

# mGuard Application Notes

## FL/TC MGUARD

Application Note  
AH EN MGUARD APPNOTES

## Application Note

### mGuard Application Notes – FL/TC MGUARD

AH EN MGUARD APPNOTES, Revision 12

2026-03-17

This application note is valid for mGuard security appliances of the series FL/TC MGUARD.

Device	Order number
FL MGUARD RS4000 TX/TX (VPN)	2700634 / (2200515)
FL MGUARD GT/GT(VPN)	2700197 / (2700198)
FL MGUARD SMART2 (VPN)	2700640 / (2700639)
FL MGUARD RS2000 TX/TX VPN	2700642
FL MGUARD RS2000 TX/TX-B	2702139
FL MGUARD DELTA TX/TX (VPN)	2700967 / (2700968)
FL MGUARD PCI4000 VPN	2701275
FL MGUARD PCIE4000 VPN	2701278
FL MGUARD RS4000 TX/TX VPN/MAN	2701866
FL MGUARD RS2005 TX VPN	2701875
FL MGUARD RS4004 TX/DTX (VPN)	2701876 / (2701877)
FL MGUARD RS4000 TX/TX-P	2702259
FL MGUARD RS4000 TX/TX VPN-M	2702465
FL MGUARD CENTERPORT	2702547
FL MGUARD CORE TX VPN	2702831
TC MGUARD RS4000 3G VPN	2903440
TC MGUARD RS2000 3G VPN	2903441
TC MGUARD RS4000 4G VPN	2903586
TC MGUARD RS2000 4G VPN	2903588
TC MGUARD RS4000 4G VZW VPN	1010461
TC MGUARD RS2000 4G VZW VPN	1010462
TC MGUARD RS4000 4G ATT VPN	1010463
TC MGUARD RS2000 4G ATT VPN	1010464
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

## Table of contents

1	For your safety .....	7
2	Update and flash FL/TC MGUARD devices .....	9
3	Device replacement and migration .....	89
4	mGuard 8.9/9.0 - Extended maintenance 2030 .....	113
5	Request and distribute mGuard licenses via MDM .....	117
6	Logging / Firewall-Logging .....	129
7	Create X.509 certificates with OpenSSL .....	165
8	Create X.509 certificates with XCA .....	181
9	Establish an IPsec VPN connection between iOS client and mGuard device .....	201
10	Establish an IPsec VPN connection between Android client and mGuard device .....	215
11	Update the mGuard configuration using pull configuration .....	227
12	Using the CGI Interface .....	231
13	LED status indicator and blinking behavior .....	259
1	For your safety .....	7
	1.1 Labeling of warning notes.....	7
	1.2 Qualification of users .....	7
2	Update and flash FL/TC MGUARD devices .....	9
	2.1 Introduction.....	10
	2.2 Update to mGuard firmware version 9.0.0 .....	11
	2.3 Update to mGuard firmware version 8.6.1 .....	14
	2.4 Update to mGuard firmware version 10.6.1 .....	16
	2.5 Update to mGuard firmware version 10.5.0 .....	16
	2.6 Migration of the configuration from mGuard firmware version 8.x to 10.x .....	17
	2.7 General information about mGuard updates.....	18
	2.8 FL MGUARD RS2000/4000 TX/TX (incl. -B, -P, -M).....	24
	2.9 FL MGUARD RS2005/4004 TX bzw. TX/DTX .....	28
	2.10 TC MGUARD RS2000/4000 3G VPN .....	32
	2.11 TC MGUARD RS2000/4000 4G VPN .....	36
	2.12 TC MGUARD RS2000/4000 4G VZW VPN .....	41
	2.13 TC MGUARD RS2000/4000 4G ATT VPN .....	45
	2.14 FL MGUARD PCI(E)4000.....	49
	2.15 FL MGUARD SMART2.....	53
	2.16 FL MGUARD CENTERPORT .....	57
	2.17 FL MGUARD GT/GT .....	62
	2.18 FL MGUARD DELTA TX/TX.....	67

2.19	FL MGuard 2102/2105, 4305/4305, 4102 PCI(E) .....	71
2.20	mGuard Flash Guide .....	75
2.21	Setting up mGuard firmware update repositories.....	87
<b>3</b>	<b>Device replacement and migration .....</b>	<b>89</b>
3.1	Migration from mGuard 8/9 to mGuard 10.x .....	89
3.2	General procedure .....	90
3.3	Saving and importing the device configuration .....	91
3.4	Cases that require manual adjustment .....	95
3.5	Resetting variables to the default settings .....	96
3.6	Device differences.....	97
<b>4</b>	<b>mGuard 8.9/9.0 - Extended maintenance 2030 .....</b>	<b>113</b>
4.1	Extended maintenance until the end of 2030.....	113
4.2	Maintenance and Support .....	114
4.3	Firmware maintenance license.....	114
<b>5</b>	<b>Request and distribute mGuard licenses via MDM .....</b>	<b>117</b>
5.1	Introduction.....	117
5.2	Prerequisites.....	117
5.3	Procedure.....	118
5.4	Troubleshooting.....	124
<b>6</b>	<b>Logging / Firewall-Logging .....</b>	<b>129</b>
6.1	Introduction.....	130
6.2	Classification into log categories .....	130
6.3	Log entry (General) .....	132
6.4	Log prefix (Firewall).....	147
<b>7</b>	<b>Create X.509 certificates with OpenSSL .....</b>	<b>165</b>
7.1	Introduction.....	165
7.2	Preparing the CA environment.....	167
7.3	Modifying the OpenSSL configuration file.....	168
7.4	Create the CA Certificate and Key.....	172
7.5	Create a Certificate Request for the mGuard.....	174
7.6	Sign the mGuard's Certificate Request with the CA.....	176
7.7	Creating the mGuard's PKCS#12 file (Machine Certificate).....	178
7.8	Example: VPN connection between two mGuard devices.....	179

---

<b>8</b>	<b>Create X.509 certificates with XCA .....</b>	<b>181</b>
8.1	Introduction.....	181
8.2	Create an XCA database.....	183
8.3	Create a certificate template.....	184
8.4	Create a CA Certificate.....	187
8.5	Create a Client Certificate.....	191
8.6	Export a certificate.....	195
8.7	Sign a Certificate Request with the CA.....	196
8.8	Using a Certificate Revocation List (CRL) .....	198
8.9	Example: VPN connection between two mGuard devices.....	199
<b>9</b>	<b>Establish an IPsec VPN connection between iOS client and mGuard device .....</b>	<b>201</b>
9.1	Introduction.....	201
9.2	Manage certificates .....	202
9.3	Configure VPN connections .....	208
9.4	Start VPN connections on the iOS client.....	212
9.5	Check VPN connections on the mGuard .....	213
<b>10</b>	<b>Establish an IPsec VPN connection between Android client and mGuard device .....</b>	<b>215</b>
10.1	Introduction.....	215
10.2	Manage certificates .....	216
10.3	Configure VPN connections .....	219
10.4	Start VPN connections on the Android client .....	224
10.5	Check VPN connections on the mGuard .....	225
<b>11</b>	<b>Update the mGuard configuration using pull configuration .....</b>	<b>227</b>
11.1	Introduction.....	227
11.2	Configure pull configuration on the mGuard device .....	227
11.3	Pull configuration using mdm.....	228
11.4	Obtain pull configuration feedback from server logs.....	228
<b>12</b>	<b>Using the CGI Interface .....</b>	<b>231</b>
12.1	Introduction.....	231
12.2	Usage .....	232
12.3	Preconditions and restrictions .....	235
12.4	Interface nph-vpn.cgi.....	236
12.5	Interface nph-diag.cgi.....	251
12.6	Interface nph.action.cgi .....	253

12.7	Interface <code>nph.status.cgi</code> .....	255
13	LED status indicator and blinking behavior .....	259
13.1	Description of LEDs.....	259
13.2	LED lighting and blinking behavior.....	261
13.3	Representation of system states .....	261

# 1 For your safety

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

## 1.1 Labeling of warning notes



This symbol together with the **NOTE** signal word alerts the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.



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

## 1.2 Qualification of users

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

- Qualified electricians 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.



## 2 Update and flash FL/TC MGUARD devices



Document-ID: 108250\_en\_17  
 Document-Description: AH EN MGUARD UPDATE  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
 It can be downloaded using the following link [phoenixcontact.com/products](https://phoenixcontact.com/products).

### Contents of this document

The following chapters describe:

1. which mGuard firmware versions can be updated to mGuard 9.0.0,
2. which mGuard firmware versions can be updated to mGuard 10.6.0,
3. which files you need to update your mGuard device,
4. how a firmware update is carried out,
5. how the flash procedure is carried out.

2.1	Introduction .....	10
2.2	Update to mGuard firmware version 9.0.0 .....	11
2.3	Update to mGuard firmware version 8.6.1 .....	14
2.4	Update to mGuard firmware version 10.6.0 .....	16
2.5	Update to mGuard firmware version 10.5.0 .....	16
2.6	Migration of the configuration from mGuard firmware version 8.x to 10.x .....	17
2.7	General information about mGuard updates .....	18
2.8	FL MGUARD RS2000/4000 TX/TX (incl. -B, -P, -M) .....	24
2.9	FL MGUARD RS2005/4004 TX bzw. TX/DTX .....	28
2.10	TC MGUARD RS2000/4000 3G VPN .....	32
2.11	TC MGUARD RS2000/4000 4G VPN .....	36
2.12	TC MGUARD RS2000/4000 4G VZW VPN .....	41
2.13	TC MGUARD RS2000/4000 4G ATT VPN .....	45
2.14	FL MGUARD PCI(E)4000 .....	49
2.15	FL MGUARD SMART2 .....	53
2.16	FL MGUARD CENTERPORT .....	57
2.17	FL MGUARD GT/GT .....	62
2.18	FL MGUARD DELTA TX/TX .....	67
2.19	FL MGUARD 2102/2105, 4305/4305, 4102 PCI(E) .....	71
2.20	mGuard Flash Guide .....	75
2.21	Setting up mGuard firmware update repositories .....	87

## 2.1 Introduction

The firmware on mGuard devices can be updated in different ways:

1. [Local Update](#)
2. [Online Update](#) (not available for FL MGUARD 2000/4000 - mGuard 10.x)
3. [Automatic Update](#)
4. [Flashing the firmware](#)

In the case of a **firmware update**, the existing configuration of the mGuard device usually remains unchanged.

**Flashing** an mGuard device deletes the existing configuration, including all passwords, and resets the device to the default status (default settings).

### Firmware version 9

Firmware version 9.0.0 is a maintenance release for the discontinued mGuard devices (platform 2) with firmware version 8.x installed. Firmware version 9.0 will be maintained and supported with security updates until the end of 2030.

Firmware version 9.0.x can only be installed if one of the following licenses has been installed on the device (see also application note AH EN MGUARD LIC FW MNT 2030 - 112009\_en\_xx, available for download at [phoenixcontact.com/product/<artikel-nummer>](http://phoenixcontact.com/product/<artikel-nummer>)).

- 1493074 - FL MGUARD LIC FW MNT 2030  
Single license in the form of a license letter (voucher). The license can be installed individually on one device at a time via web-based management.
- 1775935 - FL MGUARD LIC-E FW MNT 2030  
Bulk license in electronic form (email). The license vouchers can be installed on the devices via the mGuard Device Manager (FL MGUARD DM UNLIMITED) or individually via web-based management.
- 2702552 - FL MGUARD LIC LFS CENTER  
"Firmware maintenance license" only for FL MGUARD CENTERPORT.
- 2700184 - FL MGUARD LIC LIFETIME FW  
Devices on which a "Lifetime Support" license has already been installed do not require an additional license.

