RC Server.
3. Configure the connection to the SINEMA RC server on the device, refer to the section SINEMA RC (Page 215).
4. Set up the connected applications of the plant for data communication.

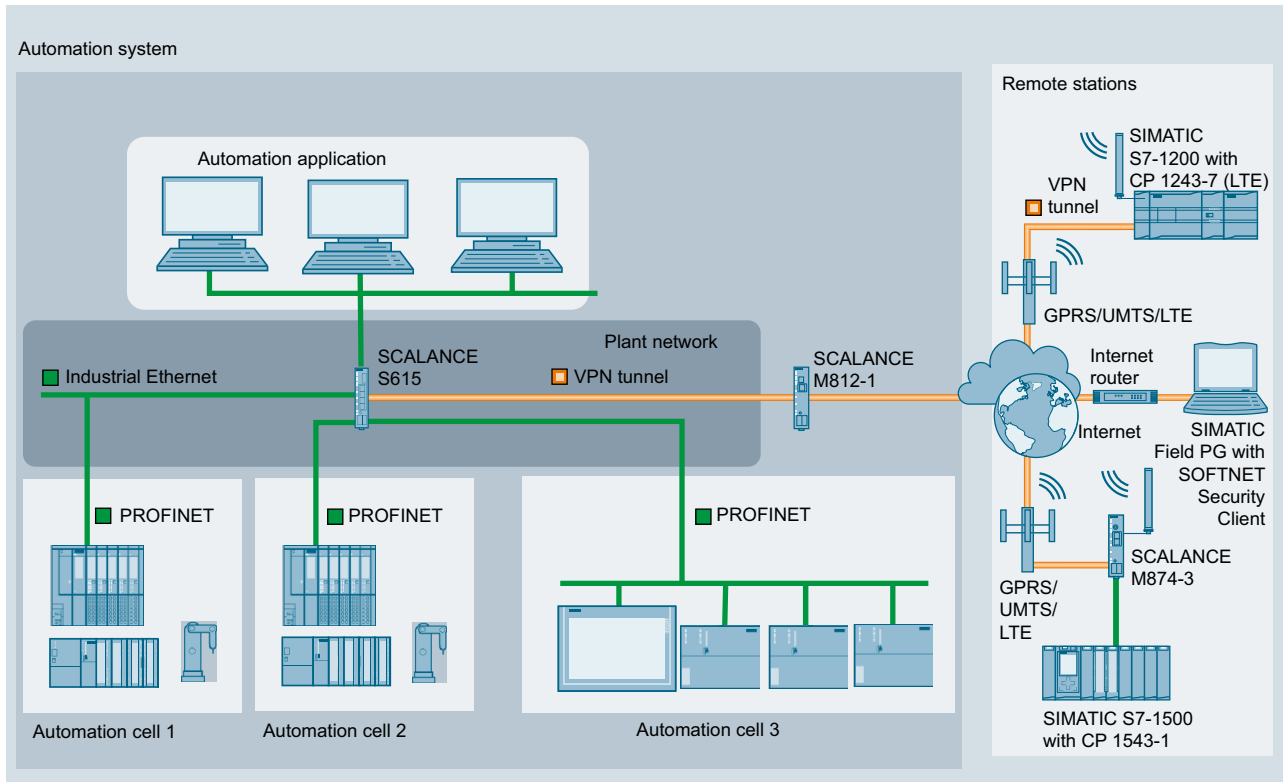
2.2.2 Secure access with S615

Secure remote access and network segmentation with SCALANCE S615

A secure connection for data exchange between an automation plant and remote stations will be established via the Internet and mobile wireless network. At the same time, a secure connection will be established when necessary for service purposes. This connection is, however, restricted to a specific plant section or a specific machine.

In the automation plant, a SCALANCE S615 is connected to the Internet via the ADSL+ router M812-1. The remote stations will be connected to the Internet via the LTE-CP 1243-7 or the HSPA + router SCALANCE M874-3. The devices establish a VPN connection to the SCALANCE S615 via which data can be exchanged securely.

When necessary, the service technician connects to the Internet. With the SOFTNET Security Client, he or she establishes a secure VPN connection to the S615. Various IP subnets are connected to the S615 between which the integrated firewall checks communication. This allows the communication of the service technician to be restricted to a specific IP subnet.



2.3 Requirements for operation

Power supply

A power supply with a voltage between 12 VDC and 24 VDC that can provide sufficient current.

You will find further information on this in the device-specific operating instructions.

Configuration

In the factory settings, the SCALANCE S615 can be reached as follows for initial configuration:

| | Default values set in the factory |
|---|--|
| Ethernet interface for the configuration (internal) | P1 ... P4 (vlan 1) |
| Ethernet interface for the connection to WAN (external) | P5 (vlan 2) |
| IP address | 192.168.1.1 |
| Subnet mask | 255.255.255.0 |
| WBM | Access using HTTPS: TCP port 443 |
| CLI | Access using SSH, TCP port 22 |
| User name | admin The user name can be changed after the first logon or after a "Restore Factory Defaults and Restart". Afterwards, renaming "admin" is no longer possible. |
| Password | admin The password needs to be changed after the first logon or after a "Restore Factory Defaults and Restart" |

You will find more information in "Web Based Management (Page 67)" and in "Starting and logging in (Page 68)".

2.3.1 Use in a PROFINET environment

Note

Validity of CCA declaration

The CCA declaration applies to PROFINET RT without the use in media redundancy structures.

Configuration information

When using the device in a PROFINET environment, follow the following configuration instructions:

- Set the "Aging Time" to 45 seconds.
- Disable Spanning Tree and enable Passive Listening.

2.3.2 TIA Portal Cloud Connector

A communication connection via the TIA Portal Cloud Connector is possible with the following components:

- TIA Portal Cloud Connector V1.1 SP3
You can find the TIA Portal Cloud Connector on the Internet pages of Siemens Industry Online Support under the following entry ID: 109764115 (<https://support.industry.siemens.com/cs/ww/en/view/109764115>)
Install the version even when a TIA Portal Cloud Connector is already installed.
You can find additional information on the TIA Portal Cloud Connector in the documentation "Working with the TIA Portal Cloud Connector (<https://support.industry.siemens.com/cs/ww/en/view/109747305>)" and "SIMATIC Instructions on the TIA Portal Cloud Connector (<https://support.industry.siemens.com/cs/ww/en/view/109742490>)".
- TIA Portal V15 Update 2 or STEP 7 V5.6

Note

- Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
 - Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector") to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server".
-

2.4 System functions

Availability of the system functions

The following table shows the availability of the system functions. Note that all functions are described in this configuration manual and in the online help. Some functions may not be available to you depending on the KEY PLUG.

We reserve the right to make technical changes.

| | | SCALANCE S615 |
|--------------|-------------------------|------------------|
| Basic Wizard | IP settings | ✓ |
| | Device Settings | ✓ |
| | Time settings | - |
| | SINEMA RC ¹⁾ | ✓ |
| | DDNS | ✓ |

| | SCALANCE S615 | |
|--------------------|--|---|
| Information | ARP Table | ✓ |
| | Log Tables | ✓ |
| | Redundancy | ✓ |
| | VRRPv3 | ✓ |
| | SINEMA RC ¹⁾ | ✓ |
| System | SMTP client | ✓ |
| | SNMP | ✓ |
| | Time setting | ✓ |
| | Automatic logout | ✓ |
| | Syslog client | ✓ |
| | Fault Monitoring | ✓ |
| | PLUG | ✓ |
| | SMS | ✓ |
| | DNS | ✓ |
| | DHCP Client | ✓ |
| | DHCP Server | ✓ |
| | cRSP/SRS | ✓ |
| | Proxy Server | ✓ |
| | SINEMA RC ¹⁾ | ✓ |
| | Connection Check | ✓ |
| Interfaces | Ethernet | ✓ |
| | PPP | ✓ |
| Layer 2 | Configuration | ✓ |
| | VLAN | ✓ |
| | Dynamic MAC aging | ✓ |
| | LLDP | ✓ |
| | Spanning Tree | ✓ |
| Layer 3 | Static routes | ✓ |
| | Subnets | ✓ |
| | Spanning Tree | ✓ |
| | NAT | ✓ |
| | VRRPv3 | ✓ |
| Security | Passwords | ✓ |
| | User | ✓ |
| | AAA (Authentication, Authoriza- tion, Accounting) | ✓ |
| | Certificates | ✓ |
| | Firewall | ✓ |
| | IPsec VPN | ✓ |
| | OpenVPN | ✓ |

¹⁾ KEY-PLUG SINEMA Remote Connect 6GK5908-0PB00

2.5 Configuration limits for WBM and CLI

Configuration limits of the device

The following table lists the configuration limits for Web Based Management and the Command Line Interface of the device.

Depending on your device, some functions are not available.

| | Configurable function | Maximum number |
|----------------|--|---|
| System | DNS server | 2 |
| | DNS records | 128 Domain name: Maximum of 256 characters |
| | Syslog server | 3 |
| | SMTP server | 3 |
| | E-mail recipient | 60 20 per SMTP server |
| | SNMPv1 trap recipient | 10 |
| | SMS receiver | 20 |
| | SNTP server | 2 |
| | NTP / NTP (secure) server | 3 One per layer 3 interface |
| | NTP / NTP (secure) client | 1 |
| | DHCP pools | 8 |
| | Static assignments per DHCP pool | 128 |
| | DHCP options (1, 2, 3, 4, 5, 6, 42, 66, 67) | 9 |
| | SINEMA RC | 1 |
| | Proxy server | 5 |
| Layer 2 | Virtual LANs (port-based; including VLAN 1) | 16 |
| | Maximum frame size | 2048 bytes |
| Layer 3 | IP interfaces | 12 |
| | Static routes | 100 |
| | NETMAP | 256 |
| | SourceNAT | 32 |
| | NAPT | 32 |
| | VRRPv3 | VRRPv3 instances (VRID): 2 Assigned IP addresses: 1 per VRID |

| | Configurable function | Maximum number |
|----------|-----------------------|--|
| Security | Users | 30 (incl. user preset in the factory "admin") |
| | Groups | 32 |
| | Roles | 32 (incl. the predefined roles) |
| | RADIUS server | 4 |
| | Firewall | IP protocols:16 IP services: 32 ICMP services:16 IP rules: 128 Dynamic firewall: <ul style="list-style-type: none"> • Maximum number: 8 rule sets • Parallel user access: 4 • Maximum of 128 IP rules per firewall rule set |
| | IPsec VPN | 20 You can create a maximum of 20 phase 2 connections per phase 1 (remote endpoint). Only with IKEv2: <ul style="list-style-type: none"> • Multiple subnets per phase 2 connection; maximum 5 |
| | OpenVPN | Connections: 5 Remote end points: 25 |

2.6 Configuration limits for SINEMA RC

Maximum overall data transfer for all devices: 800 Mbps

Maximum number of devices and users connected simultaneously: **1024** devices with 1 subnet each

User/device combinations can be freely selected up to the maximum overall quantity structure.

As the number of subnets is also dependent on the communication relationships permitted among one another, for example, these must be checked/questioned and restricted, where necessary. If devices do not need to communicate with one another, this function should be disabled to ensure optimum device behavior.

If the devices are to communicate with each other, the maximum number of devices and users connected simultaneously is: **200** devices with 8 subnets each communicating with each other

2.7 PLUG

2.7.1 C-PLUG and KEY-PLUG

The PLUG is a removable medium and is used to transfer the configuration of the old device to the new device when a device is replaced.

The following PLUG types are available:

- C-PLUG: The removable data storage medium only saves the configuration data of the device.
- KEY-PLUG: In addition to the configuration data, the removable data storage medium contains a license with which specific functions can be enabled, e.g. SINEMA RC.
- CLP (Configuration License PLUG)
The SCALANCE CLP is a removable data storage medium for the storage and securing of configuration data that can be used in all SCALANCE devices with CLP slot, e.g. SCALANCE M856-1. The SCALANCE CLP is used to transfer the configuration of the old device to the new device when a device is replaced. The CLP is a successor to the previously described PLUGs. The CLP is also referred to as PLUG in the description. The PLUG is available in the following variants:
 - PLUG Configuration
 - PLUG License

How it works

| |
|--|
| NOTICE |
| Do not remove or insert the PLUG during operation. |
| A PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. |
| If a valid PLUG with license was inserted in the device, the device changes to a defined error state following the restart. |

The device supports the following modes of operation:

- **Without PLUG**
The device saves the configuration data in the internal memory. This mode is active when no PLUG is inserted.
- **With PLUG**
If an unwritten PLUG (factory status or deleted with Clean function) is used, the local configuration already existing on the device is automatically stored on the inserted PLUG. If the PLUG contains a license, additional functions are also enabled.
A device with a written and accepted PLUG ("ACCEPTED" status) uses the configuration data of the PLUG automatically when it starts up. Acceptance is possible only when the data was written by a compatible device type.
One exception to this can be the IP configuration if it is set using DHCP and the DHCP server has not been reconfigured accordingly. Reconfiguration is necessary if you use functions based on MAC addresses.
The configuration stored on the PLUG is displayed over the user interfaces.
If changes are made to the configuration, the device stores the configuration directly on the PLUG, if this is in the "ACCEPTED" status. The internal memory is neither read nor written.

Response to errors

Inserting a PLUG that does not contain the configuration of a compatible device type, accidentally removing the PLUG/KEY-PLUG or general malfunctions of the PLUG are signaled by the diagnostics mechanisms of the device (LEDs, Web-Based Management (WBM), SNMP, Command Line Interface (CLI) and PROFINET diagnostics). The user then has the choice of either removing the PLUG again or selecting the option to reformat the PLUG.

| Type | Properties | Article number |
|----------------------------|---|--------------------|
| C-PLUG | Removable data storage medium (32 MB) for the configuration data | 6GK1900-0AB00 |
| | Removable data storage medium (256 MB) for the configuration data | 6GK1900-0AB10 |
| KEY-PLUG SINEMA RC | Removable data storage medium (256 MB) to enable the connection functionality to SINEMA Remote Connect and for storing configuration data | 6GK5908-0PB00 |
| SCALANCE CLP 2GB | Removable data storage medium for easy device replacement if a fault occurs, for storing configuration data, can be used in the following SCALANCE products with CLP slot: SCALANCE MUM856 | 6GK1900-0UB00-0AA0 |
| SCALANCE CLP EEC 2GB | Removable data storage medium with coated PCBs for simple device replacement in the event of a fault and storage of configuration data; can be used in SCALANCE products with CLP slot: SCALANCE MUM856 | 6GK1900-0UQ00-0AA0 |
| SCALANCE CLP 2GB SINEMA RC | Removable data storage medium (2 GB) to enable the connection functionality to SINEMA Remote Connect and for storing configuration data | 6GK5908-0UA00-0AA0 |

2.7.2 PRESET PLUG

PLUG with preset function (PRESET-PLUG)

With PRESET-PLUG it is possible to install the same configuration and the firmware belonging to it on several devices.

Note

Using configurations with DHCP

Create a PRESET-PLUG only from device configurations that use DHCP. Otherwise disruptions will occur in network operation due to multiple identical IP addresses.

You assign fixed IP addresses extra following the basic installation.

In a PLUG that was configured as a PRESET-PLUG, the device configuration, user accounts, certificates and the firmware are stored.

Note

Restore factory defaults and restart with a PRESET PLUG inserted

If you reset a device to the factory defaults, when the device restarts an inserted PRESET PLUG is formatted and the PRESET PLUG functionality is lost. You then need to create a new PRESET PLUG.

We recommend that you remove the PRESET PLUG before you reset the device to the factory settings.

For more detailed information on creating and using a PRESET PLUG refer to the section Device configuration with PRESET-PLUG (Page 325).

Technical basics

3.1 IP addresses

3.1.1 IPv4 / IPv6

What are the essential differences?

| | IPv4 | IPv6 |
|-------------------------------|---|--|
| IP configuration | <ul style="list-style-type: none"> DHCP server Manual | <ul style="list-style-type: none"> Stateless Address Autoconfiguration (SLAAC): Stateless autoconfiguration using NDP (Neighbor Discovery Protocol) <ul style="list-style-type: none"> Creates a link local address for every interface that does not require a router on the link. Checks the uniqueness of the address on the link that requires no router on the link. Specifies whether the global addresses are obtained via a stateless mechanism, a stateful mechanism or via both mechanisms. (Requires a router on the link.) Manual DHCPv6 (stateful) |
| Available IP addresses | 32-bit: 4, 29 * 10 ⁹ addresses | 128-bit: 3, 4 * 10 ³⁸ addresses |
| Address format | Decimal: 192.168.1.1 with port: 192.168.1.1:20 | Hexadecimal: 2a00:ad80::0123 with port: [2a00:ad80::0123]:20 |
| Loopback | 127.0.0.1 | ::1 |
| IP addresses of the interface | 4 IP addresses | Multiple IP addresses <ul style="list-style-type: none"> LLA: A link local address (formed automatically) fe80::/128 per interface ULA: Several unique local unicast addresses per interface GUA: Several global unicast addresses per interface |
| Header | <ul style="list-style-type: none"> Checksum Variable length Fragmentation in the header No security | <ul style="list-style-type: none"> Checking at a higher layer Fixed size Fragmentation in the extension header |
| Fragmentation | Host and router | Only endpoint of the communication |
| Quality of service | Type of Service (ToS) for prioritization | The prioritization is specified in the header field "Traffic Class". |
| Types of frame | Broadcast, multicast, unicast | Multicast, unicast, anycast |

3.1 IP addresses

| | IPv4 | IPv6 |
|--|---|---|
| Identification of DHCP clients/ server | Client ID: <ul style="list-style-type: none"> • MAC address • DHCP client ID • System name • PROFINET station name • IAID and DUID | DUID + IAID(s) = exactly one interface of the host DUID = DHCP unique identifier Unique identifier of server and clients IAID = Identity Association Identifier At least one per interface is generated by the client and remains unchanged when the DHCP client restarts Three methods of obtaining the DUID <ul style="list-style-type: none"> • DUID-LLT • DUID-EN • DUID-LL |
| Resolution of IP addresses in hardware addresses | ARP (Address Resolution Protocol) | NDP (Neighbor Discovery Protocol) |

3.1.2 IPv4 address

3.1.2.1 Structure of an IPv4 address

The IPv4 address consists of 4 decimal numbers separated by a dot. Each decimal number can have a value from 0 to 255.

Example: 192.168.16.2

The IPv4 address is composed of:

- Address of the (sub)network
- The address of the node (generally also called end node, host or network node)

Subnet mask

The subnet mask consists of four decimal numbers with the range from 0 to 255, each number separated by a period; example: 255.255.0.0

The binary representation of the 4 subnet mask decimal numbers must contain a series of consecutive 1s from the left and a series of consecutive 0s from the right.

The "1" values determine the network address within the IPv4 address. The "0" values determine the device address within the IPv4 address.

Example:

Correct values

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

Incorrect value:

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

In the example for the IP address mentioned above, the subnet mask shown here has the following meaning:

The first 2 bytes of the IP address determine the subnet - i.e. 192.168. The last two bytes address the device, i.e. 16.2.

The following applies in general:

- The network address results from the AND combination of IPv4 address and subnet mask.
- The device address results from the AND-NOT combination of IPv4 address and subnet mask.

Classless Inter-Domain Routing (CIDR)

CIDR is a method that groups several IPv4 addresses into an address range by representing an IPv4 address combined with its subnet mask. To do this, a suffix is appended to the IPv4 address that specifies the number of bits of the network mask set to 1. Using the CIDR notation, routing tables can be reduced in size and the available address ranges put to better use.

Example:

IPv4 address 192.168.0.0 with subnet mask 255.255.255.0

The network part of the address covers 3 x 8 bits in binary representation; in other words 24 bits.

This results in the CIDR notation 192.168.0.0/24.

The host part covers 1 x 8 bits in binary notation. This results in an address range of 2 to the power 8, in other words 256 possible addresses.

Masking additional subnets

Using the subnet mask, you can further structure a subnet assigned to one of the address classes A, B or C and form "private" subnets by setting further lower-level digits of the subnet mask to "1". For each bit set to "1", the number of "private" networks doubles and the number of nodes contained in them is halved. Externally, the network still looks like a single network.

Example:

You change the default subnet mask for a subnet of address class B (e.g. IP address 129.80.xxx.xxx) as follows:

| Masks | Decimal | Binary |
|---------------------|---------------|---|
| Default subnet mask | 255.255.0.0 | 11111111.11111111.00000000 .00000000 |
| Subnet mask | 255.255.128.0 | 11111111.11111111.10000000 .00000000 |

Result:

All devices with addresses from 129.80.1.xxx to 129.80.127.xxx are on one IP subnet, all devices with addresses from 129.80.128.xxx to 129.80.255.xxx are on another IP subnet.

Network gateway (router)

The task of the network gateways (routers) is to connect the IP subnets. If an IP datagram is to be sent to another network, it must first be sent to a router. For make this possible, you need to enter the router address for each member of the IP subnet.

The IP address of a device in the subnet and the IP address of the network gateway (router) may only be different at the points where the subnet mask is set to "0".

3.1.2.2 Initial assignment of an IPv4 address

Configuration options

An initial IP address for a SCALANCE W device cannot be assigned using Web Based Management (WBM) or the Command Line Interface (CLI) over Telnet because these configuration tools require that an IP address already exists.

The following options are available to assign an IP address to an unconfigured device currently without an IP address:

- DHCP (default)
- SINEC PNI
- STEP 7
- SINEC NMS

Note

When the product ships and following "Restore Memory Defaults and Restart", DHCP is enabled.

If a DHCP server is available in the local area network, and this responds to the DHCP request of a SCALANCE W device, the IP address, subnet mask and gateway are assigned automatically when the device first starts up. "Restore Factory Defaults and Restart" does not delete an IP address assigned either by DHCP or by the user.

3.1.2.3 Address assignment via DHCPv4

Properties of DHCP

DHCP (Dynamic Host Configuration Protocol) is a method for automatic assignment of IP addresses. It has the following characteristics:

- DHCP can be used both when starting up a device and during ongoing operation.
- The assigned IP address remains valid only for a limited time known as the lease time. When half the period of validity has elapsed, the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

- There is normally no fixed address assignment; in other words, when a client requests an IP address again, it normally receives a different address from the previous address. It is possible to configure the DHCP server so that the DHCP client always receives the same fixed address in response to its request. The parameter with which the DHCP client is identified for the fixed address assignment is set on the DHCP client. The address can be assigned via the MAC address, the DHCP client ID, PROFINET device name or the device name. You configure the parameter in "System > DHCP Client".
- The following DHCP options are supported:
 - DHCP option 3: Assignment of a router address
 - DHCP option 6: Assignment of a DNS server address
 - DHCP option 66: Assignment of a dynamic TFTP server name
 - DHCP option 67: Assignment of a dynamic boot file name

Note

DHCP uses a mechanism with which the IP address is assigned for only a short time (lease time). If the device does not reach the DHCP server with a new request on expiry of the lease time, the assigned IP address, the subnet mask and the gateway continue to be used.

The device therefore remains accessible under the last assigned IP address even without a DHCP server. This is not the standard behavior of office devices but is necessary for problem-free operation of the plant.

3.1.2.4 Address assignment with SINEC PNI

Introduction

The SINEC PNI is capable of assigning such an address to unconfigured devices that do not yet have an IP address.

SINEC PNI

- To be able to assign an IP address to the device with SINEC PNI, it must be possible to reach the device via Ethernet.
- You can find SINEC PNI on the Internet pages of Siemens Industry Online Support at the following Link: (<https://support.industry.siemens.com/cs/ww/enUS/view/109776941>)
- For additional information about assigning the IP address with SINEC PNI, refer to the online help or the "SINEC PNI network management" operating instructions.

3.1.2.5 Address assignment with STEP 7

In STEP 7, you can configure the topology, the device name and the IP address; in other words, an IP address is specified for the MAC address of the device. If you connect the unconfigured device to the controller, the controller assigns the configured device name and the IP address to the device automatically.

STEP 7 V5.x and earlier

For further information on the assignment of the IP address using STEP 7 V5.x and earlier, refer to the documentation "Configuring Hardware and Communication Connections STEP 7", in the section "Steps for Configuring a PROFINET IO System".

STEP 7 as of V13

For additional information on assigning the IP address using STEP 7 as of V13, refer to the online help "Information system", section "Addressing PROFINET devices".

3.1.3 IPv6 address

3.1.3.1 IPv6 terms

Network node

A network node is a device that is connected to one or more networks via one or more interfaces.

Router

A network node that forwards IPv6 packets.

Host

A network node that represents an end point for IPv6 communication relations.

Link

A link is, according to IPv6 terminology, a direct layer 3 connection within an IPv6 network.

Neighbor

Two network nodes are called neighbors when they are located on the same link.

IPv6 interface

Physical or logical interface on which IPv6 is activated.

Path MTU

Maximum permitted packet size on a path from a sender to a recipient.

Path MTU discovery

Mechanism for determining the maximum permitted packet size along the entire path from a sender to a recipient.

LLA

Link local address FE80::/10

As soon as IPv6 is activated on the interface, a link local address is formed automatically. Can only be reached by nodes located on the same link.

ULA

Unique Local Address

Defined in RFC 4193. The IPv6 interface can be reached via this address in the LAN.

GUA

Global unicast address

The IPv6 interface can be reached through this address, for example, via the Internet.

Interface ID

The interface ID is formed with the EUI-64 method or manually.

EUI-64

Extended Unique Identifier (RFC 4291); process for forming the interface ID. In Ethernet, the interface ID is formed from the MAC address of the interface. Divides the MAC address into the manufacturer-specific part (OUI) and the network-specific part (NIC) and inserts FFFE between the two parts.

Example:

MAC address = AA:BB:CC:DD:EE:FF

OUI = AA:BB:CC

NIC = DD:EE:FF

EUI-64 = OUI + FFFE + NIC = AA:BB:CC:FF:FE:DD:EE:FF

Scope

Defines the range of the IPv6 address.

3.1.3.2 Structure of an IPv6 address

IPv6 address format - notation

IPv6 addresses consist of 8 fields each with four-character hexadecimal numbers (128 bits in total). The fields are separated by a colon.

Example:

fd00:0000:0000:ffff:02d1:7d01:0000:8f21

Rules / simplifications:

- If one or more fields have the value 0, a shortened notation is possible.
The address fd00:**0000:0000**:ffff:02d1:7d01:0000:8f21 can also be shortened and written as follows:
fd00::**ffff**:02d1:7d01:0000:8f21
To ensure uniqueness, this shortened form can only be used once within the entire address.
- Leading zeros within a field can be omitted.
The address fd00:0000:0000:ffff:**02d1**:7d01:0000:8f21 can also be shortened and written as follows:
fd00::**ffff:2d1**:7d01:0000:8f21
- Decimal notation with periods
The last 2 fields or 4 bytes can be written in the normal decimal notation with periods.
Example: The IPv6 address fd00::**ffff.125.1.0.1** is equivalent to fd00::**ffff:7d01:1**

Structure of the IPv6 address

The IPv6 protocol distinguishes between three types of address: Unicast, Anycast and Multicast. The following section describes the structure of the global unicast addresses.

| IPv6 prefix | | Suffix |
|--------------------------|---|--|
| Global prefix: n bits | Subnet ID m bits | Interface ID 128 - n - m bits |
| Assigned address range | Description of the location, also subnet prefix or subnet | Unique assignment of the host in the network. The ID is generated from the MAC address. |

The prefix for the link local address is always fe80:0000:0000:0000. The prefix is shortened and noted as follows: fe80::

IPv6 prefix

Specified in: RFC 4291

The IPv6 prefix represents the subnet identifier.

Prefixes and IPv6 addresses are specified in the same way as with the CIDR notation (Classless Inter-Domain Routing) for IPv4.

Design

IPv6 address / prefix length

Example

IPv6 address: 2001:0db8:1234::1111/48

Prefix: 2001:0db8:1234::/48

Interface ID: ::1111

Entry and appearance

The entry of IPv6 addresses is possible in the notations described above. IPv6 addresses are always shown in the hexadecimal notation.

3.2 ICMP

The acronym ICMP stands for Internet Control Message Protocol (RFC792) and is used to exchange error and information messages.

- Error message
Informs the sender of the IP frame that when forwarding the frame an error or a parameter problem occurred.
- Information message
Can contain information about the time measurement, the address mask, the reachability of the destination or for finding the router.

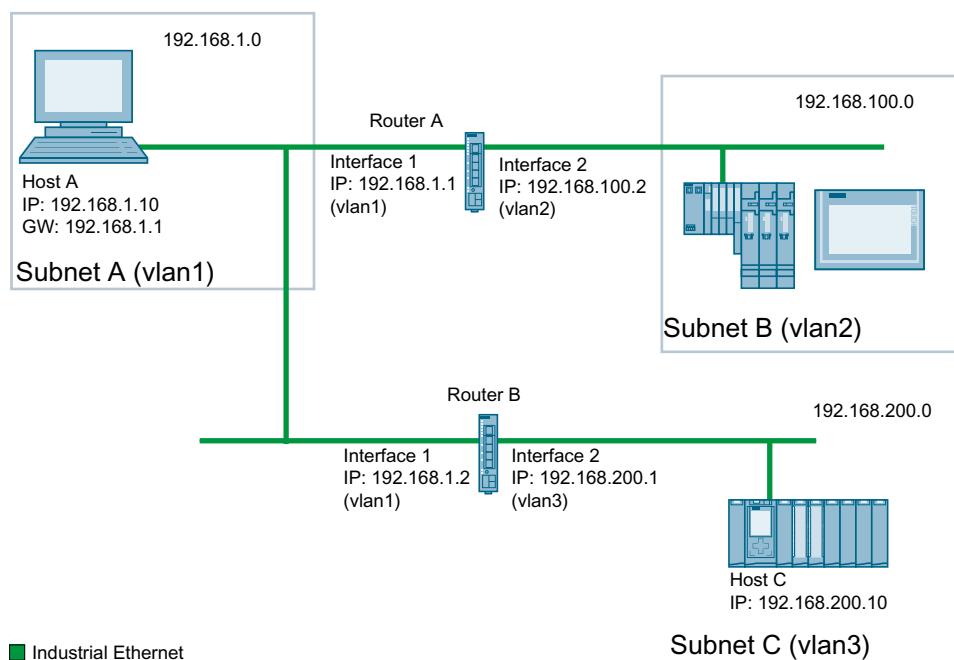
Structure of the ICMP data packet

| 0 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 31 |
|-------------------------------------|---|--|----|----------|----|----|----|----|
| ICMP packet type Type of message | | Code Further details of the message | | Checksum | | | | |
| Data (optional) | | | | | | | | |

- ICMP packet type**
 The most important ICMP packet types are as follows:
 - Redirect
The router informs the host in one of its subnets that there is a better route to the destination. This ICMP packet type is dealt with in more detail in the following description.
 - Destination Unreachable
IP frame cannot be delivered.
 - Time Exceeded
Time limit exceeded
 - Echo-Request
Echo request, better known as ping.
- Code**
 The code describes the ICMP packet type in greater detail. The selection depends on the selected ICMP packet type. With "Destination Unreachable," for example "Code 1" host cannot be reached.

You will find a full list of the ICMP packet types and codes on the website of IANA.

ICMP packet type 5 - Redirect



3.3 VLAN

Host A wants to send an IP frame to host C. Host C is not located in the same subnet as host A. For this reason host A sends the IP frame to its default gateway. The default gateway of host A is interface 1 of router A. Router A cannot forward the IP frame because it does not know the destination network. Via its routing table, however, router A knows that subnet C is reachable via router B. Router B connects subnet A with subnet C. Router A sends a redirect message to host A. In this, router A instructs host A in future to send IP frames to host C via router B whose IP address is contained in the redirect message. The initial IP frame is sent by router A directly to router B that forwards it to Host C.

Conditions for sending redirect messages

- The IP frame is received and sent via the same interface of router A.
- The source IP address (host A) is from the same subnet as the next hop address (router B) in the routing table.
- The IP frame is not affected by a source NAT rule (masquerading, source NAT or NETMAP).
- So that router A forwards the initial IP frame to router B, a firewall rule `vlanX → vlanX` is required.

3.3 VLAN

3.3.1 VLAN

Network definition regardless of the spatial location of the nodes

VLAN (Virtual Local Area Network) divides a physical network into several logical networks that are shielded from each other. Here, devices are grouped together to form logical groups. Only nodes of the same VLAN can address each other. Since multicast and broadcast frames are only forwarded within the particular VLAN, they are also known as broadcast domains.

The particular advantage of VLANs is the reduced network load for the nodes and network segments of other VLANs.

To identify which packet belongs to which VLAN, the frame is expanded by 4 bytes, refer to VLAN tagging (Page 41). This expansion includes not only the VLAN ID but also priority information.

Options for the VLAN assignment

There are various options for the assignment to VLANs:

- Port-based VLAN
Each port of a device is assigned a VLAN ID. You configure port-based VLAN in "Layer 2 > VLAN > Port-based VLAN (Page 236)".
- Protocol-based VLAN
Each port of a device is assigned a protocol group.
- Subnet-based VLAN
The IP address of the device is assigned a VLAN ID.

VLAN assignment on the device

In the factory settings, the following assignments are made on the SCALANCE S615:

| | |
|----------|---|
| P1 to P4 | vlan1 For access from the local network (LAN) to the device |
| P5 | vlan2 For access from the external network (WAN) to the device |

You can change the assignment in "Layer 2 > VLAN > General (Page 232)".

The VLANs are in different IP subnets. To allow these to communicate with each other, the route and firewall rule must be configured on the device.

3.3.2 VLAN tagging

Expansion of the Ethernet frames by four bytes

For CoS (Class of Service, frame priority) and VLAN (virtual network), the IEEE 802.1Q standard defined the expansion of Ethernet frames by adding the VLAN tag.

Note

The VLAN tag increases the permitted total length of the frame from 1518 to 1522 bytes. The end nodes on the networks must be checked to find out whether they can process this length / this frame type. If this is not the case, only frames of the standard length may be sent to these nodes.

The additional 4 bytes are located in the header of the Ethernet frame between the source address and the Ethernet type / length field:

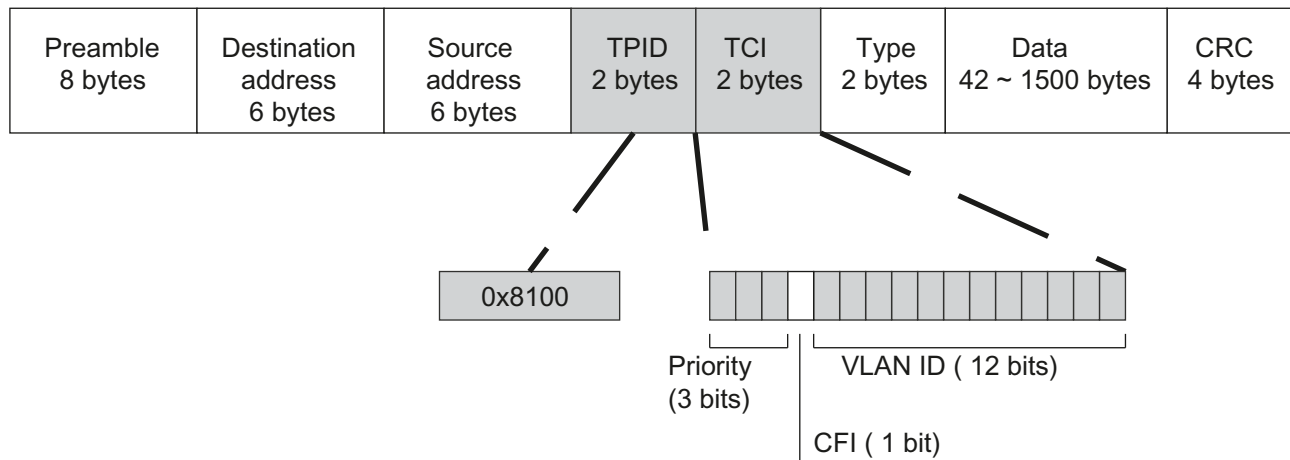


Figure 3-1 Structure of the expanded Ethernet frame

3.3 VLAN

The additional bytes contain the tag protocol identifier (TPID) and the tag control information (TCI).

Tag protocol identifier (TPID)

The first 2 bytes form the Tag Protocol Identifier (TPID) and always have the value 0x8100. This value specifies that the data packet contains VLAN information or priority information.

Tag Control Information (TCI)

The 2 bytes of the Tag Control Information (TCI) contain the following information:

QoS Trust

The tagged frame has 3 bits for the priority that is also known as Class of Service (CoS), see also IEEE 802.1Q.

| CoS bits | Priority | Type of the data traffic |
|----------|-------------|--|
| 000 | 0 (lowest) | Background |
| 001 | 1 | Best Effort |
| 010 | 2 | Excellent Effort |
| 011 | 3 | Critical Applications |
| 100 | 4 | Video, < 100 ms delay (latency and jitter) |
| 101 | 5 | Voice (language), < 10 ms delay (latency and jitter) |
| 110 | 6 | Internetwork Control |
| 111 | 7 (highest) | Network Control |

The prioritization of the data packets is possible only if there is a queue in the components in which they can buffer data packets with lower priority.

The device has multiple parallel queues in which the frames with different priorities can be processed. As default, first, the frames with the highest priority are processed. This method ensures that the frames with the highest priority are sent even if there is heavy data traffic.

Canonical Format Identifier (CFI)

The CFI is required for compatibility between Ethernet and the token Ring. The values have the following meaning:

| Value | Meaning |
|-------|---|
| 0 | The format of the MAC address is canonical. In the canonical representation of the MAC address, the least significant bit is transferred first. Standard-setting for Ethernet switches. |
| 1 | The format of the MAC address is not canonical. |

VLAN ID

In the 12-bit data field, up to 4096 VLAN IDs can be formed. The following conventions apply:

| VLAN ID | Meaning |
|---------|---|
| 0 | The frame contains only priority information (priority tagged frames) and no valid VLAN identifier. |
| 1- 4094 | Valid VLAN identifier, the frame is assigned to a VLAN and can also include priority information. |
| 4095 | Reserved |

3.4 SNMP

Introduction

With the aid of the Simple Network Management Protocol (SNMP), you monitor and control network components from a central station, for example routers or switches. SNMP controls the communication between the monitored devices and the monitoring station.

Tasks of SNMP:

- Monitoring of network components
- Remote control and remote parameter assignment of network components
- Error detection and error notification

In versions v1 and v2c, SNMP has no security mechanisms. Each user in the network can access data and also change parameter assignments using suitable software.

For the simple control of access rights without security aspects, community strings are used.

The community string is transferred along with the query. If the community string is correct, the SNMP agent responds and sends the requested data. If the community string is not correct, the SNMP agent discards the query. Define different community strings for read and write permissions. The community strings are transferred in plain text.

Standard values of the community strings:

- public
has only read permissions
- private
has read and write permissions

Note

Because the SNMP community strings are used for access protection, do not use the standard values "public" or "private". Change these values following the initial commissioning.

Further simple protection mechanisms at the device level:

- Allowed Host
The IP addresses of the monitoring systems are known to the monitored system.
- Read Only
If you assign "Read Only" to a monitored device, monitoring stations can only read out data but cannot modify it.

SNMP data packets are not encrypted and can easily be read by others.

The central station is also known as the management station. An SNMP agent is installed on the devices to be monitored with which the management station exchanges data.

The management station sends data packets of the following type:

- GET
Request for a data record from the SNMP agent
- GETNEXT
Calls up the next data record.
- GETBULK (available as of SNMPv2c)
Requests multiple data records at one time, for example several rows of a table.
- SET
Contains parameter assignment data for the relevant device.

The SNMP agent sends data packets of the following type:

- RESPONSE
The SNMP agent returns the data requested by the manager.
- TRAP
If a certain event occurs, the SNMP agent itself sends traps.

SNMPv1/v2c/v3 use UDP (User Datagram Protocol) and use the UDP ports 161 and 162. The data is described in a Management Information Base (MIB).

SNMPv3

Compared with the previous versions SNMPv1 and SNMPv2c, SNMPv3 introduces an extensive security concept.

SNMPv3 supports:

- Fully encrypted user authentication
- Encryption of the entire data traffic
- Access control of the MIB objects at the user/group level

With the introduction of SNMPv3 you can no longer transfer user configurations to other devices without taking special action, e.g. by loading a configuration file or replacing the C-PLUG.

According to the standard, the SNMPv3 protocol uses a unique SNMP engine ID as an internal identifier for an SNMP agent. This ID must be unique in the network. It is used to authenticate access data of SNMPv3 users and to encrypt it.

Depending on whether you have enabled or disabled the "SNMPv3 User Migration" function, the SNMP engine ID is generated differently.

Restriction when using the function

Use the "SNMPv3 User Migration" function only to transfer configured SNMPv3 users to a substitute device when replacing a device.

Do not use the function to transfer configured SNMPv3 users to multiple devices. If you load a configuration with created SNMPv3 users on several devices, these devices use the same SNMP engine ID. If you use these devices in the same network, your configuration contradicts the SNMP standard.

Compatibility with predecessor products

You can only transfer SNMPv3 users to a different device if you have created the users as migratable users. To create a migratable user the "SNMPv3 User Migration" function must be activated when you create the user.

3.5 Security functions

3.5.1 User management

Overview of user management

Access to the device is managed by configurable user settings. Set up users with a password for authentication. Assign a role with suitable rights to the users.

The authentication of users can either be performed locally by the device or by an external RADIUS server. You configure how the authentication is handled on the "Security > AAA > General" page.

Local logon

The local logging on of users by the device runs as follows:

1. The user logs on with user name and password on the device.
2. The device checks whether an entry exists for the user.
 - If an entry exists, the user is logged in with the rights of the associated role.
 - If no corresponding entry exists, the user is denied access.

Login via an external RADIUS server

RADIUS (Remote Authentication Dial-In User Service) is a protocol for authenticating and authorizing users by servers on which user data can be stored centrally.

Depending on the RADIUS authorization mode you have selected on the "Security > AAA > RADIUS Client" page, the device evaluates different information of the RADIUS server.

RADIUS authorization mode "Standard"

If you have set the authorization mode "conventional", the authentication of users via a RADIUS server runs as follows:

1. The user logs on with user name and password on the device.
2. The device sends an authentication request with the login data to the RADIUS server.
3. The RADIUS server runs a check and signals the result back to the device.
 - The RADIUS server reports a successful authentication and returns the value "Administrative User" to the device for the attribute "Service Type".
→ The user is logged in with administrator rights.
 - The RADIUS server reports a successful authentication and returns a different or even no value to the device for the attribute "Service Type".
→ The user is logged in with read rights.
 - The RADIUS server reports a failed authentication to the device:
→ The user is denied access.

RADIUS authorization mode "SiemensVSA"

Requirement

For the RADIUS authorization mode "Siemens VSA" the following needs to be set on the RADIUS server:

- Manufacturer code: 4196
- Attribute number: 1
- Attribute format: Character string (group name)

Procedure

If you have set the authorization mode "SiemensVSA", the authentication of users via a RADIUS server runs as follows:

1. The user logs on with user name and password on the device.
2. The device sends an authentication request with the login data to the RADIUS server.
3. The RADIUS server runs a check and signals the result back to the device.

Case A: The RADIUS server reports a successful authentication and returns the group assigned to the user to the device.

- The group is known on the device and the user is not entered in the table "External User Accounts"
→ The user is logged in with the rights of the assigned group.
- The group is known on the device and the user is entered in the table "External User Accounts"
→ The user is assigned the role with the higher rights and logged in with these rights.
- The group is not known on the device and the user is entered in the table "External User Accounts"
→ The user is logged in with the rights of the role linked to the user account.
- The group is not known on the device and the user is not entered in the table "External User Accounts"
→ The user is logged in with the rights of the role "Default".

Case B: The RADIUS server reports a successful authentication but does not return a group to the device.

- The user is entered in the table "External User Accounts":
→ The user is logged in with the rights of the linked role "".
- The user is not entered in the table "External User Accounts":
→ The user is logged in with the rights of the role "Default".

Case C: The RADIUS server reports a failed authentication to the device:

- The user is denied access.

3.5.2 Firewall

3.5.2.1 Firewall

The security functions of the device include a stateful inspection firewall. This is a method of packet filtering or packet checking.

The IP packets are checked based on firewall rules in which the following is specified:

- The permitted protocols
- IP addresses and ports of the permitted sources
- IP addresses and ports of the permitted destinations

If an IP packet fits the specified parameters, it is allowed to pass through the firewall. The rules also specify what is done with IP packets that are not allowed to pass through the firewall.

Simple packet filter techniques require two firewall rules per connection.

- One rule for the query direction from the source to the destination.
- A second rule for the response direction from the destination to the source

Stateful Inspection Firewall

You only need to specify one firewall rule for the query direction from the source to the destination. The second rule is added implicitly. The packet filter recognizes when, for example, computer "A" is communicating with computer "B" and only then does it allow replies. A query by computer "B" is therefore not possible without a prior request by computer "A".

You configure the firewall in "Security > Firewall".

Note

IP packets via layer 2 (within the same VLAN)

If the IP packets from the device are sent via a switch port (layer 2), these IP packets are not checked based on firewall rules. The firewall has no effect on packets forwarded at the layer 2 level.

Communication directions

| from | to | Meaning |
|--------|--|---|
| vlan x | vlan x | Access from IP subnet vlan x to IP subnet vlan x. Example: vlan1 (INT) → vlan2 (EXT) Access from the local IP subnet to the external IP subnet. |
| | ppp2 | Access from the IP subnet to the WAN interface of the device. |
| | Device | Access from the IP subnet to the device. |
| | SINEMA RC | Access from the IP subnet to the SINEMA RC connection. |
| | IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name> | Access from the IP subnet to the VPN tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection <Connection Name>. |
| Device | vlan x | Access from the device to the IP subnet. |
| | ppp2 | Access from the device to the WAN interface of the device. |
| | SINEMA RC | Access from the device to the SINEMA RC connection. |
| | IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name> | Access from the device to the tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection (<Connection Name>). |

| from | to | Meaning |
|--|--|---|
| SINEMA RC | vlan x | Access from SINEMA RC connections to the IP subnet. |
| | ppp2 | Access from the IP subnet to the WAN interface of the device. |
| | Device | Access from SINEMA RC connections to the device. |
| | IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name> | Access from the SINEMA RC server to the VPN tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection <Connection Name>. |
| IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name> | vlan x | Access via VPN tunnel partners to the IP subnet. |
| | ppp2 | Access from the IP subnet to the WAN interface of the device. |
| | Device | Access via VPN tunnel partners to the device. |
| | SINEMA RC | Access via VPN tunnel partners to the SINEMA RC connection. |
| ppp0/usb | vlan x | Access from the mobile wireless interface to the IP subnet. |
| | Device | Access from the mobile wireless interface to the device. |
| | SINEMA RC | Access from the mobile wireless interface to the SINEMA RC connection. |
| | IPsec (all) IPsec <Connection Name> OpenVPN (all) OpenVPN <Connection Name> | Access from the mobile wireless interface to the VPN tunnel partners that can be reached via all VPN connections (all) or via a certain VPN connection <Connection Name>. |

Firewall rules are automatically created, predefined or specially configured IP rules for data traffic.

Automatic firewall rules

The "Auto firewall rules" setting is available for the following functions:

- System > SINEMA RC
- Security > IPsec VPN> Phase 2
- Security > OpenVPN Client > Connections

The automatically created firewall rules allow packets in the following direction:

| From | To | SINEMA RC | IPsec VPN | OpenVPN |
|----------|----------|-----------|-----------|---------|
| Internal | External | ✓ | ✓ | ✓ |
| External | Internal | ✓ | ✓ | ✓ |
| Device | External | -- | -- | ✓ |

| From | To | SINEMA RC | IPsec VPN | OpenVPN |
|----------|--------|---|-----------|---------|
| External | Device | Predefined IPv4 rules When the connection is created, the following IPv4 services are enabled: | | |
| | | HTTP HTTPS SSH Ping | Ping | Ping |

Predefined firewall rules

The firewall contains predefined IPv4 rules that enable specific IPv4 services on the device.

Specify the interface via which access takes place under "Security > Firewall > Predefined IPv4".

The following options are available:

- VLANx: VLANs with configured subnet
- WAN interface of the device: pppx, usb0
- VPN connection: SINEMA RC, IPsec and OpenVPN

Factory setting

The firewall is enabled by default. In the delivery state (factory setting), the configuration of the predefined IPv4 rules is as follows:

| Service | Access | |
|-------------------------------------|--|---|
| | Local access (vlan1) to the device ¹⁾ | External access to the device M87x, M81x: ppp0/usb0 S615: vlan2 |
| Cloud Connector | - | - |
| DHCP | ✓ | ✓ (only with S615) |
| DNS | ✓ | -- |
| HTTP | ✓ | -- |
| HTTPS | ✓ | -- |
| IPsec VPN | -- | ✓ |
| Ping | ✓ | -- |
| SMS relay (only with M87x / MUM856) | ✓ | -- |
| SNMP | ✓ | -- |
| SSH | ✓ | -- |
| System Time | -- | -- |
| Telnet | ✓ | -- |
| VRRP | -- | -- |

¹⁾ With SCALANCE M826 and M804PB, only vlan1 is available in the delivery state.

3.5.3 NAT

NAT (Network Address Translation) is a method of translating IP addresses in data packets. With this, two different networks (internal and external) can be connected together.

A distinction is made between source NAT in which the source IP address is translated and destination NAT in which the destination IP address is translated.

You will find information on NAT scenarios that are implemented with the device at the following address: (<https://support.industry.siemens.com/cs/gb/en/view/109744660>)

IP masquerading

IP masquerading is a simplified source NAT. With each outgoing data packet sent via this interface, the source IP address is replaced by the IP address of the interface. The adapted data packet is sent to the destination IP address. For the destination host it appears as if the queries always came from the same sender. The internal nodes cannot be reached directly from the external network. By using NAPT, the services of the internal nodes can be made reachable via the external IP address of the device.

IP masquerading can be used if the internal IP addresses cannot or should not be forwarded externally, for example because the internal network structure should remain hidden.

You configure masquerading in "Layer 3" > "NAT" > "IP Masquerading (Page 253)".

NAPT

NAPT (Network Address and Port Translation) is a form of destination NAT and is often called port forwarding. This allows the services of the internal nodes to be reached from external that are hidden by IP masquerading or source NAT.

Incoming data packets are translated that come from the external network and are intended for an external IP address of the device (destination IP address). The destination IP address is replaced by the IP address of the internal node. In addition to address translation, port translation is also possible.

The options are available for port translation:

| from | to | Response |
|---------------|---------------------|---|
| a single port | the same port | If the ports are the same, the frames will be forwarded without port translation. |
| a single port | a single port | The frames are translated to the port. |
| a port range | a single port | The frames from the port range are translated to the same port (n:1). |
| a port range | the same port range | If the port ranges are the same, the frames will be forwarded without port translation. |

Port forwarding can be used to allow external nodes access to certain services of the internal network e.g. FTP, HTTP.

You configure NAPT in "Layer 3" > "NAT" > "NAPT (Page 253)".

Source NAT

As with masquerading, in source NAT the source address is translated. In addition to this, the outgoing data packets can be restricted. These include limitation to certain IP addresses or IP address ranges and limitation to certain interfaces.

Source NAT can be used if the internal IP addresses cannot or should not be forwarded externally, for example because a private address range such as 192.168.x.x is used.

You configure source NAT in "Layer 3" > "NAT" > "Source NAT (Page 255)".

NETMAP

With NETMAP it is possible to translate complex subnets to a different subnet. In this translation, the subnet part of the IP address is changed and the host part remains. For translation with NETMAP only one rule is required. NETMAP can translate both the source IP address and the destination IP address. To perform the translation with destination NAT and source NAT, numerous rules would be necessary. NETMAP can also be applied to VPN connections.

You configure NETMAP in "Layer 3" > "NAT" > "NETMAP (Page 257)".

3.5.4 NAT and firewall

The firewall and NAT router support the "Stateful Inspection" mechanism. If the IP data traffic from internal to external is enabled, internal nodes can initiate a communications connection into the external network.

The reply frames from the external network can pass through the NAT router and firewall without it being necessary for their addresses to be included extra in the firewall rule and the NAT address translation. Frames that are not a reply to a query from the internal network are discarded without a matching firewall rule.

NAT translation and firewall rules

Example of NAT translations

| NAT rule | | | | | | | |
|--|--------|---------------------|-----------------------|------------------|-----------------------------|-----------------------|---------------------------|
| | Type | Source Interface | Destination Interface | Source IP Subnet | Source IP translated subnet | Destination IP Subnet | Translated destination IP |
| ① | Source | vlan1 (internal) | vlan2 (external) | 192.168.1.0/24 | 10.100.1.0/24 | 10.10.10.0/24 | - |
| <p>The rule applies to packets sent from vlan1 (internal) to vlan2 (external). With the packets that arrive at vlan1 there is a check to establish whether the rule applies.</p> <p>If the source IP address in the subnet of the sender (Source IP subnet) and the destination IP address in the subnet of the recipient (Destination IP subnet), the source IP address is replaced by the suitable IP address from the "Translated source IP subnet". The subnet part of the source IP address is changed and the host part remains unchanged.</p> <p>A packet, for example with the source IP address 192.168.1.102 is changed to 10.100.1.102. For the devices connected to vlan2 it appears as if the packets were sent from the IP subnet 10.100.1.0/24. This allows for example overlaps of IP subnets to be resolved. The rule is only specified for the send direction. The retranslation is performed implicitly. If the rule does not apply, the packets are forwarded without translation.</p> | | | | | | | |

| NAT rule | | | | | | | |
|--|-------------|------------------|-----------------------|------------------|-----------------------------|-----------------------|---------------------------|
| | Type | Source Interface | Destination Interface | Source IP Subnet | Source IP translated subnet | Destination IP Subnet | Translated destination IP |
| ② | Destination | vlan2 (external) | vlan1 (internal) | 10.10.10.0/24 | - | 10.100.1.0/24 | 192.168.1.0/24 |
| <p>The rule applies to packets sent from vlan2 (external) to vlan1 (internal). With the packets that arrive at vlan2 there is a check to establish whether the rule applies.</p> <p>If the source IP address in the subnet of the sender (Source IP subnet) and the destination IP address in the subnet of the recipient (Destination IP subnet), the source IP address is replaced by the suitable IP address from the "Translated destination IP subnet".</p> <p>A packet, for example with the source IP address 10.10.10.102 is changed to 192.168.1.102. The devices connected to vlan1 can communicate with the devices connected to vlan2. This assumes that the corresponding firewall rule is set.</p> <p>The devices connected to vlan2 must address the devices connected to vlan1 with the virtual IP address from the subnet 10.100.1.0.</p> | | | | | | | |

Firewall rules for the NAT rules ① and ②

Example 1:

These IP rules allow the IP data traffic for all devices for the specified direction.

| NAT rule | IP rules | | | | | | Description |
|----------|----------|------------------|------------------|---|---------------------------------------|---------|--|
| | Action | From | To | Source (Range) | Destination (Range) | Service | |
| ① | Accept | vlan1 (internal) | vlan2 (external) | 192.168.1.0/24 (Source IP subnet) | 10.10.10.0/24 (Destination IP subnet) | all | All packets sent from vlan1 (internal) to vlan2 (external) are allowed to pass. This IP packet filter rule applies to the devices connected to vlan1. |
| ② | Accept | vlan2 (external) | vlan1 (internal) | 192.168.1.0/24 (Translated Destination IP Subnet) | 10.100.1.0/24 (Destination IP subnet) | all | All packets sent from vlan2 (external) to vlan1 (internal) are allowed to pass. |

Example 2:

These IP rules restrict the IP data traffic to a specific device.

| NAT rule | IP rules | | | | | | Description |
|----------|----------|------------------|------------------|--|---------------------------------------|---------|---|
| | Action | From | To | Source (Range) | Destination (Range) | Service | |
| ① | Accept | vlan1 (internal) | vlan2 (external) | 192.168.1.20/32 (Source IP subnet) | 10.10.10.0/24 (Destination IP subnet) | all | Only packets sent to vlan2 (external) from the IP address 192.168.1.20 are allowed to pass. |
| ② | Accept | vlan2 (external) | vlan1 (internal) | 192.168.1.20/32 (Translated Destination IP Subnet) | 10.100.1.0/24 (Destination IP subnet) | all | Only packets sent from vlan2 (external) to the IP address 192.168.1.20 are allowed to pass. |

3.5.5 Certificates

Certificate types

The device uses different certificates to authenticate the various nodes.

| Certificate | | Is used in... |
|---------------------|---|----------------------|
| CA certificate | The CA certificate is a certificate issued by a Certificate Authority from which the server, device and partner certificates are derived. To allow a certificate to be derived, the CA certificate has a private key signed by the certificate authority. The key exchange between the device and the VPN gateway of the partner takes place automatically when establishing the connection. No manual exchange of key files is necessary. | IPsec VPN (Page 310) |
| Server certificate | Server certificates are required to establish secure communication (e.g. HTTPS, VPN...) between the device and another network participant. The server certificate is an encrypted SSL certificate. The server certificate is derived from the oldest valid CA, even if this is "out of service". The crucial thing is the validity date of the CA. | SINEMA RC |
| Device certificate | Certificates with the private key (key file) with which the device identifies itself. | IPsec VPN (Page 310) |
| Partner certificate | Certificates with which the VPN gateway of the partner identifies itself with the device. | IPsec VPN (Page 310) |

File types

| File type | Description |
|-----------|--|
| *.crt | File that contains the certificate. |
| *.p12 | In the PKCS12 certificate file, the private key is stored with the corresponding certificate and is password protected. The CA creates a certificate file (PKCS12) for both ends of a VPN connection with the file extension ".p12". This certificate file contains the public and private key of the local station, the signed certificate of the CA and the public key of the CA. |
| *.pem | Certificate and key as Base64-coded ASCII text. |

3.5.6 VPN

The device supports the following VPN systems

- IPsec VPN
- OpenVPN

3.5.6.1 IPsec VPN

You configure the IPsec connections in "Security" > "IPsec VPN (Page 304)".

