FL MGUARD 1000
Web-based management
mGuardNT 1.8.x

User manual

UM EN MGUARD NT

INSPIRING INNOVATIONS

User manual
FL MGUARD 1000 – Web-based management – mGuardNT 1.8.x

UM EN MGUARD NT, Revision 12 2024-05-22

This user manual is valid for:

Designation	Order No.
FL MGUARD 1102	1153079
FL MGUARD 1105	1153078

Firmware version mGuardNT 1.8.x

For further information see mGuardNT 1.8.x firmware – Release Notes.

108420_en_12

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 For your safety

Read this user manual carefully and keep it for future reference.

1.1 Identification of warning notes

This symbol together with the **NOTE** signal word warns the reader of actions that might cause property damage or a malfunction.

Here you will find additional information or detailed sources of information.

1.2 About this user manual

The following elements are used in this user manual:

Bold	Designations of operating elements, variable names or other accentuations
Italic	– Product, module or component designations (e.g., *tftpd64.exe*, *Config API*) – Foreign designations or proper names – Other accentuations
–	Unnumbered list
1.	Numbered list
•	Operating instructions
⇒	Result of an operation

1.3 Qualification of users

The use of products described in this user manual is oriented exclusively to:

– Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

– Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

1.4 Intended use

– The devices of the FL MGUARD 1000 series are security routers for industrial use, with integrated stateful packet inspection firewall. They are suitable for distributed protection of production cells or individual machines against manipulation.

– The devices are intended for installation in a control cabinet.

1.5 Modifications to the product

Modifications to hardware and firmware of the device are not permitted.

– Incorrect operation or modifications to the device can endanger your safety or damage the device. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

1.6 IT security

You have to protect components, networks, and systems against unauthorized access and ensure the integrity of data. As a part of this, you must take organizational and technical measures to protect network-capable devices, solutions, and PC-based software.

Phoenix Contact strongly recommends using an Information Security Management System (ISMS) to manage all of the infrastructure-based, organizational, and personnel measures that are needed to ensure compliance with information security directives.

Furthermore, Phoenix Contact recommends that at minimum the following measures are taken into consideration.

More detailed information on the measures described is available on the following websites (last accessed on 2024-04-15; partly only available in German):

– bsi.bund.de/it-sik.html
– ics-cert.us-cert.gov/content/recommended-practices

Use the latest firmware version

Phoenix Contact regularly provides firmware updates. Any firmware updates available can be found on the product page for the respective device.

- Ensure that the firmware on all devices used is always up to date.
- Observe the Change Notes for the respective firmware version.
- Pay attention to the security advisories published on Phoenix Contact's Product Security Incident Response Team (PSIRT) website regarding any published vulnerabilities.

Use up-to-date security software

- Install security software on all PCs to detect and eliminate security risks such as viruses, trojans, and other malware.
- Ensure that the security software is always up to date and uses the latest databases.
- Use whitelist tools for monitoring the device context.
- Use an Intrusion-Detection system for checking the communication within your system.

Take Defense-in-Depth strategies into consideration when planning systems

It is not sufficient to take measures that have only been considered in isolation when protecting your components, networks, and systems. Defense-in-Depth strategies encompass several coordinated measures that include operators, integrators, and manufacturers.

- Take Defense-in-Depth strategies into consideration when planning systems.

Perform regular threat analyses

- To determine whether the measures you have taken still provide adequate protection for your components, networks, and systems, threat analyses should be performed regularly.
- Perform a threat analysis on a regular basis.

Deactivate unneeded communication channels

- Deactivate unnecessary communication channels (e.g., SNMP, FTP, BootP, DCP, etc.) on the components that you are using.

Do not integrate components and systems into public networks

- Avoid integrating your components and systems into public networks.
- If you have to access your components and systems via a public network, use a VPN (Virtual Private Network).

Restrict access rights

- Avoid unauthorized persons gaining physical access to the device. Accessing the hardware of the device could allow an attacker to manipulate the security functions.
- Restrict access rights for components, networks, and systems to those individuals for whom authorization is strictly necessary.
- Deactivate unused user accounts.

Secure access

- Change the default login information after initial startup.
- Use secure passwords reflecting the complexity and service life recommended in the latest guidelines.
- Change passwords in accordance with the rules applicable for their application.
- Use a password manager with randomly generated passwords.
- Wherever possible, use a central user administration system to simplify user management and login information management.

Use secure access paths for remote access

- Use secure access paths such as VPN (Virtual Private Network) or HTTPS for remote access.

Set up a firewall

- Set up a firewall to protect your networks and the components and systems integrated into them against external influences.
- Use a firewall to segment a network or to isolate a controller.

Activate security-relevant event logging

- Activate security-relevant event logging in accordance with the security directive and the legal requirements on data protection.

Secure access to SD cards

Devices with SD cards require protection against unauthorized physical access. An SD card can be read with a conventional SD card reader at any time. If you do not protect the SD card against unauthorized physical access (such as by using a secure control cabinet), sensitive data is accessible to all.

- Ensure that unauthorized persons do not have access to the SD card.
- When destroying the SD card, ensure that the data cannot be retrieved.

1.7 Latest security instructions for your product

Product Security Incident Response Team (PSIRT)

The Phoenix Contact PSIRT is the central team for Phoenix Contact as well as for its subsidiaries, authorized to respond to potential security vulnerabilities, incidents and other security issues related to Phoenix Contact products, solutions as well as services.

Phoenix Contact PSIRT manages the disclosure, investigation internal coordination and publishes security advisories for confirmed vulnerabilities where mitigations/fixes are available.

The PSIRT website (phoenixcontact.com/psirt) is updated regularly. In addition, Phoenix Contact recommends subscribing to the PSIRT newsletter.

Anyone can submit information on potential security vulnerabilities to the Phoenix Contact PSIRT by e-mail.

1.8 Support

For additional information on the device as well as release notes, user assistance and software updates, visit: phoenixcontact.net/product/<item number>.

In the event of problems with your device or with operating your device, please contact your supplier.

To get help quickly in the event of an error, make a snapshot of the device configuration immediately when a device error occurs, if possible. You can then provide the snapshot to the support team.

The usage of snapshots is described in this user manual.

2 mGuardNT basics

2.1 Device properties and scope of functions

Table 2-1 Device properties and scope of functions

Device properties	FL MGUARD	
	1102	1105
HARDWARE		
2 net zones (network interfaces)	x	x
Ethernet via RJ45 connections (transmission speed: 10/100/1,000 Mbps)	2	5
4-Port Unmanaged Switch (RJ45) (*Bridge Mode*)	-	x
Service inputs and outputs (IOs)	x	x
SD card holder	x	x
NETWORK		
Stealth mode	x	x
Router mode	x	x
Packet forwarding (router mode)		
Security router	x	x
IP masquerading (NAT)	x	x
Port forwarding	x	x
1:1 NAT	x	x
Additional static routes	x	x
Network services (client/server)		
DHCP	x	x
DNS	x	x
NTP	x	x
SNMP (only server)	x	x
HTTPS – WBM/*Config API* – (only server)	x	x
FIREWALL		
Stateful packet inspection firewall	x	x
Firewall (for routed data traffic)	x	x
Device access (for incoming data traffic)	x	x
Integrity check of data packets to increase network security	x	x
Easy Protect Mode Automatic protection of connected network clients without configuration effort directly after connection of the device.	x	x
Firewall Assistant Analysis of data traffic for the automatic creation of firewall rules.	x	x

Table 2-1 Device properties and scope of functions

Device properties	FL MGUARD	
	1102	1105
Firewall test mode Analysis of data traffic for automatic extension of existing firewall rules.	x	x
MANAGEMENT		
Administration via web-based management (WBM)	x	x
Administration via RESTful Configuration API (*Config API*)	x	x
Read access to important device parameters via SNMP	x	x
Firmware update via WBM and *Config API*	x	x
Role-based user management (WBM and *Config API*)	x	x
User authentication via LDAP server	x	x
Smart mode Access to certain management functions is gained using the Mode button on the device and without access to a management interface.	x	x
Backup and restore configuration and user manangement via SD card	x	x
Backup and restore configuration via WBM	x	x
Support tools		
TCP Dump (packet data analysis)	x	x
Ping (network analysis)	x	x
Log viewer (evaluation of log entries)	x	x
Remote logging (*syslog*)	x	x
Support snapshot (status and error analysis)	x	x

2.2 Changes compared to the previous version

Refer to the corresponding *Release Notes* for a detailed overview of all changes to the respective version.

The *Release Notes* for the latest version are available in the download area of the respective product site in the e-shop, for example phoenixcontact.net/product/1153079.

2.2.1 New in mGuardNT 1.8

- Connection tracking helper (FTP)
- Numerous improvements in the area of security.

2.2.2 New in mGuardNT 1.7

- Numerous improvements in the area of security.

2.2.3 New in mGuardNT 1.6

- Numerous improvements in the area of security (e.g.)
  - Security vulnerabilities (CVEs) found via the PSIRT process have been fixed
  - The entire system was further hardened
- Numerous usability improvements (e.g.)
  - The assignment of log entries to categories/components has been improved
  - The time information in log entries corresponds to the selected time zone
  - The snapshot content has been extended
  - Duplicate entries in firewall tables can be easily removed

2.2.4 New in mGuardNT 1.5

- IP masquerading (NAT) in both directions (net zone 1 ← → net zone 2)
- User blocking (automatic/manual)
- Backup and restore configuration (download/upload via WBM)
- Configurable hostname
- Reboot of the device via WBM and *Config API*
- Numerous improvements in the area "performance and security"
- Numerous improvements in the area "usability"

2.2.5 New in mGuardNT 1.4

- User and role management
- LDAP authentication (LDAP client)
- SNMP server
- Port ranges in firewall rules
- NAT functionality for networks
- Remote logging (*syslog*)
- External configuration storage (on SD card)
- Configurable *session timeout*

2.2.6 New in mGuardNT 1.3

- Extended firewall functions
  - Easy Protect Mode
  - Firewall Assistant
  - Firewall test mode

2.2.7 New in mGuardNT 1.2

- Extended network functions
  - Stealth mode

2.2.8 New in mGuardNT 1.1

- Router and firewall functions added

2.3 Encryption algorithms used

Some of the device functions feature the option of using encrypted communication. In these cases, the device generally uses the “TLS” (*Transport Layer Security*) encryption protocol. See Table 2-2 and 2-3 for settings.

For security reasons, all clients and servers participating in encrypted communication should always use an up-to-date TLS setting.

TLS settings used by the device:

Table 2-2 TLS settings: HTTPS interface (WBM/Config API)

Setting	Value
Protocols	TLS 1.2 / TLS 1.3
Cipher suites (TLS 1.3)	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
Cipher suites (TLS 1.2)	ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305
Certificate type	ECDSA (P-256)
TLS curves (TLS 1.3)	X25519 prime256v1 secp384r1
TLS curves (TLS 1.2)	secp384r1
Cipher preference	client chooses

Table 2-3 TLS settings: Remote logging / LDAP authentication

Setting	Value
Protocols	TLS 1.2 / TLS 1.3
Cipher suites (TLS 1.3)	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256
Cipher suites (TLS 1.2) **(Remote logging)**	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305 DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES256-GCM-SHA384
Cipher suites (TLS 1.2) **(LDAP authentication)**	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305
TLS curves	X25519 prime256v1 secp384r1

2.4 Network

As a router or gateway, the device connects subnets or net zones. For each net zone, a unique IP address is configured. The device can be reached in the network using this IP address (see Section 6.1, “Interfaces”).

The NAT functions (IP masquerading, 1:1 NAT, port forwarding) can be used to easily integrate machines (PLCs) or several subnets with the same IP configuration into an existing network, without having to change the IP configuration of the machine or the subnets.

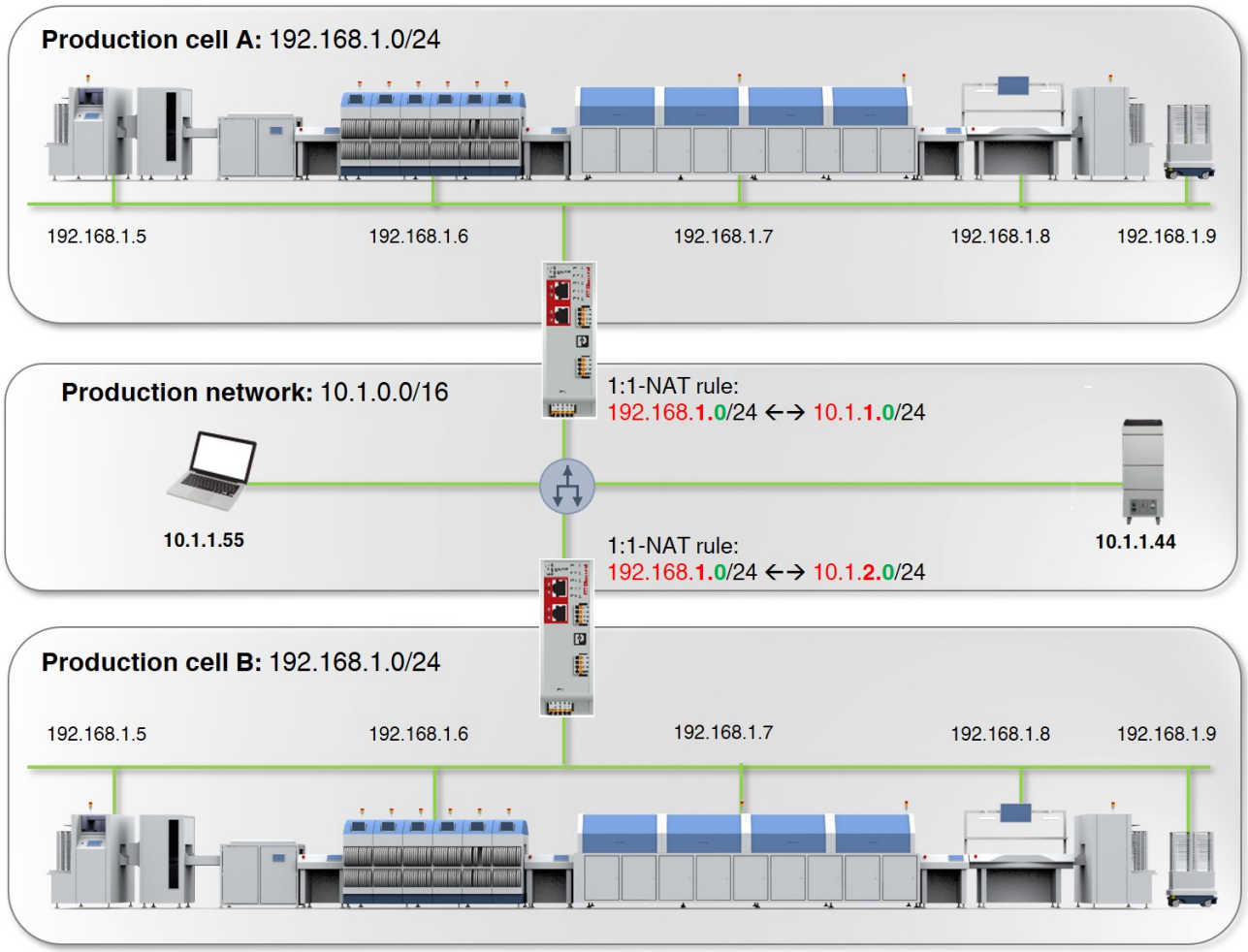


Figure 2-1 Using the device as a NAT router (example: 1:1 NAT)

2.5 Firewall

Strictly speaking, the device firewall is a packet filter through which data packets *routed* through the device are analyzed and then forwarded or blocked in accordance with the configured firewall rules (see Section 7, “Menu: Network security”).

Stateful packet inspection firewall

The mGuardNT packet filter functions as a *stateful packet inspection* firewall. This means that response packets automatically pass through the firewall if they can be clearly assigned to a related request that has already been accepted. For this reason, firewall rules are never applied to response packets.

Firewall functions

The firewall can be used and configured in different ways.

Table 2-4 Options for using the mGuard firewall

No configuration necessary	
Easy Protect Mode (see Section 2.6)	Network clients are protected against external access directly after connection of the device without the need to create firewall rules.
Configuration via web-based management (WBM) or Config API necessary	
Firewall (packet filter) (see Section 7.1)	Firewall rules are created and extended manually. The rules are entered and configured in the device firewall table.
Firewall Assistant (see Section 7.3)	The *Firewall Assistant* analyzes and acquires the data traffic *routed* through the device for any period of time (**net zone 1 ←→ net zone 2**). The captured packet data is used to derive firewall rules that are automatically entered into the device firewall table when the *Firewall Assistant* is exited.
Firewall test mode (see Section 7.1, „Firewall test mode“)	Data traffic unintentionally rejected by the firewall can be easily identified and permitted through the automated creation of corresponding firewall rules. An alarm informs the user about the event (data traffic not acquired through an existing firewall rule).

2.6 Easy Protect Mode

If the device is started in *Easy Protect Mode*, it **automatically** protects all network clients connected to net zone 2 (XF2–XF5) against external access (e.g., individual machines or production cells that are connected via a switch).

For additional information, refer to the "*FL MGUARD 1000 – Installation and startup"* user manual, available at phoenixcontact.net/product/1153079.

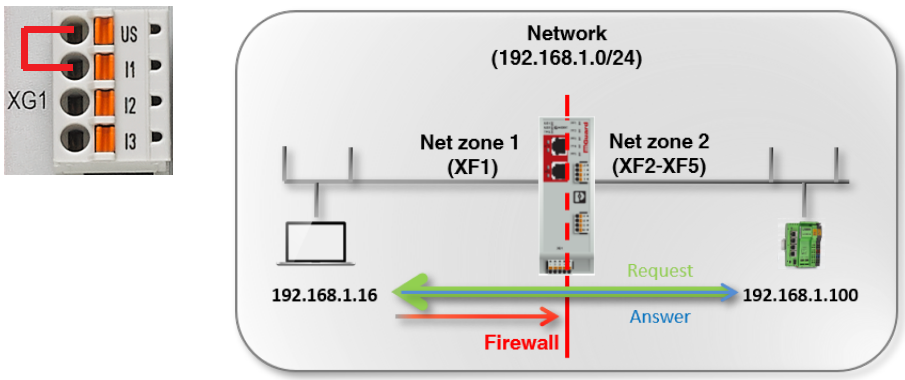


Figure 2-2 Activated *Easy Protect Mode* (via cable bridge)

Easy Protect Mode is activated via a cable bridge (see Figure 2-2)

The device is integrated into the existing network via its net zones 1 and 2 or XF1 and (XF2–XF5) without the existing network configuration of the connected devices having to be changed. The devices in net zone 2 are automatically protected.

Configuration of the mGuard device is generally not required and not possible due to the missing access option via web-based management (HTTPS).

In *Easy Protect Mode*, firmware updates can be performed via the Smart mode function "Update from SD card" (see Section A 2, "Using Smart mode").

3 Using web-based management

3.1 Establishing a network connection to the device

Establish a connection between the configuration computer and the network interface (XF2/net zone 2) of the device.

Default setting (network interface: XF2)

– IP address: 192.168.1.1
– Subnet mask: 24 (255.255.255.0)
– The DHCP server of the device is activated and available via XF2/net zone 2.

For additional information, refer to the "*FL MGUARD 1000 – Installation and startup"* user manual, available at phoenixcontact.net/product/1153079.

3.2 Logging in a user

Avoid concurrent sessions
A concurrent login of users from different instances may lead to data loss or problems with user management.

User block
Users can be blocked due to several unsuccessful login attempts or by an administrator. Blocked users cannot log in to the device. In this case, contact an administrator with appropriate access permissions.

Note: If a user has been automatically blocked, the temporary block can be prematurely removed by an administrator with the "*Super Admin*" role or by rebooting the device.

• Enter, for example, the following web address in a web browser to start the WBM: **https://192.168.1.1** (default setting for "XF2")

⇒ The login page opens.

In the default setting, the following user can log in to the device:

– User name: *admin;* Password: *private*

Immediately change the default password upon initial startup of the device, (see Section 5.1).

⇒ After logging in successfully, the following start page appears.

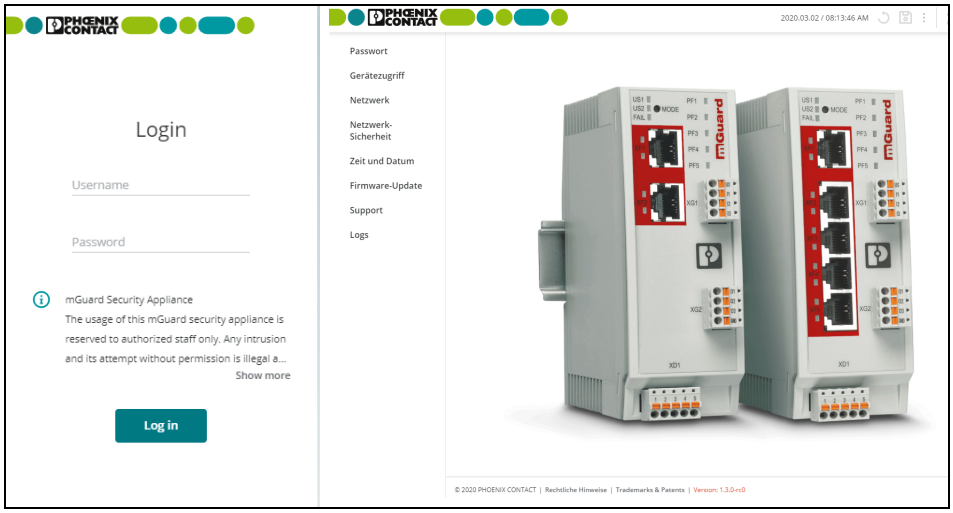


Figure 3-1 Web-based management: Login page (left) and and start page (right)

3.2.1 The user password is not remembered any more

What should be done if passwords are no longer recognized

If the passwords of all users are no longer recognized and it is therefore no longer possible to login on the device, it may be necessary to reset the device to the default settings.

NOTE: Data loss
The entire configuration, all settings, users, and their passwords, will be irrevocably deleted.

For this purpose, execute the smart mode function "*Restoring the factory settings*" (see Section A 2).

3.3 Logging out a user

Figure 3-2 User logout

To log the current user out of the device, proceed as follows:

- Click the icon.

⇒ The user is logged out.

⇒ All information about the current session is deleted.

⇒ The user is forwarded to the login page.

3.3.1 Automatic logout

The user is automatically logged out under the following conditions:

– The session times out (*session timeout*).

– The device is rebooted.

– The user is removed from user management.

3.3.2 Session expiration (timeout)

A user session is limited in time by a *session timeout*. The configurable time period of the *session timeout* is between 5 minutes and 8 hours. After the session times out, the user is logged out automatically.

The *session timeout* period begins when the user logs in (default setting: 30 minutes). If the user performs an action during a session, the *session timeout* period is reset to the configured start value (see Section 4.5).

3.4 Automatic user block

Users are automatically blocked after a configurable number (2 – 200) of unsuccessful login attempts for up to 8 hours .

The block is configurable (see Section 4.5) and can be prematurely removed by an administrator with the role “*Super Admin*” or by rebooting the device (see Section 5.1).

An automatic user block is also removed by rebooting the device.

3.5 Changing a user password

Figure 3-3 Changing the logged in user's current password

Locally logged in users can change their passwords themselves.

If you no longer know your own password, another user with appropriate access permissions can change the password and reassign it (see Section 5.1).

Proceed as follows:

- Click the icon (User settings) at the top right corner of the screen.

⇒ The dialog window for changing the password opens.

- Fill out the three required fields.

Current password	The logged in user's current password that is to be changed.
New password	The new password for the logged in user. **Input format:** To increase security, the password should contain upper case and lower case characters, numbers, and special characters. Permitted characters (min. 6, max. 64): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
Confirm new password	Enter the new password again.

- Apply the password change by clicking the **Change password** button.

⇒ The password is changed and must be entered when logging in again.

NOTE: Change the administrator password during initial login
After logging in for the first time, immediately change the default administrator password of the user "*admin*" (password = *private*).