Updating to **mGuard firmware version 9.0.0** is described in detail for all mGuard devices in Chapters 2.8 to 2.18. [Table 2-1](#) briefly lists the required update files.

### Firmware version 10

Updating to **mGuard firmware version 10.6.0** is described in detail for all mGuard devices in Chapter 2.19. [Table 2-3](#) briefly lists the required update files.

## 2.2 Update to mGuard firmware version 9.0.0



An update to **mGuard firmware version 9.0.0** is only possible from **mGuard firmware version 8.6.1** or later (maintenance license required).

If you want to update from a **firmware version < 8.6.1**, you must perform the update in several steps by first updating to version 8.6.1 (see [Section 2.3, “Update to mGuard firmware version 8.6.1”](#)). In the next step you can update this version to version 9.0.0.



An update to firmware version 9.0.0 is only possible if the function "**Encrypted State Synchronization**" (menu *Redundancy*) has been deactivated before.



The name of the update file to be used depends on the installed firmware version (source version) on the device and contains the following terms:

- Source version: 8.6.1 to 8.9.x --> Term: 8.{6-9}

The update to **mGuard firmware version 9.0.0** is described in detail in chapters [2.8](#) to [2.18](#), depending on the device (see [“Contents of this document”](#)). [Table 2-1](#) briefly lists the required update files depending on the source firmware version.

Table 2-1 Updating mGuard firmware version from **8.6.1** or later to **9.0.0**: Required files

Devices	Local Update	Firmware Flashing
FL MGuard RS2000 FL MGuard RS4000 (TX/TX) (incl. variants -B, -P, -M)	<b>Download file:</b> <i>Update_MPC_v9.0.0.zip</i> <b>Update files:</b> <i>update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_MPC_v9.0.0.zip</i> <b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i>
FL MGuard RS2005 FL MGuard RS4004 (TX respectively TX/DTX)	<b>Download file:</b> <i>Update_MPC_v9.0.0.zip</i> <b>Update files:</b> <i>update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_MPC_v9.0.0.zip</i> <b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i>
FL MGuard PCI(E)4000	<b>Download file:</b> <i>Update_MPC_v9.0.0.zip</i> <b>Update files:</b> <i>update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_MPC_v9.0.0.zip</i> <b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i>
FL MGuard SMART2	<b>Download file:</b> <i>Update_MPC_v9.0.0.zip</i> <b>Update files:</b> <i>update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_MPC_v9.0.0.zip</i> <b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i>
FL MGuard GT/GT	<b>Download file:</b> <i>Update_MPC_v9.0.0.zip</i> <b>Update files:</b> <i>update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_GTGT_v9.0.0.zip</i> <b>Update (flash) files:</b> <i>jffs2.img.mpc83xx.p7s</i> <i>install.mpc83xx.p7s</i>

## mGuard

Table 2-1 Updating mGuard firmware version from **8.6.1** or later to **9.0.0**: Required files

FL MGuard DELTA TX/TX	<p><b>Download file:</b> <i>Update_MPC_v9.0.0.zip</i></p> <p><b>Update files:</b> <i>update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b> <i>FW_MPC_v9.0.0.zip</i></p> <p><b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i></p>
FL MGuard CENTERPORT	<p><b>Download file:</b> <i>Update_X86_v9.0.0.zip</i></p> <p><b>Update files:</b> <i>update-8.{6-9}-9.0.0.default.x86_64.tar.gz</i></p>	<p><b>Download file:</b> <i>FW_X86_v9.0.0.zip</i></p> <p><b>Update (flash) files:</b> <i>firmware.img.x86_64.p7s</i> <i>install.x86_64.p7s</i></p>
TC MGuard RS2000 3G VPN TC MGuard RS4000 3G VPN	<p><b>Download file:</b> <i>Update_MPC_TC3G_v9.0.0.zip</i></p> <p><b>Update files:</b> <i>gemalto.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b> <i>FW_MPC_TC3G_v9.0.0.zip</i></p> <p><b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i> <i>pxs8_03001_0100617.usf.xz.p7s</i></p>
TC MGuard RS2000 4G VPN TC MGuard RS4000 4G VPN (Firmware update for devices with <b>Gemalto engine</b> - from Q3/2021)	<p><b>Download file:</b> <i>Update_MPC_TC4G_G_v9.0.0.zip</i></p> <p><b>Update files:</b> <i>PLS8-E.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b> <i>FW_MPC_TC4G_v9.0.0.zip</i></p> <p><b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i> <i>pls8-e_rev04.004_arn01.000.11.usf.xz.p7s</i></p>

Table 2-1 Updating mGuard firmware version from **8.6.1** or later to **9.0.0**: Required files

<p>TC MGuard RS2000 4G VPN TC MGuard RS4000 4G VPN (Firmware update for devices with <b>Huawei engine</b> - from Q3/2021)</p>	<p><b>Download file:</b> <i>Update_MPC_TC4G_H_v9.0.0.zip</i></p> <p><b>Update files:</b> <i>huaweigeneric.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b> <i>FW_MPC_TC4H_v9.0.0.zip</i></p> <p><b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i> <i>ME909u-521_UP-DATE_12.636.12.01.00.BIN.xz.p7s</i></p>
<p>TC MGuard RS2000/4000 4G VZW VPN</p>	<p><b>Download file:</b> <i>Update_MPC_TC4GVZW_v9.0.0.zip</i></p> <p><b>Update files:</b> <i>HL7518.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b> <i>FW_MPC_TC4GVZW_v9.0.0.zip</i></p> <p><b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i> <i>RHL75xx.4.04.142600.201801231340.x7160_1_signed_dwl.dwl.xz.p7s</i></p>
<p>TC MGuard RS2000/4000 4G ATT VPN</p>	<p><b>Download file:</b> <i>Update_MPC_TC4GATT_v9.0.0.zip</i></p> <p><b>Update files:</b> <i>HL7588.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b> <i>FW_MPC_TC4GATT_v9.0.0.zip</i></p> <p><b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i> <i>RHL75xx.A.2.15.151600.201809201422.x7160_3_signed_DWL.dwl.xz.p7s</i></p>

## 2.3 Update to mGuard firmware version 8.6.1



Possible from **mGuard firmware version 7.6.0**.



The name of the update file to be used depends on the installed firmware version (source version) on the device and contains the following terms:

Source version: 7.6.0 to 7.6.x --> Term: 7.{6}

Source version: 8.0.0 to 8.5.x --> Term: 8.{0-5}

Source version: 8.6.0 --> Term: 8.{6}

The update to **mGuard firmware version 8.6.1** is performed in the same way as described in chapters 2.8 to 2.18 (see “[Contents of this document](#)”). [Table 2-2](#) briefly lists the required update files depending on the source firmware version.

Table 2-2 Updating mGuard firmware version **7.6.0 or later** to **8.6.1**: Required files

Devices	Local Update	Firmware Flashing
FL MGuard RS2000 FL MGuard RS4000 (TX/TX) (incl. variants -B, -P, -M)	<b>Download file:</b> <i>Update_8.6.1_MPC.zip</i> <b>Update files:</b> <i>update-7.{6}-8.6.1.default.mpc83xx.tar.gz</i> <i>update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz</i> <i>update-8.{6}-8.6.1.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_MPC_8.6.1.zip</i> <b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i>
FL MGuard RS2005 FL MGuard RS4004 (TX respectively TX/DTX)	<b>Download file:</b> <i>Update_8.6.1_MPC.zip</i> <b>Update files:</b> <i>update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz</i> <i>update-8.{6}-8.6.1.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_MPC_8.6.1.zip</i> <b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i>
TC MGuard RS2000 3G VPN TC MGuard RS4000 3G VPN	<b>Download file:</b> <i>Update_8.6.1_TC3G_MPC.zip</i> <b>Update files:</b> <i>gemalto.update-8.{4-5}-8.6.1.default.mpc83xx.tar.gz</i> <i>gemalto.update-8.{6}-8.6.1.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_MPC_TC3G_8.6.1.zip</i> <b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i> <i>pxs8_03001_0100617.usf.xz.p7s</i>
TC MGuard RS2000 4G VPN TC MGuard RS4000 4G VPN	<b>Download file:</b> <i>Update_8.6.1_TC4G_MPC.zip</i> <b>Update files:</b> <i>huaweigeneric.update-8.{4-5}-8.6.1.default.mpc83xx.tar.gz</i> <i>huaweigeneric.update-8.{6}-8.6.1.default.mpc83xx.tar.gz</i>	<b>Download file:</b> <i>FW_MPC_TC4G_8.6.1.zip</i> <b>Update (flash) files:</b> <i>ubifs.img.mpc83xx</i> <i>install-ubi.mpc83xx.p7s</i> <i>ME909u-521_UP-DATE_12.636.12.01.00.BIN.xz.p7s</i>

Table 2-2 Updating mGuard firmware version **7.6.0 or later** to **8.6.1**: Required files

<p>FL MGuard PCI(E)4000</p>	<p><b>Download file:</b>  <i>Update_8.6.1_MPC.zip</i></p> <p><b>Update files:</b>  <i>update-7.{6}-8.6.1.default.mpc83xx.tar.gz</i>  <i>update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz</i>  <i>update-8.{6}-8.6.1.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b>  <i>FW_MPC_8.6.1.zip</i></p> <p><b>Update (flash) files:</b>  <i>ubifs.img.mpc83xx</i>  <i>install-ubi.mpc83xx.p7s</i></p>
<p>FL MGuard SMART2</p>	<p><b>Download file:</b>  <i>Update_8.6.1_MPC.zip</i></p> <p><b>Update files:</b>  <i>update-7.{6}-8.6.1.default.mpc83xx.tar.gz</i>  <i>update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz</i>  <i>update-8.{6}-8.6.1.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b>  <i>FW_MPC_8.6.1.zip</i></p> <p><b>Update (flash) files:</b>  <i>ubifs.img.mpc83xx</i>  <i>install-ubi.mpc83xx.p7s</i></p>
<p>FL MGuard CENTERPORT</p>	<p><b>Download file:</b>  <i>Update_8.6.1_x86.zip</i></p> <p><b>Update files:</b>  <i>update-7.{6}-8.6.1.default.x86_64.tar.gz</i>  <i>update-8.{0-5}-8.6.1.default.x86_64.tar.gz</i>  <i>update-8.{6}-8.6.1.default.x86_64.tar.gz</i></p>	<p><b>Download file:</b>  <i>FW_X86_8.6.1.zip</i></p> <p><b>Update (flash) files:</b>  <i>firmware.img.x86_64.p7s</i>  <i>install.x86_64.p7s</i></p>
<p>FL MGuard GT/GT</p>	<p><b>Download file:</b>  <i>Update_8.6.1_MPC.zip</i></p> <p><b>Update files:</b>  <i>update-7.{6}-8.6.1.default.mpc83xx.tar.gz</i>  <i>update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz</i>  <i>update-8.{6}-8.6.1.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b>  <i>FW_GTGT_8.6.1.zip</i></p> <p><b>Update (flash) files:</b>  <i>jffs2.img.mpc83xx.p7s</i>  <i>install.mpc83xx.p7s</i></p>
<p>FL MGuard DELTA TX/TX</p>	<p><b>Download file:</b>  <i>Update_8.6.1_MPC.zip</i></p> <p><b>Update files:</b>  <i>update-7.{6}-8.6.1.default.mpc83xx.tar.gz</i>  <i>update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz</i>  <i>update-8.{6}-8.6.1.default.mpc83xx.tar.gz</i></p>	<p><b>Download file:</b>  <i>FW_MPC_8.6.1.zip</i></p> <p><b>Update (flash) files:</b>  <i>ubifs.img.mpc83xx</i>  <i>install-ubi.mpc83xx.p7s</i></p>

## 2.4 Update to mGuard firmware version 10.6.0



An update to **mGuard 10.6.0** is possible from all mGuard firmware versions **starting with mGuard 10.5.0**.