With IPsec VPN, the frames are transferred in tunnel mode. To allow the device to establish a VPN tunnel, the remote network must have a VPN gateway as the partner.

For the VPN connections, the device distinguishes two modes:

- **Roadwarrior mode**
In this mode either the address of the partner is fixed or an IP range is entered from which the connections are taken. The device learns the reachable remote subnets from the partner.
- **Standard mode**
In this mode the address of the partner or the remote subnet is entered permanently. The device can either establish the connection actively as a VPN client or wait passively for connection establishment by the partner.

The IPsec method

The device uses the IPsec method in the tunnel mode for the VPN tunnel. Here, the frames to be transferred are completely encrypted and provided with a new header before they are sent to the VPN gateway of the partner. The frames received by the partner are decrypted and forwarded to the recipient.

To provide security, the IPsec protocol suite uses various protocols:

- The IP Authentication Header (**AH**) handles the authentication and identification of the source.
- The Encapsulation Security Payload (**ESP**) encrypts the data.
- The Security Association (**SA**) contains the specifications negotiated between the partners, e.g. about the lifetime of the key, the encryption algorithm, the period for new authentication etc.
- Internet Key Exchange (**IKE**) is a key exchange method. The key exchange takes place in two phases:
 - Phase 1
In this phase, no security services such as encryption, authentication and integrity checks are available yet since the required keys and the IPsec SA still need to be created. Phase 1 serves to establish a secure VPN tunnel for phase 2. To achieve this, the communications partners negotiate an ISAKMP Security Association (ISAKMP SA) that defines the required security services (algorithms, authentication methods used). The subsequent messages and phase 2 are therefore secure.
 - Phase 2
Phase 2 serves to negotiate the required IPsec SA. Similar to phase 1, exchanging offers achieves agreement about the authentication methods, the algorithms and the encryption method to protect the IP packets with IPsec AH and IPsec ESP. The exchange of messages is protected by the ISAKMP SA negotiated in phase 1. Due to the ISAKMP SA negotiated in phase 1, the identity of the nodes is known and the method for the integrity check already exists.

Authentication method

- CA certificate, device and partner certificate (digital signatures)
The use of certificates is an asymmetrical cryptographic system in which every node (device) has a pair of keys. Each node has a secret, private key and a public key of the partner. The private key allows the device to authenticate itself and to generate digital signatures.
- Pre-shared key
The use of a pre-shared key is a symmetrical cryptographic system. Each node has only one secret key for decryption and encryption of data packets. The authentication is via a common password.

Local ID and remote ID

The local ID and the remote ID are used by IPsec to uniquely identify the partners (VPN end point) during establishment of a VPN connection.

Encryption methods

The following encryption methods are supported. The selection depends on the phase und the key exchange method (IKE)

| | Phase 1 | | Phase 2 | |
|---------------|---------|-------|---------|-------|
| | IKEv1 | IKEv2 | IKEv1 | IKEv2 |
| 3DES | x | x | x | x |
| AES128 CBC | x | x | x | x |
| AES192 CBC | x | x | x | x |
| AES256 CBC | x | x | x | x |
| AES128 CTR | - | x | x | x |
| AES192 CTR | - | x | x | x |
| AES256 CTR | - | x | x | x |
| AES128 CCM 16 | - | x | x | x |
| AES192 CCM 16 | - | x | x | x |
| AES256 CCM 16 | - | x | x | x |
| AES128 GCM 16 | - | x | x | x |
| AES192 GCM 16 | - | x | x | x |
| AES256 GCM 16 | - | x | x | x |

x: is supported

-: is not supported

Default Ciphers

During connection establishment a preset list can be transferred to the VPN connection partners. The list contains combinations of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of these combinations. The combinations depend on the phase and the key exchange method (IKE).

| Combination | | | Phase 1 | | Phase 2 | |
|---------------|----------------------|----------------|---------|-------|---------|-------|
| Encryption | Authenticat- tion | Key derivation | IKEv1 | IKEv2 | IKEv1 | IKEv2 |
| AES128 | SHA1 | DH Group 14 | x | x | x | x |
| AES256 | SHA512 | DH Group 16 | x | x | x | x |
| AES128 CCM 16 | SHA256 | DH Group 14 | - | x | x | x |
| AES256 CCM 16 | SHA512 | DH Group 16 | - | x | x | x |
| AES128 | SHA1 | none | - | - | x | x |
| AES256 | SHA512 | none | - | - | x | x |
| AES128 CCM 16 | SHA256 | none | - | - | x | x |
| AES256 CCM 16 | SHA512 | none | - | - | x | x |

x: Combination is part of the default cipher

-: Combination is not part of the default cipher

none: For phase 2, no separate keys are exchanged. This means that Perfect Forward Secrecy (PFS) is disabled.

Requirements of the VPN partner

The VPN partner must support IPsec with the following configuration to be able to establish an IPsec connection successfully:

- Authentication with partner certificate, CA certificates or pre-shared key
- IKEv1 or IKEv2
- Support of at least one of the following DH groups: Diffie-Hellman group 1, 2, 5 and 14 - 18
- 3DES or AES encryption
- MD5, SHA1, SHA256, SHA384 or SHA512
- Tunnel mode

If the VPN partner is downstream from a NAT router, the partner must support NAT-T. Or, the NAT router must know the IPsec protocol (IPsec/VPN passthrough).

NAT traversal (NAT-T)

There may be a NAT router between the device and the VPN gateway of the remote network. Not all NAT routers allow IPsec frames to pass through. This means that it may be necessary to encapsulate the IPsec frames in UDP packets to be able to pass through the NAT router.

Dead peer detection

This is only possible when the VPN partner supports DPD. DPD checks whether the connection is still operating problem free or whether there has been an interruption on the line. Without DPD and depending on the configuration, it may be necessary to wait until the SA lifetime has expired or the connection must be reinitiated manually. To check whether the IPsec connection is still problem-free, the device itself sends DPD queries to the VPN partner station. If the VPN partner station does not reply after a certain time has elapsed, the connection to the VPN partner station will be declared invalid. You configure the settings for DPD in phase 1.

3.5.6.2 OpenVPN

With OpenVPN, virtual private networks (VPN) can be established. As an OpenVPN client, the device can establish a VPN connection to a remote network.

You configure the OpenVPN client in "Security" > "OpenVPN Client (Page 316)".

The VPN connection is established via virtual device drivers, the TAP and TUN device. During this, virtual network interfaces are created that act like a physical interface of the device and represent the endpoint of the VPN tunnel.

The device supports the following:

- TUN device: Routing mode
The LAN Interface and the virtual network interface are located in different IP subnets. The virtual tunnel interface is assigned a virtual IP address from a devised subnet by the OpenVPN server. The IP packets (layer 3) are routed between the virtual tunnel interface and the LAN interface.

Authentication

The following options are available for authenticating the OpenVPN client at the OpenVPN server:

- Certificates: CA certificate and device certificate
The use of certificates is an asymmetrical cryptographic system. Each node (device) has a secret, private key and a public key of the partner. The private key allows the device to authenticate itself and to generate digital signatures.
- User name / password
Access is restricted by a user name and a password.
- Certificates and user name / password
If both authentication methods are successful, the VPN connection is established.

Encryption methods

The device also supports the following methods:

- BF CBC
- AES128 CBC
- AES192 CBC

- AES256 CBC
- DES EDE3

3.5.6.3 VPN connection establishment

The device supports the following options for establishing a VPN connection.

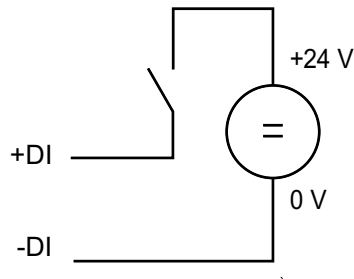
- OpenVPN: Security > OpenVPN > Connections (Page 317)
- IPsec VPN: Security > IPsec VPN > Connections (Page 307)
- SINEMA RC: System > SINEMA RC (Page 215)

| Options | Use | | | Description |
|-------------|---------|-----------|-------------------------|---|
| | OpenVPN | IPsec VPN | SINEMA RC ¹⁾ | |
| start | x | x | - | The device is "active", in other words, it attempts to establish a connection to a partner. The partner is addressed using its configured WAN IP address or the configured FQDN. |
| wait | - | x | - | The device is "passive", in other words, it waits for the partner to initiate the connection. |
| on demand | - | x | - | The device attempts to establish a connection to a partner when necessary. The receipt of requests for VPN connection establishment is also possible. For the configured local and remote subnets, an entry is created in the routing table. If a node attempts to send data packets via the VPN tunnel from one of the networks, the VPN connection is established. The settable timeout has the effect that after this time without any further data packets the VPN tunnel is terminated again. |
| start on DI | x | x | x | Connection establishment is controlled via the digital input (DI). |
| Wait on DI | - | x | - | |
| Auto | - | - | x | The device adopts the settings of the SINEMA RC server. You configure the settings on the SINEMA RC Server in "Remote Connections > Devices". You will find further information on this topic in the operating instructions "SINEMA RC Server". |
| Permanent | - | - | x | The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is established permanently |

¹⁾ For SCALANCE S615: KEY-PLUG SINEMA REMOTE CONNECT required

Digital input (DI)

The establishment of the VPN tunnel can also be controlled via the digital input, e.g. using a button. When the button is closed, voltage is applied to the digital input and the LED of the digital input lights up. The lit LED indicates that signal 1 (TRUE / HIGH) is applied. Signal 1 triggers an event on the device with which the establishment of the VPN tunnel is controlled. You will find information on connecting and the maximum current load in the operating instructions of the devices.



Requirement

- In "System > Events > Configuration" for the "Digital Input" event "VPN Tunnel" is activated. If this setting is not activated, the event is not passed on to the VPN connection.

Options

The device supports the following options for controlling the VPN tunnel via the digital input:

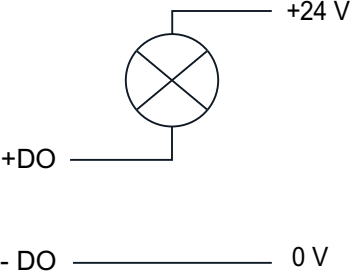
- start on DI
If the event "Digital Input" occurs, the device becomes "active". The device tries to establish a VPN connection to a remote station (OpenVPN, IPsec, SINEMA RC).
- Wait on DI
If the event "Digital Input" occurs, the device becomes "passive". The device waits for the partner to initiate the connection.

Notification options

If the status of the digital input or a VPN tunnel (IPsec, OpenVPN, SINEMA RC) changes, the device provides several options for notification on the "Events (Page 148)" page.

| Type of notification | Digital In | VPN tunnel | Behavior if there is a status change |
|----------------------|------------|------------|---|
| E-mail | x | x | The device sends an e-mail. The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp. Requirement: <ul style="list-style-type: none"> An SMTP server is set up. In "System > SMTP Client" the function is activated, a recipient and the IP address of the SMTP server are configured. |
| Trap | x | x | The device sends an SNMP trap. Requirement: <ul style="list-style-type: none"> "SNMPv1 traps" is enabled in "System > Configuration". In "System > Configuration > Traps" a recipient is configured to which the device sends the SNMP traps. |
| Log table | x | x | The device writes an entry in the event log table. The content of the event log table is displayed in "Information > Log Table". |
| Syslog | x | x | The device writes an entry to the Syslog server. Requirement: <ul style="list-style-type: none"> A Syslog server has been set up. In "System > Syslog Client" the function is activated and the IP address of the Syslog server is configured. |
| Fault LED | x | - | The fault LED lights up on the device. |

3.5 Security functions

| Type of notification | Digital In | VPN tunnel | Behavior if there is a status change |
|---|------------|------------|--|
| Digital Input | x | x | <p>Controls the digital output or signals the status change with the "DO" LED.</p> <p>A consumer can be connected to the digital output. You will find information on connecting in the operating instructions of the devices. The consumer signals a status change.</p>  <p>Note</p> <p>You can control the digital output directly via CLI or SNMP. In the WBM and CLI, you can configure the use of the digital output in "Events". Do not control the digital output directly when you use this in the WBM and CLI.</p> |
| Read out the status of the MIB variable | x | - | <p>Using the private MIB variable snMspDigitalInputLevel, you can read out the status of the digital input.</p> <ul style="list-style-type: none"> • OID of the private MIB variable snMspDigitalInputLevel: <code>iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsp(1).snMspCommon(1).snMspDigitalIO(39).snMspDigitalIOObjects(1).snMspDigitalInputTable(2).snMspDigitalInputEntry(1).snMspDigitalInputLevel(6)</code> • values of the MIB variable <ul style="list-style-type: none"> - 1: Signal 0 at the digital input (DI) - 2: Signal 1 at the digital input (DI) |

3.6 Redundancy

3.6.1 Spanning Tree

Avoiding loops on redundant connections

The spanning tree algorithm allows network structures to be created in which there are several connections between two IE switches / bridges. Spanning tree prevents loops being formed in the network by allowing only one path and disabling the other (redundant) ports for data traffic. If there is an interruption, the data can be sent over an alternative path. The functionality of the spanning tree algorithm is based on the exchange of configuration and topology change frames.

Definition of the network topology using the configuration frames

The devices exchange configuration frames known as BPDUs (Bridge Protocol Data Units) with each other to calculate the topology. The root bridge is selected and the network topology created using these frames. BPDUs also bring about the status change of the root ports.

The root bridge is the bridge that controls the spanning tree algorithm for all involved components.

Once the root bridge has been specified, each device sets a root port. The root port is the port with the lowest path costs to the root bridge.

Response to changes in the network topology

If nodes are added to a network or drop out of the network, this can affect the optimum path selection for data packets. To be able to respond to such changes, the root bridge sends configuration messages at regular intervals. The interval between two configuration messages can be set with the "Hello Time" parameter.

Keeping configuration information up to date

With the "Max Age" parameter, you set the maximum age of configuration information. If a bridge has information that is older than the time set in "Max Age", it discards the message and initiates recalculation of the paths.

New configuration data is not used immediately by a bridge but only after the period specified in the "Forward Delay" parameter. This ensures that operation is only started with the new topology after all the bridges have the required information.

3.6.1.1 RSTP

Rapid Spanning Tree Protocol (RSTP)

One disadvantage of STP is that if there is a disruption or a device fails, the network needs to reconfigure itself: The devices start to negotiate new paths only when the interruption occurs. This can take up to 30 seconds. For this reason, STP was expanded to create the "Rapid Spanning Tree Protocol" (RSTP, IEEE 802.1w). This differs from STP essentially in that the devices are already collecting information about alternative routes during normal operation and do not need to gather this information after a disruption has occurred. This means that the reconfiguration time for an RSTP controlled network can be reduced to a few seconds. This is achieved by using the following functions:

- Edge ports (end node port)
Edge ports are ports connected to an end device.
A port that is defined as an edge port is activated immediately after connection establishment. If a spanning tree BPDU is received at an edge port, the port loses its role as edge port and it takes part in (R)STP again. If no further BPDU is received after a certain time has elapsed (3 x hello time), the port returns to the edge port status.
- Point-to-point (direct communication between two neighboring devices)

By directly linking the devices, a status change (reconfiguration of the ports) can be made without any delays.

- Alternate port (substitute for the root port)

A substitute for the root port is configured. If the connection to the root bridge is lost, the device can establish a connection over the alternate port without any delay due to reconfiguration.

- Reaction to events

Rapid spanning tree reacts to events, for example an aborted connection, without delay. There is no waiting for timers as in spanning tree.

- Counter for the maximum bridge hops
The number of bridge hops a package is allowed to make before it automatically becomes invalid.

In principle, therefore with rapid spanning tree, alternatives for many parameters are preconfigured and certain properties of the network structure taken into account to reduce the reconfiguration time.

3.6.2 VRRPv3

Router redundancy with VRRPv3

With the Virtual Router Redundancy Protocol v3 (VRRPv3), the failure of a router in a network can be countered. Version 3 of VRRP (RFC 5798) is based on version 2 (RFC 5798).

VRRP can only be used with virtual IP interfaces (VLAN interfaces).

Several VRRP routers in a network segment are put together as a logical group representing a virtual router (VR). The group is defined using the virtual ID (VRID). Within the group, the VRID must be the same. The VRID can no longer be used for other groups.

A virtual IP address and a virtual MAC address are assigned to the virtual router. One of the VRRP routers within the group is specified as the master router. The master router has priority 255. The other VRRP routers are backup routers. The master router assigns the virtual IP address and the virtual MAC address to its network interface. The master router sends VRRP packets (advertisements) to the backup routers at specific intervals. With the VRRP packets, the master router signals that it is still functioning. The master router also replies to the ARP queries.

If the virtual master router fails, a backup router takes over the role of the master router. The backup router with the highest priority becomes the master router. If the priority of the backup routers is the same, the higher MAC address decides. The backup router becomes the new virtual master router.

The new virtual master router adopts the virtual MAC and IP address. This means that no routing tables or ARP tables need to be updated. The consequences of a device failure are therefore minimized.

You configure VRRP in "Layer 3 > VRRPv3".

Configuring with Web Based Management

4.1 Web Based Management

How it works

The device has an integrated HTTP server for Web Based Management (WBM). If a device is addressed with a Web browser, it returns HTML pages to the Admin PC depending on the user input.

The user enters the configuration data in the HTML pages sent by the device. The device evaluates this information and generates reply pages dynamically.

Access via HTTPS is enabled in the factory setting. With access via HTTP, the address is automatically redirected to HTTPS.

If you wish to access the WBM via an HTTP connection, you need to select "HTTP & HTTPS" for "HTTP Services" in "System > Configuration".

Requirements

WBM display

- The device has an IP address.
- There is a connection between the device and the Admin PC.
With the Windows ping command, you can check whether or not a connection exists. If the device has the factory settings, refer to "Requirements for operation (Page 22)".
- Access via HTTPS is enabled.
- JavaScript is activated in the Web browser.
- The Web browser must not be set so that it reloads the page from the server each time the page is accessed. The updating of the dynamic content of the page is ensured by other mechanisms.

In Internet Explorer, you can make the appropriate setting in the "Tools > Internet options > General" menu in the section "Browsing history" with the "Settings" button. Under "Check for newer versions of stored pages", select the option "Automatically".

4.2 Starting and logging in

- If a firewall is used, the relevant ports must be opened.
 - For access using HTTPS: TCP port 443
- The display of the WBM was tested with the following desktop Web browsers:
 - Microsoft Internet Explorer 11

Note

Compatibility view

In Microsoft Internet Explorer, disable the compatibility view to ensure correct display and to allow problem-free configuration using WBM.

- Mozilla Firefox ESR 78
- Google Chrome v83
- Microsoft Edge v83

4.2 Starting and logging in

Establishing a connection to a device

Follow the steps below to establish a connection to a device using an Internet browser:

1. There is a connection between the device and the Admin PC. With the ping command, you can check whether or not a device can be reached.
2. In the address box of the Internet browser, enter the IP address or the URL of the device. Access via HTTPS is enabled as default. If you access the device via HTTP, the address is automatically diverted to HTTPS.

Note

Information on the security certificate

Because the device can only be administered using encrypted access, it is delivered with a self-signed certificate. If certificates with signatures that the operating system does not know are used, a security message is displayed. You can display the certificate.

A message relating to the security certificate appears. Acknowledge this message and continue loading the page.

If you use a port other than the standard port, enter a colon ":" as separator between the IP address and the port number.

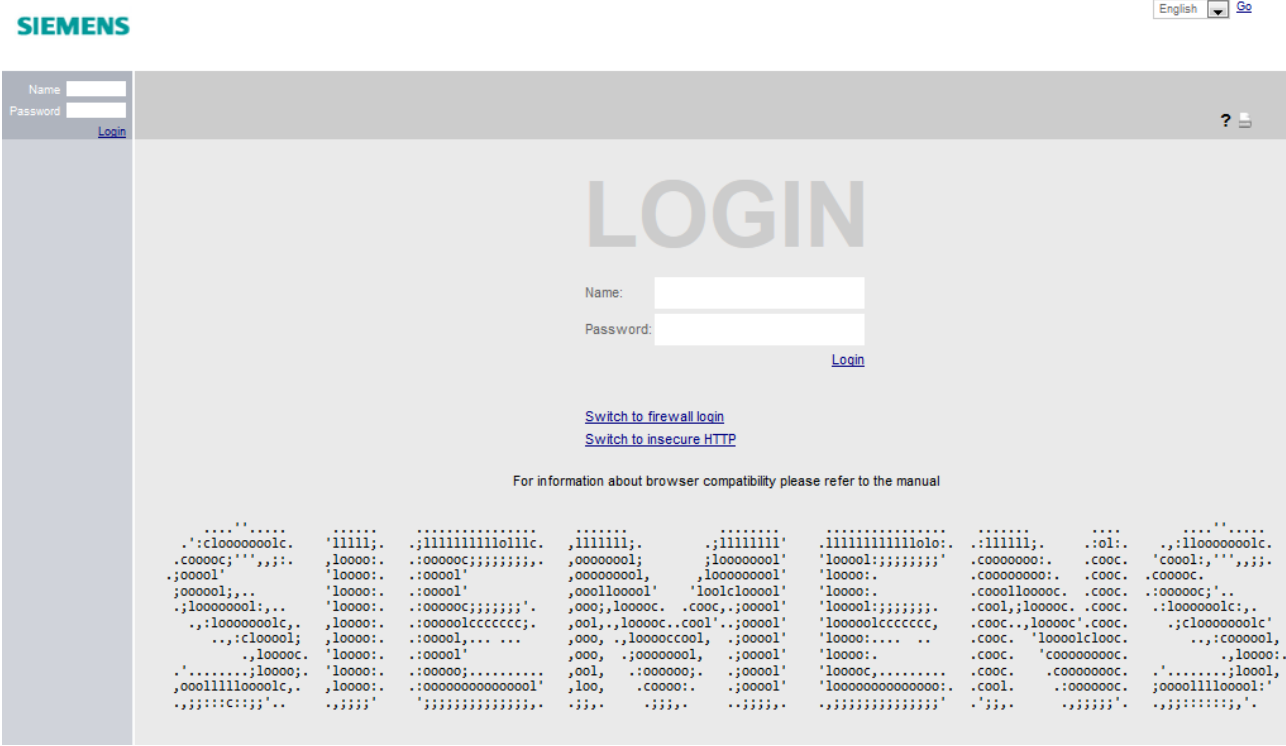
Example: `https://192.168.16.178:49152`

You change the port in "System > Configuration".

3. If there is a connection to the device, the login page of Web Based Management (WBM) is displayed.
If you wish to access the WBM via an HTTP connection, configure "HTTP & HTTPS" for "HTTP Services" in "System > Configuration".

Changing language

1. From the drop-down list at the top right, select the language version of the WBM pages.
2. Click the "Go" button to change to the selected language.



Default Login Page

Under "System > Configuration > Default Login Page", you can define which login page is opened by default.

You can change the type of login via the "Switch to..." links.

To log in, you have the following options:

- Login option in the center of the browser window.
- Login option in the upper left area of the browser window

Personalizing the login page

You can show an additional text on the login page.

1. Create a txt file that contains the desired text or the ASCII type. With ASCII type, pictograms, e.g. the Siemens company logo, are displayed based on the available characters.

Note

The use of the following special characters is not supported:

- Backslash (\)
 - Question mark (?)
 - Tabs: Use spaces instead of tabs
-

2. Load the text file into the device using "System > Load&Save".
3. Log out. The configured text is shown below the login data on the login page.

Logging in to WBM

1. "Name" input box:
 - When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the user preset in the factory "admin".
With this user account, you can change the settings of the device (read and write access to the configuration data).
 - Enter the user name of the created user account. You configure local user accounts and roles in "Security > Users".
2. "Password" input box:
 - When you log in for the first time or following a "Restore Factory Defaults and Restart", enter the password of the default user preset in the factory "admin": "admin".
 - Enter the password of the relevant user account.

3. Click the "Login" button or confirm your input with "Enter".

Note

When you log in for the first time or following a "Restore Factory Defaults and Restart", you can rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible. Enter the new name in the corresponding input box.

When you log in for the first time or following a "Restore Factory Defaults and Restart", you will be prompted to change the password.

The new password must meet the password policy "High":

- Password length: At least 8 characters, maximum 128 characters
- At least 1 uppercase letter
- At least 1 special character (special characters | § ? " ; : ß \ are not allowed)
- At least 1 number

You need to repeat the password as confirmation. The password entries must match.

4. Click the "Set Values" button to complete the action.
The changes take immediate effect. Access via DCP is write-protected after the admin password is changed. The network parameters can be read with SINEC PNI or with "DCP Discovery" but cannot be changed.

Once you have logged in successfully, the start page appears.

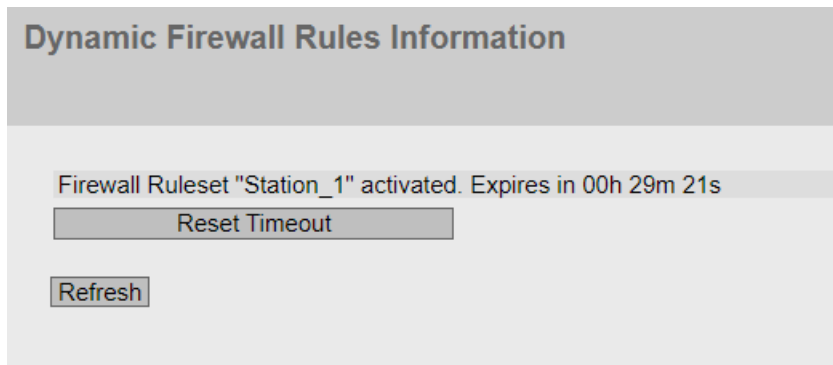
Logging into the dynamic firewall

Requirement

- The user has the right to remote access. You configure the setting "Security > Users > Local users".
- A rule set is assigned to the user.
You can find more information on this in the "Dynamic firewall" Getting Started.

Procedure

1. If the login page is not set by default for the dynamic firewall, click the link "Switch to firewall login".
2. Enter the user name of the created user account. You configure local user accounts and roles in "Security > Users".
3. Enter the password of the relevant user account.
4. Click the "Login" button or confirm your input with "Enter".
If you combine the user account with an event, this condition must also be fulfilled.



After successful login, the WBM page "Information on dynamic firewall rules" opens.

The current ruleset and the remaining time are displayed. If needed, the user can extend the access time via the "Reset Timeout" button.

Service technician login

The device also has a service technician login for servicing purposes. This is only available after activation by an administrator and may only be used by Siemens Support.

4.3 "Wizard" menu

4.3.1 Basic Wizard

Introduction

With the Basic Wizard, menus guide you through the configuration of the most important parameters. On the Basic Wizard pages, you can only configure the parameters important for the basic functionality. You make further settings when you have finished with the Basic Wizard.

Requirement

- The device has an IP address and can be reached via the Ethernet interface.
- You are logged on in the WBM as a user with administrator rights.
- When shipped or following a "Restore Factory Defaults and Restart" the device can be reached with the values preset in the factory. For more detailed information, refer to the section "Requirements for operation (Page 22)".

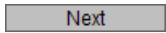

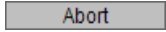

Starting the Basic Wizard

Click on "Wizard > Basic Wizard" in the navigation area to start the Basic Wizard.

If you log in the first time or log on after a "Restore Factory Defaults and Restart", the Basic wizard is started automatically after you have changed the default password.

Buttons you require often

The WBM pages of the Basic Wizard contain the following buttons:

| Button | Description |
|---|---|
|  | Goes to the next page |
|  | Goes back to the previous page |
|  | The Basic Wizard is closed without adopting the settings. |
|  | Saves the configuration and exits the Basic Wizard. |

Navigation within the pages of the Basic Wizard is possible only with the "Previous" and "Next" buttons.

4.3.2 IP

Introduction

One of the basic steps in configuration of a device is setting the IPv4 address. The IP address identifies a device in the network uniquely.

Basic Wizard: IP Settings

| IP | Device | Time | DDNS | SINEMA RC | Summary |
|---|--------|------|------|-----------|---------|
| <p>Enter the IP address and the subnet mask via which the management is accessible. If the device is intended for communication with devices (diagnostics stations, e-mail servers etc.) in another subnet, also enter the IP address of the default gateway.</p> | | | | | |
| <p>Internal (vlan1)</p> <p>IP Address: <input type="text" value="192.168.16.42"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> | | | | | |
| <p>External (vlan2)</p> <p>IP Address: <input type="text" value="192.168.50.1"/></p> <p>Subnet Mask: <input type="text" value="255.255.255.0"/></p> <p><input type="checkbox"/> DHCP</p> <p>Gateway (DHCP): <input type="text" value="-"/></p> | | | | | |
| <p>Create new Gateway</p> <p>IP Address: <input type="text" value="0.0.0.0"/></p> | | | | | |

Description

The Basic Wizard page contains the following boxes:

- **Internal (vlan1)**
In this area make the settings for connection to the LAN.
 - **IP Address**
Enter the IPv4 address of the interface that is unique within your network.
 - **Subnet Mask**
Enter the subnet mask of the subnet you are creating.
- **External (vlan2)**
In this area make the settings for connection to the WAN.
 - **DHCP**
Enable or disable the DHCP client.
When enabled, the required settings such as IP address and subnet mask are assigned to the DHCP client by the DHCP server.
The DHCP client is disabled by default.
 - **IP Address**
Enter the IPv4 address of the interface.
 - **Subnet Mask**
Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.
 - **DHCP (Gateway)**
Shows the IP address of the gateway when the DHCP server has transmitted it.
- **Create new gateway**
You define the gateway in this area.
 - **IP Address**
Enter the IP address of the default gateway to be able to communicate with devices in another subnet.

4.3.3 Device

Introduction

On this Basic Wizard page, you configure the general device information.

Basic Wizard: Device Settings

| | | | | | |
|----|--------|------|------|-----------|---------|
| IP | Device | Time | DDNS | SINEMA RC | Summary |
|----|--------|------|------|-----------|---------|

To allow better identification of the device, you can specify general device information. Here, you can enter any name for this device providing it is unique. Normally, this is the node's fully-qualified domain name. By providing a unique name you can identify the device within the context of the application. You also can enter the contact person responsible for the device and the identifier for the location at which the device is installed, for example the room number.

System Name:

System Location:

System Contact:

Description

The Basic Wizard page contains the following boxes:

- **System Name**
You can enter the name of the device. If you configure this box, this configuration is adopted and displayed in the selection area. A maximum of 255 characters are possible. The system name is also displayed in the CLI input prompt. The number of characters in the CLI input prompt is limited. The system name is truncated after 16 characters.

- **Device Location**
You can enter the location where the device is installed. The location is displayed in the selection area. A maximum of 255 characters are possible.

Note

Permitted characters

The following printable ASCII characters (0x20 to 0x7f) are permitted in the input fields:

- 0123456789
 - A...Z a...z
 - !"#\$\$%&'()*+,-./:;<=>?@ [\]_{}~^`
-

- **System Contact**
You can enter a contact person responsible for managing the device. A maximum of 255 characters are possible.

4.3.4 Time Settings

Time setting

On this Basic Wizard page, you set the date and time of the system.

Basic Wizard: Time Settings

| IP | Device | Time | DDNS | SINEMA RC | Summary |
|----|--------|------|------|-----------|---------|
|----|--------|------|------|-----------|---------|

Here you set the date and time to check the validity (time) of certificates and for the time stamps of log entries. You can set the system time yourself manually or have it synchronized automatically with a time server. There are a number of time servers on the Internet that can be used to obtain the current time precisely. The Basic Wizard is using NTP for the time server. If you want to use another method, configure these method after completing the Basic Wizard.

Time Manually
 System Time:

NTP Client
 Secure NTP Client only
 Time Zone:

| Select | NTP Server Index | NTP Server Address | NTP Server Port | Poll Interval | Key ID | Hash Algorithm | Key | Key Confirmation |
|--------------------------|------------------|--------------------|-----------------|---------------|--------|----------------|-----|------------------|
| <input type="checkbox"/> | 1 | 0.0.0.0 | 123 | 64 | 1 | DES | | |

Description

Manual time setting:

- **Time Manually**
Enable or disable manual setting of the time. If you enable the option, the "System Time" input box can be edited.
- **System Time**
Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
After a restart, the time of day begins at 01/01/2000 00:00:00
- **Use PC Time**
Click the button to use the time setting of the PC.

Automatic time-of-day setting with NTP

- **NTP Client**
Enable or disable time synchronization using NTP.
- **Secure NTP Client only**
When enabled, the device receives the system time from a secure NTP server. The setting applies to all server entries.
To enable the secure NTP client, the parameters for authentication (key ID, hash algorithm, key) must be configured.
- **Time Zone**
In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time. Settings for daylight-saving and standard time are taken into account in this box by specifying the time offset.

In the table, configure the NTP server

- **Select**
Select the row you want to delete.
- **NTP Server Index**
Number corresponding to a specific NTP server entry.
- **NTP Server Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the NTP server.
- **NTP Server Port**
Enter the port of the NTP server.
The following ports are possible:
 - 123 (standard port)
 - 1025 to 36564
- **Poll Interval**
Specify the interval between two-time queries. The greater the interval, the less accurate the time of the device.
Possible values are 64 to 2592000 seconds (30 days).
- **Key ID**
Enter the ID of the authentication key.
- **Hash Algorithm**
Specify the format for the authentication key.
- **Key**
Enter the authentication key. The length depends on the hash algorithm.
The following minimum lengths are recommended for the hash algorithm:
 - MD5: ASCII 16 characters
 - SHA1: ASCII 20 characters
- **Key Confirmation**
Enter the authentication key again to confirm it.

4.3.5 DDNS

On this Basic Wizard page, you configure the dynamic DNS client (DDNS client). The DDNS client synchronizes the assigned IP address with the hostname registered at the DDNS provider. This means that the device can always be reached using the same hostname.

Basic Wizard: DDNS Settings

| IP | Device | Time | DDNS | SINEMA RC | Summary | | | | | | | | | | | | | | | | | | |
|---|--------------------------|------|-----------|-----------|-----------------------|---------|---------|------|-----------|----------|-----------------------|-------|--------------------------|--|--|--|--|--------|--------------------------|--|--|--|--|
| <p>DDNS stands for 'dynamic domain name system'. If you log the device on to a DDNS service, the device can be reached from the external network under a hostname, e.g. 'example.no-ip.com'. Here you enter the hostname that you have agreed with your DDNS provider for the device and the login data (User name, Password) for the DDNS server. To use the required Service, select the check box 'Enabled'.</p> | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="width: 20%;">Service</th> <th style="width: 10%;">Enabled</th> <th style="width: 30%;">Host</th> <th style="width: 20%;">User name</th> <th style="width: 15%;">Password</th> <th style="width: 5%;">Password confirmation</th> </tr> </thead> <tbody> <tr> <td>No-IP</td> <td style="text-align: center;"><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>DynDNS</td> <td style="text-align: center;"><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> | | | | | | Service | Enabled | Host | User name | Password | Password confirmation | No-IP | <input type="checkbox"/> | | | | | DynDNS | <input type="checkbox"/> | | | | |
| Service | Enabled | Host | User name | Password | Password confirmation | | | | | | | | | | | | | | | | | | |
| No-IP | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | |
| DynDNS | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | |
| <div style="display: flex; justify-content: space-between; margin-top: 20px;"> Previous Abort Next </div> | | | | | | | | | | | | | | | | | | | | | | | |

Description

The table has the following columns:

- **Service**
Shows which providers are supported.
- **Enabled**
When enabled, the device logs on to the DDNS server.
- **Host**
Enter the hostname that you have agreed with your DDNS provider for the device, e.g. example.no-ip-com.
- **User Name**
Enter the user name with which the device logs on to the DDNS server.
- **Password**
Enter the password assigned to the user.
- **Password Confirmation**
Confirm the password.

4.3.6 SINEMA RC

On this Basic Wizard page, you configure the access to the SINEMA RC server.

Note

This function can only be used with a KEY PLUG (Page 28).

Basic Wizard: SINEMA Remote Connect

| IP | Device | Time | DDNS | SINEMA RC | Summary |
|----|--------|------|------|-----------|---------|
|----|--------|------|------|-----------|---------|

Here, you configure the access to the SINEMA RC server. With these settings, the device logs on to the server. The VPN tunnel between the device and the SINEMA RC server is established only after successful authentication. Depending on the configured communications relations and the security settings, the SINEMA RC server connects the individual VPN tunnels.

Enable SINEMA RC

Server Settings

SINEMA RC Address:

SINEMA RC Port:

Server Verification

Verification Type:

Fingerprint:

CA Certificate:

Device Credentials

Device ID:

Device Password:

Device Password Confirmation:

Optional Settings

Auto Firewall/NAT Rules

Type of connection:

Use Proxy:

Autoenrollment Interval [min]:

Description

The page contains the following:

- **Enable SINEMA RC**

- Enabled:
A connection to the configured SINEMA RC Server is established. These boxes cannot be edited.
- Disabled:
The boxes can be edited. Any existing connection is terminated.

"Server settings" area

- **SINEMA RC Address**
Enter the IPv4 address or the FQDN (Fully Qualified Domain Name) of the SINEMA RC Server.
- **SINEMA RC Port**
Enter the port via which the SINEMA RC Server can be reached.

"Server Verification" area

- **Verification Type**
 - Fingerprint: The identity of the server is verified based on the fingerprint.
 - CA certificate: The identity of the server is verified based on the CA certificate.
- **Fingerprint**
Only necessary with the setting "Fingerprint". Enter the fingerprint of the device. The fingerprint is assigned during commissioning of the SINEMA RC Server. Based on the fingerprint, the device checks whether the correct SINEMA RC Server is involved. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **CA Certificate**
Only necessary with the setting "CA Certificate". Select the CA certificate of the server used to sign the server certificate. Only loaded CA certificates can be selected.

"Device Credentials" area

- **Device ID**
Enter the device ID. The device ID is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Device Password**
Enter the password with which the device logs on to the SINEMA RC Server. The password is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Device Password Confirmation**
Repeat the password.

"Optional Settings" area**• Auto Firewall/NAT Rules**

– Enabled

The firewall and NAT rules are created automatically for the VPN connection. The connections between the configured exported subnets and the subnets that can be reached via the SINEMA RC Server are allowed. The NAT settings are implemented as configured in the SINEMA RC Server.

You can enable SINEMA RC to access specific services of the device under "Security > Firewall > Predefined IPv4".

– Disabled

You will need to create the firewall and NAT rules yourself.

• Type of connection

Specify the type of VPN connection. For more detailed information, refer to the section "VPN connection establishment".

– Auto

The device adopts the settings of the SINEMA RC server. You configure the settings on the SINEMA RC Server in "Remote Connections > Devices". You will find further information on this topic in the operating instructions "SINEMA RC Server".

– Permanent

The settings of the SINEMA RC server are ignored. The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is established permanently

– Digital Input

The settings of the SINEMA RC server are ignored. If the "Digital In" event occurs, the device attempts to establish a VPN connection to the SINEMA RC Server. This is on the condition that the event "Digital In" is forwarded to the VPN connection. To do this in "System > Events > Configuration" activate "VPN Tunnel" for the "Digital In" event.

• Use Proxy

Specify whether a connection to the defined SINEMA RC Server is established via a proxy server. Only the proxy servers can be selected that you configured in "System > Proxy Server".

• Autoenrollment Interval [min]

Specify the period of time in minutes after which queries are sent to the SINEMA RC server.. With these queries, the device checks whether there is a newer firmware file on the SINEMA RC server.

If you enter the value 0, this function is disabled.

• Timeout [min]

Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

4.3.7 Cloud Connector

On this wizard page, you configure the parameters for communication with the TIA Portal Cloud Connector.

Note

- Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
- Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector") to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server".

Basic Wizard: TIA Portal Cloud Connector

| | | | | | | | | |
|----|--------|-----|----------|------|------|-----------|-----------------|---------|
| IP | Device | SIM | Operator | Time | DDNS | SINEMA RC | Cloud Connector | Summary |
|----|--------|-----|----------|------|------|-----------|-----------------|---------|

The 'TIA Portal Cloud Connector' integrated in the product permits access to the PROFIBUS/MPI or PROFINET interface and the connected devices. The connection can take place from the local network or via a secure remote connection, for example, in combination with SINEMA Remote Connect. On this page, you configure the port for the communication with the TIA Portal Cloud Connector. You can also enable the 'TIA Portal Cloud Connector'.

Operation: Disabled ▼

Port: 9023

Protocol: PROFINET ▼

| Interface | Active |
|-------------|--------------------------|
| vlan1 (INT) | <input type="checkbox"/> |

Previous
Abort
Next

Requirement

- For the incoming packets to be forwarded to the device, enable the predefined IPv4 rule "Cloud Connector".

Description

The Basic Wizard page contains the following:

- **Operation**

- Enabled
Enables the integrated TIA Portal Cloud Connector.
- Disabled
Disables the integrated TIA Cloud Connector.
- Start on DI
Enabling is controlled via the digital input (DI) if the "Cloud Connector" is enabled for the event "Digital input" under "System > Events > Configuration". If this setting is not enabled, the event is not passed on to the TIA Portal Cloud Connector.

- **Port**

Communication with the TIA Portal Cloud Connector is established via this port.

- **Protocol**

This protocol is used to access the plant network.

- PROFINET via VLAN
You define the VLAN interface in the following table.

Only with M804PB

- PROFIBUS via MPI/DP
- PROFINET-PROFIBUS

The following table is only required for PROFINET:

- Interface
Only VLANs with a configured subnet are available.
- Active
When enabled, this VLAN is used for PROFINET.

4.3.8 Summary

Introduction

The settings are summarized on this page. The content of the page depends on the set parameters and the device.

Check the settings before you exit the Basic Wizard with the "Set Values" button. If settings are incorrect, go back using the "Prev" button and change the settings to the required ones.

Basic Wizard: Summary

| IP | Device | Time | DDNS | SINEMA RC | Summary |
|--|----------|--------------------|------|-----------------|---------------|
| <p>Internal (vlan1)</p> <p>IP Address: 192.168.16.42</p> <p>DHCP: disabled</p> | | | | | |
| <p>External (vlan2)</p> <p>IP Address: 192.168.50.1</p> <p>Subnet Mask: 255.255.255.0</p> <p>DHCP: disabled</p> | | | | | |
| <p>Create new Gateway</p> <p>IP Address: 0.0.0.0</p> | | | | | |
| <p>System Name: sysName Not Set</p> <p>System Location: sysLocation Not Set</p> <p>System Contact: sysContact Not Set</p> | | | | | |
| <p>Time Manually: enabled</p> <p>System Time: 10/24/2019 13:38:34</p> <p>NTP Client: disabled</p> <p>Secure NTP Client only: disabled</p> <p>Time Zone: +00:00</p> | | | | | |
| NTP Server Index | | NTP Server Address | | NTP Server Port | Poll Interval |
| 1 | | 0.0.0.0 | | 123 | 64 |
| Service | Enabled | Host | | User name | |
| No-IP | disabled | | | | |
| DynDNS | disabled | | | | |
| <p>SINEMA RC: disabled</p> | | | | | |
| <p>Click the 'Set Values' button to apply the changes!</p> | | | | | |
| <p> <input type="button" value="Previous"/> <input type="button" value="Abort"/> <input type="button" value="Set Values"/> </p> | | | | | |

Set Values

Click the "Set Values" button to exit the Basic Wizard. The settings are adopted.

4.4 "Information" menu

4.4.1 Start Page

View of the Start page

After logging in successfully, the start page of the WBM is displayed. You cannot configure anything on this page.

General layout of the WBM page

The following areas are available on every WBM page:

- Selection area (1): Top area
- Display area (2): Top area
- Navigation area (3): Left-hand area
- Content area (4): Middle area

4.4 "Information" menu




The screenshot displays the Siemens web-based management interface. At the top left, the Siemens logo is labeled with a circled '1'. Below it, the text 'Welcome admin' is labeled with a circled '2'. The left navigation menu has 'Information' highlighted with a circled '3'. The main content area is titled 'System Configuration' and contains several configuration options: 'Telnet Server' (unchecked), 'SSH Server' (checked), 'HTTPS Server only' (checked), 'SMTP Client' (unchecked), and 'Syslog Client' (unchecked). Below these are dropdown menus for 'DCP Server' (set to 'Read/Write'), 'Time' (set to 'Manual'), and 'SNMP' (set to 'SNMPv1v2cv3'). Further down, there are checkboxes for 'SNMPv1v2 Read-Only' (checked), 'SNMPv1 Traps' (unchecked), and 'SINEMA Configuration Interface' (checked). A 'Configuration Mode' dropdown is set to 'Automatic Save'. At the bottom of the configuration area, there is a 'Write Startup Config' button, which is labeled with a circled '4'. Below this button are 'Set Values' and 'Refresh' buttons. The top right of the page shows a language selector set to 'English' and a 'Go' button, along with a timestamp '03/29/2017 06:58:06'.

Selection area (1)

The following is available in the selection area:




- Logo of Siemens AG
When you click on the logo, you arrive at the Internet page of the corresponding basic device in Siemens Industry Online Support.
- Display of: "System Location / System Name"
 - "System Location" contains the location of the device.
With the settings when the device ships, the IP address of the device is displayed.
 - "System Name" is the device name.
With the settings when the device ships, the device type is displayed.






You can change the content of this display with "System > General > Devices".

- Drop-down list for language selection
- System time and date
You can change the content of this display with "System > System Time".
If the system time is not set, the status is . If the system time is configured, but the system time cannot be synchronized, a yellow warning triangle  can be seen. Check whether the time server can be reached. If necessary adapt your configuration. If the system time is set and/or can be synchronized, the status is .

Display area (2)

In the left-hand part of the display area, the full title of the currently selected menu item is always displayed.

- **LED simulation** 
Each device has one or more LEDs that provide information on the operating state of the device. Depending on its location, direct access to the device may not always be possible. Web Based Management therefore displays simulated LEDs. The meaning of the LED displays is described in the operating instructions.
If you click this button, you open the window for the LED simulation. You can show this window during a change of menu and move it as necessary. To close the LED simulation, click the close button in the LED simulation window.
- **Help** 
When you click this button, the help page of the currently selected menu item is opened in a new browser window.
- **Printer** 
When you click this button, a pop-up window opens with a view of the page content optimized for the printer.

- **Favorites**
When the product ships, the button is disabled on all pages .
If you click this button, the symbol  changes and the currently open page or currently open tab is marked as favorite. Once you have enabled the button once, the navigation area is divided into two tabs. The first tab "Menu" contains all the available menus as previously. The second tab "Favorites" contains all the pages/tabs that you selected as favorites. On the "Favorites" tab the pages/tabs are arranged according to the structure in the "Menu" tab. If you disable all the favorites you have created, the "Favorites" tab is removed again. To do this, click the  button on the relevant pages/tabs.
You can save, upload and delete the favorites configuration of a device on the "System > Load&Save" page using HTTP or TFTP.
- **Update on  / Update off **
WBM pages with overview lists can also have the additional "Update" button.
With this button, you can enable or disable updating of the content area. If updating is turned on, the display is updated every 2 seconds. To disable the update, click "On". Instead of "On", "Off" is displayed. As default, updating is always enabled on the WBM page.

Navigation area (3)

In the navigation area, you have various menus available. Click the individual menus to display the submenus. The submenus contain pages on which information is available or with which you can create configurations. These pages are always displayed in the content area.

Content area (4)

In the navigation area, click a menu to display the pages of the WBM in the content area.

The following is displayed below the picture of the device:

- System Name: System name of the device
- Device Type: The type of the device
- PLUG Configuration:
Shows the status of the configuration data on the PLUG, refer to the section "System > PLUG > Configuration".
- PLUG License:
Shows the status of the license on the PLUG, refer to the section "System > PLUG > License".
- Connection Status: Status of the connection
- Signal Strength [dBm] (only with M87x / MUM856):
Shows the signal strength of the connection.

- **DDNS Status**
If a dynamic DNS service is used, the host name of the device is displayed, e.g. example.no-ip.com. The status of the update is also displayed.
 - update successful
Update successful
 - update failed
Update unsuccessful
 - status unknown
Status unknown
- **Fault Status** Fault status of the device

Buttons you require often

The WBM pages contain the following standard buttons:

- **Refresh the display with "Refresh"**
WBM pages that display current parameters have a "Refresh" button at the lower edge of the page. Click this button to request up-to-date information from the device for the current page.

Note

If you click the "Refresh" button, before you have transferred your configuration changes to the device using the "Set Values" button, your changes will be deleted and the previous configuration will be loaded from the device and displayed here.

- **Save entries with "Set Values"**
WBM pages in which you can make configuration settings have a "Set Values" button at the lower edge. The button only becomes active if you change at least one value on the page. Click this button to save the configuration data you have entered on the device. Once you have saved, the button becomes inactive again.

Note

Changing configuration data is possible only with the "admin" role.

Note

The changes take immediate effect. But it takes some time for the changes in the configuration to be stored.

- **Create entries with "Create"**
WBM pages in which you can make new entries have a "Create" button at the lower edge. Click this button to create a new entry.
- **Delete entries with "Delete"**
WBM pages in which you can delete entries have a "Delete" button at the lower edge. Click this button to delete the previously selected entries from the device memory. Deleting also results in an update of the page in the WBM.
- **Page down with "Next"**
On WBM pages with a lot of data records the number of data records that can be displayed on a page is limited. Click the "Next" button to page down through the data records.

- **Page back with "Prev"**
On WBM pages with a lot of data records, the number of data records that can be displayed on a page is limited. Click the "Prev" button to page back through the data records.
- **Delete the display with "Clear"**
In pages with sequence logs, you can delete all table entries at the same time regardless of whether filters are selected. The display is cleared in this process. The restart counter is only reset after you have restored the device to the factory settings and restarted the device. Click the "Clear" button to completely delete the data record.
- **Button "Show all"**
You can show all entries in pages with a large number of data records. Click "Show all" to display all entries on the page. Note that displaying all messages can take some time.
- **Drop-down list for page change**
In pages with a large number of data records, you can navigate to the desired page. From the drop-down list, select the relevant page to display it.
- **"Reset Counters" button**
Click "Reset Counters" to reset all counters. The counters are reset by a restart.

Logout

You can log out from any WBM page by clicking the "Logout" link.

Messages

If you have enabled the "Automatic Save" mode and you change a parameter the following message appears in the display area "Changes will be saved automatically in x seconds. Click 'Write Startup Config' to save the changes immediately."

Note

Interrupting the save

Saving starts only after the timer in the message has elapsed. How long saving takes depends on the device.

During the save, the message "Saving configuration data in progress. Please do not switch off the device" is displayed.

- Do not switch off the device immediately after the timer has elapsed.
-

4.4.2 Versions

This WBM page shows the versions of the hardware and software of the device.

| Version Information | | | |
|---------------------|-----------------------------|-----------|---------------------|
| Hardware | Name | Revision | Order ID |
| Basic Device | SCALANCE S615 | 1 | 6GK5 615-0AA00-2AA2 |
| Software | Description | Version | Date |
| Firmware | SCALANCE M800/S615 Firmware | V05.00.00 | 11/27/2017 14:00:00 |
| Bootloader | SCALANCE S600 Bootloader | V01.05.00 | 08/02/2017 16:30:00 |
| Firmware_Running | Current running Firmware | V05.00.00 | 11/27/2017 14:00:00 |

Description

Table 1 has the following columns:

- **Hardware**
 - Basic Device
Shows the basic device
- **Name**
Shows the name of the device.
- **Revision**
Shows the hardware version of the device.
- **Order ID**
Shows the article number of the device.
- **Software**
 - Firmware
Shows the current firmware version. If a new firmware file was downloaded and the device has not yet restarted, the firmware version of the downloaded firmware file is displayed here. After the next restart, the loaded firmware is activated and used.
 - Bootloader
Shows the version of the boot software stored on the device.
 - Firmware_Running
Shows the firmware version currently being used on the device.
- **Description**
Shows the short description of the software.
- **Version**
Shows the version number of the software version.
- **Date**
Shows the date on which the software version was created.

4.4.3 Identification & Maintenance

Identification and Maintenance data

This page contains information about device-specific vendor and maintenance data such as the order number, serial number, version number etc. You cannot configure anything on this page.