3.6 Help for configuration

3.6.1 Page structure and function

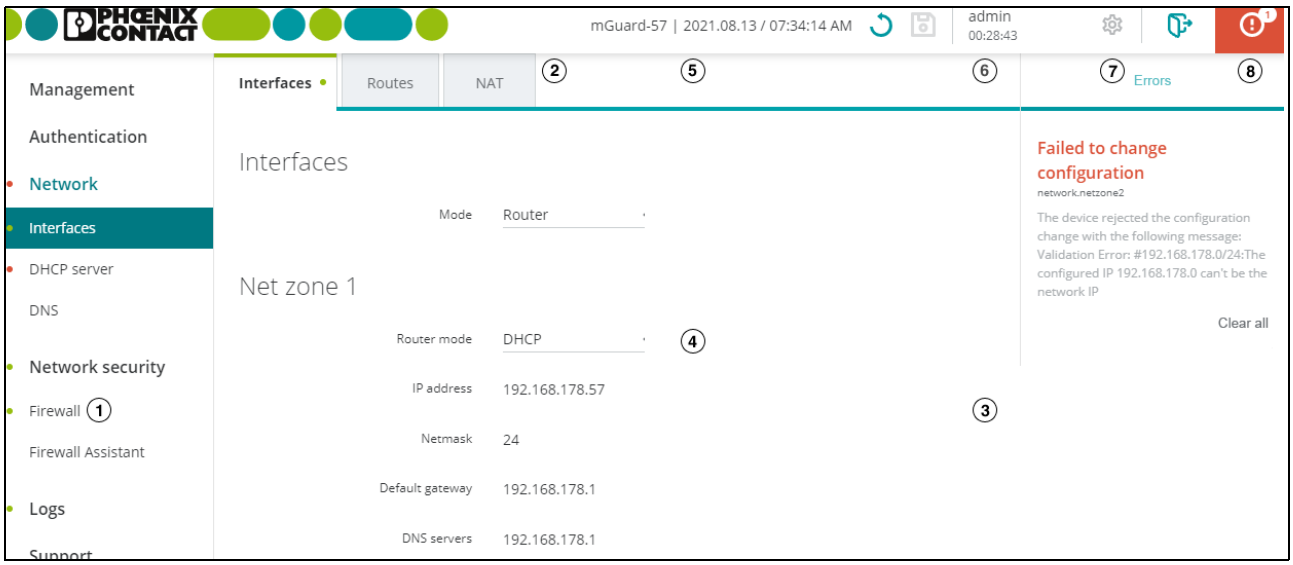


Figure 3-4 Web-based management: Menu structure and page elements

Menu structure ①

The individual configuration pages can be opened via the main and submenu structure. Configuration pages are often divided into several subpages that can be called up via *tabs*.

Tabs ②

The *tabs* can be selected via the tab bar at the upper edge of the screen.

Configuration page ③

The parameters of the individual variables can be changed in the main window of a configuration page.

Variables ④

Variable values can be selected via a drop-down menu, a checkbox, or entered manually.

Depending on the variable, letters, numbers, and/or certain special characters can be used. Some variables are entered into tables (e.g., firewall and 1:1 NAT rules).

Hostname/System time ⑤

The configured hostname (left) and the current system time (right) are displayed.

Session expiration (timeout) ⑥

A logged in user will be logged out automatically after the *session timeout* (see Section 3.3).

User settings ⑦

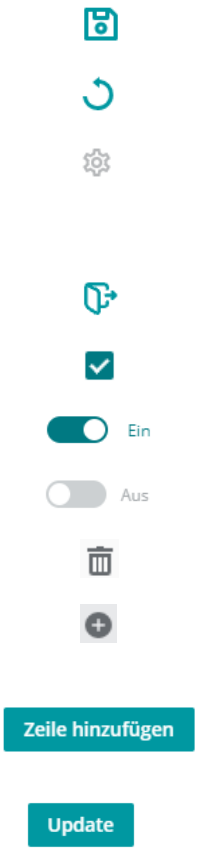
The settings of the currently logged in user, e.g., the password, can be changed.

Error message (server) ⑧

Error messages that cannot be determined upon entry are displayed as a server response on the right-hand screen edge (see Section 3.6.3).

3.6.2 Icons and buttons

The following examples show the icons and buttons available in the WBM.



- Click the **“Save” icon** to apply all changes you have made on a configuration page or in different menu items.
- To discard all changes that were not saved, click the **“Discard changes” icon**.
- To change the settings of the currently logged in user, click the **“Settings“ icon**.
- The password of the currently logged in user can be changed at this point.
- Click the **“Logout” icon** to logout the current user from the device and close the session.
- Put a check mark in the **checkbox** to activate a function.
- Slide the **switch** to the **On** position to activate a function.
- Slide the **switch** to the **Off** position to deactivate a function.
- Click the **“Trash can” icon** to delete the selected table row.
- Click the **“Plus” icon** to transfer the selected table row (*Test mode alarms*) to the associated firewall table as a new firewall rule.
- Click the **Add row** button to add a new table row below the last existing row.
- Click the **“Update” button** to select and immediately use an update file.

3.6.3 Error messages

If an error cannot be detected during entering but only when the user tries to save the change, none of the changed values will be applied.

The icon at the top right corner of the screen indicates that one or several configuration errors are present. Click the icon to have the corresponding error messages displayed in the right-hand page column (see Figure 3-4).

Correct the entries and apply the changed values by clicking the icon .

3.6.4 Entering and changing values

Changing values

To change the value of a variable and save it, you must apply the change by clicking the icon .

It is possible to first change several values on a configuration page and then apply them together by clicking the icon .

Displaying changed values

Changed values that have not been applied yet are displayed in the GUI marked by a green dot . The mark appears at the corresponding position in the main menu, submenu and on the associated tab (see Figure 3-4).

Entering impermissible values

It is not possible to apply invalid variable values. Normally, a corresponding error message will be displayed as soon as an impermissible value is entered.

Impermissible entries are also marked on the GUI by a red dot . The mark appears at the corresponding position in the main menu, submenu and on the associated tab (see Figure 3-4).

Correct the entries and apply the changed values by clicking the icon .

Entering ranges

Some values can be entered as ranges. A range is entered by entering the start and end of the range separated by a colon (Start:End).

Example (port range): start_port:end_port -->110:220

3.6.5 Discarding changes

Discarding changes before they are applied.
Values that were newly entered or changed at any position but have not been applied yet can be discarded by clicking the **icon** **„Discard changes“**.

3.6.6 Deleting the device configuration completely and safely

Resetting the device to factory settings
To make sure that no protected data remains on the device after decommissioning that can be read by unauthorized parties, the data must be safely and permanently deleted.

To safely and permanently delete all the data on the device, run the Smart mode function “Reset to factory settings” (see Section A 2, “Using Smart mode”).

3.6.7 Working with tables

Some mGuardNT settings are saved as a data record. In this case, the parameters and their values are entered in table rows in the WBM.

It is essential to observe the sequence of the table rows

The sequence of the table rows is decisive for the application of firewall rules:

The firewall rules in the table are always queried one after the other starting from the top of the list of entries until an appropriate rule is found. Subsequent rules are then ignored (see „Behavior and effects of firewall rules“).

Adding a table row (at the end of the table)

- Click the **Add row** button.

⇒ A new row is added below the lowest existing row.

- Click the icon to apply the change.

Adding a table row (below an existing table row)

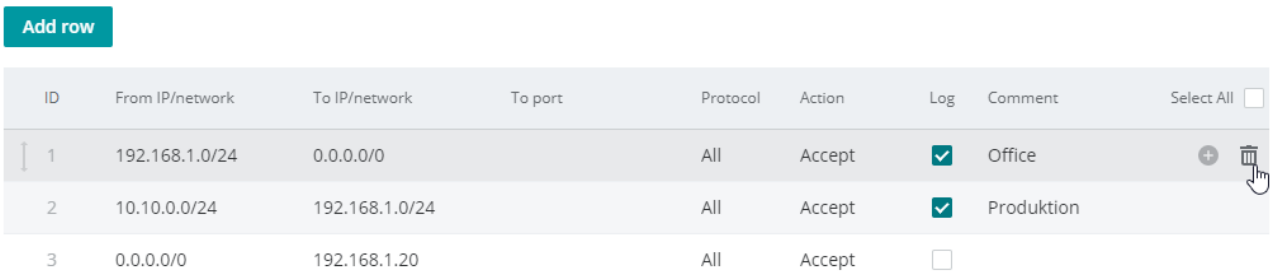
- Move the mouse pointer over the table row beneath which you would like to add the new row.
- Click the icon.

⇒ A new row is added below the existing row.

- Click the icon to apply the change.

Deleting a table row

- Move the mouse pointer over the table row that you would like to delete.
- Click the icon .



⇒ The row will be deleted.

- Click the icon to apply the change.

⇒ The table row and the data record have been deleted.

Deleting several table rows

By holding down the *Ctrl* key or the *Shift* key while simultaneously clicking on the ID numbers of the firewall rules, several rules or a range of rules can be selected.

⇒ The selected rules will be highlighted in green.

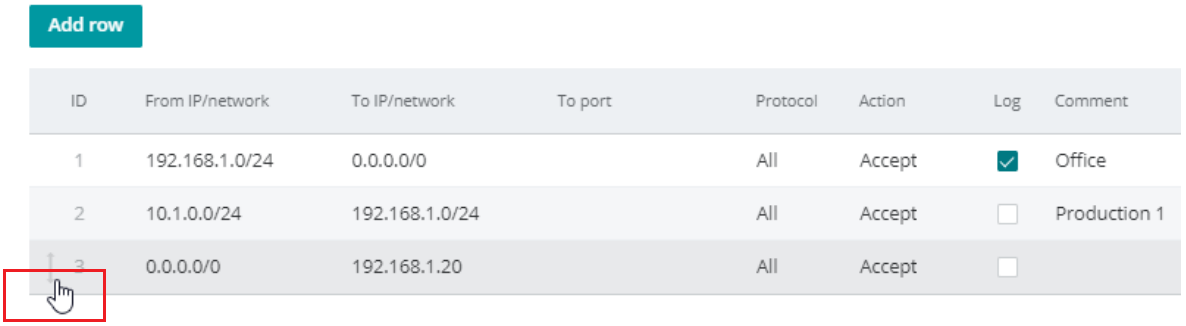
⇒ The number of rules selected will be displayed.

- Click **Delete** to delete the selected rules.
- Click the icon to apply the change.

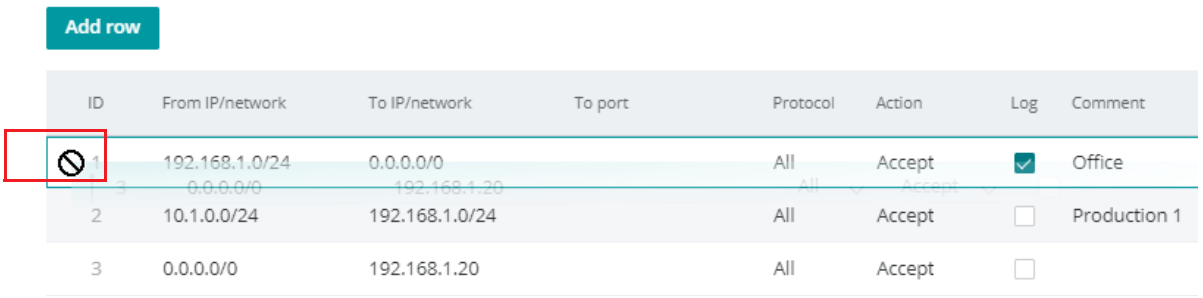
⇒ The selected table rows and the corresponding data records have been deleted.

Moving a table row

- Move the mouse pointer to the left of the table row you wish to move until the pointer changes into a hand symbol.



- Click the row and hold the mouse button down to drag and drop the row to the desired position.



- Release the mouse button.

⇒ The row has been moved to a new position.

- Click the icon to apply the change.

3.6.8 Input and format: Netmask and network

Netmask

The netmask can be entered in any one of the following formats:

– Numeric (e.g., 24)
– Decimal (e.g., 255.255.255.0)

In the web-based management, the decimal format is automatically converted to the numeric format upon entry (e.g., 255.255.0.0 --> 16).

Network

A network must be specified in CIDR format, e.g., 192.168.1.0/24, (see Section 3.6.9).

If a network is entered in the web-based management in one of the formats shown in Table 3-1, the entry is automatically converted accordingly.

Table 3-1 Examples for converting network formats in the WBM

Entered format	Converted format
10.1.1.1/32	10.1.1.1
10.1.1.1/24	10.1.1.0/24
10.1.1.1/16	10.1.0.0/16
10.1.1.1/8	10.0.0.0/8
10.1.1.1/0	0.0.0.0/0

Note: Netmask **/32** may not be used in the Config API. The IP address must be entered without netmask instead.

3.6.9 CIDR (Classless Inter-Domain Routing)

IP netmasks and CIDR combine several IP addresses to create a single address range. Here, a range comprised of consecutive addresses is handled as a network. To specify a range of IP addresses, you have to specify the address range in CIDR format (e.g., when configuring the firewall).

Table 3-2 CIDR, Classless Inter-Domain Routing

IP netmask[1]	Binary				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

1 Example: 192.168.1.0/255.255.255.0 corresponds to CIDR: 192.168.1.0/24

4 Menu: Management

4.1 Device access

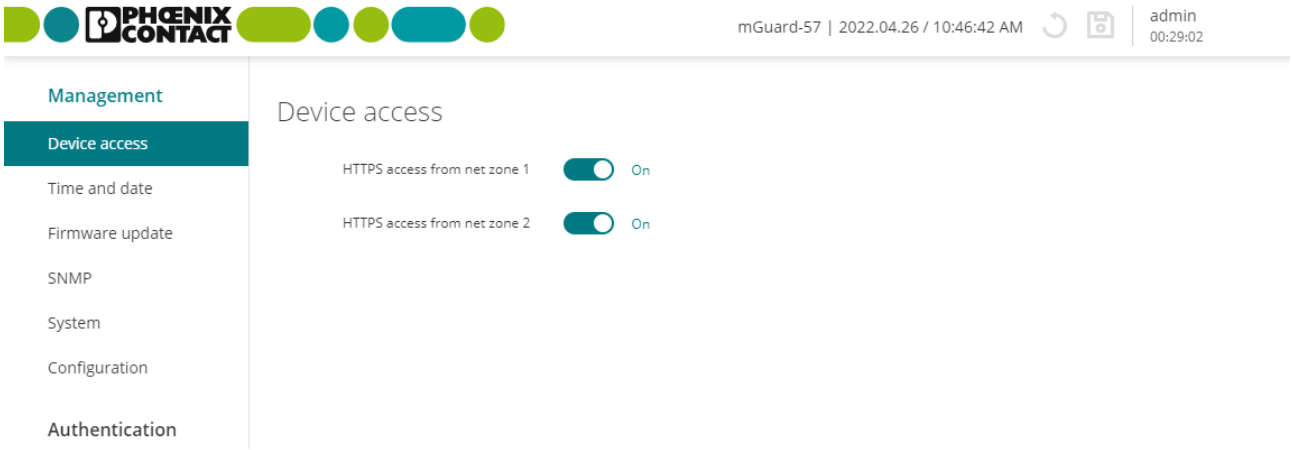


Figure 4-1 Management >> Device access

Menu: Management >> Device access	
Device access	By means of access rules, access to the web server of the device (web-based management or *Config API*) can be limited to one of the available net zones. **Access to further active services** Access to further services provided by the device is activated and deactivated on the respective configuration pages. – SNMP server (see Section 4.4): activated for net zone 2 by default – DNS server (see Section 6.3): activated for net zone 2 by default – NTP server (see Section 4.2): activated for net zone 2 by default **NOTE: Access from the Internet** It may be possible to reach the server from the Internet when the device is connected to the Internet via the activated net zone. **HTTPS access from net zone 1** When this function is activated, access from the selected net zone to the HTTPS server of the device is permitted (TCP port 443). **Default setting:** deactivated **HTTPS access from net zone 2** When this function is activated, access from the selected net zone to the HTTPS server of the device is permitted (TCP port 443). **Default setting:** activated

4.2 Time and date

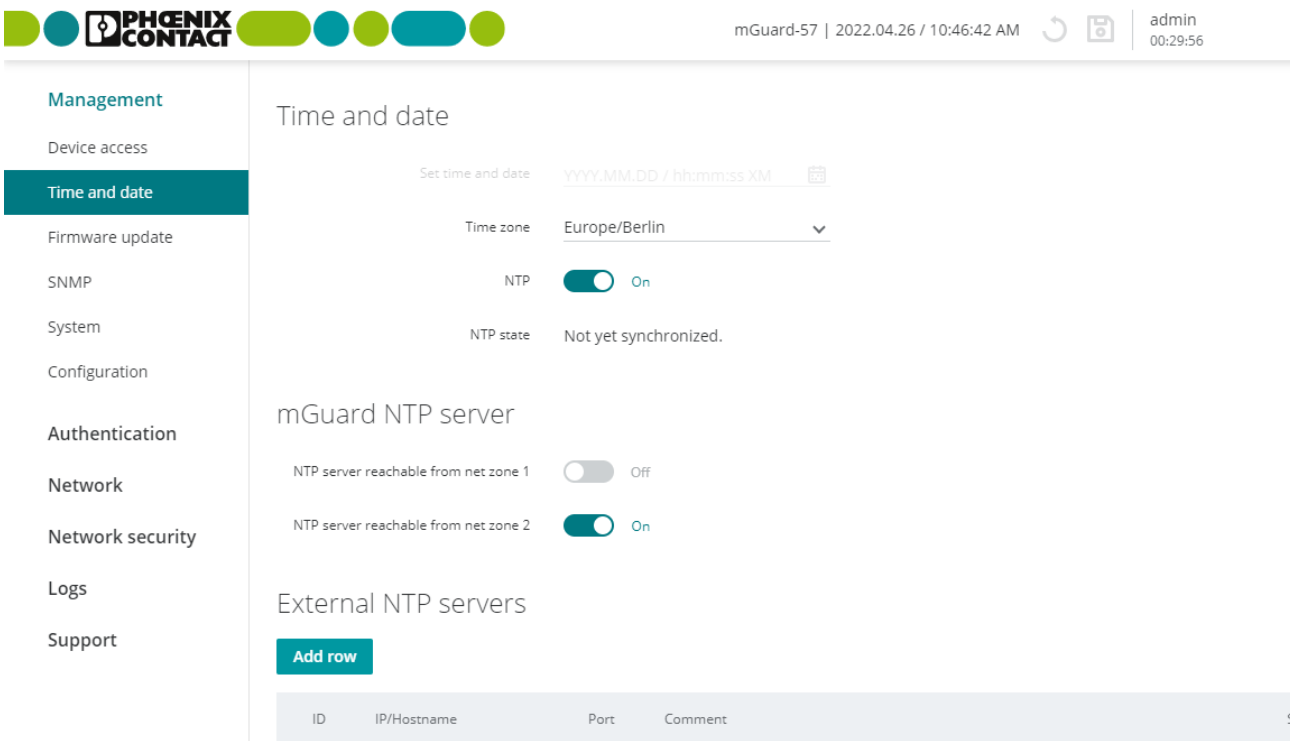


Figure 4-2 Management >> Time and date

Menu: Management >> Time and date	
Time and date	You can set the device system time manually or synchronize the system time using the NTP server of your choice. Set the time and date correctly, otherwise certain time-dependent activities cannot be carried out correctly by the device. If the power supply to the device is briefly interrupted, the buffered *real-time clock* (RTC) ensures that the time and date are retained and are available correctly and in the current time after a short interruption.
Set time and date (Only configurable if „NTP“ is deactivated.)	The device system time is configured and saved to the *real-time clock* (RTC). **Input format:** YYYY.MM.DD / hh:mm:ss XM Permitted range: >= 2018-01-01_00:00:00 <= 2069-01-01_00:00:00 The system time will be displayed in accordance with the configured time zone and used (e.g., in log entries).

Menu: Management >> Time and date		
	Time zone	The manually set or NTP-obtained system time will be displayed in accordance with the configured time zone and used (e.g., in log entries).
	NTP	This function can be used to activate the NTP client and the NTP server of the device. The NTP server of the device is only activated if access to the NTP server is permitted for at least one net zone (see below). **NTP client** When this function is activated, the device obtains its system time (time and date) from one or more NTP servers and continuously synchronizes itself with them. The status of the synchronization is displayed (see „NTP state“). The NTP server transmits the *Universal Time Coordinated* (UTC). The time on the device (system time) will be displayed in accordance with the configured time zone and used (e.g., in log entries). The *real-time clock* (RTC) of the device is automatically synchronized with the time data obtained from the NTP servers. **NTP server** When this function is activated, connected network clients can synchronize their system time via the NTP server of the device (*mGuard*). The NTP server transmits the *Universal Time Coordinated* (UTC). Access to the NTP server can be activated or deactivated for each net zone (see below). **Default setting:** activated
	NTP state	The NTP state shows whether the NTP of the device client has already been synchronized with the configured NTP servers. – Synchronized – Not yet synchronized – Deactivated Initial time synchronization can take up to 15 minutes or more. During this time, the device continuously compares the time data of the external NTP servers to its own system time so that they can be adjusted as accurately as possible.

Menu: Management >> Time and date		
mGuard NTP server	**NTP server reachable from net zone 1** (Only configurable if NTP is activated.)	When this function is activated, access from the selected net zone to the NTP server of the device is permitted (UDP port 123). The NTP server of the device is only activated if access from at least one net zone is permitted. **NOTE: Access from the Internet** It may be possible to reach the server from the Internet when the device is connected to the Internet via the activated net zone. **Default setting:** deactivated
	NTP server reachable from net zone 2 (Only configurable if NTP is activated.)	When this function is activated, access from the selected net zone to the NTP server of the device is permitted (UDP port 123). The NTP server of the device is only activated if access from at least one net zone is permitted. **NOTE: Access from the Internet** It may be possible to reach the server from the Internet when the device is connected to the Internet via the activated net zone. **Default setting:** activated
External NTP server	**IP/Hostname**	IP address or hostname of the external NTP server (time server) to which the device is to send NTP requests to obtain the current time (time and date). If several NTP servers are specified, the device automatically connects to all of them to determine the current time from all values received. **Input format:** IPv4 address or hostname **Default setting:** – 0.pool.ntp.org | Port:123 – 1.pool.ntp.org | Port:123 – 2.pool.ntp.org | Port:123 – 3.pool.ntp.org | Port:123
	Port	Port on which the external NTP server accepts NTP requests. Specifying a port is optional. **Default setting:** 123
	Comment	Freely selectable comment. Permitted characters: max. 128

4.3 Firmware update

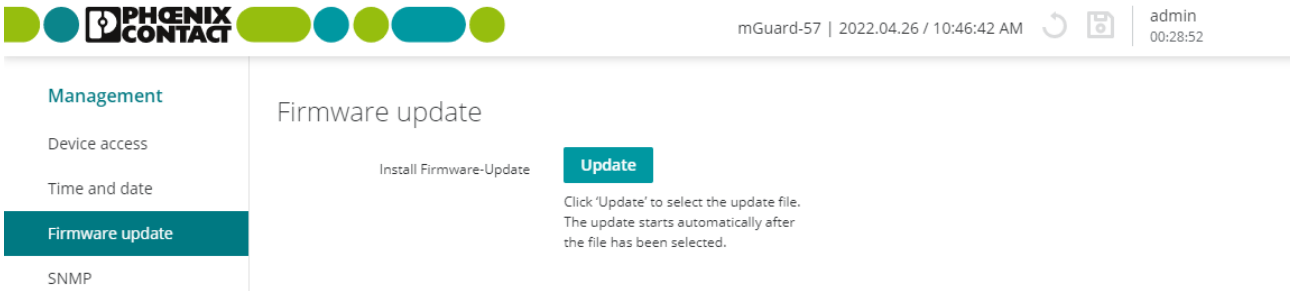


Figure 4-3 Management >> Firmware update

Table 4-1 Difference between update types

Update type	Property	Effect on the existing configuration
Before every update, always observe the current release notes. Download at phoenixcontact.net/product/1153079. Notes on the versions from which updates can be executed are described in Section A 6.		
Patch release **Patch update**	Fixes errors from previous versions. The version number changes in the third digit position: – Version 1.6.**2**, for example, is a patch release for Version 1.6.**1** or 1.6.**0**.	As a rule, the existing configuration remains unchanged. As a rule, new functions are not added.
Minor release **Minor update**	Extends the device with additional new properties and functions. The version number changes in the second digit position: – Version 1.**7**.0, for example, is a minor release for Version 1.**6**.2 or 1.**5**.2.	1. If the device is in factory settings, then: – After the update, the device will be configured with the **new** firmware version's settings. – It is possible that standard values of the existing firmware version could change or that properties and variables could be added or removed. 2. If changes have already been made to the existing device configuration, then: – The existing configuration will be applied unchanged. – New properties and variables from the **new** firmware version will be added to the existing configuration (in the factory setting). The update can only be executed if any necessary adjustments are made to the existing configuration before the update (see also Section A 6). If the update fails due to an incompatible configuration, an error message and/or log entry will inform the user of the reason for the error.
Major release **Major update**	Extends the device with completely new properties and functions. The version number changes in the first digit position: – Version **2**.0.0, for example, is a major release for Version **1**.5.0 or **1**.4.2.	

Menu: Management >> Firmware update	
Firmware update	A signed update file provided by Phoenix Contact will be uploaded from a configuration computer to the device and installed there automatically (e.g., *mguard-image-1.8.0.mguard3.update.signed)* . All current settings, passwords, and certificates are retained on the device. Downgrading from a higher to a lower firmware version is not possible. **Use the respective latest firmware version** Because security-relevant improvements are added to the product with each new firmware version, the latest firmware version should always be used. Phoenix Contact regularly provides firmware updates. You will find these on the product page of the respective device (e.g., phoenixcontact.net/product/1153079). • Ensure that the firmware of all devices used is always up to date. • Observe the Change Notes/Release Notes for the respective firmware version. • Observe the safety notes published on the Phoenix Contact Product Security Incident Response Team (PSIRT) website regarding any published vulnerabilities. **Procedure** **NOTE: Do not disconnect the power supply to the device during the update.** • Open the menu: **Management >> Firmware update**. • Click the **Update** button. • Select the update file for the firmware update. • Open the file. ⇒ Opening the file automatically starts the update process. ⇒ Following successful installation of the firmware, the device reboots automatically after a few seconds. • Wait until the device has completely booted.
Update status	Shows current messages and information on the status of the firmware update.