The name of the update file to be used depends on the installed firmware version (source version) on the device and contains the following terms:  
 – Source version: 10.5.0 to 10.6.x --> Term: *10.{5-6}*

The update to **mGuard firmware version 10.6.0** is described in chapter 2.19 (see “[Contents of this document](#)”). [Table 2-3](#) briefly lists the required update files depending on the source firmware version.

Table 2-3 Updating mGuard firmware version **10.5.0 or later** to **10.6.0**: Required files

Devices	Local Update	Firmware Flashing
FL MGuard 4302 FL MGuard 4305 FL MGuard 2102 FL MGuard 2105 FL MGuard 4102 PCI FL MGuard 4102 PCIE	<b>Download file:</b> <i>Update_mGuard-10.6.0.zip</i> <b>Update files:</b> <i>update-10.{5-6}-10.6.0.default.aarch64.tar.gz</i>	<b>Download file:</b> <i>Firmware_mGuard-10.6.0.zip</i> <b>Update (flash) files:</b> <i>firmware.img.aarch64.p7s</i> <i>install.aarch64.p7s</i>

## 2.5 Update to mGuard firmware version 10.5.0



An update to **mGuard 10.5.0** is possible from all mGuard firmware versions **starting with mGuard 10.0.0**.



The name of the update file to be used depends on the installed firmware version (source version) on the device and contains the following terms:  
 Source version: 10.0.x to 10.4.x --> Term: *10.{0-4}*

The update to **mGuard firmware version 10.5.0** is performed in the same way as described in chapters 2.19 (see “[Contents of this document](#)”). [Table 2-3](#) briefly lists the required update files depending on the source firmware version.

Table 2-4 Updating mGuard firmware version **10.0.0 or later** to **10.5.0**: Required files

Devices	Local Update	Firmware Flashing
FL MGuard 4302 FL MGuard 4305 FL MGuard 2102 FL MGuard 2105 FL MGuard 4102 PCI FL MGuard 4102 PCIE	<b>Download file:</b> <i>Update_mGuard-10.5.0.zip</i> <b>Update files:</b> <i>update-10.{0-4}-10.5.0.default.aarch64.tar.gz</i>	<b>Download file:</b> <i>Firmware_mGuard-10.5.0.zip</i> <b>Update (flash) files:</b> <i>firmware.img.aarch64.p7s</i> <i>install.aarch64.p7s</i>

## 2.6 Migration of the configuration from mGuard firmware version 8.x to 10.x

The new mGuard device platform 3 is operated with the mGuard 10.x firmware version. A direct update from firmware version 8.x/9.x to 10.x is not possible.

However, the configuration of mGuard 8.x/9.x devices can be migrated to devices with installed mGuard 10.x firmware version.

The procedure for the migration to mGuard 10.6.0 is described in the application note "Device replacement and migration" (AH DE MGuard MIGRATE 10 - 111259\_en\_xx), available at [phoenixcontact.net/product/<item-number>](http://phoenixcontact.net/product/<item-number>).

## 2.7 General information about mGuard updates

### 2.7.1 PHOENIX CONTACT Web Shop

The available update files for each mGuard device are provided for download on the product page in the PHOENIX CONTACT Web Shop under: [phoenixcontact.net/products](https://phoenixcontact.net/products). Depending on the installed firmware version, different files must be used for an update.

The screenshot shows the PHOENIX CONTACT Web Shop interface. At the top, there is a search bar and navigation links for PRODUCTS, INDUSTRIES & APPLICATIONS, COMPANY, EVENTS & NEWS, and SUPPORT & RESOURCES. The breadcrumb trail indicates the path: Home > Products > Industrial communication > Industrial routers and cybersecurity > Router - FL MG. The main product is the Router - FL MGuard RS4000 TX/TX-I, with part number 2702259. A description states it is a security appliance for process applications, supporting 10/100 Mbps, NAT, firewall, 250' tunnel, MODBUS inspector, and OPC inspector. A red box highlights the text "Free Download available. Downloads". Below the product image, there is a note: "The figure shows a version of the product" and a link "3D View and Download". The "Product Details" section is partially visible, showing tabs for Product Description, Technical Data, Commercial Data, and Downloads (highlighted with a red box). A language dropdown menu is also visible at the bottom.

Figure 2-1 PHOENIX CONTACT Web Shop – Product page

## 2.7.2 Versioning: Major, Minor and Patch Releases

The following designations are used in the versioning of the mGuard firmware:

1. Major release (major version number)  
Major releases supplement the mGuard with new properties and contain mostly larger and more fundamental changes to the mGuard firmware. Their version number changes in the first digit position. version **9.0.0**, for example, is a major release for version **8.9.4**.
2. Minor release (minor version number)  
Minor releases supplement mGuard with new properties. Their version number changes in the second digit position. version **8.6.0**, for example, is a minor release for version **8.4.2**.
3. **Patch release** (fixing of vulnerabilities / general bug fixing)  
Patch releases resolve errors in previous versions and have a version number which only changes in the third digit position. version **8.6.1**, for example, is a patch release for version **8.6.0**.

## 2.7.3 Designation of the update files (curly brackets)

The file that must be used to update your mGuard device depends on the firmware version installed on the device.

In the file name of the respective update file, it is indicated in **curly brackets** which firmware versions can be updated with this file.

### Example "Local Update" RS4000

Using the update file "*update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*", firmware versions **8.0.0** to **8.5.x** can be updated to version 8.6.1.

In this case the download file is named "*Update\_8.6.1\_MPC.zip*".

### Example "Online Update" RS4000

With the specification of the package set name "*update-7.{6}-8.6.1.default*", firmware versions **7.6.0** to **7.6.x** can be updated to version 8.6.1.

## 2.7.4 Description of the update procedure



**NOTE: Do not interrupt the power supply of the mGuard device during the update process!** Otherwise, the device could be damaged. In this case, contact the manufacturer.



You can find more information on installation, operation and updates for mGuard devices in the respective firmware reference manual and mGuard device manual (available in the PHOENIX CONTACT Web Shop under [phoenixcontact.net/products](http://phoenixcontact.net/products) or [help.mguard.com](http://help.mguard.com)):

- mGuard 9.x: 105661\_en\_xx "UM EN MGUARD"
- mGuard 9.x: 105656\_en\_xx "UM EN MGUARD DEVICES"
- mGuard 10.x: 110191\_en\_xx "UM EN FW MGUARD10"
- mGuard 10.x: 110192\_en\_xx "UM EN HW FL MGUARD 2000/4000"

### 2.7.4.1 Local Update

The update file (*tar.gz* format) is loaded from the locally connected configuration computer onto the mGuard device and installed via the mGuard web interface (**Management >> Update >> Update**).

The firmware versions which can be updated with the update file are indicated in the file names of the update file in curly brackets.

#### Example (FL MGUARD RS4000):

##### Major release update: 7.6.8 to 8.6.1:

- Download file: *Update\_8.6.1\_MPC*
- Update file: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*

##### Minor release update: 8.4.2 to 8.6.1:

- Download file: *Update\_8.6.1\_MPC*
- Update file: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*

##### Patch release update: 8.6.0 to 8.6.1:

- Download file: *Update\_8.6.1\_MPC*
- Update file: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*

## 2.7.4.2 Online Update



Not available for FL MGuard 2000/4000 devices with firmware version 10.x installed.

The update file is loaded from a configurable update server and installed.

The update is initialized through the request of a **package set** on the mGuard web interface (**Management >> Update >> Update**).

Management >> Update

Overview Update

Local Update ?

Install packages

**Online Update**

Install package set

Automatic Update

Install latest patches

Install latest minor release

Install next major version

**Update Servers**

Seq.	Protocol	Server	Via VPN	Login	Password
1 <input type="button" value="+"/> <input type="button" value="🗑"/>	https://	update.innominat.com <input type="checkbox"/>		<input type="text"/>	<input type="password"/>

The firmware versions which can be updated by means of the selection of the package set name are indicated in the package set names in curly brackets.

**Example (FL MGuard RS4000):****Major release update:** 7.6.8 to 8.6.1

– Package set name: *update-7.{6}-8.6.1.default*

**Minor release update:** 8.4.2 to 8.6.1

– Package set name: *update-8.{0-5}-8.6.1.default*

**Patch release update:** 8.6.0 to 8.6.1

– Package set name: *update-8.{6}-8.6.1.default*



**NOTE: Online or Automatic Updates** from the installed source firmware version **7.6.8** can lead to an error (see note in [Section 2.21, “Setting up mGuard firmware update repositories”](#)).

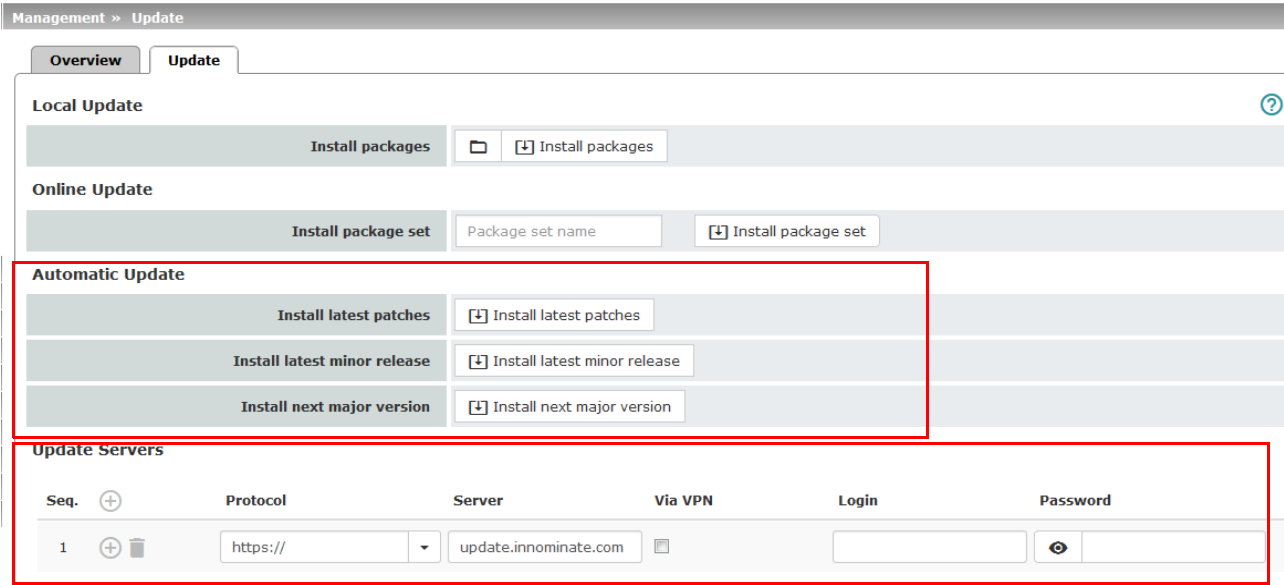


The login information (login + password) does not have to be specified if the update server which has been preset ex-works (<https://update.innominat.com>) is used.

### 2.7.4.3 Automatic Update

The update file is automatically determined from the selected update option and loaded and installed by a configurable update server.

The update is initialized via the mGuard web interface (**Management >> Update >> Update**) or the mGuard command line "*mg update*".



