

SIMATIC NET

Network components SCALANCE LPE9403 V4.0

Configuration Manual

<u>Preface</u>	1
<u>Security recommendations</u>	2
<u>System time on the SCALANCE LPE</u>	3
<u>Function Extender Interface ports (FEI ports)</u>	4
<u>Firmware update</u>	5
<u>IP address assignment</u>	6
<u>Linux Shell</u>	7
<u>Web User Interface</u>	8
<u>Applications</u>	9
<u>Appendix A "Syslog messages"</u>	A
<u>Appendix B "Supported encryption processes"</u>	B

Legal information

Warning notice system

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

DANGER

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

WARNING

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

CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

WARNING

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

Trademarks

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

Disclaimer of Liability

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

Table of contents

1	Preface	9
1.1	Additional documents	9
1.2	Cybersecurity information	9
1.3	Firmware/software support	10
1.4	License Conditions	10
1.5	Trademarks	10
2	Security recommendations	13
3	System time on the SCALANCE LPE	21
4	Function Extender Interface ports (FEI ports)	23
5	Firmware update	25
5.1	Update to firmware version 4.0	25
5.2	Update to firmware version 3.0	26
5.3	Update to firmware version 2.1	26
5.4	Update to firmware version 2.0	27
6	IP address assignment	29
6.1	Initial assignment of an IP address	29
6.2	DHCP	31
7	Linux Shell	33
7.1	Symbols for representing console commands	33
7.2	Interface names of FEI ports	33
7.3	Representation of password input	34
7.4	Size of the terminal window	34
7.5	Calling the Linux Shell	34
7.5.1	Accessing the Linux Shell via the USB console interface	34
7.5.2	Accessing the Linux Shell via a network connection	35
7.5.3	Inactivity timeout	36
7.5.3.1	Disabling the inactivity timeout temporarily	36
7.5.3.2	Changing the inactivity timeout temporarily	37
7.5.3.3	Changing the inactivity timeout permanently	37
7.6	Logging in	37
7.6.1	Default user profiles and passwords	37
7.6.2	Restrictions for User IDs and Group IDs	38
7.6.3	Logging On to a Device with Default Settings	38
7.6.4	Logging On to a Configured Device	40
7.6.5	Limiting login	40

7.6.5.1	Displaying the configuration.....	41
7.6.5.2	Configuring the login options	41
7.6.5.3	Releasing blocked IP addresses	42
7.7	Logging Off.....	42
7.8	ISO image	43
7.8.1	Displaying the content of the ISO image	43
7.8.2	Loading the ISO image from the module	44
7.8.3	Loading the ISO image onto the module (update).....	44
7.8.4	Deleting the ISO image	45
7.9	IP configuration	45
7.9.1	Displaying the ipconfig parameters.....	46
7.9.2	Displaying the IP configuration	47
7.9.3	Configuring the access rights of DCP.....	50
7.9.4	Configuring a static IPv4 address	51
7.9.5	Obtaining an IPv4 address via DHCP	51
7.9.6	Obtaining an IPv4 address for combo port P3C via DHCP.....	52
7.9.7	Disabling an interface	53
7.9.8	Configuring the default gateway statically	54
7.9.9	Configuring the default gateway dynamically	55
7.9.10	Deleting the configuration of the default gateway	55
7.9.11	Configuring IP addresses statically for DNS.....	57
7.9.12	Deleting statically configured IP addresses for DNS.....	58
7.9.13	Resetting the IP configuration.....	59
7.10	Port configuration	60
7.10.1	Enabling the Promiscuous Mode for a port	60
7.10.2	Disabling the Promiscuous Mode for a port.....	60
7.11	VXLAN configuration.....	61
7.11.1	Displaying the VXLAN configuration	62
7.11.2	Configuring a VXLAN connection.....	62
7.11.3	Locking the VXLAN configuration	64
7.11.4	Unlocking the VXLAN configuration.....	65
7.11.5	Adding the IP address of a VLXAN remote station.....	66
7.11.6	Deleting the IP address of a VLXAN remote station.....	67
7.11.7	Deleting the configuration of a VTEP	67
7.11.8	Deleting the VXLAN configuration	68
7.12	Device management	68
7.12.1	Showing device information.....	68
7.12.2	Overlay file system	70
7.12.3	Replacing the server certificate of the device	71
7.12.3.1	Creating a CSR with OpenSSL	72
7.12.3.2	Creating a certificate with OpenSSL	73
7.12.4	Firmware update.....	75
7.12.4.1	Checking the hash value of a firmware file	76
7.12.4.2	Checking the signature of a firmware file	76
7.12.4.3	Loading a firmware file via the USB interface.....	77
7.12.4.4	Loading a firmware file with SSH.....	80
7.12.5	Configuring the USB interface (Type A)	83
7.12.6	Resetting the configuration	84
7.12.7	Resetting the device to factory defaults	85

7.12.8	Configuring the log file.....	85
7.12.9	Encrypted transfer of syslog messages	86
7.12.10	Restarting the device	87
7.12.11	Shutting down the device	87
7.13	Backup file	87
7.13.1	Showing the existing backup files.....	87
7.13.2	Creating a backup file.....	88
7.13.3	Creating an encrypted backup file.....	89
7.13.4	Restoring a backup file	89
7.13.5	Restoring an encrypted backup file	90
7.13.6	Deleting a backup file.....	91
7.14	Configuring the firewall	91
7.14.1	Querying the status of firewalld.....	92
7.14.2	Displaying the firewall zones	93
7.14.3	Displaying the default zone	93
7.14.4	Displaying the configuration of a zone.....	93
7.14.5	Displaying the services of a zone	94
7.14.6	Displaying the ports of a zone	94
7.14.7	Adding a service to a zone	94
7.14.8	Removing a service from a zone	95
7.14.9	Adding a port to a zone.....	95
7.14.10	Removing a port from a zone	96
7.15	System time.....	96
7.15.1	Requirements for time synchronization with NTP	96
7.15.2	Displaying the status of NTP	97
7.15.3	Configuring an NTP server	97
7.15.4	Restarting NTP	97
7.15.5	Configuring Secure NTP.....	98
7.15.6	Configuring the system time manually.....	99
7.16	SNMP	100
7.16.1	SNMP on the SCALANCE LPE	100
7.16.2	Displaying the status of the SNMP service.....	101
7.16.3	Stopping the SNMP service.....	101
7.16.4	Starting the SNMP service	101
7.16.5	Disabling the SNMP service	101
7.16.6	Enabling the SNMP service	102
7.16.7	Data security with SNMP	102
7.16.8	Changing the access rights for SNMPv2c	103
7.16.9	Configuring SNMPv3 users (User-based Security Model).....	103
7.16.9.1	Configuration files for SNMPv3	103
7.16.9.2	Creating a new SNMPv3 user with default properties	104
7.16.9.3	Creating a new SNMPv3 user with specific properties.....	105
7.16.9.4	Changing the access rights for SNMPv3	107
7.17	SFTP	108
7.17.1	Establishing an SFTP connection	108
7.17.2	Closing an SFTP connection.....	108
7.17.3	Downloading a file	109
7.17.4	Uploading a file.....	109
7.18	Docker	110

7.18.1	Displaying Docker Containers configured in the device	110
7.18.2	Starting a Docker container	111
7.18.3	Stopping a Docker container	111
7.18.4	Restarting a Docker container	112
7.18.5	Killing the execution of a Docker container	113
7.18.6	Pausing the execution of a Docker container	114
7.18.7	Unpausing the execution of a Docker container	114
7.18.8	Removing a Docker container	115
7.18.9	Displaying Docker images saved in the device	115
7.18.10	Loading a Docker image from a repository or a registry	116
7.18.11	Running a Docker image	116
7.18.12	Displaying Docker Volumes	117
7.18.13	Network access from Docker containers	117
7.18.14	Displaying Docker Networks	118
7.18.15	Displaying information via Docker	118
7.18.16	Installing Nozomi Remote Collector	120
7.18.17	Deleting the installation file of the Nozomi Remote Collector	120
7.18.18	Docker Compose	121
7.18.18.1	Displaying information on Docker containers	121
7.18.18.2	Creating Docker containers and building resources	122
7.18.18.3	Stopping Docker containers and removing resources	122
7.18.18.4	Starting Docker containers	122
7.18.18.5	Stopping Docker containers	122
7.18.18.6	Killing Docker containers	123
7.18.18.7	Pausing Docker containers	123
7.18.18.8	Unpausing Docker containers	123
8	Web User Interface	125
8.1	Accessing the Web UI via a Network Connection	125
8.2	Inactivity timeout	126
8.2.1	Configuring the inactivity timeout for the Linux Shell	126
8.2.2	Configuring the inactivity timeout for the Web UI	127
8.3	Logging in	127
8.3.1	Default user profiles and passwords	127
8.3.2	Logging In to a Device with Default Settings	128
8.3.3	Logging In to a Configured Device	129
8.4	Logout	129
8.5	IP configuration	129
8.5.1	Displaying the IP configuration	129
8.5.2	Configuring the access rights of DCP	130
8.5.3	Configuring a static IPv4 address	131
8.5.4	Obtaining an IPv4 address via DHCP	131
8.5.5	Enabling/disabling an interface	132
8.5.6	Configuring the default gateway statically	132
8.5.7	Configuring the default gateway dynamically	133
8.6	Sfp Diagnose	133
8.6.1	Checking the operating state of an SFP	133
8.7	VXLAN configuration	134
8.7.1	Configuring a VXLAN connection	135

8.7.2	Enabling the VXLAN configuration.....	136
8.7.3	Disabling the VXLAN configuration.....	137
8.7.4	Adding a Virtual Tunnel Endpoint (VTEP)	137
8.7.5	Deleting the configuration of a VTEP	137
8.7.6	Deleting a VXLAN connection.....	138
8.8	Device management	138
8.8.1	Showing device information.....	138
8.8.2	Displaying information on the operating state	139
8.8.3	Updating the firmware or software	140
8.8.4	Web SSH	142
8.8.5	Showing applications.....	142
8.8.6	Stopping an application	142
8.8.7	Starting an application	143
8.8.8	Restarting an application	143
8.8.9	Resetting the configuration	144
8.8.10	Restarting the device	144
8.8.11	Shutting down the device	145
8.9	Backup file	145
8.9.1	Displaying the existing backup files	145
8.9.2	Creating a backup file.....	146
8.9.3	Downloading a backup file to a client PC.....	146
8.9.4	Uploading a backup file from a client PC	147
8.9.5	Restoring a backup file	147
8.9.6	Deleting a backup file.....	147
8.10	User management	148
8.10.1	Displaying the users	148
8.10.2	Creating a new user	148
8.10.3	Deleting a user.....	149
8.10.4	Changing the role of a user	149
8.10.5	Changing the password of a user.....	150
8.11	Syslog events.....	150
8.11.1	Configuring the syslog server	150
8.11.2	Configuring the directory for syslog messages	151
8.11.3	Displaying syslog messages.....	152
8.11.4	Deleting syslog messages.....	152
8.11.5	Downloading syslog messages	152
8.12	System time.....	152
8.12.1	Configuring NTP.....	153
8.12.2	Configuring Secure NTP.....	153
8.12.3	Disabling NTP	154
8.12.4	Configuring the system time manually.....	155
8.13	SNMP	155
8.13.1	Creating an SNMPv3 user.....	156
8.13.2	Changing the data of an SNMPv3 user.....	157
8.13.3	Deleting an SNMPv3 user	157
8.14	SFTP	158
8.14.1	Configuring an SFTP connection	158
8.14.2	Downloading a file	158
8.14.3	Uploading a file.....	159

8.15	Docker.....	159
8.15.1	Displaying Docker Containers configured in the device.....	160
8.15.2	Starting a Docker container.....	162
8.15.3	Stopping a Docker container.....	163
8.15.4	Restarting a Docker container.....	163
8.15.5	Killing the execution of a Docker container.....	163
8.15.6	Interrupting the execution of a Docker container.....	163
8.15.7	Resuming the execution of a Docker container.....	164
8.15.8	Deleting a Docker container.....	164
8.15.9	Displaying Docker Images saved in the device.....	164
8.15.10	Displaying Docker Volumes.....	165
8.15.11	Displaying Docker Networks.....	165
8.15.12	Displaying information via Docker.....	166
8.16	Docker installations.....	167
8.16.1	Installing Zscaler ZPA App Connector.....	167
8.16.2	Installing Nozomi Remote Collector.....	168
8.16.3	Deleting the installation file of the Nozomi Remote Collector.....	168
9	Applications.....	171
9.1	Use of software packages for the Debian GNU/Linux operating system.....	171
9.2	Updating program packages.....	172
9.3	Using your own applications.....	174
9.4	Reverse proxy.....	174
A	Appendix A "Syslog messages".....	175
A.1	Human user identification and authentication.....	176
A.2	User account management.....	177
A.3	Identifier management.....	179
A.4	Nonrepudiation.....	179
A.5	Restoration.....	179
B	Appendix B "Supported encryption processes".....	181
B.1	SSL.....	181
B.2	SSH.....	182
B.3	SNMP.....	183
	Index.....	185

Preface

This document describes how to configure and manage the SCALANCE LPE9403. The document is intended for technical network support personnel that are familiar with the operation of networks. It is also recommended for network and system planners, system programmers and network technicians.

1.1 Additional documents

The following additional documents may be of interest. Unless specified otherwise, the documents are available in the Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/15247>).

Note

The listed documents are the documents that were available at the time of the publication. Newer versions of these documents or the associated products may be available. Additional information is available in the SIOS or contact your Siemens customer service.

Product notes

Product notes are available online in the SIOS (<https://support.industry.siemens.com/cs/en/en/ps/6GK5998-3GS00-2AC2>).

Manuals

Document title	Link
Operating Instructions "SCALANCE LPE9403"	Visit (https://support.industry.siemens.com/cs/en/en/ps/6GK5998-3GS00-2AC2)
"Pluggable transceiver SFP/SFP+/SCP/STP" operating instructions	Visit (https://support.industry.siemens.com/cs/ww/en/ps/25547/man)

1.2 Cybersecurity information

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

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions 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 cybersecurity measures that may be implemented, please visit <https://www.siemens.com/cybersecurity-industry> (<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 Cybersecurity RSS Feed under <https://new.siemens.com/cert> (<https://www.siemens.com/cert>).

1.3 Firmware/software support

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

1.4 License Conditions

SCALANCE LPE uses Debian GNU/Linux as the operating system and includes other open source software.

The license terms are stored in an ISO image on the SCALANCE LPE. Please read the license conditions carefully.

For more information on accessing the license conditions, see "ISO image (Page 43)".

The license conditions are also available online in the SIOS. You can find the license conditions on the download page for the SCALANCE LPE firmware (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

1.5 Trademarks

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

- SCALANCE
- SINEC

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

The registered trademark Linux® is used according to a sublicense of LMI, the exclusive licensee of Linus Torvalds, owner of the trademark on a global basis.

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.

Security recommendations

NOTICE
Information security
Connect to the device and change the default password and the name of the default user "admin" before operating the device.

To prevent unauthorized access, note the following security recommendations.

General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products.
- 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, OpenVPN).
- Separate connections correctly (WBM, SSH etc.).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

Physical 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.
- Restrict physical access to the device to trusted personnel.
- Lock unused physical ports on the device. Unused ports can be used to access the system without authorization.
- 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 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 (e.g. 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.

Software (security functions)

- Keep the firmware up to date. Check regularly for security updates for the device. You can find information on this at the Industrial Security website.
- Inform yourself regularly about security recommendations published by Siemens ProductCERT.
- Only activate protocols that you require to use the device.
- Disable encryption methods with a low security level.
- The option of VLAN structuring provides protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- 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.
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).
- Ensure that the latest firmware version is installed, including all security-related patches. You can find the latest information on security patches for Siemens products on the Industrial Security or ProductCERT Security Advisories website.
For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.

Security by Default

Security by Default is a concept in which the configuration possibilities of the device are adapted automatically depending on the status of the device. All necessary configuration steps can be performed without restrictions in delivery state or after a reset to factory settings. After the first login and during operation, only users with administrator rights can configure security-relevant parameters. Non-secure management interfaces are either unavailable (Telnet) or disabled (HTTP, SNMPv1).

NOTICE

Security risk - risk of unauthorized access and/or misuse

By definition, DCP is not secure. The access rights of DCP depend on the status of the device.

- In the delivery state and after reset to default settings, DCP is enabled. Device parameters can be both read and modified. The access rights of DCP correspond to the `read-write` option.
The `read-write` setting could potentially be used to change the functionality of the device and thus cause the data communication to fail. Users with malicious intent who are in the same local network segment can change IP parameters and/or the PROFINET device name without authentication.
- After the first login with the default user profile **admin** and the assignment of a new password, the device changes the access rights automatically. Only read access is then possible with DCP. The device parameters can be read but not modified. From that point on, the access rights of DCP correspond to the `read-only` option.

To prevent unauthorized access and/or misuse, configure write-protected access rights for DCP (`read-only`).

Security by Default affects configuration with DCP as follows:

- **In delivery state or after a reset to factory settings**
 - Read and write access is possible via ports **P3C** and **EXTENDER1**.
 - DCP is disabled for ports **P1** and **P2** or **EXTENDER2** and **EXTENDER3**.
- **In operating state and after changing the default password**
 - Only read access is possible via ports **P3C** and **EXTENDER1**.
 - DCP is disabled for ports **P1** and **P2** or **EXTENDER2** and **EXTENDER3**.

Security by Default has no effect on DHCP. DHCP is enabled for ports **P1** to **P3C** and **EXTENDER1**. Ports **EXTENDER2** and **EXTENDER3** are disabled by default.

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.

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- 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.

Certificates and keys

- There is a preset X.509 TLS certificate in the device. Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed either by a reliable external or by an internal certification authority.
- Use a certification authority including key revocation and management to sign certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- It is recommended that you use password-protected certificates in the PKCS #12 format.
- Verify certificates and fingerprints on the server and client to prevent "man in the middle" attacks.
- It is recommended to use certificates with sufficient cryptographic security.
- Change certificates and keys immediately if there is a suspicion of compromise.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Handling certificates on the SCALANCE LPE

When the user does not have their own certificate saved in the device, SCALANCE LPE automatically uses the device certificate that is available on each device. For security reasons, this certificate is not visible in the file system.

When a user certificate with the name **server_certificate_custom.pem** exists in the **/etc/ssl/certs/edgebox_web_app/https** directory, the device uses this certificate instead of the module certificate with login via the Web UI. With login via the Linux shell, the module certificate is always used. During a reset of the configuration, all user certificates in the **/etc/ssl/certs/edgebox_web_app/https** directory are deleted.

Secure/non-secure protocols and services

- Check whether use of the following protocols and services is necessary:
 - Non-authenticated and unencrypted ports
 - Syslog
 - DHCP options 66/67
 - TFTP (The TFTP service is only active in the Rescue system.)
- The following protocols provide secure alternatives:
 - HTTP → HTTPS
 - Telnet → SSH
 - TFTP → SFTP
 - NTP → NTPsecure
- Use secure protocols when access to the device is not secured by physical protection measures.
- If you require non-secure protocols and services, operate them only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.
- If you use RADIUS for management access to the device, enable secure protocols and services.
- After commissioning, the Discovery and Basic Configuration Protocol (DCP) access rights are automatically set to write-protected. If your environment does not require DCP, it is recommended that the protocol be completely disabled.

Interface security

- Disable unused interfaces.
- Use IEEE 802.1X for interface authentication.

SCALANCE LPE uses the **firewalld** program as the firewall.

Notes on the Linux system of the device

The device uses Debian GNU/Linux as operating system. The following requirements with respect to network security result from this:

- You can install security patches from Debian directly as soon as they are published (by Debian). If this involves packets that were pre-installed by Siemens, you install the update at your own risk because Siemens cannot ensure the compatibility in advance. Proper functioning of the device can be affected. The security patches that have been published by Debian by then will be integrated by Siemens in the next firmware release.
- During a firmware update, the installed security patches are lost and you need to install them again subsequently.
- A user with Root rights can read out device certificates that could be misused in other systems. Therefore, the general rules of information security should be considered when assigning access rights.
- Applications developed by Siemens AG for this device, e.g. DCP and Web UI, are also components of the Linux system. Do not delete these applications; otherwise, proper functioning of the device could be impaired.

List of available protocols

The following is a list of all available protocols and services as well as their ports through which the device can be accessed, including the following information:

- **Protocol/service**
The protocols/services supported by the device.
- **Protocol**
The protocol used by the service.
- **Port number**
The port number assigned to the service.

Note

The table contains the preset ports. Additional ports can be opened for protocols with a configurable port number.

- **Default port status/protocol status**
The default state (i.e. open, closed, active).
- **Protocol/service configurable**
Specifies whether or not the protocol or service can be configured.
- **Port number configurable**
Specifies whether the port number can be configured.
- **Authentication**
Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.
- **Encryption**
Specifies whether the transfer is encrypted or whether the encryption can be configured.

Service	Protocol	Port number	Default port status	Protocol/service configurable	Port number configurable	Authentication	Encryption
Edgeboxwebapp	TCP	8080	Open	✓	✓	-	-
HTTP ¹⁾	TCP	80	Open	✓	✓	-	-
HTTPS	TCP	443	Open	✓	✓	✓	✓
NTP	UDP	123	Closed	✓	✓	-	-
NTP secure	UDP	123	Closed	✓	✓	✓	-
SFTP	TCP	22	Open	✓	✓	✓	✓
SNMP	UDP	161	Open	✓	✓	Configurable	-
SSH	TCP	22	Open	✓	✓	✓	✓
TFTP	UDP	69	Open ²⁾	-	-	-	-

¹⁾ Serves only as a reference to the HTTPS service.

²⁾ The TFTP service is only active in the Rescue system.

Outbound connections

Service	Protocol	Port number	Default port status	Protocol/service configurable	Port number configurable	Authentication	Encryption
DHCP	UDP	68	Closed	✓	-	-	-
Syslog	UDP	(zufällig) ¹⁾	Closed	✓	-	-	-

¹⁾ Needed to send outbound datagrams to the remote syslog server. The port number is not used for inbound traffic.

Service	Protocol	Default protocol status	Protocol/service configurable	Authentication	Encryption
DCP	PROFINET	Active	✓	-	-
LLDP	Ethernet	Active	✓	-	-
Ping	ICMP	Active	-	-	-

Secure Boot

Secure Boot is a security standard that allows a device to start only with trusted software components (bootloader, operating system etc.). Secure Boot is part of the UEFI (Unified Extensible Firmware Interface), an interface between the hardware and the operating system.

During booting with Secure Boot, each involved component is checked for authenticity and integrity. Use of software not signed by the manufacturer is not possible. Furthermore, Secure Boot allows additional security functions for which a secure boot process is essential, such as fTPM with SCALANCE LPE, to be activated.

With Secure Boot, it is no longer possible to use self-generated components for the system test (bootloader, kernel etc.). There are not restrictions during operation; any applications can be installed, updated, modified or deleted as before.

SCALANCE LPE supports the Secure Boot function as of hardware release 2. You will find the hardware release of your device on the type plate. On the type plate, the hardware release is printed as a placeholder "X". "X 2 3 4 5 6" designates a device with hardware release 1.

System time on the SCALANCE LPE

A consistent system time is essential for correct functioning of a UNIX system. There are several parameters for handling the system time in a Unix system. The parameters have the following meaning:

- **Epoch Time (Unix time)**
The Unix time was developed to represent a time of day as an integer. In conventional Unix systems, the number of seconds since 1 January 1970 is specified. Through this type of representation, time specifications can be compared without further conversion.
- **Hardware-Clock**
This time, also referred to as Real Time Clock (RTC), represents the time system of the device hardware. This time system is not affected by shutdown of the device and is the starting point for the system time of the operating system.
- **System Time**
The system time is managed by the operating system and is used by all processes that require the current time.

For an exact system time, synchronization with an external time server is recommended. In the device, a consistent reference point for determining the system time must be available regardless of synchronization with external servers. For this purpose, the following services are implemented in a SCALANCE LPE:

- **set-clock-epoch.service**
This service is executed when the device starts and checks whether the `/usr/lib/clock-epoch` file is present. If this file is not present, it is created and receives the time stamp 31 July 2023.
- **load-system-time.service**
This service is executed when the device starts and initializes the system time. The following conditions determine whether the Epoch Time or the Hardware-Clock is used:
 - If the Epoch Time has a higher value than the Hardware-Clock, the system time is initialized with the Epoch Time.
 - If the Hardware-Clock has the same value or a higher value than the Epoch Time, the system time is initialized with the Hardware-Clock.
- **tohwclock.service**
This service is executed five minutes after the device starts and then every five minutes. The Hardware-Clock is synchronized with the current system time. For this purpose, the `/usr/sbin/hwclock --systohc` command is executed.
- **save-system-time.service**
This service is executed when the device shuts down and provides the `/usr/lib/clock-epoch` file with the time stamp of the current system time. The aim is to save the current system time as Epoch Time.

Function Extender Interface ports (FEI ports)

When operating a SCALANCE LPE connected to a SCALANCE switch via the function extender interface, the three RJ45 sockets and the SFP slot of the SCALANCE LPE are disabled. These external ports cannot be used for data transmission. When plugged in, the SCALANCE LPE has three internal ports (function extender interface ports) that are functionally connected to the ports of the SCALANCE switch. The Function Extender Interface ports are displayed in the shell (`ipconfig -s`) as well as in the Web UI. The following assignment applies to the interface names:

SCALANCE LPE	SCALANCE switch
EXTENDER1	extender0/1
EXTENDER2	extender0/2
EXTENDER3	extender0/3

Note

Status of a function extender interface

With a SCALANCE LPE that is connected to a SCALANCE switch, the displayed status of a function extender interface can deviate from the actual status. This applies in the following cases:

- A function extender interface is disabled in SCALANCE LPE, for example with the command `ipconfig -i {EXTENDER1 | EXTENDER2 | EXTENDER3} -c down`. The status **up** continues to be shown for the affected interface in the SCALANCE switch.
- The `EXTENDER3` function extender interface is disabled in the SCALANCE switch. The status **up** continues to be shown for the function extender interface `EXTENDER3` in SCALANCE LPE.

With the exception of "P2" or "EXTENDER2", external and internal ports have different MAC addresses. The "EXTENDER2" RDI port always adopts the MAC address of the "P2" port.

Firmware update

This section describes which points need to be noted with respect to a firmware update for the different versions.

5.1 Update to firmware version 4.0

Requirements

Before an update to version 4.0, it is necessary to update the following software components to **firmware version 3.0**:

- **Firmware, bootloader and Rescue system**
scalance-lpe9403-upgrade_V2.1_to_V3.0.swu

You can find detailed information in section "Update to firmware version 3.0 (Page 26)".

Files for firmware version 4.0

The components for an update to firmware version 4.0 are available on the Internet at the following address:

Firmware and ISO image for the SCALANCE LPE9403 V4.0 (<https://sieportal.siemens.com/su/bkxfN>)

Procedure

You have the following options for the update:

- **Linux Shell**
Firmware update (Page 75)
- **Web UI**
Updating the firmware or software (Page 140)

5.2 Update to firmware version 3.0

Requirements

Before an update to version 3.0, it is necessary to update the following software components to **firmware version 2.1**:

- **Bootloader**
scalance-lpe-V02.01.00_Firmware_with_Bootloader.swu
- **Rescue system**
scalance-lpe-V02.01.00_rescue.swu

You can find detailed information in section "Update to firmware version 2.1 (Page 26)".

Files for firmware version 3.0

The components for an update to firmware version 3.0 are available on the Internet at the following address:

Firmware and ISO image for the SCALANCE LPE9403 V3.0 (<https://support.industry.siemens.com/cs/document/109826981>)

Procedure

Updating from firmware version 2.1 to firmware version 3.0 can **only be performed in the Rescue system** with the following file:

scalance-lpe9403-upgrade_V2.1_to_V3.0.swu

You will find the description of how to perform a firmware update in the Rescue system in the section "Resetting the device to factory defaults (Page 85)".

5.3 Update to firmware version 2.1

Requirements

Before updating to version 2.1, it is advisable to update the following software components to **version 2.0**:

- **Firmware**
lpe.sfw
- **Bootloader**
uboot.sfw
- **Rescue system**
rescue.sfw

You can find detailed information in section "Update to firmware version 2.0 (Page 27)".

Files for firmware version 2.1

The components for an update to firmware version 2.1 are available on the Internet at the following address:

Firmware and ISO image SCALANCE LPE9403 V2.1 (<https://support.industry.siemens.com/cs/document/109817856>)

Procedure

You have the following options for the update:

- **Linux Shell**
Firmware update (Page 75)
- **Web UI**
Updating the firmware or software (Page 140)

5.4 Update to firmware version 2.0

Requirements

An update from firmware version 1.0 to firmware version 2.0 or higher is not possible. If the device has firmware version V1.0, you first need to update the following software components to **firmware version 1.1**:

- **Firmware**
lpe_V1.1.sfw
- **Bootloader**
uboot_V1.1.sfw
- **Rescue system**
rescue_V1.1.sfw

The components for an update to firmware version 1.1 are available on the Internet at the following address:

Firmware and ISO image SCALANCE LPE9403 V1.1 (<https://support.industry.siemens.com/cs/document/109805118>)

Files for firmware version 2.0

The components for an update to firmware version 2.0 are available on the Internet at the following address:

Firmware and ISO image SCALANCE LPE9403 V2.0 (<https://support.industry.siemens.com/cs/document/109811123>)

Procedure

You have the following options for the update:

- **Linux Shell**
Firmware update (Page 75)
- **Web UI**
Updating the firmware or software (Page 140)

IP address assignment

This chapter describes features related to the assignment of IP addresses, such as DHCP and DNS.

6.1 Initial assignment of an IP address

Initial assignment of IP addresses for the SCALANCE LPE cannot take place with the Web user interface (Web UI) because this configuration tool can only be used if an IP address already exists.

The following options are available to assign an IP address to an unconfigured device:

- **USB console interface**

If you are connected with the SCALANCE LPE via the USB console interface, you can configure the IP address, the subnet mask and other IP parameters with the **ipconfig** command.

For more information on the **ipconfig** command, refer to "Configuring a static IPv4 address (Page 51)".

For more information on the USB console interface, see "Accessing the Linux Shell via the USB console interface (Page 34)".

- **DHCP**

DHCP is activated for the following ports by default:

- P1
- P2
- P3C
- EXTENDER1

DHCP is disabled by default for the function extender interface ports **EXTENDER2** and **EXTENDER3**. If a DHCP server is available in the local network and this responds to the DHCP request of the SCALANCE LPE, the IP address and subnet mask are assigned automatically when the module first starts up. All ports can receive a gateway address. One port is the default gateway; the presetting is port "P3C".

- **SINEC PNI** (SINEC Primary Network Initialization)

This program for initial commissioning of network devices uses the DCP (Discovery and basic Configuration Protocol) to detect devices in a network and assign an IP address.

For more information, refer to PNI (<https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=en-US>)

- **PRONETA**

PRONETA is a free application for the simple configuration of PROFINET networks based on DCP.