4.4 SNMP

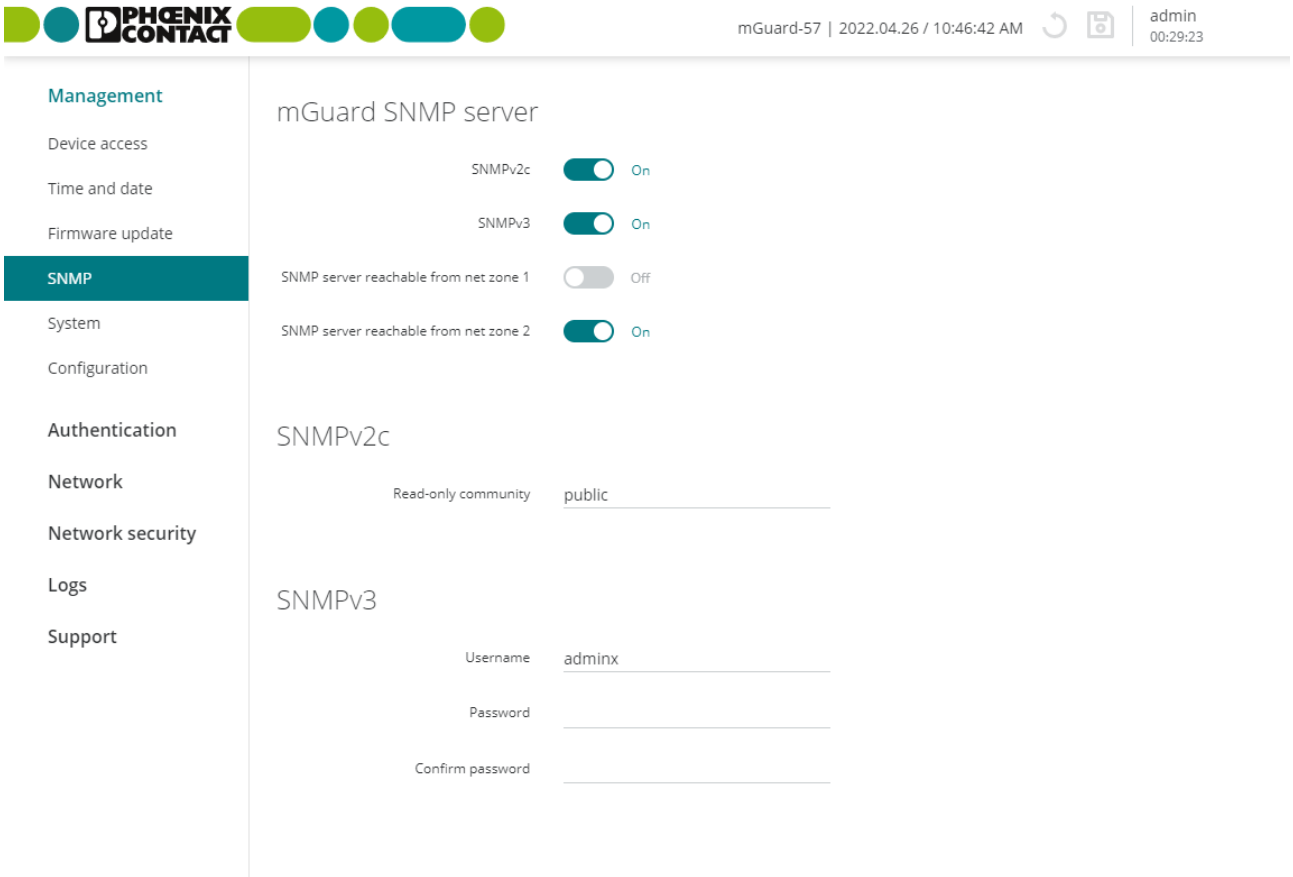


Figure 4-4 Management >> SNMP

Menu: Management >> SNMP	
SNMP	SNMP (*Simple Network Management Protocol*) is mainly used in more complex networks to monitor the state and operation of devices. The device acts as the SNMP server and supports various versions of the SNMP protocol: SNMPv1/SNMPv2c and SNMPv3. It is not currently possible to configure the device via the SNMP protocol. It is possible to activate various SNMP protocols simultaneously.

Menu: Management >> SNMP		
mGuard SNMP server	**SNMPv2c**	When this function is activated, the device can be monitored via the SNMPv2c protocol (read access). **NOTE: Non-secure SNMPv1/v2 protocol** Unlike the SNMPv3 protocol, the older versions SNMPv1/SNMPv2c do not use authentication or encryption, and are therefore not considered to be secure. The SNMPv1/2 protocol should only be used in a secure network environment that is entirely under the control of the operator. When SNMPv2c is activated, the SNMPv1 protocol is also supported. The SNMP server is only activated if access from at least one net zone is permitted (see below). **Default setting:** deactivated
	SNMPv3	When this function is activated, the device can be monitored via the SNMPv3 protocol (read access). The SNMP server is only activated if access from at least one net zone is permitted (see below). **Default setting:** deactivated
	SNMP server can be reached from net zone 1 (Only configurable if SNMP is activated.)	When this function is activated, access from the selected net zone to the device SNMP server is permitted (UDP port 161). **NOTE: Access from the Internet** It may be possible to reach the server from the Internet when the device is connected to the Internet via the activated net zone. **Default setting:** deactivated
	SNMP server can be reached from net zone 2 (Only configurable if SNMP is activated.)	When this function is activated, access from the selected net zone to the device SNMP server is permitted (UDP port 161). **NOTE: Access from the Internet** It may be possible to reach the server from the Internet when the device is connected to the Internet via the activated net zone. **Default setting:** dectivated
SNMPv2c (Only configurable if SNMPv2c is activated.)	When this function is activated, the SNMPv1 and SNMPv2c protocols are supported. **NOTE: Non-secure SNMPv1/v2 protocol** Unlike the SNMPv3 protocol, the older versions SNMPv1/SNMPv2c do not use authentication or encryption, and are therefore not considered to be secure.	

Menu: Management >> SNMP

Read-only community

With the SNMPv1/SNMPv2c version, SNMP encodes the access data as part of what is referred to as a *community*.

Here, the *read-only community* string is used as a password or access key.

Authentication via the *read-only community* string allows limited SNMP write access.

Input format: The string must begin with a letter.

Permitted characters (min. 6, max. 255):

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
0123456789_-

Default setting: Public

SNMPv3

(Only configurable if SNMPv3 is activated.)

Unlike the SNMPv1/v2c protocols, the SNMPv3 protocol is considered secure because it provides the option for user authentication and for encryption.

Encryption and hash algorithms used:

– AES-128
– SHA-2 (SHA-256) with SNMPv3 USM

User name

User name of the SNMPv3 user who would like to access the device SNMP server via the SNMPv3 protocol.

The addition of further SNMPv3 users is not supported.

Input format: Permitted characters (min. 1, max. 200):

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
0123456789_.-

Password

Password of the SNMPv3 user.

Input format: To increase security, the password should contain upper case and lower case characters, numbers, and special characters.

Permitted characters (min. 8, max. 200):

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

Confirm password

Enter the password again.

4.5 System

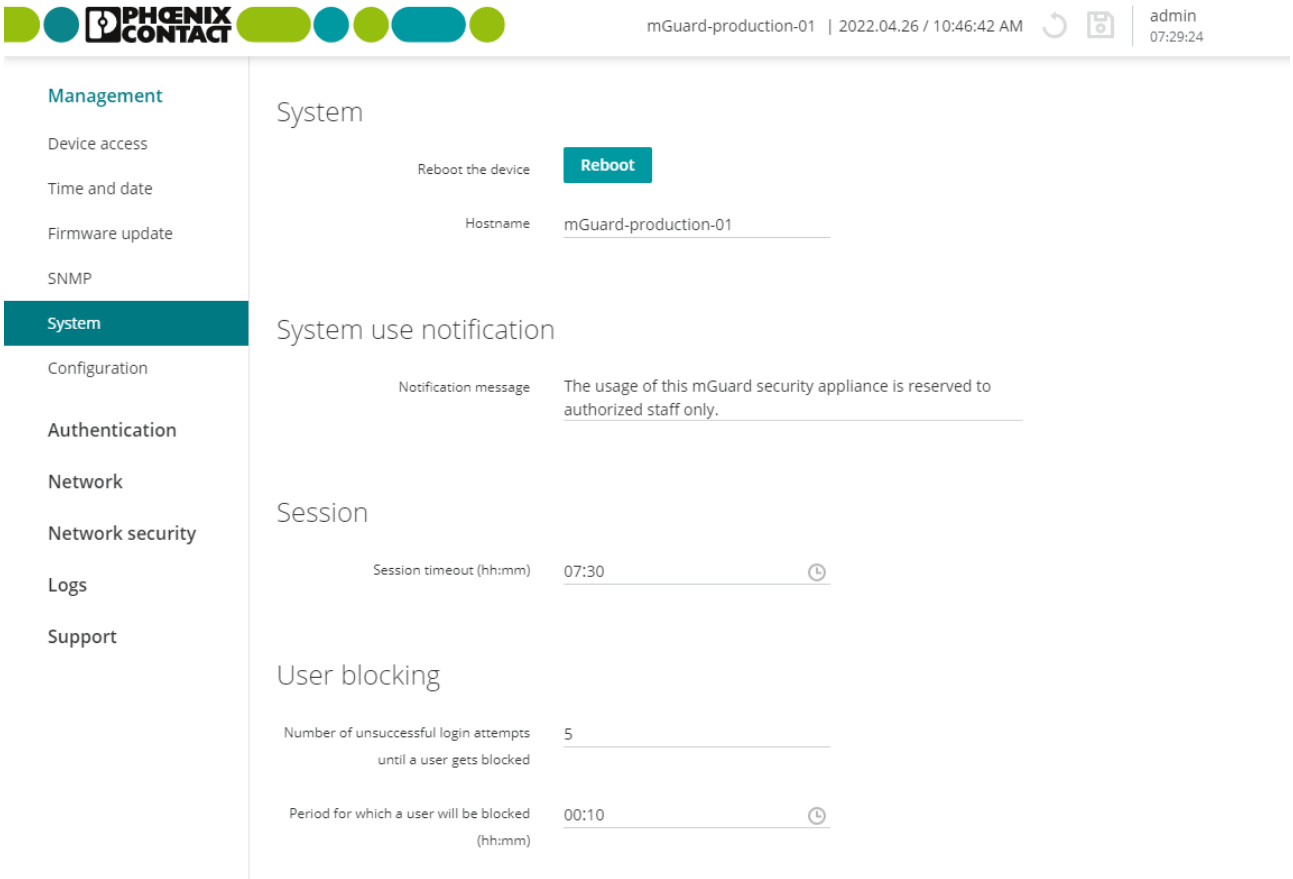


Figure 4-5 Management >> System

Menu: Management >> System		
System	**Reboot the device**	The device is rebooted. **Button** • Click the **Reboot** button to reboot the device. **Note:** All changes that have not been saved will be lost.

Menu: Management >> System		
	Hostname	Name under which the device is always visible and reachable in the network. If the hostname is resolved using the *Domain Name System* (DNS), network devices can address the device directly via its hostname. **Input format:** The name must begin and end with a letter or a number. Permitted characters (min. 1, max. 63): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789-
System use notification	**Notification message**	Freely selectable text for a system use notification that is displayed before logging onto the device (maximum 512 characters). Is displayed for: – Logging on via web-based management (WBM) **Input format:** freely selectable text **Default setting:** *The use of this security appliance is reserved for authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited*.
Session	**Session timeout (hh:mm)**	Length of the *session timeout* (time period). A user session is limited in time by a *session timeout*. The configurable time period of the *session timeout* is between 5 minutes and 8 hours. After the session times out, the user is logged out automatically. The *session timeout* period begins when the user logs in (default setting: 30 minutes). If the user executes an action during a session, the *session timeout* period is reset to the configured start value. **Input format:** hours:minutes (min. 00:05, max. 08:00) **Default setting:** 00:30
User block	**Number of unsuccessful login attempts until a user gets blocked**	Number of unsuccessful login attempts until a user is blocked. Users are automatically blocked after the configured number of unsuccessful login attempts (incorrect password entry) for up to 8 hours (see Below). **Note:** The user block can be prematurely removed by an administrator with the "*Super Admin*" role (see Section 5.1). **Note:** An automatic user block is also removed by rebooting the device. **Input format:** number (min. 1, max. 200) **Default setting:** 5

Menu: Management >> System		
	Period for which a user will be blocked (hh:mm)	Period for which a user will be blocked after unsuccessful log in attempts. Users are automatically blocked after a configurable number of unsuccessful login attempts (incorrect password entry) for up the configured period (see above). **Note:** The user block can be prematurely removed by an administrator with the "*Super Admin*" role (see Section 5.1). **Note:** An automatic user block is also removed by rebooting the device. **Input format:** hours:minutes (min. 00:01, max. 08:00) **Default setting:** 00:10

4.6 Backup configuration

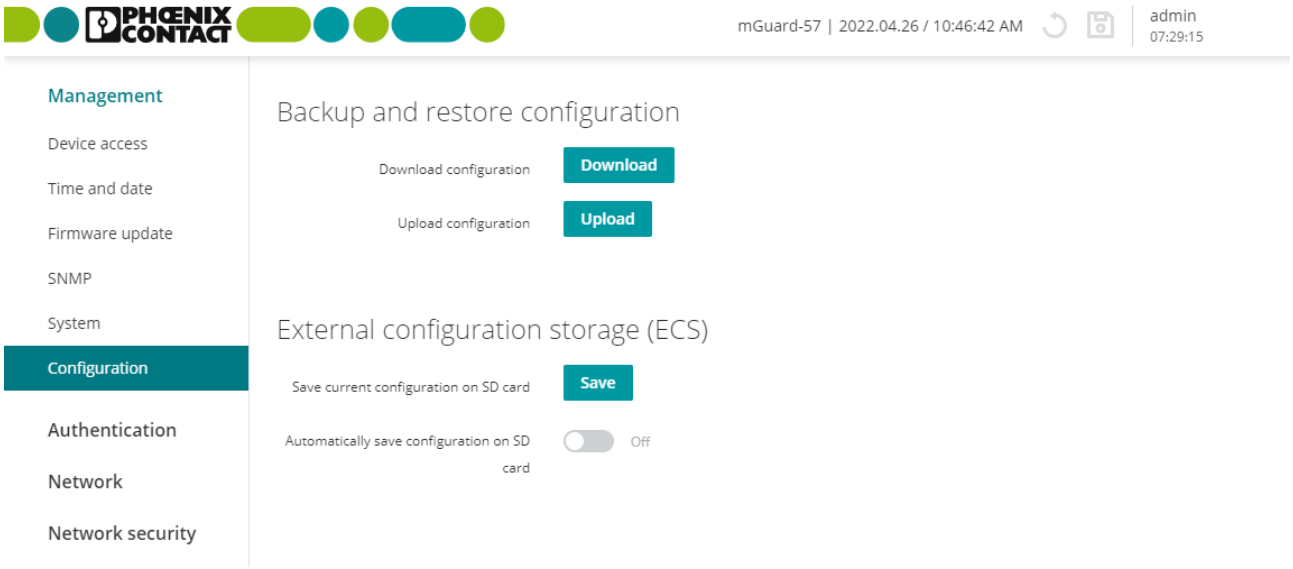


Figure 4-6 Management >> Backup configuration

Menu: Management >> Backup configuration	
Backup and restore configuration	The configuration currently saved on the device can be exported as a JSON file and downloaded to the configuration computer. **Security-relevant information and information for user management are not exported.** This applies to: – all information on user management (local users, user passwords, and LDAP server settings, see Section 5), – The SNMP password – Private encryption keys (e.g., remote logging). This makes it possible to archive any status of the configuration. The saved configuration can be restored on the same device or a different one at a later time. The variable values of the downloaded configuration can be edited with a text editor before being imported. **Prerequisite for importing** The configuration may not have been created with a minor version that is higher than the one that is already installed on the device (see also Section 4.3). The import can only be executed if any necessary adjustments were made to the saved configuration before the import (see also Section A 6). If a configuration is restored on a device with installed firmware version x.y.e (e.g. 1.7.1) that was created with an older minor version "y" (e.g. 1.5.1), the already configured variable values that were not yet present in the older version are retained.

Menu: Management >> Backup configuration

Download configuration

The configuration currently saved on the device will be exported in the JSON format and downloaded to the configuration computer.

Button

- Click the **Download** button to save the configuration to the configuration computer.

File name: *mGuard-configuration.json*

Note: You can change the file name to any name and import it under the new file name.

Note: You can change the variable values with a text editor and then import them again.

Upload a configuration

The configuration currently saved on the configuration computer will be imported to the device.

The configuration may not have been created with a minor version that is higher than the one that is already installed on the device.

Example:

OK: Importing a configuration created with version 1.6.1 to a device with installed version 1.7.0.

ERROR: Importing a version created with version 1.8.1 to a device with installed version 1.7.0.

If a configuration is restored on a device with installed firmware version x.y.e (e.g. 1.6.1) that was created with an older minor version "y" (e.g. 1.5.1), the already configured variable values that were not yet present in the older version are retained.

The import can only be executed if any necessary adjustments were made to the saved configuration before the import (see also Section A 6).

Button

- Click the **Upload** button to import the saved configuration to the device.

⇒ An existing VPN configuration is displayed but not activated yet.

⇒ Invalid variable values will also be marked with a red dot and displayed as described in Section 3.6.4. They must be changed.

- Click the icon to save and apply the configuration.

Menu: Management >> Backup configuration

External configuration memory (ECS)

The configuration/user management currently saved on the device can be exported automatically or manually to an external configuration memory (ECS). An SD card is used as the storage medium.

NOTE: Security-relevant information
The saved configuration contains security-relevant information, such as local users, authorizations, passwords (hashed), and certificates (public keys). The password for the LDAP server is included in plain text. **Exception:** Private keys are not included in the configuration.

NOTE: Security-relevant information
Ensure that only authorized persons are able to access the SD card.

The configuration can be imported from the SD card into any FL MGUARD 1000 device and applied there. In that way, new devices can easily be commissioned based on an already existing configuration.

Prerequisites:

- The devices are set to factory settings.
- The firmware version of "SD card" is lower than/equal to the firmware version of "device".
- SD card technical requirements:
  - SD and SDHC cards up to max. 8 GB
  - VFAT-compatible file system

Please note that the correct function of the SD card and the product can only be ensured when using a Phoenix Contact SD card (e.g., SD FLASH 2GB 2988162). If third-party SD cards are used, it is recommended that card compatibility be verified.

Save current configuration on SD card

The configuration currently saved on the device is written to the SD card inserted.

Ensure that only authorized persons are able to access the SD card.

Re-importing the saved configuration into the device via SD card:

The following applies to all **new devices** or devices that were reset to the factory settings via Smart mode (see Section 3.6.6):

A configuration/user management saved on the inserted SD card is automatically imported into the device and used there when the device is started or commissioned.

Prerequisite:

- The firmware version of "SD card" in the minor version is lower than/equal to the firmware version of "device".
- The SD card contains the three files (individually or bundled as *mGuard.tar.gz:* Use the individual files as first priority!).

If an error occurs during the import, the device will boot with default values. The FAIL and PF1 LEDs will also light up.

Menu: Management >> Backup configuration		
		Button • Click the **Save** button to write the configuration to the SD card. Three files will be saved: – *users_pass.json* – *snmp-pass.conf* – *configuration.json* **Note:** Do not remove the SD card until the write process has been completed.
	Automatically save configuration on SD card	When this function is activated, every configuration change that is saved in the WBM by clicking the icon will be automatically saved to the inserted SD card. Ensure that only authorized persons are able to access the SD card. Three files will be saved: – *users_pass.json* – *snmp-pass.conf* – *configuration.json* **Re-importing the saved configuration into the device via SD card:** The following applies to all **new devices** or devices that were reset to the factory settings via Smart mode (see Section 3.6.6): A configuration/user management saved on the inserted SD card is automatically imported into the device and used there when the device is started or commissioned. **Prerequisite:** – The firmware version of "SD card" is lower than/equal to the firmware version of "device". – The SD card contains the three files (individually or bundled as *mGuard.tar.gz:* Use the individual files as first priority!). If an error occurs during the import, the device will boot with default values. The FAIL and PF1 LEDs will also light up.

5 Menu: Authentication

Only visible and configurable for users with the *Super Admin* user role.

5.1 User management

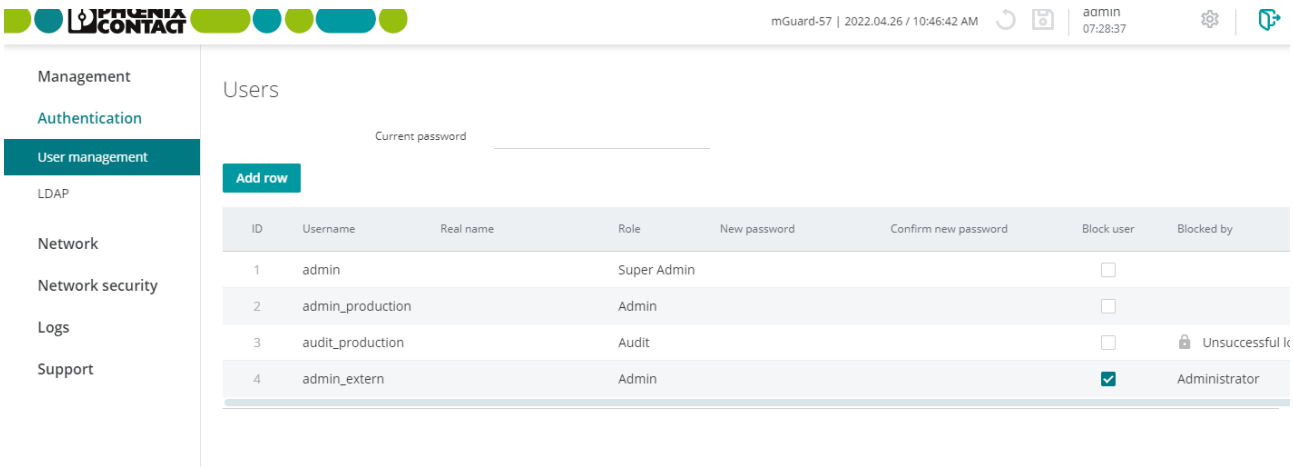


Figure 5-1 Authentication >> User management

Menu: Authentication >> User management	
Users	Users can log in with their password via the web-based management (WBM) or the *Config API*. Users are assigned certain permissions via user roles (see „User roles and permissions“). In the default setting, only the user “*admin*” with the user role “*Super Admin*” and the password “*private*” exists. **NOTE: Change the administrator password during initial login** After logging in for the first time, immediately change the default administrator password of the user “*admin*” (password = *private*). A logged in user cannot delete himself.

Menu: Authentication >> User management

User roles and permissions

Permission/Role	Super Admin	Admin	Audit
Manage users	X		
Configure LDAP	X		
Change configuration	X	X	
Execute action	X	X	
Install firmware updates	X	X	
Check configuration	X	X	X
Change own password	X	X	X
Request device status	X	X	X
Read log entries	X	X	X

What should be done if passwords are no longer recognized

If the passwords of all users are no longer recognized and it is therefore no longer possible to login on the device, it may be necessary to reset the device to the default settings.

NOTE: Data loss
The entire configuration, all settings, users, and their passwords, will be irrevocably deleted.

For this purpose, execute the smart mode function "*Restoring the factory settings*" (see Section A 2).

Logging

The activities of the users are saved in the respective log entries. This includes logging users in and out and configuration changes made by users.

Current password — The password of the logged in user must be specified if changes are made in user management.

ID — Identification number of the user (generated by the system).

User name — Unique user name that the user uses to log into the device.

Input format: The name must begin with a letter or a number. It must not end with a dot.

Permitted characters (min. 2, max. 200):

ABCDEFGHIJKLMNOPQRSTUVWXYZ
abcdefghijklmnopqrstuvwxyz
0123456789_.-

Real name — Freely assignable name for simplification of management.

Menu: Authentication >> User management		
	Role	**Super Admin, Admin, Audit** The selection of a user role assigns certain permissions to the user (see „User roles and permissions“). The standard user in the default “admin” setting has the “*Super Admin*” role. However, users with the “*Super Admin*” role cannot delete themselves.
	New password	The new password for the corresponding user. **Input format:** To increase security, the password should contain upper case and lower case characters, numbers, and special characters. Permitted characters (min. 6, max. 64): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
	Confirm new password	Enter the new password again.
	Block user	When this function is activated, the associated user is blocked and can not log into the device. A logged in user cannot block himself. Logged in users remain logged in during their ongoing session even if they are blocked by another instance. Users authenticated by an LDAP server can only be blocked using the LDAP server user management function. **Default setting:** deactivated
	Blocked by	Information on the reason for the user block: a) Unsuccessful attempt to log in (see Section 4.5) b) Administrator (see above “Block user”) If a user has been automatically blocked, the block can be prematurely removed by clicking the icon in front of the “*Unsuccessful attempt to log in*” message. An automatic user block is also removed by rebooting the device.