**Update options:**

- a) *Install latest patches*
- b) *Install latest minor release*
- c) *Install next major release*



**NOTE: Online or Automatic Updates** from the installed source firmware version **7.6.8** can lead to an error (see note in [Section 2.21, "Setting up mGuard firmware update repositories"](#)).



It may occur that a **direct Automatic Update** to the current minor or the next major release is not possible from an installed firmware version. In this case, first perform one or more updates on authorized minor or patch releases. Afterwards, you can update to the current minor or the next major release in the last step.



The login information (login + password) does not have to be specified if the update server which has been preset ex-works (<https://update.innominat.com>) is used.



The authenticity of an update server can be ensured by means of an X.509 certificate (variable "Server certificate").

#### 2.7.4.4 Flashing the firmware

The mGuard firmware is loaded from an SD card, USB flash memory (both with vfat file system) or from a TFTP update server, and installed onto the mGuard device.

Installed licenses remain on the device after flashing (in the case of devices with installed firmware version 5.0.0 or higher).

Configuration profiles and licenses can be installed and activated during the flash process (see [Section 2.20, “mGuard Flash Guide”](#)).



**NOTE:** Flashing the firmware deletes all data, passwords and configurations on the mGuard device. The device is reset to its default setting. Save any existing configuration as a configuration profile at a safe location before flashing.



**NOTE:** For mGuard 10 devices, it is not possible to downgrade the current firmware version via flash to a firmware version < 10.5.0.



**NOTE: Downgrading the pre-installed default firmware version is not supported.**  
For mGuard 8 devices produced starting in January 2018, a *downgrade* of the pre-installed default firmware version to an earlier firmware version may fail. If this is the case, flash the device again with the firmware version that was originally installed or a higher version.

## 2.8 FL MGuard RS2000/4000 TX/TX (incl. -B, -P, -M)



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.8.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

**Required files** (depending on installed firmware version!):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

– *Update\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
- (To 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.8.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard RS 4000).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.8.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management** >> **Update** >> **Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.8.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### Package set name to be used (depending on installed firmware version!):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-7.{6}-8.6.1.default*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### 2.8.2.1 Prepare online updates

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### 2.8.2.2 Perform online update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

## 2.8.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### 2.8.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### 2.8.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.8.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*

### 2.8.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard RS 4000).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**:
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s*) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGuard CENTERPORT and FL MGuard GT/GT.

### 2.8.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device until the *Stat*, *Mod*, and *Sig* LEDs light up green.
  - The device starts the flash process: It first searches for an inserted SD card and for the corresponding update file in the */Firmware* directory. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the SD card or the TFTP server.
2. If the LEDs *Stat*, *Mod*, and *Sig* flash green simultaneously, the flash process has been concluded successfully. (The flashing behavior is different in the case of simultaneous uploading of a configuration profile).
3. Restart the device.

## 2.9 FL MGuard RS2005/4004 TX bzw. TX/DTX



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.9.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### Required files (depending on installed firmware version!):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *Update\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
- (To 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.9.1.1 Download update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard RS 4004).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.9.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.9.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### **2.9.2.1 Prepare online updates**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### **2.9.2.2 Perform online update**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set:**
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

## 2.9.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### 2.9.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### 2.9.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.9.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*

### 2.9.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard RS 4004).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *FW\_MPC\_v9.0.0.zip*
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s*) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGuard CENTERPORT and FL MGuard GT/GT.

### 2.9.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device until the *Stat*, *Mod*, and *Info2* LEDs light up green.
  - The device starts the flash process: It first searches for an inserted SD card and for the corresponding update file in the */Firmware* directory. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the SD card or the TFTP server.
2. If the LEDs *Stat*, *Mod*, and *Info2* flash green simultaneously, the flash process has been concluded successfully. (The flashing behavior is different in the case of simultaneous uploading of a configuration profile).
3. Restart the device.

## 2.10 TC MGUARD RS2000/4000 3G VPN



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 (starting from 7.6.0) to version 8.6.1. In the next step, you can update this version to version 9.0.0.



**A Local Update** to mGuard firmware version **8.6.1** is possible from version 8.4.0. **Online Update** and **Automatic Update** are possible from version 8.0.0.

### 2.10.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

**Required files** (*depending on installed firmware version!*):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *Update\_MPC\_TC3G\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *gemalto.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
- (To 8.6.1: *gemalto.update-8.{4-5}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *gemalto.update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.10.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGUARD RS 4000 3G).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_TC3G\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *gemalto.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.10.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *gemalto.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*.
5. Click the **Install packages** button to start the update.

## 2.10.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### 2.10.2.1 Prepare online updates

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### 2.10.2.2 Perform online update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.10.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.10.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.10.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.10.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_TC3G\_v9.0.0.zip*

**Update files**, including modem firmware (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*
- *pxs8\_03001\_0100617.usf.xz.p7s*

### 2.10.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGUARD RS 4000 3G).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: [FW\\_MPC\\_v9.0.0.zip](#)
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s* and *pxs8\_03001\_0100617.usf.xz.p7s*) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGUARD CENTERPORT and FL MGUARD GT/GT.

### 2.10.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from an TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device until the *Stat*, *Mod*, and *Info2* LEDs light up green.
  - The device starts the flash process: It first searches for an inserted SD card and for the corresponding update file in the */Firmware* directory. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the SD card or the TFTP server.
2. If the LEDs *Stat*, *Mod* and *Info2* flash green simultaneously, the flash process has been concluded successfully (differs when uploading a configuration profile).
3. Restart the device.

## 2.11 TC MGuard RS2000/4000 4G VPN

**Order number:** 2903588 (RS2000) / 2903586 (RS4000)



### The required update files depend on the installed modem

The devices 2903588 and 2903586 were produced with two different modems depending on the series:

- until Q3/2021: manufacturer **Huawei**
- from Q3/2021: manufacturer **Gemalto**

Depending on the built-in modem, you need different update and download files for an update to firmware version 9.0.0 (see [Section 2.11.1](#)).



### An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.11.1 Local Update to 9.0.0

**Required files** (*depending on installed firmware version!*):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- Firmware update for devices with **Huawei** engine:
  - *Update\_MPC\_TC4G\_H\_v9.0.0.zip* (see below)
- Firmware update for devices with **Gemalto** engine:
  - *Update\_MPC\_TC4G\_G\_v9.0.0.zip* (see below)

**Update files** (= unpacked Zip file):

- *huaweigeneric.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
- (To 8.6.1: *huaweigeneric.update-8.{4-5}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *huaweigeneric.update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.11.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](https://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGuard RS 4000 4G).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Updat\_MPCeTC4G\_H\_v9.0.0\_.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *huaweigeneric.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.11.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.

**Huawei:**  
Update\_MPC\_TC4G\_H\_v9.0.0.zip

3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *huaweigeneric.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

**Gemalto:**  
Update\_MPC\_TC4G\_H\_v9.0.0.zip

**Update files** (= unpacked Zip file):

- *PLS8-E.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.11.1.3 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGuard RS 4000 4G).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_TC4G\_G\_v9.0.0\_.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *PLS8-E.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.11.1.4 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *PLS8-E.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.11.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-8.{4-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### 2.11.2.1 Prepare online updates

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### 2.11.2.2 Perform online update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.11.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.11.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.11.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

### 2.11.4 Flash firmware version 9.0.0

#### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_TC4G\_v9.0.0.zip*

**Update files**, including modem firmware (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*
- *ME909u-521\_UPDATE\_12.636.12.01.00.BIN.xz.p7s*
- *pls8-e\_rev04.004\_arn01.000.11.usf.xz.p7s*

#### 2.11.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGuard RS 4000 4G).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *FW\_MPC\_TC4G\_v9.0.0.zip*
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s*, *ME909u-521\_UPDATE\_12.636.12.01.00.BIN.xz.p7s*, and *pls8-e\_rev04.004\_arn01.000.11.usf.xz.p7s*,) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGuard CENTERPORT and FL MGuard GT/GT.

#### 2.11.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device until the *Stat*, *Mod*, and *Info2* LEDs light up green.
  - The device starts the flash process: It first searches for an inserted SD card and for the corresponding update file in the */Firmware* directory. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the SD card or the TFTP server.
2. If the LEDs *Stat*, *Mod* and *Info2* flash green simultaneously, the flash process has been concluded successfully (differs when uploading a configuration profile).
3. Restart the device.

## 2.12 TC MGUARD RS2000/4000 4G VZW VPN

**Order number:** 1010462 (RS2000) / 1010461 (RS4000)

### 2.12.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later (maintenance license required).

**Required files** (*depending on installed firmware version!*):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

– *Update\_MPC\_TC4GVZW\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

– *HL7418.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.12.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGUARD RS 4000 4G VZW VPN).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_TC4GVZW\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *HL7518.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.12.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *HL7518.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.12.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

– *update-8.{6-9}-9.0.0.default*

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### 2.12.2.1 Prepare online updates

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### 2.12.2.2 Perform online update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.12.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.12.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.12.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.12.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_TC4G\_VZW\_v9.0.0.zip*

**Update files**, including modem firmware (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*
- *RHL75xx.4.04.142600.201801231340.x7160\_1\_signed\_dwl.dwl.xz.p7s*

### 2.12.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGUARD RS 4000 4G VZW VPN).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *FW\_MPC\_TC4G\_VZW\_v9.0.0.zip*
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s* and *RHL75xx.4.04.142600.201801231340.x7160\_1\_signed\_dwl.dwl.xz.p7s*) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGUARD CENTERPORT and FL MGUARD GT/GT.

### 2.12.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device until the *Stat*, *Mod*, and *Info2* LEDs light up green.
  - The device starts the flash process: It first searches for an inserted SD card and for the corresponding update file in the */Firmware* directory. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the SD card or the TFTP server.
2. If the LEDs *Stat*, *Mod* and *Info2* flash green simultaneously, the flash process has been concluded successfully (differs when uploading a configuration profile).
3. Restart the device.

## 2.13 TC MGUARD RS2000/4000 4G ATT VPN

**Order number:** 1010464 (RS2000) / 1010463 (RS4000)



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.13.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

**Required files** (*depending on installed firmware version!*):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

– *Update\_MPC\_TC4GATT\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

– *HL7588.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.13.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGUARD RS 4000 4G ATT VPN).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_TC4GATT\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *HL7588.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.13.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management** >> **Update** >> **Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *HL7588.update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.13.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

– *update-8.{6-9}-9.0.0.default*

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### 2.13.2.1 Prepare online updates

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### 2.13.2.2 Perform online update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.13.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.13.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.13.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.13.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_TC4G\_ATT\_v9.0.0.zip*

**Update files**, including modem firmware (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*
- *RHL75xx.A.2.15.151600.201809201422.x7160\_3\_signed\_DWL.dwl.xz.p7s*

### 2.13.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. TC MGUARD RS 4000 4G ATT VPN).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *FW\_MPC\_TC4G\_ATT\_v9.0.0.zip*
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s* and *RHL75xx.A.2.15.151600.201809201422.x7160\_3\_signed\_DWL.dwl.xz.p7s*) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGUARD CENTERPORT and FL MGUARD GT/GT.

### 2.13.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device until the *Stat*, *Mod*, and *Info2* LEDs light up green.
  - The device starts the flash process: It first searches for an inserted SD card and for the corresponding update file in the */Firmware* directory. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the SD card or the TFTP server.
2. If the LEDs *Stat*, *Mod* and *Info2* flash green simultaneously, the flash process has been concluded successfully (differs when uploading a configuration profile).
3. Restart the device.