For more information, refer to PRONETA (<https://support.industry.siemens.com/cs/products?mfn=ps&pnid=24173&lc=en-WW>)

6.1 Initial assignment of an IP address

One IP address for each port

Observe the following when assigning IP addresses: In contrast to a switch, each port of the SCALANCE LPE is given its own IP address. No frames are forwarded between the ports of the device. Even if all ports of the SCALANCE LPE are in the same Layer 2 network, this does not create network loops. However, the ports should receive IP addresses from different subnets, if possible, and not be connected to the same Layer 2 networks.

NOTICE
Security risk - Risk of unauthorized access and/or misuse
DCP does not have mechanisms for authentication and encryption and should therefore only be used in secure networks. Write access with DCP could potentially be used to change the functionality of the device and thus cause data communication to fail. Users with malicious intent who are in the same local network segment can change IP parameters without authentication.
You can find additional information on the configuration of access rights of DCP in section Security recommendations (Page 13).

6.2 DHCP

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 lease time has elapsed, the DHCP client requests an extension of the lease time from the DHCP server. The DHCP then normally extends the lease time. After the entire time period has expired, the device deletes its IP address. If required, 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 may receive a different address from the previous address. It is possible to configure the DHCP server so that the DHCP client always receives the same address in response to its request. In the configuration of the DHCP client, the parameter via which the DHCP client is identified is defined. The following options are available:
 - MAC address
Default setting for all ports. This information is sent in the DHCP option 61.
 - DHCP Unique Identifier (DUID) and, depending on the mode, Interface Identity Association Identifier (IAID). This information is sent in DHCP option 61.
The DUID must conform to the RFC 3315 and RFC 6355 specifications (length 14 bytes, only the last 8 bytes are freely configurable, e.g. with SINEC PNI).
 - Device name
This information is sent in the DHCP option 12.

DUID, IAID and device name are only available for port P3C.

Note

With configuration of the IP address via DHCP, you must ensure that the DHCP server always assigns the same IP address to the SCALANCE LPE.

Linux Shell

The configuration of the device via the Linux Shell is described in this section. In addition to device management, the assignment of an IP address, for example, is also a subject of the description.

7.1 Symbols for representing console commands

When setting parameters of console commands, the following characters are used:

Charac- ters	Meaning	
< ... >	Mandatory parameter	Instead of the expression in parenthesis, you must enter a value
[...]	Optional parameter	Instead of the expression in parenthesis, you can enter a value
(...)	Value or range of values	Enter a value to replace the expression in parenthesis
(... - ...)	Range of values	Enter a value from this range of values
{ ... }	Selection list	Select one or more elements from the list
{ }	Exclusive selection	Select exactly one element from this list

The console commands and their outputs are listed in multiple rows in this document to take up less space. Note that they must be entered as a single row in the CLI.

7.2 Interface names of FEI ports

When operating a SCALANCE LPE connected to a SCALANCE switch via the function extender interface, the function of the ports P1, P2 and P3 changes. These ports become internal ports (function extender interface ports) with different interface names. In this case, you must use the names of the **function extender interface ports** (FEI ports) for all inputs in the shell. The following assignment applies here:

Interface name of SCALANCE LPE	Interface name of FEI ports of SCALANCE LPE
P1	EXTENDER1
P2	EXTENDER2
P3C	EXTENDER3

The description of the shell commands uses the interface names **P1**, **P2** and **P3C** consistently.

Example

To display the MAC address of the first port of SCALANCE LPE, run the following command:
`deviceinfo mac P1`

To display the MAC address of the first function extender port of SCALANCE LPE when using the function extender interface, run the following command:

```
deviceinfo mac EXTENDER1
```

7.3 Representation of password input

If the user enters a password in the console, the password is not displayed, also not symbolically by means of a placeholders. In contrast to this, in the descriptions of the commands and in the examples, password input is symbolized by several stars.

7.4 Size of the terminal window

For optimum display of the commands you have entered and their outputs, you can adjust the size of the terminal window. This setting is only relevant for the USB console interface. A size of 60 lines with 120 characters each is recommended. For correct display, the set size must correspond to the actual size of the terminal window.

You need to make the settings for the terminal window after each login with the following command:

```
stty rows 60 cols 120
```

7.5 Calling the Linux Shell

The following options are available for accessing the Linux Shell:

- A serial connection via USB between a client PC and the device,
- A network connection via SSH to the device.
- The Web SSH (menu **System** » **Web SSH** in the Web UI, only with administrator rights)

7.5.1 Accessing the Linux Shell via the USB console interface

Via the USB console interface on the device (USB socket Type B), you can access the device directly via a virtual serial connection (115200 8N1) without assigning an IP address. Access to the device is possible independent of the Ethernet ports.

Requirements

- To connect the USB console interface of the device with a client PC, you require a cable with a USB Type B plug and USB Type A plug. The connecting cable for the USB console interface can be ordered as accessory (article number: 7ML1930-1FN).
- To use the USB console interface under Windows, you must download and install the following driver to a client PC:
Driver (<https://support.industry.siemens.com/cs/ww/en/ps/6GK5998-3GS00-2AC2/dl>)

- To use the USB console interface under Linux, you must download and configure the kernel module **cp210x** on the client PC. Follow the steps outlined below:

```
~$ sudo -i
```

```
~# modprobe cp210x
```

```
~# echo 0908 0070 > /sys/bus/usb-serial/drivers/cp210x/new_id
```

Create the file **99-cp210.rules** in the directory **/etc/udev/rules.d** with the following content in one line. The multi-line display in the following paragraph is only for better readability. Use the manufacturer ID **0908** and the product ID **0070**.

```
ACTION=="add",
```

```
ATTRS{idVendor}=="0908",
```

```
ATTRS{idProduct}=="0070",
```

```
RUN+="/sbin/modprobe cp210x"
```

```
RUN+="/bin/sh -c 'echo 0908 0070 > /sys/bus/usb-serial/drivers/
cp210x/new_id'"
```

Restart the device or execute the following command:

```
~$ sudo udevadm control --reload
```

- Terminal software for establishing serial connections is available on the client PC.

Establishing a connection to the device

Proceed as follows to access the Linux Shell:

- Make the following connection settings in the terminal software:

Connection type	Serial
Transmission rate	115200
Data rate	8 bits
Parity	None
Stop	1 bit
Flow control	None

- Establish a connection to the device via the correct COM port.
- Log in.
For more information, refer to "Logging in (Page 37)".

7.5.2 Accessing the Linux Shell via a network connection

You can access the Linux Shell with an SSH client via an Ethernet port of the device. The Telnet protocol is not supported by the device.

Requirements

- The device has an IP address.

Note

The following options apply to the assignment of an IP address:

- USB console interface
- DHCP
- SINEC PNI
- PRONETA

For more information, refer to "Initial assignment of an IP address (Page 29)".

- There is a network connection between the device and the client PC.
- The network settings of the device and of the client PC match.

Note

You can use the "ping" diagnostics tool to check whether a connection exists and communication is possible.

- Terminal software for establishing SSH connections is available on the client PC.

Establishing a connection to a device

Proceed as follows to access the Linux Shell:

1. Make the following connection settings in the terminal software:

Connection type	SSH
IP address	The IP address of the device
TCP port	22

2. Establish a connection to the device.
3. Log in.
For more information, refer to "Logging in (Page 37)".

7.5.3 Inactivity timeout

An inactivity timeout is configured for interactive shells of the SCALANCE LPE via serial connections and network connections. If there is no input at the terminal during a specified period, the terminal session is automatically terminated. The default value for this period is 300 seconds.

7.5.3.1 Disabling the inactivity timeout temporarily

To disable the inactivity timeout temporarily, run the following command:

```
unset TMOUT
```

7.5.3.2 Changing the inactivity timeout temporarily

To temporarily change the duration for the inactivity timeout, run the following command:
`export TMOUT=<Duration in seconds>`

7.5.3.3 Changing the inactivity timeout permanently

To change the period for the inactivity timeout permanently, you must adapt the file **/etc/profile.d/timeout.sh**. Follow the steps outlined below:

1. Open the file `/etc/profile.d/timeout.sh` with the nano editor, for example, that is installed on the SCALANCE LPE:
`sudo nano /etc/profile.d/timeout.sh`
2. Enter the desired value for the `timeout` parameter. The value "0" disables the inactivity timeout. If you want to configure the value 600 seconds for the inactivity timeout, the following entry is required:
`timeout=600`
3. Save the file and close the editor. The change does not affect the ongoing terminal session. The new value applies to all subsequent terminal sessions. The SCALANCE LPE does not need to be rebooted.

7.6 Logging in

The various methods for logging in are described in this section.

7.6.1 Default user profiles and passwords

The following default user profiles and passwords are preconfigured:

 CAUTION
Security risk - Danger of unauthorized access and/or exploitation. Before commissioning the device, change the default passwords and user names to prevent unauthorized access. For more information, refer to "Logging On to a Device with Default Settings (Page 38)".

Profile	Password
admin	admin

7.6.2 Restrictions for User IDs and Group IDs

If fewer than 500 users, system users and groups are created and no UIDs or GIDs are specified, there are no restrictions regarding the user IDs or group IDs. Otherwise, a UID or GID must be specified according to the following rules.

If the UID is specified with the parameter **-u** for **useradd** or the GID with the parameter **-g** for **groupadd**, only values from the following ranges can be used for the UIDs or GIDs:

- **For system users and groups**
1000 ... 60000
- **For users and groups**
 - 1000 ... 1499
 - 2000 ... 60000

7.6.3 Logging On to a Device with Default Settings

This section describes how to change the default password and optionally the administrator user name. You need to change the default password in the following cases:

- On initial commissioning
- After loading a firmware file in the Rescue system
- After resetting the configuration with the console command **configreset**, via the menu **System » Reset configuration** in the Web UI or by pressing the button when the power is switched on.

When you log in to a device with default settings, follow these steps:

1. Set up a connection to the device and call the Linux Shell.
The login prompt is displayed.
For more information, refer to "Calling the Linux Shell (Page 34)".
2. Enter the factory default user name.
For more information, refer to "Default user profiles and passwords (Page 37)".
3. Enter the factory default password. If the entries are incorrect, access is denied.
4. At the following prompt, enter **y** if you want to change the user name **admin**, otherwise enter **n**.
5. [Optional] If you entered **y** at step 4, you must enter a new user name for the administrator twice. The user name must not contain any special characters except the characters "_" and "-". The user name must start with a letter or with the character "_".

6. Assign a new password. The new password must meet the following conditions:

- At least 12 characters
- Maximum of 250 characters
- At least one number
- At least one uppercase letter
- At least one lowercase letter
- At least one special character: # ! \$ % & () * + , - . / : < = > @ [] ^ _ { } ~

If the password does not meet the specified criteria, a corresponding note is displayed and you are prompted to enter a password again.

7. Confirm the new password by entering it again. If the entries are incorrect, an error message is displayed. Repeat the last steps.

8. You are now in the Linux Shell.

Example 1

```
login as: admin
admin@192.168.178.34's password: *****
Linux lpe9403-VPM7001325 5.10.104-audis-std #1 SMP PREEMPT Thu Mar
17 22:51:39 UTC 2022 aarch64
```

```
The programs included with the Debian GNU/Linux system are free
software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
Last login: Wed Mar 23 16:20:07 2022 from 192.168.178.20
```

```
Change admin username (y/n)? n
New password: *****
Retype new password: *****
passwd: password updated successfully
```

Example 2

```
login as: admin
admin@192.168.178.34's password: *****
Linux lpe9403-VPM7001325 5.10.104-audis-std #1 SMP PREEMPT Thu Mar
17 22:51:39 UTC 2022 aarch64
```

```
The programs included with the Debian GNU/Linux system are free
software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

```
Last login: Wed Mar 23 16:20:07 2022 from 192.168.178.20
```

```
Change admin username (y/n)? y
Enter a new non-default username: myname
Confirm new non-default username: myname
New password: *****
Retype new password: *****
```

7.6.4 Logging On to a Configured Device

When you log in to a configured device, follow these steps:

1. Set up a connection to the device and call the Linux Shell.
The login prompt is displayed.
For more information, refer to "Calling the Linux Shell (Page 34)".
2. Enter the user name.
Only use ASCII characters for the user name.
3. Enter the password.
The Linux Shell checks the entries.
 - If the entries are correct, you are in operating mode.
 - If the entries are incorrect, an error message is displayed. Repeat the last steps.

Example

```
login as: admin
admin@192.168.16.15's password: *****
Linux lpe9403-VPM7001325 4.19.118-audis-std #1 SMP PREEMPT
Tue May 12 18:39:32 UTC 2020 aarch 64
```

```
The programs included with the Debian GNU/Linux system are free
software;
the exact distribution terms for each program are described in the
individual files in /usr/share/*/copyright
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 12 19:11:21 2020 from 192.168.1.2
admin@lpe9403-VPM7001325:~$
```

7.6.5 Limiting login

To ensure availability of a device, the number of login attempts permitted can be limited. SCALANCE LPE uses the **fail2ban** software package for this purpose. You use the command line program **fail2ban-client** to configure both the maximum number of login attempts and the time period during which, after the maximum possible login attempts, no further login is possible.

You can configure the following access possibilities independent of each other:

- SSH client
- Login page of the Web UI
- SNMP users

The following default values apply to all access possibilities:

Parameter	Value
Maximum number of login attempts	5
Time period during which no login is possible	10 minutes

7.6.5.1 Displaying the configuration

To display the configuration for the login limitation, run the following command:

```
sudo fail2ban-client get {sshd | edgebox_web_app | snmpd}  
{maxretry | bantime}
```

The meaning of the parameters is as follows:

Parameter	Description
sshd	The value for the login with the SSH client is displayed.
edgebox_web_app	The value for the login with the Web UI is displayed.
snmpd	The value for the login of an SNMP user is displayed.
maxretry	The number of the maximum possible login attempts is displayed.
bantime	The time period, in seconds, during which a login is not possible is displayed. A negative value means that login is permanently blocked.

Example

Display of the maximum possible login attempts with the SSH client:

```
admin@lpe9403-VPM7001325:~$ sudo fail2ban-client get sshd maxretry  
5
```

Example

Display of the time period during which a login with the Web UI is not possible:

```
admin@lpe9403-VPM7001325:~$ sudo fail2ban-client get  
edgebox_web_app bantime  
600
```

7.6.5.2 Configuring the login options

To configure the login options, run the following command:

```
sudo fail2ban-client set {sshd | edgebox_web_app | snmpd}  
{maxretry <Number> | bantime <Time>}
```

The meaning of the parameters is as follows:

Parameter	Description
sshd	The value for the login with the SSH client is configured.
edgebox_web_app	The value for the login with the Web UI is configured.
snmpd	The value for the login of an SNMP user is configured.
maxretry	The number of the maximum possible login attempts is configured.
Number	The number of login attempts.
bantime	The time period, in seconds, during which a login is not possible is configured.
Time	The value in seconds. A negative value means that login is permanently blocked.

Example

Limitation of login with the SSH client to a maximum of eight attempts:

```
admin@lpe9403-VPM7001325:~$ sudo fail2ban-client set sshd maxretry 8
```

Example

Definition of the time during which a login with the Web UI is not possible to 15 minutes:

```
admin@lpe9403-VPM7001325:~$ sudo fail2ban-client set
edgebox_web_app bantime 900
```

7.6.5.3 Releasing blocked IP addresses

To lift the temporary or permanent block of the login for one or more users, run the following command:

```
sudo fail2ban-client set {sshd | edgebox_web_app | snmpd}
unbanip <IP address> . . . <IP address>
```

The meaning of the parameters is as follows:

Parameter	Description
sshd	The block of login with the SSH client is lifted for the stated IP addresses.
edgebox_web_app	The block of login with the Web UI is lifted for the stated IP addresses.
snmpd	The block of login for an SNMP user is lifted for the stated IP addresses.
IP address	The IP addresses of users whose login block is being lifted.

Example

The block of login with the Web UI is lifted for the user with IP address 192.168.2.1:

```
sudo fail2ban-client set edgebox_web_app unbanip 192.168.2.1
```

7.7 Logging Off

To log out and end the session, execute the following command in operating mode:

```
exit
```

Automatic logout

After a specific period of inactivity, the device ends the terminal session automatically. You can configure the value for the inactivity timeout. For more information, refer to "Changing the inactivity timeout permanently (Page 37)".

7.8 ISO image

An ISO image is stored on the SCALANCE LPE. The ISO image contains the license conditions, the documentation and the readme file for the current firmware version.

The ISO image is already mounted in the delivery state.

Note

The ISO image is very large. You can free up additional space on the SCALANCE LPE by copying the contents of the ISO image and deleting it from the SCALANCE LPE.

7.8.1 Displaying the content of the ISO image

Requirement

SCALANCE LPE is connected to a client PC via a serial connection. For more information, refer to "Accessing the Linux Shell via the USB console interface (Page 34)".

Alternatively, you can also set up an SSH connection.

Displaying the content of the ISO image

To display the content of the ISO image, execute the following command:

```
ls -al /mnt/lpeiso
```

Example

```
admin@lpe9403-VP7001325:~$ ls -al /mnt/lpeiso
total 1869
drwxr-xr-x 6 admin admin 2048 Nov 2 2020 .
drwxr-xr-x 3 root root 4096 Nov 2 2020 ..
drwxr-xr-x 2 admin admin 2048 Nov 2 2020 Betriebsanleitung
drwxr-xr-x 2 admin admin 2048 Nov 2 2020 LiesMich
drwxr-xr-x 2 admin admin 28672 Nov 2 2020 OSS
drwxr-xr-x 2 admin admin 2048 Nov 2 2020 Projektierungshandbuch
-rwxr-xr-x 1 admin admin 876242 Nov 2 2020
ReadMeOSS_SCALANCE_LPE9403_V1p0.html
-rwxr-xr-x 1 admin admin 995550 Nov 2 2020
ReadMeOSS_SCALANCE_LPE9403_V1p0.pdf
```

7.8.2 Loading the ISO image from the module

Requirements

- SCALANCE LPE is connected to a client PC via a serial connection. For more information, refer to "Accessing the Linux Shell via the USB console interface (Page 34)". Alternatively, you can also use an SSH connection for the data transfer.
- A USB storage medium is connected to the USB interface of the device. The following file systems are supported on the USB storage medium:
 - ext4
 - FAT

Copying the ISO image

To copy the ISO image, execute the following command:

```
cp /userdata/lpe.iso <USB path>
```

Example

```
admin@lpe9403-VPM7001325:~$ cp /userdata/lpe.iso /myusb
```

7.8.3 Loading the ISO image onto the module (update)

A firmware update has effects on the ISO image of the SCALANCE LPE:

- **Firmware update via the rescue system**
The ISO image is deleted during a firmware update via the rescue system.
- **Firmware update via the Web UI**
The ISO image is deleted during a firmware update via the Web UI. However, the information contained in the ISO image no longer applies to the updated firmware on the device.

An ISO image suitable for the firmware is available for download from Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

Requirements

- SCALANCE LPE is connected to a client PC via a serial connection. For more information, refer to "Accessing the Linux Shell via the USB console interface (Page 34)". Alternatively, you can also use an SSH connection for the data transfer.
- A USB stick contains the ISO image (.iso) at the first directory level and is connected to the USB 3.0 interface (Type A) of the device. The following file systems are supported on the USB flash drive:
 - ext4
 - FAT

Loading the ISO image onto the SCALANCE LPE

To load the ISO image onto the SCALANCE LPE, proceed as follows:

Step	Instruction	Command
	[Optional] Delete any existing ISO image.	See section "Deleting the ISO image (Page 45)".
1	Create a "usb" directory as mount point for the file system of the USB flash drive.	<code>mkdir usb</code>
2	Mount the file system of the USB flash drive.	<code>sudo mount /dev/sda1 usb</code>
3	Copy the ISO image.	<code>sudo cp /usb/lpe.iso /userdata/lpe.iso</code>
4	Mount the ISO image.	<code>sudo mount /userdata/lpe.iso /mnt/lpeiso</code>

7.8.4 Deleting the ISO image

Note

Deleting the ISO image is irreversible. The ISO image is no longer available after a restart or download of a new firmware file.

The license conditions are also available online in the SIOS. You can find the license conditions on the download page for the SCALANCE LPE firmware (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

To delete the ISO image, follow these steps:

Step	Instruction	Command
1	Unmount the directory in which the ISO image is located.	<code>sudo umount /mnt/lpeiso</code>
2	Delete the ISO image.	<code>sudo rm /userdata/lpe.iso</code>

7.9 IP configuration

This section describes functions in connection with the static and dynamic assignment of IPv4 addresses. IPv6 is not supported.

The following default settings apply in the delivery state and after a reset:

- IP address and subnet mask: DHCP is enabled for all ports.
- Default gateway: **P3C**
- DCP
 - is disabled for ports **P1** and **P2**.
 - is enabled for port **P3C** (reading and writing is possible in **Setup** DCP mode. You can find detailed information on DCP mode in the following section: Displaying the IP configuration (Page 47)).

When using the function extender interface (connecting to a SCALANCE switch), the following default settings apply:

- IP address and subnet mask
 - DHCP is enabled for FEI port **EXTENDER1**.
 - FEI ports **EXTENDER2** and **EXTENDER3** are completely disabled.
- DCP
 - is enabled for FEI port **EXTENDER1** (reading and writing is possible in **Setup** DCP mode. You can find detailed information on DCP mode in the following section: Displaying the IP configuration (Page 47)).
 - is disabled for FEI ports **EXTENDER2** and **EXTENDER3**.

Note

For the IP configuration, use only the commands described in this section. Other commands, e.g. **ip**, may lead to errors in the network configuration of SCALANCE LPE.

7.9.1 Displaying the ipconfig parameters

To display information about the ipconfig program, execute the following command:

```
ipconfig -h
```

or

```
ipconfig --help
```

Example

```
admin@lpe9403-VPM7001325:~$ ipconfig -h
IP configuration tool for SCALANCE LPE9403. Usage:
SYNOPSIS
```

```
ipconfig [-i {P1|P2|P3C}]
          [-c {<IP>/<Prefix>|dhcp|dhcp_h|dhcp_c}]
          [{-g <IP>|-G|-D}] [-d {ro|rw|off}]
          [-n {<IP1>[,<IP2>]|remove}]
ipconfig -i {P1|P2|P3C} -c down
ipconfig -s|-r [-i {P1|P2|P3C}]
```

OPTIONS

```
-h, --help
```

```

        Display this help message.
-i {P1|P2|P3C}, --interface={P1|P2|P3C}
        Configurable interfaces of the device.
-c {<IP>/<Prefix>|dhcp|dhcp_c|dhcp_h|down},
--config={<IP>/<Prefix>|dhcp|dhcp_c|dhcp_h|down}
        Configuration modes.
-g <IP>, --gw=<IP>
        IP address of static default gateway.
-D, --gw-dhcp
        Use default gateway address from DHCP.
-G, --no-gw
        Remove static gateway or refuse gateway by DHCP server.
-d {rs|ro|rw|off}, --dcp={ro|rw|off}
        Configurable DCP modes.
-n {<IP1>[,<IP2>]|remove},
--dns={<IP1>[,<IP2>]|remove}
        Set up to two or remove DNS address(es) for static
        configuration.
-s, --show
        Show interface information for all interfaces, or for
        a specified -i <interface>
-r, --reset
        Reset interface settings for all interfaces, or for
        a specified -i <interface>

```

7.9.2 Displaying the IP configuration

To display the IP configuration for all ports, execute the following command:

```
ipconfig -s
```

or

```
ipconfig --show
```

To display the IP configuration for a specific port, execute the following command:

```
ipconfig -i {P1 | P2 | P3C} -s
```

or

```
ipconfig --interface={P1 | P2 | P3C} --show
```

Note

The IP address, subnet mask and gateway information are only displayed when configured via DHCP if a port has an active link.

Example

```

admin@lpe9403-VPM7001325:~$ ipconfig -s
Name=P1
UP
Config=STATIC
DCP_N
IP=192.168.178.92

```

7.9 IP configuration

```
Netmask=255.255.255.0
Gateway=192.168.178.1
MAC=D4:F5:27:42:ED:EA
MTU=1500
Stationname:
-----

Name=P2
DOWN
Config=DHCP
DCP_N
IP=0.0.0.0
Netmask=0.0.0.0
Gateway=0.0.0.0
MAC=D4:F5:27:42:ED:EB
MTU=1500
Mode=MAC
Stationname:
-----

Name=P3C
UP
Config=DHCP
DCP_RW
IP=192.168.178.94
Netmask=255.255.255.0
DEFAULTGW
Gateway=192.168.178.1
MAC=D4:F5:27:42:ED:EC
MTU=1500
Mode=MAC
DNS=192.168.178.1
Stationname=lpe9403-VPM7001325
-----
```

Description

The following information is shown:

Parameter	Description
Name	The port name
[Port status]	<ul style="list-style-type: none">UP The port has an active link.DOWN The port does not have an active link.
Config	<p>Shows how the IP address was assigned and whether the port was disabled:</p> <ul style="list-style-type: none">DHCP, DHCP_C or DHCP_HSTATICDISABLED The port was disabled.

Parameter	Description
[Status DCP]	Shows the DCP status of the port: <ul style="list-style-type: none"> • DCP_RS If the device is in delivery state or was reset to factory settings, write access is possible with DCP. When the default password has been changed, only read access is then possible with DCP (default setting). • DCP_RO Only read access is possible with DCP. • DCP_RW Read and write access is possible with DCP. • DCP_N DCP access to the port is not possible.
IP	The IP address of the port
Netmask	The subnet mask of the port
DEFAULTGW	The port is the default gateway.
Gateway	The IP address of the gateway
Metric	The routing metric of the respective port.
MAC	The MAC address of the interface
MTU	The Maximum Transmission Unit of the port
Mode	Shows how the device is identified during addressing via DHCP: <ul style="list-style-type: none"> • MAC The MAC address of the device. (default setting) • CID The DHCP Unique Identifier (DUID). • Hostname The device name.
In CID mode: CID	The DHCP Unique Identifier (DUID)
In Hostname mode: Hostname	The device name.
DNS	The IP address of the domain name server
Stationname	The device name. No display name is displayed by default for the ports P1 and P2.

7.9.3 Configuring the access rights of DCP

NOTICE

Security risk - Risk of unauthorized access and/or misuse

DCP does not have mechanisms for authentication and encryption and should therefore only be used in secure networks. If the device management can be accessed with the default password (device is in delivery state or has been reset to factory settings), you can change the device configuration with DCP. Otherwise, write access with DCP is not possible by default.

DCP could potentially be used to change the functionality of the device and thus cause the failure of data traffic. Users with malicious intent who are in the same local network segment can change IP parameters and/or the DCP device name without authentication.

Follow these steps to configure DCP for a port:

Step	Instruction	Command
1	Configure DCP. Select one of the following options: <ul style="list-style-type: none"> • ro DCP has only read access rights to the device. Device parameters can be read but cannot be modified. The device does not respond to write DCP commands. This means, for example, that no new parameters can be assigned using an engineering tool. The device itself is visible. • rw DCP has read and write access rights to the device. Device parameters can be both read and modified. • off DCP has no access to the device. 	<pre>sudo ipconfig -i P3C -d {ro rw off} or sudo ipconfig --interface=P3C --dcp={ro rw off}</pre>
2	Check the configuration.	<pre>ipconfig [-i P3C] -s</pre>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig -i P3C -dcp ro
admin@lpe9403-VPM7001325:~$ ipconfig -i P3C -s
Name=P3C
UP
Config=DHCP
DCP_RO
IP=192.168.178.94
Netmask=255.255.255.0
Gateway=192.168.178.1
Metric=0
MAC=D4:F5:27:42:ED:EC
MTU=1500
Stationname=lpe9403-VPM7001325
-----
```

7.9.4 Configuring a static IPv4 address

Proceed as follows to configure a static IPv4 address:

Step	Instruction	Command
1	Configure the static IPv4 address and the sub-net mask.	<pre>sudo ipconfig -i {P1 P2 P3C} -c <IP address>/<Prefix length> or sudo ipconfig --interface={P1 P2 P3C} --config=<IP address>/<Prefix length></pre>
2	Check the configuration.	<code>ipconfig [-i {P1 P2 P3C}] -s</code>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig --interface=P1
--config=192.168.1.92/24
admin@lpe9403-VPM7001325:~$ ipconfig --interface=P1 --show
Name=P1
UP
Config=STATIC
DCP_N
IP=192.168.1.92
Netmask=255.255.255.0
Gateway=0.0.0.0
MAC=D4:F5:27:42:ED:EA
MTU=1500
Stationname=
-----
```

7.9.5 Obtaining an IPv4 address via DHCP

To obtain the IP address via DHCP, follow these steps:

Step	Instruction	Command
1	Configure the port for dynamic address assignment with DHCP. The client is identified via the MAC address of the interface.	<pre>sudo ipconfig -i {P1 P2 P3C} -c dhcp or sudo ipconfig --interface={P1 P2 P3C} --config=dhcp</pre>
2	Check the configuration.	<code>ipconfig [-i {P1 P2 P3C}] -s</code>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig --interface=P1
--config=dhcp
admin@lpe9403-VPM7001325:~$ ipconfig -i P1 -s
Name=P1
```

```
UP
Config=DHCP
DCP_N
IP=192.168.178.92
Netmask=255.255.255.0
Gateway=192.168.178.1
MAC=D4:F5:27:42:ED:EA
MTU=1500
Stationname=
-----
```

7.9.6 Obtaining an IPv4 address for combo port P3C via DHCP

There are two additional options for the P3C port when assigning the IP address:

- The DHCP unique identifier (DUID) is sent to the server for identification of the client.
- The host name is sent to the server for identification of the client.