The screenshot shows a web interface titled "Identification & Maintenance". It displays a list of device attributes with their corresponding values. At the bottom left, there is a "Refresh" button.

| | |
|--------------------|---------------------|
| Manufacturer ID: | 42 |
| Order ID: | 6GK5 552-0AR00-2AR2 |
| Serial Number: | VPA1472019 |
| Hardware Revision: | 3 |
| Software Revision: | T06.03.00 |
| Revision Counter: | 0 |
| Revision Date: | 00/00/0 00:00:00 |
| Function Tag: | |
| Location Tag: | |
| Date: | |
| Descriptor: | |

Refresh

Description of the displayed values

The table has the following rows:

- **Manufacturer ID**
Shows the manufacturer ID.
- **Order ID**
Shows the order ID.
- **Serial Number**
Shows the serial number.
- **Hardware Revision**
Shows the hardware version.
- **Software Revision**
Shows the software version.
- **Revision Counter**
Regardless of a version change, this box always displays the value "0".
- **Revision Date**
Date and time of the last revision

- **Function tag**
Shows the function tag (plant designation) of the device. The plant designation (HID) is created during configuration of the device with HW Config of STEP 7.
- **Location tag**
Shows the location tag of the device. The location identifier (LID) is created during configuration of the device with HW Config of STEP 7.
- **Date**
Shows the date created during configuration of the device with HW Config of STEP 7.
- **Descriptor**
Shows the description created during configuration of the device with HW Config of STEP 7.

4.4.4 ARP / neighbors

4.4.4.1 ARP-Table

Assignment of MAC address and IPv4 address

With the Address Resolution Protocol (ARP), there is a unique assignment of MAC address to IPv4 address. This assignment is kept by each network node in its own separate ARP table. The WBM page shows the ARP table of the device.

| Address Resolution Protocol (ARP) Table | | | |
|---|---------------------|---------------|------------|
| ARP Table | IPv6 Neighbor Table | | |
| Interface | MAC Address | IP Address | Media Type |
| vlan1 | 68-05-ca-36-39-0d | 192.168.16.20 | Dynamic |
| vlan1 | 68-05-ca-25-e8-62 | 192.168.16.55 | Dynamic |

2 entries.

Description of the displayed values

The table has the following columns:

- **Interface**
Shows the interface via which the row entry was learnt.
- **MAC Address**
Shows the MAC address of the destination or source device.

4.4 "Information" menu

- **IP Address**
Shows the IPv4 address of the destination device.
- **Media Type**
Shows the type of connection.
 - Dynamic
The device recognized the address data automatically.
 - Static
The addresses were entered as static addresses.

4.4.4.2 IPv6 Neighbor Table

Assignment of MAC address and IPv6 address

Via the IPv6 neighbor table, there is a unique assignment of MAC address to IPv6 address. This assignment is kept by each network node in its own separate neighbor table.

Address Resolution Protocol (ARP) Table

| Interface | MAC Address | IP Address | Media Type |
|-----------|-------------------|---------------|------------|
| vlan1 | 00-13-ce-63-59-bf | 192.168.0.97 | Dynamic |
| vlan1 | 6c-62-6d-6f-38-31 | 192.168.0.100 | Dynamic |

2 entries.

Description of the displayed values

The table has the following columns:

- **Interface**
Displays the interface via which the row entry was learnt.
- **MAC Address**
Shows the MAC address of the destination or source device.
- **IP Address**
Shows the IPv6 address of the destination device.
- **Media Type**
Shows the type of connection.
 - Dynamic
The device recognized the address data automatically.
 - Static
The addresses were entered as static addresses.

4.4.5 Log Tables

4.4.5.1 Event log

Logging events

The WBM page shows the system events that have occurred in the form of a table. Some of the system events can be configured in "System > Events", for example if the connection status of a port has changed.

The content of the table is retained even when the device is turned off. The event log file can be loaded using HTTP, TFTP or SFTP.

Log Table

Event Log | Security Log | Firewall Log

Severity Filters

Info
 Warning
 Critical

| Restart | System Up Time | System Time | Severity | Log Message |
|---------|----------------|-------------------|-------------|---|
| 432 | 00:04:16 | Date/time not set | 6 - Info | Spanning Tree: topology change detected. |
| 432 | 00:03:33 | Date/time not set | 4 - Warning | SHDSL connection check: Could not reach remote device 192.168.50.48 (Failure count 1) |
| 432 | 00:02:56 | Date/time not set | 6 - Info | Spanning Tree: topology change detected. |
| 432 | 00:02:56 | Date/time not set | 6 - Info | Link up on SHDSL 1. |
| 432 | 00:02:55 | Date/time not set | 6 - Info | Link up on SHDSL 2. |
| 432 | 00:02:46 | Date/time not set | 6 - Info | Interface SHDSL 1 connection established. |
| 432 | 00:02:45 | Date/time not set | 6 - Info | Interface SHDSL 2 connection established. |
| 432 | 00:01:49 | Date/time not set | 6 - Info | Link down on SHDSL 2. |
| 432 | 00:01:49 | Date/time not set | 6 - Info | Link down on SHDSL 1. |
| 432 | 00:01:48 | Date/time not set | 4 - Warning | Interface SHDSL 2 connection lost. |

1 - 10 of 1200 entries [Show all](#) 1 ▾ [Next](#)

Description

- **Severity Filters**
You can filter the entries in the table according to severity. To display all the entries, enable or disable all parameters.

Note

For each severity, a maximum of 400 entries in the table are possible. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

- Critical
Critical
When this parameter is enabled, all entries of the category "Critical" are displayed.
- Warning
warning
When this parameter is enabled, all entries of the category "Warning" are displayed.
- Info
Informative
When this parameter is enabled, all entries of the category "Info" are displayed.

The table has the following columns:

- **Restart**
Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
Shows the date and time when the described event occurred. If no system time is set, the box displays "Date/time not set".
- **Severity**
Sorts the entry into the categories above.
- **Log Message**
Displays a brief description of the event that has occurred.

4.4.5.2 Security Log

The WBM page shows the events that occurred during communication via a secure VPN tunnel in the form of the table.

Security Log-Tabelle

Ereignis-Log | **Security-Log** | Firewall-Log

Severity-Filter

Info
 Warning
 Critical

| Neustart | Systembetriebszeit | Systemzeit | Severity | Log-Meldung |
|----------|--------------------|-------------------|----------|---|
| 21 | 00:02:47 | Date/time not set | 6 - Info | 16[KNL] fe80::21b:1bff:fe9a:322e appeared on vlan1 |
| 21 | 00:02:47 | Date/time not set | 6 - Info | 07[KNL] interface vlan1 activated |
| 21 | 00:02:47 | Date/time not set | 6 - Info | 09[KNL] fe80::21b:1bff:fe9a:322e disappeared from vlan1 |
| 21 | 00:02:47 | Date/time not set | 6 - Info | 07[KNL] interface vlan1 deactivated |
| 21 | 00:01:34 | Date/time not set | 6 - Info | 16[CFG] loaded ca certificate "C=DE, O=Siemens, CN=P386A021C-G9FA6E9AE8D298B7D" from '/etc/ipsec.d/cacerts/M826.U7D262D88@GB985.M826b_CACert.pem' |
| 21 | 00:01:34 | Date/time not set | 6 - Info | 16[CFG] loaded RSA private key from '/etc/ipsec.d/private/M826.U7D262D88@GB985.M826b_Key.pem' |
| 21 | 00:01:34 | Date/time not set | 6 - Info | 06[CFG] added configuration 'VPN-1' |
| 21 | 00:01:34 | Date/time not set | 6 - Info | 06[CFG] CA certificate "C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298B7D" not found, discarding CA constraint |
| 21 | 00:01:34 | Date/time not set | 6 - Info | 06[CFG] CA certificate "C=DE O=Siemens CN=P386A021C-G9FA6E9AE8D298B7D" not found, discarding CA constraint |
| 21 | 00:01:34 | Date/time not set | 6 - Info | 06[CFG] id '%any' not confirmed by certificate, defaulting to 'C=DE, O=Siemens, CN=PBB5F-U7D262D88-GB985' |

1 - 10 of 426 Einträge [Alle anzeigen](#) 1 ▼ [Weiter](#)

Description

- **Severity Filters**
You can filter the entries in the table according to severity. To display all the entries, enable or disable all parameters.

Note

For each severity, a maximum of 400 entries in the table are possible. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

- Critical
Critical
When this parameter is enabled, all entries of the category "Critical" are displayed.
- Warning
warning
When this parameter is enabled, all entries of the category "Warning" are displayed.
- Info
Informative
When this parameter is enabled, all entries of the category "Info" are displayed.

The table has the following columns:

- **Restart**
Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
Shows the date and time when the described event occurred. If no system time is set, the box displays "Date/time not set".
- **Severity**
Sorts the entry into the categories above.
- **Log Message**
Displays a brief description of the event that has occurred.

4.4.5.3 Firewall Log

The firewall log logs the events that occurred on the firewall. When you create firewall rules, you can specify the event severity with which they are logged.

Firewall Log Table

Event Log | Security Log | Firewall Log

Severity Filters

Info

Warning

Critical

| Restart | System Up Time | System Time | Severity | Log Message |
|---------|----------------|-------------------|----------|--|
| 1 | 00:09:01 | Date/time not set | 6 - Info | ACCEPT(0) in:vlan1 out:lo len:60 s-mac:68:05:CA:04:D6:26 d-mac:00:1B:1B:38:16:5A s-ip:192.168.0.60 d-ip:192.168.0.20 icmp:8:0 |

1 entry.

Clear

Refresh

Description

- **Severity Filters**
You can filter the entries in the table according to severity. To display all the entries, enable or disable all parameters.

Note

For each severity, a maximum of 400 entries in the table are possible. If the maximum number of entries is reached for a severity, the oldest entries of this severity are overwritten in the table. The table remains permanently in the memory.

- Critical
Critical
When this parameter is enabled, all entries of the category "Critical" are displayed.
- Warning
warning
When this parameter is enabled, all entries of the category "Warning" are displayed.
- Info
Informative
When this parameter is enabled, all entries of the category "Info" are displayed.

4.4 "Information" menu

The table has the following columns:

- **Restart**
Counts the number of restarts since you last reset to factory settings and shows the device restart after which the corresponding event occurred.
- **System Up Time**
Shows the time the device has been running since the last restart when the described event occurred.
- **System Time**
Shows the date and time when the described event occurred. If no system time is set, the box displays "Date/time not set".
- **Severity**
Sorts the entry into the categories above.
- **Log Message**
Displays a brief description of the event that has occurred.

4.4.6 Faults

Error status

if an error occurs, it is shown on this page. On the device, errors are indicated by red fault LED lighting up.

Internal errors of the device and errors that you configure on the following pages are indicated:

- "System > Events"
- "System" > Fault Monitoring"

The calculation of the time of an error always begins after the last system start. If there are no errors present, the fault LED switches off.

The screenshot shows a web interface titled "Faults". At the top, it displays "No. of Signaled Faults: 1" next to a progress bar. Below this is a "Reset Counters" button. A table lists two fault events:

| Fault Time | Fault Description | Clear Fault State |
|------------|-----------------------|-------------------|
| 16s | Link down on P0.1. | Clear Fault State |
| 17s | Warm start performed. | Clear Fault State |

At the bottom of the interface is a "Refresh" button.

Description

- **No. of Signaled Faults**
Indicates how often the fault LED lit up and not how many faults occurred.
- **Reset Counters** button
The number is reset with this button. The counter is reset when there is a restart.

The table contains the following columns:

- **Fault Time**
Shows the time the device has been running since the last system restart when the described error/fault occurred.
- **Fault Description**
Displays a brief description of the fault/error that has occurred.
- **Clear Fault State**
Some faults can be acknowledged and thus removed from the fault list, e.g. a fault of the event "Cold/Warm Start". If the "Clear Fault State" button is enabled, you can delete the error.

4.4.7 DHCP Server

This page shows which IPv4 addresses were assigned to the devices by the DHCP server.

| DHCP Server Bindings | | | | | | |
|----------------------|---------|-----------------------|----------------------|-------------------|---------------|---------------------|
| IP Address | Pool ID | Identification Method | Identification Value | Allocation Method | Binding State | Expire Time |
| 192.168.16.90 | 1 | Client ID | OS-EC74BA03FED2 | dynamic | assigned | 01/01/2000 05:21:03 |

1 entry.

Description of the displayed values

- **IP Address**
Shows the IPv4 address assigned to the DHCP client.
- **Pool ID**
Shows the number of the IPv4 address band.

4.4 "Information" menu

- **Identification Method**
Shows the method with which the DHCP client is identified.
 - MAC address
Identification is based on the MAC address.
 - DHCP Client ID
Identification is based on a freely defined DHCP client ID.
 - System Name
Identification is based on the system name. If the system name is 255 characters long, the last character is not used for identification.
 - IAID and DUID
With this, the DHCP client can log on to DHCP servers that support parallel operation of IPv4 and IPv6.
The identification is via the IAID and the DUID and identifies precisely one IP interface of the device.
- **Identification Value**
Shows the value that is assigned to the identification method.
- **Allocation Method**
Shows whether the IPv4 address was assigned statically or dynamically. You configure the static entries in "System > DHCP > Static Leases".
- **Binding State**
Shows the status of the assignment.
 - Associated
The assignment is used.
 - not used
The assignment is not used.
 - probing
The assignment is being checked.
 - unknown
The status of the assignment is unknown.
- **Expire Time**
Shows how long the assigned IPv4 address is still valid. When half the period of validity has elapsed, the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

4.4.8 SNMP

This page displays the created SNMPv3 groups. You configure the SNMPv3 groups in "System > SNMP".

| Simple Network Management Protocol v3 (SNMPv3) Groups Overview | |
|--|-----------|
| Group Name | User Name |
| Service | Mueller |
| Wartung | Peterson |

Description

The table has the following columns:

- **Group Name**
Shows the group name.
- **User Name**
Shows the user that is assigned to the group.

4.4.9 LLDP

Status of the neighborhood table

This page shows the current content of the neighborhood table. This table stores the information that the LLDP agent has received from connected devices.

You set the interfaces via which the LLDP agent receives or sends information in the following section: "Layer 2 > LLDP".

| Link Layer Discovery Protocol (LLDP) Neighbors | | | | | |
|--|-------------------|-----------------|-----------|---------------|----------|
| System Name | Device ID | Local Interface | Hold Time | Capability | Port ID |
| M816-1A | 00:1b:1b:9a:3c:b2 | P1 | 20 | Bridge,Router | port-001 |
| M826-2 | 00:1b:1b:9a:32:2e | P2 | 20 | Bridge,Router | port-001 |

Description

The table contains the following columns:

- **System Name**
System name of the connected device.
- **Device ID**
Device ID of the connected device. The device ID corresponds to the device name assigned via PST (STEP 7). If no device name is assigned, the MAC address of the device is displayed.
- **Local Interface**
Port at which the device received the information
- **Hold Time**
An entry remains stored on the device for the time specified here. If the IE switch does not receive any new information from the connected device during this time, the entry is deleted.
- **Capability**
Shows the properties of the connected device:
 - Router
 - Bridge
 - Telephone
 - DOCSIS Cable Device
 - WLAN Access Point
 - Repeater
 - Station
 - Other
- **Port ID**
Device port that is connected to the device.

4.4.10 IPv4 Routing

Introduction

This page shows the routes currently being used.

| Layer 3: IPv4 Routing Table | | | | | |
|-----------------------------|---------------|---------|-----------|--------|------------------|
| Destination Network | Subnet Mask | Gateway | Interface | Metric | Routing Protocol |
| 192.168.16.0 | 255.255.255.0 | 0.0.0.0 | vlan1 | 0 | connected |

1 entry.

[Refresh](#)

Description

The table has the following columns:

- **Destination Network**
Shows the destination address of this route.
- **Subnet Mask**
Shows the subnet mask of this route.
- **Gateway**
Shows the gateway for this route.
- **Interface**
Shows the interface for this route.
- **Metric**
Shows the metric of the route. The higher value, the longer packets require to their destination.
- **Routing Protocol**
Shows the routing protocol from which the entry in the routing table originates. The following entries are possible:
 - Connected: Connected routes
 - Static: Static routes
 - DHCP: Routes via DHCP

4.4.11 IPv6 Routing

Introduction

This page shows the IPv6 routes currently being used.

Layer 3: IPv6 Routing Table

| Destination Network | Prefix Length | Gateway | Interface | Metric | Routing Protocol |
|---------------------|---------------|---------|-----------|--------|------------------|
| 2002:C0A8:1296:: | 48 | :: | vlan1 | 1 | connected |

1 entry.

Description

The table has the following columns:

- **Destination Network**
Shows the destination address of this route.
- **Prefix Length**
Shows the prefix length of this route.
- **Gateway**
Shows the gateway for this route.

4.4 "Information" menu

- **Interface**
Shows the interface for this route.
- **Metric**
Shows the metric of the route. The higher value, the longer packets require to their destination.
- **Routing Protocol**
Shows the routing protocol from which the entry in the routing table originates. The following entries are possible:
 - Connected: Connected routes
 - Static: Static routes
 - RIPng: Routes via RIPng
 - OSPFv3: Routes via OSPFv3
 - Other: Other routes

4.4.12 IPsec VPN

The WBM page shows the status of the activated VPN connections.

| Internet Protocol Security (IPsec) Information | | | | | | | | |
|--|---------------|---------------|------------------|---------------|---------------|-----------------|------------|-------------|
| Name | Local Host | Local DN | Local Subnet | Remote Host | Remote DN | Remote Subnet | Rekey Time | Status |
| VPN-1 | 192.168.100.1 | 192.168.100.1 | 192.168.100.0/24 | 192.168.184.2 | 192.168.184.2 | 192.168.11.0/24 | 50m 2s | established |

Description of the displayed values

This table contains the following columns:

- **Name**
Shows the name of the VPN connection.
- **Local Host**
Shows the IP address of the device.
- **Local DN**
Shows the Distinguished Name (DN) of the device that was signaled to the remote station during connection establishment. The entry is adopted from the "Local ID" box, the device certificate or the IP address of the device.
- **Local Subnet**
Shows the local subnet.
- **Remote Host**
Shows the IP address or the host name of the remote device.

- **Remote DN**
Shows the Distinguished Name (DN) signaled by the remote device during connection establishment.
- **Remote Subnet**
Shows the remote subnet.
- **Rekey Time**
Shows when the validity of the key expires.
- **Status**
Shows the status of the VPN connection.

4.4.13 SINEMA RC

Shows information on SINEMA RC Server.

Note

This function can only be used with the PLUG SINEMA RC.

SINEMA Remote Connect (SINEMA RC) Information

| | |
|------------------------------|----------|
| Status: | disabled |
| Device Name: | - |
| Device Location: | - |
| GSM Number: | - |
| Vendor: | - |
| Comment: | - |
| Type of Connection (Server): | - |
| Type of Connection (Device): | Auto |
| Fingerprint: | - |
| Remote Address: | - |
| Connected Local Subnet(s): | |
| Connected Local Host (s): | |
| Tunnel Interface Address: | - |
| Connected Remote Subnet(s): | |

Description of the displayed values

- **Status**
Shows the status of the connection to SINEMA RC Server.
- **Device Name**
If configured, the name of the device is displayed.
- **Device Location**
If configured, the location of the device is displayed.
- **GSM Number**
If configured, the phone number of the device is displayed.
- **Vendor**
If configured, the entry is displayed.
- **Comment**
If configured, the comment is displayed.
- **Type of Connection (Server)**
Shows which type of connection is set on the SINEMA RC Server.
- **Type of Connection (Device)**
Shows which type of connection is set on the device.
- **Fingerprint**
Shows the fingerprint of the server certificate. Is only displayed when the fingerprint is used for verification.
- **Remote Address**
Shows the IP address of the SINEMA RC Server.
- **Connected Local Subnet(s)**
Shows the IP addresses of the local subnets. Is only displayed when the option "Connected local subnets" is enabled on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.
- **Connected Local Host (s)**
Shows the destination IP address of the hosts that can be reached.
- **Tunnel Interface Address**
Shows the IP address of the virtual tunnel interface.
- **Connected Remote Subnet(s)**
Shows the subnets of the SINEMA RC Server that are reachable for the device. Which subnets are reachable for the device depends on the communications relations on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

4.4.14 OpenVPN client

The WBM page shows the status of the activated OpenVPN connections.

| OpenVPN Client Information | | | | | |
|--|---------------|---------------------|------------------|----------------|--------|
| Name | Remote Server | Tunnel Interface IP | Exported Subnets | Routed Subnets | Status |
| <input type="button" value="Refresh"/> | | | | | |

Description of the displayed values

This table contains the following columns:

- **Name**
Shows the name of the OpenVPN connection.
- **Remote Server**
Shows the IP address or the hostname of the OpenVPN server.
- **Tunnel Interface IP**
Shows the IP address of the virtual tunnel interface.
- **Exported Subnets**
Shows the IP address of the local subnets.
- **Routed Subnets**
Shows the subnets of the OpenVPN server.
- **Status**
Shows the status of the OpenVPN connection.

4.4.15 Redundancy

4.4.15.1 Overview

MSTP-CIST configuration

The page consists of the following parts.

- The left-hand side of the page shows the configuration of the device.
- The right-hand part shows the configuration of the root bridge that can be derived from the spanning tree frames received by a device.

The screenshot shows a web interface for MSTP-CIST configuration. It has two tabs: 'Overview' (selected) and 'Spanning Tree'. The 'Overview' tab displays two columns of configuration parameters. The left column shows the local device's configuration, and the right column shows the root bridge's configuration. A 'Refresh' button is located at the bottom left of the configuration area.

| Parameter | Value | Parameter | Value |
|----------------------|-------------------|----------------------|-------------------|
| Bridge Priority | 32768 | Root Priority | 32768 |
| Bridge Address | 00-1b-1b-9a-31-94 | Root Address | 00-1b-1b-9a-31-94 |
| Root Port | - | Root Cost | 0 |
| Topology Changes | 2 | Last Topology Change | 1min |
| Bridge Hello Time | 2 | Root Hello Time | 2 |
| Bridge Forward Delay | 15 | Root Forward Delay | 15 |
| Bridge Max Age | 20 | Root Max Age | 20 |
| Bridge Max Hop Count | 20 | Root Hop Count | 0 |

Description of the displayed values

The page contains the following boxes:

- **Bridge Priority / Root Priority**
The Bridge Priority decides which device becomes the Root Bridge. The Bridge with the highest priority becomes the Root Bridge. The lower the value, the higher the priority. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the Bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 through 61440.
- **Bridge Address / Root Address**
The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.

- **Root Port**
Shows the port via which the switch communicates with the root bridge.
- **Root Cost**
The path costs from this device to the root bridge.
- **Topology Changes / Last Topology Change**
The entry for the device shows the number of reconfiguration actions due to the spanning tree mechanism since the last startup. For the root bridge, the time since the last reconfiguration is displayed as follows:
 - Seconds: Supplement "sec" after the number
 - Minutes: Supplement "min" after the number
 - Hours: Supplement "hr" after the number
- **Bridge Hello Time / Root Hello Time**
Each bridge sends configuration frames (BPDUs) regularly. The interval between two such frames is the Hello time. The default for this parameter is 2 seconds.
- **Bridge Forward Delay / Root Forward Delay**
New configuration information is not used immediately by a bridge but only after the forwarding delay specified in the parameter. This ensures that operation is only started with the new topology after all the bridges have the required information. The default for this parameter is 15 seconds.
- **Bridge Max Age / Root Max Age**
When the max age timer elapses the received BPDU is discarded to be accepted as valid by the switch. The default value is 20s.
- **Bridge Max Hop Count**
This parameter specifies how many MSTP nodes a BPDU may pass through. If an MSTP BPDU is received and has a hop count that exceeds the value configured here, it is discarded. The default for this parameter is 20.
- **Root Hop Count**
The number of nodes that need to be run through on the way to the root bridge.

4.4.15.2 Spanning Tree

Introduction

The page shows the current information about the spanning tree and the settings of the root bridge.

Spanning Tree

Overview | **Spanning Tree**

Spanning Tree Mode: RSTP
Bridge Priority: 32768
Bridge Address: 00-1b-1b-9a-31-94
Root Priority: 32768
Root Address: 00-1b-1b-9a-31-94
Root Cost: 0
Bridge Status: This bridge is the root

| Port | Role | State | Oper. Version | Priority | Path Cost | Edge Type | P.t.P. Type |
|---------|------------|------------|---------------|----------|-----------|--------------|-------------|
| SHDSL 1 | Designated | Forwarding | RSTP | 128 | 3511236 | No Edge Port | P.t.P |
| SHDSL 2 | Designated | Forwarding | RSTP | 128 | 3511236 | No Edge Port | P.t.P |

[Refresh](#)

Description of the displayed values

The following fields are displayed:

- **Spanning Tree Mode**

Shows the set mode. You specify the mode in "Layer 2 > Configuration" and in "Layer 2 > Spanning Tree > General".

The following values are possible:

- ' '
- RSTP

- **Bridge Priority / Root Priority**

Which device becomes the root bridge is decided by the bridge priority. The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 to 32768.

- **Bridge Address / Root Address**

The bridge address shows the MAC address of the device and the root address shows the MAC address of the root switch.

- **Root Cost**

Shows the path costs from the device to the root bridge.

- **Bridge Status**

Shows the status of the bridge, e.g. whether or not the device is the root bridge.

The table has the following columns:

- **Port**

Shows the interfaces via which the device communicates.

- **Role**

Shows the status of the port. The following values are possible:

- **Disabled**
The port was removed manually from the spanning tree and will no longer be taken into account by the spanning tree.
- **Designated**
The ports leading away from the root bridge.
- **Alternate**
The port with an alternative route to a network segment
- **Backup**
If a switch has several ports to the same network segment, the "poorer" Port becomes the backup port.
- **Root**
The port that provides the best route to the root bridge.
- **Master**
This port points to a root bridge located outside the MST region.

4.4 "Information" menu

- **Status**

Shows the current status of the interface. The values are only displayed. The parameter depends on the configured protocol.

 - Discarding
The port receives BPDU frames. Other incoming or outgoing frames are discarded.
 - Listening
The port receives and sends BPDU frames. The port is involved in the spanning tree algorithm. Other outgoing and incoming frames are discarded.
 - Learning
The port actively learns the topology; in other words, the node addresses. Other outgoing and incoming frames are discarded.
 - Forwarding
Following the reconfiguration time, the port is active in the network. The port receives and sends data frames.
- **Oper. Version**

Shows the compatibility mode of Spanning Tree used by the port.
- **Priority**

If the path calculated by the spanning tree is possible over several ports of a device, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value between 0 and 240 can be entered for the priority in steps of 16. If you enter a value that cannot be divided by 16, the value is automatically adapted. The default is 128.
- **Path Cost**

This parameter is used to calculate the path that will be selected. The path with the lowest value is selected. If several ports of a device have the same value, the port with the lowest port number is selected.

If the value in the "Cost Calc" field is "0", the automatically calculated value is displayed. Otherwise, the value of the "Cost Calc" field is displayed.

The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.

Typical values for path costs with rapid spanning tree:

 - 10,000 Mbps = 2,000
 - 1000 Mbps = 20,000
 - 100 Mbps = 200,000
 - 10 Mbps = 2,000,000

- **Edge Type**
Shows the type of the connection. The following values are possible:
 - Edge Port
There is an end device at this port.
 - No Edge Port
There is a spanning tree or rapid spanning tree device at this port.
- **P.t.P. Type**
Shows the type of point-to-point link. The following values are possible:
 - P.t.P.
With half duplex, a point-to-point link is assumed.
 - Shared Media
With a full duplex connection, a point-to-point link is not assumed.

4.4.16 VRRPv3 Statistics

Introduction

This page shows the statistics of the VRRPv3 protocol and all configured virtual routers.

Virtual Router Redundancy Protocol v3 (VRRPv3) Statistics

VRID Errors: 0

Version Errors: 0

Checksum Errors: 0

| Interface | VRID | Type | Become Master | Advertisements Received | Advertisements Interval Errors |
|-----------|------|------|---------------|-------------------------|--------------------------------|
| vlan3 | 1 | IPv4 | 1 | 0 | 0 |

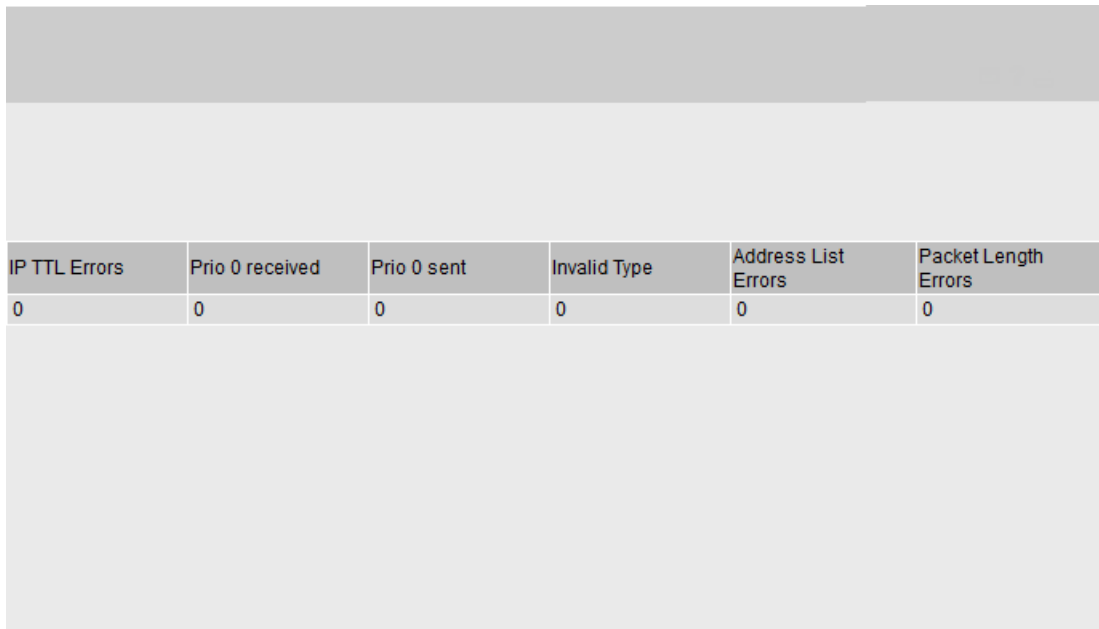
Description

The following fields are displayed:

- **VRID Errors**
Shows how many VRRPv3 packets containing an unsupported VRID were received.
- **Version Errors**
Shows how many VRRPv3 packets containing an invalid version number were received.
- **Checksum Errors**
Shows how many VRRPv3 packets containing an invalid checksum were received.

The table has the following columns:

- **Interfaces**
Interface to which the settings relate.
- **VRID**
Shows the ID of the virtual router. Valid values are 1 ... 255.
- **Address Type**
Shows the version of the IP protocol.
- **Become Master**
Shows how often this virtual router changed to the "Master" status.
- **Advertisements Received**
Shows how many VRRPv3 packets were received.
- **Advertisement Interval Errors**
Shows how many bad VRRPv3 packets were received whose interval does not match the value set locally.



| IP TTL Errors | Prio 0 received | Prio 0 sent | Invalid Type | Address List Errors | Packet Length Errors |
|---------------|-----------------|-------------|--------------|---------------------|----------------------|
| 0 | 0 | 0 | 0 | 0 | 0 |

- **IP TTL Errors**
Shows how many bad VRRPv3 packets were received whose TTL (Time to live) value in the IP header is incorrect.

- **Prio 0 received**
Shows how many VRRPv3 packets with priority 0 were received. VRRPv3 packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Prio 0 sent**
Shows how many VRRPv3 packets with priority 0 were sent. Packets with priority 0 are sent when a master router is shut down. These packets allow a fast handover to the relevant backup router.
- **Invalid Type**
Shows how many bad VRRPv3 packets were received whose value in the "Type" field of the IP header is invalid.
- **Address List Errors**
Shows how many bad VRRPv3 packets were received whose address list does not match the locally configured list.
- **Packet Length Errors**
Shows how many bad VRRPv3 packets were received whose length is not correct.

4.4.17 Security

4.4.17.1 Overview

Note

The values displayed depend on the rights of the logged-in user.

This page shows the security settings and the local and external user accounts.

Security Overview

Overview | Supported Function Rights | Roles | Groups

Services

Telnet Server: disabled

SSH Server: enabled

SSH Fingerprint: MD5: 03:36:1a:92:4b:0e:7f:ad:b3:01:98:0d:dd:27:b1:1a
SHA256: P9EnDkwg6oakEWK3xijjDX+zeZprijhJi+xbUqpeEo

Web Server: HTTP/HTTPS

SNMP: SNMPv1/v2c/v3

Login Authentication: Local

Password Policy: high

Local User Accounts

| User Account | Role |
|--------------|-------|
| admin | admin |

External User Accounts

| User Account | Role |
|--------------|-------|
| admin | admin |

Refresh

Description

Services

The "Services" list shows the security settings.

- **Telnet Server**
You configure the setting in "System > Configuration".
 - Enabled: Unencrypted access to the CLI.
 - Disabled: No unencrypted access to the CLI.
- **SSH Server**
You configure the setting in "System > Configuration".
 - Enabled: Encrypted access to the CLI.
 - Disabled: No encrypted access to the CLI.

- **SSH fingerprint**
The following SSH fingerprints are displayed:
 - MD5
 - SH256
 - **Web Server**
You configure the setting in "System > Configuration".
 - HTTP/HTTPS: Access to the WBM is possible with HTTP and HTTPS.
 - HTTPS: Access to the WBM is now only possible with HTTPS.
 - **SNMP**
You can configure setting in "System > SNMP > General".
 - "-" (SNMP disabled)
Access to device parameters via SNMP is not possible.
 - SNMPv1/v2c/v3
Access to device parameters is possible with SNMP versions 1, 2c or 3.
 - SNMPv3
Access to device parameters is possible only with SNMP version 3.
 - **Login Authentication**
You configure the setting in "Security > AAA > General".
 - Local
The authentication must be made locally on the device.
 - RADIUS
The authentication must be handled via a RADIUS server.
 - Local and RADIUS
The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server.
The user is first searched for in the local database. If the user does not exist there, a RADIUS query is sent.
 - RADIUS and fallback local
The authentication must be handled via a RADIUS server.
A local authentication is performed only when the RADIUS server cannot be reached in the network.
 - **Password Policy**
Shows which password policy is currently being used.
- The "Local User Accounts" and "External User Accounts" tables have the following columns:

- **User Account**
Shows the name of the local user.
- **Role**
Shows the role of the user. You can obtain more information on the function rights of the role in "Information > Security > Roles".

Local and external user accounts

You configure local user accounts and roles in "Security > Users".

When you create a local user account an external user account is generated automatically.

Local user accounts involve users each with a password for logging in on the device.

In the table "External User Accounts" a user is linked to a role. In this example the user "Observer" is linked to the "user" role. The user is defined on a RADIUS server. The roll is defined locally on the device. When a RADIUS server authenticates a user, the corresponding group however is unknown or does not exist, the device checks whether or not there is an entry for the user in the table "External User Accounts". If an entry exists, the user is logged in with the rights of the associated role. If the corresponding group is known on the device, both tables are evaluated. The user is assigned the role with the higher rights.

Note

The table "External User Accounts" is only evaluated if you have set "SiemensVSA" in the RADIUS Authorization Mode.

With CLI you can access external user accounts.

4.4.17.2 Supported Function Rights

Note

The values displayed depend on the role of the logged-on user.

The page shows the function rights available locally on the device.

| Function Right | Description |
|----------------|--|
| 1 | Read-only access to configuration data. |
| 15 | Read/write access to configuration data. |

Description of the displayed values

- **Function Right**
Shows the number of the function right. Different rights relating to the device parameters are assigned to the numbers.
- **Description**
Shows the description of the function right.

4.4.17.3 Roles

Note

The values displayed depend on the role of the logged-on user.

The page shows the roles valid locally on the device.

| User Roles | | | |
|------------|---------------------------|--|---------------|
| Overview | Supported Function Rights | Roles | Groups |
| Role | Function Right | Description | Remote Access |
| user | 1 | System defined role, with readonly access to configuration data of this component. | none |
| admin | 15 | System defined role, with read/write access to configuration data of this component. | none |
| default | 1 | Internal role, for authenticated users without group/role mapping in this component. | none |
| everybody | 0 | Internal role, assigned to users when authentication fails. Access will be denied. | none |

Description

The table contains the following columns:

- **Role**
Shows the name of the role.
- **Function Right**
Shows the function right of the role:
 - 1
Users with this role can read device parameters but cannot change them.
 - 15
Users with this role can both read and change device parameters.
 - 0
This is a role that the device assigns internally when a user could not be authenticated. The user is denied access to the device.
- **Description**
Shows a description of the role.
- **Remote Access**
Shows which remote access is currently being used.

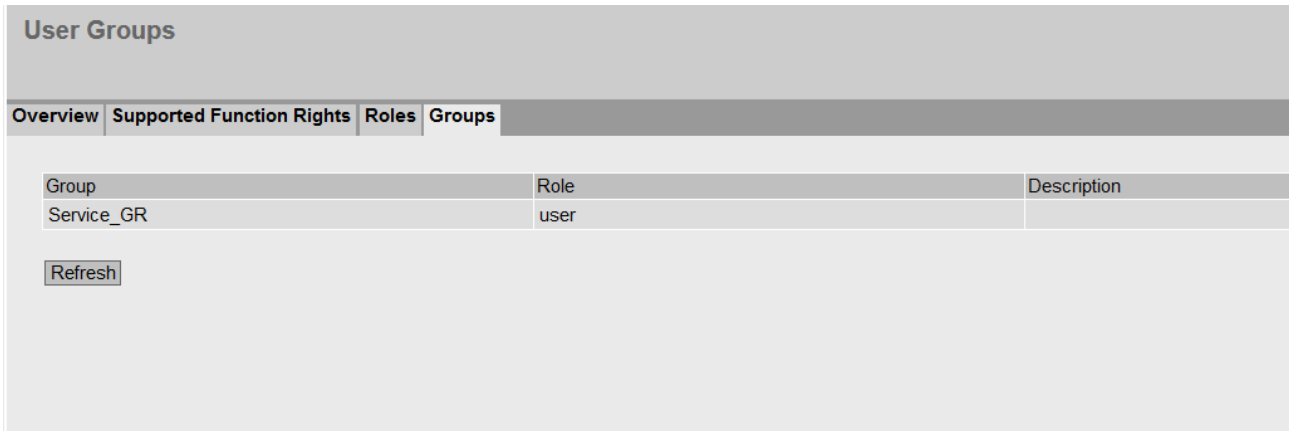
4.4.17.4 Groups

Note

The values displayed depend on the role of the logged-on user.

4.5 "System" menu

This page shows which group is linked to which role. The group is defined on a RADIUS server. The roll is defined locally on the device.



| Group | Role | Description |
|------------|------|-------------|
| Service_GR | user | |

Refresh

Description of the displayed values

The table has the following columns:

- **Group**
Shows the name of the group. The name matches the group on the RADIUS server.
- **Role**
Shows the name of the role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.
- **Description**
Shows a description for the link.

4.5 "System" menu

4.5.1 Configuration

System configuration

The WBM page contains the configuration overview of the access options of the device.

Specify the services that access the device. With some services, there are further configuration pages on which more detailed settings can be made.

The standard port can also be changed for your own services.

Note

Change standard port

Some programs can only access the service over the standard port, e.g. TIA Portal accesses HTTPS over standard port 443. Before you change the port, check which port the program uses. When you change the standard port, you must access the service over the changed port.

Firewall

The firewall is reinitialized after the ports are changed. This means that the changed ports are applied in the firewall rules. Existing connections, for example, via the dynamic firewall, can be used with restrictions during this time.

Systemkonfiguration

Telnet-Server
Telnet-Port: 23

SSH-Server
SSH-Port: 22
Stufe des SSH-Schlüsselaustausch-Algorithmus: Hoch

HTTP-Server
HTTP-Port: 80
 HTTPS-Server
HTTPS-Port: 443
HTTP-Dienste: HTTP nach HTTPS umleiten
Min. TLS-Version: TLSv1.2
Standard-Anmeldeseite: Konfiguration

SMTP-Client
 Syslog-Client
DCP-Server: Schreibgeschützt
Zeiteinstellung: Manuell
SNMP: SNMPv1/v2c/v3
 SNMPv1/v2 schreibgeschützt
 SINEMA-Konfigurationsschnittstelle
DHCP-DUID-Konfiguration
DUID-Typ: DUID-LLT
Link-layer Adresse plus Zeit: 00-01-00-01-00-00-00-02-00-1B-1B-B6-32-79
Unternehmensnummer des Herstellers: 00-02-00-00-10-E9-45-4E-31-34-38-35-39-39
Link-layer Adresse: 00-03-00-01-00-1B-1B-B6-32-79

Konfigurationsmodus: Automatisches Speichern

Schreiben der Startkonfiguration

Einstellungen übernehmen Aktualisieren

Description

The page contains the following boxes:

- **Telnet Server**
Enable or disable the "Telnet Server" service for unencrypted access to the CLI.
- **Telnet Port**
Specify the port for Telnet access to the CLI.
- **SSH Server**
Enable or disable the "SSH Server" service for encrypted access to the CLI.
- **SSH Port**
Specify the port for SSH access to the CLI.
- **SSH key exchange algorithm level**
Configure the level of SSH key exchange algorithm for SSH access to the CLI.
High (default)
 - Curve25519-sha256
 - Curve25519-sha256@libssh.org
 - Ecdh-sha2-nistp256
 - Ecdh-sha2-nistp384
 - Ecdh-sha2-nistp521
 - Diffie-hellman-group16-sha512
 - Diffie-hellman-group18-sha512Low
 - Curve25519-sha256
 - Curve25519-sha256@libssh.org
 - Ecdh-sha2-nistp256
 - Ecdh-sha2-nistp384
 - Ecdh-sha2-nistp521
 - Diffie-hellman-group16-sha512
 - Diffie-hellman-group18-sha512
 - Diffie-hellman-group14-sha256
 - Diffie-hellman-group14-sha1
- **HTTP Server**
Enable or disable HTTP access to the WBM.
- **HTTP Port**
Specify the port for HTTP access to the WBM.
- **HTTPS Server**
Enable or disable HTTPS access to the WBM.
- **HTTPS Port**
Specify the port for HTTPS access to the WBM.

4.5 "System" menu

- **HTTP Services**
Specify how the WBM is accessed:
 - HTTPS
Access to the WBM is only possible with HTTPS.
 - HTTP/HTTPS
Access to the WBM is only possible with HTTP and HTTPS.
 - Redirect HTTP to HTTPS
Access via HTTP is automatically diverted to HTTPS.
- **Min. TLS version**
Specify which minimum TLS version is used.
- **Default Login Page**
Specify the login page with which the WBM starts by default.
 - Firewall
Logging into the WBM page for dynamic firewall.
 - Configuration
Logging into the WBM.
- **SMTP Client**
Enable or disable the SMTP client. You can configure other settings in "System > SMTP Client".
- **Syslog Client**
Enable or disable the Syslog client. You can configure other settings in "System > Syslog Client".
- **DCP Server**
Specify whether or not the device can be accessed with DCP (Discovery and Configuration Protocol):
 - "-" (disabled)
DCP is disabled. Device parameters can neither be read nor modified.
 - Read/Write
With DCP, device parameters can be both read and modified.
 - Read Only
With DCP, device parameters can be read but cannot be modified.

- **Time**

Select the setting from the drop-down list. The following settings are possible:

 - Manual
The system time is set manually. You can configure other settings in "System > System Time > Manual Setting".
 - SIMATIC Time
The system time is set using a SIMATIC time transmitter. You can configure other settings in "System > System Time > SIMATIC Time Client".
 - SNTP Client
The system time is set via an SNTP server. You can configure other settings in "System > System Time > SNTP Client".
 - NTP Client
The system time is set via an NTP server. You can configure other settings in "System > System Time > NTP Client".
- **SNMP**

Select the protocol from the drop-down list. The following settings are possible:

 - "-" (SNMP disabled)
Access to device parameters via SNMP is not possible.
 - SNMPv1/v2c/v3
Access to device parameters is possible with SNMP versions 1, 2c or 3. You can configure other settings in "System > SNMP > General".
 - SNMPv3
Access to device parameters is possible only with SNMP version 3. You can configure other settings in "System > SNMP > General".
- **SNMPv1/v2 Read Only**

Enable or disable write access to SNMP variables with SNMPv1/v2c.
- **SNMPv1 Traps**

Enable or disable the sending of SNMPv1 traps (alarm frames). You can configure other settings in "System > SNMP > Traps".
- **SINEMA Configuration Interface**

If the SINEMA configuration interface is enabled, you can download configurations to the device using STEP 7 Basic / Professional.
- **DHCP Client**

Enable or disable the DHCP client. You can configure other settings in "System > DHCP".
- **DUID-Type**

Specify which DUID type is used. The DUID types are defined in RFC 3315.

 - DUID-LLT
DUID is based on the link layer address of the interface and a time stamp
 - DUID-EN
DUID is assigned by the vendor (EN = enterprise number)
 - DUID-LL
DUID is based on the link layer address of the interface

- **Link-layer Address Plus Time (LLT)**
The value is based on the link layer address of the interface and a time stamp. The value is regenerated each time the factory settings are restored.
- **Vendor Enterprise Number (EN)**
The value is based on the enterprise number specific to the vendor. The value is regenerated each time the factory settings are restored.
- **Link-layer address (LL)**
The link-layer address is based on the MAC address. The value is regenerated each time the factory settings are restored.
- **Configuration Mode**
Select the mode from the drop-down list. The following modes are possible:
 - Automatic Save
Automatic backup mode. Approximately 1 minute after the last parameter change or before you restart the device, the configuration is automatically saved.
In addition to this, the following message appears in the display area "Changes will be saved automatically in x seconds. Click 'Write Startup Config' to save the changes immediately."

Note

Interrupting the save

Saving starts only after the timer in the message has elapsed. How long saving takes depends on the device.

During the save, the message "Saving configuration data in progress. Please do not switch off the device" is displayed.

- Do not switch off the device immediately after the timer has elapsed.
-

- Trial
Trial mode. In Trial mode, although changes are adopted, they are not saved in the configuration file (startup configuration).
To save changes in the configuration file, use the "Write startup config" button. The display area also shows the message "Trial Mode Active – Press the "Write Startup Config" button to make your settings persistent" as soon as there are unsaved modifications. This message can be seen on every WBM page until the changes made have either been saved or the device has been restarted.

Procedure

1. To use the required function, select the corresponding check box.
2. Select the options you require from the drop-down lists.
3. Click the "Set Values" button.

4.5.2 General

4.5.2.1 Device

This WBM page contains the general device information.

The screenshot shows a web-based management interface for a device. At the top, there is a header labeled "Device". Below the header, there are two tabs: "Device" and "Coordinates". The "Device" tab is currently selected. The main content area displays several fields for configuration and status:

- Current System Time: 11/21/2018 01:48:39
- System Up Time: 1h 28m 18s
- Device Type: SCALANCE S615
- System Name: Name
- System Contact: Contact
- System Location: Location
- Cyclic WBM status update

At the bottom of the form, there are two buttons: "Set Values" and "Refresh".

Description

The WBM page contains the following boxes:

- **Current System Time**
Shows the current system time. The system time is either set by the user or by a time-of-day frame: either SIMATIC time-of-day frame, NTP or SNTP.
- **System Up Time**
Shows the operating time of the device since the last restart.
- **Device Type**
Shows the type designation of the device.
- **System Name**
You can enter the name of the device. The entered name is displayed in the selection area. A maximum of 255 characters are possible.
The system name is also displayed in the CLI input prompt. The number of characters in the CLI input prompt is limited. The system name is truncated after 16 characters.
- **System Contact**
You can enter the name of a contact person responsible for managing the device. A maximum of 255 characters are possible.

4.5 "System" menu

- **System Location**

You can enter the location where the device is installed. The entered installation location is displayed in the selection area. A maximum of 255 characters are possible.

Note

Permitted characters

The following printable ASCII characters (0x20 to 0x7e) are permitted in the input fields "**System Name**", "**System Contact**" and "**Device Location**":

- 0123456789
- A...Z a...z
- !"#\$%&'()*+,-./:;<=>?@ [\]_{|}~^`

- **Cyclic WBM status update**

When this is disabled, automatic update of the WBM is switched off. This is suitable for slow 2G connections or contracts with very limited data volume.

The following must be taken into account here:

- No status display update
- No automatic logoff after user inactivity
- No message in trial mode
- No message on automatic saving
- No progress display when saving or uploading files
- No automatic forwarding to the changed IP address

Procedure

1. Enter the contact person responsible for the device in the "System Contact" input box.
2. Enter the identifier for the location at which the device is installed in the "System Location" input box.
3. Enter the name of the device in the "System Name" input box.
4. Click the "Set Values" button.

Note: Steps 1 to 3 can also be performed with the SNMP Management Tool.

4.5.2.2 Coordinates

Information on geographic coordinates

In the "Geographic Coordinates" window, you can enter information on the geographic coordinates. The parameters of the geographic coordinates (latitude, longitude and the height above the ellipsoid according to WGS84) are entered directly in the input boxes of the "Geographic Coordinates" window.

Getting the coordinates

Use suitable maps for obtaining the geographic coordinates of the device.

The geographic coordinates can also be obtained using a GPS receiver. The geographic coordinates of these devices are normally displayed directly and only need to be entered in the input boxes of this page.

The screenshot shows a web interface titled "Geographic Coordinates". It features a table with two columns: "Device" and "Coordinates". Below the table, there are three input fields for entering geographic data: "Latitude: e.g. DD°MM'SS'", "Longitude: e.g. DDD°MM'SS'", and "Height: e.g. dddd m". At the bottom of the form, there are two buttons: "Set Values" and "Refresh".

Description

The page contains the following input boxes with a maximum length of 32 characters.

- "Latitude" input box**
 Geographical latitude: Here, enter the value for the northerly or southerly latitude of the location of the device.
 For example, the value +49° 1' 31.67" means that the device is located at 49 degrees, 1 arc minute and 31.67 arc seconds northerly latitude.
 A southerly latitude is shown by a preceding minus character.
 You can also append the letters N (northerly latitude) or S (southerly latitude) to the numeric information (49° 1' 31.67" N).
- "Longitude" input box**
 Geographic longitude: Here, you enter the value of the eastern or western longitude of the location of the device.
 The value +8° 20' 58.73" means that the device is located at 8 degrees, 20 minutes and 58.73 seconds east.
 A western longitude is indicated by a preceding minus sign.
 You can also add the letter E (easterly longitude) or W (westerly longitude) to the numeric information (8° 20' 58.73" E).
- Input box: "Height"**
 Height Here, you enter the value of the geographic height above sea level in meters.
 For example, 158 m means that the device is located at a height of 158 m above sea level.
 Heights below sea level (for example the Dead Sea) are indicated by a preceding minus sign.

Procedure

1. Enter the calculated latitude in the "Latitude" input box.
2. Enter the calculated longitude in the "Longitude" input box.
3. Enter the height above sea level in the "Height" input box.
4. Click the "Set Values" button.

4.5.3 Restart

Resetting to the defaults

Restart of the device can take place manually or as scheduled using this WBM page. In addition, there are various options for resetting to the device defaults.

Restart

Restart System

Restore Memory Defaults and Restart

Restore Factory Defaults and Restart

Restart in: seconds

Backup: -

Schedule restart

Cancel scheduled restart

Set Values Refresh

Note

Note the following points about restarting a device:

- You can only restart the device with administrator privileges.
 - A device should only be restarted with the buttons of this menu and not by a power cycle on the device.
 - If the device is in "Trial" mode, configuration modifications must be saved manually before a restart. Any modifications you have made only become active on the device after clicking the "Set values" button on the relevant WBM page.
 - If the device is in "Automatic Save" mode, the last changes are saved automatically before a restart.
-

Description

To restart the device, the buttons on this page provide you with the following options:

- **Restart**
Click this button to restart the system. You must confirm the restart in a dialog box. During a restart, the device is reinitialized, the internal firmware is reloaded, and the device runs a self-test. The settings of the start configuration are retained, e.g. the IP address of the device. The learned entries in the address table are deleted. You can leave the browser window open while the device restarts. After the restart you will need to log in again.
- **Restore Memory Defaults and Restart**
Click this button to restore the factory defaults of the device with the exception of the following parameters and to restart the device:
 - IP addresses
 - Subnet mask
 - IP address of the default gateway
 - DHCP client ID
 - DHCP
 - System name
 - System location
 - System contact
 - Mode of the device
 - Login text
- **Restore Factory Defaults and Restart**
Click on this button to restore the factory configuration settings. The protected defaults are also reset.
An automatic restart is triggered.

Note

By resetting to the factory configuration settings, the device is reachable again with the IP address 192.168.1.1 set in the factory, see the section "Requirements for operation".

- **Restart in**
Specify the time after which the device restarts.
- **Backup**
The configuration backups created under "System > Configuration Backup" can be selected. Before the scheduled restart, the device applies the configurations of the selected backup and continues working with them after the restart.
All configurations made up to this point that have not been saved in a backup are lost. With the "-" setting, no file is selected and the device uses the current configuration after the restart.

4.5 "System" menu

- **Scheduled restart**
When you click this button, a timer starts and runs backwards with the defined time. When the timer has expired, the device restarts.

The following message is also displayed in the display area: "The automatic restart starts in [...] minutes. Click 'Cancel scheduled restart' to cancel the restart". This message can be seen on every WBM page until you cancel the restart or the SCALANCE device is restarted.

Note

Unsaved configuration is lost after reboot

The scheduled restart is performed after the time has elapsed without any further message. Unsaved configuration changes are lost.

Save the current configuration via "System > Backup of configuration" before setting the timer for the restart.

- **Cancel scheduled restart**
With this button you disable the timer for the scheduled restart.