5.2 LDAP

Security advice
For reasons of security, an encrypted TLS connection should always be used between the device (mGuard) and the LDAP server.

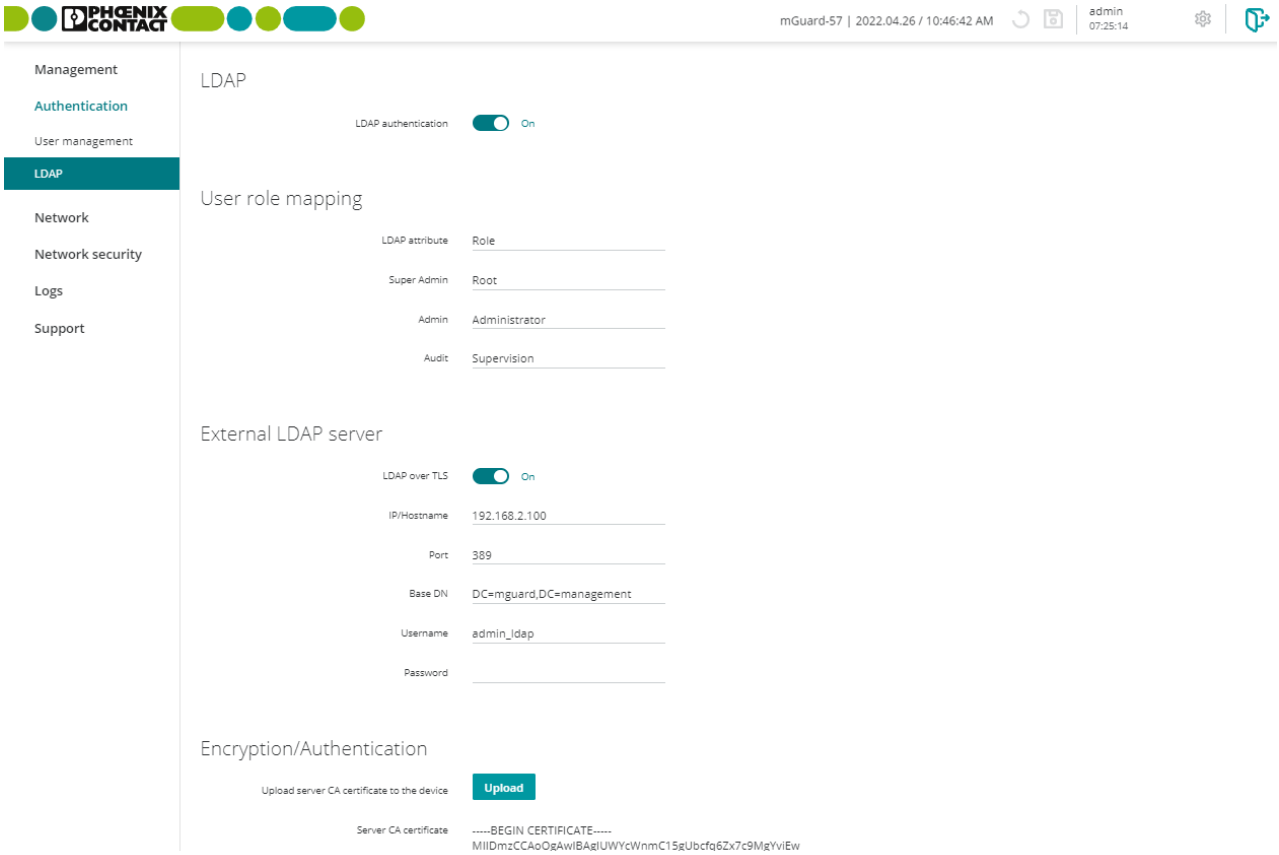


Figure 5-2 Authentication >> LDAP

Menu: Authentication >> LDAP	
LDAP	LDAP (*Lightweight Directory Access Protocol*) is a client/server protocol with which data from a remote directory service can be queried and managed via the IP network. Here, the mGuard device acts as the LDAP client. By using LDAP, the device user management can be outsourced to a central database on an LDAP server, which takes over user authentication. It is still possible to configure local users on the device, but in principle this is no longer necessary (exception: a local user with the *Super Admin* role must exist). Users managed on the LDAP server can log into the mGuard device by entering their centrally managed access data (user name and password) .

Menu: Authentication >> LDAP		
	LDAP authentication	When this function is activated, the device can access a configured LDAP server via the LDAP protocol. Users managed on the LDAP server can be authenticated when logging into the device via the LDAP protocol and entering their LDAP access data. When a user logs in (login), the device first checks whether the user has been configured as a **local user** on the device. If this is the case, the local user can only be logged in with the **locally configured user password**. In this case, the LDAP server is not queried. The role that a user logged in via LDAP is assigned on the LDAP server must also exist on the mGuard device (see Section 5.1). A user logged in via LDAP is automatically logged out when the function is deactivated during the ongoing session. **Default setting:** deactivated
User role mapping	**LDAP attribute**	Name of the attribute in which the role/user class is specified for each LDAP user. To be able to assign the roles, they must be assigned the same LDAP attribute on both the LDAP server and on the device. **Example configuration:** Configuration on the LDAP server**:** – **Role***: Role_1* – **Role***: Role_2* – **Role***: Role_3* LDAP attribute on the mGuard device**:** – **Role** Permitted characters (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.-

Menu: Authentication >> LDAP		
	Super Admin **Admin** **Audit**	When logging in via LDAP, the user role (or user roles) assigned to the LDAP user on the LDAP server must be assigned to at least one of the three available user roles on the device (see also Section 5.1). If the user role of the LDAP user cannot be assigned, it is not possible for this user to log in. **Example:** **Device <-> LDAP server** Super Admin <-> Role_1 Admin <-> Role_2 Audit <-> Role_3 If several user roles are assigned to one LDAP user, the user is logged in with the role with the highest possible authorization level when logging in. Permitted characters (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.-
External LDAP server	**LDAP via TLS**	When this function is activated, the data is transmitted with encryption using a TCP connection. **Note:** For reasons of security, an encrypted TLS connection should always be used between the device (mGuard) and the LDAP server. (See also "Encryption algorithms used" on page 15.) **Prerequisite:** To ensure the integrity and authenticity of the encrypted TCP connection, the server certificate (CA certificate) from the remote server must be installed on the device (see Below).
	IP/Hostname	IP address or hostname of the external LDAP server to which the device is supposed to send requests for user authentication. **Input format**: IPv4 address or hostname
	Port	Port on which the LDAP server accepts requests. **Default setting:** 389

Menu: Authentication >> LDAP		
	Base DN	Base address in the directory on the LDAP server. The search for the desired objects (e.g., user data) is restricted to a smaller area in the LDAP server directory tree. This takes place exclusively below the specified base address (node). **Input format:** directory path (*DC=x,DC=y,DC=z*) Permitted characters (min. 1, max. 1024): The entry must begin with one of the following characters: ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789._ These characters can each be connected by one of the following four characters: -_=, Example: *DC=mguard,DC=management,DC=user*
	User name	User name with which the device logs into and authenticates the LDAP server. Permitted characters (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.-
	Password	Password with which the device logs into and authenticates the LDAP server. **Input format:** To increase security, the password should contain upper case and lower case characters, numbers, and special characters. Permitted characters (min. 6, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!#$%&()*+,-./:;<=>?[]^_`{|}~@
Encryption/ authentication	**Use of certificates** Called “authentication,” the documentation and verification of authenticity is a fundamental element of secure communication. The X.509 authentication method relies on certificates to ensure that the “correct” partners communicate with each other and that no “incorrect” partner is involved in communication (see also Section B 3, “Explanation of terms” under „X.509 certificate“). **Certificate** A certificate is used as proof of the identity of the certificate owner. The relevant authorizing body in this case is the CA (*certificate authority*). The digital signature on the certificate is provided by the CA. By providing this signature, the CA confirms that the authorized certificate owner possesses a private key that corresponds to the public key in the certificate. The name of the certificate issuer appears under Issuer on the certificate, while the name of the certificate owner appears under Subject.	

Menu: Authentication >> LDAP		
Server certificate	**Upload server CA certificate to the device**	CA certificate with which the device authenticates the remote server (LDAP server). The CA certificate is provided by the remote server operator and must be uploaded to the device (X.509 certificate with public key). An encrypted TCP connection to the remote server can only be established successfully if it in turn has a certificate issued by the CA certificate (with the *secret* key) or a valid certificate chain with the CA certificate as the highest instance. **Button** • Click the **Upload** button to upload the CA certificate of the remote server (LDAP server) from a configuration computer to the device. **Format:** The maximum file size allowed is 1 MB. **Note:** A CA certificate that has already been uploaded will be deleted and replaced in this case.
	Server CA certificate	Displays the uploaded CA certificate.

6 Menu: Network

6.1 Interfaces

6.1.1 Interfaces

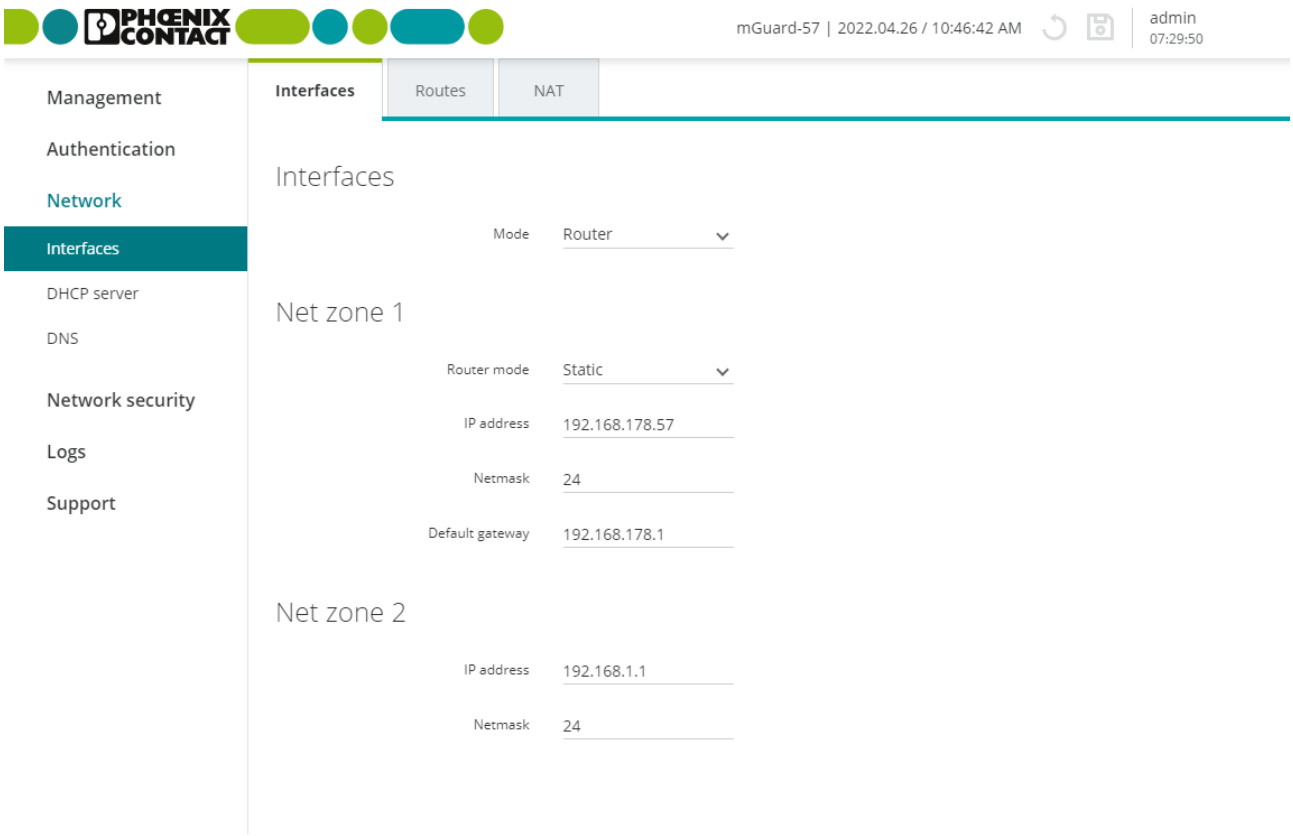


Figure 6-1 Network >> Interfaces >> Interfaces: Configure net zone 1/2

Menu: Network >> Interfaces >> Interfaces		
	Mode	The device can be operated in two network modes (*Router mode* and *Stealth mode*). **Router** See “Router mode” on page 56 **Stealth** See “Stealth mode” on page 59

Menu: Network >> Interfaces >> Interfaces

Router mode

If the device is in Router mode, it acts as a gateway between different subnets. The data traffic is *routed* between the two network interfaces (net zones) of the device.

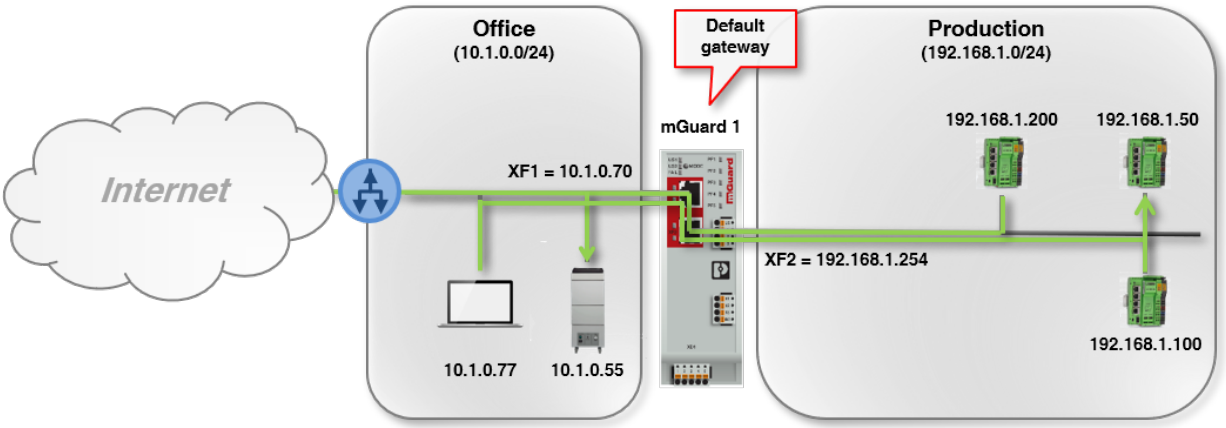


Figure 6-2 Example: Router mode

Clients in the subnet of one net zone (e.g., *Office*) can communicate and exchange data with clients in the subnet of the other net zone (e.g., *Production*).

The network configuration of net zone 1 (XF1) of the device can be entered statically or retrieved from a DHCP server. In net zone 2 (XF2–XF5), the device can act as a DHCP server.

The security and firewall functions of the device are applied to incoming and *routed* data traffic.

Net zone 1 (XF1)

(Only configurable in "*Router*" mode)

The device network interfaces are assigned to two different net zones each of which has an individual network configuration (IPv4 address and netmask).

The DHCP- or static-configured networks of the two net zones must not overlap.

Access to external networks or to the Internet is usually established via net zone 1 (XF1).

Connected network clients in the same net zone (subnet) can access the device via the configured IP address.

The network address of net zone 1 (XF1) can be statically configured on the device or assigned via DHCP.

The IP address of the corresponding net zone of the device has to be indicated as the default gateway for the connected clients so that they can use the device as a direct gateway.

NAT/IP masquerading may have to be activated on the device so that devices from one net zone can communicate with devices in other net zones or with the Internet (see "NAT" on page 62).

Menu: Network >> Interfaces >> Interfaces		
	Router mode (Only configurable in "*Router*" mode)	Mode that is used to determine how a network configuration is assigned to the net zone. **DHCP** The net zone is automatically assigned a network configuration (IP address, subnet mask, and, as an option, a default gateway and DNS server) by a DHCP server if a DHCP server is available in the network. **Static** Users have to manually assign a static network configuration to the net zone (IP address, subnet mask, and, as an option, a default gateway). **Default setting:** DHCP
	IP address (Only configurable in "*Static*" router mode) (Status information in "*DHCP*" router mode)	IP address of network interface XF1 (net zone 1). **Note:** Changing the IP address that you are currently using to access the device will cause the device to no longer be available at this address after the configuration is saved. Log back in via the changed IP address. **Input format:** IPv4 address
	Netmask (Only configurable in "*Static*" router mode) (Status information in "*DHCP*" router mode)	Subnet mask that defines the subnet where the device is located. **Input format:** CIDR or decimal format, e.g., 24 (= 255.255.255.0)
	Default gateway (Only configurable in "*Static*" router mode) (Status information in "*DHCP*" router mode)	IP address of the default gateway to which the device sends connection requests to reach unknown subnets or the Internet. A device in the subnet of net zone 1 (XF1) or in the subnet of net zone 2 (XF2–XF5) can be specified as the default gateway. An empty field without entry means that no default gateway is configured on the device. **Input format:** IPv4 address
	DNS server (Status information in "*DHCP*" router mode)	IP addresses of one or several DNS servers assigned by the DHCP server. A DNS server (DNS = *Domain Name System*) allows clients to resolve hostnames into IP addresses. **Note:** If the network configuration was assigned by the DHCP server, it is not possible to select the preset DNS root server or the configuration of the user-defined DNS server (see "External DNS server" on page 76). This also applies if the DHCP server does not assign a DNS server.

Menu: Network >> Interfaces >> Interfaces

Net zone 2 (XF2–XF5)

(Only configurable in "*Router*" mode)

The device network interfaces are assigned to two different net zones which each have an individual network configuration (IPv4 address/netmask).

The DHCP- or static-configured networks of the two net zones must not overlap.

Usually, access to the local (protected) network is established via net zone 2 (XF2–XF5).

Connected network clients in the same net zone (subnet) can access the device via the configured IP address.

The network address of net zone 2 (XF2–XF5) must be statically configured. Unlike net zone 1 (XF1), it cannot be assigned via DHCP.

The IP address of the corresponding net zone of the device has to be indicated as the default gateway for the connected clients so that they can use the device as a direct gateway.

NAT/IP masquerading may have to be activated on the device so that devices from one net zone can communicate with devices in other net zones or with the Internet (see "NAT" on page 62).

IP address	IP address of network interface XF2–XF5 (net zone 2). **Note:** Changing the IP address that you are currently using to access the device will cause the device to no longer be available at this address after the configuration is saved. Log back in via the changed IP address. **Input format:** IPv4 address **Default setting:** 192.168.1.1
Netmask	Subnet mask that defines the subnet where the device is located. **Input format:** CIDR or decimal format, e.g., 24 (= 255.255.255.0) **Default setting:** 24

Menu: Network >> Interfaces >> Interfaces

Stealth mode

Stealth mode is used to protect one or more local clients in an existing subnet (e.g., machine controls in a production network) against unwanted network access without having to change their IP settings.

To do this, the device is added between the clients and the surrounding subnet via its two network interfaces (net zones) so that all the data traffic to and from the clients is routed through the device.

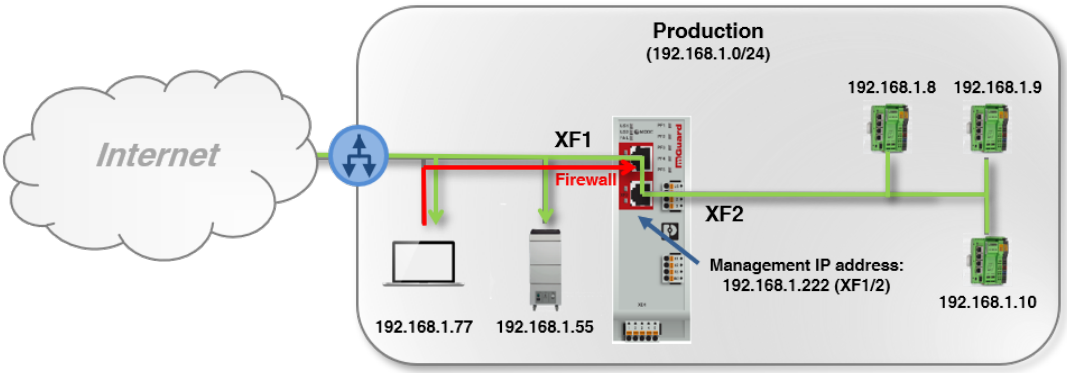


Figure 6-3 Example: Stealth mode (with activated firewall XF1 --> XF2)

The network configuration of the connected clients does not have to be changed.

The server services DHCP, NTP, SNMP, and DNS server are deactivated on the device. The security and firewall functions of the device are generally applied to incoming and routed data traffic.

(Stealth mode) (Only configurable in "*Stealth*" mode)	**Management IP address**	IP address via which the device is reachable in Stealth mode and can be managed. The management IP address is available on all network interfaces (net zones). The device is configured via the WBM or the *Config API*. **Note:** Changing the IP address that you are currently using to access the device will cause the device to no longer be available at this address after the configuration is saved. Log back in via the changed IP address. **Input format:** IPv4 address **Default setting:** 192.168.1.1
	Netmask	Subnet mask that defines the subnet where the device can be reached in Stealth mode via the management IP address. **Input format:** CIDR or decimal format, e.g., 24 (= 255.255.255.0) **Default setting:** 24

Menu: Network >> Interfaces >> Interfaces		
	Default gateway	IP address of the default gateway to which the device sends connection requests to reach unknown subnets or the Internet. In Stealth mode, the device can use it to send requests as a client, for example, to an NTP or DNS server. When a management IP address is assigned, the default gateway of the network in which the device is located must be specified. The default gateway can be reached via net zone 1 (XF1) and net zone 2 (XF2–XF5). **Input format:** IPv4 address **Default setting:** 192.168.1.254

6.1.2 Routes

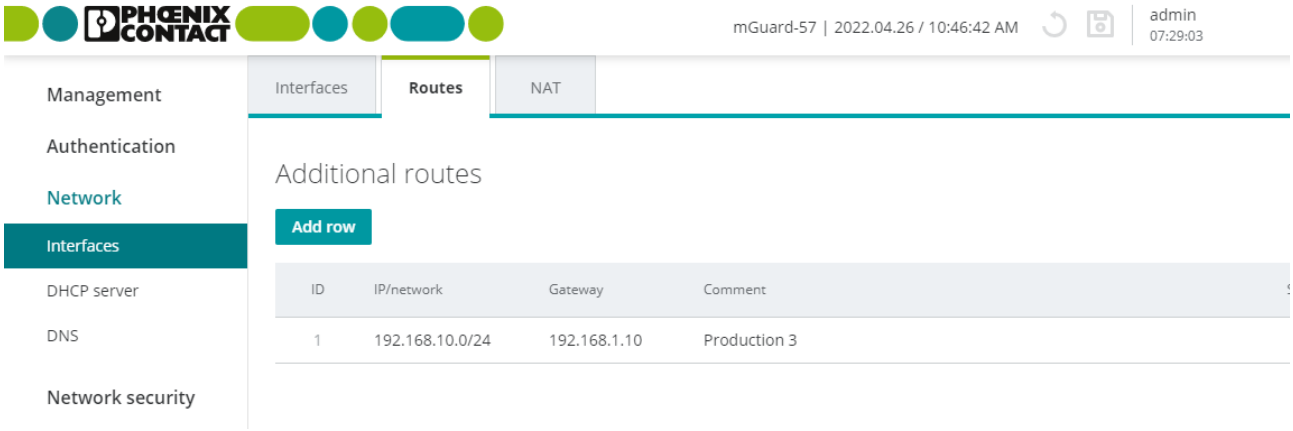


Figure 6-4 Network >> Interfaces >> Routes: Configure static routes

Menu: Network >> Interfaces >> Routes

Routes

(Only configurable in "*Router*" mode)

Using statically entered routes, the device can reach network destinations that are not known to its default gateway.

These destinations can also be reached by connected network clients that use the device as the default gateway.

The device forwards data packets to destinations that can be reached via the static route directly to the gateway specified in the static route.

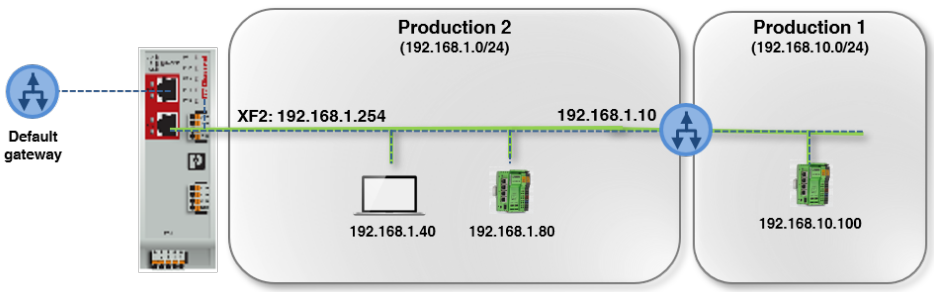


Figure 6-5 Example: Additional static routes

Requests from clients in *Production 2* which want to reach destinations in the subnet 192.168.10.0/24 are forwarded by the device via the static route 192.168.1.10.