To obtain the IP address via DHCP, follow these steps:

Step	Instruction	Command
1	Configure the port for dynamic address assignment with DHCP. The following options are available for client identification: <ul style="list-style-type: none">• dhcp The client is identified via the MAC address of the interface.• dhcp_c The client is identified via the DUID.• dhcp_h The client is identified via the device name.	<pre>sudo ipconfig -i P3C -c {dhcp dhcp_c dhcp_h} or sudo ipconfig --interface=P3C --config={dhcp dhcp_c dhcp_h}</pre>
2	Check the configuration.	<pre>ipconfig [-i P3C] -s</pre>

Example 1

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig -i P3C -c dhcp_c
admin@lpe9403-VPM7001325:~$ ipconfig -i P3C -s
Name=P3C
UP
Config=DHCP_C
DCP_RW
IP=192.168.178.94
Netmask=255.255.255.0
Gateway=192.168.178.1
MAC=D4:F5:27:5E:DD:0F
MTU=1500
Mode=CID
CID=00:02:d4:f5:27:5e:dd:0f
Stationname=lpe9403-VPM7001325
-----
```

Example 2

```

admin@lpe9403-VPM7001325:~$ sudo ipconfig -i P3C -c dhcp_h
admin@lpe9403-VPM7001325:~$ ipconfig -i P3C -s
Name=P3C
UP
Config=DHCP_H
DCP_RW
IP=192.168.178.94
Netmask=255.255.255.0
Gateway=192.168.178.1
MAC=D4:F5:27:5E:DD:0F
MTU=1500
Mode=Hostname
Stationname=lpe9403-VPM7001325
-----

```

7.9.7 Disabling an interface

To disable an interface, do the following:

Step	Instruction	Command
1	Disable the interface.	<pre> sudo ipconfig -i {P1 P2 P3C} -c down or sudo ipconfig --interface={P1 P2 P3C} --config=down </pre>
2	Check the configuration.	<pre>ipconfig [-i {P1 P2 P3C}] -s</pre>

Example

```

admin@lpe9403-VPM7001325:~$ sudo ipconfig -i P2 -c down
admin@lpe9403-VPM7001325:~$ ipconfig -i P2 -s
Name=P2
DOWN
Config=DHCP
DCP_N
IP=0.0.0.0
Netmask=0.0.0.0
Gateway=192.168.178.1
Metric=0
MAC=D4:F5:27:42:ED:EC
MTU=1500
Stationname=
DISABLED
-----

```

Note**Timeout during the systemd-networkd-wait-online service**

Depending on the IP configuration, the **systemd-networkd-wait-online** service waits during system start until the timeout has expired to end itself with an error. This behavior is attributable to the fact that there are activated interfaces without a valid IP configuration.

Therefore, disable all interfaces you are not using and that do not have a valid IP configuration. Disabled interfaces are excluded by the **systemd-networkd-wait-online** service.

7.9.8 Configuring the default gateway statically

During static configuration, this IP address is also automatically the address of the default gateway. A gateway can be configured for each port, but only one port can be configured as default gateway.

Proceed as follows to configure a gateway statically:

Step	Instruction	Command
1	Configure a port as gateway.	<pre>sudo ipconfig -i {P1 P2 P3C} -g <IP address gateway> or sudo ipconfig --interface={P1 P2 P3C} --gw=<IP address gateway></pre>
2	Check the configuration.	<pre>ipconfig [-i {P1 P2 P3C}] -s</pre>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig --interface=P1 --
gw=192.168.178.99
admin@lpe9403-VPM7001325:~$ ipconfig --interface=P1 --show
Name=P1
UP
Config=STATIC
DCP_N
IP=192.168.178.92
Netmask=255.255.255.0
DEFAULTGW
Gateway=192.168.178.99
Metric=0
MAC=D4:F5:27:42:ED:EA
MTU=1500
Stationname=
-----
```

7.9.9 Configuring the default gateway dynamically

If the gateway is configured via DHCP, this IP address also automatically becomes the address of the default gateway. A gateway can be configured for each port, but only one port can be configured as default gateway.

To configure the default gateway via DHCP, follow these steps:

Step	Instruction	Command
1	Configure the default gateway with DHCP.	<pre>sudo ipconfig -i {P1 P2 P3C} -D</pre> <p>or</p> <pre>sudo ipconfig --interface={P1 P2 P3C} --gw-dhcp</pre>
2	Check the configuration.	<pre>ipconfig [-i {P1 P2 P3C}] -s</pre>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig -i P3C -D
admin@lpe9403-VPM7001325:~$ ipconfig --interface=P3C --show
Name=P3C
UP
Config=DHCP
DCP_RW
IP=192.168.1.94
Netmask=255.255.255.0
DEFAULTGW
Gateway=192.168.178.1
Metric=0
MAC=D4:F5:27:42:ED:EA
MTU=1500
-----
```

7.9.10 Deleting the configuration of the default gateway

The gateway that is configured as default gateway depends on the metric. When the configuration is deleted for the default gateway, the value for the metric is reset to the default value of the port other than "0".

To delete the configuration of the default gateway, follow these steps:

Step	Instruction	Command
1	Delete the configuration for a default gateway that is either static or was configured with DHCP. To do so, enter the name of the port for which the default gateway is configured.	<pre>sudo ipconfig -i {P1 P2 P3C} -G</pre> <p>or</p> <pre>sudo ipconfig --interface={P1 P2 P3C} --no-gw</pre>
2	Check the configuration.	<pre>ipconfig -s</pre>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig -i P3C -G
admin@lpe9403-VPM7001325:~$ ipconfig -s
Name=P1
UP
Config=STATIC
DCP_N
IP=192.168.178.92
Netmask=255.255.255.0
Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0D
MTU=1500
Stationname=
-----
Name=P2
DOWN
Config=DHCP
DCP_N
IP=0.0.0.0
Netmask=0.0.0.0
Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0E
MTU=1500
Stationname=
-----
Name=P3C
UP
Config=DHCP
DCP_RW
IP=192.168.178.94
Netmask=255.255.255.0
Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0F
MTU=1500
Mode=MAC
DNS=192.168.178.1
Stationname=lpe9403-VPM7001325
-----
```

7.9.11 Configuring IP addresses statically for DNS

To configure IP addresses for the Domain Name Server (DNS), follow these steps:

Step	Instruction	Command
1	Enter up to two IP addresses for the Domain Name Server.	<pre>sudo ipconfig -i {P1 P2 P3C} -n {<IP address 1> [, <IP address 2>]} or sudo ipconfig --interface={P1 P2 P3C} --dns={<IP address 1> [, <IP address 2>]}</pre>
2	Check the configuration.	<pre>ipconfig [-i {P1 P2 P3C}] -s</pre>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig -i P1
-n 192.168.178.80,192.168.178.81
admin@lpe9403-VPM7001325:~$ ipconfig -s
Name=P1
UP
Config=STATIC
DCP_N
IP=192.168.178.30
Netmask=255.255.255.0
Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0D
MTU=1500
DNS=192.168.178.80 192.168.178.81
Stationname=
-----
Name=P2
DOWN
Config=DHCP
DCP_N
IP=0.0.0.0
Netmask=0.0.0.0
Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0E
MTU=1500
Stationname=
-----
Name=P3C
UP
Config=DHCP
DCP_RW
IP=192.168.178.25
Netmask=255.255.255.0
Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0F
MTU=1500
```

```
Mode=MAC
DNS=192.168.178.1
Stationname=lpe9403-VPM7001325
-----
```

7.9.12 Deleting statically configured IP addresses for DNS

To delete IP addresses for the Domain Name Server (DNS), follow these steps:

Step	Instruction	Command
1	Delete the IP address or the IP addresses for the Domain Name Server. IP addresses assigned by DHCP are excluded.	<pre>sudo ipconfig -i {P1 P2 P3C} -n remove or sudo ipconfig --interface={P1 P2 P3C} --dns=remove</pre>
2	Check the configuration.	<pre>ipconfig [-i {P1 P2 P3C}] -s</pre>

```
Example
admin@lpe9403-VPM7001325:~$ sudo ipconfig -i P1 -n remove
admin@lpe9403-VPM7001325:~$ ipconfig -s
Name=P1
UP
Config=STATIC
DCP_N
IP=192.168.178.30
Netmask=255.255.255.0
Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0D
MTU=1500
Stationname=
-----
Name=P2
DOWN
Config=DHCP
DCP_N
IP=0.0.0.0
Netmask=0.0.0.0
Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0E
MTU=1500
Stationname=
-----
Name=P3C
UP
Config=DHCP
DCP_RW
IP=192.168.178.25
Netmask=255.255.255.0
```

```

Gateway=0.0.0.0
MAC=D4:F5:27:5E:DD:0F
MTU=1500
Mode=MAC
DNS=192.168.178.1
Stationname=lpe9403-VPM7001325
-----

```

7.9.13 Resetting the IP configuration

Proceed as follows to reset the IP configuration:

Step	Instruction	Command
1	Reset the IP configuration to the factory settings.	<code>sudo ipconfig -r</code> or <code>sudo ipconfig --reset</code>
2	Check the configuration.	<code>ipconfig [-i {P1 P2 P3C}] -s</code>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ipconfig --reset
```

Note

You need to access the device via the serial interface to be able to enter the `ipconfig --show` command after a reset of the IP configuration.

```

admin@lpe9403-VPM7001325:~$ ipconfig --show
Name=P1
UP
Config=DHCP
DCP_N
IP=0.0.0.0
Netmask=0.0.0.0
Gateway=0.0.0.0
MAC=D4:F5:27:42:ED:EA
MTU=1500
Stationname=
-----
Name=P2
DOWN
Config=DHCP
DCP_N
IP=0.0.0.0
Netmask=0.0.0.0
Gateway=0.0.0.0
MAC=D4:F5:27:42:ED:EB
MTU=1500
Stationname=
-----
Name=P3C

```

```

UP
Config=DHCP
DCP_RS
IP=0.0.0.0
Netmask=0.0.0.0
DEFAULTGW
Gateway=0.0.0.0
MAC=D4:F5:27:42:ED:EC
MTU=1500
Stationname=lpe9403-VPM7001325
-----

```

7.10 Port configuration

This section describes how you configure the port properties.

7.10.1 Enabling the Promiscuous Mode for a port

To enable the Promiscuous Mode for a port, follow these steps:

Step	Instruction	Command
1	Specify for which port you want to activate Promiscuous Mode.	<code>sudo ip link set {P1 P2 P3C} promisc on</code>
2	Verify the configuration. The PROMISC flag is displayed for the port.	<code>ip address</code>

Example

```

admin@lpe9403-VPM7001325:~$ sudo ip link set P1 promisc on
admin@lpe9403-VPM7001325:~$ ip address show dev P1
1: P1: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP>
mtu 1500 qdisc mq state UP group default qlen 1000
link/ether d4:f5:27:5e:dd:0d brd ff:ff:ff:ff:ff:ff
inet 192.168.178.24/24 brd 192.168.178.255 scope global dynamic P1
valid_lft 842368sec preferred_lft 842368sec

```

7.10.2 Disabling the Promiscuous Mode for a port

To disable the Promiscuous Mode for a port, follow these steps:

Step	Instruction	Command
1	Specify for which port you want to deactivate Promiscuous Mode.	<code>sudo ip link set [P1 P2 P3C] promisc off</code>
2	Check the configuration. The PROMISC flag is not displayed for the port.	<code>ip address</code>

Example

```
admin@lpe9403-VPM7001325:~$ sudo ip link set P1 promisc off
admin@lpe9403-VPM7001325:~$ ip address show dev P1
1: P1: <BROADCAST,MULTICAST,UP,LOWER_UP>
mtu 1500 qdisc mq state UP group default qlen 1000
link/ether d4:f5:27:5e:dd:0d brd ff:ff:ff:ff:ff:ff
inet 192.168.178.24/24 brd 192.168.178.255 scope global dynamic P1
valid_lft 842368sec preferred_lft 842368sec
```

7.11 VXLAN configuration

VXLAN (Virtual Extensible LAN) according to RFC 7348 enables the emulation of Layer 2 subnets, where Layer 3 packets (UDP) are used for data transfer. A VXLAN connection requires devices that can take on the function of a Virtual Tunnel Endpoint (VTEP) as end points of this Layer 3 connection. The SCALANCE LPE can be used as VTEP.

8 bytes are defined for the VXLAN header, 24 bits of which for the VXLAN Network Identifier (VNI). This means that more than 16 million VXLANs can be configured. A special advantage of VXLAN is scalability because a limit to a maximum of 4096 VLANs does not apply. UDP port 4789 is intended for VXLAN.

The volume of the data packets increases due to the additional VXLAN header. So that data traffic of the internal network can be routed through the VXLAN tunnel without restrictions, the Maximum Transmission Unit (MTU) of the external interface is set to a sufficiently high value. Data packets that are larger than 1518 bytes, so-called "jumbo frames", have a special meaning. If the network that is connected to the external interface cannot forward jumbo frames, you need to reduce the MTU of the internal network.

The VXLAN configuration is stored in the `/etc/vxlan/config/vxlan.conf` file. The IP address and the port of the VXLAN remote station for each configured VXLAN connection are saved in the `/etc/vxlan/config/vtep<VNI>.conf` file.

A maximum of two internal interfaces and therefore two local networks can be configured for the SCALANCE LPE. One interface is configured as external interface. In the delivery state, a maximum of two VNI and a maximum of 20 VXLAN remote stations can be assigned to the external interface. This limit is defined in the `/etc/vxlan/vxlanLimit` file and can be changed by the user.

SCALANCE LPE takes on the function of a VXLAN gateway. Via the two internal ports, VXLAN packets from up to two internal Layer 2 networks can be sent and received via the external port.

Note**Changing the firewall settings**

When a VXLAN connection is configured, the firewall settings are also changed. After the VXLAN configuration, check whether the firewall settings meet the requirements.

7.11.1 Displaying the VXLAN configuration

To show the VXLAN configuration, execute the following command:

```
vxlan -S
```

or

```
vxlan --show
```

Example

```
admin@lpe9403-VPM7001325:~$ vxlan -S
```

```
--- Current VXLAN configuration ---
```

```
General:
```

```
-> VXLAN Mode: bridge
```

```
-> Config: enabled
```

```
External interface:
```

```
-> Name: P1
```

```
-> Gateway:
```

```
-> DNS:
```

```
-> MTU: 1550
```

```
VNI 7:
```

```
-> Local interface: P2
```

```
-> Local-IP: 192.168.16.29/24
```

```
-> MTU: 1500
```

```
-> External-IP: 192.168.16.28/24
```

```
-> External-Port: 4789
```

```
-> Destination-Port: 4789
```

```
-> Endpoint-IP: 192.168.16.93
```

7.11.2 Configuring a VXLAN connection

To configure a VXLAN connection, run the following command:

```
vxlan -l {P1|P2|P3C} -e {P1|P2|P3C} -v <VNI>
      -p <IP address>/<Prefix> [-u <Port>] [-g <IP address>]
      -r <IP address> [-o <Port>] [-i <IP address>/<Prefix>]
      [-d {<IP address1>[,<IP address2>] | remove}] [-t {1|2}]
```

The meaning of the parameters is as follows:

Parameter	Description	Range of values
-l or --local=	The internal interface. Different interfaces need to be specified for the external and internal interface.	P1, P2, P3C
-e or --extern=	The external interface. Different interfaces need to be specified for the external and internal interface.	P1, P2, P3C

Parameter	Description	Range of values
-v or --vni=	The VXLAN Network Identifier (VNI)	1 ... 16777215
-p or --external-ip=	The IP address of the external interface.	A valid IP address with prefix.
-u or --external-port=	[Optional] The UDP port of the external interface.	4096 ... 65535 Default: 4789
-g or --external-gw=	[Optional if the IP address of the external interface and the IP address of the VXLAN remote station belong to the same subnet, otherwise mandatory.] Designation of the gateway address.	A valid IP address.
-r or --endpoint-ip=	The IP address of the VXLAN remote station (VTEP).	A valid IP address.
-o or --endpoint-port=	[Optional] The UDP port of the VXLAN remote station.	4096 ... 65535 Default: 4789
-i or --local-ip=	[Optional] The IP address of the internal interface. The SCALANCE LPE can be reached in the internal network under this IP address.	A valid IP address with prefix.
-d or --dns=	[Optional] Up to two IP addresses of DNS servers that can be reached via the external interface.	An IP address or two IP addresses separated by commas. The configuration of the DNS server is deleted with the remove parameter.
-t or --mtu=	[Optional] Mode for the maximum packet size.	<ul style="list-style-type: none"> • 1 Maximum packet size of internal interface: 1500 bytes Maximum packet size of external interface: 1550 bytes • 2 Maximum packet size of internal interface: 1450 bytes Maximum packet size of external interface: 1500 bytes

Example

```
admin@lpe9403-VP7001325:~$ sudo vxlan -v 7 -l P2 -i
192.168.16.29/24 -e P1 -p 192.168.16.28/24 -r 192.168.16.93
```

```
[sudo] password for admin: *****
```

```

VXLAN configuration complete!
Start external interface -P1- settings...done
Start external firewall settings...done
Start local interface -P2- settings...done
Start local firewall settings for VNI 7...done
Start VTEP 7 settings...done
Start VTEP firewall settings for VNI 7...done
Start Bridge settings...
done
VXLAN configuration done!

```

```
admin@lpe9403-VPM7001325:~$ vxlan -S
```

```
--- Current VXLAN configuration ---
```

```
General:
```

```

-> VXLAN Mode: bridge
-> Config: enabled

```

```
External interface:
```

```

-> Name: P1
-> Gateway:
-> DNS:
-> MTU: 1550

```

```
VNI 7:
```

```

-> Local interface: P2
-> Local-IP: 192.168.16.29/24
-> MTU: 1500

-> External-IP: 192.168.16.28/24
-> External-Port: 4789

-> Destination-Port: 4789
-> Endpoint-IP: 192.168.16.93

```

7.11.3 Locking the VXLAN configuration

Run the following command to lock VXLAN interfaces for configuration with **ipconfig**:

```
sudo vxlan -E
```

or

```
sudo vxlan --enable
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo vxlan -E
[sudo] password for admin: *****
```

```
admin@lpe9403-VPM7001325:~$ vxlan -S
```

```
--- Current VXLAN configuration ---
```

```
General:
-> VXLAN Mode: bridge
-> Config: enabled

External interface:
-> Name: P1
-> Gateway:
-> DNS:
-> MTU: 1550

VNI 7:
-> Local interface: P2
-> Local-IP: 192.168.16.29/24
-> MTU: 1500

-> External-IP: 192.168.16.28/24
-> External-Port: 4789

-> Destination-Port: 4789
-> Endpoint-IP: 192.168.16.93
```

7.11.4 Unlocking the VXLAN configuration

If a complete VXLAN configuration has been performed, the two VXLAN interfaces are locked for configuration with **ipconfig**. Run the following command to unlock the two VXLAN interfaces for configuration with **ipconfig**:

```
sudo vxlan -X
```

or

```
sudo vxlan --disable
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo vxlan -X
[sudo] password for admin: *****
```

```
admin@lpe9403-VPM7001325:~$ vxlan -S
```

```
--- Current VXLAN configuration ---
```

```
General:
-> VXLAN Mode: bridge
-> Config: disabled

External interface:
-> Name: P1
-> Gateway:
-> DNS:
-> MTU: 1550

VNI 7:
-> Local interface: P2
-> Local-IP: 192.168.16.29/24
```

```

-> MTU: 1500

-> External-IP: 192.168.16.28/24
-> External-Port: 4789

-> Destination-Port: 4789
-> Endpoint-IP: 192.168.16.93

```

7.11.5 Adding the IP address of a VLXAN remote station

Run the following command to add the IP address of an endpoint:
`sudo vxlan -v <VNI> -r <IP address>[,<IP address>, ...]`

or

`sudo vxlan --vni=<VNI> --endpoint-ip=<IP address>[,<IP address>, ...]`

Example

```

admin@lpe9403-VPM7001325:~$ sudo vxlan -v 7 -r 192.168.16.94
[sudo] password for admin: *****

```

```

VXLAN configuration complete!
External interface -P1- settings already set
Start VTEP 7 config settings...done
Start VTEP firewall settings for VNI 7...done
VXLAN configuration done!

```

```

admin@lpe9403-VPP4223510:~$ vxlan -S
--- Current VXLAN configuration ---
General:

```

```

-> VXLAN Mode: bridge
-> Config: enabled

```

External interface:

```

-> Name: P1
-> Gateway
-> DNS:
-> MTU: 1550

```

VNI 7:

```

-> Local interface: P2
-> Local-IP: 192.168.16.29/24
-> MTU: 1500

-> External-IP: 192.168.16.28/24
-> External-Port: 4789

-> Destination-Port: 4789
-> Endpoint-IP: 192.168.16.93
-> Endpoint-IP: 192.168.16.94

```

7.11.6 Deleting the IP address of a VLXAN remote station

Run the following command to delete the IP address of an endpoint:

```
sudo vxlan -D -v <VNI> -r <IP address>[,<IP address>, ...]
```

or

```
sudo vxlan --delete --vni=<VNI> --endpoint-ip=<IP address>[,<IP address>, ...]
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo vxlan -D -v 7 -r 192.168.16.94
[sudo] password for admin: *****
```

Deleted Endpoint-IP 192.168.16.94 of VNI 7

7.11.7 Deleting the configuration of a VTEP

Run the following command to delete the configuration of a VTEP and the virtual bridges between the internal and external interface:

```
sudo vxlan -D -v <VNI>[,<VNI>]
```

or

```
sudo vxlan --delete --vni <VNI>[,<VNI>]
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo vxlan -D -v 7
[sudo] password for admin: *****
```

Interface P2 is currently in use as VXLAN interface

Deleted VTEP files for VNI 7

```
admin@lpe9403-VPM7001325:~$ sudo vxlan -S
```

--- Current VXLAN configuration ---

General:

```
-> VXLAN Mode: bridge
-> Config: enabled
```

External interface:

```
-> Name: P1
-> Gateway:
-> DNS:
-> MTU: 1550
```

No VNI configured

7.11.8 Deleting the VXLAN configuration

Run the following command to delete the entire VXLAN configuration with all VTEPs and virtual bridges:

```
sudo vxlan -D -v all
```

or

```
sudo vxlan --delete --vni all
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo vxlan -D -v all
[sudo] password for admin: *****
```

```
Deleting all settings and configuration files
Reset external interface settings...done
Reset external firewall settings...done
Reset local interface and firewall settings...done
Delete all VTEPs and bridge files...done
Reset VTEP firewall settings...done
```

7.12 Device management

This section describes commands for management of the device, e.g. for updating the firmware and backing up configuration data.

7.12.1 Showing device information

To display information about the device, execute the following command:

```
deviceinfo <Optionen>
```

Option	Description
help	Shows the options of the <code>deviceinfo</code> command with a short description.
all	Shows all information. Information that is displayed with the option <code>"sfp"</code> is exempt.
fw	Shows all information about the operating system.
fw-name	Shows the name of the operating system.
fw-version	Shows the version of the operating system.
rescue	Shows all information about the Rescue system.
rescue-name	Shows the name of the Rescue system.
rescue-version	Shows the version of the Rescue system.
uboot	Shows the version of the "U-Boot" bootloader.
hw-info	Shows all hardware information.
mlfb	Shows the order number of the device.
sn	Shows the serial number of the device.
hwr	Shows the hardware revision.

Option	Description
dcp	Displays the DCP information of the device.
dcp-name	Displays the DCP name of the device.
dcp-id	Shows the DCP ID of the device.
pld	Shows the PLD version of the device.
temp	Displays the device temperature in degrees Celsius.
power	<p>Shows the power supply of the SCALANCE LPE:</p> <ul style="list-style-type: none"> • 0x01 Power supply L1 • 0x02 Power supply L2 • 0x03 Redundant power supply via L1 and L2 <p>If the SCALANCE LPE is connected to a SCALANCE switch via the function extender interface, the power supply can be provided exclusively via the SCALANCE switch:</p> <ul style="list-style-type: none"> • 0x04 Power supply L1 of the SCALANCE switch • 0x08 Power supply L2 of the SCALANCE switch • 0x0c Redundant power supply via L1 and L2 of the SCALANCE switch
mac [P1 P2 P3C] When using the function extender interface: mac [EXTENDER1 EXTENDER2 EXTENDER3]	Shows the MAC addresses of the ports. If a port designation is entered, only the MAC address of this port is specified.
secureboot	<p>Shows the status of the Secure Boot function:</p> <ul style="list-style-type: none"> • 00 Secure Boot is inactive, either due to an error or because the affected device with hardware release 1 does not support the Secure Boot function. • 01 Secure Boot is enabled.
sfp	Displays the SFP information of the device.
clean-cache	Deletes the cache

Example

```
admin@lpe9403-VPM7001325:~$ deviceinfo all
```

```
Firmware
```

```
BUG_REPORT_URL = https://support.industry.siemens.com/cs/sc/4868/technical-support?lc=en-WW
```

```
HOME_URL = www.siemens.de/lpe
```

```
ID = debian
```

```
NAME = SCALANCE LPE9403
```

```
PRETTY_NAME = SCALANCE LPE9403 V03.00.00.00_00.00.44
```

```
SUPPORT_URL = https://support.industry.siemens.com/cs/ww/en/ps/
6GK5998-3GS00-2AC2
VARIANT = AuDis LPE image
VERSION = V03.00.00.00_00.00.44
Rescue System:
BUG_REPORT_URL = https://support.industry.siemens.com/cs/sc/4868/
technical-support?lc=en-WW
HOME_URL = www.siemens.de/lpe
ID = debian
NAME = SCALANCE LPE9403
PRETTY_NAME = SCALANCE LPE9403 V03.00.00.00_00.00.44
SUPPORT_URL = https://support.industry.siemens.com/cs/ww/en/ps/
6GK5998-3GS00-2AC2
VARIANT = Rescue Base Image
VERSION = V03.00.00.00_00.00.44
U-Boot:
Version = V03.00.00.00_00.00.44
Hardware Info
MLFB = 6GK5 998-3GS00-2AC2
S/N = VPM7001325
HWR = 02
DCP
Name = SCALANCE LPE
ID = 002a0a0e
Role = IO-Device
System Name =
System Location =
System Contact =
PLD
Version = V0.00.00.009
CPU temperature
°C = 36
Power Supply
= L1 LPE
MAC
P1 = d4:f5:27:b6:c8:2f
P2 = d4:f5:27:b6:c8:30
P3C = d4:f5:27:b6:c8:31
SecureBoot State
active
```

7.12.2 Overlay file system

Unlike the standard version of the Debian operating system, the SCALANCE LPE uses an Overlay file system for the **/etc** directory. All configuration files in the **/etc** directory are saved separately by the operating system and are automatically mounted to the directory tree of the operating system at system start. The use of the Overlay file system for **/etc** has the following effects:

Configuration files that were adapted by the user are not changed during a firmware update. The files are located in an **/etc** directory outside the memory area that is overwritten during a firmware update.

7.12.3 Replacing the server certificate of the device

In the delivery state, the SCALANCE LPE has a server certificate that is used by the HTTP server of the device. The use of a custom certificate that must meet the following requirements is strongly recommended:

- **File name**
The certificate file must have the name **server_certificate_custom.pem**.
- **Directory**
The custom certificate must be saved in the **/etc/ssl/certs/edgebox_web_app/https** directory.
- **Contents and file format**
The certificate file must contain the private key and the certificate and must be in **PEM format**.
- **Key length**
The recommended minimum key length depends on the encryption algorithm used:
 - **RSA algorithm: 4096 bits**
 - **ECDSA algorithm: 256 bits**

To get a digital certificate from a Certificate Authority (CA), you need to address a corresponding request called a **Certificate Signing Request (CSR)** to the Certificate Authority. The request must contain some information about your own organization or company in addition to the public key.

Optionally, you can use certificates that are already present in your organization. For example, there is a menu item for creating certificates in SINEMA Remote Connect Server. OpenSSL also offers the possibility to create a certificate without involvement of a CA.

SINEMA Remote Connect certificates

For detailed information on this topic, refer to the section **Configuring with Web Based Management » Security » CA certificate** in the operating instructions SINEMA Remote Connect Server (<https://support.industry.siemens.com/cs/document/109826712>).

To create a certificate with SINEMA Remote Connect Server, follow the steps below:

1. In SINEMA Remote Connect Server, navigate to **Security » CA certificate** tab.
2. Define the validity date in the **Settings** tab.
3. Click the **Export CA certificate** button. The file is exported to the node or the destination server.
4. The name of the certificate was automatically assigned by SINEMA Remote Connect Server. Change the file name to **certificate_custom.pem**.
5. Move the certificate file into the **/etc/ssl/certs/edgebox_web_app/https** directory.

7.12.3.1 Creating a CSR with OpenSSL

Follow these steps to create a Certificate Signing Request with OpenSSL:

Step	Instruction	Command
1	Create a Certificate Signing Request. Two files result: <ul style="list-style-type: none"> • <key name>.key The file with the public key. • <CSR name>.csr The file for the CSR. 	openssl req -new -newkey <rsa ecDSA>:<key length> -nodes -keyout <key name>.key -out <CSR name>.csr -subj "/C=<country code> /ST=<country> /L=<location> /O=<organization name> /OU=<department name> /CN=<domain name>"
2	Check the Certificate Signing Request.	openssl req -text -in <CSR- Name>.csr -verify

Example

(The terminal output is shown shortened in the example.)

```
admin@lpe9403-VPM7001325:~$ sudo openssl req -new -newkey rsa:4096
-nodes -keyout LPE.key -out LPE.csr -subj
"/C=DE/ST=Germany/L=Karlsruhe/O=MyCompany/OU=R&D/
CN=SCALANCE_LPE-9000"
[sudo] password for admin: *****
.....+.....+.....+.....+.....+.....+.....+.....+.....+
+++++++*..+..+...+...+...+...+...+...+...+...+...+...+
+++++++*
.
.
.
.....+...+.....+...+.....+.....+.....+.....+.....+
+++++++
-----
admin@lpe9403-VPM7001325:~$ openssl req -text -in LPE.csr -verify
Certificate request self-signature verify OK
Certificate Request:
  Data:
    Version: 1 (0x0)
    Subject: C = DE, ST = Germany, L = Karlsruhe, O = MyCompany,
    OU = R&D, CN = SCALANCE_LPE-9000
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
        00:c0:9f:04:3a:76:e7:b2:ec:e5:fe:24:b6:e5:b5:
        51:2a:4a:c1:99:68:76:8b:16:17:38:f1:77:f3:fc:
        .
        .
        .
        30:06:be:54:78:40:f7:96:0d:ce:79:e8:22:52:54:
```

```

53:14:51
Exponent: 65537 (0x10001)
Attributes:
(none)
Requested Extensions:
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
16:5a:54:92:65:8d:1f:12:e8:c4:d7:aa:82:72:0f:c3:52:03:
75:99:b8:e1:c6:b0:c7:e1:bf:f8:51:2d:d4:ab:71:99:83:6a:
.
.
.
7c:2d:0f:d3:ff:8b:e4:e3:12:cc:f4:3e:44:dd:ad:9e:d9:83:
ad:40:d6:b8:38:8c:5e:e1
-----BEGIN CERTIFICATE REQUEST-----
MIIEtjCCAp4CAQAwTELMAkGA1UEBhMCREUxEDAOBgNVBAgMB0dlcm1hbnkxEjAQ
BgNVBACMCUthcmxzcnVoZTESMBAGA1UECgwJTXlDb21wYW55MQwwCgYDVQQQLDANS
.
.
.
EEuQxzARCaIgLqLw1f4kza0aF/t7HnnXeqh6Y9rbQVt8LQ/T/4vk4xLM9D5E3a2e
2YotQNa4OIxe4Q==
-----END CERTIFICATE REQUEST-----

```

7.12.3.2 Creating a certificate with OpenSSL

Follow these steps to create a certificate without the involvement of a Certificate Authority:

Step	Instruction	Command
1	Create a certificate.	openssl req -newkey rsa:4096 -nodes -x509 -days 365 -keyout server_certificate_custom.pem -out server_certificate_custom.pem
2	Check the certificate.	sudo openssl x509 -text -in server_certificate_custom.pem -noout

Example

(The terminal output is shown shortened in the example.)

```

admin@lpe9403-VP7001325:~$ sudo openssl req -newkey rsa:4096 -nodes
-x509 -days 365 -keyout server_certificate_custom.pem -out
server_certificate_custom.pem
[sudo] password for admin: *****
..+.....+.+.+++++
+++++*..+++++
+++++*.....+.
.
.
.
+++++

```

```

-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Germany
Locality Name (eg, city) []:Karlsruhe
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:R&D
Common Name (e.g. server FQDN or YOUR name) []:SCALANCE_LPE-9000
Email Address []:mymail@xyz.de
admin@lpe9403-VPM7001325:~$ sudo openssl x509 -text -in
server_certificate_custom.pem -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:

0d:e5:a5:eb:34:31:a8:23:a6:8c:e2:6a:b5:d0:0f:8c:d1:8b:e8:9d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = DE, ST = Germany, L = Karlsruhe, O = MyCompany,
                OU = R&D, CN = SCALANCE_LPE-9000,
                emailAddress = mymail@xyz.de
        Validity
            Not Before: Aug 10 06:38:40 2024 GMT
            Not After : Aug 10 06:38:40 2025 GMT
        Subject: C = DE, ST = Germany, L = Karlsruhe, O = MyCompany,
                OU = R&D, CN = SCALANCE_LPE-9000,
                emailAddress = mymail@xyz.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
            Modulus:
                00:a1:09:3d:a2:5c:fe:d9:29:32:8b:96:a9:54:cd:
                55:c5:38:44:b7:f9:61:4f:e1:59:9b:3e:5b:4e:25:
                .
                .
                .
                79:6d:07:96:86:d2:76:b2:f3:b3:dd:4e:e9:eb:b9:
                f3:14:9d
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:

82:40:93:77:DB:38:54:C1:C8:5E:81:C9:1D:3E:FD:FA:12:E1:05:F4
            X509v3 Authority Key Identifier:

```

```

82:40:93:77:DB:38:54:C1:C8:5E:81:C9:1D:3E:FD:FA:12:E1:05:F4
      X509v3 Basic Constraints: critical
      CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
      20:07:84:b6:2c:23:0b:eb:f1:95:f4:18:0d:d8:47:39:56:2e:
      bd:88:2a:19:cc:57:ad:8f:e8:e9:72:08:c4:c2:0a:1a:23:f9:
      .
      .
      .
      c9:ca:9f:81:1b:8f:0a:ad:e7:87:14:55:e9:54:f9:ad:83:f6:
      4f:32:b6:c5:dc:e2:63:fa

```

7.12.4 Firmware update

The SCALANCE LPE operating system firmware consists of three components:

- **Bootloader**
U-Boot (Universal Boot Loader) is a bootloader that is especially suitable for Embedded Systems. No interaction with the bootloader is required on the part of the user.
- **Rescue system**
A Rescue system has all necessary components of an operating system to start a device independently of the firmware. The Rescue system is used to enabled access to a non-functional device or to reset the device to the delivery state.
- **Firmware**
The firmware contains the operating system based on Debian GNU/Linux with specific adjustments and additions for the SCALANCE LPE. This operating system is started automatically during a regular start of SCALANCE LPE.