4.5.4 Load&Save

4.5.4.1 File list

Overview of the file types

| File type | Description |
|------------------|--|
| Config | This file contains the start configuration. Among other things, this device contains the definitions of the users, roles, groups and function rights. The passwords are stored the file "Users". The file can be supplied with a password before download. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords (Page 147)". |
| ConfigPack | Detailed configuration information. for example, start configuration, users, certificates The file can be supplied with a password before download. To load the file into the device successfully, use the specified password. You enter the password on the WBM page "Passwords (Page 147)". |
| ConfigPackBackup | This ZIP file stores all the configuration backups you have created. |
| Debug | This file contains information for Siemens Support. It is encrypted and can be sent by e-mail to Siemens Support without any security risk. |
| Firmware | The firmware is signed and encrypted. This ensures that only firmware created by Siemens can be downloaded to the device. |

| File type | Description |
|----------------------|--|
| HTTPSCert | <p>Default HTTPS certificates including key</p> <p>The preset and automatically created HTTPS certificates are self-signed.</p> <p>We strongly recommend that you create your own HTTPS certificates and make them available. We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange.</p> <p>There are files to which access is password protected. To load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 147)".</p> |
| LogFile | File with entries from the event log table |
| LoginWelcomeMessage | The txt file contains the desired text or ASCII type. Only pure text files in ASCII format are supported. |
| MIB | Private MSPS MIB file |
| RunningCLI | <p>Text file with CLI commands</p> <p>This file contains an overview of the current configuration in the form of CLI commands. Passwords are masked in this file as follows: [PASSWORD]</p> <p>You can download the text file. The file is not intended to be uploaded again unchanged.</p> |
| RunningSINEMA-Config | <p>You save the current device configuration in this file type for transfer to STEP 7 Basic/Professional. The file can be imported in STEP 7 Basic/Professional and installed on a device with the same article number and firmware version.</p> <p>Before you can save a file, you must assign a password for the "RunningSINEMA-Config" in the WBM under "System > Load&Save > Passwords". You also need this password to import the file into STEP 7 Basic/Professional.</p> <p>See also "SINEMAConfig"</p> |
| Script | <p>Text file with CLI commands</p> <p>You can upload a script file in a device. The CLI commands it contains are executed appropriately.</p> <p>CLI commands for saving and loading files cannot be executed with the CLI script file.</p> |
| SINEMAConfig | <p>You load configuration data that was exported via STEP 7 Basic/Professional for transfer to the WBM with this file type.</p> <p>To load a file, you must assign a password for the "SINEMAConfig" under "System > Load&Save > Passwords". You also need this password to export the file from STEP 7 Basic/Professional.</p> <p>See also "RunningSINEMAConfig"</p> |
| StartupInfo | <p>Startup log file</p> <p>This file contains the messages that were entered in the log during the last startup.</p> |
| Users | This file contains the assignment of the user names to the corresponding passwords. |

4.5 "System" menu

| File type | Description |
|-----------|---|
| WBM Fav | WBM favorites This file contains the favorites that you created in the WBM. You can download this file and upload it into other devices. |
| X509Cert | Various nodes are certified with certificates. The following file types can be loaded into the device: <ul style="list-style-type: none"> • .crt, pem, zip: Maximum file name length 255 characters • .p12: Maximum file name length 248 characters There are files to which access is password protected. To successfully load the file into the device, enter the password specified for the file on the WBM page "Passwords (Page 147)". The loaded files are listed in "Security > Certificates > Overview (Page 286)". For more information on certificates, refer to section "Certificates (Page 54)". |

4.5.4.2 HTTP

Loading and saving data via HTTP

The WBM allows you to store device data in an external file on your client PC or to load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located on your Admin PC. On this page, the certificates required to establish a secure VPN connection can also be loaded.

Firmware

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

Configuration files

Note

Configuration files and Trial mode/Automatic Save

In "Automatic Save" mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.

In "Trial" mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

CLI commands for saving and loading files cannot be executed with the CLI script file (Script).

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
You assign the password in the WBM under "System > Load&Save > Passwords".

You can use the file types as follows:

- For offline diagnostics
You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters

Load and Save via HTTP

HTTP TFTP SFTP Passwords

| Type | Description | Load | Save | Delete |
|---------------------|--|------|------|--------|
| Config | Startup Configuration | Load | Save | |
| ConfigPack | Startup Config, Users, Certificates and WBM favourites | Load | Save | |
| Debug | Debug Information for Siemens Support | | Save | Delete |
| Firmware | Firmware Update | Load | Save | |
| HTTPSCert | HTTPS Certificate | Load | Save | Delete |
| LogFile | Event, Security, Firewall Logs | | Save | |
| MIB | SCALANCE M MSPS MIB | | Save | |
| ModemQualityLog | Modem Quality Log | | Save | Delete |
| RunningCLI | 'show running-config all' CLI settings | | Save | |
| RunningSINEMAConfig | SINEMA Running Configuration | | Save | |
| Script | Script | Load | | |
| SINEMAConfig | SINEMA Offline Configuration | Load | | |
| StartupInfo | Startup Information | | Save | |
| Users | Users and Passwords | Load | Save | |
| WBM Fav | WBM favourite pages | Load | Save | Delete |
| X509Cert | X509 Certificates | Load | Save | |

Refresh

Description

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.
- **Load**
With this button, you can upload files to the device. The button can be enabled, if this function is supported by the file type.
- **Save**
With this button, you can download files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.
- **Delete**
With this button, you can delete files from the device. The button can only be enabled if this function is supported by the file type and the file exists on the device.

Note

Following a firmware update, delete the cache of your Internet browser.

Procedure

Uploading data using HTTP

1. Start the upload function by clicking one of the "Load" buttons.

Note

Files whose access is password protected

To save and load these files on the device successfully, you need to enter the password specified for the file in "System" > "Load&Save" > "Passwords".

A dialog for uploading a file opens.

2. Select the required file and confirm the upload.
The file is uploaded.
3. If a restart is necessary, a message to this effect will be output. Click the "OK" button and run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Note

Cell firmware update M87x

After a cell firmware update, the device automatically restarts

Downloading data using HTTP

1. Start the download by clicking the one of the "Save" buttons.
2. Select a storage location and a name for the file.
3. Save the file.
The file is downloaded and saved.

Deleting files using HTTP

1. Start the delete function by clicking the one of the "Delete" buttons.
The file is deleted.

Reusing configuration data

If several devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for configuration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. Load these configuration files on all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note

Configuration data has a checksum. If you edit the files, you can no longer upload them to the IE switch.

4.5.4.3 TFTP**Loading and saving data via a TFTP server**

On this page, you can configure the TFTP server and the file names. The WBM also allows you to store device data in an external file on your client PC or to load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located on your Admin PC.

On this page, the certificates required to establish a secure VPN connection can also be loaded.

Firmware

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

Configuration files

Note

Configuration files and Trial mode/Automatic Save

In "Automatic Save" mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.

In "Trial" mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

CLI commands for saving and loading files cannot be executed with the CLI script file (Script).

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
You assign the password in the WBM under "System > Load&Save > Passwords".

You can use the file types as follows:

- For offline diagnostics
You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters

Load and Save via TFTP

HTTP | **TFTP** | SFTP | Passwords

TFTP Server Address:

TFTP Server Port:

| Type | Description | Filename | Actions |
|---------------------|--|------------------------------|-----------------|
| Config | Startup Configuration | config_SCALANCE_M800.conf | Select action ▼ |
| ConfigPack | Startup Config, Users, Certificates and WBM favourites | configpack_SCALANCE_M800.zip | Select action ▼ |
| Debug | Debug Information for Siemens Support | debug_SCALANCE_M800.bin | Select action ▼ |
| Firmware | Firmware Update | firmware_SCALANCE_M800.sfw | Select action ▼ |
| HTTPSCert | HTTPS Certificate | https_cert | Select action ▼ |
| LogFile | Event, Security, Firewall Logs | logfile_SCALANCE_M800.zip | Select action ▼ |
| MIB | SCALANCE M MSPS MIB | scalance_m_mspms.mib | Select action ▼ |
| ModemQualityLog | Modem Quality Log | modem_quality.log | Select action ▼ |
| RunningCLI | 'show running-config all' CLI settings | RunningCLI.txt | Select action ▼ |
| RunningSINEMAConfig | SINEMA Running Configuration | sinema_config_running.zip | Select action ▼ |
| Script | Script | Script.txt | Select action ▼ |
| SINEMAConfig | SINEMA Offline Configuration | sinema_config.zip | Select action ▼ |
| StartupInfo | Startup Information | startup_SCALANCE_M800.log | Select action ▼ |
| Users | Users and Passwords | users.enc | Select action ▼ |
| WBM Fav | WBM favourite pages | wbmfav.txt | Select action ▼ |
| X509Cert | X509 Certificates | x509_certs.zip | Select action ▼ |

Description

The page contains the following boxes:

- **TFTP Server Address**
Enter the IP address or the FQDN (Fully Qualified Domain Name) of the TFTP server with which you exchange data.
- **TFTP Server Port**
Enter the port of the TFTP server via which data exchange will be handled. If necessary, you can change the default value 69 to your own requirements.

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.

4.5 "System" menu

- **Filename**
A file name is preset here for every file type.

Note**Changing the file name**

You can change the file name preset in this column. After loading on the device, the changed file name can also be used with the Command Line Interface.

- **Actions**
Select the action from the drop-down list. The selection depends on the selected file type, for example, the log file can only be saved.
The following actions are possible:
 - **Save file**
With this action, you can download a file from the TFTP server.
 - **Upload file**
With this action, you can upload a file to the TFTP server.

Procedure

Loading or saving data using TFTP

1. Enter the address of the TFTP server in "TFTP server address".
2. Enter the port of the TFTP server to be used in "TFTP Server Port".
3. If applicable, enter the name of a file in which you want to save the data or take the data from in "Filename".

Note**Files whose access is password protected**

To save and load these files on the device successfully, you need to enter the password specified for the file in "System" > "Load&Save" > "Passwords".

4. Select the action you want to execute from the "Actions" drop-down list.
5. Click "Set Values" to start the selected action.
6. If a restart is necessary, a message to this effect will be output. Click the "OK" button to run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Note**Cell firmware update M87x**

After a cell firmware update, the device automatically restarts

Reusing configuration data

If several identical devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for reconfiguration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. Load these configuration files on all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note

Configuration data has a checksum. If you change the data, you can no longer upload it to the device.

4.5.4.4 SFTP

Loading and saving data via an SFTP server

SFTP (SSH File Transfer Protocol) transfers the files encrypted. On this page, you configure the access data for the SFTP server.

You can also store device data in an external file on your client PC or load such data from an external file from the PC to the devices. This means, for example, that you can also load new firmware from a file located on your Admin PC.

On this page, the certificates required to establish a secure VPN connection can also be loaded.

Firmware

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

Configuration files

Note**Configuration files and Trial mode/Automatic Save**

In "Automatic Save" mode, the data is saved automatically before the configuration files (ConfigPack and Config) are transferred.

In "Trial" mode, although the changes are adopted, they are not saved in the configuration files (ConfigPack and Config). Use the "Write Startup Config" button on the "System > Configuration" WBM page to save changes in the configuration files.

CLI script file

You can download existing CLI configurations (RunningCLI) and upload your own CLI scripts (Script).

Note

The downloadable CLI script is not intended to be uploaded again unchanged.

CLI commands for saving and loading files cannot be executed with the CLI script file (Script).

4.5 "System" menu

Exchange of configuration data with STEP 7 Basic/Professional using a file

You use the two file types "RunningSINEMAConfig" and "SINEMAConfig" to exchange configuration data between a device (WBM) and STEP 7 Basic/Professional via a file.

Requirements:

- Same article number
- Same firmware version
- Password
You assign the password in the WBM under "System > Load&Save > Passwords".

You can use the file types as follows:

- For offline diagnostics
You can save the faulty configuration of a device as "RunningSINEMAConfig" via the WBM and import it in STEP 7 Basic/Professional. No connection to a real device is required for the diagnostics in STEP 7 Basic/Professional. You can export a corrected configuration and load it as "SINEMAConfig" again using the WBM.
- For configuration
No connection to a real device is required to configure a device in STEP 7 Basic/Professional. You can export the configuration and load it as "SINEMAConfig" to the real device using the WBM.

X509 certificates

The following file types can be loaded into the device:

- .crt, pem, zip: Maximum file name length 255 characters
- .p12: Maximum file name length 248 characters

Load and Save via SFTP

HTTP | TFTP | SFTP | Passwords

SFTP Server Address:

SFTP Server Port:

SFTP User:

SFTP Password:

SFTP Password Confirmation:

| Type | Description | Filename | Actions |
|---------------------|--|------------------------------|-----------------|
| Config | Startup Configuration | config_SCALANCE_M800.conf | Select action ▼ |
| ConfigPack | Startup Config, Users, Certificates and WBM favourites | configpack_SCALANCE_M800.zip | Select action ▼ |
| Debug | Debug Information for Siemens Support | debug_SCALANCE_M800.bin | Select action ▼ |
| Firmware | Firmware Update | firmware_SCALANCE_M800.sfw | Select action ▼ |
| HTTPSCert | HTTPS Certificate | https_cert | Select action ▼ |
| LogFile | Event, Security, Firewall Logs | logfile_SCALANCE_M800.zip | Select action ▼ |
| MIB | SCALANCE M MSPS MIB | scalance_m_mspms.mib | Select action ▼ |
| ModemQualityLog | Modem Quality Log | modem_quality.log | Select action ▼ |
| RunningCLI | 'show running-config all' CLI settings | RunningCLI.txt | Select action ▼ |
| RunningSINEMAConfig | SINEMA Running Configuration | sinema_config_running.zip | Select action ▼ |
| Script | Script | Script.txt | Select action ▼ |
| SINEMAConfig | SINEMA Offline Configuration | sinema_config.zip | Select action ▼ |
| StartupInfo | Startup Information | startup_SCALANCE_M800.log | Select action ▼ |
| Users | Users and Passwords | users.enc | Select action ▼ |
| WBM Fav | WBM favourite pages | wbmfav.txt | Select action ▼ |
| X509Cert | X509 Certificates | x509_certs.zip | Select action ▼ |

Description

The page contains the following boxes:

- **SFTP Server Address**
Enter the IP address or the FQDN of the SFTP server with which you exchange data.
- **SFTP Server Port**
Enter the port of the SFTP server via which data exchange will be handled. If necessary, you can change the default value 22 to your own requirements.
- **SFTP User**
Enter the user for access to the SFTP server. This assumes that a user with the corresponding rights has been created on the SFTP server.
- **SFTP Password**
Enter the password for the user
- **SFTP Password Confirmation**
Confirm the password.

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.
- **Filename**
A file name is preset here for every file type.

Note

Changing the file name

You can change the file name preset in this column. After loading on the device, the changed file name can also be used with the Command Line Interface.

- **Actions**
Select the action from the drop-down list. The selection depends on the selected file type, for example you can only save the log file.
The following actions are possible:
 - **Save file**
With this action, you can download a file from the SFTP server.
 - **Upload file**
With this action, you can upload a file to the SFTP server.

Procedure

Loading or saving data using SFTP

1. Enter the address of the SFTP server in "SFTP Server Address".
2. Enter the port of the SFTP server to be used in "SFTP Server Port".
3. Enter the user data (user name and password) required for access to the SFTP server.

4.5 "System" menu

4. If applicable, enter the name of a file in which you want to save the data or take the data from in "Filename".

Note

Files whose access is password protected

To save and load these files on the device successfully, you need to enter the password specified for the file in "System" > "Load&Save" > "Passwords".

5. Select the action you want to execute from the "Actions" drop-down list.
6. Click "Set Values" to start the selected action.
7. If a restart is necessary, a message to this effect will be output. Click the "OK" button to run the restart. If you click the "Abort" button, there is no device restart. The changes only take effect after a restart.

Note

Cell firmware update M87x

After a cell firmware update, the device automatically restarts

Reusing configuration data

If several identical devices are to receive the same configuration and the IP addresses are assigned using DHCP, the effort for reconfiguration can be reduced by saving and reading in the configuration data.

Follow the steps below to reuse configuration data:

1. Save the configuration data of a configured device on your PC.
2. Load these configuration files on all other devices you want to configure in this way.
3. If individual settings are necessary for specific devices, these must be made online on the relevant device.

Note

Configuration data has a checksum. If you change the data, you can no longer upload it to the IE switch.

4.5.4.5 Passwords

There are files to which access is password protected. To successfully load the file into the device, enter the password specified for the file on the WBM page.

Passwords

HTTP | TFTP | SFTP | Passwords

| Type | Description | Setting | Password | Password Confirmation | Status |
|---------------------|--|--------------------------|----------|-----------------------|----------|
| Config | Startup Configuration | <input type="checkbox"/> | | | - |
| ConfigPack | Startup Config, Users, Certificates and WBM favourites | <input type="checkbox"/> | | | - |
| HTTPSCert | HTTPS Certificate | <input type="checkbox"/> | | | - |
| LoginWelcomeMessage | Login Welcome Message | <input type="checkbox"/> | | | - |
| RunningSINEMAConfig | SINEMA Running Configuration | <input type="checkbox"/> | | | Required |
| SINEMAConfig | SINEMA Offline Configuration | <input type="checkbox"/> | | | Required |
| X509Cert | X509 Certificates | <input type="checkbox"/> | | | - |

Description

The table has the following columns:

- **Type**
Shows the file type.
- **Description**
Shows the short description of the file type.
- **Setting**
Can only be enabled if a password is configured.
When enabled, a check is made during loading to ensure that the password matches the password set for the file.
- **Password**
Enter the password for the file.
- **Password Confirmation**
Confirm the new password.
- **Status**
 - "-"
No password is specified or the password is enabled but no file is loaded yet.
 - Valid
The password is used and matches the file.
 - Invalid
The password is used, but the password does not match the file.
 - Required
A password is required for loading or saving.

4.5 "System" menu

Procedure

1. Enter the password in "Password".
2. To confirm the password, enter the password again in "Password Confirmation".
3. Select the "Enabled" option.
4. Click the "Set Values" button.

4.5.5 Events

4.5.5.1 Event Configuration

Selecting system events

On the WBM page, you define which system events are reported and how, or execute a follow-up reaction.

The following messages are always entered in the event log table and cannot be deselected:

- Changing the admin password
- Starting the device
- Operational status of the device, e.g. whether or not a PLUG is inserted
- Status of errors not yet dealt with

To send these messages to a Syslog server as well, select the "Syslog" check box for the event "System General Logs".

Event Configuration

Configuration Severity Filters

| | E-mail | Trap | Log Table | Syslog | Fault | SMS | Digital Out | VPN Tunnel | Cloud Connector | Firewall | Copy To Table |
|--------------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|---------------|
| All Events | No Change ▼ | No Change ▼ | No Change ▼ | No Change ▼ | No Change ▼ | No Change ▼ | No Change ▼ | No Change ▼ | No Change ▼ | No Change ▼ | Copy To Table |
| Event | E-mail | Trap | Log Table | Syslog | Fault | SMS | Digital Out | VPN Tunnel | Cloud Connector | Firewall | |
| Cold/Warm Start | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | | | |
| Link Change | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | | | |
| Authentication Failure | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | | | |
| Fault State Change | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | | |
| Security Logs | | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | |
| Firewall Logs | | | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | |
| DDNS Client Logs | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | | | | | |
| System General Logs | | | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | | | | | |
| System Connection Status | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | | | | | |
| Digital In | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| VPN Tunnel | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | | | |
| Secure NTP | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | | | | | |
| Cloud Connector | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | | | | | |
| Configuration Change | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | | | | | |
| Service Information | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | | | | | |
| Mobile Data Usage | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | | | | | |

Description

With Table 1, you can enable or disable all check boxes of a column of Table 2 at once.

Table 1 has the following columns:

- **All Events**
Shows that the settings are valid for all events of table 2.
- **E-mail / Trap / Log Table / Syslog / Fault / SMS / Digital Out / VPN Tunnel / Cloud Connector / Firewall**
Enable or disable the required type of notification for all events. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy To Table**
If you click the button, the setting is adopted for all events of table 2.

Table 2 has the following columns:

- **Event**

The "Event" column contains the following:

- Cold/Warm Start
The device was turned on or restarted by the user. In the error memory of the device a new entry is generated with the type of restart performed.
- Link Change
This event occurs only when the port status is monitored and has changed, see "System > Fault Monitoring > Link Change".
- Authentication Failure
This event occurs when access is attempted with an incorrect password.
- Fault State Change
The fault status has changed. The fault status can relate to the activated port monitoring, the response of the digital output or the power supply monitoring.
For a fault to also be signaled by the fault LED "F", you must enable "Fault State Change" for the "Digital Out". In this case, the fault LED "F" lights up when an internal error occurs and the digital input is closed.
- Security Logs
An entry is made in the security log if the IPsec method was used for VPN.
- Firewall Logs
Each time individual firewall rules are applied, this is recorded in the firewall log. To do this, the LOG function must be enabled for the various firewall functions.
- DDNS Client Logs
The event occurs when the DDNS client synchronizes the assigned IP address with the hostname registered at the DDNS provider.
- System General Logs
Connection establishment, change to the configuration.
- System Connection Status
The connection status has changed.
- Digital In
The event occurs when the status of the digital input has changed.
- VPN Tunnel
The event occurs when the status of VPN (IPsec, OpenVPN, SINEMA RC) has changed.
- Secure NTP
This event occurs when the device receives the system time from a secure NTP server.
- Cloud Connector
This event occurs when the operating state of the Cloud Connector has changed.
- Configuration Change
This event occurs when the configuration of the device has changed.
- Service Information
For certain events, entries are made in the log table even without configuration. For these events, you can configure additional subsequent actions here (e-mail, trap, syslog).

- Mobile data usage (only with M87x)
This event occurs when 75% or 100% of the defined data volume has been reached, see "Interfaces > Mobile > General".
- Connection Check
This event occurs when connections are being monitored, see "System > Connection Check".
- **E-mail**
The device sends an e-mail. This is only possible if the SMTP server is set up and the "SMTP client" function is enabled.
- **Trap**
The device sends an SNMP trap. This is only possible if "SNMPv1 Traps" is enabled in "System > Configuration".
- **Log Table**
The device writes an entry in the event log table, see "Information > Log Table"
- **Syslog**
The device writes an entry to the system log server. This is only possible if the system log server is set up and the "Syslog client" function is enabled.
- **Faults**
The device triggers an error. The error LED lights up and the currently pending error is displayed under "Information > Faults".
- **SMS** (only with M87x)
The device sends an SMS. This is only possible if "System > SMS > Event SMS" is enabled and the telephone number of the recipient is configured.
- **Digital Out**
Controls the digital output or signals the status change with the "DO" LED.
The digital output is closed by default. The digital output is opened when you activate at least one event for the digital output. It also is no longer automatically connected to the fault LED. You connect the digital output with the fault LED under "Fault State Change".
- **VPN Tunnel**
Controls the forwarding of an event to a VPN connection (IPsec, OpenVPN, SINEMA RC). As long as the event is present, the VPN connection is switched to active.
- **Firewall**
Controls application of the user-defined rule set. This requires a rule set to be assigned to the digital input under "Security > Firewall >".
- **Cloud Connector**
Controls the forwarding of an event to the TIA Portal Cloud Connector communication. The communication connection is active as long as the event is present.

Procedure

Establishing/terminating a VPN tunnel via the digital input

1. For the "Digital Input" event, enable the "VPN Tunnel" entry.
2. Configure the VPN connection
 - IPsec:
In "Operation" set "wait on DI" or "start on DI". You will find more information on this in "IPsec > Connections" and in "VPN connection establishment".
 - OpenVPN:
In "Operation" set "start on DI". You will find more information on this in "OpenVPN > Connections" and in "VPN connection establishment".
 - SINEMA RC:
In "Type of connection" set "Auto", "Digital In" or "Digital Input & Wake up SMS" (only with M87x). With "Type of connection" "Auto", on the SINEMA RC Server you need to set the type of connection "Digital In" or "Wake up SMS & digital input (only with M87x)" in "Remote connections". You will find further information on this topic in the operating instructions "SINEMA RC Server".
3. Click the "Set Values" button.

4.5.5.2 Severity Filters

On this page, you configure the severity for the sending of system event notifications.

| Client Type | Severity |
|-------------|----------|
| E-mail | Info |
| Log Table | Info |
| Syslog | Info |

Description

The table has the following columns:

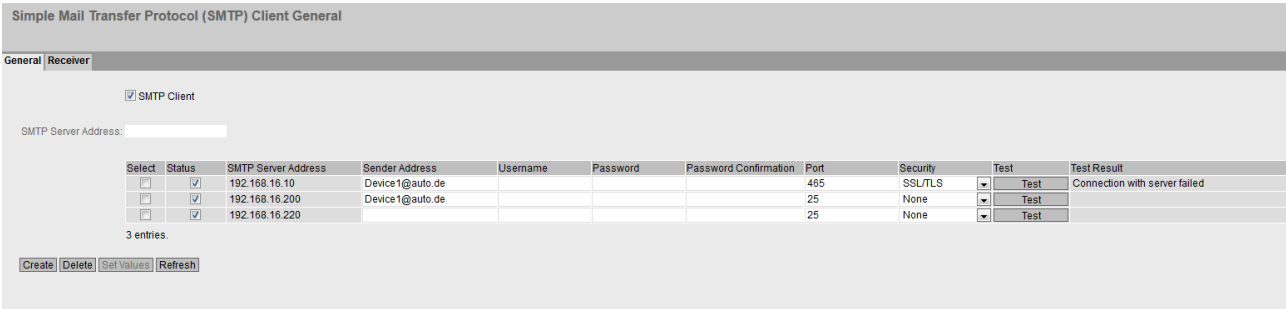
- **Client Type**
Select the client type for which you want to make settings:
 - **E-mail**
Sending system event messages by e-mail.
 - **Log Table**
Entry of system events in the log table.
 - **Syslog**
Entry of system events in the Syslog file.
- **Severity**
Select the required severity. The following settings are possible:
 - **Info**
The messages of all severities are sent or logged.
 - **Warning**
The messages of this severity and the "critical" severity are sent or logged.
 - **Critical**
Only the messages of this severity are sent or logged.

4.5.6 SMTP client

4.5.6.1 General

Network monitoring with e-mails

If events occur, the device can automatically send an e-mail, e.g. to the service technician. The e-mail contains the identification of the sending device, a description of the cause in plain text, and a time stamp. This allows centralized network monitoring to be set up for networks with few nodes based on an e-mail system.



Requirements for sending e-mails

- "E-mail" is activated for the relevant event in "System > Events > Configuration".
- The desired severity is configured under "System > Events > Severity level".
- At least one entry exists under "System > SMTP Client > Receiver" and the setting "Send" is activated.

Description

The page contains the following boxes:

- **SMTP Client**
Enable or disable the SMTP client.
- **SMTP Server Address**
Enter the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server.

The table contains the following columns:

- **Select**
Select the check box in a row to be deleted.
- **Status**
Specify whether this SMTP server will be used.
- **SMTP Server Address**
Shows the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server.
- **Sender Email Address**
Enter the e-mail address of the sender that is specified in the e-mail.
- **User Name**
If necessary, enter the user name used for authentication on the SMTP server.
- **Password**
If necessary, enter the password used for authentication on the SMTP server.
- **Password Confirmation**
Repeat the password.
- **Port**
Enter the port via which your SMTP server can be reached.
Factory settings:
 - 25 (None)
 - 465 (SSL/TLS and StartTLS)

- **Security**
Specify whether transfer of the e-mail from the device to the SMTP server is encrypted. This is only possible when the SMTP server supports the selected setting.

Note**2-factor authentication (2FA)**

2-factor authentication is not supported.

- SSL/TLS
- StartTLS
- None: The e-mail is transferred unencrypted.

- **Test**
Sends a test email to the configured receivers.
- **Test Result**
Shows whether the e-mail was sent successfully or not. If sending was not successful, the message contains possible causes.

Procedure

Configuring the SMTP server

1. Enable the "SMTP Client" function.
2. Enter the IP address or the FQDN of the SMTP server for "SMTP Server Address".
3. Click the "Create" button. A new entry is generated in the table.
4. Enter the name of the sender that will be included in the e-mail for "Sender Email Address".
5. Enter the user name and password if the SMTP server prompts you to log in.
6. Under "Security", specify whether transfer to the SMTP server is encrypted.
7. Enable the SMTP server entry.
8. Click the "Set Values" button.

Note

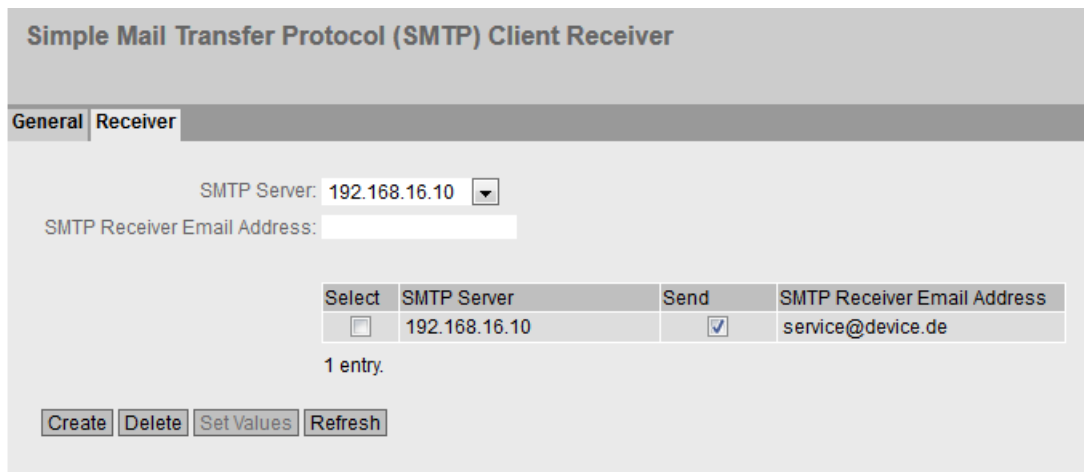
Depending on the properties and configuration of the SMTP server, it may be necessary to adapt the "Sender E-Mail Address" input for the e-mails. Check with the administrator of the SMTP server.

Testing the configuration of the SMTP server

1. Configure receivers
 - Click the "Receiver" tab.
 - Select the desired SMTP server under "SMTP server".
 - Enter the desired address under "E-mail address of the SMTP recipient".
 - Click the "Create" button. A new entry is generated in the table. The setting "Send" is enabled by default.
2. Sending a test e-mail
 - Click the "General" tab.
 - Click the "Test" button next to the SMTP server entry. The device sends a test email to every configured receiver.
 - Check the test result. If sending was not successful, the message contains possible causes.

4.5.6.2 Recipient

On this page, you specify who receives an e-mail when an event occurs.



Description

The page contains the following boxes:

- **SMTP Server**
Specify the SMTP server via which the e-mail is sent.
- **Email address of the SMTP receiver**
Enter the e-mail address to which the device sends an e-mail.

The table contains the following columns:

- **Select**
Select the check box in a row to be deleted.
- **SMTP Server**
Shows the IP address or the FQDN (Fully Qualified Domain Name) of the SMTP server to which the entry relates.
- **Send**
When enabled, the device sends an email to this receiver.
- **Email address of the SMTP receiver**
Shows the e-mail address to which the device sends an e-mail if a fault occurs.

Procedure

Configuring an SMTP receiver

1. Select the required "SMTP server".
2. Enter the email address of the SMTP receiver.
3. Click the "Create" button. A new entry is generated in the table.
4. Activate the "Send" option for the entry.
5. Click the "Set Values" button.

4.5.7 SNMP

4.5.7.1 General

Configuration of SNMP

Note

SNMPv3 configuration during a firmware update

As of firmware version 6.4, the SNMP configuration has been distributed across multiple WBM pages.

To delete the SNMPv3 configuration, follow these steps:

1. Delete all SNMPv3 views except for the predefined views **SIMATICNETRD** and **SIMATICNETWR**.
 2. Delete all SNMPv3 access.
 3. Delete all entries in the "SNMPv3 User to Group mapping" table.
 4. Delete all SNMPv3 users.
-

On this page, you make the basic settings for SNMP. Enable the check boxes according to the function you want to use.

Simple Network Management Protocol (SNMP) General

| | | | | | |
|----------------|---------------------|-------------------------------------|----------------------|---------------------|----------------------|
| General | SNMPv3 Users | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications |
|----------------|---------------------|-------------------------------------|----------------------|---------------------|----------------------|

SNMP: ▼

SNMPv1/v2c Read Only

SNMPv1/v2c Read Community String:

SNMPv1/v2c Read/Write Community String:

SNMPv3 User Migration

SNMP Engine ID:

SNMP Agent Listen Port:

Description

The page contains the following boxes:

- **SNMP**
 Select the SNMP protocol from the drop-down list. The following settings are possible:
 - "-" (Disabled)
SNMP is disabled.
 - SNMPv1/v2c/v3
SNMPv1/v2c/v3 is supported.

Note

Note that SNMP in versions 1 and 2c does not have any security mechanisms.

- SNMPv3
Only SNMPv3 is supported.
- **SNMPv1/v2c Read-Only**
 If you enable this option, SNMPv1/v2c can only read the SNMP variables.

Note

Community String

For security reasons, do not use the standard values "public" or "private". Change the community strings following the initial installation.

The recommended minimum length for community strings is 6 characters.

For security reasons, only limited access to objects of the SNMPCommunityMIB is possible with the SNMPv1/v2c Read Community String. With the SNMPv1/v2c Read/Write Community String, you have full access to the SNMPCommunityMIB.

- **SNMPv1/v2c Read Community String**
Enter the community string for read access of the SNMP protocol.
- **SNMPv1/v2c Read/Write Community String**
Enter the community string for read and write access of the SNMP protocol.
- **SNMPv3 User Migration**
 - **Enabled**
If the function is enabled, an SNMP engine ID is generated that can be migrated. You can transfer configured SNMPv3 users to a different device.
If you enable this function and load the configuration of the device on another device, configured SNMPv3 users are retained.
 - **Disabled**
If the function is disabled, a device-specific SNMP engine ID is generated. To generate the ID, the agent MAC address of the device is used. You cannot transfer this SNMP user configuration to other devices.
If you load the configuration of the device on another device, all configured SNMPv3 users are deleted.
- **SNMP Engine ID**
Shows the SNMP engine ID.
- **SNMP Agent Listen Port**
Specify the port at which the SNMP agent waits for the SNMP queries. Standard port 161 is the default. You can optionally enter the standard port 162 or a port number in the range 1024 ... 49151 or 49500 ... 65535.

Procedure

1. Select the required option from the "SNMP" drop-down list:
 - "-" (disabled)
 - SNMPv1/v2c/v3
 - SNMPv3
2. Enable the "SNMPv1/v2c Read Only" check box if you only want read access to SNMP variables with SNMPv1/v2c.
3. Enter the required character string in the "SNMPv1/v2c Read Community String" input box.
4. Enter the required character string in the "SNMPv1/v2c Read/Write Community String" input box.
5. If necessary, enable the SNMPv3 User Migration.
6. Click the "Set Values" button.

4.5.7.2 SNMPv3 Users

User-specific security settings

On the WBM page, you can create new SNMPv3 users and modify or delete existing users. The user-based security model works with the concept of the user name; in other words, a user ID is added to every frame. This user name and the applicable security settings are checked by both the sender and recipient.

| Select | User Name | Authentication Protocol | Privacy Protocol | Authentication Password | Authentication Password Confirmation | Privacy Password | Privacy Password Confirmation |
|--------------------------|-----------|-------------------------|------------------|-------------------------|--------------------------------------|------------------|-------------------------------|
| <input type="checkbox"/> | Miller | MD5 | DES | ***** | ***** | ***** | ***** |

1 entry.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Description

The page contains the following boxes:

- **User Name**
Enter a freely selectable user name. After you have entered the data, you can no longer modify the name.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **User Name**
Shows the created users.
- **Authentication Protocol**
Specify the authentication protocol for which a password will be stored. The following settings are available:
 - None
 - MD5
 - SHA
- **Privacy Protocol**
Specify the encryption protocol for which a password will be stored. This drop-down list is only enabled when an authentication protocol has been selected. The following settings are available:
 - None
 - DES
 - AES

- **Authentication Password**
Enter the authentication password in the first input box. This password must have at least 1 character, the maximum length is 32 characters.

Note**Length of the password**

As an important measure to maximize security, we recommend that the password has a minimum length of 6 characters and that it contains special characters, uppercase/lowercase letters, numbers.

- **Authentication Password Confirmation**
Confirm the password by repeating the entry.
- **Privacy Password**
Enter your encryption password. This password must have at least 1 character, the maximum length is 32 characters.

Note**Length of the password**

As an important measure to maximize security, we recommend that the password has a minimum length of 6 characters and that it contains special characters, uppercase/lowercase letters, numbers.

- **Privacy Password Confirmation**
Confirm the encryption password by repeating the entry.

Procedure

Create a new user

1. Enter the name of the new user in the "User Name" input box.
2. Click the "Create" button. A new entry is generated in the table.
3. Select the authentication algorithm for "Authentication Protocol". In the relevant input boxes, enter the authentication password and the confirmation.
4. Select the algorithm in "Privacy Protocol". In the relevant input boxes, enter the encryption password and the confirmation.
5. Click the "Set Values" button.

Delete user

1. Enable "Select" in the row to be deleted.
Repeat this for all users you want to delete.
2. Click the "Delete" button. The entry is deleted.

4.5.7.3 SNMPv3 User to Group mapping

Configuration of group members

You assign users to SNMPv3 groups on this WBM page. Each user can only be a member of one group.

Simple Network Management Protocol (SNMP) v3 Groups

| | | | | | |
|---------|--------------|------------------------------|---------------|--------------|---------------|
| General | SNMPv3 Users | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications |
|---------|--------------|------------------------------|---------------|--------------|---------------|

Group Name:

User Name:

| Select | Group Name | User Name |
|--------------------------|------------|-----------|
| <input type="checkbox"/> | Service | Miller |

1 entry.

Description

The page contains the following boxes:

- **Group Name**
Enter the group that will be assigned to the user.
- **User Name**
Select the user to be a member of the specified group. The drop-down list only contains users that are not yet assigned to a group.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Group Name**
Displays the SNMPv3 group. A group name can only be changed later if no access rights have been defined for the group yet.
- **User Name**
Shows the user that is a member of this group.

4.5.7.4 SNMPv3 Access

Security settings and assigning permissions

SNMP version 3 allows permissions to be assigned, authentication, and encryption at protocol level. The security level and read/write permissions are assigned according to groups. The settings automatically apply to every member of a group.

Note

Different access permissions for different security levels can be assigned to a group. If no access permission is defined for a security level, no access to the device is possible for members of the group using this security level.

Simple Network Management Protocol (SNMP) v3 Access

| | | | | | |
|---------|--------------|------------------------------|----------------------|--------------|---------------|
| General | SNMPv3 Users | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications |
|---------|--------------|------------------------------|----------------------|--------------|---------------|

Group Name:

Security Level:

| Select | Group Name | Security Level | Read View Name | Write View Name | Notify View Name |
|--------------------------|------------|-----------------|----------------|-----------------|------------------|
| <input type="checkbox"/> | Service | no Auth/no Priv | SIMATICNETRD | SIMATICNETWR | SIMATICNETRD |

1 entry.

Description

The page contains the following boxes:

- **Group Name**
Select the name of the group.
- **Security Level**
Select the security level (authentication, encryption) for which you want to define the access permissions of the group:
 - **No Auth/no Priv**
No authentication enabled/no encryption enabled.
 - **Auth/no Priv**
Authentication enabled/no encryption enabled.
 - **Auth/Priv**
Authentication enabled/encryption enabled.

The table has the following columns:

- **Select**
Select the row you want to delete.
 - **Group Name**
Shows the name of the SNMPv3 group.
 - **Security Level**
Shows the security level to which this access permission applies.
 - **Read View Name**
Enter an SNMPv3 view to be used for read SNMP access by members of the group with the defined security level.
 - **Write View Name**
Enter an SNMPv3 view to be used for write SNMP access by members of the group with the defined security level.
-

Note

For write access to work, you also need to enable read access.

- **Notification View Name**
Enter an SNMPv3 view for which SNMP notification to members of the group with the defined security level should be used.

Procedure

Creating a new group

1. Select the name of the group for which you are configuring SNMP access.
2. Select the required security level from the "Security Level" drop-down list.
3. Click the "Create" button to create a new entry.
4. In the "Read View Name" field, enter the SNMPv3 view for read access.
5. In the "Write View Name" field, enter the SNMPv3 view for write access.
6. In the "Notification View Name" field, enter the SNMPv3 view for notifications.
7. Click the "Set Values" button.

Modifying a group

Once a group name and the security level have been specified, they can no longer be modified after the group is created. If you want to change the group name or the security level, you will need to delete the group and create it and configure it with the new name.

Deleting a group

1. Enable "Select" in the row to be deleted.
Repeat this for all groups you want to delete.
2. Click the "Delete" button. The entries are deleted.

4.5.7.5 SNMPv3 Views

Configuration of SNMPv3 views

You configure the parameters of SNMP views on this WBM page.

Simple Network Management Protocol (SNMP) v3 Views

General | **SNMPv3 Users** | SNMPv3 User to Group mapping | SNMPv3 Access | **SNMPv3 Views** | Notifications

View Name:

MIB Tree:

| Select | View Name | MIB Tree | View Type |
|--------------------------|--------------|--|-----------|
| <input type="checkbox"/> | MY_RD | org | Included |
| <input type="checkbox"/> | MY_RD | private | Included |
| <input type="checkbox"/> | MY_WR | 1.3.6.1.3.6.18.1.1.1.1.83.73.77 | Included |
| <input type="checkbox"/> | SIMATICNETRD | iso | Included |
| <input type="checkbox"/> | SIMATICNETRD | 1.3.6.1.6.3.18.1.1 | Excluded |
| <input type="checkbox"/> | SIMATICNETRD | 1.3.6.1.6.3.18.1.1.1.1.83.73.77.65.84.73.67.78.69.84.82.68 | Included |
| <input type="checkbox"/> | SIMATICNETWR | iso | Included |

7 entries.

Note
Controlling the SNMPv1 and SNMPv2c access

The preconfigured **SIMATICNETRD** and **SIMATICNETWR** views are used internally to control the SNMPv1 and SNMPv2c access. If you delete or change these views, this directly affects the SNMPv1 and SNMPv2c access.

Description

The page contains the following boxes:

- **View Name**
Select the name of the view that you want to configure. An SNMPv3 view always needs to be assigned to an SNMPv3 access. For this reason, you need to enter a new SNMPv3 view in the table in the "SNMP Access" tab.
- **MIB Tree**
Select the Object Identifier (OID) of the MIB area that is to be used for the SNMPv3 view. The following options are possible:
 - iso
 - std
 - member-body
 - org
 - mgmt
 - private
 - snmpV2

The drop-down list only contains the OIDs that are usually used. If the configuration of a specific OID that is not listed is necessary, you can configure this via the CLI with the `snmp view` command. This OID is then also displayed in the WBM in the overview table.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **View Name**
The name of the SNMPv3 view.
- **MIB Tree**
The OID of the MIB area for the SNMPv3 view.
- **View Type**
The available options are as follows:
 - **Included**
The MIB OID and its lower-level nodes are part of the SNMPv3 view. Access to the corresponding MIB objects is possible.
 - **Excluded**
The MIB OID and its lower-level nodes are not part of the SNMPv3 view. Access to the corresponding MIB objects is not possible.

4.5.7.6 Notifications

SNMP traps and SNMPv3 notifications

If an alarm event occurs, a device can send SNMP notifications (traps and inform notifications) to up to ten different management stations at the same time. Notifications are only sent if the events specified in the "Events" menu item occur.

Simple Network Management Protocol (SNMP) Notifications

General | **SNMPv3 Users** | SNMPv3 User to Group mapping | SNMPv3 Access | SNMPv3 Views | Notifications

SNMPv1 Traps

SNMPv1/v2c Trap Community String:

SNMPv3 Notify User:

SNMPv3 Notify Security Level:

Notification Receiver Type:

Notification Receiver Address:

| Select | Notification Receiver Address | Notification Receiver Type | SNMP Engine ID | Notification |
|--------------------------|-------------------------------|----------------------------|----------------|--------------------------|
| <input type="checkbox"/> | 192.168.178.107 | SNMPv1 Trap | - | <input type="checkbox"/> |

1 entry.

Description

The page contains the following boxes:

- **SNMPv1 Traps**
Enable or disable sending of SNMPv1 traps. This setting affects all recipients of SNMPv1 traps and has no effects on recipients of SNMPv2c or SNMPv3 notifications.
- **SNMPv1/v2c Trap Community String**
Enter the community string for sending SNMPv1/v2c notifications.
- **SNMPv3 Notify User**
Select the user to which SNMPv3 notifications are to be sent.
- **SNMPv3 Notify Security Level**
Select the security level (authentication, encryption) to be used for SNMPv3 notification. The following options are possible:
 - no Auth/no Priv
No authentication enabled / no encryption enabled.
 - Auth/no Priv
Authentication enabled / no encryption enabled.
 - Auth/Priv
Authentication enabled / encryption enabled.

- **Notification Receiver Type**
The recipient type defines the SNMP version and the type of notification. SNMP inform notifications have to be acknowledged by the recipient, SNMP traps do not. The following options are possible:
 - SNMPv1 Trap
 - SNMPv2c Trap
 - SNMPv2c Inform
 - SNMPv3 Trap
 - SNMPv3 Inform
- **Notification Receiver Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the recipient station to which the device sends SNMP notifications. You can specify up to ten different recipients servers.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Notification Receiver Address**
If necessary, change the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the stations.
- **Notification Receiver Type**
Shows the defined receiver type.
- **SNMP Engine ID**
The ID of the SNMP engine to which SNMPv3 inform notifications are sent. You can only configure this parameter for the "SNMPv3-Inform" recipient type.
- **Notification**
Enable or disable sending of SNMP notifications. Stations that are entered but not selected do not receive SNMP notifications.

Note

If a table is grayed out, the corresponding notification was configured via the CLI and can only be deleted via the CLI.

Procedure

Configuring a notification

1. Select the recipient for SNMPv3 notifications in the "SNMPv3 Notify User" drop-down list.
2. Select the security level for SNMPv3 notifications in the "SNMPv3 Notify Security Level" drop-down list.
3. Select the recipient type in the "Notification Receiver Type" drop-down list.
4. In "Notification Receiver Address", enter the IP address, the FQDN or the host name of the station to which the device will send traps or notifications.
5. Click the "Create" button to create a new trap entry.

6. Activate "Notification" in the required row.
7. Click the "Set Values" button.

Deleting a trap entry

1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

4.5.8 System Time

There are different methods that can be used to set the system time of the device. Only one method can be active at any one time.

If one method is activated, the previously activated method is automatically deactivated.

4.5.8.1 Manual Setting

Manual setting of the system time

On this page, you set the date and time of the system yourself. For this setting to be used, enable "Time Manually".

The screenshot shows the 'Manual System Time Setting' web interface. At the top, there is a navigation bar with tabs: 'Manual Setting', 'DST Overview', 'DST Configuration', 'SNTP Client', 'NTP Client', 'SIMATIC Time Client', and 'NTP Server'. The 'Manual Setting' tab is selected. Below the navigation bar, there is a checkbox labeled 'Time Manually' which is checked. Underneath, the 'System Time' is displayed as '08/31/2018 12:27:05'. There is a button labeled 'Use PC Time'. Below that, the 'Last Synchronization Time' is shown as '08/29/2018 09:25:43'. The 'Last Synchronization Mechanism' is set to 'Manual'. The 'Daylight Saving Time' is set to 'active (offset + 1h)'. At the bottom, there are two buttons: 'Set Values' and 'Refresh'.

Description

The page contains the following boxes:

- **Time Manually**
Enable or disable the manual time setting. If you enable the option, the "System Time" input box can be edited.
- **System Time**
Enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
After a restart, the time of day begins at 01/01/2000 00:00:00
- **Use PC Time**
Click the button to use the time setting of the PC.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place. If no time-of-day synchronization was possible, the box displays "Date/time not set".
- **Last Synchronization Mechanism**
Shows how the last time synchronization was performed.
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
- **Daylight Saving Time**
Shows whether the daylight saving time changeover is active.
 - active (offset +1 h)
The system time was changed to daylight saving time; in other words, an hour was added. You can see the current system time at the top right in the selection area of the WBM. The set time continues to be displayed in the "System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.

Procedure

1. Enable the "Time Manually" option.
2. Click in the "System Time" input box.
3. In the "System Time" input box, enter the date and time in the format "MM/DD/YYYY HH:MM:SS".
4. Click the "Set Values" button.
The date and time are adopted and "Manual" is entered in "Last Synchronization Mechanism" box.

4.5.8.2 DST Overview

Daylight saving time switchover

On this page, you can create new entries for the daylight saving time changeover. The table provides an overview of the existing entries.

| Daylight Saving Time (DST) Overview | | | | | | | | |
|--|--------------|-------------------|-------------|-------------|---------------------|----------------|---------|------|
| Manual Setting | DST Overview | DST Configuration | SNTP Client | NTP Client | SIMATIC Time Client | NTP Server | | |
| Select | DST No | Name | Year | Start Date | End Date | Recurring Date | State | Type |
| <input type="checkbox"/> | 1 | DST 2018 | 2018 | 03/25 02:00 | 10/28 03:00 | - | enabled | Date |
| 1 entry. | | | | | | | | |
| <input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/> | | | | | | | | |

Settings

The page contains the following boxes:

- **Select**
Select the row you want to delete.
- **DST No.**
Shows the number of the entry.
If you create a new entry, a new line with a unique number is created.
- **Name**
Shows the name of the entry.
- **Year**
Shows the year for which the entry was created.
- **Start Date**
Shows the month, day and time for the start of daylight saving time.
- **End Date**
Shows the month, day and time for the end of daylight saving time.
- **Recurring Date**
With an entry of the type "Recurring", the period in which daylight saving time is active is displayed consisting of week, day, month and time of day.
With an entry of the type "Date" a "-" is displayed.

4.5 "System" menu

- **Status**
Shows the status of the entry:
 - Enabled
The entry was created correctly.
 - Invalid
The entry was created new and the start and end date are identical.
- **Type**
Shows how the daylight saving time changeover is made:
 - Date
A fixed date is entered for the daylight saving time changeover.
 - Recurring
A rule was defined for the daylight saving time changeover.

Procedure

Creating an entry

1. Click the "Create" button.
A new entry is created in the table.
2. Click on the required entry in the "DST No column."
You change to the "DST Configuration" page.
3. Select the required type in the "Type" drop-down list.
Depending on the selected type, various settings are available.
4. Enter a name name in the "Name" box.
5. If you have selected the type "Date", fill in the following boxes.
 - Year
 - Day (for start and end date)
 - Hour (for start and end date)
 - Month (for start and end date)
6. If you have selected the type "Recurring", fill in the following boxes.
 - Hour (for start and end date)
 - Month (for start and end date)
 - Week (for start and end date)
 - Day (for start and end date)
7. Click the "Set Values" button.

Deleting an entry

1. Enable "Select" in the row to be deleted.
2. Click the "Delete" button. The entry is deleted.

4.5.8.3 DST Configuration

Configuring the daylight saving time switchover

On this page, you can configure the entries for the daylight saving time changeover. As result of the changeover to daylight saving or standard time, the system time for the local time zone is correctly set.

You can define a rule for the daylight saving time changeover or specify a fixed date.

Settings

Note

The content of this page depends on the selection in the "Type" box.

The boxes "DST No.", "Type" and "Name" are always shown.

- **DST No.**
Select the type of the entry.
- **Type**
Select how the daylight saving time changeover is made:
 - Date
You can enter a fixed date for the daylight saving time changeover.
This setting is suitable for regions in which the daylight saving time changeover is not governed by rules.
 - Recurring
You can define a rule for the daylight saving time changeover.
This setting is suitable for regions in which the daylight saving time always begins or ends on a certain weekday.
- **Name**
Enter a name for the entry.
The name can be a maximum of 16 characters long.

Settings with "Date" selected

You can set a fixed date for the start and end of daylight saving time.

- **Year**
Enter the year for the daylight saving time changeover.
- **Start Date**
Enter the following values for the start of daylight saving time:
 - Day
Enter the day.
 - Hour
Enter the hour.
 - Month
Enter the month.
- **End Date**
Enter the following values for the end of daylight saving time:
 - Day
Enter the day.
 - Hour
Enter the hour.
 - Month
Enter the month.

Settings with "Recurring" selected

DST Configuration

Manual Setting | DST Overview | **DST Configuration** | SNTP Client | NTP Client | SIMATIC Time Client | NTP Server

DST No: 1
 Type: Recurring
 Name: DST 2018

Start Date End Date

Hour: 02:00 Hour: 03:00
 Month: March Month: October
 Week: First Week: First
 Day: Sunday Day: Sunday

Set Values Refresh

You can create a rule for the daylight saving time changeover.

- **Year**
Enter the year for the daylight saving time changeover.
- **Start Date**
Enter the following values for the start of daylight saving time:
 - Hour
Enter the hour.
 - Month
Enter the month.
 - Week
Enter the week.
You can select the first to fourth or the last week of the month.
 - Day
Enter the weekday.
- **End Date**
Enter the following values for the end of daylight saving time:
 - Hour
Enter the hour.
 - Month
Enter the month.
 - Week
Enter the week.
You can select the first to fourth or the last week of the month.
 - Day
Enter the weekday.

4.5.8.4 SNTP Client

Time-of-day synchronization in the network

SNTP (**Simple Network Time Protocol**) is used for synchronizing the time in the network. The appropriate frames are sent by an SNTP server in the network.

Note

To avoid time jumps, make sure that there is only one time server in the network.

Simple Network Time Protocol (SNTP) Client

Manual Setting
DST Overview
DST Configuration
SNTP Client
NTP Client
SIMATIC Time Client
NTP Server

SNTP Client

Current System Time: 08/31/2018 12:27:24

Last Synchronization Time: 08/29/2018 09:25:43

Last Synchronization Mechanism: Manual

Time Zone: +00:00

Daylight Saving Time: active (offset + 1h)

SNTP Mode: Poll

Poll Interval[s]: 64

SNTP Server Address:

| Select | SNTP Server Address | SNTP Server Port | Primary |
|--------------------------|---------------------|------------------|-------------------------------------|
| <input type="checkbox"/> | 192.168.1.1 | 123 | <input checked="" type="checkbox"/> |

1 entry.

Requirement

To receive the SNTP frames, enable the entry "System Time" under "Security > Firewall > Predefined IPv4 rules".

Description

The page contains the following boxes:

- **SNTP Client**
When enabled, the device receives the system time from an SNTP server.
- **Current System Time**
Shows the current date and current normal time received by the IE switch. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
Shows how the last time synchronization was performed. The following types are possible:
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
- **Time Zone**
In this box, enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time**
Shows whether the daylight saving time changeover is active.
 - active (offset +1 h)
The system time was changed to daylight saving time; in other words, an hour was added. You can see the current system time at the top right in the selection area of the WBM. The set time continues to be displayed in the "System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.

- **SNTP Mode**
Select the synchronization mode from the drop-down list. The following types are possible:
 - Poll
If you select this mode, the text boxes "SNTP Server Address", "SNTP Server Port" and "Poll Interval[s]" are displayed to allow further configuration. With this type of synchronization, the device is active and sends a time query to the SNTP server.
In this mode, IPv4 and IPv6 addresses are supported.
 - Listen
With this type of synchronization, the device is passive and receives SNTP frames that deliver the time of day. The settings in the text boxes "SNTP Server Address" and "SNTP Server Port" have no effect in this mode.
In this mode, IPv4 and IPv6 addresses are supported.

Note

SNTP Client in Listen mode and NTP Server cannot be enabled at the same time.

- **Poll Interval[s]**
Enter the interval between two time queries. In this box, you enter the polling interval in seconds. Possible values are 16 to 16284 seconds.
- **SNTP Server Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the SNTP server.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **SMTP Server Address**
Shows the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the SMTP server.
- **SNTP Server Port**
Enter the port of the SNTP server.
The following ports are possible:
 - 123 (standard port)
 - 1025 to 36564
- **Primary**
The check mark is set for the SNTP server that you create first. If several SNTP servers have been created, the primary server is queried first.

Procedure

1. Click the "SNTP Client" check box to enable the automatic time setting.
2. In "Time Zone", enter the local time difference to world time (UTC).
The input format is "+/-HH:MM" because the NTP server always sends UTC time, for example +02:00 for CEST, the Central European Summer Time. This time is recalculated and displayed as the local time based on the specified time zone.