## 2.14 FL MGUARD PCI(E)4000



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.14.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

**Required files** (*depending on installed firmware version!*):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

– *Update\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
- (To 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.14.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGUARD PCI4000).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.14.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management** >> **Update** >> **Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.14.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-7.{6}-8.6.1.default*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### **2.14.2.1 Prepare online updates**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### **2.14.2.2 Perform online update**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.14.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.14.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.14.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.14.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*

### 2.14.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard PCI4000).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *FW\_MPC\_v9.0.0.zip*
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s*) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGuard CENTERPORT and FL MGuard GT/GT.

### 2.14.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device: The two WAN LEDs and the upper LAN LED light up green simultaneously. Release the Reset button during this green light phase.
  - The device starts the flash process: It first searches for an inserted SD card and for the corresponding update file in the */Firmware* directory. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the SD card or the TFTP server.
2. If the two WAN LEDs and the upper LAN LED flash green simultaneously, the flash process has been concluded successfully. (The flashing behavior is different in the case of simultaneous uploading of a configuration profile).
3. Restart the device.

## 2.15 FL MGUARD SMART2



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.15.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

**Required files** (depending on installed firmware version!):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *Update\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
- (To 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.15.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGUARD SMART2).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.15.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management** >> **Update** >> **Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.15.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-7.{6}-8.6.1.default*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### **2.15.2.1 Prepare online updates**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### **2.15.2.2 Perform online update**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set:**
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.15.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.15.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.15.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.15.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*

### 2.15.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard SMART2).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: [FW\\_MPC\\_v9.0.0.zip](#)
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s*) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGuard CENTERPORT and FL MGuard GT/GT.

### 2.15.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device until all three LEDs light up green.
  - The device starts the flash process: The device searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the TFTP server.
2. If all three LEDs flash green simultaneously, the flash process has been concluded successfully. (The flashing behavior is different in the case of simultaneous uploading of a configuration profile).
3. Restart the device.

## 2.16 FL MGUARD CENTERPORT



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.16.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

**Required files** (*depending on installed firmware version!*):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

– *Update\_X86\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *update-8.{6-9}-9.0.0.default.x68\_64.tar.gz*
- (To 8.6.1: *update-7.{6}-8.6.1.default.x68\_64.tar.gz*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default.x68\_64.tar.gz*)
- (To 8.6.1: *update-8.{6}-8.6.1.default.x68\_64.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.16.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGUARD CENTERPORT).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_X86\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.x68\_64.tar.gz* .

#### 2.16.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.x68\_64.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.16.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-7.{6}-8.6.1.default*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### **2.16.2.1 Prepare online updates**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### **2.16.2.2 Perform online update**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.16.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.16.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.16.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.16.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_X86\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *firmware.img.x86\_64.p7s*
- *install.x86\_64\_p7s*

### 2.16.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard CENTERPORT).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *FW\_X86\_v9.0.0.zip*
6. Unpack the Zip file.
7. Copy the unpacked files *firmware.img.x86\_64.p7s*, *install.x86\_64\_p7s* into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the *Firmware* directory on the SD card or the USB flash drive.

### 2.16.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card / USB flash drive first. The firmware is only loaded from a TFTP server if no SD card / USB flash drive is found. The TFTP server must be installed on the locally connected computer.

1. Connect a USB keyboard and a monitor to the device.
2. Restart the device.
3. As soon as the device boots, press one of the arrow keys on the USB keyboard several times until the boot process is interrupted: ↑, ↓, ← or →.
4. The boot menu is displayed.

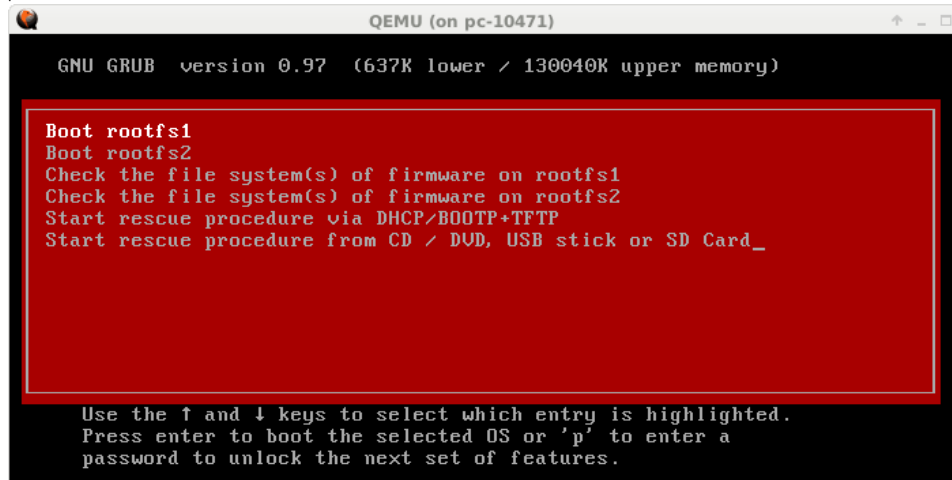


Figure 2-2 Boot menu

5. Select one of the two options to perform the flash procedure (rescue procedure) using the arrow keys ↓ or ↑:

- **Start rescue procedure via DHCP / BOOTP+TFTP**
- **Start rescue procedure from CD / DVD, USB stick or SD card**

To apply the selection, press the **Enter** key.

#### Start rescue procedure via DHCP / BootP+TFTP

**Effect:** The device downloads the necessary files from the TFTP server:

- *install.x86\_64.p7s*
- *firmware.img.x86\_64.p7s*

After the flash process concludes, the device is in the delivery state (default setting).

#### Start rescue procedure from CD/DVD, USB stick or SD card

##### General requirements:

1. A CD/DVD drive connected to the USB port or
2. A USB stick (USB Flash drive) connected to the USB port or
3. An SD memory card inserted into the SD card drive.
4. The necessary update files were copied onto the installation medium in the following directories:
  - */Firmware/install.x86\_64.p7s*
  - */Firmware/firmware.img.x86\_64.p7s*

**Effect:** After the flash process has been started by pressing the Enter key, the required data is downloaded from the selected medium. After the flash process concludes, the device is in the delivery state (default setting).

## 2.17 FL MGuard GT/GT



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.17.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

**Required files** (*depending on installed firmware version!*):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

– *Update\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
- (To 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.17.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard GT/GT).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.17.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.17.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-7.{6}-8.6.1.default*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

### **2.17.2.1 Prepare online updates**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### **2.17.2.2 Perform online update**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.17.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.17.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.17.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.17.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_GTGT\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *jffs2.img.mpc83xx.p7s*
- *install.mpc83xx.p7s*

### 2.17.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGUARD GT/GT).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *FW\_GTGT\_v9.0.0.zip*
6. Unpack the Zip file.
7. Copy all unpacked files (*jffs2.img.mpc83xx.p7s*, *install.mpc83xx.p7s*) from the directory *GTGT* into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server.

### 2.17.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer.

1. Start the flash process by pressing the mode button (see "Section 2.17.4.3, "Function selection by means of mode button (Smart mode)"").
  - The device searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the TFTP server.
2. If **05** is shown in the display, and the LEDs flash green simultaneously, the flash process has been concluded successfully. (The flashing behavior is different in the case of simultaneous uploading of a configuration profile).
3. Restart the device.

**2.17.4.3 Function selection by means of mode button (Smart mode)**

**Activate Smart mode**

The Mode button is used to call/exit Smart mode and to select the desired function. The three mode LEDs indicate the mode that is currently set and the mode which will apply when exiting Smart mode.

**Call up Smart mode**

- Disconnect the device from the power supply.
- As soon as the supply voltage is switched on, hold down the Mode button for **more than ten seconds**. The three mode LEDs flash briefly three times and indicate that Smart mode is active.
- When Smart mode is started, the device is initially in the “Exit without changes” state (“51” in the display).

**Select the desired setting**

- To select the different settings, press the Mode button briefly and select the desired operating mode using a binary light pattern of the mode LEDs and a code on the 7-segment display.

**Exit Smart mode and activating the selection**

- To exit, press and hold down the Mode button for at least five seconds. The previously selected function is executed.

**Possible functions in Smart mode**

The device supports the selection of the following functions in Smart mode (see also example below):

Table 2-5 Functions in Smart mode

Function	7-segment display	ACT LED 1	SPD LED 2	FD LED 3
Exit Smart mode without changes	51	Off	Off	<b>On</b>
Activate the recovery procedure	55	<b>On</b>	Off	<b>On</b>
Activate the flash procedure	56	<b>On</b>	<b>On</b>	Off
Apply customized default profile	57	<b>On</b>	<b>On</b>	<b>On</b>

## 2.18 FL MGUARD DELTA TX/TX



**An update to mGuard firmware version 9.0.0 is possible from version 8.6.1 or later (maintenance license required).**

If necessary, perform the update in two steps, by first updating version < 8.6.1 to version 8.6.1. In the next step, you can update this version to version 9.0.0.

### 2.18.1 Local Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

**Required files** (depending on installed firmware version!):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *Update\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
- (To 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
- (To 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.18.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGUARD DELTA).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_MPC\_v9.0.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*

#### 2.18.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management** >> **Update** >> **Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Major update: *update-8.{6-9}-9.0.0.default.mpc83xx.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.18.2 Online Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

### **Package set name to be used** (*depending on installed firmware version!*):

A package set name describes from which firmware versions updates can be made to the current firmware version.

- *update-8.{6-9}-9.0.0.default*
- (To 8.6.1: *update-7.{6}-8.6.1.default*)
- (To 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (To 8.6.1: *update-8.{6}-8.6.1.default*)

The curly bracket indicates which installed source firmware versions can be updated by specifying the package set name (see [Section 2.7.3](#)).

### **2.18.2.1 Prepare online updates**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### **2.18.2.2 Perform online update**

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Enter the name of the desired package set in the **Online Update** section under **Install package set**:
  - e.g., Major update: *update-8.{6-9}-9.0.0.default*
4. Click the **Install package set** button to start the update.

### 2.18.3 Automatic Update to 9.0.0



Possible from installed firmware version **8.6.1** or later.

#### 2.18.3.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

#### 2.18.3.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

## 2.18.4 Flash firmware version 9.0.0

### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *FW\_MPC\_v9.0.0.zip*

**Update files** (= unpacked Zip file):

- *ubifs.img.mpc83xx*
- *install-ubi.mpc83xx.p7s*

### 2.18.4.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard DELTA).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *FW\_MPC\_v9.0.0.zip*
6. Unpack the Zip file.
7. Copy all unpacked files (*ubifs.img.mpc83xx*, *install-ubi.mpc83xx.p7s*) from the *mpc* directory into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *ubifs.img.mpc83xx* and *install-ubi.mpc83xx.p7s* files can be used to flash all of the devices described in this document, with the exception of FL MGuard CENTERPORT and FL MGuard GT/GT.

### 2.18.4.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.

1. Hold down the reset button of the device until the three lower LEDs on the left (ERR, FAULT, INFO) light up green.
  - The device starts the flash process: It first searches for an inserted SD card and for the corresponding update file in the */Firmware* directory. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address. The required files are loaded and installed from the SD card or the TFTP server.
2. If the three lower LEDs on the right (ERR, FAULT, INFO) flash green simultaneously, the flash process has been concluded successfully. (The flashing behavior is different in the case of simultaneous uploading of a configuration profile).
3. Restart the device.

## 2.19 FL MGuard 2102/2105, 4305/4305, 4102 PCI(E)



An update to mGuard firmware version **10.6.0** is possible from version **10.5.0 or later**.



All device variants with the suffix K or KX are always included.

### 2.19.1 Local Update to 10.6.0

**Required files** (depending on installed firmware version!):

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

– *Update\_mGuard-10.6.0.zip*

**Update files** (= unpacked Zip file):

– *update-10.{5-6}-10.6.0.default.aarch64.tar.gz*

–

The curly bracket indicates which installed source firmware versions can be updated with the update file (see [Section 2.7.3](#)).