The following two packages are offered to update SCALANCE LPE. The placeholder **XX.XX.XX** stands for the version number of the software, e.g. in the following form:

- **scalance-lpe-VXX.XX.XX_Firmware_with_Bootloader.swu**
The U-Boot bootloader and the SCALANCE LPE firmware
- **scalance-lpe-VXX.XX.XX_rescue.swu**
The Rescue system for the SCALANCE LPE

The files are supplied in SWU format and updated with the SWUpdate program. This combination offers the possibility to check the authenticity, integrity and compatibility of the files to be installed. This provides the advantage that the user can perform a secure update with low workload. Update files can contain software packages or components of the firmware.

The procedure for updating the two SWU files is identical. Hereinafter, the symbolic name **lpe.swu** is used in place of the specific file name.

7.12.4.1 Checking the hash value of a firmware file

To manually check the hash value of a file contained in the firmware folder, follow these steps:

Step	Instruction	Command
1	Transfer the firmware file onto the SCALANCE LPE, for example with the SSH client scp or with a USB flash drive.	-
2	In the Linux shell of the SCALANCE LPE, change to the directory with the firmware file.	cd <directory name>
3	Extract the firmware file with cpio .	cpio -i < <file name>
4	The sw-description file contains the metadata of the firmware file. Output the lines with the file name and the associated hash value.	grep '<file name>' -A 1 -m 1 sw-description
5	Determine the hash value of the file.	openssl sha256 <file name>
6	Check whether the calculated value matches the corresponding value in the sw-description file.	-

Example

The **rescue.efi.zst** file in the **/home/admin** directory is to be checked.

```
admin@lpe9403-VPM7001325:~$ cpio -i < lpe.swu

admin@lpe9403-VPM7001325:~$ grep 'rescue.efi.zst' -A 1 -m 1
                        sw-description
"filename": "rescue.efi.zst",
"sha256":
"36305638742a06aca0a40a3653819048e14fc05e7b2d2e150db42888c0a7e256",

admin@lpe9403-VPM7001325:~$ openssl sha256 rescue.efi.zst
SHA256(rescue.efi.zst)=
36305638742a06aca0a40a3653819048e14fc05e7b2d2e150db42888c0a7e256
```

7.12.4.2 Checking the signature of a firmware file

Follow these steps to check the signature of a firmware file:

Step	Instruction	Command
1	Transfer the firmware file onto the SCALANCE LPE, for example with the SSH client scp or with a USB flash drive.	-
2	In the Linux shell of the SCALANCE LPE, change to the directory with the firmware file.	cd <directory name>
3	Extract the firmware file with cpio .	cpio -i < <file name>
4	Copy the sw-description and sw-description.sig files into the directory in which the certificate is saved, for example /etc/swupdate .	cp sw-description sw-description.sig /etc/swupdate

Step	Instruction	Command
5	Go to the /etc/swupdate directory.	<code>cd /etc/swupdate</code>
6	Check the signature. If the files to be checked have a valid signature, the Verification successful message is displayed. Otherwise, Verification failure is displayed.	<code>openssl cms -verify -CAfile ca-chain.cert.pem -inform DER -in sw-description.sig -content sw-description -purpose any -binary</code>

Example

```
admin@lpe9403-VPM7001325:~$ cpio -i < lpe.swu

admin@lpe9403-VPM7001325:~$ cp sw-description sw-description.sig
                             /etc/swupdate

admin@lpe9403-VPM7001325:~$ cd /etc/swupdate

admin@lpe9403-VPM7001325:/etc/swupdate$ openssl cms -verify -CAfile
ca-chain.cert.pem -inform DER -in sw-description.sig
-content sw-description -purpose any -binary
Verification successful
```

7.12.4.3 Loading a firmware file via the USB interface**Note****Updating devices with hardware release 1**

Devices with hardware release 1 cannot check all components involved in the boot process for integrity and therefore do not support the Secure Boot function.

The firmware as of version 3.0 supports Secure Boot. To install firmware of the version 3.0 on a device with hardware release 1, the following special characteristics need to be taken into consideration:

- The device has firmware, a bootloader and a Rescue system with version 2.1.
- The update must be performed via the Rescue system.
- A specific update package that is provided for this special case is used.

During this update, all data (configuration data, applications and user data) on the SCALANCE LPE is deleted.

A backup of the configuration files for devices with firmware version 2.1 cannot be used for a device with firmware version 3.0.

When the firmware is updated from version 2.1 to version 3.0, the boot process of the SCALANCE LPE is reconfigured. After this update, it is no longer possible to downgrade to versions $\leq$ V2.1.

In a device with hardware release 1 that was successfully updated to firmware version 3.0, the **deviceinfo** returns the following status information about Secure Boot:

```
SecureBoot State
inactive, hardware-revision 01 not supported
```

Note

You must have administrator rights to update firmware or software.

Requirements

- A USB flash drive contains the firmware file (file name extension **.swu**) in its top-level directory and is connected to the USB interface of the device. The following file systems are supported on the USB flash drive:
 - ext4
 - FAT
- The client PC is connected to SCALANCE LPE via an Ethernet port or the USB console interface.

Loading a firmware file into the device**NOTICE****Observe information on new firmware version**

The improper use of a new firmware can lead to a malfunction or to failure of the device.

When updating to a new firmware version, consider all information to be published for this firmware version. Information on the firmware is available from Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

NOTICE**Danger of damage to property**

If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded. Do not switch off the device during the reboot after loading the firmware. The firmware update is not complete until you are able to log in after the device has restarted. If the power supply is interrupted during the reboot, the device may not be functional any longer. Such a functional disruption can only be remedied with the help of our technical support.

Note**Data loss during a firmware update**

When you perform a firmware update in regular operation as described below, all data that is **not** in the following directories is lost:

- /userdata
- /home
- /etc
- /var/log

After the update, you need to save this data in the corresponding directories again.

Note

Any programs previously installed by the user are lost during a firmware update. You must reinstall these programs after the firmware update.

Note

An image in ISO 9660 format is stored on the SCALANCE LPE including license terms, documentation, and the readme file. After a firmware update, this information no longer applies to the updated firmware on the device.

An ISO image suitable for the firmware is available from the Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

To load a firmware file to the device, follow these steps:

Step	Instruction	Command
1	Create a "usb" directory as mount point for the file system of the USB flash drive.	<code>mkdir usb</code>
2	Mount the file system of the USB flash drive.	<code>sudo mount /dev/sda1 usb</code>
3	Switch to the mounted file system.	<code>cd usb</code>
4	Start the update process.	<code>sudo sfw_manager lpe.swu</code>
5	Only up to firmware version 2.1: After a successful firmware update, you need to restart the SCALANCE LPE.	<code>sudo reboot</code>

Example

```
admin@lpe9403-VPM7001325:~/usb$ sudo sfw_manager lpe.swu
sfw_manager version      v0.7.0
[INFO  21:35:48] /usr/share/lua/5.1/sfw_manager/main.lua:20:
sfw_manager startup complete
[INFO  21:35:48] /usr/share/lua/5.1/sfw_manager/core.lua:38:
Extracting code component to lpe.swu
[INFO  21:35:48] /usr/share/lua/5.1/sfw_manager/core.lua:86:
Starting firmware update
```

7.12.4.4 Loading a firmware file with SSH

NOTICE**Updating devices with hardware release 1**

Devices with hardware release 1 cannot check all components involved in the boot process for integrity and therefore do not support the Secure Boot function.

The firmware as of version 3.0 supports Secure Boot. To install firmware of the version 3.0 on a device with hardware release 1, the following special characteristics need to be taken into consideration:

- The device has a bootloader and a Rescue system with version 2.1.
- The update must be performed via the Rescue system.
- A specific update package that is provided for this special case is used.

During this update, all data (configuration data, applications and user data) on the SCALANCE LPE is deleted.

A backup of the configuration files for devices with firmware version 2.1 cannot be used for a device with firmware version 3.0.

When the firmware is updated from version 2.1 to version 3.0, the boot process of the SCALANCE LPE is also reconfigured. After this update, it is no longer possible to downgrade to versions <= V2.1.

In a device with hardware release 1 that was successfully updated to firmware version 3.0, the **deviceinfo** returns the following status information about Secure Boot:

```
SecureBoot State
  inactive, hardware-revision 01 not supported
```

Note

You must have administrator rights to update firmware or software.

Requirements

- The firmware file (file name extension **.swu**) is on the client PC.
- The client PC is connected to SCALANCE LPE via an Ethernet port.
- There is a client for the Secure Copy protocol on the client PC, e.g. **scp**.
- The SSH server of the SCALANCE LPE is active.

Loading a firmware file into the device

NOTICE**Observe information on new firmware version**

The improper use of a new firmware can lead to a malfunction or to failure of the device.

When updating to a new firmware version, consider all information to be published for this firmware version. Information on the firmware is available from Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

NOTICE**Danger of damage to property**

If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded. Do not switch off the device during the reboot after loading the firmware. The firmware update is not complete until you are able to log in after the device has restarted. If the power supply is interrupted during the reboot, the device may not be functional any longer. Such a functional disruption can only be remedied with the help of our technical support.

Note**Data loss during a firmware update**

When you perform a firmware update in regular operation as described below, all data that is **not** in the following directories is lost:

- /userdata
- /home
- /etc
- /var/log

After the update, you need to save this data in the corresponding directories again.

Note

Any programs previously installed by the user are lost during a firmware update. You must reinstall these programs after the firmware update.

Note

An image in ISO 9660 format is stored on the SCALANCE LPE including license terms, documentation, and the readme file. After a firmware update, this information no longer applies to the updated firmware on the device.

An ISO image suitable for the firmware is available from the Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

To load a firmware file to the device, follow these steps:

Step	Instruction	Command
1	[Optional] Check whether the SSH server is running. The SSH server is active by default. If the SSH server is active, the following message is output: Active: active (running)	<code>systemctl status ssh.service</code>
2	[Optional] If the SSH server is not active, the following message is output: Active: inactive (dead) Start the SSH Server.	<code>sudo systemctl start ssh.service</code>
3	On the client PC, open a command prompt (Windows) or a console (Unix) and navigate to the directory with the firmware file.	-
4	Transfer the firmware file with the SCP client. If you use scp on a Windows PC, execute the following command.	<code>scp lpe.swu admin@<IP address>:/home/admin</code> or <code>scp lpe.swu admin@<IP address>:~</code>
5	Enter the password for the admin user. The file transfer starts. The file transfer is complete when a status bar indicating "100%" is shown in the command prompt.	*****
6	In the Linux shell of the SCALANCE LPE, change to the directory with the firmware file.	<code>cd /home/admin</code> or <code>cd</code>
7	Start the update process.	<code>sudo sfw_manager lpe.swu</code>
8	Only up to firmware version 2.1: After a successful firmware update, you need to restart the SCALANCE LPE.	<code>sudo reboot</code>

Example

```

scp lpe.swu admin@192.168.1.94:/home/admin
admin@192.168.1.94's password: *****
lpe.swu                | 29932 kB | 855.2 kB/s | ETA: 00:04:05 |
12%

...

lpe.swu                | 239943 kB | 4798.9 kB/s | ETA: 00:00:00 |
100%
```

7.12.5 Configuring the USB interface (Type A)

SCALANCE LPE has a USB interface (type A) on the front of the enclosure. For a device with factory settings, only memory expansions can be connected to this USB interface. After the USB configuration is modified, other USB devices (DVD drive, webcam etc.) can use this interface.

NOTICE

Only memory expansions allowed

The USB interface (Type A) is approved for connection of a storage medium. Any other use of the USB interface (Type A), for example the connection of a USB camera, is at the user's own risk.

If devices other than memory expansions are to be used, they need to be released, e.g. with the **usbauth** program. You can find more information on this program on the usbauth (<https://manpages.debian.org/buster/usbauth/usbauth.1.en.html>) web page.

In the **/etc/usbauth.conf** configuration file, you can define the device classes for which access is possible. To display the content of the **/etc/usbauth.conf** configuration file, execute the following command:

```
cat /etc/usbauth.conf
```

Example

```
admin@lpe9403-VPM7001325:~$ cat /etc/usbauth.conf
deny all
    # deny all by default
allow bDeviceClass==09 bInterfaceClass==09
    # allow USB hubs
allow idVendor==0908 bInterfaceClass==08 busnum==1
    # allow USB storages on the CLP USB 2.0 interface
allow idVendor==0908 bInterfaceClass==08 busnum==2
    # allow USB storages on the CLP USB 3.0 interface
allow bInterfaceClass==08 busnum==3
    # allow USB storages on the front USB 2.0 interface
allow bInterfaceClass==08 busnum==4
    # allow USB storages on the front USB 3.0 interface
```

To release the interface for a webcam, for example, the configuration rules must allow access of devices of the "Video" device class. You can find information on the parameters of the individual device classes on the web page of the USB Implementers Forum (<https://www.usb.org/defined-class-codes>) web page.

Example

The **bInterfaceClass** parameter has the value **0x0E** for the device class "Video". To release the USB interface (Type A) on the front of the housing for a webcam, add the following line in the file **/etc/usbauth.conf**. You can only modify this file if you have Root rights.

```
allow bInterfaceClass==0e busnum==3
```

The **busnum** parameter designates the interface and the USB version. The following assignment applies to the SCALANCE LPE:

Interface	USB version	busnum
USB interface (Type A) on the front of the housing	USB 2.0	3
	USB 3.0	4

When a USB device is connected to the SCALANCE LPE, an entry is written to the log file **/var/log/eventmgr.log**.

Example

The webcam is equipped with a microphone. If the **/etc/usbauth.conf** configuration file was modified as in the previous example, devices of the "Video" device class are allowed. Connection of devices of the "Audio" device class is denied.

```
admin@lpe9403-VPM7001303:~$ tail /var/log/eventmgr.log
2021-05-04 11:15:52,454 usbauth: deny interface
/sys/devices/platform/soc/3000000.usb3/xhci-hcd.1.auto/
usb3/3-1/3-1:1.2/authorized
2021-05-04 11:15:52,455 com.siemens.lpe.eventmgr: deny interface
1.2 of USB device 3-1
2021-05-04 11:15:52,458 usbauth: allow interface
/sys/devices/platform/soc/3000000.usb3/xhci-hcd.1.auto/
usb3/3-1/3-1:1.1/authorized
2021-05-04 11:15:52,459 com.siemens.lpe.eventmgr: allow interface
1.1 of USB device 3-1
2021-05-04 11:15:52,462 usbauth: allow interface
/sys/devices/platform/soc/3000000.usb3/xhci-hcd.1.auto/
usb3/3-1/3-1:1.0/authorized
2021-05-04 11:15:52,462 com.siemens.lpe.eventmgr: allow interface
1.0 of USB device 3-1
2021-05-04 11:15:52,466 usbauth: deny interface
/sys/devices/platform/soc/3000000.usb3/xhci-hcd.1.auto/
usb3/3-1/3-1:1.3/authorized
2021-05-04 11:15:52,466 com.siemens.lpe.eventmgr: deny interface
1.3 of USB device 3-1
```

7.12.6 Resetting the configuration

By resetting the configuration, all the settings you have made are overwritten by factory defaults. The software components you have installed or other changes to the device outside of the **/etc** configuration directory are retained.

To reset the configuration, execute the following command:

```
sudo configreset
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo configreset
[sudo] password for admin: *****
This will delete all your custom settings. Are you sure to proceed?
[Yes|No]
Yes
```

```
This process will force a reboot. Are you sure to proceed? [Yes|No]
Yes
[26404.309443] reboot: Restarting system
```

7.12.7 Resetting the device to factory defaults

A complete reset of all settings to the factory settings (factory reset) is only possible in the Rescue system by overwriting the firmware file. **All** information stored on the device is deleted during the reset.

You can find information on the firmware update in the Rescue system in the SCALANCE LPE9403 Operating Instructions (<https://support.industry.siemens.com/cs/ww/de/ps/26683/man>).

NOTICE

Observe information on new firmware version

The improper use of a new firmware can lead to a malfunction or to failure of the device.

When updating to a new firmware version, consider all information to be published for this firmware version. Information on the firmware is available from Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

7.12.8 Configuring the log file

SCALANCE LPE uses the **eventmgr** service and the associated log file **/var/log/eventmgr.log** for logging the system messages. You change the configuration of **eventmgr** by adapting the **/etc/eventmgr/eventmgr.yml** file.

The default setting is local storage of the system alarms that you configure with the following entry:

```
logfile: "/var/log/eventmgr.log"
```

If the device is to send system alarms to a remote syslog server unencrypted via UDP, the following entry is required:

```
logaddr: ["<host name>.tld", <Port number>]
```

Instead of the host name, you can also enter the IP address.

7.12.9 Encrypted transfer of syslog messages

Encrypted transfer of SCALANCE LPE system messages with TLS (Transport Layer Security) via a TCP connection is also possible. The following parameters must be configured in the **/etc/eventmgr/eventmgr.yml** file for this purpose:

- **enabled**
The **true** value enables encrypted transfer of syslog messages.
- **address**
The IP address of the syslog server.
- **port**
The port of the syslog server.
- **tls_ca**
The directory path and file name of the CA certificate.
- **tls_cert**
The directory path and file name of the client certificate.
- **tls_key**
The directory path and the name of the file with the client key.

Example

Possible content of the **/etc/eventmgr/eventmgr.yml** file:

```
#Configuration for local logfile
logfile: "/var/log/eventmgr.log"

#Configuration for unencrypted Syslog Server (UDP)
logaddr: ["localhost", 514]

#Configuration for encrypted Syslog Server (TCP)
tls:
  enabled: false
  address: ["192.168.137.252", 6514]
  tls_ca: "/home/admin/ca.pem"
  tls_cert: "/home/admin/client-cert.pem"
  tls_key: "/home/admin/client-key.pem"
```

7.12.10 Restarting the device

Note

If the SCALANCE LPE is connected to a SCALANCE switch via the function extender interface, the SCALANCE LPE can be restarted independently of the SCALANCE switch. The SCALANCE LPE can also be restarted in the WBM of the SCALANCE switch. For more detailed information, refer to Configuration manual of the SCALANCE XCH-300/XCM-300/XRH-300/XRM-300 (<https://support.industry.siemens.com/cs/document/109964110>).

When the SCALANCE switch restarts, the SCALANCE LPE also restarts.

Run one of the following commands to restart the device:

- `sudo reboot`
- `systemctl reboot`

7.12.11 Shutting down the device

Run one of the following commands to shut down the device. The device will then restart automatically.

- `sudo halt`
- `sudo poweroff`
- `sudo shutdown`
- `systemctl halt`
- `systemctl poweroff`

7.13 Backup file

Note

You can only create, load, restore, and delete backup files with administrator rights.

A backup file contains all changes made by the user to the configuration files in the `/etc` directory.

7.13.1 Showing the existing backup files

To display the backup files, execute the following command:
`backupmanager list`

Example

```
admin@lpe9403-VPM7001325:~$ backupmanager list
20200916115707_v01.00.00.00_lpe9403-VPM7001325_auto
20200701115319_v01.00.00.00_lpe9403-VPM7001325_manual
20200701114454_v01.00.00.00_lpe9403-VPM7001325_manual
```

Description

A list of the backup files is displayed. The file name contains the following items of information, separated by underscores:

- Time stamp of creation
- Firmware version
- Device name
- Type of creation

The **.tar.gz** or **.tar.gz.gpg** file type is not displayed in this list.

The backup files are saved in the **/userdata/backup** directory.

7.13.2 Creating a backup file

Note

The backup of the configuration files can only be used for devices that have the same firmware version as the device with which the backup was created.

To create a backup file, follow these steps:

Step	Instruction	Command
1	Create a backup of the configuration files in the directory /etc .	<code>sudo backupmanager create</code>
2	Check the result.	<code>backupmanager list</code>

Example

```
admin@lpe9403-VPM7001325:~$ sudo backupmanager create
Backup successfully created!
admin@lpe9403-VPM7001325:~$ backupmanager list
20200701115319_v01.00.00.00_lpe9403-VPM7001325_manual
20200701114454_v01.00.00.00_lpe9403-VPM7001325_manual
```

7.13.3 Creating an encrypted backup file

To create an encrypted backup file, do the following:

Step	Instruction	Command
1	Create a backup of the configuration files in the directory <i>/etc</i> .	<code>sudo backupmanager -p create</code> or <code>sudo backupmanager --password create</code>
2	Enter the password to encrypt the backup file. To finish entering the password or cancel the process, select the field <OK> or <Cancel> with the tab key.	*****
3	Confirm the password by entering it again.	*****
4	Check the result.	<code>backupmanager list</code>

Example

```
admin@lpe9403-VPM7001325:~$ sudo backupmanager -p create
```

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Enter passphrase x
x x x
x x x
x Passphrase: ***** x
x x x
x <OK> <Cancel> x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Please re-enter this passphrase x
x x x
x Passphrase: ***** x
x x x
x <OK> <Cancel> x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

```
Backup successfully created!
admin@lpe9403-VPM7001325:~$ backupmanager list
20200701115319_V01.00.00.00_lpe9403-VPM7001325_manual
20200701114454_V01.00.00.00_lpe9403-VPM7001325_manual
```

7.13.4 Restoring a backup file

Note

The backup of the configuration files can only be used for devices that have the same firmware version as the device with which the backup was created.

To restore the backup file of the configuration, execute the following command:

```
sudo backupmanager -f <File name> restore
```

or

```
sudo backupmanager --filename <File name> restore
```

Enter which backup file should be restored. You do not need to specify the file extension ".tar.gz". After the configuration files are restored successfully, a restart is performed automatically.

Example

```
admin@lpe9403-VPM7001325:~$ sudo backupmanager -f
20200701115319_V01.00.00.00_lpe9403-VPM7001325_manual restore
This will delete all your custom settings. Are you sure to proceed?
[yes|no]
yes
This process will force a reboot. Are you sure to proceed? [yes|no]
yes
Start restoring 20200701115319_V01.00.00.00_lpe9403-
VPM7001325_manual.tar.gz
Restore backup done!
Reboot
```

7.13.5 Restoring an encrypted backup file

Follow these steps to restore an encrypted backup file of the configuration:

Step	Instruction	Command
1	Enter which backup file should be restored. You do not need to specify the file extension ".tar.gz.gpg".	<pre>sudo backupmanager -f <File name> restore</pre> <p>or</p> <pre>sudo backupmanager --filename <File name> restore</pre>
2	Confirm the prompt to delete the user-specific settings.	yes
3	Confirm the prompt to restart the device.	yes
4	Enter the password to encrypt the backup file. To finish entering the password or cancel the process, select the field <OK> or <Cancel> with the tab key. After the configuration files are restored successfully, a restart is performed automatically.	*****

Example

```
admin@lpe9403-VPM7001325:~$ sudo backupmanager -f
20210506140635_V01.01.00.00_00.00.33_lpe9403-VPM7001325_manual
restore
This will delete all your custom settings. Are you sure to proceed?
[yes|no]
yes
This process will force a reboot. Are you sure to proceed? [yes|no]
yes
```

7.13.6 Deleting a backup file

Step	Instruction	Command
1	Enter which backup file should be deleted. You do not need to specify the file extension ".tar.gz" or ".tar.gz.gpg".	<pre>sudo backupmanager -f <File name> delete</pre> <p>or</p> <pre>sudo backupmanager --filename <File name> delete</pre>
2	Check the result.	<pre>backupmanager list</pre>

```
admin@lpe9403-VPM7001325:~$ sudo backupmanager -f
20200701114454_v01.00.00.00_lpe9403-VPM7001325_manual delete
[sudo] password for admin: *****
This will delete the backup 20200701114454_v01.00.00.00_lpe9403-
VPM7001325_manual.
Are you sure to proceed? [yes|no]
yes
Delete 20200701114454_v01.00.00.00_lpe9403-VPM7001325_manual.tar.gz
admin@lpe9403-VPM7001325:~$ backupmanager list
20200701115319_v01.00.00.00_lpe9403-VPM7001325_manual
```

SCALANCE LPE uses **firewalld** as the firewall. This program is installed in the factory state and enabled by default. **firewalld** uses the functionality of **nftables**, a program for filtering data

packets. **firewalld** and **nftables** cannot, however, be used simultaneously and independently of each other.

The installation package already includes several pre-defined zones that cover some standard packet processing cases. For example, if you want to block incoming data traffic, the corresponding interface must be included in the **block** zone.

This section describes basic commands to view and modify information about the configuration of **firewalld**. The **firewalld** configuration files are located in the **/usr/lib/firewalld/zones** directory.

You can find more information about the commands and how to configure the firewall on the homepage of **firewalld** (<https://firewalld.org/documentation/man-pages/firewall-cmd.html>).

7.14.1 Querying the status of firewalld

Query with firewall-cmd

To view the status of **firewalld** using the **firewall-cmd** command line tool, execute the following command:

```
sudo firewall-cmd --state
```

The following states are possible for the firewall:

- **running**
The firewall daemon is running without errors.
- **not running**
The firewall daemon is not running.
- **failed**
The firewall daemon is running, but an error occurred at startup.

Example

```
admin@lpe9403-VPM7001325:~$ sudo firewall-cmd --state
running
```

Query with systemctl

To view the status of **firewalld** using the **systemctl** command line tool, execute the following command:

```
sudo systemctl status firewalld
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo systemctl status firewalld
• firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/lib/systemd/system/firewalld.service; enabled;
         vendor preset: enabled)
  Active: active (running) since Thu 2022-03-03 07:43:14 UTC;
         7h 36min ago
  Docs: man:firewalld(1)
  Main PID: 334 (firewalld)
  Tasks: 2 (limit: 4459)
```

```
Memory: 41.9M
CPU: 5.148s
CGroup: /system.slice/firewalld.service
└─334 /usr/bin/python3 /usr/sbin/firewalld
      --nofork --nopic
```

7.14.2 Displaying the firewall zones

To display the zones of the firewall, execute the following command:
`sudo firewall-cmd --get-zones`

Example

```
admin@lpe9403-VPM7001325:~$ sudo firewall-cmd --get-zones
block dmz docker drop external home internal public trusted work
```

For each zone, there is a configuration file in XML format in the `/usr/lib/firewalld/zones` directory. To view the configuration files of the zones, execute the following command:

```
admin@lpe9403-VPM7001325:~$ ls /usr/lib/firewalld/zones
block.xml drop.xml home.xml public.xml work.xml
dmz.xml external.xml internal.xml trusted.xml
```

7.14.3 Displaying the default zone

To display the default zone of the firewall, execute the following command:
`sudo firewall-cmd --get-default-zone`

Example

```
admin@lpe9403-VPM7001325:~$ sudo firewall-cmd --get-default-zone
drop
```

In the delivery state and after a factory reset, the **drop** zone is configured as the default zone. For **drop**, data traffic is restricted to the maximum extent: All received data packets for which there is no exception (HTTP, HTTPS, SSH, SNMP and ICMP Echo) are dropped without further processing.

7.14.4 Displaying the configuration of a zone

To view the configuration of a zone, execute the following command:
`sudo firewall-cmd --zone=<name of zone> --list-all`

Example

```
admin@lpe9403-VPM7001325:~$ sudo firewall-cmd --zone=drop --list-all
drop
target: DROP
icmp-block-inversion: no
interfaces:
sources:
services: http https snmp ssh
```

7.14 Configuring the firewall

```
ports:
protocols:
forward: no
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
```

The most comprehensive restrictions apply to the **drop** zone: Incoming packets are not forwarded (`forward: no`) and only HTTP, HTTPS, SNMP, and SSH protocols are allowed (`services: http https snmp ssh`).

7.14.5 Displaying the services of a zone

To view the services that are allowed in a firewall zone, execute the following command:

```
sudo firewall-cmd --zone=<name of zone> --list-services
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo firewall-cmd --zone=drop --list-
services
http https snmp ssh
```

For each service, there is a configuration file in XML format in the `/usr/lib/firewalld/services` directory, such as `http.xml`, `https.xml`, `snmp.xml` and `ssh.xml`.

7.14.6 Displaying the ports of a zone

By ports, in the context of this command, we do not mean the physical interfaces of the device. The port in this case is a number between 0 and 65536 and identifies a service that is accessible through the corresponding IP address. By default, all ports are blocked by the firewall. To view the ports that are open for a firewall zone, execute the following command:

```
sudo firewall-cmd --zone=<name of zone> --list-ports
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo firewall-cmd --zone=public --list-
ports
53/udp
```

The **public** zone is classified as untrusted. Port 53 as the default port of the "Domain Name System" protocol is open in the example configuration to use the DNS functionality.

7.14.7 Adding a service to a zone

To add a service to a zone, execute the following command:

```
sudo firewall-cmd --zone=<name of zone> --add-service=<name of
service> [--permanent]
```

The optional `--permanent` parameter changes the configuration permanently. The changes will take effect only after the firewall is restarted or the device is rebooted.

Example

The following command adds the HTTP service to the **public** zone. The services of this zone are then displayed.

```
admin@lpe9403-VP7001325:~$ sudo firewall-cmd --zone=public --add-service=http
success
admin@lpe9403-VPN3185785:~$ sudo firewall-cmd --zone=public --list-services
dhcpv6-client http ssh
```

7.14.8 Removing a service from a zone

To remove a service from a zone, execute the following command:

```
sudo firewall-cmd --zone=<name of zone> --remove-service=<name of service> [--permanent]
```

The optional `--permanent` parameter changes the configuration permanently. The changes will take effect only after the firewall is restarted or the device is rebooted.