3. Select one of the following options from the "SNTP Mode" drop-down list:
 - Poll
For this mode, you need to configure the following:
 - time zone difference (step 2)
 - query interval (step 4)
 - time server (step 5)
 - Port (step 7)
 - complete the configuration with step 8.
 - Listen
For this mode, you need to configure the following:
 - time difference to the time sent by the server (step 2)
 - time server (step 5)
 - port (step 7)
 - complete the configuration with step 8.
4. In "SNTP Server Address", enter the address of the SNTP server whose frames will be used to synchronize the time of day.
5. In "SNTP Server Port", enter the port via which the SNTP server is available. The port can only be modified if the IP address of the SNTP server is entered.
6. In "Poll Interval[s]", enter the time in seconds after which a new time query is sent to the time server.
7. Click the "Set Values" button.

4.5.8.5 NTP Client

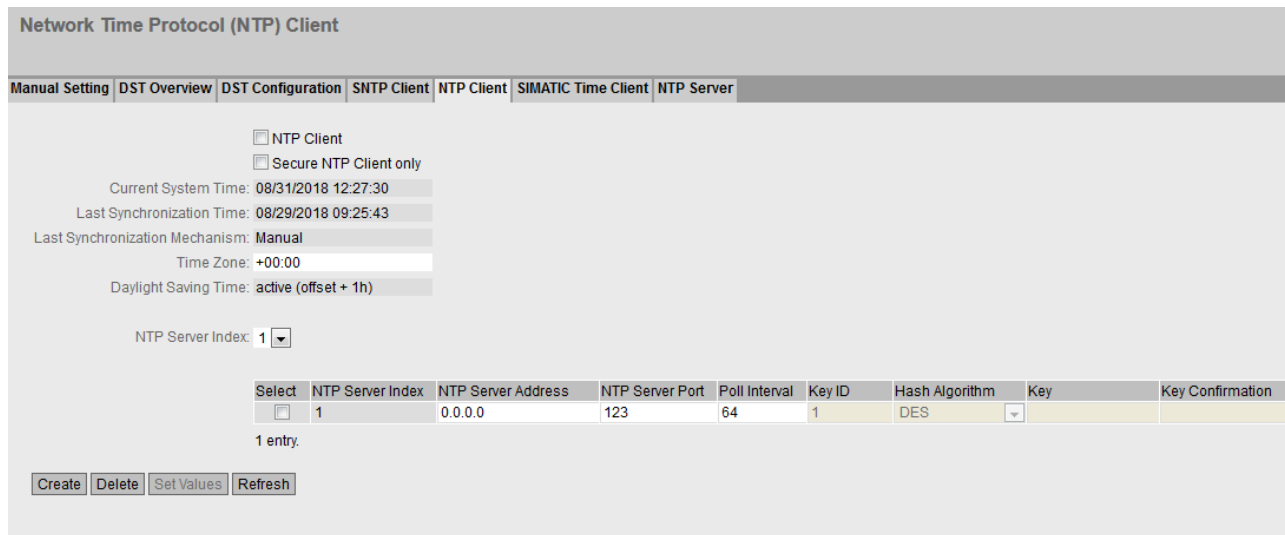
Automatic time-of-day setting with NTP

If time synchronization is to take place via NTP, define the time server that is used to synchronize the time.

Note

To avoid time jumps, make sure that there is only one time server in the network.

4.5 "System" menu



Requirement

To receive the NTP frames, enable the entry "System Time" under "Security > Firewall > Pre-defined IPv4 rules".

Description

The page contains the following boxes:

- **NTP client**
When enabled, the device receives the system time from an NTP server.
- **Secure NTP Client only**
When enabled, the device receives the system time from a secure NTP server. The setting applies to all server entries.
To use the secure NTP client, you configure the parameters for authentication (key ID, hash algorithm, key).
- **Current System Time**
Shows the current date and current normal time received by the device. If you specify a time zone, the time information is adapted accordingly.
- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.

- **Last Synchronization Mechanism**

Shows how the last time synchronization was performed. The following methods are possible:

 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
 - PTP
Automatic time-of-day synchronization with PTP
- **Time Zone**

Enter the time zone you are using in the format "+/- HH:MM". The time zone relates to UTC standard world time.
The time in the "Current System Time" box is adapted accordingly.
- **Daylight Saving Time**

Shows whether the daylight saving time changeover is active.

 - active (offset +1 h)
The system time was changed to daylight saving time; in other words, an hour was added. You can see the current system time at the top right in the selection area of the WBM. The set time continues to be displayed in the "System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.
- **NTP Server Index**

Select the index of the NTP server. The NTP servers are queried in the order of the NTP Server Index. The time of the server that is found first is applied. If time frames of an NTP server with a smaller stratum value are received, this time is applied. The switchover to the time with the smaller stratum takes about 30 minutes

In the table, configure the NTP server

- **Select**

Select the row you want to delete.
- **NTP Server Index**

Number corresponding to a specific NTP server entry.
- **NTP Server Address**

Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the NTP server.

4.5 "System" menu

- **NTP Server Port**
Enter the port of the NTP server.
The following ports are possible:
 - 123 (standard port)
 - 1025 to 36564
- **Poll Interval**
Specify the interval between two-time queries. The greater the interval, the less accurate the time of the device.
Possible values are 64 to 2592000 seconds (30 days).

The following columns are only relevant for a secure NTP client. If the check box "Secure NTP Client only" is not selected, these boxes are grayed out:

- **Key ID**
Enter the ID of the authentication key.
- **Hash Algorithm**
Specify the format for the authentication key.
- **Key**
Enter the authentication key. The length depends on the hash algorithm.
 - DES: ASCII 8 characters
 - MD5: ASCII 16 – 128 characters
 - SHA1: ASCII 20 – 128 characters
- **Key confirmation**
Repeat the authentication key.

Procedure

Time-of-day synchronization with NTP server

1. Click in the "NTP Client" check box to enable the automatic time setting using NTP.
2. In "Time Zone", enter the local time difference to world time (UTC).
The input format is "+/-HH:MM" because the NTP server always sends UTC time, for example +02:00 for CEST, the Central European Summer Time. This time is recalculated and displayed as the local time based on the specified time zone.
3. Select the "NTP Server Index".
4. Click the "Create" button.
A new row is inserted in the table for the NTP server.
5. In "NTP Server Address", enter the address of the NTP server whose frames are used to synchronize the time of day.
6. In "NTP Server Port", enter the port via which the NTP server is available. The port can only be modified if the address of the NTP server is entered.
7. In the "Poll Interval" column, enter the interval in seconds after which a new time-of-day query is sent to the time server.
8. Click the "Set Values" button.

Time-of-day synchronization via a secure NTP server

To synchronize the time of day via a secure NTP server, the following additional steps are necessary:

1. Click the "Secure NTP Client only" check box to enable the automatic time setting using Secure NTP.
2. Configure the authentication.
 - In "Key ID" enter the ID of the authentication key.
 - In "Hash Algorithm" select the required format.
 - In "Key" enter the authentication key.

With these entries, the NTP client authenticates itself with the secure NTP server. These entries must be present on the secure NTP server.

3. Click the "Set Values" button.

4.5.8.6 SIMATIC Time Client

Time setting via SIMATIC time client

Note

To avoid time jumps, make sure that there is only one time server in the network.

Description

The page contains the following boxes:

- **SIMATIC Time Client**
Select this check box to enable the device as a SIMATIC time client.
- **Current System Time**
Shows the current system time.

4.5 "System" menu

- **Last Synchronization Time**
Shows when the last time-of-day synchronization took place.
- **Last Synchronization Mechanism**
Shows how the last time synchronization was performed. The following methods are possible:
 - Not set
The time was not set.
 - Manual
Manual time setting
 - SNTP
Automatic time-of-day synchronization with SNTP
 - NTP
Automatic time-of-day synchronization with NTP
 - SIMATIC
Automatic time-of-day synchronization using the SIMATIC time frame
- **Daylight Saving Time**
Shows whether the daylight saving time changeover is active.
 - active (offset +1 h)
The system time was changed to daylight saving time; in other words, an hour was added. You can see the current system time at the top right in the selection area of the WBM. The set time continues to be displayed in the "System Time" box.
 - inactive (offset +0 h)
The current system time is not changed.

Procedure

1. Click the "SIMATIC Time Client" check box to enable the SIMATIC Time Client.
2. Click the "Set Values" button.

4.5.8.7 NTP Server

On this WBM page, you configure the device as an NTP server or as an NTP server of the type "NTP (secure)". The other devices can call up the time made available by the device via this NTP server. This means that the supplied devices are not dependent on a connection to an external time server.

Note

Time synchronization

Also configure the device as NTP client so that it synchronizes the connected devices to a correct time. As NTP client, the device gets the precise time from an external time server and as NTP server distributes it to its NTP clients.

The NTP server does not send cyclic messages with time information on its own, but only responds to corresponding requests. Settings in the function as a client (time zone and daylight saving time) do not influence the time information that the device sends as a server.

Network Time Protocol (NTP) Server

Manual Setting | DST Overview | DST Configuration | SNTP Client | NTP Client | SIMATIC Time Client | NTP Server

NTP Server

Interface:

| Select | Interface | Listen | Server Port | Secure | Key ID | Hash Algorithm | Key | Key Confirmation |
|--------------------------|-----------|-------------------------------------|-------------|--------------------------|--------|----------------|-----|------------------|
| <input type="checkbox"/> | vlan1 | <input checked="" type="checkbox"/> | 123 | <input type="checkbox"/> | 1 | DES | | |

1 entry.

Requirement

- To receive the NTP frames, enable the entry "System Time" under "Security > Firewall > Predefined IPv4 rules".

Description

The page contains the following boxes:

- NTP Server**
Enable or disable the service of the NTP server.

Note

SNTP Client in Listen mode and NTP Server cannot be enabled at the same time.

- Interface**
Specify the interface via which the time is transferred using NTP.

The table has the following columns:

- Select**
Select the row you want to delete.
- Interface**
Via this interface the time is transferred using NTP.
- Listen**
When enabled, the other devices can call up the time via this interface.
- Server Port**
Enter the port of the NTP server.
The following ports are possible:
 - 123 (standard port)
 - 1025 to 36564
- Secure**
When this is enabled, the NTP server becomes an NTP server of the type "NTP (secure)".

4.5 "System" menu

The following columns are only relevant for "NTP (secure)". Otherwise, these boxes cannot be edited:

- **Key ID**
Enter the ID of the authentication key.
- **Hash Algorithm**
Specify the format for the authentication key.
- **Key**
Enter the authentication key. The length depends on the hash algorithm. The following minimum lengths are recommended for the hash algorithm:
 - DES: ASCII 8 characters
 - MD5: ASCII 16 characters
 - SHA1: ASCII 20 characters
- **Key Confirmation**
Enter the authentication key for confirmation.

4.5.9 Auto Logout

Setting the automatic logout

On this page, set the times after which there is an automatic logout from the WBM or the CLI following user inactivity.

If you have been logged out automatically, you will need to log in again.

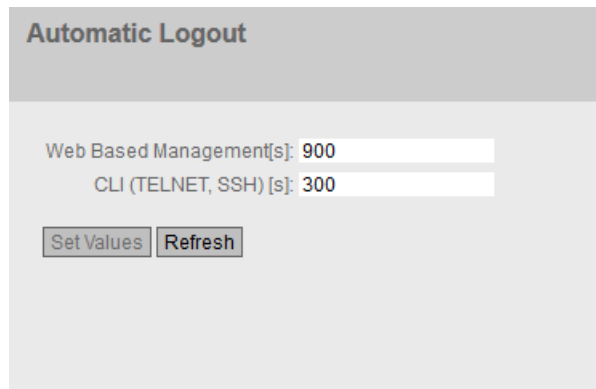
Note

No automatic logout from the CLI

If the connection is not terminated after the set time, check the "Keep alive" setting on the Telnet client.

If the interval for "Keep alive" is shorter than the configured time, the connection is maintained although no user data is transferred. You have set, for example, 300 seconds for the automatic logoff and the "Keep alive" function is set to 120 seconds. In this case, a packet is sent every 120 seconds that keeps the connection uninterrupted.

- Turn off the "Keep alive" (interval time=0)
or
 - Set the interval high enough so that the underlying connection is terminated when there is inactivity.
-



Automatic Logout

Web Based Management[s]: 900

CLI (TELNET, SSH) [s]: 300

Procedure

1. Enter a value of 60-3600 seconds in the "Web Base Management [s]" input box. If you enter the value 0, the automatic logout is disabled.
2. Enter a value of 60-600 seconds in the "CLI (TELNET, SSH) [s]" input box. If you enter the value 0, the automatic logout is disabled.
3. Click the "Set Values" button.

4.5.10 Button

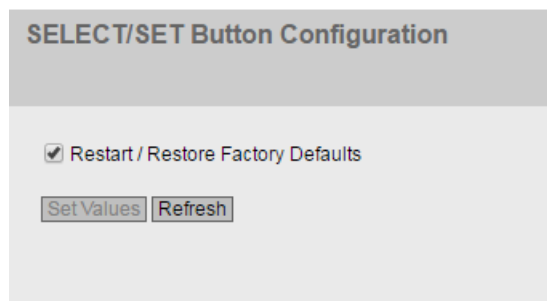
Functionality

The SELECT/SET button is used to:

- Restart
- Load new firmware
- Reset to factory settings.

You will find a detailed description of the functions in the operating instructions for the device.

On this page, the functionality of the button can be restricted.




SELECT/SET Button Configuration

Restart / Restore Factory Defaults

Description

The following functionality is possible:

- **Restart / Restore Factory Defaults**
When disabled, the SELECT/SET button cannot be used for a restart or to restore factory settings.

 **CAUTION**

Button function "Restart / Restore Factory Defaults" active during startup

If you have disabled this function in your configuration, disabling is only valid during operation. When restarting, for example after power off, the function is active until the configuration is loaded and the device can therefore inadvertently be reset to the factory settings. This may cause unwanted disruption in network operation since the device then needs to be reconfigured. An inserted PLUG is also deleted and returned to the status as shipped.

You will find more information on how to restore the device to the factory defaults despite disabled functions in the section "Upkeep and maintenance (Page 330)".

4.5.11 Syslog Client

On this page, you configure the Syslog client. The Syslog messages can be sent to the Syslog server unencrypted or encrypted.

Requirements for sending Syslog messages

- The Syslog client is enabled.
- In "System > Events > Configuration", "Syslog" is activated for the relevant event.
- There is a Syslog server in your network that receives the Syslog messages.
- The IP address or the FQDN (Fully Qualified Domain Name) of the Syslog server is entered in the device.

System Logging (Syslog) Client

Syslog Client

Syslog Server Address:

| Select | Syslog Server Address | Server Port | TLS |
|--------------------------|-----------------------|-------------|--------------------------|
| <input type="checkbox"/> | 192.168.16.100 | 514 | <input type="checkbox"/> |

1 entry.

Description

The page contains the following boxes:

- **Syslog Client**
Enable or disable the Syslog client on the device.
- **Syslog Server Address**
Enter the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the Syslog server.

This table contains the following columns

- **Select**
Select the row you want to delete.
- **Syslog Server Address**
Shows the IP address, the FQDN (Fully Qualified Domain Name) or the host name of the Syslog server.
- **Server Port**
Enter the port of the Syslog server being used.
- **TLS**
 - Enabled
The syslog messages are sent using TLS encryption over TCP.
 - Disabled
Syslog messages are sent unencrypted over UDP.

Procedure

Enabling function

1. Select the "Syslog Client" check box.
2. Click the "Set Values" button.

Creating a new entry

1. In the "Syslog Server Address" input box, enter the address of the Syslog server to which the Syslog messages are sent.
2. Click the "Create" button. A new row is inserted in the table.
3. In the "Server Port" input box, enter the number of the server port.
4. Click the "Set Values" button.

Note

The default setting of the server port is 514.

Changing the entry

1. Delete the entry.
2. Create a new entry.

Deleting an entry

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. All selected entries are deleted and the display is refreshed.

4.5.12 Fault Monitoring

4.5.12.1 Link Change

Configuration of fault monitoring of status changes on connections

On this page, you configure whether or not an error message is triggered if there is a status change on a network connection.

If connection monitoring is enabled, an error is signaled

- when there should be a link on a port and this is missing.
- or when there should not be a link on a port and a link is detected.

A fault causes the fault LED on the device to light up and, depending on the configuration, can trigger a trap, an e-mail, or an entry in the event log table.

| | Setting | Copy to Table |
|-----------|-------------|---------------|
| All ports | No Change ▼ | Copy to Table |

| Port | Setting |
|------|---------|
| P1 | Up ▼ |
| P2 | Down ▼ |
| P3 | - ▼ |
| P4 | - ▼ |
| P5 | - ▼ |

Set Values Refresh

Description

Table 1 has the following columns:

- **1st column**
Shows that the settings are valid for all ports.
- **Setting**
Select the setting from the drop-down list. You have the following setting options:
 - "-" (disabled)
 - Up
 - Down
 - No Change: The setting in table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports and link aggregations. The port is made up of the module number and the port number, for example port 0.1 is module 0, port 1.
- **Setting**
Select the setting from the drop-down list. You have the following options:
 - Up
Error handling is triggered when the port changes to the active status.
(From "Link down" to "Link up")
 - Down
Error handling is triggered when the port changes to the inactive status.
(From "Link up" to "Link down")
 - "-" (disabled)
The error handling is not triggered.

Procedure

Configure error monitoring for a port

1. From the relevant drop-down list, select the options of the slots / ports whose connection status you want to monitor.
2. Click the "Set Values" button.

Configure error monitoring for all ports

1. Select the required setting from the drop-down list of the "Setting" column.
2. Click the "Copy to table" button. The setting is adopted for all ports of table 2.
3. Click the "Set Values" button.

4.5.13 PLUG

4.5.13.1 Configuration

NOTICE

Do not remove or insert a C-PLUG / KEY-PLUG during operation!

A PLUG may only be removed or inserted when the device is turned off.

The device checks whether or not a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE M, the available wireless interfaces are deactivated in this case.

If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

Information about the configuration of the KEY-PLUG

This page provides detailed information about the configuration stored on the C-PLUG. It is also possible to reset the PLUG to "factory defaults" or to load it with new contents.

Note

Incompatibility with older firmware versions with PLUG inserted

During the installation of an older firmware version, the configuration data can be lost. In this case, reset the device to the factory settings after the firmware has been installed.

In this situation, when a PLUG is inserted in the device, following the restart, this has the status "NOT ACCEPTED" because the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using "System > PLUG".

Note

The action is only executed after you click the "Set Values" button.

The action cannot be undone.

If you decide against executing the function after making your selection, click the "Refresh" button. As a result the data of this page is read from the device again and the selection is canceled.

PLUG Configuration (KEY-PLUG)

Configuration
License

State: ACCEPTED

Device Group: SCALANCE M800

Device Type: SCALANCE M874-3

Configuration Revision: 1

File System: UBIFS

File System Size: 29933568

File System Usage: 11164

Info String: 6GK5 874-3AA00-2AA2
SCALANCE M874-3
HW: 3
SW: T04.03.00.00_09.01.01
Firmware on PLUG not present

Firmware on PLUG

Modify PLUG: Select action ▼

Set Values
Refresh

Description

The table has the following rows:

- **Status**
Shows the status of the PLUG. The following are possible:
 - ACCEPTED
There is a PLUG with a valid and suitable configuration in the device.
 - NOT ACCEPTED
Invalid or incompatible configuration on the inserted PLUG.
 - NOT PRESENT
There is no C-PLUG or KEY-PLUG inserted in the device.
 - FACTORY
PLUG is inserted and does not contain a configuration. This status is also displayed when the PLUG was formatted during operation.
 - MISSING
There is no PLUG inserted. Functions are configured on the device for which a license is required.
- **Device Group**
Shows the SIMATIC NET product line that used the C-PLUG or KEY-PLUG previously.

- **Device Type**
Shows the device type within the product line that used the C-PLUG or KEY-PLUG previously.
- **Configuration Revision**
The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove additional components (modules or extenders), it can, however, change if you update the firmware.
- **File System**
Displays the type of file system on the PLUG.
- **File System Size**
Displays the maximum storage capacity of the file system on the PLUG.
- **File System Usage**
Displays the memory utilization of the file system of the PLUG.
- **Firmware on PLUG**
When the function is enabled (default), the firmware will be stored on the PLUG. This means that automatic firmware updates/downgrades can be made with the PLUG. The "Info" box shows whether or not the firmware is stored on the PLUG.
- **Info String**
Shows additional information about the device that used the PLUG previously, for example, article number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.
If a PLUG was configured as a PRESET PLUG this is shown here as additional information in the first row. For more detailed information on creating and using a PRESET PLUG refer to the section "Maintenance".
- **Modify PLUG**
Select the setting from the drop-down list. You have the following options for changing the configuration on the C-PLUG or KEY-PLUG:
 - Write Current Configuration to the PLUG
This option is available only if the status of the PLUG is "NOT ACCEPTED" or "FACTORY".
The configuration in the internal flash memory of the device is copied to the PLUG.
 - Erase PLUG to factory default
Deletes all data from the PLUG and triggers low-level formatting.

Procedure

1. You can only make settings in this box if you are logged on as "Administrator". Here, you decide how you want to change the content of the PLUG.
2. Select the required option from the "Modify PLUG" drop-down list.
3. Click the "Set Values" button.

4.5.13.2 License

| |
|---|
| NOTICE |
| <p>Do not remove or insert a C-PLUG / KEY-PLUG during operation!</p> <p>A PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a PLUG is present at one second intervals. If it is detected that the PLUG was removed, there is a restart. If a valid KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart. With SCALANCE M, the available wireless interfaces are deactivated in this case.</p> <p>If the device was configured at some time with a PLUG, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.</p> |

Note

Incompatibility with previous versions with PLUG inserted

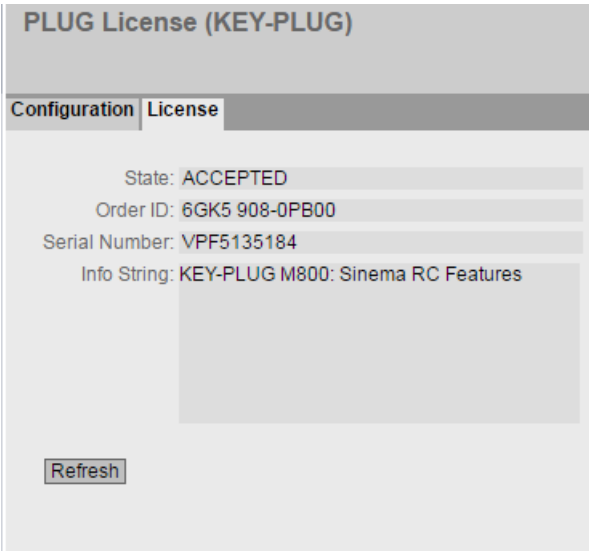
During the installation of a previous version, the configuration data can be lost. In this case, the device starts up with the factory settings after the firmware has been installed. In this situation, if a PLUG is inserted in the device, following the restart, this has the status "NOT ACCEPTED" since the PLUG still has the configuration data of the previous more up-to-date firmware. This allows you to return to the previous, more up-to-date firmware without any loss of configuration data.

If the original configuration on the PLUG is no longer required, the PLUG can be deleted or rewritten manually using "System > PLUG".

Information about the license of the KEY-PLUG

A C-PLUG can only store the configuration of a device. In addition to the configuration, a KEY-PLUG also contains a license that enables certain functions of your SIMATIC NET device.

This page provides detailed information about the license on the KEY-PLUG.



Description

- **Status**
Shows the status of the KEY-PLUG. The following are possible:
 - ACCEPTED
There is a KEY-PLUG with a valid and matching license in the device.
 - NOT ACCEPTED
The license of the inserted KEY-PLUG is not valid.
 - NOT PRESENT
No KEY-PLUG is inserted in the device.
 - MISSING
There is no KEY-PLUG inserted with the "FACTORY" status. Functions are configured on the device for which a license is required.
 - WRONG
The inserted KEY-PLUG is not suitable for the device.
 - UNKNOWN
Unknown content of the KEY-PLUG.
 - DEFECTIVE
The content of the KEY-PLUG contains errors.
- **Order ID**
Shows the order ID of the KEY-PLUG. The KEY-PLUG is available for various functional enhancements and for various target systems.
- **Serial Number**
Shows the serial number of the KEY-PLUG.
- **Info String**
Shows additional information about the device that used the KEY-PLUG previously, for example, article number, type designation, and the versions of the hardware and software. The displayed software version corresponds to the version in which the configuration was last changed. With the "NOT ACCEPTED" status, further information on the cause of the problem is displayed.

Note

When you save the configuration, the information about whether or not a KEY-PLUG was inserted in the device at the time is also saved. This configuration can then only work if a KEY-PLUG with the same order number / license is inserted.

4.5.14 Ping

Reachability of an address in an IPv4 network

With the ping function, you can check whether a certain IPv4 address is reachable in the network.

The screenshot shows a web interface titled "Ping". It features a "Destination Address:" input field, a "Repeat:" input field with the value "3", and a "Ping" button. Below these is a large "Ping Output:" area, and at the bottom left is a "Clear" button.

Description

The table has the following columns:

- **Destination Address**
Enter the IPv4 address or the FQDN of the device.
- **Repeat**
Enter the number of ping requests.
- **Ping**
Click this button to start the ping function.
- **Ping Output**
This box shows the output of the ping function.
- **Clear**
Click this button to empty the "Ping Output" box.

4.5.15 DCP Discovery

On this page, you can select an interface and search for devices that are reachable via the interface and support DCP. DCP Discovery only searches for devices located in the same subnet as the interface. The reachable devices are listed in a table. In the table you can check and adapt the network parameters of the devices. To identify and configure the devices the Discovery Configuration Protocol (DCP) is used.

Note

DCP Discovery

The function is only available with the VLAN associated with the TIA interface. You can configure the TIA interface with "Layer 3 > Subnets > Configuration".

Discovery and Set via PROFINET Discovery and Configuration Protocol (DCP)

Timeout[s]:

Interface:

| Port | MAC Address | Device Type | Device Name | IP Address | Mask Address | Gateway Address | Name Status | IP Status | Timeout[s] | Blink |
|------|-------------------|----------------|-----------------|----------------|---------------|-----------------|-------------|---------------|------------|--------------------------------------|
| P0.2 | 00-10-10-00-00-00 | SCALANCE W-700 | | 192.168.16.177 | 255.255.255.0 | 0.0.0.0 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE X-500 | | 192.168.16.150 | 255.255.255.0 | 0.0.0.0 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE M-800 | | 192.168.16.48 | 255.255.255.0 | 0.0.0.0 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE M-800 | | 192.168.16.50 | 255.255.255.0 | 0.0.0.0 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE M-800 | | 192.168.16.46 | 255.255.255.0 | 0.0.0.0 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE S-600 | securityxb10657 | 192.168.16.42 | 255.255.255.0 | 0.0.0.0 | Discovered | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE X-300 | | 192.168.16.33 | 255.255.255.0 | 192.168.16.33 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE X-400 | | 192.168.16.144 | 255.255.255.0 | 0.0.0.0 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE M-800 | | 192.168.1.1 | 255.255.255.0 | 192.168.1.20 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |
| P0.2 | 00-10-10-00-00-00 | SCALANCE X-500 | | 192.168.16.155 | 255.255.255.0 | 0.0.0.0 | None | Discovered/IP | 5 | <input type="button" value="Blink"/> |

1 - 10 of 20 entries [Show all](#) 1

Requirement:

To adapt network parameters, DCP requires write access to the device. If access is write-protected, the network parameters cannot be configured.

On SCALANCE devices, you configure access under "System > Configuration".

Description

The page contains the following boxes:

- **Timeout**
Specify the time for flashing. When the time elapses, flashing stops.
- **Blink Own LEDs**
Makes the LEDs port of your own device flash.

- **Interface**
Select the required interface.
- **Discover**
Starts the search for devices reachable via the selected interface.
On completion of the search the reachable devices are listed in the table. The table is limited to 100 entries.

The table has the following columns:

- **Port**
Shows the port via which the device can be reached.
- **MAC Address**
Shows the MAC address of the device.
- **Device Type**
Shows the product line or product group to which the device belongs.
- **Device Name**
Adapt the PROFINET device name if necessary.
The device name must be DNS-compliant. If the device name is not used, the box is empty.
- **IP Address**
If necessary, adapt the IPv4 address of the device.
The IPv4 address should be unique within your network and should match the network. The IPv4 address 0.0.0.0 means that no IPv4 address has yet been set.
- **Subnet mask**
If necessary, adapt the subnet mask of the device.
- **Gateway Address**
Adapt the IPv4 address of the gateway if necessary.
- **Status Device Name**
 - None: The device name is not used.
 - Discovered: The set device name is used.
 - Configured: The device was assigned a new device name.
- **Status IP address**
 - Discovered/IP: The device uses a static IPv4 address.
 - Discovered/DHCP: The device has obtained the IPv4 address from a DHCP server.
 - Configured: The device was assigned a new IPv4 address.
- **Timeout**
Specify the time for flashing. When the time elapses, flashing stops.
- **Flash**
Makes the port LEDs of the selected device flash.

Procedure

1. Select the TIA interface.
2. To show all devices that can be reached via the TIA interface, click the "Browse" button.

4.5 "System" menu

3. Adapt the desired properties.
4. Click the "Set Values" button.
The status of the modified properties changes to "Configured".
5. To ensure that the properties were applied correctly, click the "Browse" button again.
The status of the modified properties changes to "Discovered".

4.5.16 DNS

4.5.16.1 DNS Client

On the WBM page you specify whether or not the device uses the DNS server of the network provider or another DNS server.

Domain Name System (DNS) Client

DNS Client | DNS Proxy | DDNS Client | DNS Records

DNS Client

Used DNS Servers: all ▼

DNS Server Address:

| Select | DNS Server Address | Origin |
|--------------------------|--------------------|--------|
| <input type="checkbox"/> | 192.168.10.1 | manual |
| <input type="checkbox"/> | 192.168.10.2 | manual |

2 entries.

Create Delete Set Values Refresh

Description

The page contains the following boxes:

- **DNS client**
Enable or disable depending on whether the device should operate as a DNS client.
- **Used DNS Servers**
Specify which DNS server the device uses:
 - learned only
The device uses only the DNS servers assigned by DHCP.
 - manual only
The device uses only the manually configured DNS servers. The DNS servers must be connected to the Internet. A maximum of two DNS servers can be configured.
 - all
The device uses all available DNS servers.
- **DNS Server Address**
Enter the IP address of the DNS server.

The table has the following columns:

- **Select**
Activate the check box in the row to be deleted
- **DNS Server Address**
Shows the IP address of the DNS server.
- **Origin**
Shows whether the DNS server was configured manually or was assigned by DHCP.

4.5.16.2 DNS Proxy

The device provides a DNS server for the local network. If you enter the IP address of the device in the local application as a DNS server, the device answers the DNS requests from its cache.

If the device does not know the IP address for a domain address, it forwards the query to an external DNS server. How long the device keeps a domain address in the cache depends on the host being addressed. In addition to the IP address, a DNS request to an external DNS server also supplies the life span of this information.

DNS Proxy

DNS Client | **DNS Proxy** | **DDNS Client** | **DNS Records**

Enable DNS Proxy
 Cache Name Errors (NXDOMAIN)

Description

The page contains the following boxes:

- **Enable DNS Proxy**
Enable or disable the proxy of the DNS server.
- **Cache Name Errors (NXDOMAIN)**
Enable or disable the caching of NXDOMAIN replies. If you enable the option, the domain names that were unknown to the DNS server remain in the cache.

4.5.16.3 DDNS Client

The DDNS (Dynamic Domain Name System) is an Internet service that allows a fixed hostname to be set up as a pseudonym for a dynamically changing IP address.

The DDNS client synchronizes the assigned IP address with the hostname registered at the DDNS provider. This means that the device can always be reached using the same hostname.

DDNS-Client

DNS-Client
DNS-Proxy
DDNS-Client
DNS Records

| Dienst | Aktiviert | Host | Benutzername | Passwort | Passwort bestätigen |
|--------|--------------------------|------|--------------|----------|---------------------|
| No-IP | <input type="checkbox"/> | | | | |
| DynDNS | <input type="checkbox"/> | | | | |

Einstellungen übernehmen
Aktualisieren

Description

The table has the following columns:

- **Service**
Shows which providers are supported.
- **Enabled**
When enabled, the device logs on to the DDNS server.
- **Host**
Enter the host name that you have agreed with your DDNS provider for the device, e.g. example.no-ip-com.
- **User Name**
Enter the user name with which the device logs on to the DDNS server.
- **Password**
Enter the password assigned to the user.
- **Password Confirmation**
Confirm the password.

Procedure

Requirement:

- User name and password that gives you the right to use the DDNS service.
 - Registered hostname, e.g. example.no-ip.com
 - UDP port 53 for DNS is enabled and is not used for NAT.
1. In "Host", enter the hostname that you have agreed with your DDNS provider for the device, e.g. example.no-ip-com.
 2. Enter the login data (user name, password) for the DDNS server.
 3. Select "Enabled". This hostname is used for the device.
 4. Click on "Set Values".

4.5.16.4 DNS record

You configure a DNS address directory on this WBM page. To do this, enter the IPv4 address associated with an FQDN.

The device checks if there is an entry for DNS requests and converts the URL into the corresponding IPv4 address.

| Select | Domain | IP Address | Comment |
|--------------------------|------------|-------------|---------|
| <input type="checkbox"/> | example.de | 192.168.1.1 | |

1 entry.

Description

The page contains the following boxes:

- **Enable DNS Records**
When this is enabled, the address directory is used.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted
- **Domain**
Enter the FQDN (Fully Qualified Domain Name).

4.5 "System" menu

- **IP Address**
Enter the corresponding IPv4 address.
- **Comment**
If needed, enter a comment.

4.5.17 DHCP

4.5.17.1 DHCP Client

If the device is configured as a DHCP client, it starts a DHCP request. As the reply to the query the device receives an IPv4 address from the DHCP server. The server manages an address range from which it assigns IPv4 addresses. It is also possible to configure the server so that the client always receives the same IPv4 address in response to its request.

The screenshot shows the 'Dynamic Host Configuration Protocol (DHCP) Client' configuration page. It features a tabbed interface with 'DHCP Client' selected. The configuration includes checkboxes for 'Keep Alive' and 'DHCP Client Configuration Request (Opt.66, 67)', both of which are checked. The 'DHCP Mode' is set to 'via MAC Address'. Below this is a table with columns for 'Interface', 'DHCP', and 'IAID Value'. The table contains one entry for 'vlan1' with the DHCP checkbox checked and the IAID Value '00-00-01-C2'. At the bottom, there are 'Set Values' and 'Refresh' buttons.

| Interface | DHCP | IAID Value |
|-----------|-------------------------------------|-------------|
| vlan1 | <input checked="" type="checkbox"/> | 00-00-01-C2 |

Description

The page contains the following boxes:

- **Keep Alive**
When this is enabled, the IP address is retained in the event of a connection breakdown and is not reset to 0.0.0.0. Keep Alive is enabled by default. When Keep Alive is disabled, the IP address is reset to 0.0.0.0 in the event of a communication breakdown.
- **DHCP Client Configuration Request (Opt. 66, 67)**
When enabled, the DHCP client uses the options to download the configuration file (option 67) from the TFTP server (option 66). After the restart, the device uses the data from the configuration file.

Note

Configuration file and firmware version

The configuration file is used to store and read in configuration data within a firmware version, e.g. 4.3. Configuration files created with a firmware version <4.2 cannot be read in to a device with a firmware version 4.3.

- **DHCP Mode**
Specify the type of identifier with which the DHCP client logs on with its DHCP server.
 - via MAC Address
Identification is based on the MAC address.
 - via DHCP Client ID
Identification is based on a freely defined DHCP client ID.
 - via System Name
Identification is based on the system name. If the system name is 255 characters long, the last character is not used for identification.
 - via Iaid and Duid
With this the DHCP client can log on with DHCP servers that support parallel operation of IPv4 and IPv6.
The identification is via the IAID and the DUID and identifies precisely one IP interface of the device.
IAID (Interface Association Identifier): At least one IAID is generated for each IP interface
The IAID remains unchanged when the DHCP client restarts
DUID (DHCP Unique Identifier): Uniquely identifies server and clients and applies to all IP interfaces of the device. The DUID remains unchanged when there is a restart.

Note

DHCP mode "via PROFINET device name"

With firmware version 5.0, the setting "via PROFINET device name" was removed.

4.5 "System" menu

The table has the following columns:

- **Interface**
Interface to which the setting relates.
- **DHCP**
Enable or disable the DHCP client for the relevant interface.
- **IAID Value**
Value with which the interface (DHCP client) identifies itself with the DHCP server.

Procedure

Follow the steps below to configure the IP address using the DHCP client ID:

1. Select the identification method in the "DHCP Mode" drop-down list.
If you select the DHCP mode "via DHCP Client ID" an input box appears.
In the enabled input box "DHCP client ID" enter a string to identify the device. This is then evaluated by the DHCP server.
2. Select the "DHCP Client Configuration Request (Opt. 66, 67)", if you want the DHCP client to use options 66 and 67 to download and then enable a configuration file.
3. Enable the "DHCP" option in the table.
4. Click the "Set Values" button.

Note

If a configuration file is downloaded, this can trigger a system restart. If the currently running configuration and the configuration in the downloaded configuration file differ, the system restarts.

Make sure that the option "DHCP Client Configuration Request (Opt. 66, 67)" is no longer set.

4.5.17.2 DHCP Server

You can operate the device as a DHCP server. This allows IP addresses to be assigned automatically to the connected devices. The IP addresses are either distributed dynamically from an address band (pool) you have specified or a specific IP address is assigned to a particular device.

On this page, specify the address band from which the device receives any IP address. You configure the static assignment of the IP addresses in "Static Leases".

Dynamic Host Configuration Protocol (DHCP) Server

DHCP Client | **DHCP Server** | **DHCP Options** | **Static Leases**

DHCP Server
 Probe address with ICMP Echo before offer

| Select | Pool ID | Interface | Enable | Subnet | Lower IP Address | Upper IP Address | Lease Time [sec] |
|--------------------------|---------|-------------|-------------------------------------|-----------------|------------------|------------------|------------------|
| <input type="checkbox"/> | 1 | vlan1 (INT) | <input checked="" type="checkbox"/> | 192.168.16.0/24 | 192.168.16.50 | 192.168.16.50 | 3600 |

1 entry.

Requirement

- The connected devices are configured so that they obtain the IP address from a DHCP server.

Description

The page contains the following boxes:

- DHCP Server**
Enable or disable the DHCP server on the device.

Note

To avoid conflicts with IPv4 addresses, only one device may be configured as a DHCP server in the network.

- Probe address with ICMP echo before offer**
When selected, the DHCP server checks whether or not the IP address has already been assigned. To do this the DHCP server sends ICMP echo messages (ping) to the IPv4 address. If no reply is received, the DHCP server can assign the IPv4 address.

Note

If there are devices in your network on which the echo service is disabled as default, there may be conflicts with the IPv4 addresses. To avoid this, assign these devices an IPv4 address outside the IPv4 address band.

The table has the following columns:

- Select**
Select the check box in the row to be deleted.
- Pool ID**
Shows the number of the IPv4 address band. If you click the "Create" button, a new row with a unique number is created (pool ID).

4.5 "System" menu

- **Interface**
Select a VLAN IP interface. The IPv4 addresses are assigned dynamically via this interface. The requirement for the assignment is that the IPv4 address of the interface is located in the subnet of the IPv4 address band. If this is not the case, the interface does not assign any IPv4 addresses.
- **Enable**
Specify whether or not this IPv4 address band will be used.

Note

If you enable the IPv4 address band, its settings in this and the other DHCP tabs are grayed out and can no longer be edited.

- **Subnet**
Enter the network address range that will be assigned to the devices. Use the CIDR notation.
- **Lower IP Address**
Enter the IPv4 address that specifies the start of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".
- **Upper IP address**
Enter the IPv4 address that specifies the end of the dynamic IPv4 address band. The IPv4 address must be within the network address range you configured for "Subnet".
- **Lease Time (sec)**
Specify for how many seconds the assigned IPv4 address remains valid. When half the period of validity has elapsed, the DHCP client can extend the period of the assigned IPv4 address. When the entire time has elapsed, the DHCP client needs to request a new IPv4 address.

4.5.17.3 DHCP Options

On this page you specify which DHCP options the DHCP server supports. The various DHCP options are defined in RFC 2132.

Dynamic Host Configuration Protocol (DHCP) Options

DHCP Server | **DHCP Options** | Static Leases

Pool ID:

Option Code:

| Select | Pool ID | Option Code | Use Interface IP | Value |
|--------------------------|---------|-------------|--------------------------|-----------------------|
| <input type="checkbox"/> | 1 | 1 | | 255.255.255.255 |
| <input type="checkbox"/> | 1 | 3 | <input type="checkbox"/> | 0.0.0.0 |
| <input type="checkbox"/> | 1 | 6 | <input type="checkbox"/> | 0.0.0.0 |
| <input type="checkbox"/> | 1 | 66 | | |
| <input type="checkbox"/> | 1 | 67 | | Bootfile name not set |

5 entries.

Description

The page contains the following boxes:

- **Pool ID**
Select the required address band.
 - **Option Code**
Enter the number of the required DHCP option.
-

Note

DHCP options supported

The DHCP options 1, 2, 3, 4, 5, 6, 42, 66, 67 are supported.

The DHCP options 1, 3, 6, 66 and 67 are created automatically when the IPv4 address band is created. With the exception of option 1, the options can be deleted.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted
- **Pool ID**
Shows the number of the address band.
- **Option Code**
Shows the number of the DHCP option.

4.5 "System" menu

- **Use Interface IP**
Specify whether or not the internal IP address of the device will be used.
- **Value**
Enter the DHCP parameter that is transferred to the DHCP client. The content depends on the DHCP option.

| Value | Option name | | |
|-------|-----------------------|--|---|
| 1 | Subnet Mask | The subnet mask is entered automatically. | Option cannot be deleted. |
| 2 | Offset time | Offset time to the coordinated universal time UTC. | Enter the offset time in seconds in hexadecimal format. |
| 3 | Router | The IPv4 address for router in the subnet of the DHCP client. If the device itself is the router, the IPv4 address of the interface is used. | You can specify several IPv4 addresses separated by commas. |
| 4 | Time server | The IPv4 address of the time server available to the DHCP client. | |
| 5 | Name server | The IPv4 address of the name server available to the DHCP client. | |
| 6 | DNS Server | The IPv4 address of the DNS server available to the DHCP client. If the device itself is the DNS server, the IPv4 address of the interface is used. | |
| 42 | NTP Server | The IPv4 address of the NTP server available to the DHCP client. | |
| 66 | TFTP server | The IPv4 address or the hostname of the TFTP server available to the DHCP client. | Enter the address of the TFTP server. |
| 67 | Name of the boot file | The name of the boot file that the client downloads from the TFTP server. | Enter the name of the boot file in the string format. |

4.5.17.4 Static Leases

On this page you specify that certain devices will be assigned a certain IP address. The address assignment is made based on the MAC address, the client ID or the DUID.

Static Leases

DHCP Client | DHCP Server | DHCP Options | **Static Leases**

Pool ID:

Client Identification Method:

Value:

| Select | Pool ID | Identification Method | Value | IP Address | Comment |
|--------------------------|---------|-----------------------|-------------------|---------------|---------|
| <input type="checkbox"/> | 1 | MAC | 00-1b-1b-b6-32-79 | 192.168.16.48 | Router |

1 entry.

Description

The page contains the following boxes:

- **Pool ID**
Select the required address band.
- **Client Identification Method**
Select the method according to which a client is identified.
 - Ethernet MAC
Identification is based on the MAC address. Enter the MAC address in "Value". A MAC address consists of six bytes separated by hyphens in hexadecimal notation, e.g. 00-ab-1d-df-b4-1d.
 - Client ID
Identification is based on a freely defined DHCP client ID. Enter the required designation in "Value".
 - DUID
Identification is based on the DUID and IAID. Enter the required designation in "Value" e.g. 00-00-01-C2-00-01-00-01-00-00-00-72-00-1B-1B-B6-32-9D.
- **Value**
Enter the required value. The entry depends on the selected identification method of the client.

Note

The maximum is 128 entries.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Pool ID**
Shows the number of the address band.
- **Identification Method**
Shows the method with which the client identifies itself with the DHCP server.
- **Value**
Shows the MAC address or client ID or DUID of the client.
- **IP Address**
Specify the IPv4 address that will be assigned to the client. The IPv4 address must be within the address band.
- **Comment**
Enter a description for the address assignment.
The maximum is 32 characters.

4.5.18 cRSP / SRS

Note

Common Remote Service Platform (cRSP) / Siemens Remote Service (SRS) is a remote maintenance platform via which remote maintenance access is possible.

To use the platform, additional service contracts are necessary and certain constraints must be kept to. If you are interested in cRSP / SRS, call your local Siemens contact or visit Web page (<https://support.industry.siemens.com/cs/gb/en/sc/2281>).

On this page, you configure the access data for the SRS / cRSP acc. to URI syntax. The Uniform Resource Identifier (URI) is defined in RFC 3986.

DDNS for cRSP / SRS

Enable DDNS for cRSP / SRS
 Update Interval [s]:
 Validate Server Certificate

| Index | Select | Scheme | Authority | Path | Query | Frag. | Status | Enabled |
|-------|--------------------------|--------|-----------|------|-------|-------|--------|--------------------------|
| 1 | <input type="checkbox"/> | https | :// | | ? | | # | <input type="checkbox"/> |

1 entry.

Description

The page contains the following boxes:

- **Enable DDNS for cRSP / SRS**
Enable or disable the use of cRSP / SRS.
- **Update Interval**
Enter the time interval.
- **Validate Server Certificate**
When enabled, the device checks the validity of the received server certificate.

The table has the following columns:

- **Index**
The number of the entry.
- **Select**
Select the check box in the row to be deleted.

4.5 "System" menu

- **Scheme**
Identifies the access method and the resource type.
https: Secure access to a Web page.
- **Authority**
Contains the address of the destination server
- **Path**
Contains the target path to the resource. The target path can correspond to a directory name or file name.
- **Query**
A query can contain parameter values for an application.
 - WAN_IP (keyword): Replaces WAN_IP with current external IP address of the device to the destination server.
- **Frag.**
Addresses local parts of the resource, e.g. the anchor attribute of a Web page.
- **Status**
Shows the status of the last cRSP / SRS access of the entry.
- **Enabled**
When enabled, this entry is used.

4.5.19 Proxy Server

On this WBM page, you configure the proxy server that is used by various components, for example SINEMA RC.

Proxy Server

Proxy Name:

| Select | Name | Address | Type | Port | Auth. Method | Username | Password | Password Conf. |
|--------------------------|---------|--------------|------|------|--------------|----------|----------|----------------|
| <input type="checkbox"/> | company | 192.168.16.1 | HTTP | 0 | Basic | | | |

1 entry.

Description

- **Proxy Name**
Enter a name for the proxy server.
- The table has the following columns:
- **Select**
Select the check box in the row to be deleted.
 - **Name**
Shows the name of the proxy server.

- **Address**
Enter the IPv4 address of the proxy server.
- **Type**
Specify the type of the proxy server.
 - HTTP: Proxy server only for access using HTTP.
 - SOCKS: Universal proxy server
- **Port**
Enter the port on which the proxy service runs.
- **Auth. Method**
Specify the authentication method.
 - None
Without authentication
 - Basic
Standard authentication. User name and password are sent unencrypted.
 - NTLM (NT LAN Manager)
Authentication according to the NTLM standard (Windows user logon)
- **User Name**
Enter the user name for access to the proxy server.
- **Password**
Enter the password for access to the proxy server.
- **Password Confirmation**
Enter the password again to confirm it.

4.5.20 SINEMA RC

On the WBM page, you configure the access to the SINEMA RC server.

Note

This function can only be used with a KEY PLUG (Page 28).

Description

The page contains the following:

- **Enable SINEMA RC**
 - Enabled:
 - A connection to the configured SINEMA RC Server is established. These boxes cannot be edited.
 - Disabled:
 - The boxes can be edited. Any existing connection is terminated.

"Server settings" area

- **SINEMA RC Address**
 - Enter the IPv4 address or the FQDN (Fully Qualified Domain Name) of the SINEMA RC Server.
- **SINEMA RC Port**
 - Enter the port via which the SINEMA RC Server can be reached.

"Server Verification" area

- **Verification Type**

- Fingerprint: The identity of the server is verified based on the fingerprint.
- CA certificate: The identity of the server is verified based on the CA certificate.

- **Fingerprint**

Only necessary with the setting "Fingerprint". Enter the fingerprint of the device. The fingerprint is assigned during commissioning of the SINEMA RC Server. Based on the fingerprint, the device checks whether the correct SINEMA RC Server is involved. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

- **CA Certificate**

Only necessary with the setting "CA Certificate". Select the CA certificate of the server used to sign the server certificate. Only loaded CA certificates can be selected.

"Device Credentials" area

- **Device ID**

Enter the device ID. The device ID is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

- **Device Password**

Enter the password with which the device logs on to the SINEMA RC Server. The password is assigned when configuring the device on the SINEMA RC Server. You will find further information on this in the Operating Instructions of the SINEMA RC Server.

- **Device Password Confirmation**

Repeat the password.

"Optional Settings" area**• Auto Firewall/NAT Rules**

- Enabled

The firewall and NAT rules are created automatically for the VPN connection. The connections between the configured exported subnets and the subnets that can be reached via the SINEMA RC Server are allowed. The NAT settings are implemented as configured in the SINEMA RC Server.

You can enable SINEMA RC to access specific services of the device under "Security > Firewall > Predefined IPv4".

- Disabled

You will need to create the firewall and NAT rules yourself.

• Type of connection

Specify the type of VPN connection. For more detailed information, refer to the section "VPN connection establishment".

- Auto

The device adopts the settings of the SINEMA RC Server. You configure the settings on the SINEMA RC Server in "Remote connections > Devices". You will find further information on this topic in the operating instructions "SINEMA RC Server".

- Permanent

The settings of the SINEMA RC Server are ignored. The device establishes a VPN connection to the SINEMA RC Server. The VPN tunnel is established permanently

- Wake-up SMS (only with M87x)

The settings of the SINEMA RC Server are ignored. When the device receives a command SMS message (wake-up SMS message), it attempts to establish a connection to the SINEMA RC Server. On condition that in "System > SMS > SMS Command" it is specified who a command SMS of the class "System" will be accepted from.

- Digital In

The settings of the SINEMA RC Server are ignored. If the "Digital In" event occurs, the device attempts to establish a VPN connection to the SINEMA RC Server. This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this in "System > Events > Configuration" activate "VPN Tunnel" for the "Digital In" event.

- Digital In & Wake-up SMS (only with M87x)

The settings of the SINEMA RC Server are ignored. If the "Digital In" event occurs or when the device receives an SMS command, it attempts to establish a VPN connection to the SINEMA RC Server.

• Use Proxy

Specify whether a connection to the defined SINEMA RC Server is established via a proxy server. Only the proxy servers can be selected that you configured in "System > Proxy Server".

• Autoenrollment Interval [min]

Specify the period of time in minutes after which queries are sent to the SINEMA RC server. With this query, the device checks whether there is a newer firmware file on the SINEMA RC server or whether the connection settings have changed. If you enter the value 0, this function is disabled.

• Timeout [min]

Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

4.5.21 Cloud Connector

On this WBM page, you configure the parameters for communication with the TIA Portal Cloud Connector.

Note

- Use the "TIA Portal Cloud Connector" integrated in the product via a VPN solution (e.g. SINEMA RC).
 - To prevent unauthorized access by network nodes to the "TIA Portal Cloud Connector Server", enable the item "Cloud Connector" under "Security > Firewall > Pre-defined IPv4 Rules".
 - You can only enable this function on one interface at a time.
-

| Interface | Active |
|-------------|--------------------------|
| vlan1 (INT) | <input type="checkbox"/> |

Requirement

- For the incoming packets to be forwarded to the device, enable the predefined IPv4 rule "Cloud Connector".

Description

The page contains the following:

- **Operation**
 - Enabled
Enables the integrated TIA Portal Cloud Connector.
 - Disabled
Disables the integrated TIA Portal Cloud Connector.
 - Start on DI
Enabling is controlled via the digital input (DI) if the "Cloud Connector" is enabled for the event "Digital input" under "System > Events > Configuration". If this setting is not enabled, the event is not passed on to the TIA Portal Cloud Connector.
- **Port**
Communication with the TIA Portal Cloud Connector is established via this port.
- **Protocol**
This protocol is used to access the plant network.
 - PROFINET via VLAN
You define the VLAN interface in the following table.Only with M804PB
 - PROFIBUS via MPI/DP
 - PROFINET-PROFIBUS

The following table is only required for PROFINET:

- **Interface**
Only VLANs with a configured subnet are available.
- **Active**
When enabled, this VLAN is used for PROFINET.
- **Reset Parameters**
Resets the properties of the interface to the default values.

4.5.22 Configuration Backup

Backup

On this page, you can create backups of the configuration. The maximum number depends on the size of the backup and the available memory space.

The created backups are saved under the "ConfigPackBackup" file type. On the "System > Load&Save > HTTP/TFTP/SFTP" page, you can save configuration backups in ZIP format on your client PC or load them from there.

Configuration Package Backup

Name:

| Select | Name | Size[kBytes] | Restore |
|--------------------------|------------------|--------------|---------|
| | Available memory | 90 | |
| <input type="checkbox"/> | Backup | 60 | Restore |

2 entries.

Description

The page contains the following boxes:

- **Name**
Enter a name for the backup.

The table contains the following columns:

- **Select**
Select the row you want to delete.
- **Name**
Shows the name of the backup.
- **Size [KB]**
The first row "Available memory" shows how much memory is available for backups on the device. When you create a backup, the available memory space is reduced accordingly. The other rows show the size of each backup.
- **Restore**
Click the "Restore" button to load the relevant backup on the device.

Procedure

1. Enter the required name.
2. Click the "Create" button.
The current configuration is saved as a configuration backup. Saving the backup may take some time. A new row is created for the backup. The size of the backup is displayed and subtracted from the available memory space.

4.5.23 Connection Check

On this page, you activate a ping test that monitors connections. During the ping test, the device sends ICMP echo request packets (pings) to the configured destination address at regular intervals. If this destination address does not respond, the device tries to reach the destination address again. If all ping attempts (retries) are unsuccessful, the ping test is considered to have failed or the group is considered unreachable. If the group is not reachable, the device initiates the configured action on the selected interface. If all 5 actions have been executed or after a restart, the device starts again with the first action.

Connection Check

Connection Check

Enable Connection Check

| Group Idx | Name | Source Interface | Interval | TTL | Retries | 1st Ping Target | 2nd Ping Target | 3d Ping Target |
|-----------|------|------------------|----------|-----|---------|-----------------|-----------------|----------------|
| 1 | LAN | usb0 | 30 | 128 | 3 | 192.168.1.20 | | |
| 2 | | Auto | 180 | 128 | 5 | | | |
| 3 | | Auto | 300 | 128 | 3 | | | |
| 4 | | Auto | 300 | 128 | 3 | | | |
| 5 | | Auto | 300 | 128 | 3 | | | |

| LAN | Group 2 | Group 3 | Group 4 | Group 5 | Action for | 1st Action | 2nd Action | 3rd Action | 4th Action | 5th Action |
|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------|------------|------------|------------|------------|------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | usb0 | None | None | None | None | None |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Device | None | None | Restart | None | None |

Description

- **Enable Connection Check**
Enable or disable the ping test for connection monitoring.