#### 2.19.1.1 Download the update file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](http://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard 4305).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the **download file** *Update\_mGuard-10.6.0.zip*.
6. Unpack the Zip file.
7. Use the **update file** provided for the firmware version installed on your device (see [Section 2.7.3](#)):
  - e. g. Minor update: *update-10.{5-6}-10.6.0.default.aarch64.tar.gz*

#### 2.19.1.2 Install Local Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management** >> **Update** >> **Update**.
3. In the **Local Update** section, click the  **No file selected** symbol under **Install packages**.
4. Select the downloaded **update file**:
  - e. g. Minor update: *update-10.{5-6}-10.6.0.default.aarch64.tar.gz*
5. Click the **Install packages** button to start the update.

## 2.19.2 Automatic Update to 10.6.0

### 2.19.2.1 Prepare Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Make sure that at least one valid update server is entered in the **Update Servers** section.

### 2.19.2.2 Start Automatic Update

1. Log on as *admin* user on the web interface of the mGuard device.
2. Select **Management >> Update >> Update**.
3. Click the button of the desired update process in the **Automatic Update** section to start the update:
  - a) Install latest patches
  - b) Install latest minor release
  - c) Install next major release

### 2.19.3 Flash firmware version 10.6.0s



**NOTE: The device may be damaged if the update process is interrupted.**

Do not switch the device off or interrupt the power supply to the device during the flash process.

#### Required files:

**Download file** on the device-specific product page in the Phoenix Contact Web Shop:

- *Firmware\_mGuard-10.6.0.zip*

**Update files** (= unpacked Zip file):

- *firmware.img.aarch64.p7s*
- *install.aarch64.p7s*

#### 2.19.3.1 Download flash file

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](https://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard 4305).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the following **download file**: *Firmware\_mGuard-10.6.0.zip*
6. Unpack the Zip file.
7. Copy all unpacked files (*firmware.img.aarch64.p7s*, *install.aarch64.p7s*) into a freely selected directory (e.g. *mGuard-Firmware*) on your TFTP server or in the */Firmware* directory on the SD card.



The *firmware.img.aarch64.p7s* and *install.aarch64.p7s* files can be used to flash the devices described in this document (platform 3 devices with installed firmware version 10.x).

#### 2.19.3.2 Flash mGuard device



**NOTE:** Flashing the firmware deletes all passwords and configurations on the mGuard device. The device is reset to its default setting.



During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.

The TFTP server must be installed on the locally connected computer.



#### **Damage to the device in case of premature termination**

Do not restart the device until the flash procedure is completed. (Duration: approximately 2-3 minutes.)

**FL MGuard 2102/4302**  
**FL MGuard 2105/3405**

**Performing a flash procedure (rail mounted devices)**

- Press and hold the Mode button of the device for at least nine seconds until the **“PF1–5” LEDs** light up green.
- Release the Mode button. Otherwise, the device will be restarted.
- ↳ The flash procedure is executed.
- ↳ After approximately 20 seconds, the **PF1-3** LEDs light up in “Running light” mode (green). The **FAIL** LED lights up (red):
  - The device first searches for an inserted SD card and for the corresponding update files in the */Firmware* directory.
  - If the device does not find an SD card, it searches for a DHCP server via the LAN interface (XF2) in order to obtain an IP address.
- ↳ The required files are loaded and installed from the SD card or the TFTP server.
- ↳ The device is automatically restarted again during the flash procedure.  
Do not switch off the device prematurely under any circumstances. Wait until the flash procedure has finished **completely**.
- ↳ The **FAIL** LED then lights up permanently (red).
- ↳ After another approximately 60 seconds, the **PF1-3** LEDs flash (green).
- ↳ The flash procedure has been completed successfully. Duration: approximately 2 minutes.
- Restart the device by briefly pressing the Mode button or temporarily disconnecting the device from the power supply.
- ↳ The device is ready to operate when the **PF1** LED flashes green (heartbeat).

**FL MGuard 4102 PCI(E)**

**Performing a flash procedure (PCI cards)**

- Press and hold the Mode button on the front panel of the device for at least nine seconds until the **PF1 LED** as well as the **LEDs of the Ethernet sockets (XF1/2)** light up green.
- Release the Mode button. Otherwise, the device will be restarted.
- ↳ The flash procedure is executed.
  - The device first searches for an inserted SD card and for the corresponding update files in the */Firmware* directory.
  - If the device does not find an SD card, it searches for a DHCP server via the LAN interface (XF2) in order to obtain an IP address.
- ↳ The required files are loaded and installed from the SD card or the TFTP server.
- ↳ The device is automatically restarted again during the flash procedure.
- ↳ The **PF1/FAIL** LED then lights up and flashes green and red.
- ↳ After another approximately 60 seconds, the **SPD LEDs** (XF1/2) flash additionally (green).
- ↳ The flash procedure has been completed successfully. Duration: approximately 2 minutes.
- Restart the device.
- ↳ The device is ready to operate when the **PF1** LED flashes green (heartbeat).

## 2.20 mGuard Flash Guide

### 2.20.1 Flashing mGuard devices

The mGuard firmware is loaded and installed onto the mGuard device from an SD card, USB flash memory (both with vfat file system) or from a TFTP update server. All data, passwords, and configurations on the device are deleted. The device is reset to its default setting.

Carrying out the flash process is described individually for every mGuard device in this document (see the device-specific Section "*Flash firmware version x.x.x*").



**NOTE:** For mGuard 10 devices, it is not possible to downgrade the current firmware version via flash to a firmware version < 10.5.0.



**NOTE: Downgrading the pre-installed default firmware version is not supported.**

For mGuard devices produced starting in January 2018, a *downgrade* of the pre-installed default firmware version to an earlier firmware version may fail. If this is the case, flash the device again with the firmware version that was originally installed or a higher version.

### 2.20.2 Problems with incompatible SD cards

When you flash the mGuard device with an SD card from a manufacturer other than PHOENIX CONTACT, the flashing procedure described in this document may fail.

To avoid problems flashing with SD cards of other manufacturers, proceed as follows during the described flashing procedure:

1. Push the card lightly into the device without engaging it.
2. Start the flash procedure as described for your device.
3. Hold down the reset button of the device until the corresponding LEDs light up.
4. Release the reset button.
5. Immediately push the card firmly into the slot until it engages.
6. Wait until the flashing procedure is over, then restart the device.

### 2.20.3 Uploading configuration profile during the flash process

You can automatically upload and activate a created configuration profile (ATV profile) onto the mGuard device during the flash process.



The flashing behavior of the LEDs after the flash process deviates in this case from the standard flashing behavior: On DIN rail devices, for example, PF1 and PF3 flash simultaneously and alternately with PF2.

### 2.20.3.1 Preparation

Create the file *preconfig.sh* with the following contents:

#### For unencrypted ATV profiles

```
#!/bin/sh -ex
exec gaiconfig --factory-default --silent --set-all < /bootstrap/preconfig.atv
```

#### For encrypted ATV profiles (mGuard firmware version 10.0 or later)

```
#!/bin/sh -ex
/Packages/mguard-tpm2_0/mbin/tpm2_pkcs7 < /bootstrap/preconfig.atv.p7e > /bootstrap/preconf.atv
gaiconfig --factory-default --set-all < /bootstrap/preconf.atv
```

#### For encrypted ATV profiles (mGuard firmware version 8.x / 9.0)

```
#!/bin/sh -ex
/Packages/mguard-tpm_0/mbin/tpm_pkcs7 < /bootstrap/preconfig.atv.p7e > /bootstrap/preconf.atv
gaiconfig --factory-default --set-all < /bootstrap/preconf.atv
```



If you wish to upload a configuration profile encrypted with the device certificate, you should change the file's name from *\*.atv* to *\*.atv.p7e*. Encrypted and unencrypted configuration profiles can be kept apart easier in this way.

The mGuard device treats the ATV profile equally, independent of the file ending.

During the flash process, the device searches for the following files and uploads them:

- /Rescue Config/<Seriennummer>.atv
- /Rescue Config/<Seriennummer>.atv.p7e
- /Rescue Config/preconfig.atv
- /Rescue Config/preconfig.atv.p7e
- /Rescue Config/preconfig.sh

### 2.20.3.2 Loading configuration profile from SD card

In order to upload and activate a configuration profile during the flash process, proceed as follows:

1. Besides the *Firmware* directory, also create the *Rescue Config* directory.
2. Rename the saved configuration profile as *preconfig.atv* or *<Seriennummer>.atv*.
3. Copy the configuration profile to the *Rescue Config* directory.
4. Copy the *preconfig.sh* file (UNIX-Format) to the *Rescue Config* directory.
5. Carry out the flash process as described for your device.

### 2.20.3.3 Loading configuration profile from the TFTP server

In order to load and activate a configuration profile during the flash process, see the description in [Section 2.20.5, “Setting up DHCP and TFTP servers”](#).

## 2.20.4 Uploading licence file during the flash process



Not for FL MGuard 2000/4000 series devices with firmware version mGuard 10.x installed.

A licence file can be uploaded onto the mGuard device and activated during the flash process as follows (e. g. a licence for more VPN connections *FL MGuard LIC VPN-10* or for a lifetime software update *FL MGuard LIC LIFETIME FW*).

### 2.20.4.1 From SD card

In order to upload and activate a licence file during the flash process, proceed as follows:

1. Create the *Rescue Config.* directory on the installation medium.
2. Copy the licence file in the *Rescue Config.* directory.
3. Rename the licence file as *license.lic* or *<Seriennummer>.lic*.
4. Carry out the flash process as described for your device.

### 2.20.4.2 From the TFTP server

In order to load and activate a licence file during the flash process, see [Section 2.20.5, "Setting up DHCP and TFTP servers"](#).

## 2.20.5 Setting up DHCP and TFTP servers



### Network problems

If you install a second DHCP server in a network, this could affect the configuration of the entire network.



### Third-party software

Phoenix Contact does not undertake any guarantee or liability for the use of third-party products. Any reference to third-party software does not constitute a recommendation, rather serves as an example of a program that could be used.

### 2.20.5.1 Under Windows

If you wish to use the third-party program "*TFTPD32.exe*", obtain the program from a trustworthy source, and proceed as follows:

1. If the Windows PC is connected to a network, disconnect it from the network.
2. On the Windows PC, create a directory that you wish to use for the flash process of mGuard devices. This directory is later selected as root directory of the TFTP server. All the files required are loaded from this directory during the flash process.
3. Copy the desired firmware image file(s) into the created directory.
4. **(Uploading licence file)** If a **licence file** is to be uploaded and installed onto the mGuard device during the flash process, copy the file into the directory that has been created. Name the file as follows:
  - *license.lic* or
  - *<Serial number>.lic*.
5. **(Uploading configuration profile)** If a configuration profile is to be uploaded and activated on the mGuard device during the flash process, copy the corresponding **roll-out script** (*rollout.sh*, see [Section 2.20.6, "Sample script: rollout.sh \(firmware version mGuard 10.x\)"](#)) and the **configuration profile** in the directory that has been created. Name the configuration profile as follows:
  - *preconfig.atv* (if all mGuard devices should receive the same configuration) or
  - *<Seriennummer>.atv* (if each mGuard device should receive an individual configuration).
6. Start the *TFTPD32.exe* program.  
The host IP to be specified is: **192.168.10.1**. It must also be used as the address for the network card.
7. Click the **Browse** button to switch to the directory where the mGuard image files are saved: (e. g. *install-ubi.mpx83xx.p7s*, *ubifs.img.mpc.p7s*).