IP/network

Destination (network or IP address) that should be reached via an additional route.

Input format: IPv4 address, IPv4 network (CIDR notation)

Gateway

IP address of the gateway via which the destination can be reached using the additional route.

Input format: IPv4 address

Comment

Freely selectable comment.

Permitted characters: max. 128

6.1.3 NAT

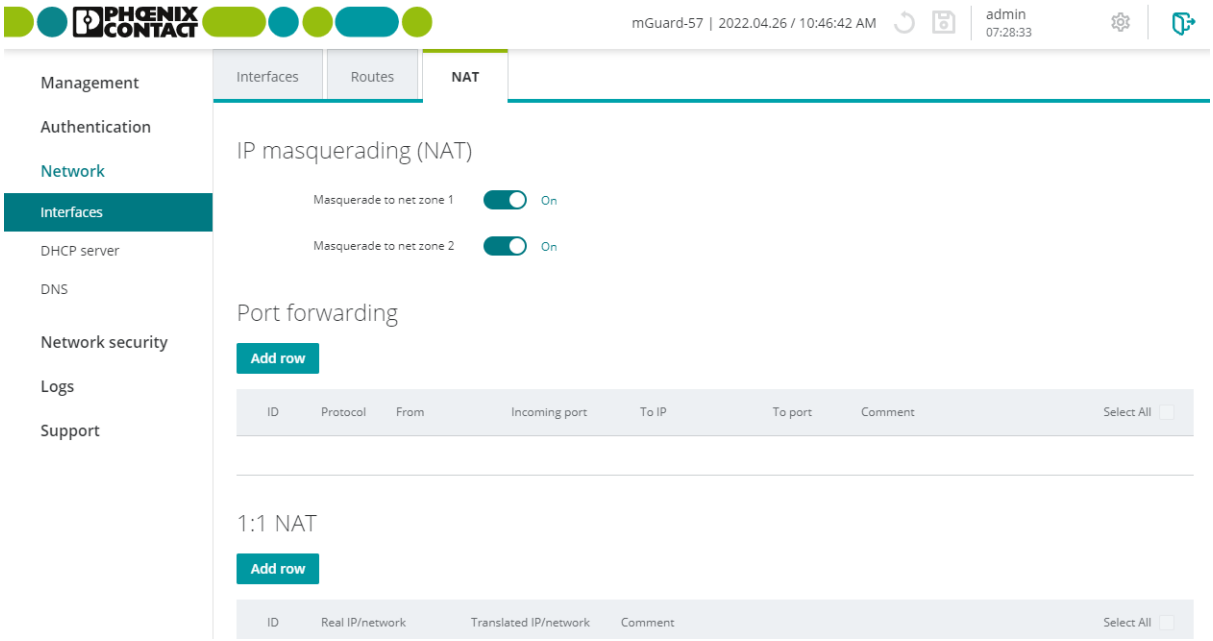


Figure 6-6 Network >> Interfaces >> NAT: IP masquerading, port forwarding, and 1:1-NAT configuration

Menu: Network >> Interfaces >> NAT	
Network Address Translation (NAT) (Only configurable in "*Router*" mode)	**IP masquerading and 1:1 NAT** *Network Address Translation* (NAT) is used to hide the real IP address of connected network clients from external network devices. To do so, the device, in its function as NAT router, replaces the sender address specified in the IP header of a requesting client with – its own IP address (**"IP masquerading (NAT)"**) or – a translated (virtual) IP address (**"1:1-NAT"**). With this (translated) IP address as the sender address, the device forwards requests to external network devices. They send their response packets to the (translated) sender address, which the device then translates into the real IP address of the requesting client. In cases of 1:1 NAT, network devices can also send individual requests to the translated IP address. This way, for example, an entire ("private") network can be hidden behind the device. The real IP addresses of clients in the "private" network remain hidden during communication with the other network. See **"IP masquerading (NAT)" on page 63** and **"1:1-NAT" on page 68**. **Port forwarding** With port forwarding, data packets that are sent (from external devices) to a certain device port are forwarded to a defined destination IP address and a defined destination port in the (local) device subnet. See **"Port forwarding" on page 65**.

Menu: Network >> Interfaces >> NAT

IP masquerading (NAT)

(Only configurable in "*Router*" mode)

With **IP masquerading,** the device masks the IP addresses of senders from network clients with its own external IP address in order to hide network structures, for example:

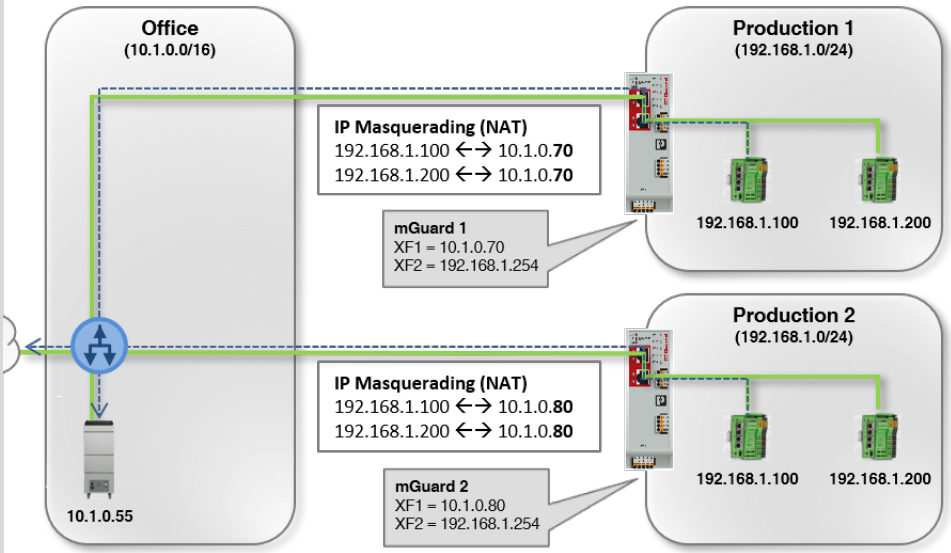
When network clients transmit data through the device, the device replaces the source IP addresses (*src_ip*) with its own IP address (of the outgoing interface).

As the source IP address, the data recipients are always informed of the IP address of the mGuard device. They then transmit their response packets back to the mGuard device, which in turn forwards it to the original sender (network client).

The IP addresses of the requesting clients and the associated network structure are masked and remain hidden to external network devices.

To do so, the connection data in the data packets of the requests are saved in a *Connection Tracking* table and compared to the connection data of the responses.

If the masked clients are to be reached from outside, the IP address of the device **cannot** be used to do this. In cases of external requests, the masked clients must be contacted using their real IP address. (The network and general routing settings must be configured accordingly.)



Requests from the **PCLs (Production)** are sent to the IP address of the **Office server (10.1.0.55)** and masked with the IP address of **the mGuard device (10.1.0.70** resp. **10.1.0.80)** as the source address.

Figure 6-7 Example: IP masquerading to net zone 1

Example

IP masquerading is often used if the "private" IP addresses cannot or should not be routed externally, for example because a private address range such as 192.168.1.x or the internal network structure of a production network should be hidden.

This way, several production cells with identical IP settings can be easily integrated into the network infrastructure.

Menu: Network >> Interfaces >> NAT		
	Masquerade to net zone 1	When this function is activated, the NAT masquerading rule is applied to data packets (requests) that leave the device via the selected network interface (XF1/net zone 1). In the data packet, the sender's IP address is translated into the IP address of the network interface (XF1/net zone 1). **Default setting:** activated
	Masquerade to net zone 2	When this function is activated, the NAT masquerading rule is applied to data packets (requests) that leave the device via the selected network interface (XF2–XF5/net zone 2). In the data packet, the sender's IP address is translated into the IP address of the network interface (XF2–XF5/net zone 2). **Default setting:** deactivated

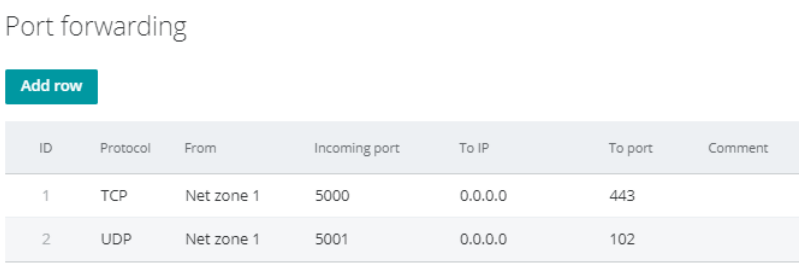
Menu: Network >> Interfaces >> NAT

Port forwarding

(Only configurable in "*Router*" mode)

With port forwarding, data packets that are sent to the IP address and to a specific device port are forwarded to another destination IP address and another destination port in the network.

The original destination IP address and the original destination port in the header of the incoming data packet are translated according to the port forwarding rule.



The header translation is entered in the device's *Connection Tracking* table. Response packets are compared to these entries and the header data is translated back to the original values.

The firewall automatically permits data traffic to and from the defined IP addresses and ports which were defined in a port forwarding rule.

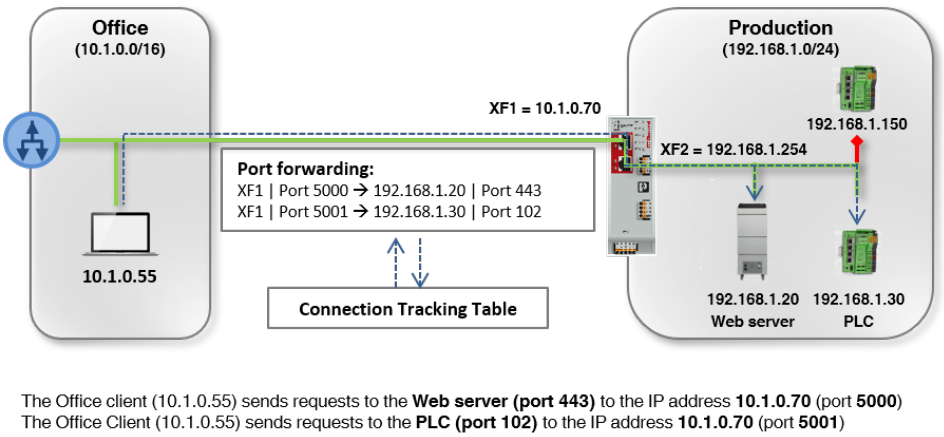


Figure 6-8 Example: Port forwarding

Example

Port forwarding is often used to make individual devices or server services in a local network (e.g., web servers) systematically reachable from the external network or the Internet (see figure):

- The **web server (192.168.1.20/port 443)** in the production network can be reached from the office network via the IP address of the device (**XF1 = 10.1.0.70**) and port **5000**.
- The **PLC (192.168.1.30/port 102)** in the production network can be reached from the office network via the IP address of the device (**XF1 = 10.1.0.70**) and port **5001**.

All other devices in the production network (e.g., PLC 192.168.1.150) will not be reached from the outside. They are protected by the firewall.

Menu: Network >> Interfaces >> NAT

Port forwarding rules are applied before firewall rules

The rules for port forwarding are applied before the configured firewall rules for routed data traffic are applied (see Section 7).

This means that a firewall rule that blocks all incoming data traffic is not applied if a port forwarding rule applies.

ID	Identification number of the rule (generated by the system) The ID determines the order in which the rules are applied, starting with the lowest ID.
Protocol	**TCP, UDP** Network protocol that must be used to transmit the data packets so that the rule is applied. **Default setting:** TCP
From	**Net zone 1, net zone 2** Net zone from which the data packets must be sent to the device so that the rule is applied. **Default setting:** Net zone 2
Incoming port	Device network port to which the data packets must be sent so that the rule is applied. Data packets sent to this port are usually forwarded to the specified destination IP address (*To IP*) and the defined destination port (*To port*): – The destination IP address in the data packet header is translated into the destination IP address defined in the rule (*To IP*). – The destination port in the data packet header is translated into the destination port defined in the rule (*To port*). **Input format:** 1 – 65535, excluding the following ports, because they are used by the device's services: DNS (53), HTTPS (443), NTP (123), SNMP (161), DHCP (67, 68) **Default setting:** 1
To IP	IP address of the destination client to which the incoming data packets are forwarded when the rule is applied. The original destination address in the header of the data packet is translated into this IP address. **Input format:** IPv4 address **Default setting:** 0.0.0.0

Menu: Network >> Interfaces >> NAT		
	To port	Network port to which the incoming data packets are forwarded if the rule is applied. The original destination port in the data packet header (see "Incoming port") is translated into this port. **Input format:** 1 – 65535 **Default setting:** 1
	Comment	Freely selectable comment. Permitted characters: max. 128

Menu: Network >> Interfaces >> NAT

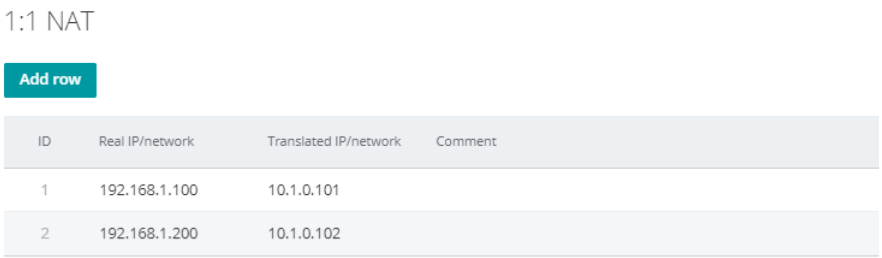
1:1-NAT

(Only configurable in "*Router*" mode)

A **real network** is mapped to a **translated (virtual) network**.

The IP addresses of the clients in the real network are translated in accordance with the 1:1 NAT rule such that communication with clients in the other (translated) network does not take place via the real, but rather the translated IP addresses.

The real network (mostly private) therefore remains hidden from the network participants in the other network (mainly public).



Example 1

With their real IP addresses, machine control systems (PLCs) in the production network are hidden from network participants in the office network. They communicate with the office network via their translated IP addresses (e.g., 192.168.1.100 <--> 10.1.0.100).

The are available for requests from the office network via their translated IP addresses. ARP requests from the office network are responded to by the mGuard device as the representative.

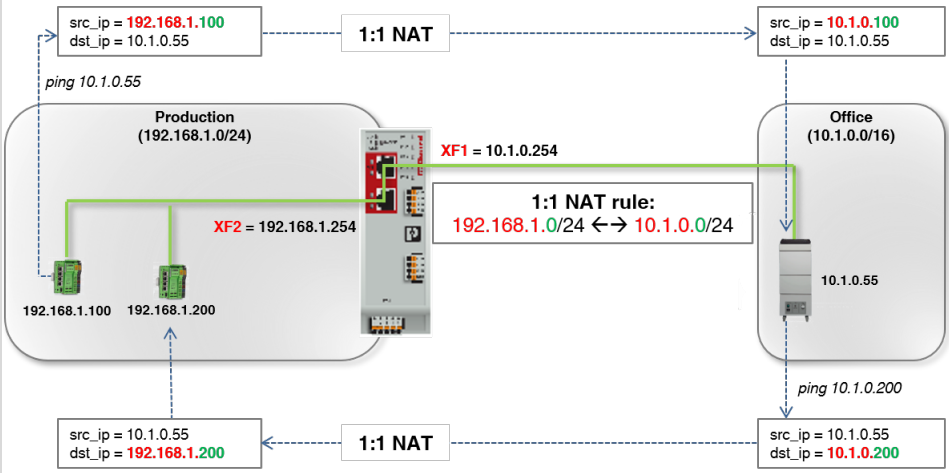


Figure 6-9 Example: 1:1 NAT (two networks)

Menu: Network >> Interfaces >> NAT

Example 2

In practice, an identical IP configuration for connected machines is often used in different production cells. This would lead to address conflicts.

To resolve this problem via 1:1 NAT, the device replaces each network part of the real client IP addresses in the production network with the network part of a subnet in the office network: e.g., 192.168.1.0/24 <--> 10.1.1.0/24.

Clients in the office network and in the production networks can now communicate with each other in both directions.

ARP requests from the office network are responded to automatically by the mGuard device as the representative.

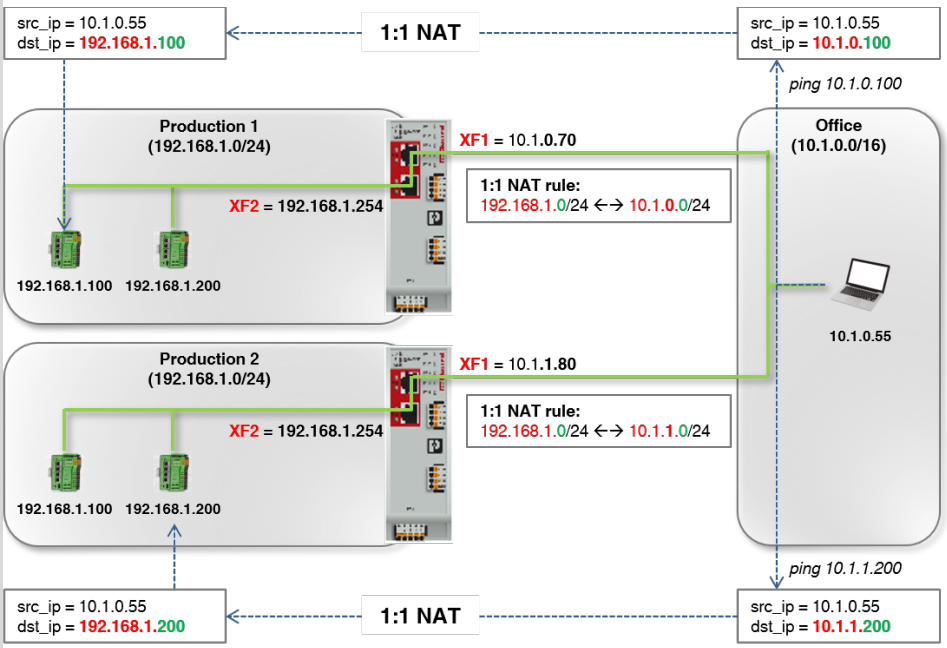


Figure 6-10 Example: 1:1 NAT (identical networks)

ID

Identification number of the rule (generated by the system)

The ID determines the order in which the rules are applied, starting with the lowest ID.

Menu: Network >> Interfaces >> NAT

Real IP/network

Data traffic sent from or to network clients of the real network are subject to the 1:1 NAT rule.

1:1 NAT

With 1:1 NAT, the network part (red) of the IP addresses of clients in the real network are translated to the network part of another (translated) network (see example).

The host part (green) of the IP addresses assigned to the clients remain unchanged.

Example (Figure 6-9 and 6-10)

1:1 NAT rule: 192.168.1.0/**24** <-> 10.1.0.0/**24**

⇒ **Translation:** 192.168.1.100 <-> 10.1.0.100

⇒ **Translation:** 192.168.1.200 <-> 10.1.0.200

The network part and host part of an IP address are defined by the subnet mask (e.g., 192.168.70.80/**16** or 10.1.1.30/**24**).

Real IP

If the netmask is 32, individual IP addresses and not networks are translated by the 1:1 NAT rule:

Note: The netmask **/32** may not be used in the configuration in the Config API. The IP address must be entered without netmask instead.

1:1 NAT rule: 192.168.1.40 <-> 10.1.5.40

⇒ **Translation:** 192.168.1.40 <-> 10.1.5.40

In practice

Clients in both networks can communicate with each other in both directions. At the same time, the real (mostly private) network is not visible in the other (mostly public) network:

– The respective translated client IP addresses in the real network appear as the sender address to the network participants in the other network.
– To reach clients in the real network from the other network, their translated IP addresses must be used.
– ARP requests to the translated client addresses in the real network are automatically responded to by the device as the representative.

Prerequisite

– Both the real and the translated networks must use the same subnet mask.
– The translated IP client addresses in the real network must not yet be assigned in the other (translated) network.
– Firewall rules are generally also applied to translated IP addresses.

Input format: IPv4 address, IPv4 network (CIDR notation)

Menu: Network >> Interfaces >> NAT		
	Translated IP/network	The network to which the real IP addresses of the clients in the real network are to be translated (see “Real IP/network”). **Prerequisite** – Both the real and the translated networks must use the same subnet mask. – The translated IP client addresses in the real network must not yet be assigned in the other (translated) network. **Translated IP** If the netmask is 32, individual IP addresses and not networks are translated by the 1:1 NAT rule. **Input format:** IPv4 address, IPv4 network (CIDR notation)
	Comment	Freely selectable comment. Permitted characters: max. 128

6.2 DHCP server

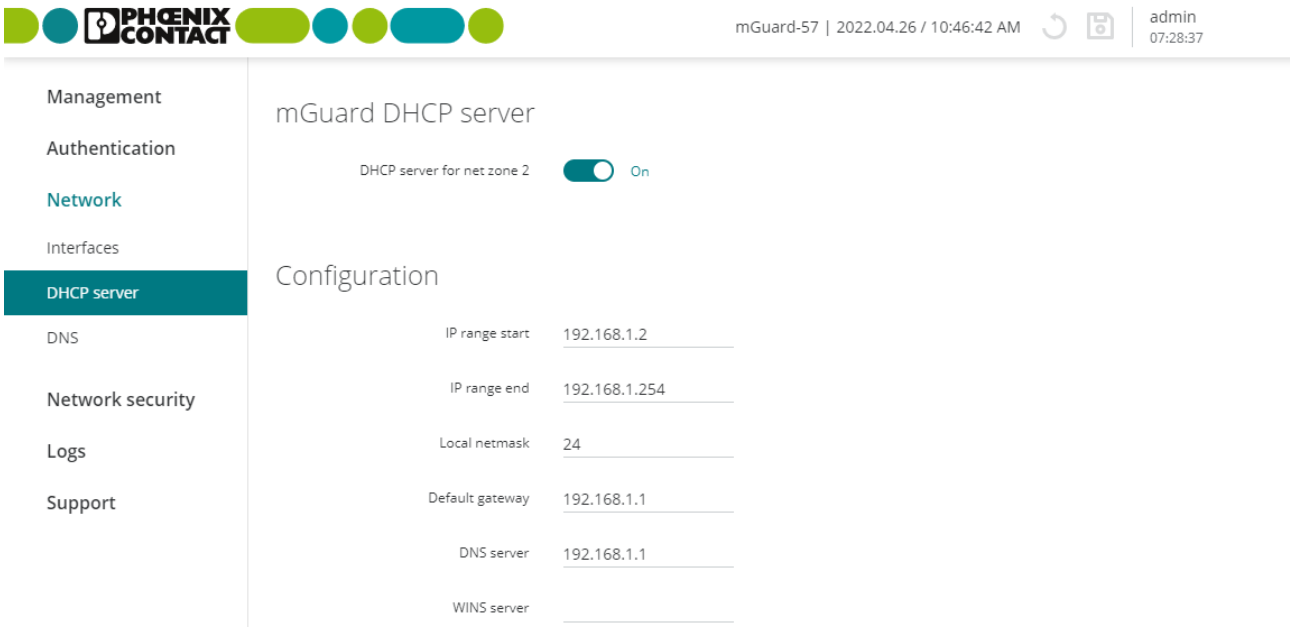


Figure 6-11 Network >> DHCP server: Configure DHCP server

Menu: Network >> DHCP server		
mGuard DHCP server	With the *Dynamic Host Configuration Protocol* (DHCP), requesting network clients are automatically assigned a network configuration. Connected clients must be configured in such a way that they send a DHCP request to receive a network configuration from a DHCP server. In the other case, the configuration must be statically configured for each client.	
	DHCP server for net zone 2	When this function is activated, requesting clients that are connected to the device via net zone 2 are assigned a network configuration. **Note:** The requests to UDP port 67 are always accepted regardless of the firewall table settings of the device if the DHCP server is activated. The server then assigns IP addresses to the clients from the configured IP address range. **Default setting:** activated
Configuration (Only configurable if the DHCP server is activated for net zone 2.)	**IP range start**	Start of the IP address range from which the DHCP server assigns IP addresses to requesting clients. The range should be chosen such that the IP addresses it contains can be reached in the assigned subnet (see below, ""Local netmask""). **Input format:** IPv4 address **Default setting:** 192.168.1.2

Menu: Network >> DHCP server		
	IP range end	End of the IP address range from which the DHCP server assigns IP addresses to requesting clients. The range should be chosen such that the IP addresses it contains can be reached in the assigned subnet (see below "Local netmask"). **Input format:** IPv4 address **Default setting:** 192.168.1.254
	Local netmask	Subnet mask that the DHCP server assigns to requesting clients. The range from which network clients are assigned IP addresses should be chosen such that the IP addresses can be reached in the assigned subnet (see above, "IP range start" and "IP range end"). **Input format:** CIDR or decimal format, e.g., 24 (= 255.255.255.0) **Default setting:** 24
	Default gateway	IP address of the default gateway the DHCP server assigns to requesting clients. Usually this is the internal IP address of the device. **Input format:** IPv4 address **Default setting:** 192.168.1.1
	DNS server	IP address of a DNS server that the DHCP server assigns to requesting clients. A DNS server (DNS = *Domain Name System*) allows clients to resolve hostnames into IP addresses. If the DNS server of the device is to be used, the IP address of the net zone on which this service is active must be specified (default setting: net zone 2 = 192.168.1.1). **Input format:** IPv4 address **Default setting:** 192.168.1.1
	WINS server	IP address of a WINS server that the DHCP server assigns to requesting clients. A WINS (*Windows Internet Naming Service*) server allows clients to resolve hostnames (*NetBIOS* names) into IP addresses. **Input format:** IPv4 address **Default setting:** Empty