The "Group" table contains the following columns:

- **Group Identifier**
Index of the group.
- **Name**
Specify a name for the group. The entry is displayed in the "Action" table as column name.
- **Source Interface**
Specify the interface via which reachability of the destination addresses is monitored.
- **Interval**
Specify the interval at which the ping tests take place.
- **TTL (Time to live)**
Specify the TTL value.

- **Retries**
Specify how often the ping attempt is repeated.
The time interval between the ping attempts is 100 ms. With a large number of ping attempts, this can result in a time delay.
If none of the configured addresses responds, the ping test is considered to have failed (error). In the "Action" table, you define whether a specific action is executed.

- **1. - 3. Ping destination**
Specify the destination address that is used as reference for the reachability.

The "Group" table contains the following columns:

- **Group 1 - 5**
If a name is configured, it is used as column name. Assign the groups to the desired interface. The interface is considered reachable when all assigned groups are reachable. If only one of the groups is not reachable, the configured action is executed on the selected interface.
- **Action for**
Indicates the interface on which the action is executed.
- **1st action - 5th action**
The following actions are possible:
 - None (default)
 - Restart
Restart the device. After the restart, the device waits for 10 minutes and then sends a ping to the first destination address.
 - Soft-Reset (only with M87x / MUM856)
Restart of the mobile network engine via the software
 - Hard-Reset (only with M87x / MUM856)
Restart of the mobile network engine
 - Fallback (only with M876-4)
If the main connection fails, the data traffic is handled via the fallback connection. Provided the "Connection Fallback" function is configured.

4.5.23.1 Connection Fallback

The "Connection Fallback" function allows you to connect a network via 2 interfaces, e.g. the Internet. The priority determines whether the interface is the main connection or the fallback connection. If the main connection fails, the system switches over to the fallback connection. If the main connection is available again, the system switches over again. To monitor the main connection, use the "Connection Check" function.

Connection Check

Enable Connection Check

| Group Idx | Name | Source Interface | Interval | TTL | Retries | 1st Ping Target | 2nd Ping Target | 3d Ping Target |
|-----------|------|------------------|----------|-----|---------|-----------------|-----------------|----------------|
| 1 | LAN | usb0 | 60 | 128 | 3 | 192.168.1.20 | | |
| 2 | | Auto | 180 | 128 | 3 | | | |
| 3 | | Auto | 300 | 128 | 3 | | | |
| 4 | | Auto | 300 | 128 | 3 | | | |
| 5 | | Auto | 300 | 128 | 3 | | | |

| LAN | Group 2 | Group 3 | Group 4 | Group 5 | Action for | 1st Action | 2nd Action | 3rd Action | 4th Action | 5th Action |
|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------|------------|------------|------------|------------|------------|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | usb0 | None | Soft-Reset | None | Hard-Reset | None |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Device | None | None | Restart | None | None |

Description

- **Enable Connection Fallback**
Enable or disable the fallback function.
- **Priority**
 - 1 - Main connection
 - 2 - Fallback connection
- **Interface**
Specify the interface for the connection.
- **Status**
Shows the status of the connection:
 - Active: All data traffic is handled via the interface.
 - Fallback: If the main connection fails, the data traffic is processed via the fallback connection.
 - Not used: The connection is not used.
 - Not reachable: If the main connection fails, the status changes to "Not reachable".

4.6 "Interfaces" menu

4.6.1 Ethernet

4.6.1.1 Overview

The page shows the configuration for the data transfer for all ports of the device. You cannot configure anything on this page.

| Ports Overview | | | | | | | | | |
|------------------------|-----------|-------------------------|---------|-----------|------|---------|------|-------------|-------------------|
| Overview Configuration | | | | | | | | | |
| Port | Port Name | Port Type | Status | OperState | Link | Mode | MTU | Negotiation | MAC Address |
| P1 | | Switch-Port VLAN Hybrid | enabled | up | up | 100M FD | 1500 | enabled | 00-1b-1b-9a-31-94 |
| P2 | | Switch-Port VLAN Hybrid | enabled | down | down | 100M FD | 1500 | enabled | 00-1b-1b-9a-31-95 |
| P3 | | Switch-Port VLAN Hybrid | enabled | down | down | 100M FD | 1500 | enabled | 00-1b-1b-9a-31-96 |
| P4 | | Switch-Port VLAN Hybrid | enabled | down | down | 100M FD | 1500 | enabled | 00-1b-1b-9a-31-97 |

Refresh

Description

The table has the following columns:

- **Port**
Shows the configurable ports. The entry is a link. If you click on the link, the corresponding configuration page is opened.
- **Port Name**
Shows the name of the port.
- **Port Type** (only with routing)
Shows the type of the port. The following types are possible:
 - Switch Port VLAN Hybrid
 - Switch Port VLAN Trunk
- **Status**
Shows whether the port is on or off. Data traffic is possible only over an enabled port.
- **OperState**
Displays the current operational status. The operational status depends on the configured "Status" and the "Link". The available options are as follows:
 - Up
You have configured the status "enabled" for the port and the port has a valid connection to the network.
 - Down
You have configured the status "disabled" or "Link down" for the port or the port has no connection.

4.6 "Interfaces" menu

- **Link**
Shows the connection status to the network. With the connection status, the following is possible:
 - Up
The port has a valid link to the network, a link integrity signal is being received.
 - Down
The link is down, for example because the connected device is turned off.
- **Mode**
Shows the transfer parameters of the port.
- **Negotiation**
Shows whether the automatic configuration is enabled or disabled.
- **MAC Address**
Shows the MAC address of the port.

4.6.1.2 Configuration

Configuring ports

With this page, you can configure all the ports of the device.

The screenshot shows the 'Ports Configuration' web interface. At the top, there are two tabs: 'Overview' and 'Configuration', with 'Configuration' being the active tab. Below the tabs, the configuration for a specific port is displayed. The 'Port' is set to 'P1'. The 'Status' is 'enabled'. The 'Port Name' field is empty. The 'MAC Address' is '00-1b-1b-9a-32-2e'. The 'Mode Type' is 'Auto negotiation'. The 'Mode' is '100M FD'. The 'Negotiation' is 'enabled'. The 'Port Type' is 'Switch-Port VLAN Hybrid'. The 'OperState' is 'up' and the 'Link' is 'up'. At the bottom of the configuration area, there are two buttons: 'Set Values' and 'Refresh'.

Description

- **Port**
Select the port to be configured from the drop-down list.
 - **Status**
Specify whether the port is enabled or disabled.
 - enabled
The port is enabled. Data traffic is possible only over an enabled port.
 - disabled
The port is disabled but the connection remains.
-
- Note**
- Turn off unused ports.
-
- link down
The port is disabled and the connection to the partner device is terminated.
- **Port Name**
Here, enter a name for the port.
 - **MAC Address**
Shows the MAC address of the port.
 - **Mode Type**
From this drop-down list, select the transmission speed and the transfer mode of the port. The following settings are possible:
 - 10 Mbps full duplex (FD) or half duplex (HD)
 - 100 Mbps full duplex (FD) or half duplex (HD)
 - Auto negotiationIf you set the mode to "Auto negotiation", these parameters are automatically negotiated with the connected end device or network component. This must also be in the "Autonegotiation" mode.
-
- Note**
- Before the port and partner port can communicate with each other, the settings must match at both ends.
-
- **Mode**
Shows the transmission speed and the transmission mode of the port. The display depends on the set "Mode Type".
 - **Negotiation**
Shows whether the automatic configuration of the connection to the partner port is enabled or disabled.

4.6 "Interfaces" menu

- **Port Type**
 Select the type of port from the drop-down list.
 - Switch Port VLAN Hybrid
 The port sends tagged and untagged frames. It is not automatically a member of a VLAN.
 - Switch-Port VLAN Trunk
 The port only sends tagged frames and is automatically a member of all VLANs.
- **OperState**
 Displays the current operational status. The operational status depends on the configured "Status" and the "Link". The available options are as follows:
 - Up
 You have configured the status "enabled" for the port and the port has a valid connection to the network.
 - Down
 You have configured the status "disabled" or "Link down" for the port or the port has no connection.
- **Link**
 Shows the physical connection status to the network. The available options are as follows:
 - Up
 The port has a valid link to the network, a link integrity signal is being received.
 - Down
 The link is down, for example because the connected device is turned off.

4.6.2 PPP

4.6.2.1 Overview

This page shows the current status of the PPP connection.

PPP Overview

Overview | Configuration

| Interface | Name | Type | Operation | Status |
|-----------|------|------------------|-----------|---------|
| ppp2 | ppp2 | PPPoE (External) | disabled | Unknown |

Refresh

Description of the displayed values

This table contains the following columns:

- **Interface**
Shows the PPP interface. The entry is a link. If you click on the link, the corresponding configuration page is opened.
- **Name**
Shows the name of the PPP interface.
- **Type**
Shows the protocol of the PPP connection.
- **Operation**
Shows whether the PPP connection is activated or deactivated.
- **Status**
Shows the status of the PPP connection.
 - Ready
The PPP connection can be configured and enabled.
 - Connecting
The PPP connection is configured, enabled and the connection is being established.
 - Connected
The PPP connection is established.
 - Error
Error status in which operator intervention is required, e.g. wrong password.
 - Stopped
Error message of the server, e.g. incorrect login data. There is a wait time before login is attempted again.

4.6.2.2 Configuration

On this page, you configure the PPP connection. The point-to-point protocol (PPP) allows the connection of an external ADSL modem to an Ethernet interface and via this then a connection to the Internet. The interface is also called PPP interface.

The device acts as a router and logs in with the user name and password. All connected devices can use the PPP connection.

Description

The page contains the following:

- **Interface**
Select the PPP interface to be configured.
- **Name**
Shows the name of the PPP interface. You can change the name in "Layer 3 > Subnets".
- **Type**
Specify the protocol for the PPP connection.
 - PPPoE (Point-to-Point over Ethernet)
The PPP data is encapsulated in an Ethernet frame.
- **Operation**
Specify whether the PPP connection is activated or deactivated.
- **L2 Interface**
Specify the interface via which the PPP connection is established. Only VLANs with a configured subnet can be selected.
- **User Name**
Enter the user name. You will receive the user name from the DSL provider.
- **Password**
Enter the password. You will receive the password from the DSL provider.
- **Password Confirmation**
Repeat the password.

- **Forced Disconnect**
After a certain time, the DSL provider terminates the connection. Enable this option if you want to shift the forced disconnect of your provider to a specific time of day, for example at night outside normal office hours.
- **Time for Forced Disconnect**
Specify the time of day to which you want to shift the forced disconnect of the DSL provider. This is only possible if the correct system time is set on the device.
Input format: HH:MM

Procedure

1. Specify how the PPP interface obtains the IP address. The following options are available:
 - Dynamic
Activate the DHCP function on the PPP interface. You can configure this setting in "Layer 3 > Subnets > Configuration".

Note

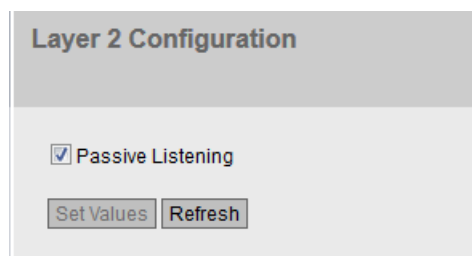
- With the subnets, a maximum of one interface can have a dynamic IP configuration.
-
- Static IP address
Deactivate the DHCP function on the PPP interface. Enter the IP address and the subnet mask.
2. Configure the PPP interface.
 3. Select "Enabled" for operation to activate the PPP interface.
 4. Click "Set Values" to adopt the settings.

4.7 "Layer 2" menu

4.7.1 Layer 2 configuration

Configuring layer 2

On this page, you create a basic configuration for the functions of layer 2.



The screenshot shows a web interface for "Layer 2 Configuration". At the top, the title "Layer 2 Configuration" is displayed in a grey header. Below the header, there is a checkbox labeled "Passive Listening" which is checked. At the bottom of the configuration area, there are two buttons: "Set Values" and "Refresh".

Description

- **Passive Listening**
When enabled the function ensures that the BPDUs from the RSTP network are forwarded transparently and return again. If this was not the case, loops would form at the connection point between RSTP and the ring.

4.7.2 VLAN

4.7.2.1 General

VLAN configuration page

On this page you specify whether or not the device forwards frames with VLAN tags transparently (IEEE 802.1D/VLAN-unaware mode) or takes VLAN information into account (IEEE 802.1Q/VLAN-aware mode). If the device is in the "802.1Q VLAN Bridge" mode, you can define VLANs and specify the use of the ports.

The possible settings on this page depend on what you select in the "Base Bridge Mode" box.

Note

Changing the Agent VLAN ID

If the configuration PC is connected directly to the device via Ethernet and you change the agent VLAN ID, the device is no longer reachable via Ethernet following the change.

Virtual Local Area Network (VLAN) General

General | **Port Based VLAN**

Base Bridge Mode: 802.1Q VLAN Bridge

VLAN ID:

| Select | VLAN ID | Name | Status | P1 | P2 | P3 | P4 |
|--------------------------|---------|------|--------|----|----|----|----|
| <input type="checkbox"/> | 1 | | Static | U | U | U | U |
| <input type="checkbox"/> | 2 | | Static | - | - | - | - |

2 entries.

Description

The page contains the following boxes:

- **Base Bridge Mode**

Note**Changing Base bridge mode**

Note the section "Changing Base bridge mode" in this chapter. This section describes how a change affects the existing configuration.

Select the required mode from the drop-down list. The following modes are possible:

- 802.1Q VLAN Bridge
Sets the mode "VLAN-aware" for the device. In this mode, VLAN information is taken into account.
- 802.1D Transparent Bridge
Sets the mode "VLAN-unaware" for the device. In this mode, VLAN tags are not taken into account or changed but are forwarded transparently. In this mode, you cannot create any VLANs. Only a management VLAN is available: VLAN 1.

- **VLAN ID**

Enter the VLAN ID in the "VLAN ID" input box.

Range of values: 1 ... 4094

The table has the following columns:

- **Select**

Select the row you want to delete.

- **VLAN ID**

Shows the VLAN ID. The VLAN ID (a number between 1 and 4094) can only be assigned once when creating a new data record and can then no longer be changed. To make a change, the entire data record must be deleted and created again.

- **Name**

Enter a name for the VLAN. The name only provides information and has no effect on the configuration. The length is a maximum of 32 characters.

- **Status**
Shows the status type of the entry in the internal port filter table. Here, "Static" means that the VLAN was entered statically by the user.
- **List of ports**
Specify the use of the port. The following options are available:
 - "-"
The port is not a member of the specified VLAN.
With a new definition, all ports have the identifier "-".
 - M
The port is a member of the VLAN. Frames sent in this VLAN are forwarded with the corresponding VLAN tag.
 - U (uppercase)
The port is an untagged member of the VLAN. Frames sent in this VLAN are forwarded without the VLAN tag. Frames without a VLAN tag are sent from this port.
 - u (lowercase)
The port is an untagged member of the VLAN, but the VLAN is not configured as a port VLAN. Frames sent in this VLAN are forwarded without the VLAN tag.
 - F
The port is not a member of the specified VLAN and cannot become a member of this VLAN even if it is configured as a trunk port.
 - T
This option is only displayed and cannot be selected in the WBM.
This port is a trunk port making it a member in all VLANs.
You configure this function in the CLI (Command Line Interface) using the "switchport mode trunk" command or in the WBM under "Interfaces > Ethernet > Configuration".

Changing Base bridge mode

VLAN-unaware (802.1D transparent bridge) → VLAN-aware (802.1Q VLAN bridge)

If you change the Base bridge mode from VLAN-unaware to VLAN aware, this has the following effects

- All static and dynamic unicast entries are deleted.

VLAN-aware (802.1Q VLAN bridge) → VLAN-unaware (802.1D transparent bridge)

If you change the Base bridge mode from VLAN-aware to VLAN-unaware, this has the following effects

- All VLAN configurations are deleted.
- A management VLAN is created: VLAN 1.
- All static and dynamic unicast entries are deleted.

802.1Q VLAN Bridge: Important rules for VLANs

Make sure you keep to the following rules when configuring and operating your VLANs:

- Frames with the VLAN ID "0" are handled as untagged frames but retain their priority value.
- As default, all ports on the device send frames without a VLAN tag to ensure that the end node can receive these frames.
- You will find the factory assignment of the ports in the section "VLAN (Page 40)".
- The VLANs are in different IP subnets. To allow these to communicate with each other, the route and firewall rule must be configured on the device.
- If an end node is connected to a port, outgoing frames should be sent without a tag (static access port). If, however, there is a further switch at this port, the frame should have a tag added (trunk port).

Procedure

Requirement:

For Base Bridge mode "802.1Q VLAN Bridge" is set

Creating a new VLAN

1. Enter an ID in the "VLAN ID" input box.
2. Click the "Create" button. A new entry is generated in the table. As default, the boxes have "-" entered.
3. Enter a name for the VLAN under Name.
4. Specify the use of the port in the VLAN. If, for example you select M, the port is a member of the VLAN. The frame sent in this VLAN is forwarded with the corresponding VLAN tag.
5. Specify the mode of the device.
6. Click the "Set Values" button.

4.7.2.2 Port Based VLAN

Processing received frames

On this WBM page, you specify the configuration of the port properties for receiving frames.

Port Based Virtual Local Area Network (VLAN) Configuration

General | **Port Based VLAN**

| | Priority | Port VID | Acceptable Frames | Ingress Filtering | Copy to Table |
|-----------|-------------|-------------|-------------------|-------------------|---------------|
| All ports | No Change ▾ | No Change ▾ | No Change ▾ | No Change ▾ | Copy to Table |

| Port | Priority | Port VID | Acceptable Frames | Ingress Filtering |
|------|----------|----------|-------------------|-------------------------------------|
| P1 | 0 ▾ | VLAN1 ▾ | All ▾ | <input checked="" type="checkbox"/> |
| P2 | 0 ▾ | VLAN1 ▾ | All ▾ | <input checked="" type="checkbox"/> |
| P3 | 0 ▾ | VLAN1 ▾ | All ▾ | <input checked="" type="checkbox"/> |
| P4 | 0 ▾ | VLAN1 ▾ | All ▾ | <input checked="" type="checkbox"/> |

Description

Table 1 has the following columns:

- **All ports**
Shows that the settings are valid for all ports of table 2.
- **Priority / Port VID / Acceptable Frames / Ingress Filtering**
In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports.
- **Priority**
Select the required priority assigned to untagged frames.
The CoS priority (Class of Service) used in the VLAN tag. If a frame is received without a tag, it will be assigned this priority. This priority specifies how the frame is further processed compared with other frames.
There are a total of eight priorities with values 0 to 7, where 7 represents the highest priority (IEEE 802.1p Port Priority).
- **Port VID**
Select the required VLAN ID. Only VLAN IDs defined in "VLAN > General" can be selected.
If a received frame does not have a VLAN tag, it has a tag with the VLAN ID specified here added to it and is sent according to the rules at the port.

- **Acceptable Frames**
Specify which types of frames will be accepted. The following alternatives are possible:
 - Tagged Frames Only
The device discards all untagged frames. Otherwise, the forwarding rules apply according to the configuration.
 - All
The device forwards all frames.
- **Ingress Filtering**
Specify whether the VID of received frames is evaluated.
You have the following options:
 - Enabled
The VLAN ID of received frames decides whether they are forwarded: To forward a VLAN tagged frame, the receiving port must be a member in the same VLAN. Frames from unknown VLANs are discarded at the receiving port.
 - Disabled
All frames are forwarded.

Steps in configuration

1. In the row of the port to be configured, click on the relevant cell in the table to configure it.
2. Enter the values to be set in the input boxes as follows.
3. Select the values to be set from the drop-down lists.
4. Click the "Set Values" button.

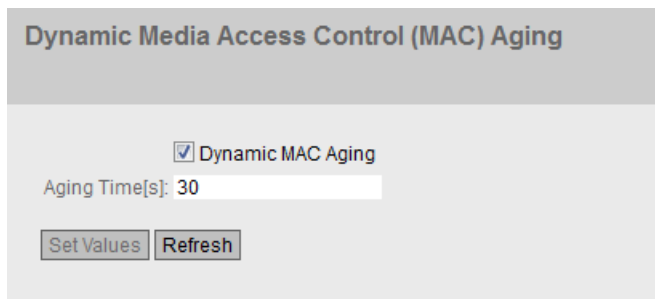
4.7.3 Dynamic MAC Aging

Protocol settings and switch functionality

The device automatically learns the source addresses of the connected nodes. This information is used to forward data frames to the nodes specifically involved. This reduces the network load for the other nodes.

If a device does not receive a frame whose source address matches a learnt address within a certain time, it deletes the learnt address. This mechanism is known as "Aging". Aging prevents frames being forwarded incorrectly, for example when an end device is connected to a different port.

If the check box is not enabled, a device does not delete learned addresses automatically.



Description of the displayed boxes

The page contains the following boxes:

- **Dynamic MAC Aging**
Enable or disable the function for automatic aging of learned MAC addresses.
- **Aging Time[s]**
Enter the time in seconds in steps of 15. After this time, a learned address is deleted if the device does not receive any further frames from this sender address.
Range of values: 15 - 630 (seconds)

Note

Rounding of the values, deviation from desired value

When you input the Aging Time, note that it is rounded to correct values. If you enter a value that cannot be divided by 15, the value is automatically rounded down.

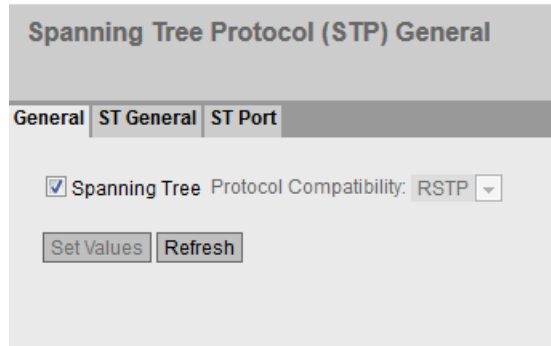
Steps in configuration

1. Select the "Dynamic MAC Aging" check box.
2. Enter the time in seconds in the "Aging Time[s]" input box.
3. Click the "Set Values" button.

4.7.4 Spanning Tree

4.7.4.1 General

This is the basic page for spanning tree. As default, Rapid Spanning Tree is enabled.



Spanning Tree Protocol (STP) General

General | ST General | ST Port

Spanning Tree Protocol Compatibility: RSTP

Set Values Refresh

Description

The page contains the following boxes:

- **Spanning Tree**
Enable or disable spanning tree.
- **Protocol Compatibility**
The following setting is available:
 - RSTP

Procedure

1. Select the "Spanning Tree" check box.
2. Click the "Set Values" button.

4.7.4.2 ST general

The page consists of the following parts.

- The left-hand side of the page shows the configuration of the device.
- The right-hand part shows the configuration of the root bridge that can be derived from the spanning tree frames received by a device.

Description

The page contains the following boxes:

- **Bridge Priority / Root Priority**
Which device becomes the root bridge is decided by the bridge priority. The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several devices in a network have the same priority, the device whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the bridge identifier. Since the root bridge manages all path changes, it should be located as centrally as possible due to the delay of the frames. The value for the bridge priority is a whole multiple of 4096. Range of values: 0 - 61440
- **Bridge Address / Root Address**
The bridge address shows the MAC address of the device and the root address shows the MAC address of the root bridge.
- **Root port**
Shows the port via which the switch communicates with the root bridge.
- **Root Cost**
The path costs from this device to the root bridge.

- Topology Changes / Last Topology Change**
 The entry for the device shows the number of reconfiguration actions due to the spanning tree mechanism since the last startup. For the root bridge, the time since the last reconfiguration is displayed as follows:
 - Seconds: Unit "sec" after the number
 - Minutes: Unit min after the number
 - Hours: Unit hr after the number
- Bridge hello time [s] / Root hello time [s]**
 Each bridge sends configuration frames (BPDUs) regularly. The interval between two configuration frames is the "Hello Time".
 Factory setting: 2 seconds
- Bridge Forward Delay[s] / Root Forward Delay[s]**
 New configuration data is not used immediately by a bridge but only after the period specified in the Forward Delay parameter. This ensures that operation is only started with the new topology after all the bridges have the required information.
 Factory setting: 15 seconds
- Bridge Max Age[s] / Root Max Age[s]**
 If the BPDU is older than the specified "Max Age" it is discarded.
 Factory setting: 20 seconds
- Reset Counters**
 Click this button to reset the counters on this page.

4.7.4.3 ST port

When the page is called, the table displays the current status of the configuration of the port parameters.

To configure them, click the relevant cells in the port table.

Spanning Tree (ST) Port

General | ST General | ST Port

| Port | Spanning Tree Status | Priority | Cost Calc. | Path Cost | State | Fwd. Trans. | Edge Type | Edge | Pt.P. Type | Pt.P. |
|---------|-------------------------------------|----------|------------|-----------|------------|-------------|-----------|--------------------------|------------|-------------------------------------|
| P1 | <input checked="" type="checkbox"/> | 144 | 0 | 200000 | Forwarding | 1 | Auto | <input type="checkbox"/> | - | <input checked="" type="checkbox"/> |
| P2 | <input type="checkbox"/> | 128 | 0 | 2000000 | Discarding | 0 | Auto | <input type="checkbox"/> | - | <input checked="" type="checkbox"/> |
| P3 | <input type="checkbox"/> | 128 | 0 | 2000000 | Discarding | 0 | Auto | <input type="checkbox"/> | - | <input checked="" type="checkbox"/> |
| P4 | <input type="checkbox"/> | 128 | 0 | 2000000 | Discarding | 0 | Auto | <input type="checkbox"/> | - | <input checked="" type="checkbox"/> |
| SHDSL 1 | <input checked="" type="checkbox"/> | 144 | 0 | 3511236 | Discarding | 355 | Auto | <input type="checkbox"/> | - | <input checked="" type="checkbox"/> |
| SHDSL 2 | <input checked="" type="checkbox"/> | 144 | 0 | 3511236 | Discarding | 356 | Auto | <input type="checkbox"/> | - | <input checked="" type="checkbox"/> |

Set Values Refresh

Description

Table 1 has the following columns:

- **All ports**
Shows that the settings are valid for all ports of table 2.
- **Spanning Tree Status**
In the drop-down list, select the setting for all ports. If "No Change" is selected, the entries of the corresponding column in table 2 remain unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

Table 2 has the following columns:

- **Port**
Shows the available ports.
- **Spanning Tree Status**
Specify whether or not the port is integrated in the spanning tree.

Note

If you disable the "Spanning Tree Status" option for a port, this may cause the formation of loops. The topology must be kept in mind.

- **Priority**
Enter the priority of the port. The priority is only evaluated when the path costs are the same. The value must be divisible by 16. If the value that cannot be divided by 16, the value is automatically adapted.
Range of values: 0 - 240.
The default is 128.
- **Cost Calc.**
Enter the path cost calculation. If you enter the value "0" here, the automatically calculated value is displayed in the "Path costs" box.
- **Path Cost**
This parameter is used to calculate the path that will be selected. The path with the lowest value is selected as the path. If several ports of a device have the same value for the path costs, the port with the lowest port number is selected.
If the value in the box "Cost Calc." is "0", the automatically calculated value is shown. Otherwise, the value of the "Cost Calc." box is displayed.
The calculation of the path costs is largely based on the transmission speed. The higher the achievable transmission speed is, the lower the value of the path costs.
Typical values for path costs with rapid spanning tree:
 - 10,000 Mbps = 2,000
 - 1000 Mbps = 20,000
 - 100 Mbps = 200,000
 - 10 Mbps = 2,000,000

The values can, however, also be set individually.

- **Status**

Displays the current status of the port. The values are only displayed and cannot be configured. The "Status" parameter depends on the configured protocol. The following values are possible:

 - Disabled
The port only receives and is not involved in STP, MSTP and RSTP.
 - Discarding
In the "Discarding" mode, BPDU frames are received. Other incoming or outgoing frames are discarded.
 - Listening

In this status, BPDUs are both received and sent. The port is involved in the spanning tree algorithm.
 - Learning
Stage prior to the "Forwarding" status, the port is actively learning the topology (in other words, the node addresses).
 - Forwarding
Following the reconfiguration time, the port is active in the network; it receives and forwards data frames.
- **Fwd. Trans**

Specifies the number of changes from the "Discarding" status to the "Forwarding" status.
- **Edge Type**

Specify the type of "edge port". You have the following options:

 - "-"
Edge port is disabled. The port is treated as a "no Edge Port".
 - Admin
Select this option when there is always an end device on this port. Otherwise a reconfiguration of the network will be triggered each time a connection is changed.
 - Auto
Select this option if you want a connected end device to be detected automatically at this port. When the connection is established the first time, the port is treated as a "no Edge Port".
 - Admin/Auto
Select these options if you operate a combination of both on this port. When the connection is established the first time, the port is treated as an "Edge Port".

4.7 "Layer 2" menu

- **Edge**
Shows the status of the port.
 - Enabled

An end device is connected to this port.
 - Disabled
There is a Spanning Tree or Rapid Spanning Tree device at this port.With an end device, a switch can change over the port faster without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the "Disabled" setting.
- **P.t.P. Type**
Select the required option from the drop-down list. The selection depends on the port that is set.
 - "-"
Point to point is calculated automatically. If the port is set to half duplex, a point-to-point link is not assumed.
 - P.t.P.

Also with half duplex, a point-to-point link is assumed.
 - Shared Media
Even with a full duplex connection, a point-to-point link is not assumed.

Note

Point-to-point link means a direct connection between two devices. A shared media connection is, for example, a connection to a hub.

4.7.5 LLDP

Identifying the network topology

LLDP (Link Layer Discovery Protocol) is defined in the IEEE 802.1 AB standard.

LLDP is a method used to discover the network topology. Network components exchange information with their neighbor devices using LLDP.

Network components that support LLDP have an LLDP agent. The LLDP agent sends information about itself and receives information from connected devices at periodic intervals. The received information is stored in the MIB.

Applications

PROFINET uses LLDP for topology diagnostics. In the factory setting, LLDP is enabled for all available ports; in other words, LLDP frames are sent on the ports.

The information sent is stored on every device with LLDP capability in an LLDP MIB file. Network management systems can access these LLDP MIB files using SNMP and therefore recreate the existing network topology. In this way, an administrator can find out which network components are connected to each other and can localize disruptions.

On this page, you have the option of enabling or disabling sending and/or receiving per port.

Link Layer Discovery Protocol (LLDP)

| | Setting | Copy to Table |
|-----------|--|---------------|
| All ports | No Change ▼ | Copy to Table |

| Port | Setting |
|------|--|
| P1 | Rx & Tx ▼ |
| P2 | Rx & Tx ▼ |
| P3 | Rx & Tx ▼ |
| P4 | Rx & Tx ▼ |
| P5 | Rx & Tx ▼ |

Description

Table 1 has the following columns:

Table 1 is only available when the device has more than one port.

- **All Ports**
Shows that the settings are valid for all ports.
- **Setting**
Select the setting from the drop-down list. If "No Change" is selected, the entry in table 2 remains unchanged.
- **Copy to Table**
If you click the button, the setting is adopted for all ports of table 2.

4.8 Menu "Layer 3 (IPv4)"

Table 2 has the following columns:

- **Port**
Shows the available ports.
- **Setting**
Specify the LLDP functionality. The following options are available:
 - Rx
This port can only receive LLDP frames.
 - Tx
This port can only send LLDP frames.
 - Rx & Tx
This port can receive and send LLDP frames.
 - "-" (disabled)
This port can neither receive nor send LLDP frames.

Procedure

1. Select the LLDP functionality of the port from the "Setting" drop-down list.
2. Click the "Set Values" button.

4.8 Menu "Layer 3 (IPv4)"

4.8.1 Static routes

On this page, you specify the routes via which data exchange can take place between the various subnets. Dynamic routing protocols are not supported, for example RIP, OSPF.

Static Routes

Destination Network:

Subnet Mask:

Gateway:

Interface:

Administrative Distance:

| Select | Destination Network | Subnet Mask | Gateway | Interface | Administrative Distance | Status |
|--------------------------|---------------------|-------------|--------------|-----------|-------------------------|--------|
| <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | 192.168.40.2 | vlan2 | not used | active |

1 entry.

Description

The page contains the following boxes:

- **Destination Network**
Enter the network address of the destination that can be reached via this route.
- **Subnet Mask**
Enter the corresponding subnet mask.
- **Interface**
Specify whether the network address can be reached via a certain interface or via the gateway (auto).
- **Gateway**
Enter the IPv4 address of the gateway via which this network address is reachable.
- **Administrative Distance**
Enter the metric for the route. The metric corresponds to the quality of a connection, for example speed, costs. If there are several equal routes, the route with the lowest metric value is used.
If you do not enter anything, "not used" is entered automatically. The metric can be changed later.
Range of values: 1 - 255 or -1 for "not used".
Here, 1 is the value for the best possible route. The higher value, the longer packets require to their destination.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Destination Network**
Shows the network address of the destination.
- **Subnet Mask**
Shows the corresponding subnet mask.
- **Gateway**
Shows the IPv4 address of the next gateway.
- **Interface**
Shows the interface of the route.
- **Administrative Distance**
Enter the metric for the route. When creating the route, "not used" is entered automatically. The metric corresponds to the quality of a connection, based for example on speed or costs. If there are several equal routes, the route with the lowest metric value is used.
Range of values: 1 - 255
Here, 1 is the value for the best possible route. The higher value, the longer the packets require to their destination.
- **Status**
Shows whether or not the route is active.

Procedure

1. Enter the network address of the destination in the "Destination Network" input box.
2. Enter the corresponding subnet mask in the "Subnet Mask" input box.
3. For "Interface", select the entry "auto".
4. Enter the gateway in the "Gateway" input box.
5. Enter the weighting of the route in "Administrative Distance".
6. Click the "Create" button. A new entry is generated in the table.
7. Click the "Set Values" button.

4.8.2 Subnets

4.8.2.1 Overview

The page shows the subnets for the selected interface. A subnet always relates to an interface and is created in the "Configuration" tab.

Connected Subnets Overview

Overview | **Configuration**

Interface:

| Interface | TIA Interface | Status | Interface Name | MAC Address | IP Address | Subnet Mask | Address Type | IP Assgn. Method | Address Collision Detection Status | MTU |
|-----------|---------------|----------|----------------|-------------------|-------------|---------------|--------------|------------------|------------------------------------|------|
| vlan1 | yes | enabled | INT | 00-1b-1b-cd-f2-17 | 192.168.1.1 | 255.255.255.0 | Primary | Static | Active | 1500 |
| ppp0 | - | disabled | ppp0 | 00-00-00-00-00-00 | 0.0.0.0 | 0.0.0.0 | Primary | Dynamic (DHCP) | Not supported | 1500 |

2 entries.

Description

The page contains the following box:

- **Interface**
Select the interface on which you want to configure another subnet.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Interface**
Shows the interface.
- **TIA Interface**
Shows whether the interface is a TIA interface.

- **Status**
Shows whether or not the interface is enabled.
- **Interface Name**
Shows the name of the interface.
- **MAC Address**
Shows the MAC address.
- **IP Address**
Shows the IPv4 address of the subnet.
- **Subnet Mask**
Shows the subnet mask.
- **Address Type**
Shows the address type. The following values are possible:
 - Primary
The first IPv4 address that was configured on the IPv4 interface.
 - Secondary
All other IPv4 addresses that were configured on the IPv4 interface.
- **IP Assignment Method**
Shows how the IPv4 address is assigned. The following values are possible:
 - Static
The IPv4 address is static. You enter the settings in "IP Address" and "Subnet Mask".
 - Dynamic (DHCP)
The device obtains a dynamic IPv4 address from a DHCPv4 server.

- **Address Collision Detection Status**

If new IPv4 addresses become active in the network, the "Address Collision Detection" function checks whether this can result in address collisions. The allows IPv4 addresses that would be assigned twice to be detected.

Note

The function does not run a cyclic check.

This column shows the current status of the function. The following values are possible:

- Idle
The interface is not enabled and does not have an IPv4 address.
- Starting
This status indicates the start-up phase. In this phase, the device initially sends a query as to whether the planned IPv4 address already exists. If the address is not yet been assigned, the device sends the message that it is using this IP address as of now.
- Conflict
The interface is not enabled. The interface is attempting to use an IPv4 address address that has already been assigned.
- Defending
The interface uses a unique IPv4 address. Another interface is attempting to use the same IPv4 address.
- Active
The interface uses a unique IPv4 address. There are no collisions.
- Not supported
The function for detection of address collisions is not supported.
- Disabled
The function for detection of address collisions is disabled.

- **MTU**

Shows the packet size.

4.8.2.2 Configuration

On this page, you configure the subnet for the interface.

Connected Subnets Configuration

Overview | **Configuration**

Interface (Name): vlan1 (INT) ▾
Status: enabled ▾
Interface Name: INT
MAC Address: 00-1b-1b-b6-32-79
 DHCP
IP Address: 192.168.16.42
Subnet Mask: 255.255.255.0
Broadcast IP Address: 192.168.16.255
Address Type: Primary
 TIA Interface
MTU: 1500

Description

The page contains the following:

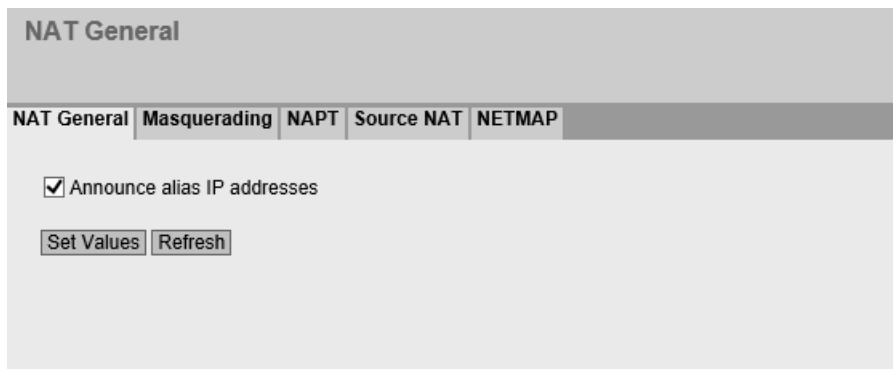
- **Interface (Name)**
Select the interface from the drop-down list.
- **Status**
Enable or disable the interface.
- **Interface Name**
Enter the name of the interface.
- **MAC Address**
Displays the MAC address of the selected interface.
- **DHCP**
When enabled, the interface obtains the IPv4 address from a DHCP server.
- **IP Address**
Enter the IPv4 address of the interface. The IPv4 addresses must not be used more than once.
- **Subnet Mask**
Enter the subnet mask of the subnet you are creating. Subnets on different interfaces must not overlap.
- **Broadcast IP Address**
If a specific IP address is to be used as the broadcast IP address of the subnet, enter this. Otherwise the last IP address of the subnet will be used.

- **Address Type**
Shows the address type. The following values are possible:
 - Primary
The first subnet of the interface.
 - Secondary
All further subnets of the interface.
- **TIA Interface**
Select whether this interface should become the TIA interface. The TIA interface defines on which VLAN the PROFINET functionalities are available. This mainly affects the device search with or via DCP.
- **MTU**
MTU (Maximum Transmission Unit) specifies the maximum size of the packet. If packets are longer than the set MTU, they are fragmented. The MTU covers the IP header and the headers of the higher layers.
The range of values is from 90 to 1500 bytes.

4.8.3 NAT

4.8.3.1 NAT General

On this WBM page, you enable Gratuitous ARP for alias IP addresses.



Description

On this page, you can enable the following option:

- **Announce alias IP addresses**
When the option is enabled, a Gratuitous ARP is sent for each alias IP address. This announces the IP address in the network, and the other devices can update their ARP cache. The Gratuitous ARP is only sent at the time of configuration, that is, during device startup or when an NAT rule (NETMAP) is being configured.

4.8.3.2 Masquerading

On this WBM page, you enable the rules for IP masquerading.

| Internet Protocol (IP) Masquerading | |
|---|-------------------------------------|
| NAT General Masquerading NAPT Source NAT NETMAP | |
| Interface | Enable Masquerading |
| vlan1 (INT) | <input type="checkbox"/> |
| vlan2 (EXT) | <input type="checkbox"/> |
| vlan3 | <input type="checkbox"/> |
| ppp2 | <input checked="" type="checkbox"/> |

Description

The table has the following columns:

- **Interface**
Interface to which the setting relates. Only interfaces with a configured subnet are available.
- **Enable Masquerading**
When enabled, with each outgoing data packet sent via this interface, the source IP address is replaced by the IP address of the interface.

4.8.3.3 NAPT

On this WBM page, you can configure a port translation in addition to the address translation.

The following port translations are possible:

- From a single port to the same port:
If the ports are the same, the frames will be forwarded without port translation.
- From a single port to a single port
The frames are translated to the port.
- From a port range to a single port
The frames from the port range are translated to the same port (n:1).
- From a port range to the same port range
If the port ranges are the same, the frames will be forwarded without port translation.

IP Network Address Port Translation (NAPT) (Port Forwarding)

Masquerading | **NAPT** | Source NAT | NETMAP

Source Interface:
 Traffic Type:
 Use Interface IP from Source Interface

Destination IP Address:
 Destination Port:
 Translated Destination IP Address:
 Translated Destination Port:

| Select | Source Interface | Traffic Type | Interface IP | Destination IP | Destination Port | Translated Destination IP | Translated Destination Port |
|--------------------------|------------------|--------------|-------------------------------------|----------------|------------------|---------------------------|-----------------------------|
| <input type="checkbox"/> | vlan2 | UDP | <input checked="" type="checkbox"/> | 10.10.0.100 | 8080 | 192.168.1.12 | 4500 |
| <input type="checkbox"/> | vlan2 | TCP | <input checked="" type="checkbox"/> | 10.10.0.100 | 4500 | 192.168.1.100 | 80 |

2 entries.

Description

The page contains the following boxes:

- **Source Interface**
Select the interface on which the queries will arrive.
- **Traffic Type**
Specify the protocol for which the address assignment is valid.
- **Use Interface IP from Source Interface**
When enabled, the IP address of the selected interface is used for "Dest IP Address".
- **Destination IP**
Enter the destination IP address. The frames are received at this IP address. Can only be edited if "Use Interface IP from Source Interface" is disabled.
- **Destination Port**
Enter the destination port. Incoming frames with this port as the destination port are forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
- **Translated Destination IP**
Enter the IP address of the node to which this frame will be forwarded.
- **Translated Destination Port**
Enter the number of the port. This is the new destination port to which the incoming frame will be forwarded. If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Source Interface**
Shows the interface from which the packets need to come. Only these packets are considered for port forwarding.
- **Traffic Type**
Shows the protocol for which the address assignment applies.

- **Interface IP**
Shows whether the IP address of the interface is used.
- **Destination IP**
Shows the destination IP address. The frames are received at this IP address.
- **Destination Port**
Shows the destination port. Incoming frames with this port as the destination port are forwarded.
- **Translated Destination IP**
Shows the IP address of the node to which the packets will be forwarded.
- **Translated Destination Port**
Shows the destination port to which the packets are translated.

4.8.3.4 Source NAT

On this page, you configure the rules for source NAT.

IP Source Network Address Translation (SNAT)

Masquerading | **NAPT** | **Source NAT** | NETMAP

Source Interface: vlan1 (INT) ▼
 Destination Interface: vlan1 (INT) ▼
 Source IP Address(es):
 Use Interface IP from Destination Interface
 Translated Source IP Address: 192.168.16.42
 Destination IP Address(es):

| Select | Source Interface | Destination Interface | Source IP Address(es) | Use Interface IP | Translated Source IP Address | Destination IP Address(es) |
|--------------------------|------------------|-----------------------|-----------------------|-------------------------------------|------------------------------|----------------------------|
| <input type="checkbox"/> | vlan1 | vlan2 | 192.168.1.50 | <input checked="" type="checkbox"/> | 10.10.0.100 | 0.0.0.0 |
| <input type="checkbox"/> | vlan1 | IPsec IPsec_to_M826 | 192.168.20.0 | <input type="checkbox"/> | 192.168.200.0 | 192.168.100.0 |

2 entries.

Note

Firewall rule with source NAT

Address translation with source NAT was only performed after the firewall; the non-translated addresses are therefore used.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Addresses"
- Destination (Range): Input from "Destination IP Addresses"

Description

- **Source Interface / Destination Interface**
Specify the direction of the connection establishment. Only connections established in this specified direction are taken into account.
The virtual interfaces of VPN connections can also be selected:
 - VLANx: VLANs with configured subnet
 - pppx or usb0: WAN interface
 - SINEMA RC: Connection to SINEMA RC Server
 - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection
 - OpenVPN: Either all OpenVPN connections (all) or a specific OpenVPN connection
-

Note

When you configure a NAT address translation to or from the direction of the VPN tunnel, only the IP addresses involved in the NAT address translation rules can be reached via the VPN tunnel.

- **Source IP Address(es)**
Specify the source IP addresses for which this source NAT rule is valid. Only the packets that correspond to the addresses entered are taken into account.
The following entries are possible:
 - IP address: Applies precisely to the specified IP address.
 - IP address range: Applies to a certain IP address range: Start IP address "-" End IP address, e.g. 192.168.100.10 - 192.168.100.20
 - IP subnet: Applies to several IPv4 addresses grouped together to form an IP address range: IP address/number of bits of the network part (CIDR notation)
- **Use Interface IP from Destination Interface**
When enabled, the IP address of the selected destination interface is used in "Translated Source IP Address".
- **Translated Source IP Address**
Enter the IP address with which the IP address of the sender is replaced. Can only be edited if "Use Interface IP from Destination Interface" is disabled.
- **Destination IP Address(es)**
Specify the destination IP addresses for which this source NAT rule is valid. Only the packets whose destination IP address is in the range of entered addresses are taken into account.
 - IP address: Applies precisely to the specified IP address.
 - IP address range: Applies to a certain IP address range: Start IP address "-" End IP address, e.g. 192.168.100.10 - 192.168.100.20
 - IP subnet: Applies to several IPv4 addresses grouped together to form an IP address range: IP address/number of bits of the network part (CIDR notation)

The table has the following columns:

- **Select**
Activate the check box in the row to be deleted.
- **Source Interface**
Shows the source interface.
- **Destination Interface**
Shows the destination interface.
- **Source IP Address(es)**
Shows the IP addresses of the senders for which address translation is required.
- **Use Interface IP**
Shows whether the IP address of the selected destination interface is used in "Translated Source IP Address".
- **Translated Source IP Address**
Shows the IP address with which the IP address of the sender is replaced.
- **Destination IP Address(es)**
Shows the IP addresses of the recipients for which address translation is required.

See also

NAT and firewall (Page 52)

4.8.3.5 NETMAP

On this WBM page, you specify the rules for NETMAP. NETMAP is static 1:1 mapping of network addresses in which the host part is retained. For more information, refer to the section "NAT and firewall (Page 51)".

NETMAP

Masquerading | **NAPT** | Source NAT | **NETMAP**

Type:

Source Interface:

Destination Interface:

Source IP Subnet:

Translated Source IP Subnet:

Destination IP Subnet:

Translated Destination IP Subnet:

Bidirectional Rule

Auto Firewall Rule

| Select | Type | Source Interface | Destination Interface | Source IP Subnet | Translated Source IP Subnet | Destination IP Subnet | Translated Destination IP Subnet |
|--------------------------|-------------|--------------------|-----------------------|------------------|-----------------------------|-----------------------|----------------------------------|
| <input type="checkbox"/> | Destination | vlan1 | ppp0 | 192.168.20.0/24 | - | 192.168.100.0/24 | 192.168.20.0/24 |
| <input type="checkbox"/> | Destination | vlan1 | IPsec M876_to_M816 | 192.168.20.0/24 | - | 192.168.100.0/24 | 192.168.10.0/24 |
| <input type="checkbox"/> | Source | ppp0 | vlan1 | 192.168.20.0/24 | 192.168.100.0/24 | 192.168.20.0/24 | - |
| <input type="checkbox"/> | Source | IPsec M876_to_M816 | vlan1 | 192.168.10.0/24 | 192.168.100.0/24 | 192.168.20.0/24 | - |

4 entries.

Note

Firewall rule with source NAT

Address translation with source NAT was only performed after the firewall; the non-translated addresses are therefore used.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Subnet"
- Destination (Range): Input from "Destination IP Subnet"

Firewall rule with destination NAT

Address translation with NAT was already performed before the firewall; the translated addresses are therefore used in the firewall.

Security > Firewall > IP rules

- Source (Range): Input from "Source IP Subnet"
 - Destination (Range): Input from "Translated Destination IP Subnet"
-

Description

- **Type**
Specify the type of address translation.
 - Source: Replacement of the source IP address
 - Destination: Replacement of the destination IP address
- **Source Interface**
Specify the source interface.
 - VLANx: VLANs with configured subnet
 - pppx or usb0: WAN interface
 - SINEMA RC: Connection to SINEMA RC Server
 - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection
 - OpenVPN: Either all OpenVPN connections (all) or a specific OpenVPN connection
- **Destination Interface**
Specify the destination interface.
 - VLANx: VLANs with configured subnet
 - pppx or usb0: WAN interface
 - SINEMA RC: Connection to SINEMA RC Server
 - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection
 - OpenVPN: Either all OpenVPN connections (all) or a specific OpenVPN connection
- **Source IP Subnet**
Enter the subnet of the sender.
The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation.

- **Translated Source IP Subnet**
Enter the subnet with which the subnet of the sender is replaced. Can only be edited with the setting "Source".
The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation.
- **Destination IP Subnet**
Enter the subnet of the recipient.
The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation.
- **Translated Destination IP Subnet**
Enter the subnet that will replace the subnet of the receiver. Can only be edited with the setting "Destination".
The subnet can also be a single PC or another subset of the subnet. Use the CIDR notation.
- **Bidirectional rule**
When this is enabled, the NETMAP rule for the opposite direction is automatically created when the NETMAP rule is created.
The NETMAP rules are not connected to one another after creation. This means that no synchronization takes place between the NETMAP rules when they are changed or deleted.
- **Auto Firewall Rule**
When this is enabled, the corresponding firewall rule is automatically created when the NETMAP rule is created. These firewall rules are displayed under "Security > Firewall > IP rules". If you change or delete the NETMAP rules, the corresponding firewall rules are adjusted or deleted.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Type**
Shows the direction of the address translation.
- **Source Interface**
Shows the source interface.
- **Destination Interface**
Shows the destination interface.
- **Source IP Subnet**
Shows the subnet of the sender. This entry can be changed when necessary.
- **Translated Source IP Subnet**
Shows the subnet of the sender with which the subnet of the sender is replaced. This entry can be changed when necessary.
- **Destination IP Subnet**
Shows the subnet of the recipient. This entry can be changed when necessary.
- **Translated Destination IP Subnet**
Shows the subnet of the recipient with which the subnet of the recipient is replaced. This entry can be changed when necessary.

See also

NAT and firewall (Page 52)

4.8.4 VRRPv3

4.8.4.1 Router

Introduction

Using the "Create" button, you can create new virtual routers. A maximum of 2 virtual routers can be configured. You can configure other parameters on the "Configuration" tab.

Virtual Router Redundancy Protocol v3 (VRRPv3) Router

Router **Configuration** Addresses Overview Addresses Configuration Interface Tracking

VRRPv3
 VRID-Tracking

Interface: vlan1

| Select | Interface | VRID | Virtual MAC Address | Primary Address | Router State | Master Address | Priority | Advert. Interval | Preempt |
|--------------------------|-----------|------|---------------------|-----------------|--------------|----------------|----------|------------------|---------|
| <input type="checkbox"/> | vlan3 | 1 | 00-00-5e-00-01-01 | 10.10.10.60 | Master | 10.10.10.60 | 100 | 100 | yes |

1 entry.

Note

- You can use VRRPv3 on VLAN interfaces.

Requirement

For the incoming packets to be forwarded to the device, enable the predefined IPv4 rule "VRRP".

Description

The page contains the following:

- VRRPv3**
 Enable or disable routing using VRRPv3.
- VRID-Tracking**
 Enable or disable VRID tracking.
 When enabled, all VRRP instances are monitored. If the status of a VRRP instance changes to "Initialize", the priority of all VRRP instances is reduced to the value "1".
 If the status of a VRRP instance changes, the original priority of all VRRP instances is restored.
- Interface**
 Select the required VLAN interface operating as virtual router.
- VRID**
 Enter the ID of the virtual router. This ID defines the group of routers that form a virtual router (VR). In the group, this is the same. It can no longer be used for other groups.
 Values 1...255 are valid.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Interface**
Shows the Interface that functions as the virtual router.
- **VRID**
Shows the ID of the virtual router.
- **Virtual MAC Address**
Shows the virtual MAC address of the virtual router.
- **Primary IP Address**
Shows the numerically lowest IPv4 address in this VLAN. The entry 0.0.0.0 means that the "Primary" address on this VLAN is used. Otherwise all IPv4 addresses configured on this VLAN in the "Layer 3 (IPv4) > Subnets" menu are valid values.
- **Router State**
Shows the current status of the virtual router. Possible values are:
 - Master
The router is the master router and handles the routing functionality for all assigned IPv4 addresses.
 - Backup
The router is the backup router. If the master router fails, the backup router takes over the tasks of the master router.
 - Initialize
The virtual router has just been turned on. It will soon change to the "Master" or "Backup" status.
- **Master IP Address**
Shows the IPv4 address of the master router.
- **Priority**
Shows the priority of the virtual router.
Valid values are 1-254.
If an IPv4 address is assigned to the VRRP router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRP routers. The higher the priority, the earlier the VRRP router becomes "Master".
- **Advert. Internal**
Shows the interval at which the master router sends VRRPv3 packets.
- **Preempt**
Shows the precedence of a router when changing roles between backup and master.
 - yes
This router has precedence when changing roles.
 - no
This router does not have precedence when changing roles.

VRRP and DHCP server

If you want to operate a DHCP server on the devices of a VRRP group, the DHCP server must be configured on the master router. Backup routers do not react to DHCP queries. Make sure that the master router is statically configured and that after a failure, becomes the master of the VRRP group again.

Procedure

1. Select the "VRRPv3" check box.
2. Select the required interface.
3. Enter the ID of the virtual router in the "VRID" input box.
4. Click the "Create" button. A new row is inserted in the table.
5. Select the "Reply to pings on virtual interfaces" check box so that virtual IPv4 addresses reply to pings as well.
6. Select the "VRID Tracking" check box to monitor the VRID.
7. Click the "Set Values" button. To configure the virtual router, click on the "Configuration" tab.

4.8.4.2 Configuration

Introduction

On this page, you configure the virtual router.