Example

The following command removes the HTTP service from the **public** zone. The services of this zone are then displayed.

```
admin@lpe9403-VP7001325:~$ sudo firewall-cmd --zone=public --remove-service=http
success
admin@lpe9403-VPN3185785:~$ sudo firewall-cmd --zone=public --list-services
dhcpv6-client ssh
```

7.14.9 Adding a port to a zone

To add a port to a zone, execute the following command:

```
sudo firewall-cmd --zone=<name of zone> --add-port=<port number>/<protocol> [--permanent]
```

The optional `--permanent` parameter changes the configuration permanently. The changes will take effect only after the firewall is restarted or the device is rebooted.

Example

```
admin@lpe9403-VP7001325:~$ sudo firewall-cmd --zone=public --add-port=53/udp
success
```

The ports that are assigned to each service is specified in the **/etc/services** file. To display the lines for the SMTP protocol from the **/etc/services** file, execute the following command:

```
admin@lpe9403-VPM7001325:~$ grep smtp /etc/services
smtp 25/tcp mail
submissions 465/tcp ssmtp smtps urd # Submission over TLS [RFC8314]
```

7.14.10 Removing a port from a zone

To remove a port from a zone, execute the following command:

```
sudo firewall-cmd --zone=<name of zone> --remove-port=<port
number>/<protocol> [--permanent]
```

The optional `--permanent` parameter changes the configuration permanently. The changes will take effect only after the firewall is restarted or the device is rebooted.

Example

```
admin@lpe9403-VPM7001325:~$ sudo firewall-cmd --zone=public --
remove-port=53/udp
success
```

7.15 System time

SCALANCE LPE supports time synchronization according to the NTP and Secure NTP standards. This section describes how to configure one or more time servers with which SCALANCE LPE is synchronized. If the device is not to synchronize its system time with an external server, you can disable NTP. You can also configure the system time manually independent of a time server.

SCALANCE LPE has a separate hardware clock, the function of which can be maintained by a capacity in the device for several hours after the power supply has been interrupted. During this period, the system time from the hardware clock is applied when the device is started until a time server can be reached. The system time of the hardware clock is used while time synchronization is in progress with an available time server.

7.15.1 Requirements for time synchronization with NTP

Access to an NTP server

Time synchronization with NTP is only possible if the SCALANCE LPE has access to an NTP server. This can be a public NTP server on the Internet or a private NTP server in a network without Internet connection.

Activated NTP daemon

The Network Time Service of the device must be active. This requirement is met in the delivery state or after a reset to factory settings.

If the Network Time Service is not active, start this service with the following command:

```
sudo systemctl restart ntpsec.service
```

7.15.2 Displaying the status of NTP

To verify the status of the NTP service, execute the following command:

```
admin@lpe9403-VPM7001325:~$ systemctl status ntpsec
ntpsec.service - Network Time Service
   Loaded: loaded (/lib/systemd/system/ntpsec.service;
           enabled; vendor preset: enabled)
   Active: active (running) since Wed 2020-08-05 15:29:39 UTC;
           52min ago
     Docs: man:ntpd(8)
  Process: 2896 ExecStart=/usr/lib/ntp/ntp-systemd-wrapper
           (code=exited, status=0/SUCCESS)
 Main PID: 2899 (ntpd)
    Tasks: 1 (limit: 2235)
  Memory: 820.0K
   CGroup: /system.slice/ntpsec.service
           └─2899 /usr/sbin/ntpd -p /run/ntpd.pid
             -c /etc/ntpsec/ntp.conf -g -N -u ntpsec:ntpsec
```

The status of the NTP service is displayed in the `Active` section. The `active (running)` display means that the service is running. The `enabled` display in the `Loaded` section means that the service is started automatically.

7.15.3 Configuring an NTP server

The NTP configuration is stored in the `/etc/ntpsec/ntp.conf` file. Among other things, this file defines which NTP servers the SCALANCE LPE requests. However, the servers are not listed individually in this file with their IP address. The name of one or multiple server pools is listed in the configuration file. The following entries exist in the delivery state:

```
pool 0.siemens.pool.ntp.org iburst
pool 1.siemens.pool.ntp.org iburst
pool 2.siemens.pool.ntp.org iburst
pool 3.siemens.pool.ntp.org iburst
```

Alternatively, you can also specify the IP address of your NTP server. In this case, you must comment out the rows of the server pools.

```
server <IP address | DNS name> iburst
```

The `iburst` option reduces the time until the first synchronization.

Configuration changes only become effective after you have restarted the NTP service.

7.15.4 Restarting NTP

To restart the NTP service, run the following command:

```
sudo systemctl restart ntpsec.service
```

7.15.5 Configuring Secure NTP

If you want to synchronize the time using Secure NTP, you must disable the NTP servers provided by DHCP. If these time servers are active, the Secure NTP server might not be used. The time can be manipulated in this case which impacts network security. To do this, change the option **IGNORE_DHCP** in the **/etc/default/ntpsec** configuration file to **yes**, as shown in the following example.

Example:

```
admin@lpe9403-VP7001325:~$ cat /etc/default/ntpsec
NTPD_OPTS="-g -N"
# Set to "yes" to ignore DHCP servers returned by DHCP.
IGNORE_DHCP="yes"
```

Requirement for the use of Secure NTP is that there are matching keys on the client and the server. This is usually only possible when using your own servers. The configuration information for Secure NTP is saved in the **/etc/ntpsec/ntp.conf** file. The keys have their own file.

The following parameters are configured in **/etc/ntpsec/ntp.conf**:

- **keys**
The file in which the keys are stored.
Example:
`keys /etc/ntpsec/ntp.keys`
- **trustedkey**
The IDs of the keys in the file configured with **keys** that are to be used. The file can contain additional keys.
Example:
`trustedkey 1234 2345 3456`
- **key**
The ID of the key that must be used for a specific server.
Example:
`server <IP address> iburst key <ID of the key>`

The key file has the following structure: There is a separate row for each key; each row must contain three pieces of information.

- **The ID of the key**
A number between 1 and 65535 for identification of the key. The same keys must be stored for a specific ID on the client and server.
- **The encryption algorithm**
The following options are supported:
 - MD5
 - SHA1
 - SHA256
 - SHA512
 - SHA3-256
 - SHA3-512
 - AES-128
 - AES-256
- **The key**
Up to a key length of 20 characters, the string is interpreted as ASCII; with more than 20 characters, it is considered to be hexadecimal.

Example:

```
2345 md5 abcdefghijklmnop
3456 sha1 abcdefghijklmnopqrst
```

The trivial strings used for the keys in the example are for demonstration purposes only and should not be used.

7.15.6 Configuring the system time manually

Follow these steps to configure the system time manually:

Step	Instruction	Command
1	Show information about the system time and the time zone.	<code>timedatectl</code>
2	[Optional] If you want to configure a different time zone, view the names for the time zones.	<code>timedatectl list-timezones</code>
3	[Optional] Configure the suitable time zone.	<code>sudo timedatectl set-timezone <Zeitzone></code>
4	Configure the date and the time. [Optional] Specify only the date or time as parameter. The missing parameter is displayed in this case.	<code>sudo timedatectl set-time <"YYYY-MM-DD hh:mm:ss"></code>
5	Check the configuration.	<code>timedatectl</code>

Example

```

admin@lpe9403-VPM7001325:~$ timedatectl
          Local time: Fri 2024-08-02 06:20:03 EDT
          Universal time: Fri 2024-08-02 10:20:03 UTC
              RTC time: Fri 2024-08-02 10:20:03
          Time zone: America/New_York (EDT, -0400)
System clock synchronized: no
              NTP service: n/a
          RTC in local TZ: no
admin@lpe9403-VPM7001325:~$ timedatectl list-timezones
...
Europe/Belgrade
Europe/Berlin
Europe/Bratislava
...
admin@lpe9403-VPM7001325:~$ sudo timedatectl set-timezone Europe/
                        Berlin
[sudo] password for admin: *****
admin@lpe9403-VPM7001325:~$ timedatectl set-time "2024-08-03 07:40"
admin@lpe9403-VPM7001325:~$ timedatectl
          Local time: Sat 2024-08-03 07:40:02 CEST
          Universal time: Sat 2024-08-03 05:40:02 UTC
              RTC time: Sat 2024-08-03 05:40:02
          Time zone: Europe/Berlin (CEST, +0200)
System clock synchronized: no
              NTP service: n/a
          RTC in local TZ: no

```

7.16 SNMP

SNMP is a UDP-based, open protocol for central configuration, control and administration of network components, such as routers and switches. SNMP also offers diagnostic functions and functions for notifications known as traps.

7.16.1 SNMP on the SCALANCE LPE

The SNMP packet contains numerous command line programs to use SNMP for the network management. SNMP is pre-installed on the SCALANCE LPE when it is shipped from the factory. The SNMP service starts automatically when the device is switched on. Read access is possible with SNMPv2 by default.

Configuration file

If you want to change the SNMP configuration, you must adapt the file **/etc/snmp/snmpd.conf**. A change of this configuration file may be necessary, for example, when you want to expand the area of the read-only OIDs.

7.16.2 Displaying the status of the SNMP service

To verify the status of the SNMP service, execute the following command:

```
admin@lpe9403-VPM7001325:~$ systemctl status snmpd
```

```
• snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled;
           vendor preset: enabled)
   Active: active (running) since Wed 2020-10-07 06:54:55 UTC;
           5h 15min ago
   Process: 379 ExecStartPre=/bin/mkdir -p /var/run/agentx
           (code=exited, status=0/SUCCESS)
  Main PID: 389 (snmpd)
    Tasks: 1 (limit: 2235)
   Memory: 7.3M
   CGroup: /system.slice/snmpd.service
           └─389 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-snmp
               -g Debian-snmp -I -smux mteTrigger mteTriggerConf
               -f -p /run/snmpd.pi
```

7.16.3 Stopping the SNMP service

To stop the SNMP service, follow these steps:

Step	Instruction	Command
1	Stop the SNMP service.	<code>sudo systemctl stop snmpd</code>
2	Check the status.	<code>systemctl status snmpd</code>

7.16.4 Starting the SNMP service

To start the SNMP service, follow these steps:

Step	Instruction	Command
1	Start the SNMP service.	<code>sudo systemctl start snmpd</code>
2	Verify the status.	<code>systemctl status snmpd</code>

7.16.5 Disabling the SNMP service

For reasons of network security, it may be necessary to disable the SNMP service. After disabling the SNMP service, you must restart the device for the change to become effective.

To disable the SNMP service, follow these steps:

Step	Instruction	Command
1	Disable the SNMP service.	<code>sudo systemctl disable snmpd</code>
2	Stop the SNMP service.	<code>sudo systemctl stop snmpd</code>
3	Verify the status.	<code>systemctl status snmpd</code>

7.16.6 Enabling the SNMP service

To enable the SNMP service, follow these steps:

Step	Instruction	Command
1	Enable the SNMP service.	<code>sudo systemctl enable snmpd</code>
2	Restart the SNMP service.	<code>sudo systemctl start snmpd</code>
3	Verify the status.	<code>systemctl status snmpd</code>

7.16.7 Data security with SNMP

Since the first version of SNMP came out in 1988, SNMP has undergone continuous further development. This has primarily involved the data transfer functionality and the implemented security mechanisms.

- **SNMPv1**
SNMPv1 defines multiple message types for querying and modifying data of devices. The sole security feature is the community string, which is transferred unencrypted together with the message. If the community string is correct, the SNMP agent executes the requested action, e.g. the sending of data. If the community string is not correct, the SNMP agent discards the request. SNMPv1 is disabled for SCALANCE LPE by default.
- **SNMPv2**
Version 2 has multiple variants: Version SNMPv2c offers improved functionality for retrieving data but no additional security features. In version SNMPv2p, the community string is encrypted. User names were introduced with version SNMPv2u. With SNMPv2c, only read access is possible for SCALANCE LPE by default. If you change the SNMP configuration, write access for the following items of OID 1.3.6.1.2.1.1, among others, is also possible:
 - **OID 1.3.6.1.2.1.1.4** (sysContact)
 - **OID 1.3.6.1.2.1.1.5** (sysName)
 - **OID 1.3.6.1.2.1.1.6** (sysLocation)The procedure is described in section Changing the access rights for SNMPv2c (Page 103).
- **SNMPv3**
SNMPv3 has a comprehensive security concept with mechanisms for authentication and encryption:
 - Fully encrypted user authentication based on MD5 or SHA.
 - Encryption of all data communication with DES or AES encryption
 - Configuration of users and access rights on MIB objects.

This system, which is called the **User-based Security Model (USM)**, was specified in the RFC 3414 standard in 2002. Numerous other standards have also been established for version 3. For example, the definition of the Management Information Base (MIB) was expanded and updated with RFC 3418.

7.16.8 Changing the access rights for SNMPv2c

Note

You can configure the access rights of SNMPv2c only with administrator rights.

With SNMPv2c, only read access is possible for SCALANCE LPE by default. To configure SNMPv2c for write access as well, follow these steps:

Step	Instruction	Command
1	Stop the SNMP service.	<code>sudo systemctl stop snmpd</code>
2	Open the file <code>/etc/snmp/snmpd.conf</code> in an editor and replace line <pre>view v_read included .1.3.6.1.2.1.1</pre> with line <pre>view v_write included .1.3.6.1.2.1.1</pre>	[Dependent on the editor used]
3	Restart the SNMP service.	<code>sudo systemctl restart snmpd</code>

7.16.9 Configuring SNMPv3 users (User-based Security Model)

You create new users for SNMPv3 with the command **net-snmp-create-v3-user**. Optionally, instead of calling the command with all the necessary parameters, you can also call this command without parameters. In this case, the program prompts for the user names and passwords for authentication and encryption. For all other parameters, the default values are used: The MD5 hash function is used for encryption of the authentication, and the DES algorithm is used for encryption of the data communication.

Note

You can only perform the configuration steps described in this section with administrator rights.

7.16.9.1 Configuration files for SNMPv3

The configuration information for the users created with `net-snmp-create-v3-user` is contained in the following files:

- **/etc/snmp/snmpd.conf**
This file contains the names of the users with information on whether the user has read access and write access rights or only read access rights.
Two lines with the following content are added to this file for each new SNMPv3 user:

```
group <user name> usm <user name>
access <user name> "" usm authpriv exact v_read v3_write none
```
- **/var/lib/snmp/snmpd.conf**
In addition to the device ID for each user, this file contains the passwords and the methods for authentication and encryption.

7.16.9.2 Creating a new SNMPv3 user with default properties

To create a new user with default values, follow these steps:

Step	Instruction	Command
1	Stop the SNMP service.	<code>sudo systemctl stop snmpd</code>
2	Check the status.	<code>systemctl status snmpd</code>
3	Run <code>net-snmp-create-v3-user</code> without parameters. The input prompt for the SNMPv3 user name is displayed.	<code>sudo net-snmp-create-v3-user</code>
4	Enter the name for the SNMPv3 user. The input prompt for the authentication password is displayed.	<Benutzername>
5	Enter the authentication password for the SNMPv3 user. The input prompt for the encryption password is displayed.	<Authentifizierungspasswort>
6	Enter the encryption password for the SNMPv3 user. If you simply press the Enter key, the authentication password is also used for encryption of the data communication. The user is created with read access and write access rights. The program indicates which lines in the configuration files <code>/var/lib/snmp/snmpd.conf</code> and <code>/snmp/snmpd.conf</code> were added.	<Verschlüsselungspasswort>
7	Start the SNMP service.	<code>sudo systemctl start snmpd</code>
8	Check the status.	<code>systemctl status snmpd</code>

Example

```
admin@lpe9403-VPM7001325:~$ sudo systemctl stop snmpd
admin@lpe9403-VPM7001325:~$ sudo systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled;
   vendor preset: enabled)
   Active: inactive (dead) since Thu 2022-07-07 19:09:16 UTC; 35s
   ago
     Process: 174255 ExecStartPre=/bin/mkdir -p /var/run/agentx
   (code=exited, status=0/SUCCESS)
     Process: 174256 ExecStart=/usr/sbin/snmpd -Lsd -Lf /dev/null -u
   Debian-snmp -g Debian-snmp -I -smux,mteTrigger,mteTriggerConf -f >
   Main PID: 174256 (code=exited, status=0/SUCCESS)
      CPU: 434ms
[4]+  Stopped                  sudo systemctl status snmpd

admin@lpe9403-VPM7001325:~$ sudo net-snmp-create-v3-user
Enter a SNMPv3 user name to create:
User1
Enter authentication pass-phrase:
```

```

U1_esarhp-a
Enter encryption pass-phrase:
[press return to reuse the authentication pass-phrase]
U1_esarhp-e
adding the following line to /var/lib/snmp/snmpd.conf:
    createUser rh1 MD5 "U1_esarhp-a" DES "U1_esarhp-e"
adding the following line to /snmp/snmpd.conf:
    rwuser User1
admin@lpe9403-VPM7001325:~$ sudo systemctl start snmpd
admin@lpe9403-VPM7001325:~$ sudo systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled;
 vendor preset: enabled)
   Active: active (running) since Thu 2022-07-07 19:15:12 UTC;
 56s ago
     Process: 174738 ExecStartPre=/bin/mkdir -p /var/run/agentx
 (code=exited, status=0/SUCCESS)
    Main PID: 174739 (snmpd)
      Tasks: 1 (limit: 4459)
     Memory: 3.2M
        CPU: 166ms
    CGroup: /system.slice/snmpd.service
            └─174739 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-
snmp -g Debian-snmp -I
                  -smux mteTrigger mteTriggerConf -f -p /run/>

```

7.16.9.3 Creating a new SNMPv3 user with specific properties

To create a new user with specific values for all parameters, follow these steps:

Note

When the hash functions **MD5** and **SHA** are used, the value **NONE** is shown in the Web UI in the table of SNMPv3 users in the **Hash function** column.

Step	Instruction	Command
1	Stop the SNMP service.	<code>sudo systemctl stop snmpd</code>
2	Check the status.	<code>systemctl status snmpd</code>

Step	Instruction	Command
3	<p>Run net-snmp-create-v3-user with all the required parameters. The meaning of the parameters is as follows:</p> <ul style="list-style-type: none"> • -ro The user only has read access rights. • -A <Authentication password> Password for authentication of the user. • -X <Encryption password> Password for encryption of the data communication • -a <Hash function> The following values are possible for the hash function: <ul style="list-style-type: none"> – MD5 (default) – SHA – SHA-512 – SHA-384 – SHA-256 – SHA-224 • -x <Encryption method> The following values are possible for the encryption method: <ul style="list-style-type: none"> – DES (default) – AES • <User name> Name of the SNMPv3 user <p>The user is created. The program indicates which lines in the configuration files /var/lib/snmp/snmpd.conf and /snmp/snmpd.conf were added.</p>	<pre>sudo net-snmp-create-v3-user [-ro] [-A <Authentication password>] [-X <Encryption password>] [-a MD5 SHA SHA-512 SHA-384 SHA-256 SHA-224] [-x DES AES] <User name></pre>
7	Start the SNMP service.	<pre>sudo systemctl start snmpd</pre>
8	Check the status.	<pre>systemctl status snmpd</pre>

Example

Creation of a user named **User2** and the following parameters:

- Password for authentication: **U2_esarhp-a**
- Password for encryption of the data communication: **U2_esarhp-e**
- Hash function for authentication: **SHA-512**
- Encryption method for the data communication: **AES**

```
admin@lpe9403-VPM7001325:~$ sudo systemctl stop snmpd
```

```
admin@lpe9403-VPM7001325:~$ sudo systemctl status snmpd
```

- **snmpd.service** - Simple Network Management Protocol (SNMP) Daemon.
Loaded: loaded (/lib/systemd/system/snmpd.service; enabled;

```

vendor preset: enabled)
    Active: inactive (dead) since Thu 2022-07-07 19:09:16 UTC; 35s
ago
    Process: 174255 ExecStartPre=/bin/mkdir -p /var/run/agentx
(code=exited, status=0/SUCCESS)
    Process: 174256 ExecStart=/usr/sbin/snmpd -Lsd -Lf /dev/null -u
Debian-snmp -g Debian-snmp -I -smux,mteTrigger,mteTriggerConf -f >
    Main PID: 174256 (code=exited, status=0/SUCCESS)
    CPU: 434ms
[4]+  Stopped                  sudo systemctl status snmpd
admin@lpe9403-VPN3185785:~$ sudo net-snmp-create-v3-user -A
U2_esarhp-a -X U2_esarhp-e -a SHA-512 -x AES User2
[sudo] password for admin: *****
adding the following line to /var/lib/snmp/snmpd.conf:
    createUser User2 SHA-512 "U2_esarhp-a" AES "U2_esarhp-e"
adding the following line to /snmp/snmpd.conf:
    rwuser User2
admin@lpe9403-VPM7001325:~$ sudo systemctl start snmpd
admin@lpe9403-VPM7001325:~$ sudo systemctl status snmpd
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
    Loaded: loaded (/lib/systemd/system/snmpd.service; enabled;
vendor preset: enabled)
    Active: active (running) since Thu 2022-07-07 19:15:12 UTC;
56s ago
    Process: 174738 ExecStartPre=/bin/mkdir -p /var/run/agentx
(code=exited, status=0/SUCCESS)
    Main PID: 174739 (snmpd)          Tasks: 1 (limit: 4459)      Memory:
3.2M
    CPU: 166ms
    CGroup: /system.slice/snmpd.service
            └─174739 /usr/sbin/snmpd -Lsd -Lf /dev/null -u Debian-
snmp -g Debian-snmp -I
                -smux mteTrigger mteTriggerConf -f -p /run/>

```

7.16.9.4 Changing the access rights for SNMPv3

With SCALANCE LPE, read and write access is possible by default with SNMPv3. To disable the write access of an SNMPv3 user, follow these steps:

Step	Instruction	Command
1	Stop the SNMP service.	<code>sudo systemctl stop snmpd</code>
2	Open the <code>/etc/snmp/snmpd.conf</code> file with the nano editor, for example, that is installed on the SCALANCE LPE.	<code>sudo nano /etc/snmp/snmpd.conf</code>
3	In the line of the affected user, replace the <code>v3_write</code> string with the <code>none</code> string.	--
4	Restart the SNMP service.	<code>sudo systemctl restart snmpd</code>

Note

If a user has only read access rights, you must indicate which MIBs the user is permitted to access in the line for this user. To grant read permission comparable to version SNMPv2c, you must add the following text in the line for the user:

```
-v v_read
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo systemctl stop snmpd
admin@lpe9403-VPM7001325:~$ sudo nano /etc/snmp/snmpd.conf
```

Changing the following line for the USER1 user in the editor:

```
...
access USER1 "" usm authpriv exact v_read none
...
```

Changed line for the USER1 user:

```
...
access USER1 "" usm authpriv exact none none
...
```

```
admin@lpe9403-VPM7001325:~$ sudo systemctl restart snmpd
```

7.17 SFTP

SFTP (SSH File Transfer Protocol) enables the secure transfer of files between client and server. In contrast to FTP, data is exchanged over an encrypted SSH connection with SFTP. SFTP uses port 22 by default, which must be taken into account in the firewall settings. SFTP offers the same range of functions as FTP. In addition to exchanging files, it is also possible to rename and delete elements in the file system of the connected device and to display directory contents.

7.17.1 Establishing an SFTP connection

The prerequisite for file transfer is the establishment of an SFTP connection between the client and server. To establish an SFTP connection, run the following command:

```
Drive:\Path>sftp <User name>@<Server IP address>
```

Example

```
D:\>sftp admin@192.168.16.28
admin@192.168.16.28's password: *****
Connected to 192.168.16.28.
sftp>
```

7.17.2 Closing an SFTP connection

To close an SFTP connection, run the following command:

```
sftp> bye
```

7.17.3 Downloading a file

To download a file after establishing an SFTP connection, follow these steps:

Step	Instruction	Command
1	[Optional] Check whether the directory containing the file to be transferred is the current directory.	sftp> pwd
2	[Optional] Change to the directory containing the file to be transferred, if necessary.	sftp> cd <Verzeichnis>
3	Download the file. The file is saved in the directory in which the SFTP connection was established.	sftp> get <Pfad/Dateiname>
4	Close the SFTP connection	sftp> bye
5	Check whether the file was transferred.	<Drive>:\> dir

Example

```
sftp> pwd
Remote working directory: /home/admin
sftp> cd myfiles
sftp> get description.txt
Fetching /home/admin/myfiles/description.txt to description.txt
/home/admin/myfiles/description.txt 100% 728KB 9.0MB/s 00:00
sftp> bye
D:\>dir
Volume in drive D: is DATA
Volume serial number: 942F-FD6C
```

Directory of D:\

```
25.11.2022 10:56          745.849 description.txt
              1 file(s),          745.849 Bytes
```

7.17.4 Uploading a file

To upload a file after establishing an SFTP connection, follow these steps:

Step	Instruction	Command
1	[Optional] Check the target directory of the file transfer.	sftp> pwd
2	[Optional] Change to a suitable directory, if necessary.	sftp> cd <Verzeichnis>

Step	Instruction	Command
3	Upload the file.	<code>sftp> put <Pfad\Dateiname></code>
4	Check whether the file is present in the target directory.	<code>sftp> ls</code>

Example

```
sftp> pwd
Remote working directory: /home/admin
sftp> cd myfiles
sftp> put D:\projectfiles\description.txt
Uploading D:/projectfiles/description.txt to /home/admin/myfiles/
description.txt
D:/projectfiles/description.txt      100%   728KB   9.0MB/s   00:00
sftp> ls
description.txt
sftp>
```

7.18 Docker

The Docker software facilitates the installation and management of applications through the combination of all libraries and other components of an application in "Docker images". This section describes the basic steps for using Docker containers.

You can find additional information on the Docker homepage (<https://www.docker.com/>).

Note

If the firewall configuration has been reloaded (for example, with the command `sudo firewall-cmd --reload`), connections to Docker containers may be lost. To resolve the error, do one of the following:

- Restart the SCALANCE LPE.
- Restart Docker (for example, with the command `sudo systemctl restart docker`)

All Docker components (Containers, Networks, Volumes, Images, Bind Mounts, etc.) are saved in the **/userdata/docker** directory. The contents of this directory are also retained in the event of a firmware update.

7.18.1 Displaying Docker Containers configured in the device

To display the Docker Containers saved in the device, execute the following command:
`sudo docker ps -a`

Example

```
admin@lpe9403-VPM7001325:~$ sudo docker ps -a
[sudo] password for admin: *****
CONTAINER ID          IMAGE                                COMMAND                  CREATED
```

c25a1df191f9	hello-world	"/hello"	4 hours ago
STATUS		PORTS	NAMES
Exited (0) 4 hours ago			trusting_curran

7.18.2 Starting a Docker container

To start a Docker container, run the following command:

```
sudo docker start <Container ID | Container name> [Container ID | Container name] ...
```

Example

The example includes the following three steps:

- Displaying the Docker container present in the device.
- Starting the Docker container **httpd**.
- Checking if the Docker container was started.

```
admin@lpe9403-VPN7001325:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd          "httpd-foreground"      34 minutes ago
81e3145b5f2b   hello-world    "/hello"                 5 days ago

STATUS          PORTS          NAMES
Exited (0) 32 minutes ago    exciting_franklin
Exited (0) 26 hours ago      frosty_rhodes

admin@lpe9403-VPN7001325:~$ sudo docker start 517cd50861c5
517cd50861c5
admin@lpe9403-VPN7001325:~$ sudo docker ps -f "status=running"
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50761c5   httpd          "httpd-foreground"      35 minutes ago
81e3145b5f2b   hello-world    "/hello"                 5 days ago

STATUS          PORTS          NAMES
Up 3 seconds    80/tcp         exciting_franklin
Exited (0) 45 hours ago      frosty_rhodes
```

7.18.3 Stopping a Docker container

To stop a Docker container, run the following command:

```
sudo docker stop <Container ID | Container name> [Container ID | Container name] ...
```

If the container cannot be stopped, the signal for killing the container is sent after a defined period (default: 10 seconds).

Example

The example includes the following three steps:

- Displaying the Docker container present in the device. The **STATUS** column indicates whether a container is running.
- Stopping the Docker container with ID `517cd50861c5`.
- Checking the status of the Docker container. The exit code **0** indicates that the Docker container was stopped and not killed.

```
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED
517cd50861c5	httpd	"httpd-foreground"	20 hours ago
81e3145b5f2b	hello-world	"/hello"	5 days ago

STATUS	PORTS	NAMES
Up 19 hours	80/tcp	exciting_franklin
Exited (0) 45 hours ago		frosty_rhodes

```
admin@lpe9403-VPN3185785:~$ sudo docker stop 517cd50861c5
517cd50861c5
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED
517cd50861c5	httpd	"httpd-foreground"	20 hours ago
81e3145b5f2b	hello-world	"/hello"	5 days ago

STATUS	PORTS	NAMES
Exited (0) 40 seconds ago		exciting_franklin
Exited (0) 45 hours ago		frosty_rhodes

7.18.4 Restarting a Docker container

To stop and restart a running Docker container, run the following command:

```
sudo docker restart <Container ID | Container name> [Container ID | Container name] ...
```

Example

The example includes the following three steps:

- Displaying the Docker container present in the device. The **STATUS** column indicates whether a container is running.
- Restarting the Docker container with ID `517cd50861c5`.
- Checking the status of the Docker container.

```
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED
517cd50861c5	httpd	"httpd-foreground"	20 hours ago
81e3145b5f2b	hello-world	"/hello"	5 days ago

STATUS	PORTS	NAMES
Up 5 minutes	80/tcp	exciting_franklin

```

Exited (0) 45 hours ago          frosty_rhodes

admin@lpe9403-VPN3185785:~$ sudo docker restart 517cd50861c5
517cd50861c5
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd          "httpd-foreground"      20 hours ago
81e3145b5f2b   hello-world    "/hello"                 5 days ago

STATUS                PORTS          NAMES
Up 5 seconds          80/tcp        exciting_franklin
Exited (0) 45 hours ago          frosty_rhodes

```

7.18.5 Killing the execution of a Docker container

To kill a Docker container, run the following command:

```
sudo docker kill <Container ID | Container name> [Container ID | Container name] ...
```

Example

The example includes the following three steps:

- Displaying the Docker container present in the device. The `STATUS` column indicates whether a container is running.
- Killing the Docker container with ID `517cd50861c5`.
- Checking the status of the Docker container. The exit code **137** indicates that the Docker container was killed and not stopped.

```

admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd          "httpd-foreground"      20 hours ago
81e3145b5f2b   hello-world    "/hello"                 5 days ago

STATUS                PORTS          NAMES
Up 19 hours          80/tcp        exciting_franklin
Exited (0) 45 hours ago          frosty_rhodes

admin@lpe9403-VPN3185785:~$ sudo docker kill 517cd50861c5
517cd50861c5
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd          "httpd-foreground"      20 hours ago
81e3145b5f2b   hello-world    "/hello"                 5 days ago

STATUS                PORTS          NAMES
Exited (137) 58 seconds ago      exciting_franklin
Exited (0) 45 hours ago          frosty_rhodes

```

7.18.6 Pausing the execution of a Docker container

To pause a running Docker container, run the following command:

```
sudo docker pause <Container ID> [<Container ID> ...]
```

Example

The example includes the following three steps:

- Displaying the Docker container present in the device. The `STATUS` column indicates whether a container is running.
- Pausing the Docker container with ID `517cd50861c5`.
- Checking the status of the Docker container. The information `(Paused)` in the `STATUS` column indicates that the execution of the Docker container was paused.