6.3 DNS

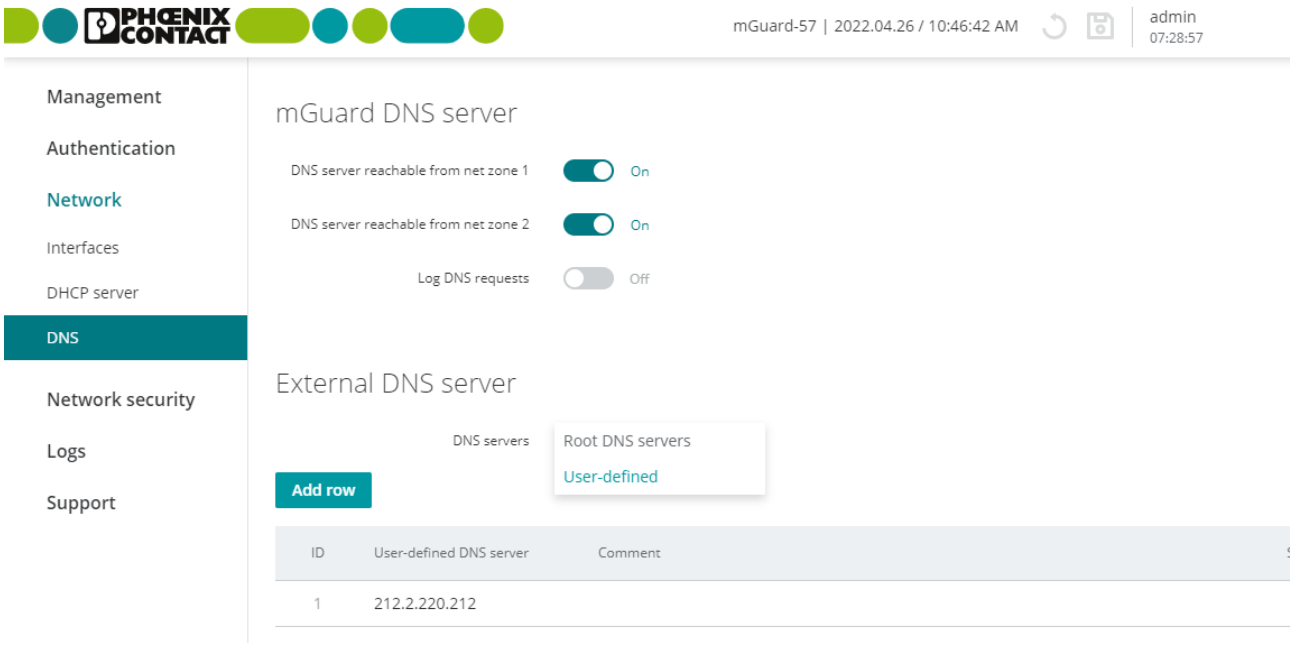


Figure 6-12 Network >> DNS: Configure DNS server and DNS client

Menu: Network >> DNS	
mGuard DNS server	If the device is to establish a connection to a peer (e.g., to an NTP server) whose address is specified in the form of a hostname (e.g., *www.ntp-server.com*), the device must determine which IP address belongs to the hostname. To do so, the device, as the DNS client, connects to an **external DNS server** to query the corresponding IP address there. The information regarding a request returned by the DNS server; i.e., the resolution of a hostname into an IP address, is saved to the DNS cache of the device. When using host names, there is always the risk of an attacker manipulating or blocking DNS requests (i.e. *DNS spoofing*). You should therefore only configure trustworthy and secure DNS servers on the mGuard device – if possible from your internal company network – ,so as to avoid these types of attacks. Network clients connected to the device can use the device as an **mGuard DNS server** and send DNS requests to the device. If the connected clients receive their network configuration from the device via DHCP, the device will be assigned automatically to the clients as the DNS server.

Menu: Network >> DNS		
	DNS server reachable from net zone 1	When this function is activated, access from the selected net zone to the DNS server of the device is permitted (UDP/TCP port 53). **NOTE: Access from the Internet** It may be possible to reach the server from the Internet when the device is connected to the Internet via the activated net zone. **Default setting:** deactivated
	DNS server reachable from net zone 2	When this function is activated, access from the selected net zone to the DNS server of the device is permitted (UDP/TCP port 53). **NOTE: Access from the Internet** It may be possible to reach the server from the Internet when the device is connected to the Internet via the activated net zone. **Default setting:** activated
	Log DNS requests	When this function is activated, a log entry is created for all requests to the DNS server of the device (UDP/TCP). Log entries can be analyzed via the **Logging** menu (see Section 8) or in the *journal* file, which can be created and downloaded via a snapshot (see Section 9.3). Log entries can have different prefixes (see Section 8). **Default setting:** deactivated

Menu: Network >> DNS		
External DNS server (Only configurable if the device network configuration is **not assigned via DHCP**.)	**DNS server**	Users can select whether the preset “root DNS servers” or “user-defined DNS servers” are used in the device for the resolution of hostnames. **Note:** This choice is only available if the device **does not receive its network configuration from a DHCP server** (see Section 6.1.1). When using host names, there is always the risk of an attacker manipulating or blocking DNS requests (i.e. *DNS spoofing*). You should therefore only configure trustworthy and secure DNS servers on the mGuard device – if possible from your internal company network – ,so as to avoid these types of attacks. **Root DNS server** **Only** the preset root DNS servers in the device are used for the resolution of hostnames (see list in Section A 5, “Root DNS servers”). The first available root DNS server will be used. **User-defined** **Only** the user-defined DNS servers are used for the resolution of hostnames. Several DNS servers can be specified. If a DNS server is not specified, hostnames are not resolved. **Default setting:** Root DNS server
	User-defined DNS server (Only configurable if “user-defined” has been selected.)	IP address of one or more DNS servers that are queried by the device for resolving hostnames. **Input format:** IPv4 address
	Comment	Freely selectable comment. Permitted characters: max. 128

7 Menu: Network security

7.1 Firewall

Data packets that are *routed* through the device are analyzed by its firewall (packet filter) and then forwarded or blocked in accordance with the configured firewall rules.

The term *routed* data traffic is used to describe data connections that do not terminate at the device (such as requests to the device's NTP server) but instead are routed (*Router mode*) or forwarded (*Stealth mode*) by the device.

The connections can also be received and forwarded on the same network interface (net zone).

The firewall rules are configured in various tables depending on the direction of the initial data traffic (*net zone 1* → *net zone 2* and *net zone 2* → *net zone 1*).

Firewall logging
Log entries are only created for packets with *Ether type IPv4*. Packets with other *Ether types* (e.g., *ARP, IPv6*) are not recorded in the log files. (Exception: Entries that affect the rate limit – *fw-input-rate-limit*)

Stateful packet inspection

The firewall of the device operates on the principle of the *stateful packet inspection firewall*: This means that response packets for requests that were permitted by the firewall on the way into one direction automatically pass the firewall on their way back if they can be clearly related to the request.

For this, the information on each data connection is saved to a *connection tracking* table and compared with the response packets to be able to clearly relate them to the corresponding requests.

Firewall rules are never applied to response packets.

7.1.1 Settings

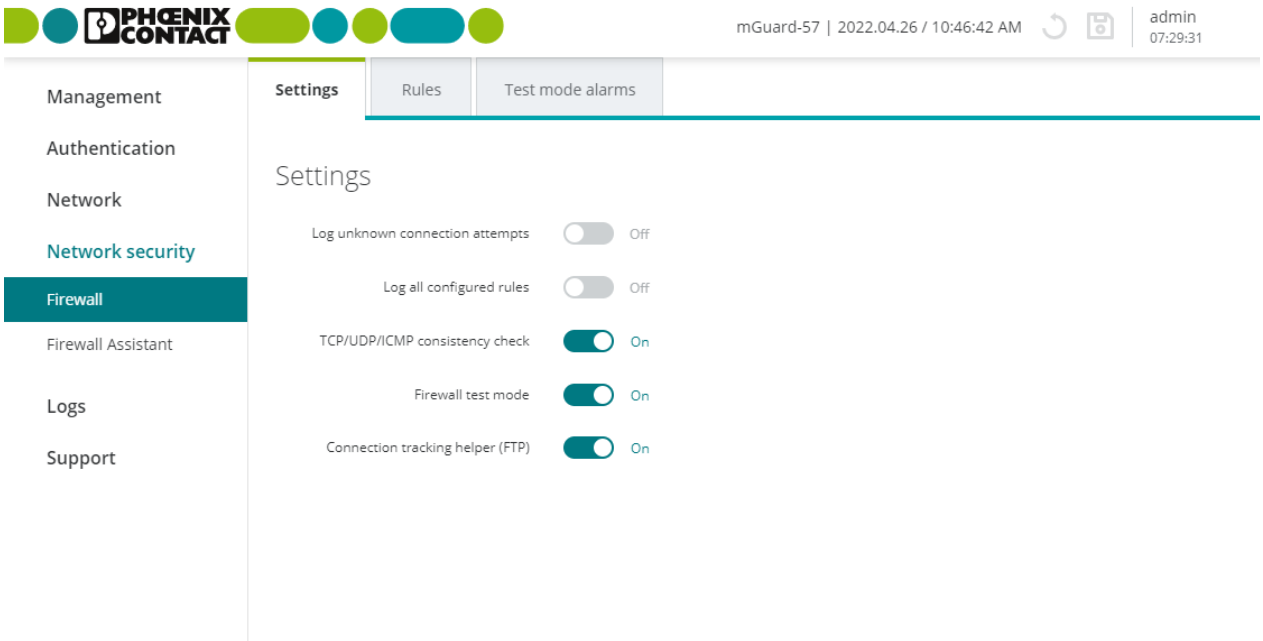


Figure 7-1 Network security >> Firewall >> Settings

Menu: Network security >> Firewall >> Settings		
Settings	**Log unknown connection attempts**	When this function is activated, a corresponding log entry is created for each data connection to which no configured firewall rules apply. Log entries can be analyzed via the **Logging** menu (see Section 8) or in the *journal* file, which can be created and downloaded via a snapshot (see Section 9.3). Log prefix: *fw-forward-policy-* **Default setting:** deactivated
	Log all configured rules	When this function is activated, a corresponding log entry is created for each data connection to which any firewall rule applies. This also applies to rules where logging is deactivated using the "*„Log“*" function. Log entries can be analyzed via the **Logging** menu (see Section 8) or in the *journal* file, which can be created and downloaded via a snapshot (see Section 9.3). Log prefix: *fw-forward-* **Default setting:** deactivated

Menu: Network security >> Firewall >> Settings		
	TCP/UDP/ICMP consistency check	The consistency check increases the protection of connected network clients against *Denial of Service* (DoS) attacks. When this function is activated, data packets that are routed through the device and forwarded to connected network clients are checked for malicious elements: **ICMP packets** Only known ICMP code is used. **UDP packets** Destination port in the UDP packet is not equal to zero. **TCP packets** Source and destination port in the TCP packet are not equal to zero. **IPv4 packets** Protocol is not set to zero. Data packets that do not meet the specified requirements are dropped by the firewall and not forwarded. **Default setting:** activated
	Allow forwarding of DHCP packets (Only configurable in "*Stealth*" mode)	**In Stealth mode, the following applies:** When the function is activated, clients in net zone 2 can obtain their IP configuration **automatically and independently of the settings in the firewall tables** from a DHCP server in net zone 1. Firewall rules configured in the firewall table that would block this DHCP data traffic are not considered. It is not necessary to manually configure firewall rules to allow DHCP data traffic. **Default setting:** activated

Menu: Network security >> Firewall >> Settings

Firewall test mode

Data traffic unintentionally rejected by the firewall can be easily identified and permitted through the automated creation of corresponding firewall rules.

NOTE: The firewall is partially deactivated
In *Firewall test mode*, data packets that are not captured by any of the already configured firewall rules will not be discarded, as is normally the case, but instead will be forwarded

Prerequisite
For the *Firewall test mode* to be able to generate entries, the existing firewall table must not contain an overriding rule that rejects all data traffic.

Method of operation

When this function is activated, the data traffic *routed* through the device is analyzed by the firewall.

If a previously configured firewall rule applies to a data packet, the rule is applied to the data packet **as normal** (*Accept*, *Reject*, or *Drop*).

If none of the configured rules apply to a data packet, the packet is **not discarded, as is usually the case**, but forwarded.

At the same time, the user is informed via an event:

1. The “PF2” LED on the device lights up red.
2. The “O1” switching output on the “XG2” COMBICON connector of the device switches to *high level*.
   (If a signal light is connected, it would light up in this case.)
3. An entry is generated in the *Test mode alarms* table which can be analyzed by the user.

If the data traffic that has triggered a *test mode alarm* is to be allowed in the future, the user can automatically create an appropriate firewall rule from the corresponding entry in the *Test mode alarms* table (see below and Section 7.1.3).

Creating firewall rules from test mode alarms

Entries in the *Test mode alarms* table can be selected and automatically added at the end of the existing firewall tables as a new firewall rule (see Section 7.1.3).

The newly added rules would then allow the respective data traffic in the future (*Action* = *Accept*).

Deactivating Firewall test mode

If the *firewall test mode* is deactivated, all entries in the *Test mode alarms* table will be deleted and signaling via the “PF2” LED and the “O1” switching output will stop.

Default setting: deactivated

Menu: Network security >> Firewall >> Settings

Connection tracking helper (FTP)

Activating this function helps to enable desired data connections via the FTP protocol that are blocked by the firewall.

If a connection is established via the FTP protocol, data can be transferred in two ways:

1. With "active FTP", the called FTP server establishes an additional counter-connection to the caller (FTP client) in order to transfer the data via this connection.
2. With "passive FTP", the caller (FTP client) establishes an additional connection to the server in order to transfer the data.

To ensure that the additional connection is not blocked by the firewall, the connection tracking helper for FTP must be activated in both cases.

The activated function is also applied to data packets that are forwarded using port forwarding.

NOTE: No connection in stealth mode with "active FTP".

For connections in stealth mode with "active FTP", no connection is established even if the connection tracking helper is activated.

In this case, either use "passive FTP" or create an additional firewall rule that allows a data connection from the server to the client according to the requirements (e.g. Allow: *Net zone 1* → *Net zone 2* , Protocol: *TCP*, From IP: *192.168.1.100*, To IP: *192.168.1.200*).

Default setting: deactivated

7.1.2 Rules

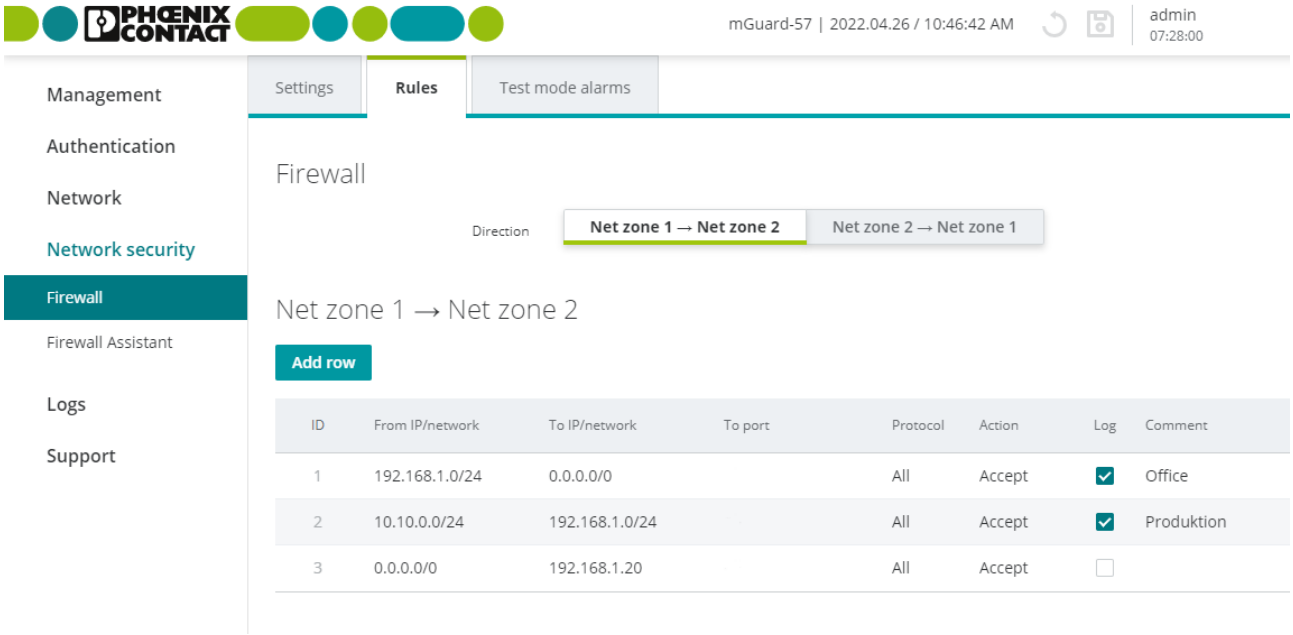


Figure 7-2 Network security >> Firewall >> Rules

Menu: Network security >> Firewall >> Rules	
Firewall	The firewall rules are configured in two different tables depending on the direction of the initial data traffic: – *Net zone 1 → Net zone 2* – *Net zone 2 → Net zone 1* **NOTE: Note the direction of the data traffic** The rules in a firewall table are only applied to the data traffic that is *routed* through the device in the specified direction from one net zone to the other. **Net zone 1 → Net zone 2** Displays the firewall table whose rules are applied to the data traffic routed in the specified direction (**Net zone 1 → Net zone 2**). **Net zone 2 → Net zone 1** Displays the firewall table whose rules are applied to the data traffic routed in the specified direction (**Net zone 2 → Net zone 1**).

Menu: Network security >> Firewall >> Rules

Net zone X → Net zone Y

Behavior and effects of firewall rules
How does the configuration of firewall rules affect the *routed* data traffic?

1. **No rule configured:** All data packets are dropped**.**
2. **None of the configured rules apply:** All data packets are dropped**.**
3. **One rule is configured and applies:**
   The rule is applied and the configured action performed.
4. **Several rules are configured and apply:**
   The rules are queried one after the other starting from the top until a rule is found that applies. This rule is applied and the configured action performed.
   In this case, none of the succeeding rules are considered even if they would apply.
   It is not necessary to create a final rule that overrides all other rules.

In *Firewall test mode*, no *test mode alarms* can be generated if a final rule exists that overrides all other rules.

If a firewall is reconfigured, all existing entries in the status table (*connection tracking table*) are deleted.

If identical entries exist several times in the table, a hint is is displayed in the table header. Identical entries can be deleted by clicking on the **Delete duplicates** button, whereby the first entry is kept in each case.

Structure of firewall rules

A firewall rule is made up of different parameters. The entire rule applies only if all configured parameters of a rule apply to a packet.

Some parameters of a rule can be configured in such a way that they always apply (e.g., *All* or *0.0.0.0/0*).

ID
Identification number of the rule (generated by the system)

The ID determines the order in which the rules are queried, starting with the lowest ID.

From IP/network
Source (network or IP address) from which the data packets have to be sent so that the rule applies here.

Note: If “0” is specified as the subnet mask, the rule applies to all sources (all IP addresses and networks) here.

Input format: IPv4 address, IPv4 network (CIDR notation)

Default setting:
- Net zone 1 → Net zone 2: no rule
- Net zone 2 → Net zone 1: 0.0.0.0/0

Menu: Network security >> Firewall >> Rules

To IP/network	Destination (network or IP address) to which the data packets have to be sent so that the rule applies here. **Note:** If “0” is specified as the subnet mask, the rule applies to all destinations (all IP addresses and networks) here. **Input format:** IPv4 address, IPv4 network (CIDR notation) **Default setting:** – Net zone 1 → Net zone 2: no rule – Net zone 2 → Net zone 1: 0.0.0.0/0
To port (Only configurable if *TCP* or *UDP* is selected as "Protocol")	Destination port or port range where the data packets have to be sent so that the rule applies here. **Input format:** 1 – 65535, start_port:end_port, all **Note:** All = all ports; start_port:end_port = port range **Default setting:** – Net zone 1 → Net zone 2: no rule – Net zone 2 → Net zone 1: all
Protocol	**TCP, UDP, ICMP, GRE, ESP, All** Network protocol that has to be used to transmit the data packets so that the rule applies here. **Note:** All = all protocols **Default setting:** – Net zone 1 → Net zone 2: no rule – Net zone 2 → Net zone 1: all
Action	**Accept, Reject, Drop** The action that will be performed if all parameters configured in the access rule apply to a packet. **Accept:** The data packets may pass through. **Reject:** The data packets are rejected. The sender is informed. **Drop:** The data packets are dropped. The sender is not informed. **Note (Stealth mode):** In *Stealth mode*, selection of the *Reject* action leads to the same behavior as that of the action *Drop*. Because the device does not have its own IP address in *Stealth mode*, data packets are dropped in both cases and the sender is not informed. In these cases, the log entries will be listed as the action “*Drop*” and not “*Reject*”. **Default setting:** – Net zone 1 → Net zone 2: no rule – Net zone 2 → Net zone 1: Accept

Menu: Network security >> Firewall >> Rules		
	Log	When this function is activated, a corresponding log entry is created for each data connection this rule applies to. For rules in which the function is deactivated, a log entry is not created unless the "„Log all configured rules“" function is activated. Log entries can be analyzed via the **Logging** menu (see Section 8) or in the *journal* file, which can be created and downloaded via a snapshot (see Section 9.3). Log prefix: *fw-forward-* **Default setting:** deactivated
	Comment	Freely selectable comment. Permitted characters: max. 128

7.1.3 Test mode alarms

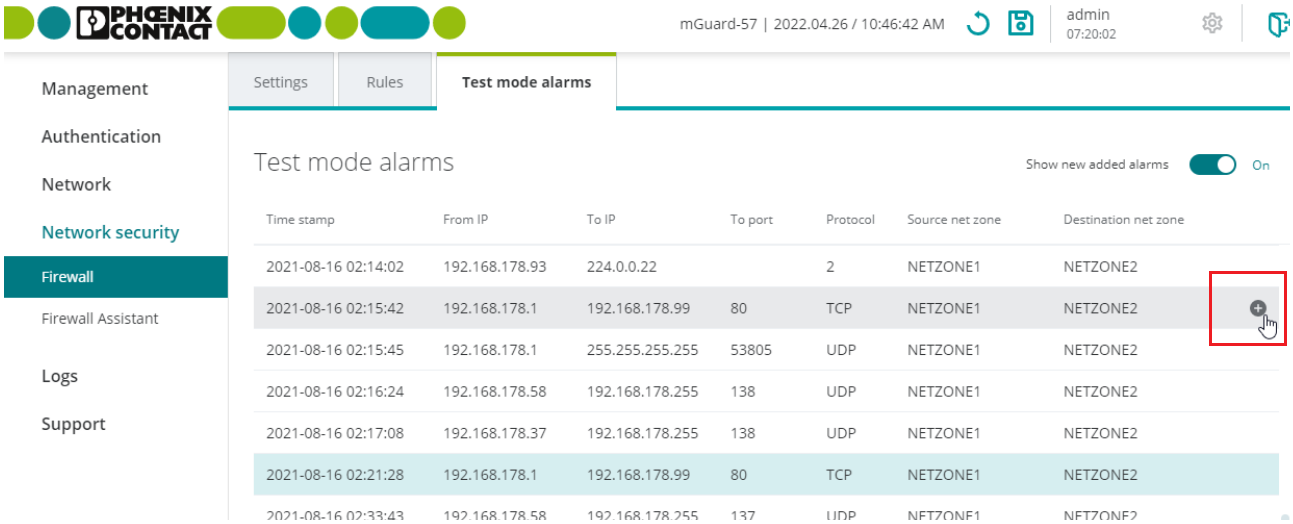


Figure 7-3 Network security >> Firewall >> Test mode alarms

Menu: Network security >> Firewall >> Test mode alarms

Test mode alarms

(The “Test mode alarms” tab is only visible if the “Firewall test mode” is activated.)

In *Firewall test mode*, the data traffic *routed* through the device is analyzed and a table is automatically created with entries for the data packets that are not acquired by the already configured firewall rules.

The entries recorded in this table can then be selected and added to the end of the relevant firewall tables of the device as firewall rules. (Menu: **Network security >> Firewall >> Rules**; see Section 7.1.2).

Added rules allow the corresponding data traffic (**Action = Accept**).

NOTE: Automatically created firewall rules will be activated.
Immediately check the newly created firewall rules and adapt them according to your security requirements.