- Make sure that this really is the correct licence file for the device (under “Management >> Update” on the web interface).

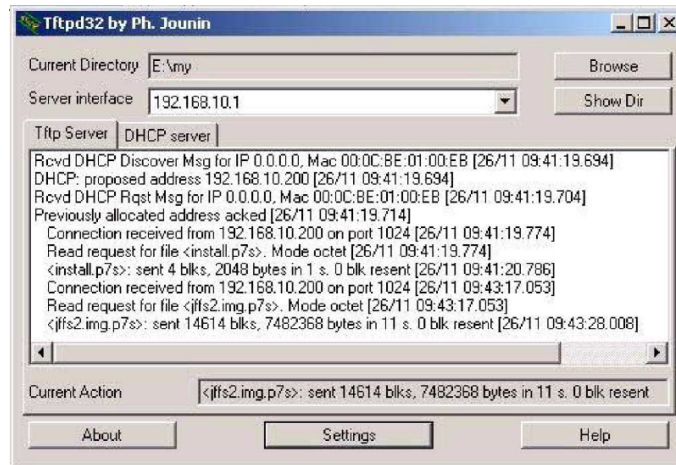


Figure 2-3 Entering the host IP

- Switch to the “TFTP Server” or “DHCP Server” tab and click the “Settings” button to set the parameters as follows:

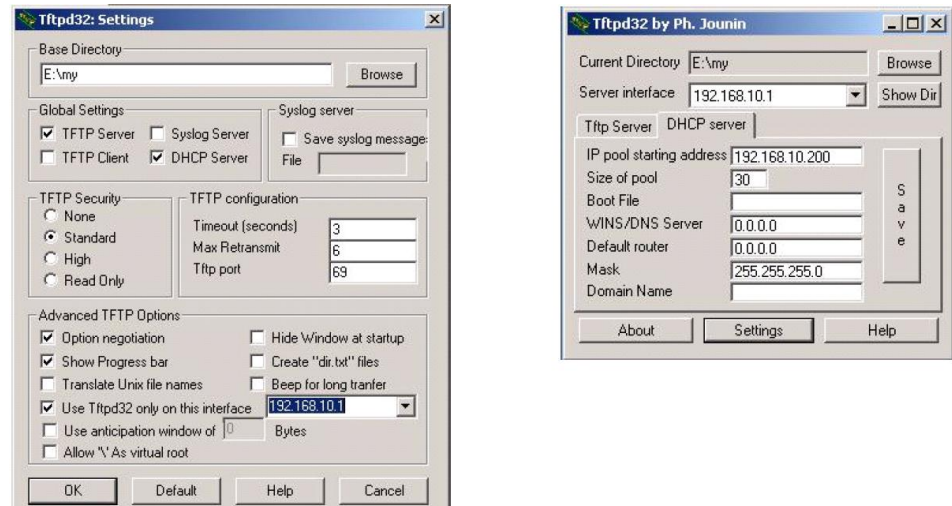


Figure 2-4 Settings

### 2.20.5.2 Under Linux

All current Linux distributions include DHCP and TFTP servers.

1. Install the corresponding packages according to the instructions provided for the respective distribution.

2. Configure the DHCP server by making the following settings in the `/etc/dhcpd.conf` file:

```
subnet 192.168.134.0 netmask 255.255.255.0 {  
  range 192.168.134.100 192.168.134.119;  
  option routers 192.168.134.1;  
  option subnet-mask 255.255.255.0;  
  option broadcast-address 192.168.134.255;}  
This example configuration provides 20 IP addresses (.100 to .119). It is assumed  
that the DHCP server has the address 192.168.134.1 (settings for ISC DHCP 2.0).
```

This example configuration provides 20 IP addresses (.100 to .119). It is assumed that the DHCP server has the address 192.168.134.1 (settings for ISC DHCP 2.0).

The required TFTP server is configured in the following file: `/etc/inetd.conf`

3. In this file, insert the corresponding line or set the necessary parameters for the TFTP service. (Directory for data: `/tftpboot`)

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

The mGuard image files must be saved in the `/tftpboot` directory: e. g. `install-ubi.mpx83xx.p7s`, `ubifs.img.mpc.p7s`.

4. **(Uploading licence file)** If a **licence file** is to be uploaded and installed onto the mGuard device during the flash process, copy the file into the `/tftpboot` directory. Name the file as follows:
  - `license.lic` or
  - `<Serial number>.lic`.
5. **(Uploading configuration profile)** If a configuration profile is to be uploaded and activated on the mGuard device during the flash process, copy the corresponding **roll-out script** (`rollout.sh`, see [Section 2.20.6, “Sample script: rollout.sh \(firmware version mGuard 10.x\)”](#)) and the *configuration profile* in the `/tftpboot` directory. Name the configuration profile as follows:
  - `preconfig.atv` (if all mGuard devices should receive the same configuration) or
  - `<Seriennummer>.atv` (if each mGuard device should receive an individual configuration).
6. Then restart the `inetd` process to apply the configuration changes.
7. If using a different mechanism, e.g., `xinetd`, please consult the corresponding documentation.

### 2.20.5.3 TFTP server: Error messages

During the flash process, the mGuard device searches by default for the files *rollout.sh*, *license.lic* and *<Seriennummer>.lic*. If these files are not available, a corresponding error message is displayed:

```
File rollout.sh: error 2 in system call CreateFile The system cannot find the file specified.  
File <serial number>.lic : error 2 in system call CreateFile The system cannot find the file specified.  
File licence.lic: error 2 in system call CreateFile The system cannot find the file specified.
```

The error message can be ignored if no licence file is uploaded, or the mGuard device should not be preconfigured via the *rollout.sh* script. The flash process is continued as planned in such cases.

## 2.20.6 Sample script: rollout.sh (firmware version mGuard 10.x)



### Use of rollout scripts

The implementation and use of a rollout script is not a part of the mGuard product or mGuard firmware supported by PHOENIX CONTACT. Responsibility for the implementation and use of a rollout script lies solely with the customer and not PHOENIX CONTACT.



### Valid for firmware version mGuard 10.0 or later

For older firmware versions or devices of the older mGuard generation (platform 2), the script must be adapted accordingly.

During the flash process, the mGuard device checks the presence of the *rollout.sh* file. This file must be located in the same directory as the firmware image file on the TFTP server. If the file exists, it is uploaded on the mGuard device and run there.

The *rollout.sh* file must be a UNIX shell script. The configuration data for the mGuard device can be requested from the TFTP server with the script, and the configuration program of the mGuard device (*gaiconfig*), started.

The rollout script documented here serves as a template and only can be used in a manner individually adapted by the customer. In principle, the rollout support can be implemented in two ways, so that

- "all" mGuard devices receive the same configuration (**static TFTP**), or
- "every" mGuard receives its own individual configuration depending on its serial number (**dynamic TFTP**).

### 2.20.6.1 Static TFTP (standard configuration for every mGuard device)

A sample *rollout.sh* script is documented below. This downloads a standard configuration file for installation on mGuard devices from the TFTP server via *tftp*. The name of the configuration file defined in the script is *preconfig.atv*.

#### For **unencrypted** atv profiles (mGuard 10.0 or later)

```
#!/bin/sh -ex
# The IP address of the DHCP/TFTP server
# is supplied by install.aarch64.p7s
server=$1

# This is the filename of the user supplied static configuration file
# on the host in the TFTP-server directory
cfg_name=preconfig.atv
export PATH=/bin:/bootstrap

# fetch the static configuration-file "preconfig.atv"
tftp -g -l /bootstrap/preconfig.atv -r "$cfg_name" "${server}"

# create a small configuration-script that installs the
# configuration fetched from ${server}
cat >/bootstrap/preconfig.sh <<EOF

#!/bin/sh -ex
gaiconfig --factory-default --silent --set-all < /bootstrap/preconfig.atv
EOF

# Make it executable. It will be executed after all packets
# are installed completely.
chmod 755 /bootstrap/preconfig.sh
```

**For encrypted atv profiles (mGuard 10.0 or later)**

```
#!/bin/sh -ex
# The IP address of the DHCP/TFTP server
# is supplied by install.aarch64.p7s
server=$1
export PATH=/bin:/bootstrap

# This is the filename of the user supplied static configuration file
# on the host in the TFTP-server directory
cfg_name=preconfig.atv.p7e

# fetch the static configuration-file "preconfig.atv"
tftp -g -l /bootstrap/preconfig.atv.p7e -r "$cfg_name" "${server}"

# create a small configuration-script that installs the
# configuration fetched from ${server}
cat >/bootstrap/preconfig.sh <<EOF

#!/bin/sh -ex
/Packages/mguard-tpm2_0/sbin/tpm2_pkcs7 < /bootstrap/preconfig.atv.p7e > /bootstrap/preconf.atv
gaiconfig --factory-default --set-all < /bootstrap/preconf.atv
EOF

# Make it executable. It will be executed after all packets
# are installed completely.
chmod 755 /bootstrap/preconfig.sh
```

**2.20.6.2 Dynamic TFTP (individual configuration for every mGuard device)**

A sample *rollout.sh* script is documented below. This downloads a device-specific configuration file from the TFTP server via *tftp*. The name of the configuration file defined in the script is *<SERIAL>.atv*.

**For unencrypted atv profiles (mGuard 10.0 or later)**

```
#!/bin/sh -ex
# The IP address of the DHCP/TFTP server
# is supplied by install.aarch64.p7s
server=$1

# This is the filename of the user supplied static configuration file
# on the host in the TFTP-server directory
SERIAL="` /Packages/ihal_0/bin/ihal param oem_serial ` "
cfg_name=${SERIAL}.atv
export PATH=/bin:/bootstrap

# fetch the static configuration-file "preconfig.atv"
tftp -g -l /bootstrap/preconfig.atv -r "$cfg_name" "${server}"

# create a small configuration-script that installs the
# configuration fetched from ${server}
cat >/bootstrap/preconfig.sh <<EOF

#!/bin/sh -ex
gaiconfig --factory-default --silent --set-all < /bootstrap/preconfig.atv
EOF

# Make it executable. It will be executed after all packets
# are installed completely.
chmod 755 /bootstrap/preconfig.sh
```

**For encrypted atv profiles (mGuard 10.0 or later)**

```
#!/bin/sh -ex
# The IP address of the DHCP/TFTP server
# is supplied by install.aarch64.p7s
server=$1
export PATH=/bin:/bootstrap
SERIAL="" ` /Packages/ihal_0/bin/ihal param oem_serial ` "

# This is the filename of the user supplied static configuration file
# on the host in the TFTP-server directory
cfg_name=${SERIAL}.atv.p7e

# fetch the static configuration-file "preconfig.atv"
tftp -g -l /bootstrap/preconfig.atv.p7e -r "$cfg_name" "${server}"

# create a small configuration-script that installs the
# configuration fetched from ${server}
cat >/bootstrap/preconfig.sh <<EOF

#!/bin/sh -ex
/Packages/mguard-tpm2_0/sbin/tpm2_pkcs7 < /bootstrap/preconfig.atv.p7e > /bootstrap/preconf.atv
gaiconfig --factory-default --set-all < /bootstrap/preconf.atv
EOF

# Make it executable. It will be executed after all packets
# are installed completely.
chmod 755 /bootstrap/preconfig.sh
```

## 2.21 Setting up mGuard firmware update repositories



If you have questions, please contact Support at your local PHOENIX CONTACT subsidiary.

To update your mGuard devices, you can use your own update server (Unix or Windows server). You can download the required update files on the device-specific product pages in the Phoenix Contact Web Shop.