The screenshot shows the 'Virtual Router Redundancy Protocol v3 (VRRPv3) Konfiguration' page. At the top, there is a navigation bar with tabs: Router, Konfiguration (selected), Adressübersicht, Adresskonfiguration, Schnittstellenüberwachung, and Adressenüberwachung. Below the navigation bar, the configuration fields are as follows:

- Schnittstelle / VRID:
- Primäre Adresse:
- Priorität:
- Advertisement-Intervall[cs]:
- Track-ID:
- Priorität verringern:
- Aktuelle Priorität:

At the bottom of the configuration area, there are two buttons: 'Einstellungen übernehmen' and 'Aktualisieren'.

Description

The page contains the following:

- **Interface / VRID**
Select the ID of the virtual router to be configured.
- **Primary Address**
Select the primary IPv4 address. If the router becomes master router, the router uses this IPv4 address.

Note

If you only configure one subnet on this VLAN, no entry is necessary. The entry is then 0.0.0.0.

If you configure more than one subnet on the VLAN and you want a specific IPv4 address to be used as the source address for VRRP packets, select the IPv4 address. Otherwise, the numerically lowest IPv4 address will be used.

- **Priority**
Enter the priority of this virtual router. Valid values are 1-254.
If an IPv4 address is assigned to the VRRPv3 router that is also actually configured on the local IPv4 interface, the value 255 is entered automatically. All other priorities can be distributed freely among the VRRPv3 routers. The higher the priority, the earlier the VRRPv3 router becomes "Master".
- **Advertisement interval**
Enter the time interval after which a master router sends another VRRPv3 packet. Specified in centiseconds.
- **Track ID**
Select a track ID.
- **Decrement Priority**
Enter the value by which the priority of the VRRPv3 interface will be reduced.
- **Current Priority**
Shows the priority of the VRRPv3 interface after the monitored interface has changed to the "down" status.

Procedure

To configure a virtual router as the master router, follow the steps below:

1. Select the ID of the virtual router you want to configure from the "Interface / VRID" drop-down list.
2. Select the "Status" check box.
3. Select the source address from the "Primary Address" drop-down list.
4. From the "Priority" drop-down list, enter the priority of this virtual router.
5. Enter the interval in "Advertisement Interval".
6. Select a track ID.
7. Enter the value by which the priority of the VRRPv3 interface will be reduced
8. Click the "Set Values" button.

4.8.4.3 Address overview

Overview

This page shows which IPv4 addresses the virtual router monitors. Each virtual router can monitor one IPv4 address.

| Virtual Router Redundancy Protocol v3 (VRRPv3) Associated IP Addresses Overview | | | | | | |
|---|---------------|---------------------|---------------------------|---------------------------|---------------------------|---------------------------|
| Router | Configuration | Addresses Overview | Addresses Configuration | Interface Tracking | | |
| Interface | VRID | Number of Addresses | Associated IP Address (1) | Associated IP Address (2) | Associated IP Address (3) | Associated IP Address (4) |
| vlan3 | 1 | 1 | 10.10.10.150 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 |

Description of the displayed values

The table has the following columns:

- **Interface**
Shows the Interface that functions as the virtual router.
- **VRID**
Shows the ID of this virtual router.
- **Number of Addresses**
Shows the number of IPv4 addresses.
- **Associated IP Address (1) ...Associated IP Address (4)**
Shows the router IPv4 addresses monitored by this virtual router. If a router takes over the role of master, the routing function is taken over by this router for all these IPv4 addresses.

4.8.4.4 Address Configuration

Creating or changing the monitored IP addresses

On this page, you can create, modify or delete the IPv4 addresses to be monitored. Each virtual router can monitor one IPv4 address.

Virtual Router Redundancy Protocol v3 (VRRPv3) Associated IP Addresses Configuration

Router
Configuration
Addresses Overview
Addresses Configuration
Interface Tracking

Interface / VRID:

Associated IP Address:

| Select | Associated IP Address |
|--------------------------|-----------------------|
| <input type="checkbox"/> | 10.10.10.150 |

1 entry.

Description

The page contains the following:

- **Interface / VRID**
Select the ID of the virtual router.
- **Associated IP Address**
Enter the IPv4 address that the virtual router will monitor.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted
- **Associated IP Address**
Shows the IPv4 addresses that the virtual router monitors.

Procedure

1. Select the ID of the virtual router.
2. Enter the IPv4 address that the virtual router will monitor.
3. Click the "Create" button. A new entry is generated in the table.

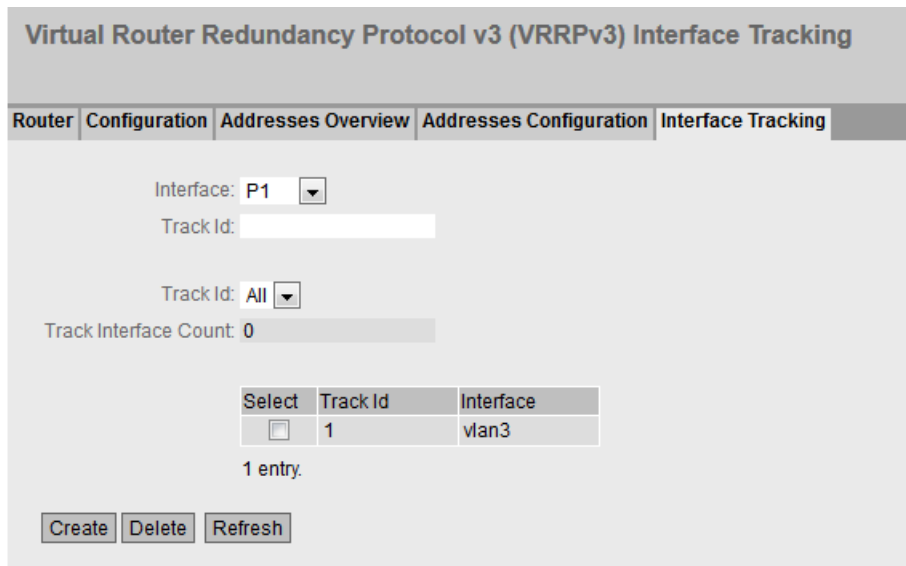
4.8.4.5 Interface Tracking

Introduction

On this page, you configure the monitoring of interfaces.

When the link of a monitored interface changes from "up" to "down", the priority of the assigned VRRP interface is reduced. You configure the value by which the priority is reduced on the page "Layer 3 > VRRPv3 > Configuration".

When the link of the interface changes back from "down" to "up", the original priority of the VRRP interface is restored.



Description

The page contains the following boxes:

- **Interface**
From the drop-down list, select the interface to be monitored.
- **Track ID**
Enter a track ID.
- **Track ID**
Select a track ID.
- **Track Interface Count**
Enter how many monitored interfaces need to change to the "down" status, before the priority is changed.

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Track ID**
Shows the track ID.
- **Interface**
Shows the interface that is being monitored.

Procedure

1. Select the required interface from the "Interface" drop-down list.
2. In the "Track ID" box, enter the required ID.
3. Click the "Create" button.
4. Select an ID from the "Track-ID" drop-down list:
5. In the "Track Interface Count" enter the number of interfaces.
6. Click the "Set Values" button.
7. Link the monitoring to a VRRP interface in the "Configuration" tab.

4.8.4.6 Address monitoring

Introduction

You configure the monitoring of IPv4 addresses on this page. The router sends a ping request to each of the configured IPv4 addresses within the specified time period. If no response is received within a specified time period, the VRRP priority of the corresponding interface is reduced.

Virtual Router Redundancy Protocol v3 (VRRPv3) Address Tracking

| Router | Configuration | Addresses Overview | Addresses Configuration | Interface Tracking | Address Tracking | | | | | | | | | | | | | | | |
|--|---------------|--------------------|-------------------------|--------------------|------------------|--------|----------|------------|----------------|------------------|--------------------------|----|----------------|---|----|--------------------------|----|----------------|---|----|
| Track Id: <input style="width: 150px;" type="text"/> IP Address: <input style="width: 350px;" type="text"/> | | | | | | | | | | | | | | | | | | | | |
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Select</th> <th style="width: 15%;">Track Id</th> <th style="width: 20%;">IP Address</th> <th style="width: 15%;">Ping Period[s]</th> <th style="width: 15%;">Ping Timeout [s]</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>17</td> <td>192.168.16.172</td> <td style="text-align: center;">5</td> <td style="text-align: center;">15</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td>45</td> <td>192.168.16.199</td> <td style="text-align: center;">5</td> <td style="text-align: center;">15</td> </tr> </tbody> </table> | | | | | | Select | Track Id | IP Address | Ping Period[s] | Ping Timeout [s] | <input type="checkbox"/> | 17 | 192.168.16.172 | 5 | 15 | <input type="checkbox"/> | 45 | 192.168.16.199 | 5 | 15 |
| Select | Track Id | IP Address | Ping Period[s] | Ping Timeout [s] | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | 17 | 192.168.16.172 | 5 | 15 | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | 45 | 192.168.16.199 | 5 | 15 | | | | | | | | | | | | | | | | |
| 2 entries. | | | | | | | | | | | | | | | | | | | | |
| <input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Set Values"/> <input type="button" value="Refresh"/> | | | | | | | | | | | | | | | | | | | | |

Description

The page contains the following boxes:

- **Track ID**
Enter the track ID.
- **IP Address**
Enter the IPv4 address to be monitored. You can enter a maximum of five IPv4 addresses.

The table has the following columns:

- **Select**
Select the row you want to delete.
- **Track ID**
Shows the track ID.
- **IP Address**
Shows the IPv4 address to be monitored.
- **Ping Period**
Shows the cycle time in seconds between two ping requests.
- **Ping Timeout**
Shows the time in seconds that the router waits for a ping response. The minimum duration is three times the ping period.

Procedure

1. In the "Track ID" box, enter the required ID.
2. In the "IPv4 Address" field, enter the IPv4 address that the virtual router is to monitor.
3. Click the "Create" button. A new entry is generated in the table.

4.9 Menu "Layer 3 (IPv6)"

4.9.1 Subnets

Connected Subnets

On this page, you can enable IPv6 on the interface. The interface is also called an IPv6 interface. An IPv6 interface can have several IPv6 addresses.

Connected Subnets

Subnets

Interface: vlan1

IPv6 Enable

Note: Once IPv6 is enabled on an interface it currently can only be disabled by deleting the interface.

IPv6 Address:

Prefix Length:

IPv6 Address Type: Unicast

Address Autoconfiguration (SLAAC)

| Select | Interface Name | IPv6 Address | Prefix Length | IPv6 Address Type | Address Autoconfiguration (SLAAC) | Duplicate Address Detection Status |
|--------------------------|----------------|--------------------------|---------------|-------------------|-----------------------------------|------------------------------------|
| <input type="checkbox"/> | vlan1 | 2222:4:: | 96 | Unicast | Enabled | Complete |
| | vlan1 | FE80::21B:1BFF:FECD:F217 | 64 | Link Local | Enabled | Complete |

2 entries.

Description

The page contains the following:

- **Interface**
Select the IP interface on which IPv6 will be enabled.
- **IPv6 Enable**
Enable or disable IPv6 on the interface.

Note

Disabling IPv6

If IPv6 is enabled on an interface, you can only disable IPv6 by deleting interface.

- **IPv6 Address**
Enter the IPv6 address. The entry depends on the selected address type.
- **Prefix Length**
Enter the number of left-hand bits belonging to the prefix.

- **IPv6 Address Type**
Select the address type.
 - Unicast
 - Anycast
 - Link Local: IPv6 address is only valid on the link
- **Address Autoconfiguration (SLAAC)**
Enable or disable the SLAAC (Stateless Address Auto Configuration) mechanism for the address configuration.
If SLAAC is enabled, there will be stateless auto configuration via NDP (Neighbor Discovery Protocol).

The table has the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Interface Name**
Shows the name of the interface.
- **IPv6 Address**
Shows the IP address of the subnet.
- **Prefix Length**
Shows the prefix length.
- **IPv6 Address Type**
Displays the address type. The following values are possible:
 - Unicast
 - Anycast
 - Link Local

- **Loopback**
Shows whether the "loopback" property is enabled. You configure the "loopback" property on the page "Layer 3 (IPv4) > Subnets > Overview".
- **Duplicate Address Detection Status**
In Address Autoconfiguration (SLAAC), the "Duplicate Address Detection Status" function prevents IPv6 addresses from being assigned twice. The device can only use free IPv6 addresses during autoconfiguration.
When the function is enabled, the check via NDP takes place automatically.

Note

The function does not run a cyclic check.

This column shows the current status of the function. The following values are possible:

- **Tentative**
This status indicates that the selected IPv6 address is being checked. The device sends a neighbor solicitation message to the selected IPv6 address.
- **Conflict**
This status indicates that the IPv6 address is already being used. In this case, a neighbor advertisement message with the selected IPv6 address is returned to the device.
- **Complete**
This status indicates that the selected IPv6 address can be used. In this case, the device did not receive feedback within a period of time and assumes that the IPv6 address is not yet assigned.
- **Down**
This status indicates that the interface is not active. No check is carried out.

Procedure

Automatically form link local address

1. Select the required interface.
2. Enable IPv6.
3. Click the "Create" button. In the table an entry with the interface is created and the automatically formed IPv6 address is displayed.

Assign link-local address

1. Select the required interface.
2. Enable IPv6.
3. In "IPv6 Address" enter the link local address, e.g. FE80::21B:1BFF:FE40:9155
4. Enter "64" in "Prefix Length".
5. For "IPv6 Address Type" select the entry "Link Local".
6. Click the "Create" button. In the table an entry with the interface is created and the IPv6 address is displayed.

4.9.2 NAT

4.9.2.1 Masquerading

On this WBM page, you enable the rules for IPv6 masquerading.

| Internet Protocol (IP) Masquerading | |
|---|-------------------------------------|
| Masquerading NAPT Source NAT NETMAP | |
| Interface | Enable Masquerading |
| vlan1 (INT) | <input type="checkbox"/> |
| vlan2 (EXT) | <input type="checkbox"/> |
| vlan3 | <input type="checkbox"/> |
| ppp2 | <input checked="" type="checkbox"/> |

Set Values Refresh

Description

The table has the following columns:

- **Interface**
Interface to which the setting relates. Only interfaces with a configured subnet are available.
- **Enable Masquerading**
When enabled, with each outgoing data packet sent via this interface, the source IP address is replaced by the IPv6 address of the interface.

4.10 "Security" menu

4.10.1 Users

4.10.1.1 Local users

On this page, you create local users with the corresponding rights. To create a user account, the logged on user must have the "admin" role.

Local Users

Local Users Roles Groups

User Account:

Password Policy: **high**

Password:

Password Confirmation:

Role: user

| Select | User Account | Role | Description | Remote Access |
|--------------------------|--------------|-------|---------------------------|---------------------------------|
| <input type="checkbox"/> | admin | admin | System defined local user | none <input type="text"/> |
| <input type="checkbox"/> | Service | user | | additional <input type="text"/> |

2 entries.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Description

The page contains the following:

- **User Account**

Enter the name for the user. The name must meet the following conditions:

- It must be unique.
- It must be between 1 and 250 characters long.
- The following characters must not be included: | § ? " ; : ß
- The characters for Space and Delete also cannot be included.

Note

User name cannot be changed

After creating a user, the user name can no longer be modified.

If a user name needs to be changed, the user must be deleted and a new user created.

Note

User names: admin

You can configure the device with this user name.

When you log in for the first time or log in after a "Restore Factory Defaults and Restart", you will be prompted to change the predefined password "admin". You can also rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible.

- **Password Policy**

Shows which password policy is being used.

- High
Password length: at least 8 characters, maximum 128 characters
At least 1 uppercase letter
At least 1 special character
At least 1 number
- User-defined
The password must meet the configured requirements. You configure the requirements under "Security > Passwords > Options".

- **Password**

Enter the password. The strength of the password depends on the set password policy.

It may not contain any of the following characters: | § ? " ; : ß \

- **Password Confirmation**

Enter the password again to confirm it.

- **Role**

Select a role.

You can choose between default and self-defined roles, refer to the page "Security > Users > Roles."

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
-
- Note**
- The users preset in the factory as well as logged in users cannot be deleted or changed.
-
- **User Account**
Shows the user name.
 - **Role**
Shows the role of the user.
 - **Description**
Displays a description of the user account. The description text can be up to 100 characters long.
 - **Remote Access**
 - Only
Only remote access, which means no rights other than logging into the WBM page for user-specific firewall.
 - None
No remote access. The user cannot log on to the user-specific firewall, but only to the WBM of the device.
 - Additional
The user can log on to both the WBM of the device and the user-specific firewall.

Procedure

Note

Changes in "Trial" mode

Even if the device is in "Trial" mode, changes that you carry out on this page are saved immediately.

Creating users

1. Enter the name for the user.
2. Enter the password for the user.
3. Enter the password again to confirm it.
4. Select the role of the user.
5. Click the "Create" button.
6. Enter a description of the user.
7. Click the "Set Values" button.

4.10 "Security" menu

Deleting users

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

4.10.1.2 Roles

Roles

On this page, you create roles that are valid locally on the device.

Note

The values displayed depend on the rights of the logged-in user.

The screenshot shows the 'User Roles' configuration interface. At the top, there are tabs for 'Local Users', 'Roles', and 'Groups', with 'Roles' selected. Below the tabs is a 'Role Name:' input field. The main area contains a table with the following data:

| Select | Role | Function Right | Description | Remote Access |
|--------------------------|-----------|----------------|--|---------------|
| <input type="checkbox"/> | user | 1 | System defined role, with readonly access to configuration data of this component. | none |
| <input type="checkbox"/> | admin | 15 | System defined role, with read/write access to configuration data of this component. | none |
| <input type="checkbox"/> | default | 1 | Internal role, for authenticated users without group/role mapping in this component. | none |
| <input type="checkbox"/> | everybody | 0 | Internal role, assigned to users when authentication fails. Access will be denied. | none |
| <input type="checkbox"/> | Radius | 1 | | additional |

Below the table, it says '5 entries.' and there are four buttons: 'Create', 'Delete', 'Set Values', and 'Refresh'.

Description

The page contains the following:

- **Role Name**
Enter the name for the role. The name must meet the following conditions:
 - It must be unique.
 - It must be between 1 and 64 characters long.

Note

Role name cannot be changed

After creating a role, the name of the role can no longer be changed.

If a name of a role needs to be changed, the role must be deleted and a new role created.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.

Note

Predefined roles and assigned roles cannot be deleted or modified.

- **Role**
Shows the name of the role.
- **Function Right**
Select the function rights of the role:
 - 1
Users with this role can read device parameters but cannot change them. Users with this role can change their own password.
 - 15
Users with this role can both read and change device parameters.

Note

Function right cannot be changed

If you have assigned a role, you can no longer change the function right of the role.

If you want to change the function right of a role, follow the steps outlined below:

1. Delete all assigned users.
 2. Change the function right of the role:
 3. Assign the role again.
-

- **Description**
Enter a description for the role. With predefined roles a description is displayed. The description text can be up to 100 characters long.
- **Remote Access**
 - None
No remote access. The user cannot log in to the dynamic firewall, but only to the WBM of the device.
 - Additional
The user can log in to both the WBM of the device and the dynamic firewall.

Procedure

Creating a role

1. Enter the name for the role.
2. Click the "Create" button.
3. Select the function rights of the role.
4. Enter a description of the role.
5. Click the "Set Values" button.

4.10 "Security" menu

Deleting a role

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

4.10.1.3 Groups

User groups

On this page you link a group with a role.

In this example the group "Administrators" is linked to the "admin" role: The group is defined on a RADIUS server. The role is defined locally on the device. When a RADIUS server authenticates a user and assigns the user to the "Administrators" group, this user is given rights of the "admin" role.

Note

The values displayed depend on the rights of the logged-in user.



Description

The page contains the following:

- **Group Name**
Enter the name of the group. The name must match the group on the RADIUS server. The name must meet the following conditions:
 - It must be unique.
 - It must be between 1 and 64 characters long.
 - The following are not permitted: § ? " ; :

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Group**
Shows the name of the group.

- **Role**
Select a role. Users who are authenticated with the linked group on the RADIUS server receive the rights of this role locally on the device.
You can choose between system-defined and self-defined roles, refer to the page "Security > Users > Roles."
- **Description**
Enter a description for the link of the group to a role. The description text can be up to 100 characters long.

Procedure

Linking a group to a role.

1. Enter the name of a group.
2. Click the "Create" button.
3. Select a role.
4. Enter a description for the link of a group to a role.
5. Click the "Set Values" button.

Deleting the link between a group and a role

1. Select the check box in the row to be deleted.
2. Click the "Delete" button. The entries are deleted and the page is updated.

4.10.2 Passwords

4.10.2.1 Passwords

Configuration of the passwords

A user with the "admin" role can change the password of already created users. With the "user" role, users can only change their own password.

Account Passwords

Passwords | **Options**

Current User: admin

Current User Password:

User Account: admin

Password Policy: custom

New Password:

Password Confirmation:

Description

The page contains the following:

- **Current User**
Shows the user that is currently logged in.
- **Current User Password**
Enter the password for the currently logged in user.
- **User Account**
Select the user whose password you want to change.

- **Password Policy**
Shows which password policy is being used when assigning new passwords.
 - High
Password length: at least 8 characters, maximum 128 characters
At least 1 uppercase letter
At least 1 special character
At least 1 number
 - User-defined
The password must meet the configured requirements. You configure the requirements under "Security > Passwords > Options"

- **New Password**
Enter the new password for the selected user.
It may not contain any of the following characters: | § ? " ; : ß \

Note

When you log in for the first time or log in after a "Restore Factory Defaults and Restart", you will be prompted to change the predefined password "admin". You can also rename the "admin" user preset in the factory once. Afterwards, renaming "admin" is no longer possible.

The factory setting for the password when the devices ship is as follows:

- admin: admin

Note**Changing the password in Trial mode**

Even if you change the password in Trial mode, this change is saved immediately.

- **Password Confirmation**
Enter the new password again to confirm it.

4.10.2.2 Options

On this page, you specify which password policy will be used when assigning new passwords.

Password Options

Passwords
Options

Password Policy: high

New Password Policy: high ▼

Password Policy Details:

Minimum Password Length: 8

Minimum Number of Numeric Characters: 1

Minimum Number of Special Characters: 1

Minimum Number of Uppercase Letters: 1

Minimum Number of Lowercase Letters: 0

Set Values
Refresh

Description

- **Password Policy**
Shows which password policy is currently being used.
- **New Password Policy**
Select the required setting from the drop-down list.
 - High
Password length: at least 8 characters, maximum 128 characters
At least 1 number
At least 1 special character
At least 1 uppercase letter
 - Low
Password length: at least 6 characters, maximum 128 characters
 - User-defined
Configure the desired password requirements under "Password Policy Details".
- **Password Policy Details**
When you have selected the "High" or "Low" password policy, the relevant password requirements are displayed.
When you have selected the "User-defined" password policy, you can configure the relevant password requirements.
 - Minimum Password Length
Specifies the minimum length of a password.
 - Minimum Number of Numeric Characters
Specifies the minimum number of numeric characters in a password.
 - Minimum Number of Special Characters
Specifies the minimum number of special characters in a password.
 - Minimum Number of Uppercase Letters
Specifies the minimum number of uppercase characters in a password.
 - Minimum Number of Lowercase Letters
Specifies the minimum number of lowercase characters in a password.

4.10.3 AAA

4.10.3.1 General

Login of network nodes

The designation "AAA" stands for "Authentication, Authorization, Accounting". This feature is used to identify and allow network nodes, to make the corresponding services available to them and to specify the range of use.

On this page, you configure the login.

Description

The page contains the following boxes:

Note

To be able to use the login authentication "RADIUS", "Local and RADIUS" or "RADIUS and fallback Local", a RADIUS server must be stored and configured for user authentication.

- **Login Authentication**

Specify how the login is made:

- Local
The authentication must be made locally on the device.
- RADIUS
The authentication must be handled via a RADIUS server.
- Local and RADIUS
The authentication is possible both with the users that exist on the device (user name and password) and via a RADIUS server.
The user is first searched for in the local database. If the user does not exist there, a RADIUS request is sent.
- RADIUS and fallback Local
The authentication must be handled via a RADIUS server.
A local authentication is performed only when the RADIUS server cannot be reached in the network.

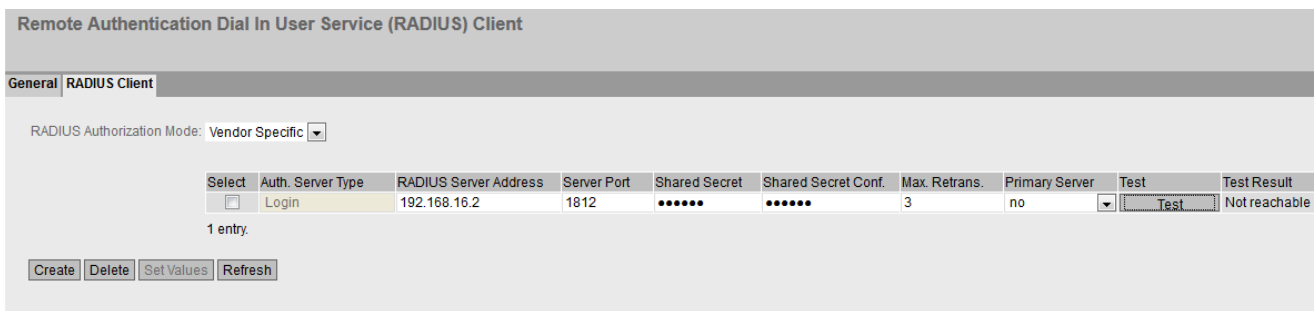
4.10.3.2 RADIUS client

Authentication over an external server

The concept of RADIUS is based on an external authentication server.

Each row of the table contains access data for one server. In the search order, the primary server is queried first. If the primary server cannot be reached, secondary servers are queried in the order in which they are entered.

If no server responds, there is no authentication.



Description

The page contains the following boxes:

- **RADIUS Authorization Mode**

For the login authentication, the RADIUS authorization mode specifies how the rights are assigned to the user with a successful authentication.

- Conventional

In this mode the user is logged in with administrator rights if the server returns the value "Administrative User" to the device for the attribute "Service Type". In all other cases the user is logged in with read rights.

- SiemensVSA

In this mode, the assignment of rights depends on whether and which group the server returns for the user and whether or not there is an entry for the user in the table "External User Accounts".

The table has the following columns:

- **Select**

Select the row you want to delete.

- **RADIUS Server Address**

Enter the IP address or the FQDN (Fully Qualified Domain Name) of the RADIUS server.

- **Server Port**

Here, enter the input port on the RADIUS server. As default, input port 1812 is set. The range of values is 1 to 65535.

- **Shared Secret**

Enter your access ID here. The range of values is 1...128 characters

- **Shared Secret Conf.**

Enter your access ID again as confirmation.

- **Max. Retrans.**

Here, enter the maximum number of retries for an attempted request.

The initial connection attempt is repeated the number of times specified here before another configured RADIUS server is queried or the login counts as having failed. As default 3 retries are set, this means 4 connection attempts. The range of values is 1 to 5.

- **Primary Server**

Using the options in the drop-down list, specify whether or not this server is the primary server. You can select one of the options "yes" or "no".

- **Test**
With this button, you can test whether or not the specified RADIUS server is available. The test is performed once and not repeated cyclically.
- **Test Result**
Shows whether or not the RADIUS server is available:
 - Not reachable
The IP address is not reachable.
The IP address is reachable, the RADIUS server is, however, not running.
 - Reachable, key not accepted
The IP address is reachable, the RADIUS server does not, however accept the shared secret.
 - Reachable, key accepted
The IP address is reachable, the RADIUS server accepts the specified shared secret.

Procedure

Entering a new server

1. Click the "Create" button. A new entry is generated in the table.
The following default values are entered in the table:
 - RADIUS Server Address: 0.0.0.0
 - Server Port: 1812
 - Max. Retrans.: 3
 - Primary server: No
 2. In the relevant row, enter the following data in the input boxes:
 - RADIUS Server Address
 - Server Port
 - Shared Secret
 - Shared Secret Conf
 - Max. Retrans.: 3
 - Primary server: No
 3. If necessary check the reachability of the RADIUS server.
 4. Click the "Set Values" button.
- Repeat this procedure for every server you want to enter.

4.10 "Security" menu

Modifying servers

1. In the relevant row, enter the following data in the input boxes:
 - RADIUS Server Address
 - Server Port
 - Shared Secret
 - Shared Secret Conf
 - Max. Retrans.
 - Primary Server
2. If necessary check the reachability of the RADIUS server.
3. Click the "Set Values" button.

Repeat this procedure for every server whose entry you want to modify.

Deleting servers

1. Click the check box in the first column before the row you want to delete to select the entry for deletion.
Repeat this for all entries you want to delete.
2. Click the "Delete" button. The data is deleted from the memory of the device and the page is updated.

4.10.4 Certificates

4.10.4.1 Overview

All loaded files (certificates and keys) are shown on this WBM page. You have the following options for loading files on the device:

- System > Load&Save > HTTP
- System > Load&Save > TFTP
- System > Load&Save > SFTP

| Certificates Overview | | | | |
|--------------------------|--------------|--|-------|---|
| Overview | | Certificates | | |
| Select | Type | Filename | State | Subject DN |
| <input type="checkbox"/> | Key File | Configuration 1.UAE938401@GF13A.Module1_Key.pem | valid | C=DE O=Siemens CN=PEA46-UAE938401-GF13A |
| <input type="checkbox"/> | Machine Cert | Configuration 1.UAE938401@GF13A.Module1_Cert.pem | valid | C=DE O=Siemens CN=PEA46-UAE938401-GF13A |
| <input type="checkbox"/> | CA Cert | Configuration 1.UAE938401@GF13A.Module1_CACert.pem | valid | C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99 |
| <input type="checkbox"/> | Remote Cert | Configuration 1.Group1.Module1.cer | valid | C=DE O=Siemens CN=PEA46-UAE938401-GF13A |

4 entries.

Figure 4-1 Part 1

| Issuer DN | Issue Date | Expiry Date | Used |
|---|---------------------|---------------------|------|
| C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99 | 12/04/2017 14:42:41 | 12/04/2037 23:59:59 | - |
| C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99 | 12/04/2017 14:42:41 | 12/04/2037 23:59:59 | - |
| C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99 | 12/04/2017 14:42:36 | 12/04/2037 23:59:59 | - |
| C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99 | 12/04/2017 14:42:41 | 12/04/2037 23:59:59 | - |

Figure 4-2 Part 2

Description

- **Select**
Select the check box in the row to be deleted. Only unused certificates can be deleted.
- **Type**
Shows the type of the loaded file.
 - CA Cert
The CA certificate is signed by a CA (Certification Authority).
 - Machine certificate
 - Key File
 - Remote Cert
Partner certificate

4.10 "Security" menu

- **Filename**
Shows the file name.
- **Status**
Shows whether the certificate is valid or has already expired.
- **Subject DN**
Shows the name of the applicant.
- **Issuer DN**
Shows the name of the certificate issuer.
- **Issue Date**
Shows the start of the period of validity of the certificate
- **Expiry Date**
Shows the end of the period of validity of the certificate.
- **Used**
Shows which function uses the certificate.

4.10.4.2 Certificates

The format of the certificate is based on X.509, a standard of the ITU-T for creating digital certificates. This standard describes the schematic structure of X509 certificates. You will find further information on this on the Internet at "<http://www.itu.int>".

On this WBM page, the content of the following structure elements can be displayed. If the structure element does not exist or is not completed in the selected certificate, nothing is shown in the box on the right. Certain entries can only be edited if they are supported.

Certificate Properties

Overview
Certificates

Filename: Configuration 1.UAE938401@GF13A.Module1_Key.pem ▼

Type: Key File

Subject DN: C=DE O=Siemens CN=PEA46-UAE938401-GF13A

Issuer DN: C=DE O=Siemens CN=P0642039A-GF3973FF368C54A99

Subject Alternate Name: N/A

Issue Date: 12/04/2017 14:42:41

Expiry Date: 12/04/2037 23:59:59

Serial: N/A

Used: -

Crypto Algorithm: RSA

Key Usage:

Extended Key Usage:

Key File: Configuration 1.UAE938401@GF13A.Module1_Key.pem

Certificate Revocation List 1st URL: -

Certificate Revocation List 2nd URL: -

Certificate: Configuration 1.UAE938401@GF13A.Module1_Cert.pem

Passphrase:

Passphrase Confirmation:

Set Values
Refresh

Description

- **Filename**
Select the required certificate.
- **Type**
Shows the type of the loaded file.
 - CA Cert
The CA certificate is signed by a CA (Certification Authority).
 - Machine certificate
 - Key File
 - Remote Cert
Partner certificate
- **DN**
Shows the name of the applicant.

4.10 "Security" menu

- **Issuer DN**
Shows the name of the certificate issuer.
- **Subject Alternate Name**
If it exists, an alternative name of the applicant is displayed.
- **Issue Date**
Shows the start of the period of validity of the certificate
- **Expiry Date**
Shows the end of the period of validity of the certificate.
- **Serial Number**
Shows the serial number of the certificate.
- **Used**
Shows which function uses the certificate.
- **Crypto Algorithm**
Shows which cryptographic method is used.
- **Key Usage**
Shows the purpose that the key belonging to the certificate is used for, e.g. to verify digital signatures.
- **Extended Key Usage**
Shows whether the purpose is additionally restricted, e.g. only to verify signatures of the CA certificate.
- **Key File**
Shows the key file.
- **Certificate Revocation List 1st URL**
Enter the URL with which the revocation list can be called up. Can only be edited if supported by the certificate.
- **Certificate Revocation List 2nd URL**
Enter an alternative URL. If the revocation list cannot be called up using the 1st URL, the alternative URL is used. Can only be edited if supported by the certificate.
- **Certificate**
Shows the name of the certificate.
- **Passphrase**
Enter the password for the certificate. Can only be edited if the encrypted file is password protected.
- **Passphrase Confirmation**
Enter the password again. Can only be edited if the encrypted file is password protected.

4.10.5 Firewall

4.10.5.1 General

On this WBM page, you enable the firewall.

Note

Please remember that if you disable the firewall, your internal network is unprotected.

Description

The page contains the following:

- **Activate Firewall**
When enabled, the firewall is active.
- **TCP Idle Timeout [s]**
Enter the required time in seconds. If no data exchange takes place, the TCP connection is terminated automatically when this time has elapsed.
The range of values is 1 to 21474836.
Default setting: 86400 seconds
- **UDP Idle Timeout [s]**
Enter the required time in seconds. If no data exchange takes place, the UDP connection is terminated automatically when this time has elapsed.
The range of values is 1 to 21474836.
Default setting: 300 seconds
- **ICMP Idle Timeout [s]**
Enter the required time in seconds. If no data exchange takes place, the ICMP connection is terminated automatically when this time has elapsed.
The range of values is 1 to 21474836.
Default setting: 300 seconds
- **Enable State Synchronization**
- **Local Interface**
Interfaces with DHCP cannot be selected.

4.10 "Security" menu

- Local IP Address
- IP Address Sync Partner
- Port Sync Partner

4.10.5.2 Predefined

The WBM page contains predefined IP packet filter rules. If you create your own IP packet filter rules, these have a higher priority than the predefined IP packet filter rules.

Set which IPv4 services of the device should be reachable from which interface.

Predefined

General | **Predefined** | User Specific | IP Services | ICMP Services | IP Protocols | IP Rules

Allow device services:

| Interface | IP Version | All | HTTP | HTTPS | DNS | SNMP | Telnet | SMS Relay | IPsec VPN | SSH | DHCP | Ping | System Time | Cloud Connector | VRPP |
|-------------|------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|
| vlan1 (INT) | IPv4 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| vlan1 (INT) | IPv6 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ppp0 | IPv4 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ppp0 | IPv6 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Set Values Refresh

Description

- **Interface**

The list is dynamic.

 - pppx or usb0 (only with M876-4)
Allows access from the WAN interface to the device.
 - VLANx
Allows access from the IP subnet to the device. VLANs with configured IP subnet are available.
 - SINEMARC
Allows access from the SINEMA RC server to the device. Only available with KEY-PLUG SINEMA RC.
 - OpenVPN connection, IPsec VPN connection
Allows the VPN tunnel partners reachable via the VPN connection to access the device. If you have created a VPN connection, the connection name will be displayed in the list.
 - **IP Version**
Shows the IP version to which the firewall rules apply.
IPv4
IPv6 (only with M876-4)
- Access over the firewall is permitted to the following IPv4 services:
 - All
All predefined IPv4 services.
 - HTTP
For access to Web Based Management.
 - HTTPS
For secure access to Web Based Management.

Note

HTTP and HTTPS deactivated

If you disable HTTP and HTTPS, the WBM of the device can no longer be reached.

HTTPS disabled

When you disable HTTPS, you can only access the WBM using HTTP. This assumes that "HTTP & HTTPS" is set in "System > Configuration > HTTP Services". If for example "Redirect HTTP to HTTPS" is set, access via HTTP cannot be redirected to HTTPS. This means that the WBM of the device can no longer be reached.

- DNS
DNS queries to the device. Necessary only if the "DNS-Relay" function is enabled on the device.
- SNMP
Incoming SNMP connections. Required, for example, to access the SNMP information of the device using a MIB browser.
- Telnet
For unencrypted access to the CLI.

4.10 "Security" menu

- SMS Relay (M874 / M876 only)
For sending SMS messages from the local network.
- IPsec VPN
Allows IKE (Internet Key Exchange) data transfer from the external network to the device.
Necessary if an IPsec VPN remote station needs to establish a connection to this device.
- SSH
For encrypted access to the CLI.
- DHCP
Access to the DHCP server or the DHCP client.
- Ping
Access to the ping function.
- System time
Access to NTP and SNTP.
- Cloud Connector
Access to the integrated TIA Portal Cloud Connector Server and the devices accessible via the interface.
- VRRP
Access to VRRPv3

4.10.5.3 Dynamic Rules

On this page, you define dynamic rule sets. Firewall rules that are required for remote access, for example, can be summarized with a rule set.

You can assign a rule set to one or more users. If login of this user was successful, the firewall rule set intended for this user is enabled.

A timer is started after login. When the time expires, the user is automatically logged out from the device.

You can also control the rule sets over time. A start time and an end time are configured. Between these times, the firewall rules assigned to the rule set are enabled.

Dynamic Rules

General | Predefined | **Dynamic Rules** | IP Services | ICMP Services | IP Protocols | IP Rules

Rule Set
Name:

| Select | No. | Name | Comment | Timeout [min] |
|--------------------------|-----|---------|---------|---------------|
| <input type="checkbox"/> | 1 | Service | | 30 |

1 entry.

Rule Set Assignment
Type:

| User Account | Role | Rule Set | Combined | Remaining Time | Force Deactivate |
|--------------|------|----------|----------|----------------|---|
| Service | user | - | None | - | <input type="button" value="Force Deactivate"/> |

Description

"Rule set" area

- **Name**
Define a unique name for the rule set. If you click the "Create" button, a new row with a unique number is created.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **No.**
Shows the unique number of the entry.
- **Name**
Name of the rule set. The name can be changed if required.
- **Comment**
Comment that describes the rule set in more detail.
- **Timeout [min]**
Access is time-limited. Specify the duration of the access. If needed, the user can extend the access time via the "Reset Timeout" button on the "Dynamic Firewall Rules Information" page.

"Rule Set Assignment" area

- **Type**
Specify which rule set will be assigned to whom. The display of the following table depends on the selection for "Type".
 - User Account
The rule set is activated through a local user account.
 - Digital Input
The rule set is executed by controlling the digital input. The prerequisite for this is that the entry "Digital Input" is activated for the "Firewall" event under "System > Events > Configuration".
 - Radius Role
The rule set is activated through a RADIUS role.
 - RADIUS User
The rule set is activated through a RADIUS user.
 - Time triggered
Enforcement of the rule set is time-triggered.

The "User Account" table contains the following columns:

- User Account
Only users with the remote access "only" or "additional" are displayed.
- Role
Shows the role of the user.
- Rule set
Define the rule set that is valid for this user.
- Combined with
Combines the user login with an event, e.g. the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and user login must be successful.
- Remaining Time
When this user is logged on, the remaining time for access is displayed.
- Force Deactivate
A user with administrator rights can log off the active user with this button.

The "**Digital Input**" table contains the following columns:

- Digital Input
The available digital inputs.
- Rule set
Define the rule set that is controlled via the digital input.
- Dynamic Source (Range)
Enter the IP address or an IP range that is allowed to send IP packets.
- Status
Shows the remaining time for access.

The "**RADIUS Role**" table contains the following columns:

- **Role**
Shows the role name. Only roles with the remote access "additional" are displayed. The prerequisite is that the role is created on the RADIUS server and users are assigned to the role.
- **Rule set**
Define the rule set that is valid for this RADIUS role.
- **Combined with**
Combines the logon with an event, e.g. the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and login must be successful.
- **Number**
After successful login, the number of users active via RADIUS that are assigned to the RADIUS role is displayed.
- **Force Deactivate**
A user with administrator rights can log out the RADIUS role with this button.

The "**RADIUS User**" table contains the following columns:

- **User**
Shows the users assigned to the role.
A role with the remote access "additional" is created on the device and assigned to a group. The names of the group must match exactly the names of the user groups on the RADIUS server.
- **Role**
The role assigned to the RADIUS user.
- **Remaining Time**
When this user is logged on, the remaining time for access is displayed.
- **Force Deactivate**
A user with administrator rights can log out the RADIUS role with this button.

The "**Time triggered**" table contains the following columns:

- **Time triggered**
Index of the entry.
- **Rule set**
Define the rule set that is time triggered.
- **Combined with**
Combines the time triggering with an event, for example, the "Digital Input" event. To log in to the WBM page for the dynamic firewall, voltage must be present at the digital input and login must be successful.
- **Cycle**
Specify the enforcement cycle for the time triggering.
 - Daily
 - Weekly
 - Monthly

4.10 "Security" menu

- Days
If "Weekly" or "Monthly" is set for the cycle, specify the days.
Enter the days separated by commas, e.g. 1,3,4
 - Weekly: 1 - 7
 - Monthly: 1 - 31
- Dynamic Source (Range)
 - Individual IP address: Specify the IP address
 - IP range: Specify the range with start address "-" end address, e.g.
IPv4: 192.168.100.10 - 192.168.100.20
IPv6: fe80:: - febf::
 - All IP addresses:
IPv4: " 0.0.0.0/0"
IPv6: ":::"
 - If the rule set is activated by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.
- Start time
Enter the start time in the format HH:MM.
- End time
Enter the end time in the format HH:MM.
- Enable
When enabled, the rule set is time-triggered. The connection is briefly interrupted when the time-triggered firewall rules are initiated.

4.10.5.4 IP services

On this WBM page, you define IP services. Using the IP service definitions, you can define firewall rules for specific services. You select a name and assign the service parameters to it. When you configure the IP rules, you simply use this name.

Internet Protocol (IP) Services

General | Predefined IPv4 | IP Services | ICMP Services | IP Protocols | IP Rules

Service Name:

| Select | Service Name | Transport | Source Port (Range) | Destination Port (Range) |
|--------------------------|--------------|-----------|---------------------|--------------------------|
| <input type="checkbox"/> | DNS | UDP | * | 53 |
| <input type="checkbox"/> | HTTP | TCP | * | 80 |

2 entries.

Create | Delete | Set Values | Refresh

Description

The page contains the following:

- **Service Name**
Enter the name of the IP service. The name must be unique.

This table contains the following columns:

- **Select**
Activate the check box in the row to be deleted.
- **Service Name**
Shows the name of the IP service.
- **Transport**
Specify the protocol type.
 - UDP
The rule applies only to UDP frames.
 - TCP
The rule applies only to TCP frames.
- **Source Port (Range)**
Enter the source port. The rule applies specifically to the specified port.
 - If the rule is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
 - If the rule is intended to apply to all ports, enter "*".
- **Destination Port (Range)**
Enter the destination port. The rule applies specifically to the specified port.
 - If the rule is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
 - If the rule is intended to apply to all ports, enter "*".

4.10.5.5 ICMP services

On this page, you define ICMP services. Using the ICMP service definitions, you can define firewall rules for specific services. You select a name and assign the service parameters to it. When you configure the IP rules, you simply use this name.

Internet Control Message Protocol (ICMP) Services

| General | Predefined | User Specific | IP Services | ICMP Services | IP Protocols | IP Rules |
|---------|------------|---------------|-------------|---------------|--------------|----------|
|---------|------------|---------------|-------------|---------------|--------------|----------|

Service Name:

| Select | Service Name | Protocol | Type | Code |
|--------------------------|--------------|----------|-----------------------------|----------------------|
| <input type="checkbox"/> | ipv4wbm | ICMPv4 | Destination Unreachable (3) | Port Unreachable (3) |

1 entry.

Description

The page contains the following:

- **Service Name**
Enter a name for the ICMP service. The name must be unique.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Service Name**
Shows the name of the ICMP service.
- **Protocol**
Shows the version of the ICMP protocol.
- **Type**
Specify the ICMP packet type. A few examples are shown below:
 - Destination Unreachable
IP frame cannot be delivered.
 - Time Exceeded
Time limit exceeded
 - Echo-Request
Echo request, better known as ping.
- **Code**
The code describes the ICMP packet type in greater detail. The selection depends on the selected ICMP packet type.
With "Destination Unreachable", for example "Code 1" host cannot be reached.

4.10.5.6 IP protocols

On this WBM page, you can configure user-defined protocols, e.g. IGMP for multicast groups. You select a protocol name and assign the service parameters to it. When you configure the IP rules, you simply use this protocol name.

Internet Protocol (IP) Protocols

General | Predefined IPv4 | IP Services | ICMP Services | **IP Protocols** | IP Rules

Protocol Name:

| Select | Protocol Name | Protocol Number |
|--------------------------|---------------|-----------------|
| <input type="checkbox"/> | IGMP | 2 |

1 entry.

Description

The page contains the following:

- **Protocol Name**
Enter a name for the protocol.

The page contains the following check boxes:

- **Select**
Select the check box in the row to be deleted.
- **Protocol Name**
Shows the protocol name.
- **Protocol Number**
Enter the protocol number, for example 2. You will find list of the protocol numbers on the Internet pages of iana.org

Procedure

Create IGMP protocol

1. Enter IGMP in "Protocol Name".
2. Click the "Set Values" button. A new entry is generated in the table.
3. Enter "2" in "Protocol Number".

4.10.5.7 IP rules

On this WBM page, you specify your own IP rules for the firewall.

The IP rules set here have priority:

- Over the predefined IP rules and
- Over the IP rules created automatically due to a connection configuration (SINEMA RC).

Internet Protocol (IP) Rules

General Predefined User Specific IP Services ICMP Services IP Protocols IP Rules

IP Version: IPv4
Rule Set: -

show all

| Select | Protocol | Action | From | To | Source (Range) | Destination (Range) | Service | Log | Precedence▲ | Assign to | Assigned |
|--------------------------|----------|--------|-------------|-------------|-----------------|---------------------|---------|------|-------------|--------------------------|----------|
| <input type="checkbox"/> | IPv6 | Drop | vlan1 (INT) | Device | FE80:: - FEBF:: | FE80:: - FEBF:: | all | none | 0 | <input type="checkbox"/> | - |
| <input type="checkbox"/> | IPv4 | Drop | vlan1 (INT) | vlan1 (INT) | 0.0.0.0/0 | 0.0.0.0/0 | all | none | 1 | <input type="checkbox"/> | - |
| <input type="checkbox"/> | IPv6 | Drop | vlan1 (INT) | Device | :: | :: | all | none | 2 | <input type="checkbox"/> | - |

< 3 entries.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

Description

- **IP Version**
Specify the IP version to which the firewall rules apply.
- **Rule set**
Select the required rule set. Only the IP rules that are assigned to this rule set will then be displayed in the table, provided that "Show all" is disabled.
- **Show all**
When enabled, all available IP rules are displayed. With the "Assign" setting, you assign an IP rule to the selected rule set.

The table contains the following columns:

- **Select**
Activate the check box in the row to be deleted.
- **Protocol**
Shows the version of the IP protocol.
- **Action**
Select how incoming IP packets are handled:
 - "Accept" - The data packets can pass through.
 - "Reject" – The data packets are rejected, and the sender receives a corresponding message.
 - "Drop" – The data packets are discarded without any notification to the sender.
- **From / To**
Specify the communications direction of the IP rule.
 - VLANx: VLANs with configured subnet
 - Device: Device
 - ppp0 or usb0 (only with M876-4/MUM856-1): WAN interface
 - SINEMA RC: Connection to the SINEMA RC server
 - IPsec: Either all IPsec VPN connections (all) or a specific IPsec VPN connection

- **Source (Range)**

Enter the IP address or an IP range that is allowed to receive IP packets.

- Individual IP address: Specify the IP address
- IP range: Specify the range with start address "-" end address, e.g.
IPv4: 192.168.100.10 - 192.168.100.20
IPv6: fe80:: - febf::
- All IP addresses:
IPv4: " 0.0.0.0/0"
IPv6: "::"
- If the rule set is activated by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.

Note

Digital input and DYNAMIC placeholder

If the rule set is executed by controlling the digital input, the placeholder DYNAMIC is replaced by the setting for "Dynamic Source (Range)". You configure the setting under "Security > Firewall > Dynamic Rules".

- **Destination (Range)**

Enter the IP address or an IP range that is allowed to receive IP packets.

- Individual IP address: Specify the IP address
- IP range: Specify the range with start address "-" end address, e.g.
IPv4: 192.168.100.10 - 192.168.100.20
IPv6: fe80:: - febf::
- All IP addresses:
IPv4: " 0.0.0.0/0"
IPv6: "::"
- If the rule set is activated by a user, the placeholder DYNAMIC is replaced by the IP address of the end device used.

- **Service**

Select the service or the protocol name for which this rule is valid.

- **Log**

Specify whether or not there should be a log entry every time the rule comes into effect and specify the severity of the event.

The following settings are available:

- none
The rule coming into effect is not logged.
- info / warning / critical
The rule coming into effect is logged with the selected event severity. The log file is displayed in "Information" > "Log Tables" > "Firewall Log".

- **Precedence**

In ascending order starting with 0, you define the sequence in which the IP rules of the firewall are processed.

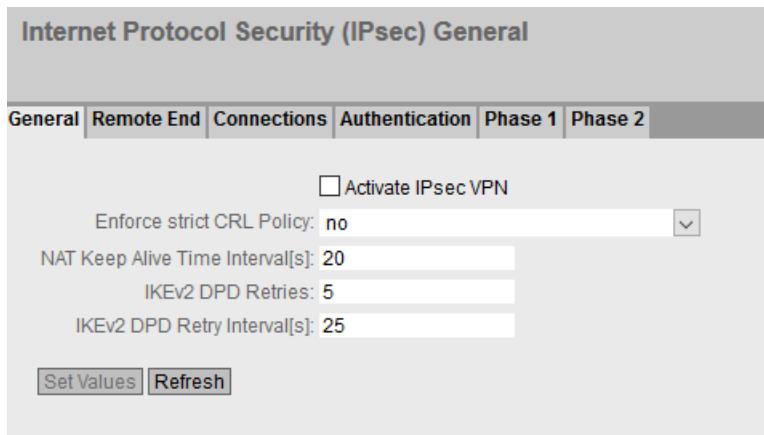
4.10 "Security" menu

- **Assign**
To assign the IP rules to the selected rule set, activate the setting for the desired IP rules and click the "Set Values" button.
- **Assigned**
Shows the rule set to which this IP rule is assigned. The IP rules can also be assigned to multiple rule sets. If the IP rule is assigned to all rule sets, "all" is displayed.
- **Name**
Shows who created the IP rule.
 - NETMAP - automatically created firewall rule

4.10.6 IPsec VPN

4.10.6.1 General

On the WBM page, you configure the basic settings for VPN.



Description

The page contains the following:

- **Activate IPsec VPN**
Enable or disable the IPsec protocol for VPN.
- **Enforce strict CRL Policy**
When enabled, the validity of the certificates is checked based on the CRL (Certificate Revocation List). The certificate revocation list lists the certificates issued by the certification authority that have lost their validity before the set expiry date. You configure the certificate revocation list to be used on the WBM page "Certificates (Page 288)".
- **NAT Keep Alive Time Interval**
Specify the time interval at which keep alive telegrams are sent. If there is a NAT device between two VPN endpoints, when there is inactivity, the connection is deleted from its dynamic NAT table. To prevent this, keepalives are sent.

- **IKEv2 DPD retries**
Specify the number of allowed failed attempts after which the IKEv2 connection is considered disrupted. The setting applies to all IKEv2 connections.
- **IKEv2 DPD Retry Interval[s]**
Specify the interval at which the failed attempts are sent.

4.10.6.2 Remote End

On this WBM page, you configure the partner (VPN end point).

Internet Protocol Security (IPsec) Remote End Settings

General Remote End Connections Authentication Phase 1 Phase 2

Remote End Name:

| Select | Name | Remote Mode | Remote Type | Remote Address | Remote Subnet | Virtual IP Mode | Virtual IP |
|--------------------------|--------|-------------|-------------|----------------|------------------|-----------------|------------|
| <input type="checkbox"/> | CP1628 | Standard | manual | | 192.168.184.0/24 | none | |

1 entry.

Description

The page contains the following:

- **Remote End Name**
Enter the name of the remote station and click "Create" to create a new remote station.

This table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Name**
Shows the name of the partner.
- **Remote Mode**
Specify the role the remote stations will adopt.
 - Roadwarrior
The reachable remote addresses are entered. The reachable remote subnets are learned from the partner.
 - Standard
The reachable remote address and the reachable remote subnets are entered permanently.

- **Remote Type**
Specify the type of remote station address.
 - Manual
The address of the partner is known. The device can either establish the VPN connection actively as a VPN client or wait passively for connection establishment by the partner.
 - Any
Accepts the connection from remote stations with any IP address address. The device can only wait for VPN connections but cannot establish a VPN tunnel as the active partner.
- **Remote Address**
Can only be edited with the remote type "Manual".
 - In standard mode, enter the WAN IP address or the DDNS hostname of the partner. The network mask is always 32
 - In Roadwarrior mode, you can specify either the address of the partner or enter an IP range from which connections will be accepted.
- **Remote Subnet**
 - In standard mode, enter the remote subnet of the remote station. Use the CIDR notation. Multiple subnets can be used only with IKEv2. The enter the subnets separated by a comma.
 - In Roadwarrior mode, the remote address informs the device of its accessible subnets and the device learns them.
- **Virtual IP Mode**
Specify whether or not the remote station is offered a virtual IP address.
The following options are available:
 - User defined IPv4
The virtual IP address is from the band specified in "Virtual IP".
 - None
No virtual IP address. The VPN tunnel is established dynamically to the internal IP address of the remote station.
- **Virtual IP**
Specify the subnet (CIDR) from which the remote station is offered a virtual IP address.
Can only be edited if "user defined IPv4" is selected in "Virtual IP Mode".

Procedure

Configure VPN standard mode

1. Enter the name of the remote station in "Remote End Name".
2. Click the "Create" button. A new entry is generated in the table.
3. For "Remote Mode", select "Standard".
4. For "Remote Type", select "manual".
5. In "Remote Address", enter the WAN IP address and in "Remote Subnet" the subnet of the remote station.
6. Click the "Set Values" button.