```
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd          "httpd-foreground"      20 hours ago
81e3145b5f2b   hello-world    "/hello"                 5 days ago

STATUS          PORTS          NAMES
Up 5 minutes    80/tcp         exciting_franklin
Exited (0) 45 hours ago    frosty_rhodes
```

```
admin@lpe9403-VPN3185785:~$ sudo docker pause 517cd50861c5
517cd50861c5
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd          "httpd-foreground"      20 hours ago
81e3145b5f2b   hello-world    "/hello"                 5 days ago

STATUS          PORTS          NAMES
Up 5 minutes (Paused)  80/tcp         exciting_franklin
Exited (0) 45 hours ago    frosty_rhodes
```

7.18.7 Unpausing the execution of a Docker container

To resume the paused execution of a Docker container, run the following command:

```
sudo docker unpause <Container ID> [<Container ID> ...]
```

The example includes the following three steps:

- Displaying the Docker container present in the device. The information `(Paused)` in the `STATUS` column indicates that the execution of the Docker container was paused.
- Pausing the Docker container with ID `517cd50861c5`.
- Checking the status of the Docker container.

```
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd          "httpd-foreground"      20 hours ago
81e3145b5f2b   hello-world    "/hello"                 5 days ago
```

```

                STATUS                PORTS    NAMES
                Up 8 minutes (Paused)  80/tcp   exciting_franklin
                Exited (0) 45 hours ago  frosty_rhodes

admin@lpe9403-VPN3185785:~$ sudo docker unpause 517cd50861c5
517cd50861c5
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd         "httpd-foreground"      20 hours ago
81e3145b5f2b   hello-world   "/hello"                 5 days ago

                STATUS                PORTS    NAMES
                Up 8 minutes            80/tcp   exciting_franklin
                Exited (0) 45 hours ago  frosty_rhodes

```

7.18.8 Removing a Docker container

To remove a Docker container, run the following command:
`sudo docker rm <Container ID> [<Container ID> ...]`

The example includes the following three steps:

- Displaying the Docker container present in the device.
- Removing the Docker container with ID 517cd50861c5.
- Checking whether the Docker container was removed.

```

admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
517cd50861c5   httpd         "httpd-foreground"      20 hours ago
81e3145b5f2b   hello-world   "/hello"                 5 days ago

                STATUS                PORTS    NAMES
                Exited (0) 4 minutes ago  80/tcp   exciting_franklin
                Exited (0) 45 hours ago  frosty_rhodes

admin@lpe9403-VPN3185785:~$ sudo docker rm 517cd50861c5
517cd50861c5
admin@lpe9403-VPN3185785:~$ sudo docker ps -a
CONTAINER ID   IMAGE          COMMAND                  CREATED
81e3145b5f2b   hello-world   "/hello"                 5 days ago

                STATUS                PORTS    NAMES
                Exited (0) 45 hours ago  frosty_rhodes

```

7.18.9 Displaying Docker images saved in the device

To display the Docker images saved in the device, execute the following command:
`sudo docker images`

Example

```
admin@lpe9403-VPM7001325:~$ sudo docker images
[sudo] password for admin: *****
REPOSITORY          TAG             IMAGE ID          CREATED
SIZE
ubuntu               latest          1cb4829d6243     42 hours ago
66.7MB
httpd                latest          2b598305371b     4 weeks ago
155MB
hello-world          latest          a29f45ccde2a     6 months ago
9.14kB
```

7.18.10 Loading a Docker image from a repository or a registry

In order to load an image, a connection must exist between the SCALANCE LPE and a Docker registry. This can be a local registry or the Docker Hub.

Note

The pre-installed Docker stores all images in the `/userdata/docker/` directory.

To load a Docker image into the device, execute the following command:

```
sudo docker pull <Image-Name | Image-ID>
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo docker pull httpd
[sudo] password for admin: *****
Using default tag: latest
latest: Pulling from library/httpd
33cc09c9b190: Pull complete
0adc4d0b81bf: Pull complete
f0ef0544557a: Pull complete
7bbd2835dd10: Pull complete
a649f7fe9206: Pull complete
Digest:
sha256:387f896f9b6867c7fa543f7d1a686b0ebe777ed13f6f11efc8b94bec743a1e51
Status: Downloaded newer image for httpd:latest
docker.io/library/httpd:latest
```

7.18.11 Running a Docker image

To start a new Docker container, run the following command:

```
sudo docker run <Image name | Image-ID>
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo docker run hello-world
[sudo] password for admin: *****
Hello from Docker!
```

This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:

1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub. (arm64v8)
3. The Docker daemon created a new container from that image which runs the executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it to your terminal.

To try something more ambitious, you can run an Ubuntu container with:

```
$ docker run -it ubuntu bash
```

7.18.12 Displaying Docker Volumes

To display the existing Docker volumes, execute the following command:

```
sudo docker volume ls
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo docker volume ls
[sudo] password for admin: *****
DRIVER          VOLUME NAME
local           volume_01
```

7.18.13 Network access from Docker containers

The Docker installation on the SCALANCE LPE already contains all the required components for network access of Docker containers.

Docker creates a virtual network interface for each container and connects the interface to a Docker network. If no network is specified when creating a container, the default network is used.

The IP configuration outside of Docker containers is performed exclusively with the **ipconfig** tool.

There are multiple network drivers for different applications for Docker networks:

- **bridge**

This driver is the default network driver that the Docker network uses to perform the function of a network bridge. The driver **bridge** is primarily used when the application runs in a stand-alone container and must communicate with other containers. Containers can communicate with each other and the host if they are in the same subnet. If no IP address is specified when creating a container, Docker assigns an IP address from the defined subnet.

- **host**

A driver for direct use of network resources of the host computer. The IP address configured with **ipconfig** for the host is used by the container.

- **macvlan**
A driver for Layer 2 communication. Docker containers receive unique IP and MAC addresses and can handle Layer 2-based communication.
The names P1, P2 and P3C must be specified on selection of the interfaces, for example during configuration of macvlan.
Example:

```
sudo docker network create -d macvlan --subnet=192.168.35.0/24  
-o parent=P3C pub_net
```
- **overlay**
A driver that connects multiple Docker daemons with each other. This means swarming services can communicate with each other.
- **none**
A driver that disables all network connections for the connected container.

More information can be found in the Docker documentation (<https://docs.docker.com/network/>).

SCALANCE LPE uses the **firewalld** program as a firewall, which assigns the host-side Docker network interface to the "drop" zone. This means all incoming packages are discarded and the device does not respond. The firewall only permits outgoing network connections. Docker containers can communicate with each other via the network driver **bridge**. However, no external packages can be sent to the Docker container.

If explicit network access to the container is configured in Docker, the firewall setting is made with **dockerd**. The user does not need to configure **firewalld** any further.

Before setting up a container, Docker attempts to remove all rules in **firewalld**. If no rules are present, **firewalld** outputs corresponding error messages. These error messages are saved both in the log file of **firewalld** and in the log table for system events. The device may also forward these error messages to external Syslog servers. You can ignore these error messages because they have no effects on the function of the Docker container.

7.18.14 Displaying Docker Networks

To display the Docker Networks of the device, execute the following command:

```
sudo docker network ls
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo docker network ls  
[sudo] password for admin: *****  
NETWORK ID          NAME                DRIVER              SCOPE  
fdd868dc7c51        bridge             bridge              local  
b9e33ee02e29        host               host                local  
dace0faa4e1b        none               null                local
```

7.18.15 Displaying information via Docker

To display information about the Docker installation of the device, execute the following command:

```
sudo docker info
```

Example

```
admin@lpe9403-VPM7001325:~$ sudo docker info
[sudo] password for admin: *****
Client:
  Debug Mode: false
Server:
  Containers: 5
    Running: 0
    Paused: 0
    Stopped: 5
  Images: 2
  Server Version: 19.03.12
  Storage Driver: overlay
    Backing Filesystem: extfs
    Supports d_type: true
  Logging Driver: json-file
  Cgroup Driver: cgroupfs
  Plugins:
    Volume: local
    Network: bridge host ipvlan macvlan null overlay
    Log: awslogs fluentd gcplogs gelf journald json-file local
logentries splunk syslog
  Swarm: inactive
  Runtimes: runc
  Default Runtime: runc
  Init Binary: docker-init
  containerd version: 7ad184331fa3e55e52b890ea95e65ba581ae3429
  runc version: dc9208a3303feef5b3839f4323d9beb36df0a9dd
  init version: fec3683
  Security Options:
    seccomp
    Profile: default
  Kernel Version: 4.19.118-audis-std
  Operating System: SIEMENS LPE9403 GNU/Linux V01.00.00.00
  OSType: linux
  Architecture: aarch64
  CPUs: 4
  Total Memory: 1.838GiB
  Name: lpe9403-VPM7001325
  ID: OVHH:I33S:XMTD:TNMD:OVUU:DPCC:JSCO:UE3P:AW6G:6B6R:ODH6:MHOS
  Docker Root Dir: /userdata/docker
  Debug Mode: false
  Registry: https://index.docker.io/v1/
  Labels:
  Experimental: false
  Insecure Registries:
    127.0.0.0/8
  Live Restore Enabled: false
WARNING: No swap limit support
WARNING: the overlay storage-driver is deprecated, and will be
removed in a future release.
```

7.18.16 Installing Nozomi Remote Collector

This section describes how to install the **Nozomi Remote Collector** application using the Linux shell. Required for the installation is an appropriate license from Nozomi Networks Inc.

Note

The **Nozomi Remote Collector** cannot be used without the **Nozomi Guardian** application.

Note

Before downloading and installing, check that the use is permitted in the intended country of use.

Required is an installation file for the Nozomi Remote Collector, which is available on the SCALANCE LPE in factory state. This file can be deleted if you do not want to install the Nozomi Remote Collector or once the installation has been completed.

The installation file for the Nozomi Remote Collector is not a component of the firmware. If the firmware has been updated via the Rescue system, you first need to upload the installation file for the Nozomi Remote Collector to the SCALANCE LPE and save it in the **/userdata** directory.

To install the Nozomi Remote Collector on the SCALANCE LPE, proceed as follows:

The installation file for the Nozomi Remote Collector is also available from **Siemens Industry Online Support SIOS** (<https://support.industry.siemens.com>).

1. Ensure that there is a connection between the SCALANCE LPE and the Internet.
2. Run the following command:

```
sudo sfw_manager /userdata/nozomiV<Version number>.swu
```

The required files are downloaded from the Internet, the build process of Docker starts. This process can take up to 30 minutes.
3. Run the following command:

```
sudo docker images
```

If the Docker image is successfully created, you will find a line for the Nozomi Remote Collector in the list that appears.
4. Configure the installed Nozomi Remote Collector according to the manufacturer's instructions.

7.18.17 Deleting the installation file of the Nozomi Remote Collector

SCALANCE LPE contains an installation file for the Nozomi Remote Collector in the factory state. This file can be deleted if you do not want to install the Nozomi Remote Collector or once the installation has been completed.

Deleting the installation file for the Nozomi Remote Collector does not affect a Docker image already created with this installation file. The functionality of the Nozomi Remote Collector application is not affected.

To delete the Nozomi Remote Collector installation file, execute the following command:

```
rm /userdata/nozomiV<Versionsnummer>.swu
```

7.18.18 Docker Compose

Docker Compose is an extension of Docker for automated configuration of Docker containers. All configuration information is contained in the file **docker-compose.yml**. This includes information about Docker volumes, Docker networks, the storage location of Docker images and environment variables. A YAML file **docker-compose.yml** is required for all user actions that are described in the following sections. The directory in which the **docker-compose.yml** file is stored must be the current directory. Otherwise, you must specify the parameter **--file <Dateiname>** or **--project-directory <Pfad>**.

It is particularly advantageous to use Docker Compose for applications requiring multiple Docker containers or for Docker containers whose start requires the configuration of numerous parameters. With Docker Compose, all Docker containers defined in the **docker-compose.yml** file can be run, paused or stopped with a single shell command.

As of firmware version 2.1, Docker Compose version 1.25.0 is preinstalled on SCALANCE LPE.

Example

The **docker-compose.yml** file below contains an example configuration for the PostgreSQL Docker container.

```
version: '3'
services:
  postgresdb:
    image: postgresdb:latest
    restart: always
    environment:
      - POSTGRES_USER=dbuser
      - POSTGRES_PASSWORD=dbpassword
      - POSTGRES_DB=nemo
    volumes:
      - /home/${SUDO_USER}/ta/postgres:/var/lib/postgresql/data
    logging:
      driver: "json-file"
      options:
        max-size: "5mb"
        max-file: "5"
        mode: non-blocking
```

7.18.18.1 Displaying information on Docker containers

To display information on the Docker containers of a Docker Compose project, run the following command:

```
sudo docker-compose ps
```

7.18.18.2 Creating Docker containers and building resources

The Docker Compose program can perform the following tasks when starting Docker containers if the **docker-compose.yml** file contains corresponding configuration information:

- Downloading, starting and stopping of Docker containers
- Creating and mounting of Docker volumes
- Initialization and linking of Docker networks
- Configuration of port mappings
- Setting of environment variables
- Definition of login data

To start Docker containers with the configuration in the **docker-compose.yml** file, run the following command:

```
sudo docker-compose up
```

If the YAML file has a different name, run the following command:

```
sudo docker-compose -f <Filename> up
```

The containers are stopped when the terminal session is closed. To keep Docker containers running even after the terminal session is closed, run the following command with the parameter **-d** or **--detach**:

```
sudo docker-compose up -d
```

7.18.18.3 Stopping Docker containers and removing resources

To stop running Docker containers and remove all Docker volumes, Docker networks and Docker images, run the following command:

```
sudo docker-compose down
```

If parameters are not specified, only the Docker containers and Docker networks that were built by **docker-compose up** are removed. If containers of services not defined in the **docker-compose.yml** file are to be removed, you must specify the parameter **--remove-orphans**.

7.18.18.4 Starting Docker containers

You can only start Docker containers that already exist.

To start Docker containers that are required for services in the **docker-compose.yml** file, run the following command:

```
sudo docker-compose start
```

7.18.18.5 Stopping Docker containers

To stop running Docker containers without having to remove the Docker containers, Docker volumes, Docker networks and Docker images, run the following command:

```
sudo docker-compose stop
```

7.18.18.6 Killing Docker containers

To kill all running Docker containers, run the following command:

```
sudo docker-compose kill
```

Example

The example includes the following two steps:

- Killing the Docker containers.
- Checking if the Docker containers were stopped.

```
admin@lpe9403-VPN7001325:~/postgres_compose$ sudo docker-compose
kill
Killing postgres_compose_postgresdb_1 ...
[20257.561340] br-14b4b8a32769: port 1(veth8f8a78a) entered
disabled state
[20257.568347] veth0365e4d: renamed from eth0
[20257.641030] br-14b4b8a32769: port 1(veth8f8a78a) entered
disabled state
[20257.649255] device veth8f8a78a left promiscuous mode
Killing postgres_compose_postgresdb_1 ... done

admin@lpe9403-VPN1204376:~/postgres_compose$ sudo docker-compose ps
              Name                      Command
-----
postgres_compose_postgresdb_1  docker-entrypoint.sh postgres

      State      Ports
-----
Exit 137
```

7.18.18.7 Pausing Docker containers

The content of the RAM of a Docker container whose execution has been paused is retained.

To pause the execution of Docker containers that are required for services in the **docker-compose.yml** file, run the following command:

```
sudo docker-compose pause
```

7.18.18.8 Unpausing Docker containers

To resume the execution of Docker containers whose execution was paused with command **docker-compose pause**, run the following command:

```
sudo docker-compose unpause
```


Web User Interface

This section describes how to configure the device using the Web UI. In addition to device management, the assignment of an IP address, for example, is also a subject of the description.

8.1 Accessing the Web UI via a Network Connection

To access the Web UI (Web User Interface), establish a remote connection between a client PC and a device via the network.

The device has an integrated HTTP server for this purpose. If you address a device using an Internet browser, it returns HTML pages to the client PC depending on the user input.

Requirements

- The device has an IP address.

Note

The following options apply to the assignment of an IP address:

- DHCP
- SINEC PNI
- PRONETA

For more information, refer to "IP address assignment (Page 29)"

- There is a network connection between the device and the client PC.
- The network settings of the device and of the client PC match.

Note

You can use the **ping** diagnostics tool to check whether a connection exists and communication is possible.

- An Internet browser is available on the client PC.
The display of the Web UI was tested with the following Internet browsers:
 - Microsoft Edge 83 or higher
 - Mozilla Firefox 78 or higher
 - Google Chrome 83 or higher
- JavaScript is activated in the Internet browser.

Establishing a connection to a device

To access the Web UI, follow these steps:

1. Open an Internet browser.
2. In the address box of the Internet browser, enter the IP address or the URL of the device and confirm it with **Enter**. If there is a problem-free connection to the device, the login page of the Web UI is displayed.
A warning is displayed during the first login; it warns the user that the browser does not consider the module certificate of the SCALANCE LPE to be secure. Confirm the insecure connection. If you want to access the SCALANCE LPE using public networks, you should store your own certificate on the device. For more information on handling certificates, see "Security recommendations (Page 13)".
3. Log in.
For more information, refer to "Logging in (Page 127)".

8.2 Inactivity timeout

An inactivity timeout has been configured for a session with the Linux Shell or the Web UI. If no user action takes place within the configured time, the session is automatically closed. The time remaining until the session will automatically close is displayed on the right side of the header with the Web UI.

8.2.1 Configuring the inactivity timeout for the Linux Shell

Note

You must have administrator rights to configure the inactivity timeout.

To configure the inactivity timeout for the Linux Shell, follow these steps:

1. Navigate to **System » Inactivity timeout**.
2. Enter a new value in minutes in the **Inactivity timeout shell** text box.
Range of values: 0 ... 99
Default: 5 minutes
If you enter the value **0**, the inactivity timeout for the Linux Shell is disabled. If you enter an invalid value, an error message is displayed under the text box.
3. Click the **Apply** button.
A dialog box informs you that the values have been changed. The change does not affect an ongoing terminal session. The new value applies to all subsequent terminal sessions. The SCALANCE LPE does not need to be rebooted.

8.2.2 Configuring the inactivity timeout for the Web UI

Note

You must have administrator rights to configure the inactivity timeout.

To configure the inactivity timeout for the Web UI, follow these steps:

1. Navigate to **System » Inactivity timeout**.
2. Enter a new value in minutes in the **Inactivity timeout Web UI** text box.
Range of values: 0 ... 99
Default: 10 minutes
If you enter the value **0**, the inactivity timeout for the Web UI is disabled. If you enter an invalid value, an error message is displayed under the text box.
3. Click the **Apply** button.
A dialog box informs you that the values have been changed.

8.3 Logging in

The various methods for logging in are described in this section.

8.3.1 Default user profiles and passwords

The following default user profiles and passwords are preconfigured:

 CAUTION
Security risk - Danger of unauthorized access and/or exploitation. Before commissioning the device, change the default passwords and user names to prevent unauthorized access. For more information, refer to "Logging In to a Device with Default Settings (Page 128)".

Profile	Password
admin	admin

8.3.2 Logging In to a Device with Default Settings

When you log in to a device with default settings, follow these steps:

1. Establish a connection to the device and call the Web UI.
The login page of the Web UI is displayed.
For more information, refer to "Accessing the Web UI via a Network Connection (Page 125)".
2. Click the **User name** field and enter the factory default user name.
For more information, refer to "Default user profiles and passwords (Page 127)".
3. Click the **Password** field and enter the factory default password.
4. Click the **Log in** button or confirm your input with **Enter**.
The device checks the entries.
 - If the entries are correct, additional text boxes for changing the user name and password will appear.
 - If the entries are incorrect, a red exclamation mark appears to the right of the fields and an error message is displayed. Repeat the last steps.
5. [Optional] Enter a new user name in the text box under the **Change admin username** check box if you do not want to keep **admin**. The user name must not contain any special characters except the characters "_" and "-". The user name must start with a letter or with the character "_".
6. If you do not want to change the **admin** user name, clear the **Change admin username** check box.
The text box for the new user name is no longer displayed.
7. Click the **New password** field and assign a new password. The new password must meet the following conditions:
 - At least 12 characters
 - Maximum of 250 characters
 - At least one number
 - At least one uppercase letter
 - At least one lowercase letter
 - At least one special character: # ! \$ % & () * + , - . / : < = > @ [] ^ _ { } ~If the password does not meet the specified criteria, a corresponding note is displayed and you are prompted to enter a password again.
8. Click the **New password confirmation** field and enter the new password again.
9. Click the **Log in** button or confirm your input with **Enter**.
The device checks the entries. As optical feedback, a load symbol appears beside the fields on the right.
 - If the entries are correct, a green checkmark appears briefly to the right of the fields. To activate the changes, the Web UI session is automatically reloaded after a few seconds. Log in with the user name and the new password.
 - If the entries are incorrect, a red exclamation mark appears to the right of the fields and an error message is displayed. Repeat the last steps.

8.3.3 Logging In to a Configured Device

When you log in to a configured device, follow these steps:

1. Establish a connection to the device and call the Web UI.
The login page of the Web UI is displayed.
For more information, refer to "Accessing the Web UI via a Network Connection (Page 125)".
2. Click the **User name** field and enter the user name.
3. Click the **Password** field and enter the corresponding password.
4. Click the ?? button or confirm your input with **Enter**.
The device checks the entries. As optical feedback, a load symbol appears beside the fields on the right.
 - If the entries are correct, a green checkmark appears briefly to the right of the fields and the start page of the Web UI is displayed.
 - If the entries are incorrect, a red exclamation mark appears to the right of the fields and an error message is displayed. Repeat the last steps.

8.4 Logout

Proceed as follows to log out:

1. Click the button for the **user profile** in the status bar.
2. Click the **Log out** button.

8.5 IP configuration

Note

You can configure the IP parameters only with administrator rights.

This section describes how you configure the IP parameters of the device via the Web UI. This includes, for example, assigning an IP address and defining a gateway.

8.5.1 Displaying the IP configuration

To view the IP configuration, navigate to **Interfaces » IP interfaces**.

In the table, there is a row for each interface with the following information:

- The port name
- Type of address assignment. IP addresses can be assigned statically or with DHCP.
- The IP address of the interface
- The link status, i.e. **Up** or **Down**.

If you click the V icon on the right edge of the table row, additional information is displayed:

Parameter	Description
Configuration	Type of address assignment. IP addresses can be assigned statically or with DHCP.
DCP mode	Shows how you can access the port with the DCP protocol: <ul style="list-style-type: none"> • Setup If the device is in delivery state or was reset to factory settings, write access is possible with DCP. When the default password has been changed, only read access is then possible with DCP (default setting). • Read Only read access is possible. • Read/write Read and write access is possible. • - DCP is disabled for the port.
DCP device name	Device name assigned via DCP.
Default gateway	If this check box is selected, the default gateway is reached via this interface.
Status	Shows whether the interface is enabled or disabled.
For port P3C only: DHCP client ID or DHCP device name	If the IP address for port P3C is assigned via DHCP, you can configure the method for identification of the client. If the client is not identified using the MAC address of the interface, this field contains either the DHCP Client ID or the DHCP device name.
MAC address	The MAC address of the interface
IP address	The IP address of the interface
Subnet	The subnet mask of the interface
Gateway	The gateway IP address
DNS server	The IP address of the DNS server. You can enter a maximum of two IP addresses, separated by a comma and without spaces.

8.5.2 Configuring the access rights of DCP

Follow these steps to configure DCP for a port:

1. Navigate to **Interfaces » IP interfaces**.
2. Open the configuration parameters area by clicking the V icon on the right edge of the table row for the respective port.
3. Ensure that the **Enable** entry is selected for the port in question in the **Status** drop-down list. Otherwise, the drop-down list in the **DCP mode** column is disabled and you cannot select anything there.

4. Select one of the following entries in the **DCP mode** drop-down list:
 - **Setup**
If the device is in delivery state or was reset to factory settings, write access is possible with DCP. When the default password has been changed, only read access is then possible with DCP (default setting).
 - **Read**
Parameters of the device configuration can only be read with the DCP protocol.
 - **Read/write**
Parameters of the device configuration such as IP address can be read and, depending on the configuration status of the device, written with the DCP protocol. If the device is in factory default status, write access is possible. If the default password was changed during the first login via the shell and Web UI, only read access is still possible.
 - -
Parameters of the device configuration cannot be read or written with the DCP protocol.
5. Click the **Apply** button.

8.5.3 Configuring a static IPv4 address

To configure a static IP address, follow these steps:

1. Navigate to **Interfaces** » **IP interfaces**.
2. Open the configuration parameters area by clicking the V icon on the right edge of the table row for the respective port.
3. Ensure that the **Enable** entry is selected for the port in the **Status** drop-down list. If **Disable** is displayed, the entry fields for **Gateway**, **IP address**, and **Subnet** are grayed out and you cannot enter anything there.
4. In the **Configuration** drop-down list, select **Static**.
5. Enter the **IP address** in the IP address text box.
6. Enter the subnet mask in the **Subnet** text box.
7. Click the **Apply** button.

8.5.4 Obtaining an IPv4 address via DHCP

To obtain an IP address via DHCP, follow these steps:

1. Navigate to **Interfaces** » **IP interfaces**.
2. Open the configuration parameters area by clicking the V icon on the right edge of the table row for the respective port.
3. Ensure that the **Enable** entry is selected for the port in the **Status** drop-down list. Otherwise, the **Configuration** drop-down list is inactive and you cannot select anything there.
4. In the **Configuration** drop-down list, select **DHCP**.

5. [Optional for port **P3C**]
Select the method for identifying the client for the combo port **P3C**. The following options are available:
 - **DHCP**
The client is identified via the MAC address of the interface.
 - **DHCP_C**
The client is identified via the DUID. The DUID is displayed in the **DHCP Client ID** field. This field only exists if **DHCP_C** mode was configured.
 - **DHCP_H**
The client is identified by the device name. The device name is displayed in the **DHCP device name** field. This field only exists if **DHCP_H** mode was configured.
6. Click the **Apply** button. The values assigned by DHCP are displayed in the **IP address** and **Subnet** text boxes. In addition, the IP address is displayed in the header of the configuration parameters area.

8.5.5 Enabling/disabling an interface

To enable or disable a port, follow these steps:

1. Navigate to **Interfaces** » **IP interfaces**.
2. Open the configuration parameters area by clicking the V icon on the right edge of the table row for the respective port.
3. Select the port status in the **Status** drop-down list:
 - **Enable**
The interface is enabled. If this interface is or will be connected to a network, it works according to its configuration.
 - **Disable**
The interface is disabled. Even when connected to a network, no communication takes place via this interface.
4. Click the **Apply** button.

8.5.6 Configuring the default gateway statically

You can only configure one gateway. The existing gateway address is overwritten if necessary. To configure the **default gateway** statically, follow these steps:

1. Navigate to **Interfaces** » **IP interfaces**.
2. Open the configuration parameters area by clicking the V icon on the right edge of the table row for the respective port.
3. Ensure that the **Enable** entry is selected for the port in the **Status** drop-down list. Otherwise, the **Configuration** drop-down list is inactive and you cannot select anything there.
4. Select **Static** from the **Configuration** drop-down list. If **DHCP** is displayed, the **Gateway** text box is grayed out and you cannot enter an IP address there.

5. Select the **Default gateway** check box.
6. Enter the IP address of the default gateway in the **Gateway** text box.
7. Click the **Apply** button. The IP address is applied for the other ports. The configured IP address is also displayed in the **Default gateway** section.

8.5.7 Configuring the default gateway dynamically

You can only configure one gateway. The existing gateway address is overwritten if necessary. To configure the **default gateway** dynamically, follow these steps:

1. Navigate to **Interfaces** » **IP interfaces**.
2. Open the configuration parameters area by clicking the V icon on the right edge of the table row for the respective port.
3. Ensure that the **Enable** entry is selected for the port in the **Status** drop-down list. Otherwise the **Default gateway** check box is inactive and you cannot make any changes there.
4. Select the **Default gateway** check box.
5. Click the **Apply** button. The value assigned by DHCP is displayed in the **Gateway** text box and applied to the other ports. The value assigned by DHCP is also displayed in the **Default gateway** section.

8.6 Sfp Diagnose

This section describes how you check the current operating state of an SFP. This includes, for example, the temperature, the transmission performance and the electrical parameters.

On this page, you run error diagnostics for each individual SFP port. This test is performed without needing to remove the cable, connect a cable tester or install a loopback module at the other end.

Note

Note that this test is permitted only when no data connection is established on the port to be tested. If, however, there is a data connection to the port to be tested, this is briefly interrupted. Automatic re-establishment of the connection can fail; in this case, the connection may need to be re-established manually.

8.6.1 Checking the operating state of an SFP

Follow these steps to check the operating state of an SFP:

Navigate to **Interfaces** » **SFP diagnostics** and click the **Update** button. The table in the **Sfp Diagnose** section displays the following information for each SFP interface:

Parameter	Description
Interface	The port name
Link State	Shows whether the port has an active link.
SFP-Temperature [°C]	The temperature of the SFP.
Rx power [dBm]	Shows the receive power of the interface in decibel milliwatts.
Tx power [dBm]	Shows the send power of the interface in decibel milliwatts.
Voltage [V]	Shows the voltage applied to the interface in volts.
Current [mA]	Shows the current consumption of the interface in milliamperes.

Note

Deviations of the displayed values from the technical specifications

The values displayed for the send or receive power can vary slightly from the values specified in the Operating Instructions. The values displayed on the Web UI page are relevant.

The table in the **Interface and SFP Information** section displays the following information for each SFP interface:

Parameter	Description
Interface	The port name
SFP Vendor (Name)	The name of the SFP vendor.
SFP Article Number	The article number of the SFP.
SFP bit rate [Mbps]	Shows the nominal bit rate of the interface.
SFP Serial Number	The serial number of the SFP.
SFP Revision	The revision of the SFP.
Max Link Length 50.0µm [m]	Shows the maximum distance in meters that is possible with this medium.
Max Link Length 62.5µm [m]	Shows the maximum distance in meters that is possible with this medium.

8.7 VXLAN configuration

This section describes creating and deleting VXLAN connections via the Web UI.

8.7.1 Configuring a VXLAN connection

Note

You must have administrator rights to configure a VXLAN connection.

To configure a VXLAN connection, follow these steps:

1. Navigate to **Interfaces » Virtual Extensible LAN**.
2. Click the **Add VXLAN** button.
The **Configure new VXLAN interface** dialog box is displayed.
3. Enter the VXLAN Network Identifier in the **VNI** text box.
Range of values: 1 ... 16777215
4. Select the interface for connection to the internal network from the **Internal interface** drop-down list.
5. Select the interface for connection to the external network from the **External interface** drop-down list.
Different interfaces need to be specified for the external and internal interface.
6. In the **External IP address** text box, enter the IP address and the prefix of the external interface.
7. [Optional if the IP address of the external interface and the IP address of the VXLAN remote station belong to the same subnet, otherwise mandatory.]
Enter the IP address of the gateway to the VXLAN remote station in the **Gateway** text box. You can enter a maximum of two IP addresses, separated by a comma.
8. Enter the IP address of the VXLAN remote station in the **IP address of the end point** text box.
The option box is enabled depending on the IP address:
 - **Unicast**
With an IP address in the range 0.0.0.0 ... 223.255.255.255
 - **Multicast**
With an IP address in the range 224.0.0.0 ... 239.255.255.255
9. [Optional] In the **UDP port external interface** text box, enter the port of the external interface.
Range of values: 4096 ... 65535
Default: 4789
10. [Optional] Enter the port of the VXLAN remote station in the **Port of the end point** text box.
Range of values: 4096 ... 65535
Default: 4789
11. Click the **Save** button.
The entered data is displayed in the **Configuration of the external interface** and **Configured VXLAN** sections.

8.7 VXLAN configuration

12. [Optional] Select a value for the maximum packet size in the **MTU** column of the table in section **Configuration of the external interface**.

Possible values:

- 1500 (default)
- 1550

13. Click the **Apply** button.

A small dialog box appears at the bottom edge of the browser window with a message indicating that the configuration has been applied.

Configuration of a second VXLAN connection

The configuration of a second VXLAN interface is optional. In contrast to the configuration of the first VXLAN connection, no values for the following two parameters can be entered in the **Configure new VXLAN interface** dialog box:

- **External interface**
- **Gateway**

In addition, the following two parameters are already preset with values:

- **Internal interface**
SCALANCE LPE has three interfaces. Consequently, after the configuration of the first VXLAN interface, only the interface that is not yet configured is available as internal interface for the second VXLAN configuration.
- **External IP address**
There is only one external interface, so the external IP address is already configured after the configuration of the first VXLAN interface.

8.7.2 Enabling the VXLAN configuration

Note

You must have administrator rights to enable the VXLAN configuration.

You can only enable VXLAN if at least one VXLAN has been configured. Otherwise, the **Enable VXLAN** button is disabled.

To enable the VXLAN configuration, follow these steps:

1. Navigate to **Interfaces » Virtual Extensible LAN**.
2. Click the **Enable VXLAN** button.

8.7.3 Disabling the VXLAN configuration

Note

You must have administrator rights to disable the VXLAN configuration.

You can only disable VXLAN if VXLAN is active. Otherwise, the **Disable VXLAN** button is not displayed.

To disable the VXLAN configuration, follow these steps:

1. Navigate to **Interfaces » Virtual Extensible LAN**.
2. Click the **Disable VXLAN** button.

8.7.4 Adding a Virtual Tunnel Endpoint (VTEP)

Note

You must have administrator rights to add a Virtual Tunnel Endpoint.

To add a Virtual Tunnel Endpoint, follow these steps:

1. Navigate to **Interfaces » Virtual Extensible LAN**, section **Configured VXLAN**.
2. Click on the plus icon (**Add end point**) under the table with the VTEPs.
A dialog box for entering the configuration data is displayed.
3. Enter the IP address of the Virtual Tunnel Endpoint in the **IP address** text box.
4. Enter the port number of the Virtual Tunnel Endpoint in the **Port number** text box.
5. Click the **Save** button.
A new row with the entered IP address is displayed in the **End points** table.
6. Click the **Apply** button.

8.7.5 Deleting the configuration of a VTEP

Note

You must have administrator rights to delete a Virtual Tunnel Endpoint.

To delete a Virtual Tunnel Endpoint, follow these steps:

1. Navigate to **Interfaces** » **Virtual Extensible LAN**, section **Configured VXLAN**.
2. Click the trashcan icon (**Delete end point**) in the table row of the end point to be deleted in the last table column.
The configuration of the VTEP and the corresponding table row are deleted.
3. Click the **Apply** button.

8.7.6 Deleting a VXLAN connection

Note

You must have administrator rights to delete a VXLAN connection.

To delete a VXLAN connection, follow these steps:

1. Navigate to **Interfaces** » **Virtual Extensible LAN**, section **Configured VXLAN**.
2. Click on the **Delete** button in the section of the VXLAN connection that you want to delete.
The section for this VXLAN connection is deleted.
3. Click the **Apply** button.

8.8 Device management

This section describes how you manage the device. This includes, for example, how you display information about the device or update the firmware.

8.8.1 Showing device information

To display information about the device, navigate to **System** » **Dashboard** or click the "SIEMENS" logo on the left side of the header.

The following information is displayed in the **Device data** field:

Parameter	Description
Host name	The device name
Device type	The type designation of the device
Status Secure Boot	Shows whether the Secure Boot function is enabled or disabled.
Bootloader version	The version of the bootloader
Version Rescue system	The version of the Rescue system
Firmware version	The firmware version
Device Temperature (°C)	The device temperature in °C
Load average	The load of the processor in the last 1, 5 and 15 minutes.

Parameter	Description
Memory (used/total, load)	Used work memory, available work memory and utilization of the work memory as percentage.
RootFS (used / total, load)	The load of the part of the file system reserved for root, the total size of the part of the file system reserved for root, and the utilization as a percentage.
User Space (used/total, load)	The load of the part of the file system reserved for users, the total size of the part of the file system reserved for users, and the utilization as a percentage.
External Device <partitionName> (used/total, load)	The load of an external device, the total size of the external device and the utilization as a percentage. This field is only displayed if an external device is connected to the LPE or a CLP is inserted.
Sfp Diagnose	Information on whether an SFP is inserted.

8.8.2 Displaying information on the operating state

To view information about the operating status of the device, navigate to **System » Charts**.

This page contains multiple charts that display the following values:

Parameter	Description
Device Temperature (°C)	The device temperature in °C
CPU Load Average (%)	The average load of the processor in percent.
Free Memory (%)	Utilization of the work memory in percent.
Rootfs usage (%)	The load of the part of the file system reserved for root as a percentage.
User Space Usage (%)	The load of the part of the file system reserved for users as a percentage.
External Device Usage (%)	The load of an external device as a percentage. This chart is only displayed if an external device was mounted.

The display covers the period of the past two hours. If you move the cursor over a value in the chart, the date and time are displayed for this value.

8.8.3 Updating the firmware or software

NOTICE**Updating devices with hardware release 1**

Devices with hardware release 1 cannot check all components involved in the boot process for integrity and therefore do not support the Secure Boot function.

The firmware as of version 3.0 supports Secure Boot. To install firmware of the version 3.0 on a device with hardware release 1, the following requirements must be met:

- The device has a bootloader and a Rescue system with version 2.1.
- The update must be performed via the Rescue system.
- A specific update package that is provided for this special case is used.

During this update, all data (configuration data, applications and user data) on the SCALANCE LPE is deleted.

A backup of the configuration files for devices with firmware version 2.1 cannot be used for a device with firmware version 3.0.

When the firmware is updated from version 2.1 to version 3.0, the boot process of the SCALANCE LPE is also reconfigured. After this update, it is no longer possible to downgrade to versions $\leq$ V2.1.

NOTICE**Observe information on new firmware version**

The improper use of a new firmware can lead to a malfunction or to failure of the device.

When updating to a new firmware version, consider all information to be published for this firmware version. Information on the firmware is available from Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

NOTICE**Danger of damage to property**

If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded. Do not switch off the device during the reboot after loading the firmware. The firmware update is not complete until you are able to log in after the device has restarted. If the power supply is interrupted during the reboot, the device may not be functional any longer. Such a functional disruption can only be remedied with the help of our technical support.

Note**Data loss during a firmware update**

When you perform a firmware update in regular operation as described below, all data that is **not** in the following directories is lost:

- /userdata
- /home
- /etc
- /var/log

After the update, you need to save this data in the corresponding directories again.

Note

Any programs previously installed by the user are lost during a firmware update. You must reinstall these programs after the firmware update.

Note

An image in ISO 9660 format is stored on the SCALANCE LPE including license terms, documentation, and the readme file. After a firmware update, this information no longer applies to the updated firmware on the device.

An ISO image suitable for the firmware is available from the Siemens Industry Online Support (SIOS) (<https://support.industry.siemens.com/cs/ww/en/ps/26683/dl>).

Note

You must have administrator rights to update firmware or software.

To update the firmware or software, do the following:

1. Navigate to **System » Firmware/software update**.
The page contains a table in the **Currently installed** section with information about the currently installed versions of the bootloader, firmware, and Rescue system.
2. To open a dialog box for selecting a file, click the button next to the **Firmware/software update** field.
3. Select the corresponding file via the dialog and click **Open**.
In the **Confirm firmware/software update?** section, the version of the selected file is displayed in the **Uploaded version** field.
4. To start the update process, click the **Confirm** button. Under the field for file selection, a bar shows the progress of the update. When the update is completed, a message to this effect is displayed.
5. To restart the system with the updated firmware or software, click the **Restart** button.

8.8.4 Web SSH

Note

You can use the Web SSH only with administrator rights.

The Web UI offers the option to access the device via an SSH connection without additional programs. This functionality is called "Web SSH". After the **System** » **Web SSH** menu is selected, the part of the browser window below the menu bar of the Web UI behaves like the terminal window of an SSH client. If the user changes to another page of the Web UI, the status of the Web SSH session is not retained. The user first needs to log in again when Web SSH is called again.

Restart shellinabox

The functionality of Web SSH is made available by the **shellinabox** service. If this service is not active, the following message is displayed after selection of the **Web SSH** menu: "Web SSH is not active. Please check shellinabox service!". Execute the following shell command to restart the **shellinabox** service:

```
sudo systemctl restart shellinabox.service
```

8.8.5 Showing applications

To show a table with the most important applications, navigate to **System** » **Applications**.

The following information is displayed in the table on this page:

Parameter	Description
-	A check box with which you select the applications that you want to start or stop.
Name	Name of the application.
Status	The status of the application (active, inactive) with specification of date and time since which the application is in this state.
Additional information	The last column contains detailed application-specific information.

8.8.6 Stopping an application

Note

You must have administrator rights to stop an application.

To stop an application, follow these steps:

1. Navigate to **System » Applications**.
2. Select the check box of the application you want to stop in the first table column. Multiple selection is possible.
The **Stop** button is enabled. If you have selected an inactive application in the first column, this button remains disabled. If you have selected inactive and active applications in the first column, all buttons are enabled.
3. Click the **Stop** button. This action only affects active applications.
A dialog box shows whether the application has been stopped. If multiple applications have been stopped, a dialog box is shown for each application.

8.8.7 Starting an application

Note

You must have administrator rights to start an application.

To start an application, follow these steps:

1. Navigate to **System » Applications**.
2. Select the check box of the application you want to start in the first table column. Multiple selection is possible.
The **Start** button is enabled. If you have selected an active application in the first column, this button remains disabled. If you have selected inactive and active applications in the first column, all buttons are enabled.
3. Click the **Start** button. This action only affects inactive applications.
A dialog box shows whether the application has been started. If multiple applications have been started, a dialog box is shown for each application.

8.8.8 Restarting an application

Note

You must have administrator rights to restart an application.

To restart an application, follow these steps:

1. Navigate to **System » Applications**.
2. Select the check box of the application you want to restart in the first table column. Multiple selection is possible.
The **Restart** button is enabled. If you have selected an inactive application in the first column, this button remains disabled. If you have selected inactive and active applications in the first column, all buttons are enabled.
3. Click the **Restart** button. This action only affects active applications.
A dialog box shows whether the application has been restarted. If multiple applications have been restarted, a dialog box is shown for each application.

8.8.9 Resetting the configuration

By resetting the configuration, all the settings you have made are overwritten by factory defaults. The software components you have installed or other changes to the device outside of the **/etc** configuration directory are retained.

Note

You must have administrator rights to reset the device.

To reset the configuration via the Web UI, follow these steps:

1. Navigate to **System » Reset configuration**.
2. Click the **Reset configuration** button. The browser shows a dialog box with the following prompt: "Confirm configuration reset?"
3. Click the **OK** button. The configuration is reset. A dialog box informs you that the login page of the Web UI will be displayed if the same IP address was assigned again.

8.8.10 Restarting the device

Note

You can only restart the device with administrator rights.

Note

If the SCALANCE LPE is connected to a SCALANCE switch via the function extender interface, the SCALANCE LPE can be restarted independently of the SCALANCE switch. When the SCALANCE switch restarts, the SCALANCE LPE also restarts.

To restart the device, follow these steps:

1. Navigate to **System » On / Off**.
2. Click the **Restart** button. The browser shows a dialog box with the following prompt: "Confirm device restart?".
3. Click the **OK** button. The device is restarted.

8.8.11 Shutting down the device

Note

You can only shut down the device with administrator rights.

To shut down the unit, do the following:

1. Navigate to **System » On / Off**.
2. Click the **Shut down** button. The browser shows a dialog box with the following prompt: "After shutdown, the device does not restart automatically. Do you confirm the device shutdown?".
3. Click the **OK** button. The device is shut down.

8.9 Backup file

Note

You can only create, load, restore, and delete backup files with administrator rights.

A backup file contains all changes made by the user to the configuration files in the **/etc** directory.

8.9.1 Displaying the existing backup files

To view the backup files present on the SCALANCE LPE, navigate to **System » Backup file**.

The **Backup file** field contains a list of backup file names. The file name contains the following items of information, separated by underscores:

- Time stamp of creation
- Firmware version
- Device name
- Type of creation

Example

20220321165745_v01.01.00.00_00.00.97_lpe9403-VPM7001325_manual

8.9.2 Creating a backup file

Note

The backup of the configuration files can only be used for devices that have the same firmware version as the device with which the backup was created.

You can exchange backup files with a client PC via the Web UI.

Follow these steps to create a backup of the configuration files:

1. Navigate to **System » Backup file**.
2. Click the **Create** button.
A dialog box is displayed for the optional entry of a password for the encryption of the backup file.
3. [Optional] If you want the backup file to be encrypted, enter a password in the two text boxes. If you do not make an entry, the backup file is not encrypted.
4. Click the **Create** button.
The Web UI window briefly displays a message indicating whether the backup file was successfully created. An additional table row with the name of the created backup file is displayed in the **Backup file** field.

8.9.3 Downloading a backup file to a client PC

To download a backup file existing on the SCALANCE LPE to a client PC, proceed as follows:

1. Navigate to **System » Backup file**.
2. In the **Backup file** field, select the name of the backup files you want to download to a client PC.
The **Download** button is enabled.
3. Click the **Download** button.
The backup file is saved in the download folder configured in the Web UI browser.

8.9.4 Uploading a backup file from a client PC

A backup file on a client PC must first be uploaded to the SCALANCE LPE before it can be restored. To upload a backup file from a client PC to the SCALANCE LPE, proceed as follows:

1. Navigate to **System » Backup file**.
2. To open a dialog box for selecting a file, click the button next to the **Upload** field.
3. In the dialog box, select the appropriate backup file and click **Open**.
The backup file will be uploaded to the SCALANCE LPE. If there is already a file with the same name on the SCALANCE LPE, it will be overwritten there. A progress bar is displayed for the load operation.

8.9.5 Restoring a backup file

You can only restore a backup file if the following requirements are met:

- The backup of the configuration files can only be used for devices that have the same firmware version as the device with which the backup was created.
- The backup file must be stored on the SCALANCE LPE. Backup files on a client PC must first be loaded onto the SCALANCE LPE before restoring.

To restore a backup file, proceed as follows:

1. Navigate to **System » Backup file**.
2. In the **Backup file** field, select the name of the backup files you want to restore.
The **Restore** button is enabled.
3. Click the **Restore** button.
A dialog box displays the file name.
4. To confirm restoring the backup file, click the **Restore** button in the dialog box.
If the backup file was successfully restored, the Web UI window briefly displays the message "The backup file was successfully loaded." In the event of an error, the message "Unable to upload backup file." is displayed.
A dialog box appears with a note to reboot the device and configure the IP address. When the address is assigned via DHCP, the login page of the Web UI appears again automatically after a restart.

8.9.6 Deleting a backup file

To delete an existing backup file on the SCALANCE LPE, proceed as follows:

1. Navigate to **System » Backup file**.
2. In the **Backup file** field, select the name of the backup files you want to delete.
The **Delete** button is enabled.
3. Click the **Delete** button.
A dialog box displays the file name.
4. To confirm the deletion of the backup file, click the **Delete** button in this dialog box.
The Web UI window briefly displays the message **Backup file deleted**.

8.10 User management

This section describes all the configuration steps for the user management. You can create and delete users in the Web UI. You can also change the role and the password of a user.

8.10.1 Displaying the users

To display the users registered for the device, navigate to **System » User management**. A list of the users is displayed.

Which users are displayed is dependent on the role with which a user has logged in:

- Users with **Admin** role see a list of all users
- Users with the **Guest** role only see their own user account.

8.10.2 Creating a new user

Note

You must have administrator rights to create new users.

To create a new user, follow these steps:

1. Navigate to **System » User management**.
2. Click the **New** button. The dialog box **Create new user** is displayed.
3. Enter the name of the new user in the **User name** text box. The user name must have the following characteristics:
 - At least 4 characters, maximum 32 characters
 - The first character must be a letter or "_".
 - The user name must not contain any special characters except "-" and "_".
4. Select the appropriate entry from the **Role** drop-down list:
5. In the **Password** text box, enter the password for the user. The password must have the following characteristics:
 - At least 12 characters, maximum 250 characters
 - At least one number
 - At least one uppercase letter
 - At least one lowercase letter
 - At least one special character: # ! \$ % & () * + , - . / : < = > @ [] ^ _ { } ~

If the password does not meet the specified criteria, the text box is framed in red. A message indicating which criterion is not met is displayed below the text box.

6. Enter the password again in the **Confirm password** input box.
7. Click the **Create** button. A small dialog box appears at the bottom edge of the browser window with a message about creation of the user account.

8.10.3 Deleting a user

Note

You must have administrator rights to delete users.

The logged-in user can delete all users listed in the table except for his own user account.

To delete users, follow these steps:

1. Navigate to **System » User management**.
2. The first column of the table contains a check box for each user. Select this check box for the user you want to delete. Multiple selection is also possible. The previously disabled **Delete** button is enabled.
3. Click the **Delete** button. The user(s) selected beforehand are deleted from the table. A small dialog box appears at the bottom edge of the browser window for each deleted user with a message about the deletion. Even if the check box was selected for the logged-in user, this user is not deleted.

8.10.4 Changing the role of a user

Note

You must have administrator rights to change the role of a user.

The logged-in user can change the role of all other users except for their own role: A user with **Administrator** role can be given the **Guest** role, and vice versa.

To change the role of a user, follow these steps:

1. Navigate to **System » User management**.
2. Click the icon in the **Change** column in the table row of the user whose role you want to change.
The **Change user data** dialog box is displayed.
3. Select the desired entry from the **Role** drop-down list.
4. Click the **Save** button.
The new role is applied to the table. A small dialog box appears at the bottom edge of the browser window for each changed role with a message about the change.

8.10.5 Changing the password of a user

Note

Users with **Administrator** role can change the password for all users. Users with **Gast** role can only change their own password.

To change the password of a user, follow these steps:

1. Navigate to **System » User management**.
2. Click the icon in the **Change** column in the table row of the user whose role you want to change.
The **Change user data** dialog box is displayed.
3. Enter the new password in the **Password** text box. The password must have the following characteristics:
 - At least 12 characters, maximum 250 characters
 - At least one number
 - At least one uppercase letter
 - At least one lowercase letter
 - At least one special character: # ! \$ % & () * + , - . / : < = > @ [] ^ _ { } ~If the password does not meet the specified criteria, the text box is framed in red. A dot is displayed in the text box for each character of the password.
4. Enter the new password in the **Confirm password** text box.
5. Click the **Save** button. A small dialog box appears at the bottom edge of the browser window with a message about the change that was made.

8.11 Syslog events

Syslog according to RFC 3164 (BSD Syslog Protocol) is used for transferring short, unencrypted text messages over UDP in the IP network. The prerequisite is that the network contains a syslog server that receives the log entries. Since this involves a UDP connection, there is no acknowledgment to the sender.

8.11.1 Configuring the syslog server

Note

You must have administrator rights to configure the syslog server.

To configure the syslog server, follow these steps:

1. Navigate to **System » Syslog events**.
2. In the **Name** text box, enter a name for the syslog server where the log entries are to be saved.
3. In the **IP address Syslog server** text box, enter the IP address or FQDN of the syslog server.
4. In the **UDP port** text box, enter the input port of the syslog server.
Value range: 0 ... 65535
Default: 514
5. Click the **Apply** button. If invalid values are entered, the **Apply** button remains disabled.

To cancel the entry, click the **Cancel** button.

To delete the configuration for the syslog server, click the **Delete** button.

8.11.2 Configuring the directory for syslog messages

Note

You must have Administrator rights to configure the directory for syslog messages.

To configure the directory for the syslog messages, follow these steps:

1. Navigate to **System » Syslog events** and section **Logbook**.
2. In the **Internal path for Syslog** text box, enter the path and the name for the file in which the syslog messages are to be saved. The path must begin with "/" and end with the file name extension **.log**.

The file with the syslog messages cannot be saved in one of the following directories:

- **/etc**
- **/proc**
- **/sys**
- **/root**
- **/bin**
- **/sbin**

3. Click the **Apply** button. If invalid values are entered, the **Apply** button remains disabled.

To cancel the entry, click the **Cancel** button.

To delete the configuration for the internal syslog directory, click the **Delete** button. The previously configured file is retained.

8.11.3 Displaying syslog messages

To display syslog messages, follow these steps:

1. Navigate to **System » Syslog events**. Up to 15 messages are displayed in the **Logbook** section. You can make additional messages visible with the scrollbar at the right edge of the display box.
2. To update the display, click the **Show Syslog** button.
3. To search for specific text in the syslog messages, enter it in the text box at the upper edge of the display box. Then, only rows containing the searched for text can be seen in the display box. The searched for text is highlighted in color.
Only the syslog messages that are currently being displayed are searched. The syslog file may contain additional messages.

8.11.4 Deleting syslog messages

Note

You must have administrator rights to delete syslog messages.

To delete the content of the log file and thus all messages from the display box, follow these steps:

1. Navigate to **System » Syslog events** and section **Logbook**.
2. Click the **Delete messages** button. A dialog box with the **Cancel** and **Continue** buttons is displayed.
3. To delete the content of the log file, click the **Continue** button.

8.11.5 Downloading syslog messages

To save syslog messages on the client PC, follow these steps:

1. Navigate to **System » Syslog events** and section **Logbook**. The **Internal path for Syslog** text box shows the file in which the syslog messages are saved.
2. Click the **Download Syslog** button. The file with the syslog messages is saved in the download folder that is configured in the browser.

8.12 System time

SCALANCE LPE supports time synchronization according to the NTP and Secure NTP standards. This section describes how to configure one or more time servers with which SCALANCE LPE is synchronized. If the device is not to synchronize its system time with an external server, you can disable NTP. You can also configure the system time manually independent of a time server.

8.12.1 Configuring NTP

Note

You must have administrator rights to configure NTP.

To configure NTP, follow these steps:

1. Navigate to **System » System time**, under **Network Time Protocol**.
2. [Optional] The **NTP client** option is enabled by default. If the default setting is not active, enable this option.
3. Five time servers are preconfigured in the table in the delivery state. If you want to use a different time server, you need to change an existing entry.
Click the icon in the **Change** column in the table row of the time server you want to change. The **Configure NTP server** dialog box is displayed.
4. Select the **Active** check box if the SCALANCE LPE is to synchronize with this time server.
5. Enter the IP address or the name of an NTP server in the **IP address/FQDN** box.
6. If you want faster time synchronization the first time a connection is established, select the **iBurst enabled** check box.
7. Click the **Save** button.
8. Click the **Apply** button.
This configuration is applied to the file **/etc/ntpsec/ntp.conf**.
A small dialog box appears at the bottom edge of the browser window with a message regarding the configuration of the NTP server.

8.12.2 Configuring Secure NTP

Note

You must have administrator rights to configure Secure NTP.

To configure Secure NTP, follow these steps:

1. Navigate to **System » System time**, under **Network Time Protocol**.
2. The **NTP client** option is enabled by default. Enable the **Secure NTP client** option.
A row for configuring the secure NTP server is added to the table with the time servers.

Note

If you select the NTP client check box, the row for the NTP secure server is no longer shown in the table. If a secure NTP server has been configured, the configuration data is retained in the **/etc/ntpsec/ntp.conf** and **/etc/ntpsec/ntp.keys** files. This data is displayed when you select the **Secure NTP client** check box.

3. Click the icon in the **Change** column in the table row of the secure NTP server.
The **Configure secure NTP server** dialog box is displayed.

4. Enter the IP address or the name of an NTP server in the **IP address/FQDN** box.
5. If you want faster time synchronization the first time a connection is established, select the **iBurst enabled** check box.
6. Enter a number for the key in the **Key ID** text box.
Value range: 1 ... 65535
7. Select one of the following encryption algorithms for Secure NTP from the **Algorithm** drop-down list:
 - SHA256
 - SHA512 (default)
 - SHA3-256
 - SHA3-512
 - AES-128
 - AES-256
8. Enter a key for Secure NTP in the **Key** text box. A Secure NTP client can only be synchronized with an NTP server for which a suitable algorithm and key has been configured under the specified key ID.
9. Click the **Save** button.
10. Click the **Apply** button.
The server address and the **Key ID** are applied to the `/etc/ntpsec/ntp.conf` file.
The **Key ID**, **algorithm** and **key** are found in file `/etc/ntpsec/ntp.keys`.
A small dialog box appears at the bottom edge of the browser window with a message regarding the configuration of the NTP server.

8.12.3 Disabling NTP

Note

You can only disable NTP with administrator rights.

To disable NTP, do the following:

1. Navigate to **System » System time**, under **Network Time Protocol**.
2. Enable the **No NTP** option button.
The table with the data for the NTP server or secure NTP server is disabled.
3. Click the **Apply** button.
4. A small dialog box appears at the bottom edge of the browser window with a message indicating that the configuration has been applied.

8.12.4 Configuring the system time manually

Note

You can only configure the system time with administrator rights.

Follow these steps to configure the system time manually:

1. Navigate to **System** » **System time**, under **Manual setting**.
2. In the **Date** input box, enter the desired date in the format **YYYY-MM-DD** (according ISO 601).
[Optional] Click the button with the calendar symbol next to the **Date** input box. Select the suitable date in the month calendar that is displayed.
3. Enter the local time in the **Time** input boxes.
[Optional] Click the buttons with the arrow symbols to select hours and minutes.
4. [Optional] Click the **Use PC Time** button. The system time of the PC is applied as local time for the SCALANCE LPE.
5. Click the **Apply** button.
A small dialog box appears at the bottom edge of the browser window with a message indicating that the configuration has been applied.
6. In the **Time zone** drop-down list, select the time zone for the device location.
7. Click the **Apply** button.
A small dialog box appears at the bottom edge of the browser window with a message indicating that the configuration has been applied.

The configured values are shown for the following parameters in the **System Time** section:

- **Coordinated Universal Time UTC**
The time in the time zone of the zero meridian.
- **Local time**
The time at the device location.
- **Time zone**
The time zone for the device location.

8.13 SNMP

You can find general information on SNMP in sections Linux Shell » SNMP (Page 100) and Linux Shell » Data security with SNMP (Page 102).

8.13.1 Creating an SNMPv3 user

Note

You must have administrator rights to create SNMPv3 users.

To create a new SNMPv3 user, follow these steps:

1. Navigate to **System » Simple Network Management Protocol v3**.
2. Click the **New** button.
The **Create new user** dialog box appears.
3. Enter the name of the new user in the **User name** text box.
The user name must have the following characteristics:
 - At least 4 characters, maximum 32 characters
 - The first character must be a letter or "_".
 - The user name must not contain any special characters except "-" and "_".
4. Select one of the following values from the **Hash function** drop-down list:
 - SHA-512 (Default)
 - SHA-384
 - SHA-256
 - SHA-224

Note

If the hash functions **MD5** and **SHA** functions were configured for SNMPv3 users, the **NONE** value is shown for the hash function Web UI. This can be the case when SNMPv3 users were created with the Shell command **net-snmp-create-v3-user**. MD5 and SHA cannot be selected in the Web UI.

5. Select one of the following values from the **Encryption method** drop-down list:
 - AES (default)
 - DES
6. In the **Authentication password** text box, enter the password for authentication of the user.
The password must have the following characteristics:
 - At least 12 characters, maximum 250 characters
 - At least one number
 - At least one uppercase letter
 - At least one lowercase letter
 - At least one special character: # \$ % & () * + , - . / : < = > @ [] ^ _ { } ~

If the password does not meet the specified criteria, the text box is framed in red. A message indicating which criterion is not met is displayed below the text box.

7. In the **Encryption password** text box, enter the password for encryption of the user. The password must meet the same criteria as the **Authentication password**. If the password does not meet the specified criteria, the text box is framed in red. A message indicating which criterion is not met is displayed below the text box.
8. Click the **Create** button.
A row for the new user is added to the table. A corresponding message is displayed at the bottom edge of the browser window.
If this button is disabled, it means that values for one or more parameters are invalid.

8.13.2 Changing the data of an SNMPv3 user

Note

You must have administrator rights to change the data of an SNMPv3 user.

To change the data of an SNMPv3 user, follow these steps:

1. Navigate to **System » Simple Network Management Protocol v3**.
2. Click the icon in the **Change** column in the table row of the user whose data you want to change.
The **Change user data** dialog box is displayed.
3. Enter new data in the text boxes or select other values in the drop-down lists.
4. Click the **Save** button.
A small dialog box appears at the bottom edge of the browser window with a message about the change that was made.

8.13.3 Deleting an SNMPv3 user

Note

You must have administrator rights to delete SNMPv3 users.

To delete an SNMPv3 user, follow these steps:

1. Navigate to **System » Simple Network Management Protocol v3**.
2. Select the check box in the first table column for the user you want to delete.
3. Click the **Delete** button.
The table row for this user is removed. A corresponding message is displayed at the bottom edge of the browser window.

8.14 SFTP

Note

You must have administrator rights to configure and use SFTP.

You can find general information on SFTP in section Linux Shell » SFTP (Page 108).

8.14.1 Configuring an SFTP connection

The prerequisite for file transfer is the establishment of an SFTP connection between the client and server. The IP address of the SFTP server must be known for this. In addition, you must have a user account with corresponding rights on the target system.

To configure an SFTP connection, follow these steps:

1. Navigate to **System » SSH File Transfer Protocol**.
2. In the **Remote system user name** text box, enter the name you use to access the SFTP server. The user name must not contain any special characters except the characters "_" and "-".
3. In the **Password** text box, enter the password of this user.
4. In the **IP address of SFTP server** text box, enter the IPv4 address or FQDN of the SFTP server you want to access.
5. In the **Port** text box, enter the number of the port the server uses for SFTP.
Value range: 1 ... 65535
Default: Port 22

To delete the configured values, click the **Cancel** button. This button is disabled if you open another page of the Web UI.

8.14.2 Downloading a file

The prerequisite for file transfer is a configured SFTP connection. For more information, refer to "Configuring an SFTP connection (Page 158)". To download a file, follow these steps:

Note

Paths and file names must not contain any special characters, except the following:

- "/"
 - "."
 - "-"
 - " "
-

1. Navigate to **System » SSH File Transfer Protocol**, section **Download file from a remote system (get)**.
2. In the **Remote system path** text box, enter the path of the file location on the SFTP server.

3. In the **Remote system file** text box, enter the name of the file you want to download.
4. In the **Local path** text box, enter the path of the file location on the client device.
5. To start the download click the **get** button.
If this button is disabled, it means that values for one or more parameters in section **SSH File Transfer Protocol** or section **Download file from a remote server (get)** are invalid. A message indicating if the download was successful is displayed at the bottom edge of the browser window.
The display box in section **Log messages** contains the output of the **get** command. The information in this box is not saved. When the page is reloaded or the user closes the session, this information is no longer available.

8.14.3 Uploading a file

The prerequisite for file transfer is a configured SFTP connection. For more information, refer to "Configuring an SFTP connection (Page 158)". To upload a file, follow these steps:

Note

Paths and file names must not contain any special characters, except the following:

- "."
 - "-"
 - " "
-

1. Navigate to **System » SSH File Transfer Protocol**, section **Upload file to a remote system (put)**.
2. In the **Local path** text box, enter the path of the file location on the client device.
3. In the **Local file** text box, enter the name of the file you want to upload.
4. In the **Remote system** text box, enter the path of the file location on the SFTP server.
5. To start the upload, click the **Put** button.
If this button is disabled, it means that values for one or more parameters in section **SSH File Transfer Protocol** or section **Upload file to a remote server (put)** are invalid. A message indicating if the upload was successful is displayed at the bottom edge of the browser window.
The display box in section **Log messages** contains the output of the **put** command. The information in this box is not saved. When the page is reloaded or the user closes the session, this information is no longer available.

8.15 Docker

The Docker software facilitates the installation and management of applications through the combination of all libraries and other components of an application in "Docker images". This section describes the basic steps for using Docker containers.

You can find additional information on the Docker homepage (<https://www.docker.com/>).

Note

If the firewall configuration has been reloaded (for example, with the command `sudo firewall-cmd --reload`), connections to Docker containers may be lost. To resolve the error, do one of the following:

- Restart the SCALANCE LPE.
- Restart Docker (for example, with the command `sudo systemctl restart docker`)

All Docker components (Containers, Networks, Volumes, Images, Bind Mounts, etc.) are saved in the `/userdata/docker` directory. The contents of this directory are also retained in the event of a firmware update.

8.15.1 Displaying Docker Containers configured in the device

To display the Docker containers stored in the device, navigate to **Docker » Containers**. The table displays the following information for each Docker container:

Parameter	Description
Container ID	The unique ID that is assigned automatically to the container when it is created.
Image	The Docker image that was executed in this container.
Command	The command with which the Docker container was started.
Created	The time since the Docker container started.
Status	Shows whether the Docker container is still running or when it was ended.
Ports	IP port mappings of the Docker container.
Name	The name of the Docker container.
Details	Link to section Output/Configuration/Statistics

The Web UI offers two ways to display detailed information on a Docker container:

- Click an entry in the **Container ID** column. The page with detailed information for the selected Docker container is displayed.
- Click the "i" icon in the **Details** column. The section **Output/Configuration/Statistics** on the page with detailed information for the selected Docker container is displayed.

Section "Docker Container Details"

Parameter	Description
Container ID	The unique ID that is assigned automatically to the container when it is created.
Name	The name of the Docker container.
Status	Shows the current status of the Docker container.
Created	The time since the Docker container started.

Parameter	Description
Image	The Docker image that was executed in this container.
Command	The command with which the Docker container was started.

Note

The contents of the **Image** row are highlighted and linked to the **Docker Image Details** page. You can find a description of this page in the following section: "Displaying Docker Images saved in the device (Page 164)"

Section "Docker Container Volumes"

Parameter	Description
Volume name	The name of the volume.
Path in container	The mount point of the volume in the container.

Note

The contents of the **Volume name** column are highlighted and linked to the **Docker Volume Details** page. You can find a description of this page in the following section: "Displaying Docker Volumes (Page 165)"

Section "Docker Container Networks"

Parameter	Description
Name	The network name. The bridge, host and none networks are created automatically by Docker.
Network ID	The unique ID that is assigned automatically to the network when it is initialized.
IP address	The IP address of the container.
Gateway	The gateway of the container.
MAC Address	The MAC address of the container.

Note

The contents of the **Name** column are highlighted and linked to the **Docker Network Details** page. You can find a description of this page in the following section: "Displaying Docker Networks (Page 165)"

Section "Output/Configuration/Statistics"

This section contains the following three tabs:

- **Output**
The window in this tab contains the text that is output when shell command `sudo docker logs <Container ID>` is run.
You can use the **Download** button to download the content of the window to a client PC. The text file is saved in the download folder that is configured in the browser.
- **Configuration**
The window in this tab contains detailed information about the configuration of the Docker container. The content of the window corresponds to the output of the shell command `sudo docker inspect <Container ID>`.
You can use the **Download** button to download the content of the window to a client PC. The text file is saved in the download folder that is configured in the browser.
- **Statistics**
This page contains multiple charts that display the following values:

Parameter	Description
Memory (%)	Utilization of the work memory in percent.
CPU (%)	The average utilization of the processor in percent.
Network RX (MB) Network TX (MB)	The read or write data transfer over the network in megabytes.
Read I/O (MB) Write I/O (MB)	The data volume of read or write operations of the CPU in megabytes.

The content of the window corresponds to the output of the shell command `sudo docker stats <Container ID>`.

8.15.2 Starting a Docker container

To start a Docker container, follow these steps:

1. Navigate to **Docker » Containers**.
2. Select the check box in the first table column for the Docker container you want to start. If the Docker container is not running, the **Start** button is enabled.
3. Click the **Start** button. This has the same effect as the shell command `docker start <Container ID>`.
The **Status** column shows that the Docker container was started.

8.15.3 Stopping a Docker container

To stop a Docker container, follow these steps:

1. Navigate to **Docker » Containers**.
2. Select the check box in the first table column for the Docker container you want to stop. If the Docker container is running, the **Stop** button is enabled.
3. Click the **Stop** button. This has the same effect as the shell command `docker stop <Container ID>`.
The **Status** column shows that the Docker container was stopped.

8.15.4 Restarting a Docker container

To restart a Docker container, follow these steps:

1. Navigate to **Docker » Containers**.
2. Select the check box of the Docker container you want to restart in the first table column. If the Docker container is running, the **Restart** button is enabled.
3. Click the **Restart** button. This has the same effect as the shell command `docker restart <Container ID>`.
The **Status** column shows that the Docker container was restarted.

8.15.5 Killing the execution of a Docker container

To kill the execution of a Docker container, follow these steps:

1. Navigate to **Docker » Containers**.
2. Select the check box in the first table column for the Docker container you want to kill. If the Docker container is running, the **Cancel** button is enabled.
3. Click the **Cancel** button. This has the same effect as the shell command `docker kill <Container ID>`.
The **Status** column shows that the Docker container was killed.

8.15.6 Interrupting the execution of a Docker container

To interrupt the execution of a Docker container, follow these steps:

1. Navigate to **Docker » Containers**.
2. Select the check box of the Docker container you want to interrupt in the first table column. If the Docker container is running, the **Interrupt** button is enabled.
3. Click the **Interrupt** button. This has the same effect as the shell command `docker pause <Container ID>`.
The **Status** column shows that the execution of the Docker container was interrupted.

8.15.7 Resuming the execution of a Docker container

To resume the execution of a Docker container, follow these steps:

1. Navigate to **Docker » Containers**.
2. Select the check box of the Docker container you want to resume in the first table column. If the Docker container is running, the **Resume** button is enabled.
3. Click the **Resume** button. This has the same effect as the shell command `docker unpause <Container ID>`.
The **Status** column shows that the execution of the Docker container was resumed.

8.15.8 Deleting a Docker container

To delete one or more Docker containers, follow these steps:

1. Navigate to **Docker » Containers**.
2. Select the check box of the Docker container you want to delete in the first table column. If the containers are not running, the **Delete** button is enabled.
3. [Optional] If a Docker container is running, click the **Stop** button and once again select the check box in the first table column for the Docker container you want to remove.
4. Click the **Delete** button. This has the same effect as the shell command `docker rm <Container ID>`.
The associated rows are deleted from the table.

8.15.9 Displaying Docker Images saved in the device

To display the Docker images stored in the device, navigate to **Docker » Images**. The table displays the following information for each Docker Image:

Parameter	Description
Image ID	The unique ID that is assigned automatically to the Image when it is created.
Repository	The name of the Docker Repository for this Image.
Tag	The version of the Image.
Created	The time since the Image was created.
Size	The size of the Image.

To display detailed information on a Docker image, click an entry in the **Image ID** column. The page displays the following information for the selected Docker Image:

Section "Docker Image Detail"

Parameter	Description
Image Name	The name of the Image.
Size	The size of the Image.

Parameter	Description
Created	The time at which the Image was created.
Build	The Build number of the Image.

If you click the text **See more** at the bottom of the page, you can show more information. When you click the text **See less**, you hide the additional information.

8.15.10 Displaying Docker Volumes

SCALANCE LPE stores Docker volumes in the `/userdata/docker/volumes` directory. To display the existing Docker volumes, navigate to **Docker » Volumes**. The table displays the following information for each Docker volume:

Parameter	Description
Volume name	The name of the Docker volume.
Driver	The Volume driver used.

To display detailed information on a Docker volume, click an entry in the **Volume name** column. The page displays the following information for the selected Docker image:

Section "Docker Volume Details"

Parameter	Description
Volume Name	The name of the Docker volume.
Mount Path	The mount point of the Docker volume.
Created	The time at which the Docker volume was created.
Driver	The Volume driver used.

If you click the text **See more** at the bottom of the page, you can show more information. When you click the text **See less**, you hide the additional information.

8.15.11 Displaying Docker Networks

To display the Docker networks of the device, navigate to **Docker » Networks**. The table displays the following information for each Docker network:

Parameter	Description
Name	The network name. The bridge, host and none networks are created automatically by Docker.
Network ID	The unique ID that is assigned automatically to the network when it is initialized.
Driver	The network driver used.
Scope	The domain of the network driver.
Created	Time at which the network was configured.
Subnet	If no IP address is specified when creating a container, Docker assigns an IP address from this subnet

To display detailed information on a Docker network, click an entry in the **Name** column. The page displays the following information for the selected Docker network:

Section "Docker Network Details"

Parameter	Description
Name of the network	The network name. The bridge, host and none networks are created automatically by Docker.
Network ID	The unique ID that is assigned automatically to the network when it is initialized.
Driver	The network driver used.
Scope	The domain of the network driver.
Attachable	<ul style="list-style-type: none">• true Docker containers can be added to the network.• false No Docker containers can be added to the network.
Internal	<ul style="list-style-type: none">• true External access to the network is not possible.• false External access to the network is possible.

If you click the text **See more** at the bottom of the page, you can show more information. When you click the text **See less**, you hide the additional information.

8.15.12 Displaying information via Docker

To display information about the Docker installation of the device, navigate to **Docker** » **Information**. The Web UI page contains the following two sections:

- **Information**
Information on the hardware of the SCALANCE LPE and the parameters of the Docker installation.
- **Version**
Version information on the Docker installation

8.16 Docker installations

8.16.1 Installing Zscaler ZPA App Connector

Web UI provides a simplified installation of the **Zscaler Private Access** (ZPA) application that manages and secures access to the SCALANCE LPE. This is done by installing the **Zscaler ZPA App Connector** on the device. Required for the installation is an appropriate license from Zscaler Inc.

Note

The Zscaler ZPA App Connector cannot be used without the **Zscaler Cloud Tenant** application.

Note

Before downloading and installing, check that the use is permitted in the intended country of use.

To install the Zscaler ZPA App Connector on the SCALANCE LPE, follow these steps:

1. Ensure that there is a connection between the SCALANCE LPE and the Internet.
2. Navigate to **Docker » Installation**.
3. To create a **provisioning key** for SCALANCE LPE, click the link to Zscaler Zscaler (<https://help.zscaler.com/zpa/about-connector-provisioning-keys>) in the **Zscaler installation** section and follow the description on this Internet page.
4. Enter the created key in the **Provisioning key** text box.
5. Click the **Install and Start Zscaler App Connector** button.

The following command is executed automatically:

```
sudo docker run -d \  
  --cap-add cap_net_admin \  
  --cap-add cap_net_bind_service \  
  --cap-add cap_net_raw \  
  --cap-add cap_sys_nice \  
  --cap-add cap_sys_time \  
  --restart always \  
  --name lpe9403_zscaler \  
  -e ZPA_PROVISION_KEY="<Provisioning key>" \  
  zscaler/zpa-connector:latest.arm64
```

If you want to install a version other than **latest**, you must install the Zscaler ZPA App Connector using the shell.

Once the image is downloaded, the container is immediately launched along with the inserted provisioning key.

8.16.2 Installing Nozomi Remote Collector

Web UI provides a simplified installation of the **Nozomi Remote Collector** application, which collects and prepares plant and network data. Required for the installation is an appropriate license from Nozomi Networks Inc.

Note

The **Nozomi Remote Collector** cannot be used without the **Nozomi Guardian** application.

Note

Before downloading and installing, check that the use is permitted in the intended country of use.

Required is an installation file for the Nozomi Remote Collector, which is available on the SCALANCE LPE in factory state. This file can be deleted if you do not want to install the Nozomi Remote Collector or once the installation has been completed.

The installation file for the Nozomi Remote Collector is not a component of the firmware. If the firmware has been updated via the Rescue system, you first need to upload the installation file for the Nozomi Remote Collector to the SCALANCE LPE and save it in the **/userdata** directory.

The installation file for the Nozomi Remote Collector is also available from **Siemens Industry Online Support** SIOS (<https://support.industry.siemens.com>).

To install the Nozomi Remote Collector on the SCALANCE LPE, proceed as follows:

1. Ensure that there is a connection between the SCALANCE LPE and the Internet.
2. Navigate to **Docker » Installation**.
3. In the **Nozomi Networks Remote Collector installation** section, click the **Install Nozomi** button.
The required files are downloaded from the Internet, the build process of Docker starts. This process can take up to 30 minutes.
4. Navigate to **Docker » Images**.
If the Docker image is successfully created, you will find a row for Nozomi Remote Collector in the table on this page.
5. Navigate to **System » Web SSH** and configure the installed Nozomi Remote Collector according to the manufacturer's instructions.

8.16.3 Deleting the installation file of the Nozomi Remote Collector

SCALANCE LPE contains an installation file for the Nozomi Remote Collector in the factory state. This file can be deleted if you do not want to install the Nozomi Remote Collector or once the installation has been completed.

Deleting the installation file for the Nozomi Remote Collector does not affect a Docker image already created with this installation file. The functionality of the Nozomi Remote Collector application is not affected.

To delete the Nozomi Remote Collector installation file, do the following:

1. Navigate to **Docker » Installation**.
2. In the **Nozomi Networks Remote Collector installation** section, click the **Delete installation file** button.
3. Confirm the deletion of the file in the dialog box that appears.

Applications

SCALANCE LPE uses Debian GNU/Linux as the operating system. This means you can run your own applications for Debian GNU/Linux on the device. This section describes what you must observe when using your own applications.

Note

The export markers defined for the SCALANCE LPE are valid for the device in the factory state. If applications are added to the SCALANCE LPE, the export identifier of the overall system can change and necessitate a new export rating.

9.1 Use of software packages for the Debian GNU/Linux operating system

You can use software packages developed for the Debian GNU/Linux operating system and compiled for the ARM64 architecture on SCALANCE LPE. We recommend the Advanced Packaging Tool (APT) for the efficient installation and management of these programs. APT supports the Debian package format (file name extension ".deb") and is comparable to the RPM Package Manager for RPM packages. APT can be used directly via command line programs. There is also the Aptitude front end for the console. When a software package already exists on the SCALANCE LPE, you can also use the **dpkg** (Debian Package) program directly for the installation.

Example 1. Installation of a deb package from the local directory

dhex is a Hex editor for the console. In this example, the **dhex_0.69-1_arm64.deb** software package is located in the **/home/admin** directory. To install the software, run the following command:

```
admin@lpe9403-VPM7001325:~$ sudo dpkg -i dhex_0.69-1_arm64.deb
[sudo] password for admin:
Selecting previously unselected package dhex.
Reading database ...
Preparing to unpack dhex_0.69-1_arm64.deb ...
Unpacking dhex (0.69-1) ...
Setting up dhex (0.69-1) ...
```

Example 2. Installation of a deb package from the Debian repository

htop is a task manager for the console. The **htop-2.2.0-1+b1** software package is available in the Debian software directory. Before you install the program, you must update the software directory:

```
admin@lpe9403-VPM7001325:~$ sudo apt update
Hit:1 http://deb.debian.org/debian buster InRelease
Hit:2 http://deb.debian.org/debian-security buster/updates InRelease
Hit:3 http://deb.debian.org/debian buster-updates InRelease
Hit:4 https://download.docker.com/linux/debian buster InRelease
Reading package lists... Done
```

9.2 Updating program packages

```
Building dependency tree
Reading state information... Done
78 packages can be upgraded. Run 'apt list --upgradable' to see
them.

To install the software, run the following command:
admin@lpe9403-VPM7001325:~$ sudo apt install htop
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  lsof strace
The following NEW packages will be installed:
  htop
0 upgraded, 1 newly installed, 0 to remove and 78 not upgraded.
Need to get 82.7 kB of archives.
After this operation, 217 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main arm64 htop arm64
2.2.0-1+b1 [82.7 kB]
Fetched 82.7 kB in 0s (938 kB/s)
debconf: unable to initialize frontend: Dialog
debconf: (No usable dialog-like program is installed, so the dialog
based frontend cannot be used. at /usr/share/perl5/Debconf/FrontEnd/
Dialog.pm line 76, <> line 1.)
debconf: falling back to frontend: Readline
Selecting previously unselected package htop.
(Reading database ... 19628 files and directories currently
installed.)
Preparing to unpack .../htop_2.2.0-1+b1_arm64.deb ...
Unpacking htop (2.2.0-1+b1) ...
Setting up htop (2.2.0-1+b1) ...
```

9.2 Updating program packages

Debian GNU/Linux regularly distributes new versions of software packages to fix bugs or close security vulnerabilities. You can update program packages you have installed yourself with the package manager when a new version is available. In the factory setting, security updates are only displayed for installed packages.

Note

Updating the pre-installed packages

Because Siemens cannot check pre-installed packages for compatibility after updates, we do not recommend such updates. If you update pre-installed packages at your own risk, however, Siemens does not guarantee the continued fault-free function of the device.

You need the following commands for updating:

- `sudo apt update`
Updates the software directory. The command also shows for how many packages newer versions are available:
8 packages can be upgraded. Run '`apt list --upgradable`' to see them.
- `sudo apt list --upgradable`
Shows which packages can be upgraded as well as their old and new versions.
Use the list to verify which packages are affected. You have the following options for updating the packages:
 - `sudo apt install <paket1> [<paket2> ...]`
Updates individual packages and, if necessary, dependencies between the packages.
 - `apt-mark hold <paket>`
Sets the "hold" status for a package. This means the listed package is exempt from updates. You can update the package again when you remove the "hold" selection.

NOTICE

Overwriting the firmware by updating the system

The Advanced Packaging Tool (APT) and other systems for package management give you the option to update the entire operating system or install a newer version of the operating system. In this case, parts of the firmware of the SCALANCE LPE are also overwritten. The device may **no longer be functional** after the update.

Therefore, you should **not** use any commands that change multiple program packages automatically.

For APT, these are the following commands, among others:

```
apt upgrade
apt full-upgrade
apt autoremove
apt-get upgrade
apt-get dist-upgrade
aptitude upgrade
aptitude full-upgrade
aptitude safe-upgrade
```

9.3 Using your own applications

NOTICE

Device failure in case of program errors

When you use applications on the SCALANCE LPE that you have written yourself, program errors may result in a complete failure of the device. This means the operating system may not work without errors any longer. This can lead to consequential damages, such as the loss of data.

We recommend using the Docker virtualization software for your own applications. If applications in a Docker container fail, this does not affect the operating system. For more information on Docker, see "Docker (Page 159)".

9.4 Reverse proxy

The Web User Interface of the SCALANCE LPE is a client-server application that uses the HTTP server of the device. Depending on the use case of the SCALANCE LPE, it may be necessary to use custom server applications. For this purpose, the device offers reverse proxy functionality based on the nginx program package.

If you want to use your own server application, you need to define a new endpoint in the `/etc/edgebox_web_app/nginx/includes/config/custom/endpoint.conf` configuration file.

Example

Access to a server application should be configured with the following parameters:

- Program name: **myServer**
- Port number: **2000**

Add the following entry in the `/etc/edgebox_web_app/nginx/includes/config/custom/endpoint.conf` file:

```
location /myServer {  
    proxy_pass https://localhost:2000;  
}
```

After this change, the web page of the server can be reached with the following input:
<IP address>/myServer

Appendix A "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 sudo su userdel groupdel ssh http useradd
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

Parameter	Description	Possible values or example
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
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.1 Human user identification and authentication

{Protocol}: User {user name} logged in.

Example	https / ssh: User admin logged in.
Explanation	Valid login information that is specified during login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {user name} failed to log in.

Example	https / ssh: User admin failed to log in.
Explanation	Incorrect user name or password specified during login.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} logged in from {IP address}.

Example	https / ssh: User admin logged in from 192.168.0.1.
Explanation	Valid login information that was specified during login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} failed to log in from {IP address}.

Example	https / ssh: User admin failed to log in from 192.168.0.1.
Explanation	Incorrect user name or password specified during login.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {user name} logged out.

Example	https / ssh: User admin logged out.
Explanation	User session ended - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} logged out from {IP address}.

Example	https / ssh: User admin logged out from 192.168.0.1.
Explanation	Session ended with user logout.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

A.2 User account management

{Protocol}: User {User name} disabled user-account {Destination user name}.

Example	usermod: User root disabled user-account user1.
Explanation	An authenticated user blocks the user account of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Default admin account was changed to {User name}.

Example	Default admin account was changed to maier.
Explanation	The default administrator account was changed.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} created user-account {Destination user name} with role {Role}.

Example	useradd: User admin created user-account admin2 with role Administrator.
Explanation	A user has created a user account and has assigned a user profile to the account. In the example, the "admin" user created the "admin2" user account and assigned the "Administrator" user profile to the account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} deleted user-account {Destination user name}.

Example	userdel: User admin deleted user-account admin2.
Explanation	A user has deleted an existing user account. In the example, the "admin" user deleted the "admin2" user account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} changed user-account {Destination user name} with role {Role}.

Example	usermod: User admin changed user-account admin3 with role Administrator.
Explanation	The administrator has changed an existing account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} enabled user-account {Destination user name}.

Example	usermod: User admin enabled user-account user1.
Explanation	An authenticated user enables the user account of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: Password changed for user {User name}.

Example	usermod: Password changed for user user1.
Explanation	A user password has been changed. The password of the user1 user was changed in this example.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

A.3 Identifier management

{Protocol}: User {User name} created group {Group} and assigned to role {Role}.

Example	groupadd / ssh / Console: User root 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

{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.

Example	userdel / groupdel / ssh / Console: User admin 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

A.4 Nonrepudiation

{Protocol}: User {User name} has initiated a reset to factory defaults.

Example	SSH: User admin has initiated a reset to factory defaults.
Explanation	A user has initiated a reset to default settings. In the example, the user "admin" has initiated a reset to default settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

A.5 Restoration

{Protocol}: Firmware {Version} was activated.

Example	swupdate: Firmware V03.00.00.00_00.00.54 was activated.
Explanation	The specified firmware version was activated.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: Firmware activation failed.

Example	swupdate: Firmware activation failed.
Explanation	The firmware version could not be activated.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Appendix B "Supported encryption processes"

B.1 SSL

The following table contains the supported encryption processes for SSL communication with HTTPS or for Docker.

Encryption algorithm	HTTPS	Docker
ECDH >= 250 bits	●	-
ffdhe2048	-	●
secp256r1 (prime256v1)	●	●
secp384r1	●	●
secp521r1	●	●
sha1+ecdsa	-	●
sha1+rsa	-	●
sha256+ecdsa	●	●
sha384+ecdsa	●	●
sha512+ecdsa	●	●
sha256+rsa	●	●
sha384+rsa	●	●
sha512+rsa	●	●
sha256+rsaepss	●	●
sha384+rsaepss	●	●
sha512+rsaepss	●	●
TLSv1.2	●	●
TLSv1.3	●	●
TLS_AES_128_GCM_SHA256	●	●
TLS_AES_256_GCM_SHA384	●	●
TLS_CHACHA20_POLY1305_SHA256	●	●
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	-	●
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	-	●
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	-	●
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	●	●
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	-	●
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	-	●
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	-	●
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	-	●
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	●	●
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	-	●
TLS_RSA_WITH_AES_128_CBC_SHA	-	●
TLS_RSA_WITH_AES_256_CBC_SHA	-	●
TLS_RSA_WITH_AES_128_GCM_SHA256	-	●

Encryption algorithm	HTTPS	Docker
TLS_RSA_WITH_AES_256_GCM_SHA384	-	●
X25519	●	●
X448	●	-

Note

The following key lengths are supported for HTTPS:

- **RSA**
 - 2048 bits
 - 4096 bits
 - 8192 bits
- **ECDSA**
 - 256 bits
 - 384 bits

B.2 SSH

The following table contains the supported encryption processes for SSH communication and for SFTP.

Encryption algorithm	SSH	SFTP
aes128-ctr	●	●
aes192-ctr	●	●
aes256-ctr	●	●
aes128-gcm@openssh.com (AEAD_AES_128_GCM)	●	●
aes256-gcm@openssh.com (AEAD_AES_256_GCM)	●	●
chacha20-poly1305@openssh.com	●	●
curve25519-sha256	●	●
curve25519-sha256@libssh.org	●	●
diffie-hellman-group16-sha512	●	●
diffie-hellman-group18-sha512	●	-
ECDH >= 250 bits	●	●
ecdsa-sha2-nistp256	-	●
ecdsa-sha2-nistp384	-	●
ecdsa-sha2-nistp521	-	●
hmac-sha2-256-etm@openssh.com	●	●
hmac-sha2-512-etm@openssh.com	●	●
SSHv2.0	●	●
ssh-ed25519	●	●
umac-128@openssh.com	-	●
umac-128-etm@openssh.com	●	●

B.3 SNMP

The following list contains the supported encryption processes for SNMP.

- aes128-cbc
- des-cbc
- HMAC-MD5-96
- HMAC-SHA-96
- HMAC-SHA-224
- HMAC-SHA-256
- HMAC-SHA-512

Index

A

Application
 Displaying, 142
 Restarting, 144
 Starting, 143
 Stopping, 143

B

Backup file
 Creating, 146
 delete, 147
 Display, 145
 Downloading, 146
 restore, 147
 upload, 147
backupmanager
 create, 88, 89
 delete, 91
 list, 87
 restore, 89, 90
Bootloader, 75

C

CA certificate, 71
Certificate, 16, 71
Client-server application, 174
Configuration backup
 creating, 88, 89
 Deleting, 91
 Displaying, 87
 restore, 89, 90
Configuring a gateway
 Deleting, 55
 DHCP, 55, 133
 static, 54, 132
Configuring an IP address
 Combo ports, 52
 DHCP, 51, 131
 static, 51, 131
Configuring DCP, 50, 130
Configuring the DNS server
 static, 57
CSR, 71

D

Device information
 Console, 68
 Web UI, 138
deviceinfo, 68
Disable interface, 53
Docker container
 Deleting, 164
 Displaying, 160
 Interrupting, 163
 kill, 113
 Killing, 163
 pause, 114
 restart, 112
 Restarting, 163
 Resuming, 164
 rm, 115
 start, 111
 Starting, 162
 stop, 111
 Stopping, 163
 unpause, 114
docker-compose
 down, 122
 kill, 123
 pause, 123
 start, 122
 stop, 122
 unpause, 121, 123
 up, 122

E

eventmgr, 85

F

Factory reset, 85
fail2ban, 40
fail2ban-client
 get, 41
 set, 41
 unbanip, 42
Firmware, 75
 Update, 70
 Update via SSH, 80

- Update via the Rescue system, 85
- Update via USB interface, 78
- Function extender interface, 23
- Function extender interface port, 23
- Function extender interface ports, 33

H

- halt, 87

I

- Inactivity timeout, 126
 - Linux Shell, 126
 - Web UI, 127
- Interface names, 23, 33
- IP configuration
 - Display, 129
 - Displaying, 47
 - Resetting, 59
- ipconfig
 - Configuring a gateway, 54, 55
 - Configuring an IP address, 51
 - Configuring client identification, 52
 - Configuring DCP, 50
 - Configuring DHCP, 51
 - Configuring the DNS server, 57
 - Deleting a DNS server, 58
 - Deleting a gateway, 55
 - Disable interface, 53
 - Display configuration, 47
 - Resetting the configuration, 59
 - Showing parameters, 46

K

- Key, 16

N

- net-snmp-create-v3-user
 - with parameters, 105
 - without parameters, 104
- Nozomi
 - delete, 120, 168
 - Installing, 120, 168
- NTP
 - Configuring, 97, 153
 - Requirements, 96
 - Show status, 97

O

- OpenSSL, 71
 - Certificate, 73
 - CSR, 72
- Overlay file system, 70

P

- PEM format, 71
- PKCS #12 format, 16
- poweroff, 87
- Promiscuous Mode
 - disable, 60
 - enable, 60

R

- Rescue system, 75
- Resetting the configuration, 84, 144
 - Web UI, 144
- Resetting the device to the delivery state, 85
- Restart, 145
- Reverse proxy, 174

S

- Secure Boot, 19
- Secure NTP, 98, 153
- server_certificate_custom.pem, 71
- Sfp Diagnose, 133
- SFTP, 108
 - Connection in the Web UI, 158
 - Download, 109
 - Downloading a file, 158
 - Establish connection, 108
 - Upload, 109
 - Uploading a file, 159
- sfw_manager, 78, 80
- shellinabox, 142
- shutdown, 87
- Shutdown, 145
- SNMP
 - Changing user data, 157
 - Creating users, 156
 - Deleting users, 157
- SNMPv3, 103
 - Configuration files, 103
- sudo apt list --upgradable, 173

- sudo apt update, 173
- Switching off a port, 132
- Syslog
 - Configuring the directory, 151
 - Configuring the server, 150
 - Deleting messages, 152
 - Displaying messages, 152
 - Downloading messages, 152
 - Encrypting messages, 86
- System time, 96, 152
 - configure manually, 99, 155
- systemctl halt, 87
- systemctl poweroff, 87

T

- Time zone, 99
- timedatectl, 99

U

- U-Boot, 75
- User-based Security Model, 103
- Users
 - Changing the password, 150
 - Changing the status, 149
 - Creating, 148
 - Deleting, 149
 - Displaying, 148

V

- VXLAN, 61
 - Configuring a connection, 62
 - Deleting the VTEP configuration, 67
 - Display configuration, 62
 - Locking the configuration, 64
 - Unlocking the configuration, 65

W

- Web SSH, 142

X

- X.509 TLS certificate, 16