NOTE: Limit for 2000 test mode alarms reached!
If the limit is reached, new entries will not be added to the table. It can then be assumed that the alarms recorded in the table are incomplete.
That is why you must proceed as follows to generate additional test mode alarms:

- Add the required entries to your firewall rules (see below).
- Then end the Firewall test mode.
- Reboot the firewall test mode in order to generate new alarms.

Menu: Network security >> Firewall >> Test mode alarms

Adding test mode alarms to the firewall rules:

- Check the table entries.
- Identify the firewall rules that you would like to add as new firewall rules, taking your security requirements into consideration.
- Click an entry to mark any existing identical entries in the list that were created at different points in time.
- Move the mouse pointer over the entry that you would like to apply as a new firewall rule to the relevant firewall table.

⇒ The ⊕ icon will appear at the end of the row.

- Click ⊕ to copy the rule to the corresponding firewall tables.

⇒ The firewall rule is added at the end of the corresponding firewall table.

- Change to the **Network security >> Firewall >> Rules** menu.
- Check the rules and modify them, if necessary.
- Click the 💾 icon to apply the changes.

⇒ The newly added firewall rules are activated and immediately allow the corresponding data traffic.

Show new added alarms	If activated, the display always focuses on the last alarms added to the table. The device continuously checks whether new test mode alarms are generated and adds them to the end of the existing table. To view older alarms that have already been added, the function should be deactivated. **Default setting:** activated
Time stamp	Time at which the entry was generated by the relevant data traffic. **Note:** The time is displayed in accordance with the set time zone. **Format:** YYYY-MM-DD hh:mm:ss
From IP	Source (IP address) from which the data packet was sent.
To IP	Destination (IP address) to which the data packet was sent.
To port	Destination port to which the data packet was sent. – No entry means that a destination port was not specified in the data packet (e.g., ICMP data packets).
Protocol	Network protocol that was used for transmitting the data packet. The **TCP**, **UDP**, **ICMP**, **GRE,** and **ESP** protocols are accepted. For all other protocols, the value **All** is entered.
Source net zone	Net zone in which the data connection was initiated. The direction of the data connection determines the firewall table in which the data may be entered (see Section 7.1.2).

Menu: Network security >> Firewall >> Test mode alarms		
	Destination net zone	Net zone to which the data was sent. The direction of the data connection determines the firewall table in which the data may be entered (see Section 7.1.2)

7.2 Firewall test mode

See “Firewall test mode” on page 80.

7.3 Firewall Assistant

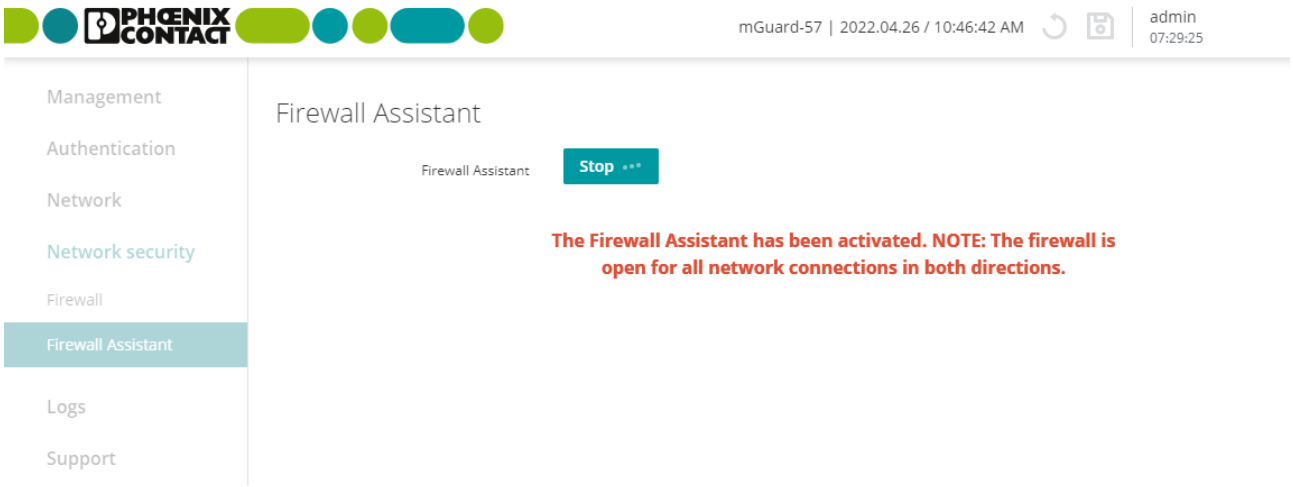


Figure 7-4 Network security >> Firewall Assistant

If activated, the *Firewall Assistant* analyzes and captures the data traffic *routed* through the device (**Net zone 1 ←→ Net zone 2**).

In the process, the firewall is open in both directions.

The captured packet data is used to derive firewall rules that are automatically entered into the corresponding firewall table of the device upon exiting the *Firewall Assistant*.

The data traffic defined in these firewall rules will be allowed in the future (**Action = Accept**). All other connections will be dropped.

The firewall tables created using the *Firewall Assistant* can be adapted and extended as required.

Table 7-1 Firewall Assistant: Conversion of packet data into firewall rules

Header entry	**Entry in firewall rule**	**Example**
Source IP address	**From IP/network**	*10.1.1.55*
Destination IP address	**To IP/network**	*192.168.1.100*
The respective netmask of the source and destination network is not captured. Only the individual IP addresses are captured and applied in the firewall rule.		
Destination port	**To port**	*443*
If a destination port is not transmitted (e.g., as with the *ICMP* protocol), no value is entered in the firewall rule.		
Protocol	**Protocol**	*TCP*
The following protocols can be applied as values in the firewall rule: – *TCP, UDP, ICMP, GRE, ESP* For all other protocols, the value *"All"* is entered in the firewall rule.		
—	**Action**	*Accept*
In all firewall rules created via the *Firewall Assistant* or *Firewall test mode*, "*Accept*" is always entered as the action value.		

Procedure

Start the Firewall Assistant

NOTE: The firewall is deactivated
When the *Firewall Assistant* is activated, connected network clients are no longer protected by the firewall.

The *Firewall Assistant* can only be started if **all firewall rules** in all firewall tables were previously deleted under **Network security >> Firewall >> Rules** (see Section 7.1.2).

Firewall rules are only applied when the Firewall Assistant is stopped via the **Stop** button.

NOTE: Limit for packet data reached
The Firewall Assistant is automatically stopped when the maximum possible amount of packet data has been analyzed. **In this case, no rules are entered in the firewall tables!** Restart the Firewall Assistant with a shorter runtime.

Proceed as follows:

- Click the **Start** button to activate the *Firewall Assistant*.

⇒ Data traffic is analyzed and captured.

⇒ The firewall is open in both directions.

Stop the Firewall Assistant and create firewall rules

NOTE: The automatically created firewall rules are active without prior checking.
Immediately check the newly created firewall rules and adapt them according to your security requirements.

Proceed as follows:

- Click the **Stop** button to deactivate the *Firewall Assistant*.

⇒ The captured packet data is used to automatically create firewall rules, which are entered in the corresponding firewall tables (menu: **Network security >> Firewall >> Rules**, see Section 7.1.2).

⇒ The entered rules immediately and permanently allow the corresponding data traffic (**Action = Accept**) (see Table 7-1).

The firewall tables created using the *Firewall Assistant* can be adapted and extended as required.

8 Menu: Logging

Logging refers to the recording of messages relating to events that occurred (e.g., configuration changes, application of firewall rules, error messages).

Log entries are temporarily saved to the device and can also be transferred to a remote server using the *syslog* protocol.

Sensitive data and security-relevant information (e.g., passwords or secret cryptographic/hashed keys) are not included in the log files.

8.1 Log entries

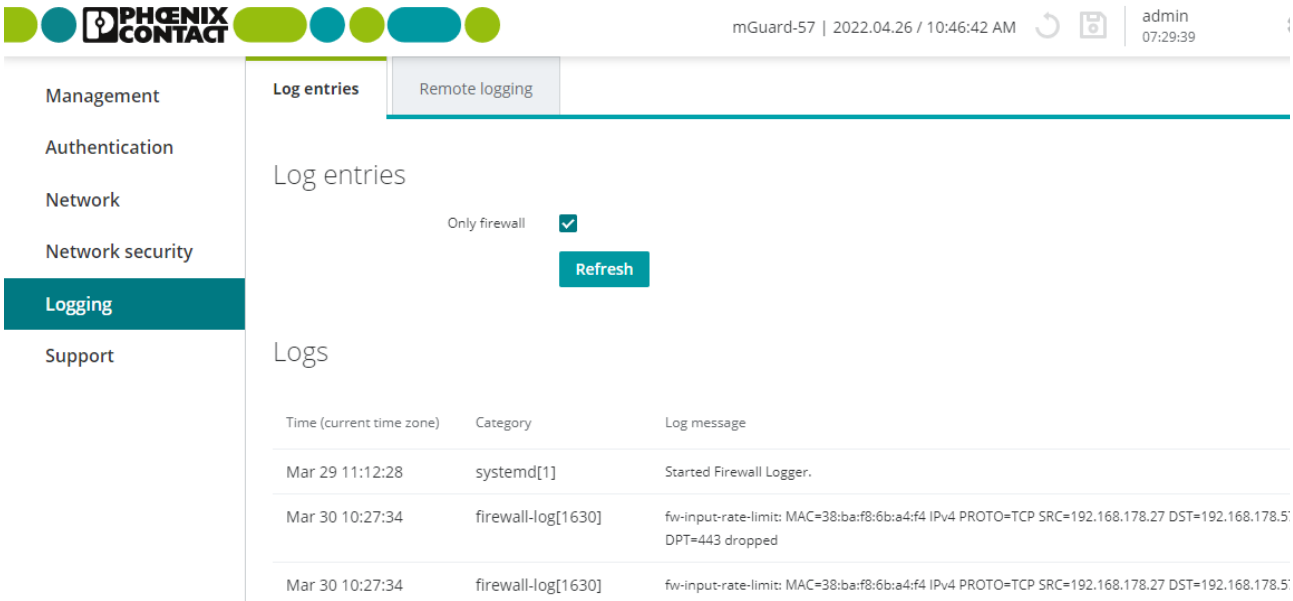


Figure 8-1 Logging >> Log entries

Menu: Logging >> Log entries	
Log entries	Log entries are recorded in the RAM of the device. If the memory space has been used up, the oldest log entries are automatically overwritten by new entries. If the device is switched off, all log entries will be deleted. To save log entries for the longer term, they can be transferred to a remote server in accordance with the syslog protocol (see Section 8.2, “Remote logging”). In rare cases, generating a large number of log entries may result in a log entry not being transmitted. To be able to check this, each log entry, as described in the syslog protocol, is assigned a consecutive sequence ID (e.g., meta sequenceId="728").

Menu: Logging >> Log entries

Users may first have to activate log entries for specific events if necessary.

Firewall logging
Log entries are only created for packets with *Ether type IPv4*. Packets with other *Ether types* (e.g., *ARP, IPv6*) are not recorded in the log files. (Exception: Entries that affect the rate limit – *fw-input-rate-limit*)

For data connections (e.g., UDP, TPC, or ICMP), always only the first packet of the connection will be logged (if logging is activated) because the connection is subject to *Connection Tracking*.

Log prefixes

Log entries are categorized differently and marked accordingly with specific prefixes.

Log prefixes (firewall logging)

forward = Relates to the firewall (Routing/Stealth) for routing traffic:
- **fw-forward** = A firewall rule was applied to a packet.
- **fw-forward-policy =** A packet **for which no rules have been defined** was dropped.
- **fw-forward-testmode** = Relates to entries (*„Test mode alarms“*) generated via the *„Firewall test mode“* function (is only displayed if all log entries are displayed; see below „Only firewall“).

input = Relates to the *incoming firewall* for accessing the device:
- **fw-input** = An *incoming firewall* rule was applied to a packet.
- **fw-input-policy** = A packet **for which no rules have been defined** was dropped.
- **fw-input-dnscache** = Relates to accessing the DNS server of the device.
- **fw-input-rate-limit** = Due to excessive access to the device during a defined period of time (e.g., via HTTPS), the data rate was throttled.

Explanation of abbreviations

- IPv4 PROTO = Network protocol
- SRC = Source IP address
- DST = Destination IP address
- SPT = Source port (TCP and UDP)
- DPT = Destination Port (TCP and UDP)
- MAC = Source MAC address

Only firewall

When this function is activated, only the log entries relating to the firewall (*firewall - Routing/Stealth* and *incoming firewall*) will be displayed.

When the function is deactivated, all log entries will be displayed.

Default setting: activated

Button

Refresh
- Click the **Refresh** button to update the log entry display.

Menu: Logging >> Log entries		
Logs	**Time (current time zone)**	Time when the log entry was created. In the WBM, the time is displayed according to the currently saved time zone. **Format:** Month Day Hour:Minute:Second **Note:** A timestamp within a log message is not adapted to the current time zone.
	Category	Category (component/unit) to which the log entry is assigned.
	Log message	The message associated with the log entry. **Note:** A timestamp within a log message is not adjusted to the current time zone.

8.2 Remote logging

Security advice
For reasons of security, an encrypted TLS connection should always be used between the device (mGuard) and the *syslog* server.

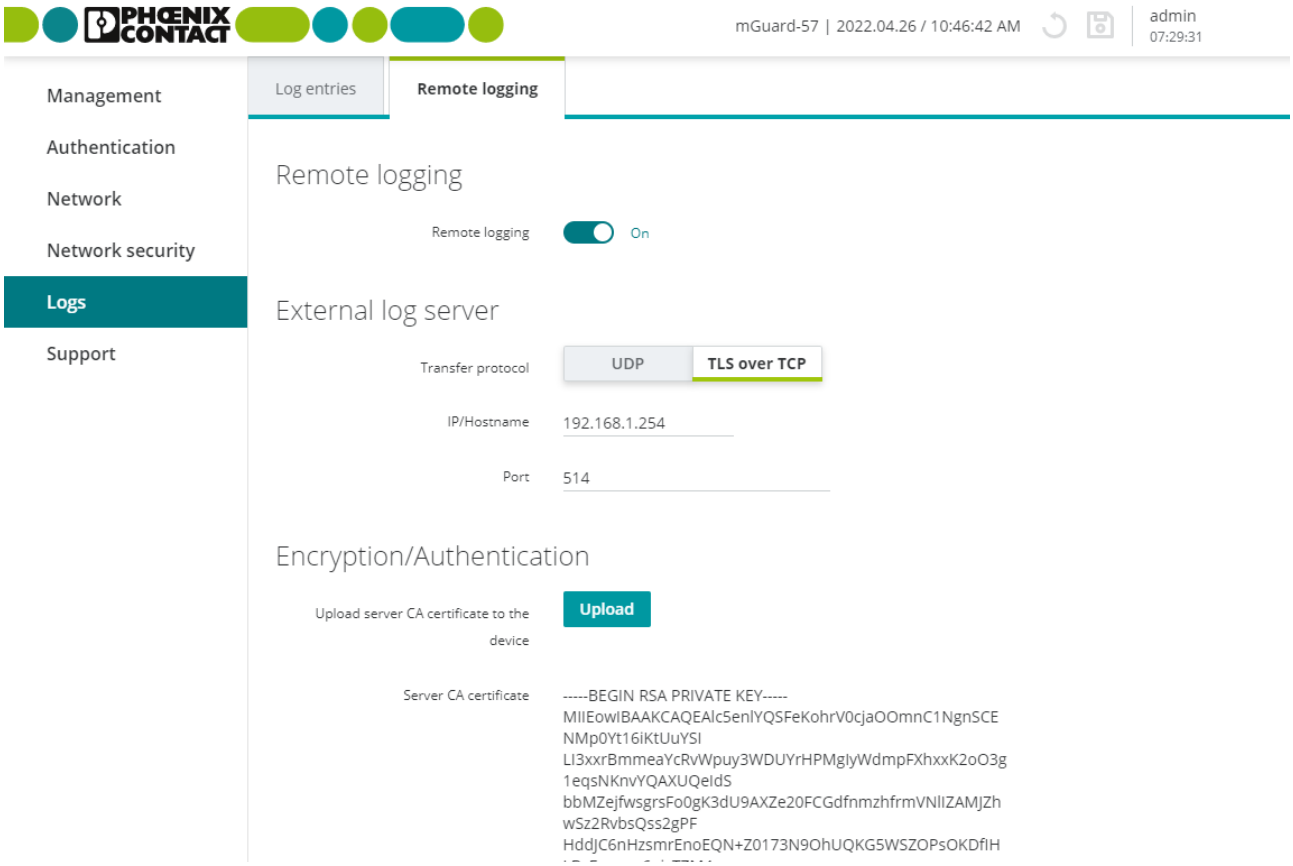


Figure 8-2 Logging >> Remote logging (syslog)

Menu: Logging >> Remote logging		
Remote logging	**Remote logging**	When this function is activated, all the device's log entries will be transmitted to a remote server using the *syslog* protocol (see RFC 5424) (see below). You can choose whether the information is transmitted using the unencrypted UDP protocol or encrypted using the TCP protocol. **Default setting:** deactivated

Menu: Logging >> Remote logging		
External log server	**Transfer protocol**	Network protocol that is used to establish a connection to the remote server (*syslog* server). **Note:** For reasons of security, an encrypted TLS connection should always be used between the device (mGuard) and the *syslog* server. **UDP** When this function is activated, the data is transmitted unencrypted using the UPD protocol. Mutual authentication between the device and the remote server does not take place. **TLS over TCP** When this function is activated, the data is transmitted with encryption using a TCP connection. (See also "Encryption algorithms used" on page 15.) Mutual authentication between the device and the remote server takes place via X.509 certificates (see below). **Prerequisite:** Conditions needed to ensure the integrity and the authenticity of the encrypted TCP connection: 1. A server certificate (CA certificate) for the remote server must be installed on the device (see Below) 2. A client certificate must be generated on the device, downloaded, and installed on the remote server (see Below) **Default setting:** UDP
	IP/Hostname	IP address or hostname of the remote server (*syslog* server) to which the log entries are to be sent. **Input format**: IPv4 address or hostname **Default setting:** 192.168.1.254
	Port	Network port on which the remote server accepts data packets (standard port: *514/UDP*). **Input format:** 1 – 65535 **Default setting:** 514
Encryption/authentication (Only configurable if TLS is activated over TCP.)	**Use of certificates** Called "authentication," the documentation and verification of authenticity is a fundamental element of secure communication. The X.509 authentication method relies on certificates to ensure that the "correct" partners communicate with each other and that no "incorrect" partner is involved in communication (see also Section B 3, "Explanation of terms" under „X.509 certificate").	

Menu: Logging >> Remote logging		
	Certificate	A certificate is used as proof of the identity of the certificate owner. The relevant authorizing body in this case is the CA (*certificate authority*). The digital signature on the certificate is provided by the CA. By providing this signature, the CA confirms that the authorized certificate owner possesses a private key that corresponds to the public key in the certificate. The name of the certificate issuer appears under Issuer on the certificate, while the name of the certificate owner appears under Subject.
	Upload server CA certificate to the device	The CA certificate with which the device authenticates the remote server (*syslog* server) is uploaded to the device. The CA certificate is provided by the remote server operator and must be uploaded to the device (X.509 certificate with public key). An encrypted TCP connection to the remote server can only be established successfully if it in turn has a certificate issued by the CA certificate (with the *secret* key) or a valid certificate chain with the CA certificate as the highest instance. **Button** • Click the **Upload** button to upload the CA certificate of the remote server (*syslog* server) from a configuration computer to the device. **Format:** The maximum file size allowed is 1 MB. **Note:** A CA certificate that has already been uploaded will be deleted and replaced in this case.
	Server CA certificate	Displays the currently uploaded CA certificate.
Client certificate	**Create new client certificate on the device**	The self-signed client certificate with which the device authenticates itself to the remote server (*Syslog*-Server) is created on the device and saved there. The operator must download and upload it to the remote server (X.509 certificate with *public* key). **NOTE: The current certificate will be deleted** When you create a new client certificate, the certificate currently saved on the device will be deleted permanently. The newly created certificate must be uploaded to the remote server again. **Button** • Click the **Create** button to create a new client certificate on the device. **Note:** A previously created certificate will be deleted and replaced in this case.

Menu: Logging >> Remote logging		
	Download client certificate	The created client certificate (see Below) will be downloaded to the configuration computer. **Button** • Click the **Download** button to download the client certificate (with the *public* key). The certificate's *secret key* will always remain on the device. The downloaded client certificate can now be uploaded to the remote server. File name: *Client_certificate.crt*
	Client certificate	Displays the client certificate currently used by the device.

9 Menu: Support

9.1 Ping

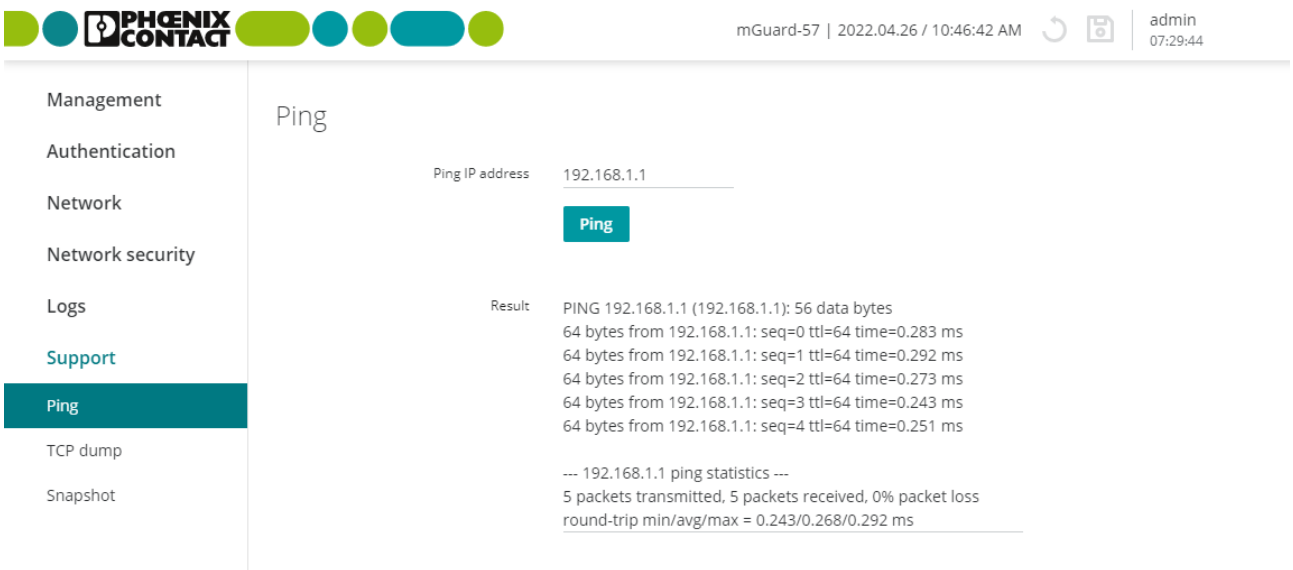


Figure 9-1 Support >> Ping

Menu: Support >> Ping	
Ping	A ping request (*ICMP request*) can be used to check whether a network client is connected to an interface of the device via its IP address and can be reached via the ICMP protocol.
	IP address — A ping request (*ICMP request*) is sent to the specified IP address of a network client. If the client can be reached via the *ICMP* protocol and any net zone of the device, it sends a response to the device. **Procedure** • Open the **Support >> Ping** menu. • Enter the IP address of the client to be checked in the field. • Click on the **Ping** button. ⇒ If the client can be reached via *ICMP*, the response from the client is displayed after a few seconds: e.g., *5 packets transmitted, 5 packets received*. ⇒ If the client cannot be reached via *ICMP*, a corresponding message is displayed: e.g., *100% packet loss*). **Input format:** IPv4 address

9.2 TCP dump

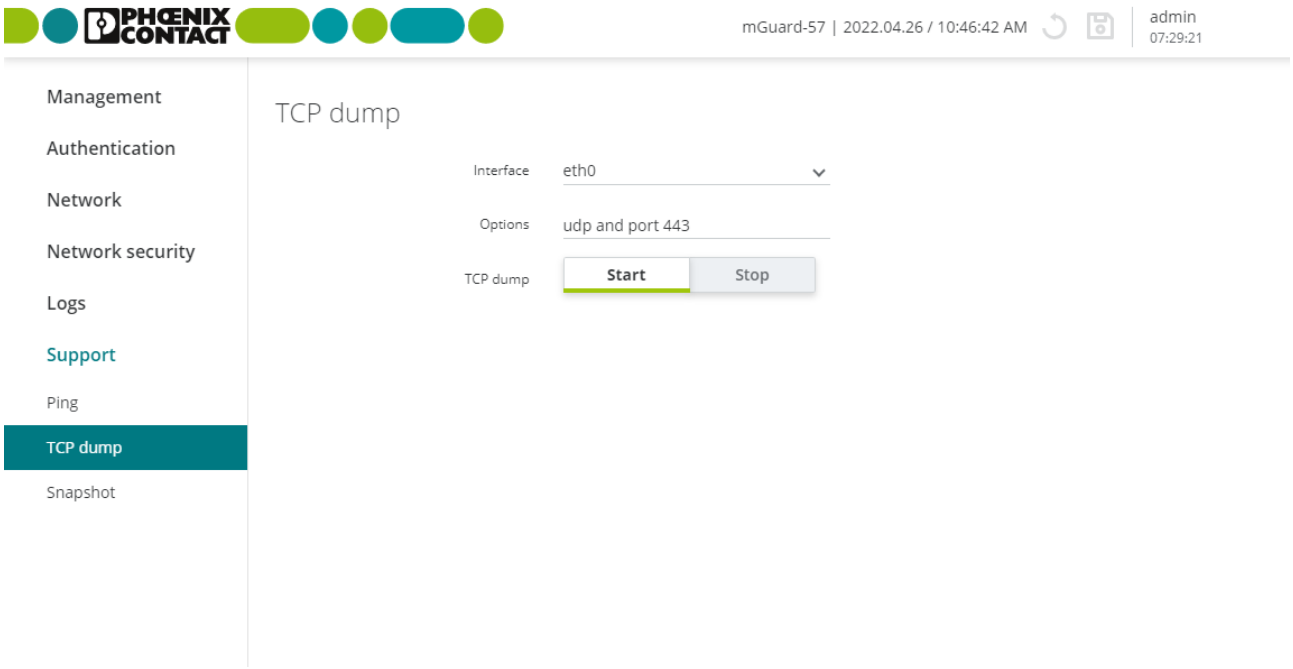


Figure 9-2 Support >> TCP dump

Menu: Support >> TCP dump	
TCP dump	By means of a packet analysis (*tcpdump*), the content of network packets that are sent or received via a specified network interface can be analyzed. Filter options are used to define which network packets are to be analyzed. The result of the analysis is saved to a file (*.*pcap*), downloaded and deleted from the device. If the device is restarted while an analysis is running, the data acquired until then is deleted. If the file (*.*pcap*) exceeds a size of 50 MB, the analysis is aborted with an error. The data acquired until then is deleted. **Procedure** • Open the **Support >> TCP dump** menu. • Select the **interface** whose network packets are to be analyzed. • Enter the required **Options** to limit the analysis. • To start the analysis, click on the **Start** button. • To stop and download the analysis, click on the **Stop** button. ⇒ The result of the analysis was saved to a file (*.*pcap*), downloaded and deleted from the device.