Configure VPN Roadwarrior mode

1. Enter the name of the remote station in "Remote End Name".
2. Click the "Create" button. A new entry is generated in the table.
3. For "Remote Mode", select "Roadwarrior".
4. For "Remote Type", select "Any".
5. In "Remote Address", enter the IP address of the remote network.
6. In "Virtual IP Mode", specify how the IP address of the VPN gateway is obtained.
7. Click the "Set Values" button.

4.10.6.3 Connections

On the WBM page, you configure the basic settings for the VPN connection. With these settings, the device (local endpoint) can establish a secure VPN tunnel to the partner. You specify the security settings on the WBM page "Authentication".

Note**Several IPsec VPN connections via the same VPN endpoint**

If you have created IPsec VPN connections to different remote subnets via the same VPN endpoint, the first configured VPN connection (lowest index) is the main connection (parent).

Via the main connection all other IPsec VPN connections (children) are created and established. If all VPN tunnels are now established and the main (parent) connection is terminated all child connections are interrupted. After the DPD timeout has expired, all IPsec VPN connections are reestablished via the main connection.

If only one child connection is terminated, the parent connection and the other child connections are retained.

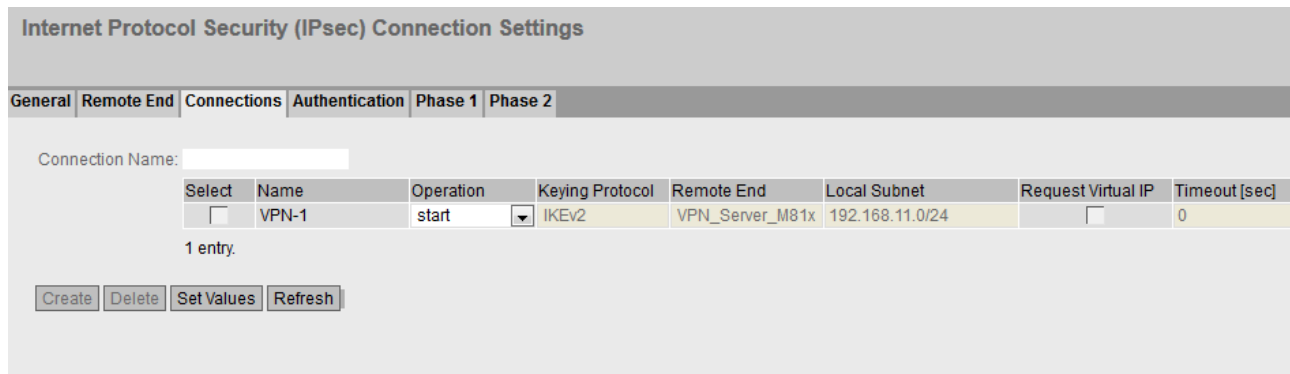
Note**IPsec: Restrictions for phase 2 connections**

Create a maximum of 20 phase 2 connections per phase 1 (remote endpoint).

Note

If you use "NETMAP"

- only auto firewall rules are supported
 - For "Operation" the setting "on demand" cannot be selected.
-



Description

The page contains the following boxes:

- **Connection name**
Enter a name for the VPN connection and click "Create" to create a new connection.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Name**
Shows the name of the VPN connection.

- **Operation**

Specify who establishes the VPN connection. You will find more detailed information in "Technical basics > VPN connection establishment (Page 59)".

 - Disabled
The VPN connection is disabled.
 - start
The device attempts to establish a VPN connection to the partner.
 - wait
The device waits for the remote station to initiate the connection establishment.
 - on demand
The VPN connection is established when necessary.
 - start on DI
If the event "Digital In" occurs the device attempts to establish a VPN connection to the remote station.
This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this in "System > Events> Configuration" activate "VPN Tunnel" for the "Digital In" event.
 - wait on DI
If the event "Digital In" occurs, the device waits for the remote station to initiate connection establishment.
This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this in "System > Events> Configuration" activate "VPN Tunnel" for the "Digital In" event.
 - Start on SMS (only with M87x / MUM 856)
If the device receives a command SMS, the device attempts to establish a VPN connection to the remote station. This assumes that the device accepts a command SMS of the class "System" from certain senders. You configure the senders in "System > SMS > SMS Command".
 - Wait on SMS (only with M87x / MUM 856)
When the device receives an SMS command, the device waits until the connection establishment is initiated by the remote station. This assumes that the device accepts a command SMS of the class "System" from certain senders. You configure the senders in "System > SMS > SMS Command".
- **Keying Protocol**

Specify whether IKEv2 or IKEv1 will be used.
- **Remote End**

Select the required remote station. Only partners can be configured that have been configured on the "Remote End" WBM page.
- **Local Subnet**

Enter the local subnet. Use the CIDR notation. The local network can also be a single PC or another subset of the local network.
Multiple subnets can be used only with IKEv2. The enter the subnets separated by a comma.
- **Request Virtual IP**

When enabled, a virtual IP address is requested from the remote station during connection establishment.
- **Timeout [min]**

Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

4.10.6.4 Authentication

On this WBM page, you specify how the VPN connection partners authenticate themselves with each other.

Internet Protocol Security (IPsec) Authentication Settings

General | Remote End | Connections | **Authentication** | Phase 1 | Phase 2

| Name | Authentication | CA Certificate | Local Certificate | Local ID | Remote Certificate | Remote ID | PSK | PSK Confirmation |
|-------|----------------|----------------|-------------------|----------|--------------------|---------------|-------|------------------|
| VPN-1 | PSK | - | - | | - | 162.168.184.2 | ••••• | ••••• |

Set Values Refresh

Description

This table contains the following columns:

- **Name**
Shows the name of the VPN connection to which the settings relate.
- **Authentication**
Select the authentication method. For the VPN connection, it is essential that the partner uses the same authentication method.
 - Disabled
No authentication method is selected. Connection establishment is not possible.
 - Remote Cert
The remote certificate is used for authentication. You specify the certificate in "Remote Certificate"
 - CA Cert
The certificate of the certification authority is used for authentication. You specify the certificate in "CA Certificate".
 - PSK
A key is used for authentication. You configure the key in "PSK".

Note

For this "PSK" authentication method, specify the "Local ID" and "Remote ID". If the entries remain empty, IPsec uses the IP address of the interface as the ID and prevents the VPN tunnel from being set up.

- **CA Certificate**
Select the certificate. Only loaded certificates can be selected.
- **Local Certificate**
Select the machine certificate.
You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".

- **Local ID**
Enter the local ID from the partner certificate. Only when you use the partner certificate can you leave the box empty. The box is automatically filled with the value from the partner certificate.
- **Remote Certificate**
Select the remote station certificate. Only loaded remote certificates can be selected. You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".
- **Remote ID**
Enter the "Distinguished Name" or "Alternate Name" from the partner certificate. Only when you use the partner certificate can you leave the box empty. The box is automatically filled with the value from the partner certificate.
- **PSK**
Enter the key.
- **PSK Confirmation**
Repeat the key.

4.10.6.5 Phase 1

Phase 1: Encryption agreement and authentication (IKE = Internet Key Exchange)

On this WBM page, you set the parameters for the protocol of the IPsec key management. The key exchange uses the standardized IKE method for which you can set the following protocol parameters.

Internet Protocol Security (IPsec) Phase 1 Settings

| General | Remote End | Connections | Authentication | Phase 1 | Phase 2 | | | | | |
|--|-------------------------------------|-----------------|----------------|----------------|--------------|----------------|-------------------------------------|------------------|-------------------|--------------------------|
| | | | | | | | | | | |
| Name | Default Ciphers | Encryption | Authentication | Key Derivation | Keying Tries | Lifetime [min] | DPD | DPD Period [sec] | DPD Timeout [sec] | Aggressive Mode |
| VPN-1 | <input checked="" type="checkbox"/> | AES128 GCM 16 ▾ | SHA256 ▾ | DH group 14 ▾ | 0 | 180 | <input checked="" type="checkbox"/> | 30 | 150 | <input type="checkbox"/> |
| 1 entry. | | | | | | | | | | |
| <input type="button" value="Set Values"/> <input type="button" value="Refresh"/> | | | | | | | | | | |

Description

The table contains the following columns:

- **Name**
Shows the name of the VPN connection to which the settings relate.
- **Default Ciphers**
When enabled, a preset list is transferred to the VPN connection partner during connection establishment. The list contains a combination of the three algorithms (Encryption, Authentication, Key Derivation). To establish a VPN connection, the VPN connection partner must support at least one of the combinations. The selection depends on the key exchange method. Additional information can be found in the section "IPsec VPN".

- **Encryption**
For phase 1, select the required encryption algorithm. Can only be selected if "Default Ciphers" is disabled.
The selection depends on the key exchange method. Additional information can be found in the section "IPsec VPN".

Note

The AES modes CCM and GCM contain separate mechanisms for authenticating data. If you use a mode AES x CCM for "Encryption", this is also used for authentication. Then only the pseudo random function will be derived from the "Authentication" parameter. So that a VPN connection can be established, all devices need to use the same settings.

- **Authentication**
Specify the method for calculating the checksum. Can only be selected if "Default Ciphers" is disabled.
The following methods are supported:
 - MD5
 - SHA1
 - SHA512
 - SHA256
 - SHA384
- **Key derivation**
Select the required Diffie-Hellmann group (DH) from which a key will be generated. Can only be selected if "Default Ciphers" is disabled.
The following DH groups are supported:
 - DH group 1
 - DH group 2
 - DH group 5
 - DH group 14
 - DH group 15
 - DH group 16
 - DH group 17
 - DH group 18
- **Keying Tries**
Enter the number of repetitions for a failed connection establishment. If you enter the value 0, the connection establishment will be attempted endlessly.
- **Lifetime [min]**
Enter a period in minutes to specify the lifetime of the authentication. When the time has elapsed, the VPN endpoints involved must authenticate themselves with each other again and generate a new key

- **DPD**
When enabled, DPD (Dead Peer Detection) is used. Using DPD, it is possible to find out whether the VPN connection still exists or whether it has aborted.
-
- Note**
- Sending DPD queries increases the amount of data sent and received. This can lead to increased costs.
-
- **DPD Period [sec]**
Enter the period after which DPD requests are sent. These queries test whether or not the remote station is still available
 - **DPD Timeout [sec]**
Only adjustable for IKEv1. For IKEv2, configure the setting under "Security > IPsec > General". Enter a period. If there is no response to the DPD queries, the connection to the remote station is declared to be invalid after this time has elapsed.
-
- Note**
- To avoid unwanted connection breakdowns, set the DPD timeout significantly higher than the DPD period. We recommend setting it at least 2 minutes longer than the DPD period.
-
- **Aggressive Mode**
 - Disabled:
Main Mode is used.
 - Enabled
Aggressive Mode is used

The difference between main and aggressive mode is the "identity protection" used in main mode. The identity is transferred encrypted in main mode but not in aggressive mode.

4.10.6.6 Phase 2

Phase 2: Data exchange (ESP = Encapsulating Security Payload)

On this WBM page, you set the parameters for the protocol of the IPsec data exchange. The entire communication during this phase is encrypted using the standardized security protocol ESP for which you can set the following protocol parameters.

| Internet Protocol Security (IPsec) Phase 2 Settings | | | | | | | | | |
|--|-------------------------------------|-----------------|----------------|----------------------|----------------|----------|----------|--------------|-------------------------------------|
| General | Remote End | Connections | Authentication | Phase 1 | Phase 2 | | | | |
| Name | Default Ciphers | Encryption | Authentication | Key Derivation (PFS) | Lifetime [min] | Lifeytes | Protocol | Port (Range) | Auto Firewall Rules |
| VPN-1 | <input checked="" type="checkbox"/> | AES128 GCM 16 ▾ | SHA256 ▾ | DH group 14 ▾ | 60 | 0 | * | * | <input checked="" type="checkbox"/> |
| 1 entry. | | | | | | | | | |
| <input type="button" value="Set Values"/> <input type="button" value="Refresh"/> | | | | | | | | | |

Description

The table contains the following columns:

- **Name**
Shows the name of the VPN connection to which the settings relate.
- **Default Ciphers**
When enabled, a preset list is transferred to the VPN connection partner during connection establishment. The list includes combinations of the three algorithms (encryption, authentication, key derivation). To establish a VPN connection, the VPN connection partner must support at least one of the combinations. Further information can be found in the section "IPsec VPN".
- **Encryption**
For phase 2, select the required encryption algorithm. Can only be selected if "Default Ciphers" is disabled.
Further information can be found in the section "IPsec VPN".

Note

The AES modes CCM and GCM contain separate mechanisms for authenticating data. If you use a mode AES x CCM or AES x GCM for "Encryption", this will also be used for authentication. Then only the pseudo random function will be derived from the "Authentication" parameter.

- **Authentication**
Specify the method for calculating the checksum. Can only be selected if "Default Ciphers" is disabled.
The following methods are supported:
 - MD5
 - SHA1
 - SHA512
 - SHA256
 - SHA384

- **Key Derivation (PFS)**

The device supports Deffie-Hellmann key exchange (DH) with the Perfect Forward Secrecy (PFS) property.

Select the desired DH group from which a key is generated. Can only be selected if "Default Ciphers" is disabled.

The following DH groups are supported:

- None: For phase 2, no separate keys are exchanged. This disables PFS.
- DH group 1
- DH group 2
- DH group 5
- DH group 14
- DH group 15
- DH group 16
- DH group 17
- DH group 18

Note

So that a VPN connection can be established, all devices need to use the same settings or provide compatible key procedures..

- **Lifetime [min]**

Enter a period in minutes to specify the lifetime of the agreed keys. When the time expires, the key is renegotiated.

- **Lifeytes**

Enter the data limit in bytes that specifies the lifetime of the agreed key. When the data limit is reached, the key is renegotiated.

- **Protocol**

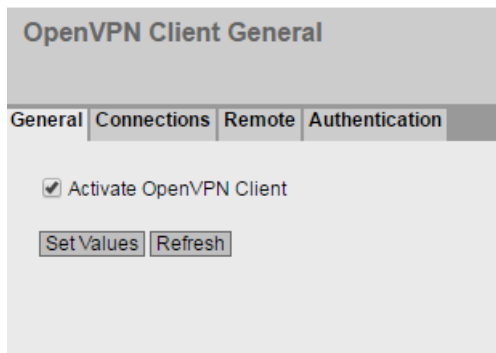
Specify the protocol for which the VPN connection is valid e.g. UDP, TCP, ICMP. If the setting is intended to apply to all protocols, enter "**".

- **Port (Range)**
Specify the port via which the VPN tunnel can communicate. The setting applies specifically to the specified port
 - If the setting is intended to apply to a port range, enter the range with start port "-" end port, for example 30 - 40.
 - If the setting is intended to apply to all ports, enter "*".The setting is only effective for port-based protocols.
- **Auto Firewall Rules**
 - Enabled
For the VPN connection, the firewall rules for access from "External" to "Internal" and vice versa are created automatically. You can enable access to specific services of the device under "Security > Firewall > Predefined IPv4". Ping is enabled by default.
 - Disabled
You will need to create the firewall rules yourself.

4.10.7 OpenVPN client

4.10.7.1 General

On this WBM page, you enable the OpenVPN client.



Description

The page contains the following:

- **Activate OpenVPN Client**
Enable or disable the OpenVPN client.

4.10.7.2 Connections

On this WBM page, you configure the basic settings for the OpenVPN connection. You specify the security settings on the WBM page "Authentication".

OpenVPN Connection Settings

General | **Connections** | Remote | Authentication

Connection Name:

| Select | Name | Operation | Encryption | Authentication | LZO Comp. | Auto Firewall Rules | Enable NAT | Timeout[min] |
|--------------------------|---------|-----------|------------|----------------|-----------|-------------------------------------|--------------------------|--------------|
| <input type="checkbox"/> | To_M826 | disabled | AES128 CBC | SHA256 | - | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 0 |

1 entry.

Description

- **Connection name**
Enter a unique name for the OpenVPN connection and click "Create" to create a new connection.

The table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Name**
Shows the name of the OpenVPN connection.
- **Operation**
Specify how the VPN connection is established. You will find more detailed information in "Technical basics > VPN connection establishment (Page 59)".
 - start
The device attempts to establish a VPN connection to the partner.
 - Start on DI
If the event "Digital In" occurs the device attempts to establish a VPN connection to the remote station.
This is on condition that the event "Digital In" is forwarded to the VPN connection. To do this in "System > Events > Configuration" activate "VPN Tunnel" for the "Digital In" event.
 - Start on SMS (only with M87x / MUM856)
If the device receives a command SMS, the device attempts to establish a VPN connection to the partner. This assumes that the device accepts a command SMS of the class "System" from certain senders. You configure the senders in "System > SMS > SMS Command".
 - Disabled
The VPN connection is disabled.

4.10 "Security" menu

- **Encryption**
Select the required encryption algorithm.
 - AES-128-CBC (default)
 - AES-192-CBC
 - AES-256-CBC
 - DES-EDE3
 - BF-CBC
- **Authentication**
Specify the method for calculating the checksum.
 - SHA256 (default)
 - SHA384
 - SHA512
 - SHA224
 - SHA1
 - MD5
- **Use LZO**
When enabled, the data is compressed with the LZO algorithm.
- **Auto Firewall Rules**
 - Enabled
For the VPN connection, the firewall rules for access from "External" to "Internal" and vice versa are created automatically. In addition to this, access from the device to the outside is allowed. You can enable access to specific services of the device under "Security > Firewall > Predefined IPv4". Ping is enabled by default.
 - Disabled
You will need to create the suitable firewall rules yourself.
- **Enable NAT**
With this setting, you enable automatic IP masquerading for this interface. The local devices are not directly reachable from the outside, but only via the IP address of the interface. The local devices can, however, connect to the devices downstream from the OpenVPN server. You will find more information on NAT in "Technical basics > NAT"
- **Timeout [min]**
Specify the period of time in minutes. If no data exchange takes place, when this time has elapsed the VPN tunnel is automatically terminated.

4.10.7.3 Remote

On this WBM page, you configure the partner (OpenVPN end point). Per connection, you can specify several OpenVPN partners. The device tries all configured OpenVPN partners one after the other until a connection is successfully established.

OpenVPN Client Remote End Settings

General | **Connections** | Remote | Authentication

Remote Name:

| Select | Name | Connection | Remote Address | Port | Protocol | Proxy |
|--------------------------|--------|------------|----------------|------|----------|-------|
| <input type="checkbox"/> | remote | none | | 1194 | udp | none |

1 entry.

Description

The page contains the following:

- **Remote Name**
Enter a name for the OpenVPN partner and click "Create" to create a new partner.

This table contains the following columns:

- **Select**
Select the check box in the row to be deleted.
- **Name**
Shows the name of the Open VPN partner.
- **Connection**
Select the corresponding connection. Only connections can be configured that have been configured on the "Connections" WBM page.
- **Remote Address**
Enter the WAN IP address or the DNS host name of the OpenVPN partner.
- **Port**
Specify the port via which the OpenVPN tunnel can communicate. The setting applies specifically to the specified port.
- **Protocol**
Specify the protocol for which the OpenVPN connection will be used.
- **Proxy**
Specify whether the OpenVPN tunnel to the defined OpenVPN partner is established via a proxy server. Only the proxy servers can be selected that you configured in "System > Proxy Server".

4.10.7.4 Authentication

On this WBM page, you specify how the VPN connection partners authenticate themselves with each other.

OpenVPN Authentifizierungs-Einstellungen

Allgemein | Verbindungen | Client | **Authentifizierung**

| Name | TLS-Auth. Key | Richtung | Methode | CA-Zertifikat | Gerätezertifikat | Benutzername | Passwort | Passwort bestätigen |
|------|---------------|----------|-------------|---------------|------------------|--------------|----------|---------------------|
| M826 | - | none | Deaktiviert | - | - | | | |

Description

This table contains the following columns:

- **Name**
Shows the name of the VPN connection to which the settings relate.
- **TLS Auth. Key**
Select the key file used to sign the TLS packets. If the incoming TLS packets are not signed with this key, they are discarded.
- **Direction**
Specify the direction. If you select 0, 1 must be set on the partner and vice versa. With this setting, you restrict the clients that can authenticate themselves.
Select "none" if nothing is set on the OpenVPN server. With "none", this setting is disabled.
- **Method**
Select the authentication method. For the VPN connection, it is essential that the partner uses the same authentication method.
 - Disabled
No authentication method is selected. Connection establishment is not possible.
 - Certificates
Certificates are used for the authentication.
 - User Name/Password
The user name / password are used for the authentication.
 - Cert/User Name/Password
For authentication, a user name and password are required in addition to the certificate. The VPN connection is established only if both operations are successful.
- **CA Certificate**
Select the certificate. Only loaded certificates can be selected.
You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".
- **Machine certificate**
Select the machine certificate. Only loaded certificates can be selected.
You load the certificates on the device with "System > Load&Save". The loaded certificates and key files are shown on the WBM page "Security > Certificates".

- **User Name**
Specify the user name.
- **Password**
Enter the password.
- **Password Confirmation**
Repeat the password.

4.10.8 Brute Force Prevention

Brute Force Prevention (BFP) refers to the protection of the device from unauthorized access by trying a sufficiently large number of passwords. The number of incorrect login attempts within a specific time period is limited for this purpose.

Brute Force Prevention

User Specific BFP is Enabled

Acceptable Invalid Login Attempts Per User:

IP Specific BFP is Enabled

Acceptable Invalid IP Login Attempts Per IP:

Global Parameters

BFP Trigger Interval[min]:

BFP Automatic Reset Timer[min]:

User Specific BFP:

| User | Failed Logins | Last Failed[s] | Blocked[s] | Clear |
|--------------|---------------|----------------|-------------|--------------------------------------|
| Unknown User | 0 | 0 | not blocked | <input type="button" value="Clear"/> |
| admin | 0 | 0 | not blocked | <input type="button" value="Clear"/> |
| 1 | 0 | 0 | not blocked | <input type="button" value="Clear"/> |

3 entries.

IP Specific BFP:

| IP | Failed Logins | Last Failed[s] | Blocked[s] | Clear |
|---------------|---------------|----------------|-------------|--------------------------------------|
| 192.168.16.20 | 0 | 0 | not blocked | <input type="button" value="Clear"/> |

Description

The page contains the following boxes:

- **User Specific BFP is Enabled. / User Specific BFP is Disabled.**
 - Enabled:
With login authentication, the "Local" or "Local and RADIUS" mode is set and the maximum number of invalid login attempts is greater than 0.
 - Disabled:
With login authentication, the "RADIUS" or "RADIUS and fallback Local" mode is set or the maximum number of invalid login attempts is 0.

You configure the login authentication under "Security > AAA > General > Login Authentication".
- **Acceptable Invalid Login Attempts Per User**
The maximum number of invalid login attempts for a user accepted by the device. Further login attempts for this user are blocked for a specific time.
The users that are not configured as local users for the device are summarized under the user name "UnknownUser".
0: User Specific BFP is Disabled.
- **IP Specific BFP is Enabled. / IP Specific BFP is Disabled.**
Shows whether the IP-specific Brute Force Prevention is enabled.
- **Acceptable Invalid Login Attempts Per IP**
The maximum number of invalid login attempts for an IP address accepted by the device. Further login attempts for this IP address are blocked for a specific time.
0: IP Specific BFP is Disabled.
- **Trigger Interval BFP [min]**
The time in minutes that is relevant for counting invalid login attempts.
If the maximum number of invalid login attempts is exceeded during this time, the device blocks login for a specific period of time.
Invalid login attempts per user and per IP address are handled independently of one another.
- **BFP Automatic Reset Timer [min]**
Time in minutes for which the device blocks login because the maximum number of invalid login attempts was exceeded.
0: The timer is disabled.

The **User Specific BFP** table has the following columns:

- **User**
The users configured locally on the device. The users that are not locally configured on the device are summarized under the user name "UnknownUser".
- **Failed Logins**
The number of failed login attempts.
- **Last Failed [s]**
Time in seconds (s) since the last failed login attempt. To display the current value, click the "Refresh" button.

- **Blocked [s]**
The time in seconds (s) until the blocking will be removed. To display the current value, click the "Refresh" button.
When a blocked user attempts to log in before the timer expires, the timer restarts.
- **Delete**
Ends blocking for the user and resets the displays in the "Last Failed [s]" and "Blocked [s]" boxes.

The **IP Specific BFP** table has the following columns:

- **IP**
The IP address of the device for the login attempt.
- **Failed Logins**
The current number of failed login attempts.
- **Last Failed [s]**
Time in seconds (s) since the last failed login attempt. To display the current value, click the "Refresh" button.
- **Blocked [s]**
The time in seconds (s) until the blocking will be removed. To display the current value, click the "Refresh" button.
When a blocked IP address attempts to log in before the timer expires, the timer restarts.
- **Delete**
Ends blocking for the IP address and resets the displays in the "Last Failed [s]" and "Blocked [s]" boxes.

4.10 "Security" menu

Upkeep and maintenance

5.1 Device configuration with PRESET-PLUG

Please not the additional information and security notes in the operating instructions of your device.

| |
|---|
| NOTICE |
| Do not remove or insert a PLUG during operation |
| A PLUG may only be removed or inserted when the device is turned off. |

Note

Support as of V4.3

The PRESET-PLUG functionality is supported as of firmware version V4.3.

With the PRESET-PLUG, you can install the same device configuration (start configuration, user accounts, certificates) including the corresponding firmware on multiple devices.

The PRESET PLUG is write-protected.

You configure the PRESET PLUG using the Command Line Interface (CLI).

Creating a PRESET-PLUG

You create the PRESET PLUG using the Command Line Interface (CLI). You can create a PRESET-PLUG from any PLUG. To do this, follow the steps outlined below:

Note

Using configurations with DHCP

Create a PRESET-PLUG only from device configurations that use DHCP. Otherwise disruptions will occur in network operation due to multiple identical IP addresses.

You assign fixed IP addresses extra following the basic installation.

Requirement

- A PLUG is inserted in the device on which you want to configure the PRESET-PLUG functionality.

Procedure

1. Start the remote configuration using CLI and log on as a user with the "admin" role. The CLI connection works either with Telnet (port 23) or SSH (port 22).
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.

5.1 Device configuration with PRESET-PLUG

4. Create the PRESET-PLUG with the "presetplug" command.
The firmware version of the device and the current device configuration incl. user accounts and certificates are stored on the PLUG and the PLUG is then write protected.
5. Turn off the power to the device.
6. Remove the PRESET-PLUG.
7. Start the device either with a new PLUG inserted or with the internal configuration.

Procedure for installation with the aid of the PRESET-PLUG

1. Turn off the power to the device.
2. If it exists, remove the PLUG from the slot. You will find further information on this in the operating instructions of your device.
3. Insert the PRESET-PLUG correctly oriented into the slot. The PRESET-PLUG is correctly inserted when it is completely inside the device and does not jut out of the slot.
4. Turn on the power to the device again.
If there is a different firmware version on the device to be installed compared with that on the PRESET-PLUG, an upgrade/downgrade of the firmware is performed. You can recognize this by the red F-LED flashing (flashing interval: 2 sec on/0.2 sec off). Afterwards the device is restarted and the device configuration incl. users and certificates on the PRESET-PLUG is transferred to the device.
5. Wait until the device has fully started up.
(the red F-LED is off)
6. Turn off the power to the device after the installation.
7. Remove the PRESET-PLUG.
8. Start the device either with a new PLUG inserted or with the internal configuration.

Note

KEY-PLUG

If you have created the PRESET-PLUG from a KEY-PLUG, for operation with this configuration, you require an inserted KEY-PLUG with factory settings.

IN this case before recommissioning the device you need to insert the relevant KEY-PLUG.

Note

Restore factory defaults and restart with a PRESET PLUG inserted

If you reset a device to the factory defaults, when the device restarts an inserted PRESET PLUG is formatted and the PRESET PLUG functionality is lost. You then need to create a new PRESET PLUG. The keys stored on the KEY-PLUG for releasing functions are retained.

We recommend that you remove the PRESET PLUG before you reset the device to the factory settings.

Formatting a PRESET-PLUG (resetting the preset function)

You format the PRESET PLUG using the Command Line Interface (CLI) to reset the preset function. To do this, follow the steps outlined below:

1. Start the remote configuration using Telnet (CLI) and log on with a user with the "admin" role.
2. Switch to the global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Enter the command "factoryclean".
The PRESET-PLUG is formatted and the preset function is reset.
5. Write the current configuration of the device with the "write" command.

5.2 Firmware update - via WBM

Requirement

- The device has an IP address.
- The user is logged in with administrator rights.

Firmware update via HTTP

1. Click "System" > "Load&Save" in the navigation area. Click the "HTTP" tab.
2. Click the "Loading" button next to "Firmware".
3. Go to the storage location of the firmware file.
4. Click the "Open" button in the dialog.

Firmware update via TFTP

1. Click "System > Load&Save" in the navigation area. Click the "TFTP" tab.
2. Enter the IP address of the TFTP server in the "TFTP Server Address" input box.
3. Enter the port of the TFTP server in the "TFTP Server Port" input box.
4. Click the "Load file" button in the "Firmware" table row.
5. Go to the storage location of the firmware file.
6. Click the "Open" button in the dialog. The file is uploaded.

Firmware update via SFTP

1. Click "System > Load&Save" in the navigation area. Click the "SFTP" tab.
2. Enter the IP address of the SFTP server in the "SFTP Server Address" input box.
3. Enter the port of the SFTP server in the "SFTP Server Port" input box.
4. Enter the user and the password for access to the SFTP server.

5.3 Firmware update via WBM and CLI not possible

5. Click the "Load file" button in the "Firmware" table row.
6. Go to the storage location of the firmware file.
7. Click the "Open" button in the dialog. The file is uploaded.

Result

When the firmware is successfully loaded a dialog is displayed . Confirm the dialog with "OK". The device is restarted.

In "Information" > "Versions" there is the additional entry "Firmware_Running".
Firmware_Running shows the version of the current firmware. Firmware shows the firmware version stored after loading the firmware.

| Version Information | | | |
|---------------------|-----------------------------|-----------|---------------------|
| Hardware | Name | Revision | Order ID |
| Basic Device | SCALANCE S615 | 1 | 6GK5 615-0AA00-2AA2 |
| Software | Description | Version | Date |
| Firmware | SCALANCE M800/S615 Firmware | V05.00.00 | 11/27/2017 14:00:00 |
| Bootloader | SCALANCE S600 Bootloader | V01.05.00 | 08/02/2017 16:30:00 |
| Firmware_Running | Current running Firmware | V05.00.00 | 11/27/2017 14:00:00 |

5.3 Firmware update via WBM and CLI not possible

Cause

If there is a power failure during the firmware update, it is possible that the device is no longer accessible using WBM and CLI.

Requirement

- The PC is connected to the device via the interface.
- A TFTP client is installed on the PC and the firmware file exists.

Solution

You can then also transfer firmware to the device using TFTP. Follow the steps below to load new firmware using TFTP:

1. Now press the SET button.
2. Hold down the button until the red fault LED (F) starts to flash after approximately 3 seconds.

Note

If you hold down the SET button for approximately 10 seconds, the device is reset to its factory settings and can be reached with the IP address 192.168.1.1.

3. Now release the button. The bootloader waits in this state for new firmware file that you can download by TFTP.

Note

If you want to exit the bootloader without making changes, press the SET button briefly. The device restarts with the loaded configuration.

4. Connect a PC to the device over the Ethernet interface.
5. Open a DOS box and change to the directory where the new firmware file is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.
If you are not sure that the IP address is correct, you can check this, for example with SINEC PNI.

Note**Use of CLI and TFTP in Windows 10**

If you want to access the CLI or TFTP in Windows 10, make sure that the relevant functions are enabled in Windows 10.

Result

The firmware is transferred to the device.

Note

Please note that the transfer of the firmware can take several minutes. During the transmission, the red error LED (F) flashes.

Once the firmware has been transferred completely to the device, the device is restarted automatically.

5.4 Restoring the factory settings

| |
|---|
| NOTICE |
| Previous settings If you reset, all the settings you have made will be overwritten by factory defaults. |
| NOTICE |
| Inadvertent reset An inadvertent reset can cause disturbances and failures in a configured network with further consequences. |

With the reset button

When pressing the button, remember the information in the section "Reset button" in the operating instructions.

Follow the steps below to reset the device parameters to the factory settings:

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
4. Now release the button and wait until the fault LED (F) goes off again.
5. The device then starts automatically with the factory settings.

Via the configuration

You will find detailed information on resetting the device parameters using the WBM and CLI in the configuration manuals:

- Web Based Management, section "Restart"
- Command Line Interface, section "Reset and Defaults"

Appendix A

A.1 Format of the syslog messages

The devices generate Syslog messages (UDP default port 514) according to RFC 5424 that contain the following boxes.

HEADER

- TIMESTAMP according to RFC 3339
- Host name
- APPNAME, PROCID and MSGID: If no information is known, the "-" character is output.

PRIORITY

PRIORITY contains the coded priority of the Syslog message broken down into a Severity and Facility box.

- Facility
- Severity

VERSION

- Set to 1.

HOSTNAME_CONTENT:

- IPv4 address according to RFC1035: Each byte is represented in decimal, with a dot separating it from the previous one. XXX.XXX.XXX.XXX
- IPv6 address according to RFC4291 Section 2.2

STRUCTURED DATA

- timeQuality block

MESSAGE:

- ASCII string in English

Note

Additional information about the meaning of the boxes is available in RFC 5424.

A.2 Parameters in Syslog messages

The Syslog messages can contain the following parameters:

| Parameter | Description | Possible values or example |
|------------------------|--|--|
| ip address | IPv4 or IPv6 address | IP address according to RFC1035 or RFC4291 Section 2.2 |
| src port dest port | Port that is shown as decimal number. Format: %d | 0 ... 65535 |
| dest mac src mac | MAC address Format: %02x:%02x:%02x:%02x:%02x:%02x | 00:0C:29:2F:09:B3 |
| protocol | Name of the service that has generated this event or of the Layer 4 protocol used. Format: %s | Possible entries of: UDP TCP WBM Telnet SSH TFTP SFTP |
| group | String that identifies the group based on its name Format: %s | it-service |
| user name | String that identifies the authenticated user based on his/her name without spaces Format: %s | maier |
| action user name | Identifies the user based on his/her name This is not the authenticated user. Format: %s | Peter.Maier |
| role | Symbolic name for the group role Format: %s | Administrator |
| time minute timeout | Number of minutes Format: %d | 44 |
| failed login count | Number of failed logins Format: %d | 10 |
| max sessions | Number of sessions Format: %d | 10 |
| trigger pin | String for an IO pin that triggers the event without spaces Format: %s | DI1 |
| firewall rule | String for a firewall rule with spaces Format: %s | Rule1 |
| subject | String for the subject in the certificate. Used as part of the certificate-based authentication with spaces and must also include Unicode characters Format: (% S) or (% S% S) for UTF8 code. | (Peter Maier) |
| config detail | String for the configuration with spaces Format: %s | OpenVPN |
| connection name | Name of the VPN connection | to_Baugruppe1 |

| Parameter | Description | Possible values or example |
|------------------------|---|----------------------------|
| firewall accept | Firewall action executed (accepted package) | ACCEPT |
| firewall action reject | Firewall action executed (rejected package) | REJECT DROP |
| length | Length of the network packet (in bytes) Format: %d | 52 |
| network interface | Symbolic name of a network interface Format: %s | vlan1 |

A.3 Syslog messages

Note

Severity

Some severities are grouped in the firmware:

- Info + Notice = Info
- Warning + Error = Warning
- Critical + Emergency = Critical

Identification and authentication of human users

| | |
|--------------|--|
| Message text | {protocol}: User {User name} has logged in from {ip address}. |
| Example | WBM: User "Admin" has logged in from 192.168.0.1. |
| Explanation | Valid login information that is specified during remote login. |
| 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" has failed to log in from 192.168.0.1. |
| Explanation | Incorrect user name or incorrect password (login information) specified during remote login. |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.1 |

| | |
|--------------|--|
| Message text | {protocol}: User {User name} has logged out from {ip address}. |
| Example | SSH: User "Admin" has 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 | SSH: Default user admin logged in from 192.168.0.1. |
| Explanation | The default user is logged in via the IP address. |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5) |

Identification and authentication of devices (access via firewall)

| | |
|--------------|---|
| Message text | {firewall action accept}(1) in:{network interface} out:{network interface} len:{length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port} |
| Example | ACCEPT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:158.85.11.68 tcp:53788->443 |
| Explanation | A known device requested a connection. |
| Severity | Info or Warning or Error (configurable) |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.2 |

| | |
|--------------|---|
| Message text | {firewall action reject}(1) in:{network interface} out:{network interface} len:{length} s-mac:{src mac} d-mac:{dest mac} s-ip:{ip address} d-ip:{ip address} {protocol}:{src port}->{dest port} |
| Example | REJECT(1) in:vlan1 out:ppp0 len:52 s-mac:58:EF:68:B3:FA:CE d-mac:00:1B:1B:A7:5B:D8 s-ip:172.23.1.6 d-ip:217.194.40.109 tcp:53773->443 |
| Explanation | An unknown device requested a connection. The request was denied. |
| Severity | Info or Warning or Error (configurable) |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.2 |

User account management

| | |
|--------------|--|
| Message text | {protocol}: User {user name} changed own password. |
| Example | WBM: User admin changed own password. |
| Explanation | User has changed own password. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR1.3 |

| | |
|--------------|---|
| Message text | {protocol}: User {user name} changed password of user {action user name}. |
| Example | Telnet: User admin changed password of user test. |
| Explanation | User has changed the password of another user. |

| | |
|----------|--------------------------------|
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR1.3 |

| | |
|--------------|---|
| Message text | {protocol}: User {user name} created user-account {action user name}. |
| Example | WBM: User admin created user-account service. |
| Explanation | The user has created an account. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR1.3 |

| | |
|--------------|---|
| Message text | {protocol}: User {user name} deleted user-account {action user name}. |
| Example | WBM: User admin deleted user-account service. |
| Explanation | The administrator deleted an existing account. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR1.3 |

Management of the identifiers

| | |
|--------------|---|
| Message text | {Protocol}: User {User name} created group {Group} and assigned to role {Role}. |
| Example | WBM: User admin created group it-service and assigned to role service. |
| Explanation | The administrator has created a group and assigned it to a role. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.4 |

| | |
|--------------|--|
| Message text | {Protocol}: User {User name} deleted group {Group} and the role {Role} assignment. |
| Example | WBM: User maier deleted group it-service and the role service assignment. |
| Explanation | The administrator has deleted an existing group and the role assignment. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.4 |

Unsuccessful logon attempts

| | |
|--------------|---|
| Message text | {User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts. |
| Example | User service account is locked for 44 minutes after 10 unsuccessful login attempts. |
| Explanation | If there are too many failed logins, the corresponding user account was locked for a specific period of time. |
| Severity | Warning |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.11 |

Access via untrusted networks (IPsec)

| | |
|--------------|--|
| Message text | [IKE] <{connection name}{{config detail}}> IKE_SA {connection name}{{config detail}} established between {ip address}{{config detail}}...{ip address}{{config detail}} |
| Example | [IKE] <c1 3> IKE_SA c1[1] established between 192.168.55.210[lokal].. 192.168.55.211[remote] |
| Explanation | VPN connection is established (IPsec). |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1) |

| | |
|--------------|--|
| Message text | [IKE] <{connection name}{{config detail}}> deleting IKE_SA {connection name} {{config detail}} between {ip address}{{config detail}}...{ip address}{{config detail}} |
| Example | [IKE] <c1 3> deleting IKE_SA c2[1] between 192.168.55.211[lokal].. 192.168.55.210[remote] |
| Explanation | VPN tunnel is closed (IPsec). |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1) |

| | |
|--------------|--|
| Message text | [IKE] <{connection name}{{config detail}}> received AUTHENTICATION_FAILED notify error |
| Example | [IKE] <c1 1> received AUTHENTICATION_FAILED notify error |
| Explanation | Authentication of VPN connection failed (IPsec). |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R3) |

Access via untrusted networks (OpenVPN)

| | |
|--------------|--|
| Message text | OVPN_{connection name}{{config detail}}: Initialization Sequence Completed |
| Example | OVPN_Conn_1[2427]: Initialization Sequence Completed |
| Explanation | VPN connection is established (OpenVPN). |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1) |

| | |
|--------------|--|
| Message text | OpenVPN connection {connection name} has been deactivated. |
| Example | OpenVPN connection c1 has been deactivated. |
| Explanation | VPN connection was closed (OpenVPN). |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R1) |

Access via untrusted networks (SINEMA Remote Connect)

| | |
|--------------|--|
| Message text | SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established. |
| Example | SINEMA RC - State of Digital Input changed to HIGH. SINEMA RC - OpenVPN connection established. |
| Explanation | Remote access is permitted. (SINEMA RC, Digital Input) |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.13 |

| | |
|--------------|---|
| Message text | SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established. |
| Example | SINEMA RC - Received Wakeup SMS. SINEMA RC - OpenVPN connection established. |
| Explanation | Remote access is permitted. (SINEMA RC, Wakeup SMS) |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.13 |

| | |
|--------------|---|
| Message text | SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated. |
| Example | SINEMA RC - State of Digital Input changed to LOW. SINEMA RC - OpenVPN terminated. |
| Explanation | Remote access denied (SINEMA RC, Digital Input) |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.13 |

| | |
|--------------|---|
| Message text | SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated. |
| Example | SINEMA RC - Received Shutdown SMS. SINEMA RC - OpenVPN terminated. |
| Explanation | Remote access denied (SINEMA RC, Wakeup SMS) |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 1.13 |

Authorization enforcement (access via custom firewall)

| | |
|--------------|--|
| Message text | User specific firewall user "{user name}" activated rule set "{firewall rule}" with ip address "{ip address}". Timeout: {timeout} minutes. |
| Example | User specific firewall user "usf" activated rule set "rs1" with ip address "172.23.1.14". Timeout 5 minutes. |
| Explanation | The user has logged onto the user-specific firewall. (USF Digital User Login) |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2) |

| | |
|--------------|---|
| Message text | User specific firewall digital input {trigger pin} activated rule set "{firewall rule}" with ip "{ip address}". |
| Example | User specific firewall digital input 1 activated rule set "cpu2" with ip "192.168.16.1". |
| Explanation | The user has logged onto the user-specific firewall. (USF Digital Input Login) |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: n/a (NERC CIP 005-R2)4820486 |

| | |
|--------------|--|
| Message text | User specific firewall user "{user name}" ruleset "{firewall rule}" time expired. |
| Example | User specific firewall user "usf" ruleset "rs1" time expired. |
| Explanation | The access to the user-specific firewall was denied. The access time is expired. (USF User Logout) |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 2.1 |

| | |
|--------------|---|
| Message text | User specific firewall user "{user name}" logged out by administrator configuration. |
| Example | User specific firewall user "usf" logged out by administrator configuration. |
| Explanation | The access to the user-specific firewall was denied. The device administrator deactivates the user using the "Force Deactivate" button. (USF user force log out by admin) |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 2.1 |

| | |
|--------------|---|
| Message text | User specific firewall user "{user name}" deactivated by administrator configuration. |
| Example | User specific firewall user "usf" deactivated by administrator configuration. |
| Explanation | The access to the user-specific firewall was denied. The device administrator has deactivated the user. (USF user deactivated by admin) |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 2.1 |

| | |
|--------------|--|
| Message text | User specific firewall digital input {trigger pin} deactivated rule set "{firewall rule}". |
| Example | User specific firewall digital input 1 deactivated rule set "rs1". |
| Explanation | The access to the user-specific firewall was denied. The corresponding set of rules has been deactivated. (USF Digital Input Logout) |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 2.1 |

Session lock

| | |
|--------------|--|
| Message text | The session of user {user name} was closed after {time} seconds of inactivity. |
| Example | The session of user admin was closed after 60 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 |

Closing a remote access session

| | |
|--------------|--|
| Message text | [JOB] <{connection name}{{config detail}}> deleting CHILD_SA after {time second} seconds of inactivity |
| Example | [JOB] <to_Baugruppe1 21> deleting CHILD_SA after 20 seconds of inactivity |
| Explanation | The remote session was ended after a period of inactivity (IPsec). |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 2.6 |

| | |
|--------------|--|
| Message text | OVPN_{connection name}{{config detail}}: [{config detail}] Inactivity timeout (--ping-restart), restarting |
| Example | OVPN_c1[26296]: [router] Inactivity timeout (--ping-restart), restarting |
| Explanation | The remote session was ended after a period of inactivity (OpenVPN). |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 2.6 |

Limiting the number of simultaneous sessions

| | |
|--------------|---|
| 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 parallel connections is exceeded. |
| Severity | Warning |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 2.7 |

Nonrepudiation

| | |
|--------------|--|
| Message text | Device configuration changed. |
| Example | Device configuration changed. |
| Explanation | The device configuration has been changed permanently. |
| Severity | Info |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR2.12 |

Communication integrity

| | |
|--------------|---|
| Message text | [IKE] {connection name} {config detail} received invalid DPD sequence number {config detail} (expected {config detail}), ignored. |
| Example | [IKE] "c1" "1" received invalid DPD sequence number 10 (expected 12), ignored. |
| Explanation | Integrity check failed (IPsec) |
| Severity | Error |

| | |
|----------|---------------------------------|
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 3.1 |

| | |
|--------------|--|
| Message text | OVPN_{connection name}{config detail}: Authenticate/Decrypt packet error: packet HMAC authentication failed. |
| Example | OVPN_c1[25409]: Authenticate/Decrypt packet error: packet HMAC authentication failed. |
| Explanation | Integrity check failed (OpenVPN). |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 3.1 |

Session integrity

| | |
|--------------|--|
| Message text | {Protocol}: Session ID verification from {ipaddress} failed. |
| Example | WBM Session ID verification from 192.168.1.1 failed. |
| Explanation | The session ID of 192.168.1.1 is invalid. |
| Severity | Error |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR 3.8 |

Data backup in automation system

| | |
|-------------|---|
| Log text | {protocol}: Saved file type ConfigPack. |
| Standard | IEC 62443-3-3 Reference: SR7.3 |
| Description | The ConfigPack file was saved. |
| Example | TFTP: Saved file type ConfigPack |
| Severity | Notice |
| Facility | local0 |

| | |
|-------------|---|
| Log text | {protocol}: User {user name} saved file type ConfigPack |
| Standard | IEC 62443-3-3 Reference: SR7.3 |
| Description | User has saved the ConfigPack file. |
| Example | WBM: User admin saved file type ConfigPack.. |
| Severity | Notice |
| Facility | local0 |

| | |
|-------------|---|
| Log text | {protocol}: User {user name} failed to save file type ConfigPack. |
| Standard | IEC 62443-3-3 Reference: SR7.3 |
| Description | User failed to save the ConfigPack file. |
| Example | WBM: User admin failed to save file type ConfigPack. |
| Severity | Info |
| Facility | local0 |

| | |
|----------|--|
| Log text | {protocol}: Failed to save file type ConfigPack. |
| Standard | IEC 62443-3-3 Reference: SR7.3 |

| | |
|-------------|--|
| Description | The ConfigPack file could not be saved. |
| Example | TFTP: Failed to save file type ConfigPack. |
| Severity | Error |
| Facility | local0 |

Restoration of the automation system

| | |
|--------------|---|
| Message text | {protocol}: Loaded file type Firmware {version} (restart required). |
| Example | TFTP: Loaded file type Firmware V02.00.00 (restart required). |
| Explanation | The firmware was successfully loaded. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR7.4 |

| | |
|--------------|--|
| Message text | {protocol}: User {user name} loaded file type Firmware {version} (restart required). |
| Example | WBM: User admin loaded file type Firmware V02.00.00 (restart required). |
| Explanation | The user has successfully loaded the firmware. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR7.4 |

| | |
|--------------|--|
| Message text | {protocol}: Failed to load file type Firmware. |
| Example | WBM: Failed to load file type Firmware. |
| Explanation | Firmware upload has failed. |
| Severity | Warning |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR7.4 |

| | |
|--------------|---|
| Message text | {protocol}: Loaded file type Config (restart required). |
| Example | TFTP: Loaded file type Config (restart required). |
| Explanation | The configuration is applied. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR7.4 |

| | |
|--------------|---|
| Message text | {protocol}: Loaded file type ConfigPack (restart required). |
| Example | TFTP: Loaded file type ConfigPack (restart required). |
| Explanation | The configuration is applied. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR7.4 |

| | |
|--------------|--|
| Message text | {protocol}: User {user name} loaded file type Config (restart required). |
| Example | WBM: User admin loaded file type Config (restart required). |
| Explanation | The configuration is applied. |
| Severity | Notice |

| | |
|----------|--------------------------------|
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR7.4 |

| | |
|--------------|--|
| Message text | {protocol}: User {user name} loaded file type ConfigPack (restart required). |
| Example | WBM: User admin loaded file type ConfigPack (restart required). |
| Explanation | The configuration is applied. |
| Severity | Notice |
| Facility | local0 |
| Standard | IEC 62443-3-3 Reference: SR7.4 |

Index

A

- Aging
 - Dynamic MAC Aging, 238
- Authentication, 160
- Available system functions, 24

B

- Backup, 220
- Basic Wizard
 - Starting, 72
- BFP, 321
- Bridge, 110, 240
 - Bridge priority, 110, 240
 - Root bridge, 110, 240
- Bridge Max Age, 111, 241
- Bridge Max Hop Count, 111
- Brute Force Prevention, 321
- button, 187

C

- CA certificate, 54
- Certificates, 289
- Configuration
 - PPP, 230
- Configuration manuals, 330
- Configuration mode, 128
- Configuring the network via Ethernet
 - Connecting to network, 34
- CoS (Class of Service), 42
- C-PLUG
 - Formatting, 194
 - Saving the configuration, 194

D

- DCP Discovery, 198
- DCP server, 126
- Dead peer detection, 58
- Device
 - Basic Wizard, 75
 - System, 129
- Device certificate, 54

- DHCP
 - Client, 205
- DST
 - Daylight saving time, 171, 173

E

- Error status, 100

F

- Factory defaults, 330
- Factory setting, 330
- Fault monitoring
 - Connection status change, 190
- Forward Delay, 111, 241

G

- Geographic coordinates, 130
- Glossary, 4
- Groups, 278

H

- Hardware Revision, 92
- Hello time, 111, 241
- HTTP
 - Server, 125
- HTTPS
 - Server, 125

I

- ICMP, 39
- Information
 - ARP table, 93
 - Groups, 122
 - Hardware, 91
 - IPsec VPN, 106
 - IPv6 Neighbor Table, 94
 - LLDP, 103
 - Log table, 95, 99
 - OpenVPN client, 109
 - Role, 121
 - Security, 118, 120
 - Security log, 97

- SINEMA RC, 107
- SNMP, 103
- Software, 91
- Spanning Tree, 112
- Start page, 85
- Versions, 91
- IP address
 - Assignment with STEP 7, 36
 - Configuration, 251
- IPsec method, 55
- IPsec VPN
 - NETMAP, 52
 - Source NAT, 52
- IPv4
 - VRRPv3, 64
- IPv4 routing
 - Routing table, 104
- IPv6
 - Notation, 37
- IPv6 routing
 - Routing table, 105

K

- KEY-PLUG, 195
 - Formatting, 194

L

- Layer 2, 231
- Layer 3, 195
- LLDP, 103, 244
- Location, 130
- Log table
 - Event log, 95
 - Firewall log, 99
 - Security log, 97
- Login, 321
- Logout
 - Automatic, 186

M

- Maintenance data, 92
- Manufacturer, 92
- Manufacturer ID, 92

N

- NAPT
 - Configuring, 254
- NAT
 - 1-to-1 NAT, 258
 - Configuring, 253, 272
 - Masquerading, 51
 - NAPT, 51
 - NAT traversal, 57
 - NETMAP, 52
 - Source NAT, 52
- NAT traversal, 57
- NTP
 - Client, 179
 - Server, 185

O

- Order ID, 92

P

- Password, 280
 - Options, 282
- Ping, 197
- PLUG, 195
 - C-PLUG, (C-PLUG)
- point-to-point, 64
- Port
 - Port configuration, 225
- PPP
 - Configuration, 230
 - Overview, 228

Q

- QoS Trust, 42

R

- RADIUS, 283
- Redundant networks, 110, 240
- Requirement
 - Power supply, 22
- Reset, 132
- RESET button, 187
- Reset device, 330
- Reset timer BFP, 321

- Restart, 132
- Restore Factory Defaults, 330
- Roles, 276
- Root Max Age, 111, 241
- Routing, 246
 - ICMP, 39
 - IPv4 routing table, 104
 - IPv6 routing table, 105
 - Static routes, 246
- RSTP, 239

S

- Security settings, 163
- SELECT/SET button, 187
- Serial number, 92
- Server certificate, 54
- Service & Support, 4
- SFTP
 - Load/save, 143
- SHA algorithm, 163
- SIMATIC NET glossary, 4
- SIMATIC NET manual, 4
- SMTP
 - Client, 126
- SNAT
 - Configuring, 256
- SNMP, 43, 127, 157, 163
 - Groups, 162
 - Overview, 103
 - SNMPv1, 43
 - SNMPv2c, 43
 - SNMPv3, 43
 - Trap, 167
- SNMPv3
 - Access, 163
 - Groups, 162
 - Notifications, 167
 - Users, 160
 - Views, 165
- Software version, 92
- Source NAT
 - Masquerading, 51
- Spanning tree, 239
- Spanning Tree
 - Information, 112
 - Rapid Spanning Tree, 64
- SSH
 - Server, 125
- Standard mode, 55
- Start page, 85
- Stateful Inspection Firewall, 48

- Subnet
 - Configuration, 251
 - Overview, 248
- Subnets
 - Configuration (IPv6), 269
 - Connected Subnets (IPv6), 269
- Syslog
 - Client, 126
- System
 - Configuration, 122
 - Device, 129
 - General information, 129
 - Load and Save via HTTP, 136
- System event log
 - Agent, 188
- System events
 - Configuration, 148
 - Severity filter, 153
- System Time, 169

T

- Telnet
 - Server, 125
- TFTP
 - Load/save, 139
- Time
 - Time zone, 182
 - UTC time, 182
- Time of day
 - Manual setting, 76, 170
 - NTP Client, 76
 - SIMATIC Time Client, 183
 - SNTP (Simple Network Time Protocol), 176
 - System time, 76, 169
 - Time zone, 178
 - Time-of-day synchronization, 176
 - UTC time, 178
- Time setting, 127
- Training, 4
- Trigger interval BFP, 321

U

- User groups, 278

V

- VLAN, 40
 - Port VID, 236
 - Priority, 236

- Tag, 236
- VLAN ID, 43
- VLAN tag, 41
- VPN connection
 - Status, 106
 - Status OpenVPN client, 109
- VRRP
 - VRRP addresses overview (IPv4), 264
 - VRRPv3 Addresses Configuration (IPv4), 265
 - VRRPv3 Configuration (IPv4), 262
 - VRRPv3 routers (IPv4), 260
- VRRPv3
 - Backup router, 64
 - Interface Tracking, 266
 - Master router, 64
 - Virtual router, 64
 - VRRPv3 router, 64
 - VRRPv3 Statistics, 115

W

- Web Based Management, 67
 - Requirement, 67