Menu: Support >> TCP dump		
	Interface	Only data packets that are sent or received via the selected network interface are analyzed. Net zone 1: – **eth0** Net zone 2: – **lan0** – **lan1** – **lan2** – **lan3**
	Options	Options can be used to limit the packet analysis to a selection of the elements below. Options can be linked via the logical operators "*and*, *or*, *not*". *Example: "tcp and net 192.168.1.0/24 and not port 443"*
	Available options:	
	tcp	TCP protocol
	udp	UDP protocol
	arp	ARP protocol
	icmp	ICMP protocol
	esp	ESP protocol
	host <ip>	IPv4 address
	port <1-65535>	Network port (single port number)
	net <nw_cidr>	Network (in CIDR format, e.g., 192.168.1.0/24)
	and, or, not	Logic operators
	TCP dump	**Start (button)** Click the **Start** button to start an analysis. **Stop (button)** Click the **Stop** button to stop a running analysis. ⇒ The acquired packet contents are summarized in a file (**.pcap*) and automatically downloaded from the device. Afterwards, the file is deleted from the device. The time of the file download is indicated in the file name as follows: <YYYY-MM-DD_hh:mm:ss> (Example: *tcpdump_2019-10-09_22_00_00.pcap*)

9.3 Snapshot

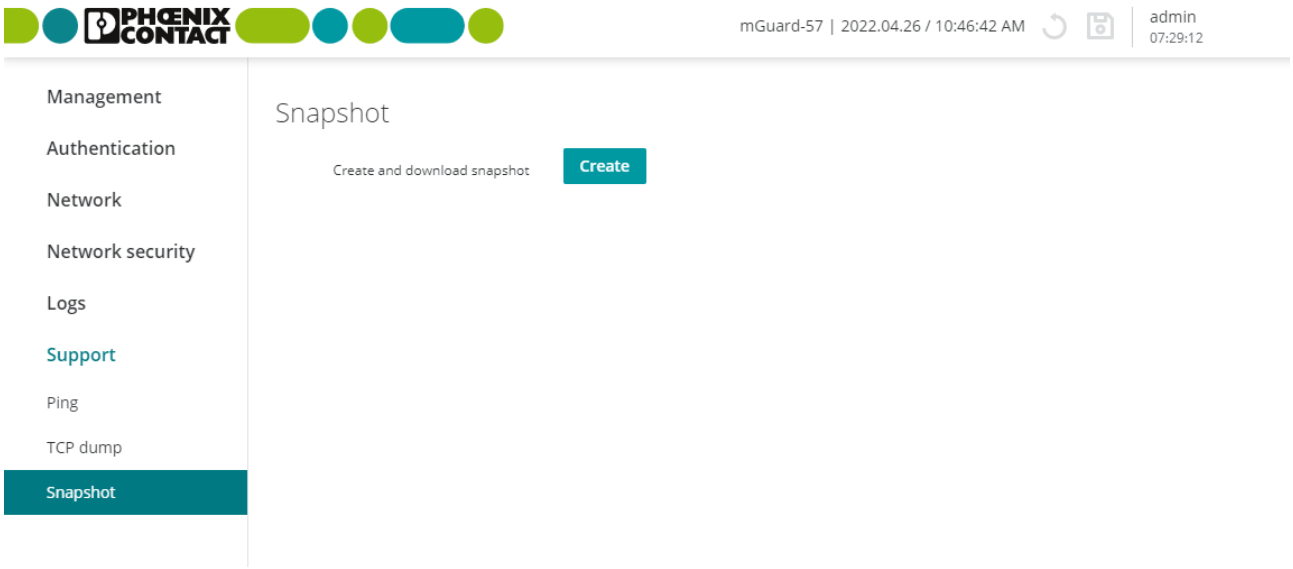


Figure 9-3 Support >> Snapshot

Menu: Support >> Snapshot	
Snapshot	A snapshot can be used for error diagnostics and during communication with the support team. The snapshot is created and downloaded as a compressed file (in tar.gz format). The snapshot contains the current configuration, user management information, and other device system information (see "Content of a snapshot" on page 103). Sensitive data and security-relevant information (e.g., passwords or secret cryptographic/hashed keys) are not included in the snapshot.
Create and download snapshot	**Create (Button)** Click the **Create** button to create the snapshot. The created snapshot (**.tar.gz)* will be downloaded automatically from the device. The time the snapshot was created is specified in the file name as follows: <YYYY-MM-DD_hh:mm:ss> Example: *snapshot_2021-10-09_22_00_00.tar.gz*

Content of a snapshot

Table 9-1 Content of a snapshot

File name	Content/description
File format: *json*	
config.json	Shows the current device configuration.
serdata.json	Shows the serialization data that was linked to the device during creation.
ldap.json	Shows the current configuration for LDAP authentication via LDAP server.
users.json	Shows current informations about the local users on the device.
File format: *txt*	
bootloader_version	Shows the version of the currently installed bootloader.
conntrack	Shows the current content of the status table (*connection tracking table*).
df	Shows the current amount of disk space available on the file system
eds	Shows the current dynamic status information of certain device functions.
ethtool_eth0	Shows information about the Ethernet port *eth0* (XF1 / net zone 1).
ethtool_eth1	Shows information about the Ethernet port *eth0* (XF2–5 / net zone 2).
ipset_list	Shows information about the currently used IP set.
ip_neight	Shows the current connection information for connected (*neighbored*) devices.
ip_route	Shows the current routing table.
ip_link	Shows the current connection status of the network interfaces.
ip_addr	Shows the current network configuration.
issue	Information on the firmware image.
journal	Shows the current log file of the system.
ls_mnt_hfs	Shows the files and directories currently in the device file system (/mnt/hfs).
mount	Shows the mounted file systems
nft_ruleset	Shows the firewall rules currently configured.
nft_tables	Shows the firewall tables currently configured.
proc_net_dev	Shows current information about the network traffic of all network interfaces (file */proc/net/dev)*.
proc_net_snmp	Shows information about the network traffic via the SNMP protocol (file */proc/net/snmp*).
pstree	Shows information about currently running processes.
services	Shows the services currently started on the system (*systemd*).
tpm2_fixed	Shows fiexed information about the TPM chip that cannot be changed.
tpm2_variable	Shows variable information of the TPM chip that can be changed.
uptime	Shows the current operating time and the load average of the system.
userid	Shows the user ID and the group membership.
version	Shows the firmware version currently installed.

A Appendix

A 1 Using the RESTful Configuration API

The device can be configured via the web-based management, but also via the *RESTful Configuration API* (or *Config API* for short).

Only experienced users should use the *Config API*.

As a machine-to-machine interface, the *RESTful Configuration API* allows automated and dynamic control and configuration of the device.

See the "*FL MGUARD 1000 – RESTful Configuration API"* user manual, available at phoenixcontact.net/product/1153079).

A 2 Using Smart mode

Using *Smart mode* is described in the "*FL MGUARD 1000 – Installation and startup*" user manual (UM EN FL MGUARD 1000).
It is available in the download area of the respective product page in the Phoenix Contact webshop, for example at phoenixcontact.net/product/1153079.

Using *Smart mode*, device functions can be called up without access to one of the device's management interfaces (WBM or *Config API*).

The following functions are available:

– Restoring the configuration access
– Restoring the factory settings (irrevocable deletion of all files)
– Updating from an SD card

A 3 Legal notice (Software License Terms)

The *Software License Terms* (SLT) currently valid for the product can be created and downloaded via the **Legal notice** link at the lower edge of the screen.

A 4 Third-party licenses

The **Legal Notices** link at the bottom of the screen can be used to view the third-party software components (modules) used on the device and the associated license information.

A 5 Root DNS servers

- nameserver 1.1.1.1
- nameserver 1.0.0.1
- nameserver 193.17.47.1
- nameserver 185.43.135.1
- nameserver 185.95.218.42
- nameserver 185.95.218.43
- nameserver 192.99.183.132
- nameserver 149.56.228.45
- nameserver 216.146.35.35
- nameserver 216.146.36.36
- nameserver 84.200.69.80
- nameserver 84.200.70.40
- nameserver 80.80.80.80
- nameserver 80.80.81.81
- nameserver 8.8.8.8
- nameserver 8.8.4.4
- nameserver 156.154.70.1
- nameserver 156.154.70.5
- nameserver 156.154.71.5
- nameserver 9.9.9.10
- nameserver 91.239.100.100
- nameserver 89.233.43.71
- nameserver 64.6.64.6
- nameserver 64.6.65.6
- nameserver 77.88.8.1
- nameserver 77.88.8.8

A 6 Update options

Table 9-2 lists the mGuardNT firmware versions from which an update to the target version can be performed.

Table 9-2 Update options

Initial version	Target version	Comment
1.3.x	1.8.x	Before the update, it must be ensured in the configuration of the initial version that the networks of net zones 1 and 2 do not overlap (see Section 6.1.1).
1.4.x		
1.5.x		
1.6.x		
1.7.x		
1.8.y (with y < x)		

B Appendixes

B 1 List of figures

Section 1

Section 2

Section 3

Section 4

Section 5

Section 6

Section 7

Section 8

Section 9

Appendix A

Appendix B

B 2 List of tables

Section 1

Section 2

Section 3

Section 4

Section 5

Section 6

Section 7

Section 8

Section 9

Appendix A

Appendix B

B 3 Explanation of terms

Asymmetrical encryption

In asymmetrical encryption, data is encrypted with one key and decrypted with a second key. Both keys are suitable for encryption and decryption. One of the keys is kept secret by its owner (private key), while the other is made available to the public (public key), i.e., to potential communication partners.

A message encrypted with the public key can only be decrypted and read by a recipient in possession of the associated private key. A message encrypted with the private key can be decrypted by any recipient in possession of the associated public key. Encryption using the private key shows that the message actually originated from the owner of the associated public key. Therefore, the expression “digital signature” is also often used.

However, asymmetrical encryption methods such as RSA are both slow and susceptible to certain types of attack. As a result, they are often combined with some form of symmetrical encryption (→ “Symmetrical encryption” on page 118). On the other hand, concepts are available enabling the complex additional administration of symmetrical keys to be avoided.

CA certificate

How trustworthy is a certificate and the issuing CA (certification authority)? (→ “X.509 certificate” on page 117) A CA certificate can be consulted in order to check a certificate bearing this CA's signature. This check only makes sense if there is little doubt that the CA certificate originates from an authentic source (i.e., is authentic). In the event of doubt, the CA certificate itself can be checked. If (as is usually the case) the certificate is a sub-CA certificate (i.e., a CA certificate issued by a sub-certification authority), then the CA certificate of the superordinate CA can be used to check the CA certificate of the subordinate instance. If a superordinate CA certificate is in turn subordinate to another superordinate CA, then its CA certificate can be used to check the CA certificate of the subordinate instance, etc. This “chain of trust” continues down to the root instance (the root CA or certification authority). The root CA's CA file is necessarily self-signed, since this instance is the highest available and is ultimately the basis of trust. No-one else can certify that this instance is actually the instance in question. A root CA therefore is a state or a state-controlled organization.

The mGuard can use its imported CA certificates to check the authenticity of certificates shown by peers. In the case of VPN connections, for example, peers can only be authenticated using CA certificates. This requires all CA certificates to be installed on the mGuard in order to form a chain with the certificate shown by the peer. In addition to the CA certificate from the CA whose signature appears on the certificate shown by the VPN partner to be checked, this also includes the CA certificate of the superordinate CA, and so forth, up to the root certificate. The more meticulously this “chain of trust” is checked in order to authenticate a peer, the higher the level of security will be.

Client/server

In a client/server environment, a server is a program or computer which accepts and responds to queries from client programs or client computers.

In data communication, the computer establishing a connection to a server (or host) is also called a client. In other words, the client is the calling computer and the server (or host) is the computer called.

Datagram

In IP transmission protocols, data is sent in the form of data packets. These are known as IP datagrams. An IP datagram is structured as follows

IP header	TCP, UDP, ESP, etc. header	Data (payload)

The IP header contains:

– The IP address of the sender (source IP address)
– The IP address of the recipient (destination IP address)

– The protocol number of the protocol on the superordinate protocol layer (according to the OSI layer model)
– The IP header checksum used to check the integrity of the received header

The TCP/UDP header contains the following information:

– The port of the sender (source port)
– The port of the recipient (destination port)
– A checksum covering the TCP header and some information from the IP header (including source and destination IP address)

Default route

If a computer is connected to a network, the operating system creates a routing table internally. The table lists the IP addresses that the operating system has identified based on the connected computers and the routes available at that time. Accordingly, the routing table contains the possible routes (destinations) for sending IP packets. If IP packets are to be sent, the computer's operating system compares the IP addresses stated in the IP packets with the entries in the routing table in order to determine the correct route.

If a router is connected to the computer and its internal IP address (i.e., the IP address of the router's LAN port) has been relayed to the operating system as the default gateway (in the network card's TCP/IP configuration), then this IP address is used as the destination if all other IP addresses in the routing table are not suitable. In this case, the IP address of the router specifies the default route because all IP packets whose IP address has no counterpart in the routing table (i.e., cannot find a route) are directed to this gateway.

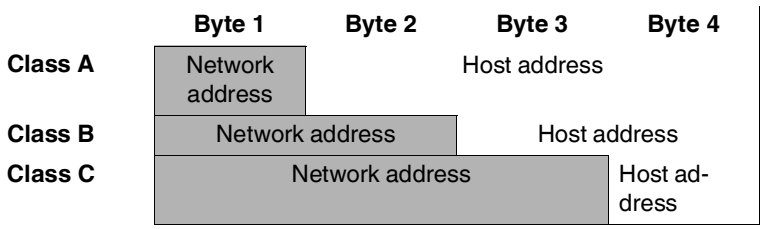
IP address

Every host or router on the Internet/Intranet has its own unique IP address (IP = Internet Protocol). An IP address is 32 bits (4 bytes) long and is written as four numbers (each between 0 and 255), which are separated by a dot.

An IP address consists of two parts: the network address and the host address.

Network address	Host address

All network hosts have the same network address, but different host addresses. The two parts of the address differ in length depending on the size of the respective network (networks are categorized as Class A, B or C).



The first byte of the IP address determines whether the IP address of a network device belongs to Class A, B or C. The following is specified:

	Value of byte 1	Bytes for the network address	Bytes for the host address
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Based on the above figures, the number of Class A networks worldwide is limited to 126. Each of these networks can have a maximum of 256 x 256 x 256 hosts (3 bytes of address area). There can be 64 x 256 Class B networks and each of these networks can have up to 65,536 hosts (2 bytes of address area: 256 x 256). There can be 32 x 256 x 256 Class C networks and each of these networks can have up to 256 hosts (1 byte of address area).

Subnet mask

Normally, a company network with access to the Internet is only officially assigned a single IP address, e.g., 128.111.10.21. The first byte of this example address indicates that this company network is a Class B network; in other words, the last two bytes are free to be used for host addressing. Accordingly, an address area for up to 65,536 possible hosts (256 x 256) can be computed.

Such a huge network is not practical and generates a need for subnetworks to be built. The subnet mask is used here. Like an IP address, the mask is 4 bytes long. The bytes representing the network address are each assigned the value 255. The primary purpose of doing this is to enable a portion of the host address area to be “borrowed” and used for addressing subnetworks. For example, if the subnet mask 255.255.255.0 is used on a Class B network (2 bytes for the network address, 2 bytes for the host address), the third byte, which was actually intended for host addressing, can now be used for subnetwork addressing. This computes to potential support for 256 subnetworks, each with 256 hosts.

Subject, certificate

In a certificate, confirmation is provided by a certification authority (CA) that the certificate does actually belong to its owner. This is done by confirming specific owner properties. Furthermore, the certificate owner must possess the private key that matches the public key in the certificate. (→ “X.509 certificate” on page 117).

Example

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 1 (0x1)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
      Validity
         Not Before: Oct 29 17:39:10 2000 GMT
→     Subject: CN=anywhere.com,E=doctrans.de,C=DE,ST=Hamburg,L=Hamburg,O=Phoenix Contact,OU=Security
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
               d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
               9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
               90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
               1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
               7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
               50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
               8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
               f0:b4:95:f5:f9:34:9f:f8:43
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Subject Alternative Name:
            email:xyz@anywhere.com
         Netscape Comment:
            mod_ssl generated test server certificate
         Netscape Cert Type:
            SSL Server
   Signature Algorithm: md5WithRSAEncryption
      12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
      3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
      82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
      cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
      4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
      d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
      44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
      ff:8e
```

The *subject distinguished name* (or *subject* for short) uniquely identifies the certificate owner. The entry consists of several components. These are called attributes (see the example certificate above). The following table contains a list of possible attributes. The sequence of attributes in an X.509 certificate can vary.

Table 9-3 X.509 certificate

Abbreviation	Name	Explanation
CN	Common name	Identifies the person or object to whom or which the certificate belongs. Example: CN=server1
E	E-mail address	Specifies the e-mail address of the certificate owner.
OU	Organizational unit	Specifies the department within an organization or company. Example: OU=Development
O	Organization	Indicates the organization or company. Example: O=Phoenix Contact
L	Locality	Indicates the location Example: L=Hamburg
ST	State	Specifies the state or county. Example: ST=Bavaria
C	Country	Two-letter code that specifies the country. (Germany=DE) Example: C=DE

A filter can be set for the subject (i.e., the certificate owner) during VPN connections and remote service access to the mGuard using SSH or HTTPS. This would ensure that only certificates from peers that have certain attributes in the subject line are accepted.

NAT (IP masquerading)

Network Address Translation (NAT) (also known as *IP masquerading*) “hides” an entire network behind a single device, known as a NAT router. If you communicate externally via a NAT router, the internal computers in the local network and their IP addresses remain hidden. The remote communication partner will only see the NAT router with its IP address.

In order to allow internal computers to communicate directly with external computers (on the Internet), the NAT router must modify the IP datagrams that are sent from internal computers to remote partners and received by internal computers from remote partners.

If an IP datagram is sent from the internal network to a remote partner, the NAT router modifies the UDP and TCP headers of the datagram, replacing the source IP address and source port with its own official IP address and a previously unused port. For this purpose, the NAT router uses a table in which the original values are listed together with the corresponding new ones.

When a response datagram is received, the NAT router uses the specified destination port to recognize that the datagram is intended for an internal computer. Using the table, the NAT router replaces the destination IP address and port before forwarding the datagram via the internal network.

Port number

A port number is assigned to each device in UDP and TCP protocol-based communication. This number makes it possible to differentiate between multiple UDP or TCP connections between two computers and use them simultaneously.

Certain port numbers are reserved for specific purposes. For example, HTTP connections are usually assigned to TCP port 80 and POP3 connections to TCP port 110.

Proxy

A proxy is an intermediary service. A web proxy (e.g., Squid) is often connected upstream of a large network. For example, if 100 employees access a certain website frequently over a web proxy, then the proxy only loads the relevant web pages from the server once and then distributes them as needed among the employees. Remote web traffic is reduced, which saves money.

Router

A router is a device that is connected to different IP networks and communicates between them. To do this, the router has an interface for each network connected to it. A router must find the correct path to the destination for incoming data and define the appropriate interface for forwarding it. To do this, it takes data from a local routing table listing assignments between available networks and router connections (or intermediate stations).

X.509 certificate

A type of “seal” that certifies the authenticity of a public key (“Asymmetrical encryption” on page 113) and the associated data.

It is possible to use certification to enable the user of the public key (used to encrypt the data) to ensure that the received public key is indeed from its actual issuer (and thus from the instance that should later receive the data). A *certification authority* (CA) certifies the authenticity of the public key and the associated link between the identity of the issuer and its key. The certification authority verifies authenticity in accordance with its rules (for example, it may require the issuer of the public key to appear before it in person). After successful authentication, the CA adds its (digital) signature to the public key. This results in a certificate.

An X.509(v3) certificate thus consists of a public key, information about the key owner (the Distinguished Name (DN)), authorized use, etc., and the signature of the CA (“CA certificate” on page 113).

The signature is created as follows: the CA creates an individual bitstring from the bitstring of the public key, owner information, and other data. This bitstring can be up to 160 bits in length and is known as the HASH value. The CA then encrypts this with its own private key and then adds it to the certificate. The encryption with the CA's private key proves the authenticity of the certificate (i.e., the encrypted HASH string is the CA's digital signature). If the certificate data is tampered with, then this HASH value will no longer be correct and the certificate will be rendered worthless.

The HASH value is also known as the fingerprint. Since it is encrypted with the CA's private key, anyone who has the corresponding public key can decrypt the bitstring and thus verify the authenticity of the fingerprint or signature.

The involvement of a certification authority means that it is not necessary for key owners to know each other. They only need to know the certification authority involved in the process. The additional key information also simplifies administration of the key.

X.509 certificates are used for e-mail encryption with S/MIME or IPsec, for example.

Protocol, transmission protocol

Devices that communicate with each other must follow the same rules. They have to “speak the same language”. Rules and standards of this kind are called protocols or transmission protocols. Some of the more frequently used protocols are IP, TCP, PPP, HTTP, and SMTP.

Spoofing, anti-spoofing

In Internet terminology, spoofing means supplying a false address. Using this false Internet address, a user can create the illusion of being an authorized user.

Anti-spoofing is the term for mechanisms that detect or prevent spoofing.

Symmetrical encryption

In symmetrical encryption, the same key is used to encrypt and decrypt data. Two examples of symmetrical encryption algorithms are DES and AES. They are fast, but also increasingly difficult to administrate as the number of users increases.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Network protocols used to connect two computers on the Internet.

IP is the base protocol.

UDP is based on IP and sends individual packets. The packets may reach the recipient in a different order than that in which they were sent or they may even be lost.

TCP is used for connection security and ensures, for example, that data packets are forwarded to the application in the correct order.

UDP and TCP add port numbers between 1 and 65535 to the IP addresses. These distinguish the various services offered by the protocols.

A number of additional protocols are based on UDP and TCP. These include HTTP (Hyper Text Transfer Protocol), HTTPS (Secure Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3), and DNS (Domain Name Service).

ICMP is based on IP and contains control messages.

SMTP is an e-mail protocol based on TCP.

IKE is an IPsec protocol based on UDP.

ESP is an IPsec protocol based on IP.

On a Windows PC, the WINSOCK.DLL (or WSOCK32.DLL) handles the processing of both protocols.

(→ “Datagram” on page 113)

VPN (Virtual Private Network)

A **V**irtual **P**rivate **N**etwork (VPN) connects several separate private networks (subnetworks) via a public network (e.g., the Internet) to form a single common network. A cryptographic protocol is used to ensure confidentiality and authenticity. A VPN is therefore an inexpensive alternative to using permanent lines for building a nationwide company network.

B 4 Index

T

U

V

W

Please observe the following notes

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com **phoenixcontact.com**

108420_en_12
Order No. —12

INSPIRING INNOVATIONS