### Download file:

- **FL MGuard CENTERPORT**  
**Unix and Windows Server:** *mguard-firmware-repositories\_x86\_v9.0.0.zip*
- **Other FL/TC MGuard devices (mGuard 8.x)**  
**Unix and Windows Server:** *mguard-firmware-repositories\_mpc\_v9.0.0.zip*
- **Other FL MGuard devices (mGuard10.x)**  
**Unix and Windows Server:** *mguard-firmware-repositories\_10.6.0.zip*

To operate an update server, proceed as follows:

1. Open the website of the Phoenix Contact Web Shop in a web browser at: [phoenixcontact.com/products](https://phoenixcontact.com/products).
2. Search for the device's product name (e.g. FL MGuard RS 4000).
3. Open the desired product page.
4. Select the *Downloads* tab and the *Firmware update* category.
5. Download the desired **Download file:**  
*mguard-firmware-repositories\_mpc\_v9.0.0.zip*
6. Copy the contents of the ZIP folder onto your update server.
7. Enter the update server on the mGuard web interface under **Management >> Update >> Update** (see [Section 2.7.4.3, "Automatic Update"](#)).
8. You can now carry out **Online Updates** or **Automatic Updates** from your update server.



**NOTE: Online or Automatic Updates** from the installed source firmware version **7.6.8** can lead to an error when the update server is operated with newer versions of the Apache Web Server (e.g. 2.4.18).

This problem will not occur if the Phoenix Contact update server (<https://update.innomainate.com>) is used (default setting).

To avoid the problem, an update server such as *nginx* or *fnord* can be used instead of an Apache Web Server.



### 3 Device replacement and migration

- 3.1 Migration from mGuard 8/9 to mGuard 10.x ..... 89
- 3.2 General procedure ..... 90
- 3.3 Saving and importing the device configuration ..... 91
- 3.4 Cases that require manual adjustment ..... 95
- 3.5 Resetting variables to the default settings ..... 96
- 3.6 Device differences ..... 97

#### 3.1 Migration from mGuard 8/9 to mGuard 10.x

The devices of the new FL MGUARD 2000/4000 series are compatible with the devices of the previous series (previous models with mGuard firmware 8.x/9.x) (see [Table 3-1](#)).

It is therefore possible to import and activate a configuration profile created on the predecessor model (mGuard 8.x/9.x) on the new device (mGuard 10.x).

The configuration can be migrated or imported in three ways:

- Import via web interface ([Section 3.3.1](#))
- Import via SD card ([Section 3.3.2](#))
- Import via “mGuard device manager (mdm)” (see mdm user manual)

For the majority of applications, the migration is performed directly and without additional configuration effort.

Table 3-1 Migration of the configuration of compatible devices:  
mGuard 8.x/9.x --> 10.6

New devices – mGuard 10	Item number	Previous models – mGuard 8/9	Item number
FL MGUARD 4302	1357840	FL MGUARD RS4000 TX/TX (VPN)	2700634 / (2200515)
FL MGUARD 4302/KX	1696708	FL MGUARD RS4000 TX/TX-P	2702259
FL MGUARD 4305	1357875	FL MGUARD RS4004 TX/DTX (VPN)	2701876 / (2701877)
FL MGUARD 4305/KX	1696779		
FL MGUARD 2102	1357828	FL MGUARD RS2000 TX/TX VPN	2700642
		FL MGUARD RS2000 TX/TX-B	2702139
FL MGUARD 2105	1357850	FL MGUARD RS2005 TX VPN	2701875
FL MGUARD 4102 PCI	1441187	FL MGUARD PCI4000 VPN	2701275
FL MGUARD 4102 PCIE	1357842	FL MGUARD PCIE4000 VPN	2701278
The models specified on the right do not represent predecessor models in the true sense. However, your configuration can still be migrated to the new devices with corresponding adjustments.		FL MGUARD GT/GT (VPN)	2700197 / (2700198)
		FL MGUARD SMART2 (VPN)	2700640 / (2700639)
		FL MGUARD DELTA TX/TX (VPN)	2700967 / (2700968)
		FL MGUARD RS4000 TX/TX VPN-M	2702465



In rare cases and for certain configurations, it may be necessary to adapt the existing configuration (mGuard 8/9) before migrating (see [Section 3.4](#)).



Please note that configurations of FL MGUARD (RS)4000 series devices can only be migrated after adjustments to FL MGUARD 2000 series devices.

## 3.2 General procedure

- Start the old device (mGuard 8/9).
- Save the current configuration of the old device to an external data carrier.
- Check whether unsupported functions are activated.
- If necessary, set unsupported functions to the default settings.
- Save and export the adapted configuration of the old device.
- Start the new device (mGuard 10).
- Import the previously exported configuration onto the new device.
- Check exactly whether the configuration has been imported successfully.
- If not already done so: Activate the imported configuration on the new device.
- Disconnect the old device from the power supply.
- Disconnect the old device from the network.
- If necessary, disconnect the service contacts (I/Os) of the old device.
- Connect the new device to the network.
- If necessary, connect the service contacts (I/Os) of the new device.
- Start the new device.
- ↳ Firewall rules are activated.
- ↳ Network connections and VPN connections are established.
- Check whether the connections in your network behave as expected.
- If necessary, remove the SD card from the device.

### Result

- ↳ The old device configuration was imported and activated on the new device.
- ↳ All migrated functions are executed on the new device as usual.
- ↳ The old device can be removed and taken out of operation (Decommissioning mode).

### Video

The process of device migration is also shown in a short video on the Phoenix Contact website.

Link to the video: [phoe.co/security-router-mGuard](https://phoe.co/security-router-mGuard)

## 3.3 Saving and importing the device configuration

### 3.3.1 Import via web-based management (WBM)



In rare cases and for certain configurations, it may be necessary to adapt the existing configuration (mGuard 8/9) before migrating (see [Section 3.4](#)).

To export a configuration via the WBM from an mGuard 8/9 device and import it to an mGuard 10.6 device, proceed as follows.

**Configuration Profiles**

Configuration Profiles

Status	Name	Size	Action
	Factory Default	37544	
	Migration	50697	

Save current configuration to profile  Save

*Please note:* Only applied changes will be saved.

Upload configuration to profile  Upload

#### Exporting the configuration profile

First, create and export a configuration profile on the old device (mGuard 8/9):

- Open the menu “Management >> Configuration Profiles >> Configuration Profiles”.
- At “Save current configuration to profile”:
  - Give the profile a profile name.
  - Click on „Save“.
- ↳ The configuration profile appears in the list of saved profiles.
- Click on the name of the configuration profile you want to migrate.
- ↳ The profile is downloaded to the configuration computer: <name>.atv

#### Importing the configuration profile

Then import the exported configuration profile into the new device (mGuard 10.6):

- Open the menu “Management >> Configuration Profiles >> Configuration Profiles”.
- At “Upload configuration to profile”:
  - Give the profile a profile name.
  - Click on the icon to select the previously created configuration profile.
  - Click on “Upload”.
- ↳ The configuration profile is imported into the device and appears in the list of saved profiles.
- Activate the profile by clicking on the “Restore profile” icon .
- ↳ The configuration profile is activated .

### 3.3.2 Import via SD card (ECS)



In rare cases and for certain configurations, it may be necessary to adapt the existing configuration (mGuard 8/9) before migrating (see [Section 3.4](#)).

To export an SD card configuration from an mGuard 8/9 device and import it to an mGuard 10.6 device, proceed as follows.

#### Exporting a configuration

Save the configuration of the old device (mGuard 8/9) on an SD card:

- Open the menu “Administration >> Configuration Profiles >> External Configuration Storage (ECS)”:
  - At “Save current configuration on the ECS”:
    - Enter the password of the user *Root* on.
    - Click on the “Save” button
- ↳ The currently stored configuration is written to the SD card inserted.



The configuration on the external storage medium also contains the encrypted passwords (hashed) for the *root*, *admin*, *netadmin*, *audit*, and *user* users, as well as for SN-MPV3 users. These are also applied during charging.

#### Importing a configuration

The configuration can be imported in two ways:

##### 1. Automatically on startup

- Insert the SD card with the saved configuration **before startup** into the new device.
  - Start the device.
- ↳ The configuration is automatically loaded and activated.

##### 2. Manual

- Insert the SD cards with the saved configuration **after the start** into the new device.
  - Log in to the web interface (WBM) of the device.
  - Open the menu “Administration >> Configuration Profiles >> External Configuration Storage (ECS)”.
  - Start the “Load configuration from the ECS” function.
- ↳ The configuration is loaded and activated.

### 3.3.3 Signed configuration profiles

From firmware version mGuard 10.5.0, it is possible to sign configuration profiles. On devices configured accordingly, it is then only possible to import and use signed configuration profiles. Unsigned configurations will be rejected.

If you still want to import unsigned, already exported configuration profiles on such a device, you can also sign them manually with a machine certificate of the mGuard device before importing them. The procedure is described below.

#### Required files

Make the following files available.

Table 3-2 Required files (the names are examples)

<b>my_profile.atv</b> = configuration profile	Configuration profile (e.g. <i>my_profile.atv</i> ) that is to be signed.
<b>sign.crt</b> = machine certificate	Machine certificate with which the configuration profile is to be signed. (The associated private key is <i>sign.pem</i> ).  The machine certificate, but not the associated private key, can be downloaded from an mGuard device (or, like <i>sign.pem</i> , provided using a saved file).  The certificate must be PEM-encoded. It is a text file. It begins with "-----BEGIN CERTIFICATE-----".
<b>sign.pem</b> = private key	Private key of the machine certificate. (The corresponding machine certificate is <i>sign.crt</i> ).  The private key must be PEM-encoded. The text file begins with "-----BEGIN RSA PRIVATE KEY-----".

#### Requirements

The configuration profile (e.g. *my\_profile.atv*)

- must not contain an existing signature. Lines beginning with "#sig" must be removed (see below).
- must use the Unix convention for line endings (simple "Newline"). If the file uses the Windows convention ("Carriage Return" followed by "Newline"), it must be recoded accordingly.
- must end with an end-of-line character ("Newline").

#### Creating a signature

You can use the *sign.crt* and *sign.pem* files to create the signature with which the *my\_profile.atv* configuration profile is to be signed:

- Use the following Linux command to create a signature:
 

```
openssl cms -sign -signer sign.crt -inkey sign.pem -in my_profile.atv -binary -out signature.pem -outform PEM
```
- ↪ The command creates the signature file *signature.pem*.
- Open the *signature.pem* file in a text editor.
- Remove the header ("-----BEGIN CMS-----") and footer ("-----END CMS-----").
- Prefix each line with the text string "#sig" followed by a space character. To do this, use the following Linux command (including all space characters):
 

```
sed '/^-/d; s/^/#sig /' signature.pem > signature.txt
```
- ↪ The modified file is saved in the new *signature.txt* file.

**Signing the configuration profile**

You can sign the configuration profile *my\_profile.atv* with the created signature (*signature.txt*).

- Use the following Linux command:  
cat signature.txt >> my\_profile.atv
- ↳ The signature is appended to the configuration profile *my\_profile.atv* and the profile is signed.
- ↳ You can now import the signed configuration profile on devices that only accept signed configuration profiles. The corresponding certificates for verification must be installed on these devices (machine certificate *sign.crt* or corresponding CA certificates that form a chain of trust with *sign.crt*).

**Example: ATV file with signature**

```
[...]
VPN_TCPENCAP_LISTEN_PORT = "443"
VPN_UNIQUE_IDS = "no"
VPN_XFRM4_GC_THRESH = "2"
WWW_LANGUAGE = "de"
WWW_LEVEL = "10"
WWW_TIMEOUT = "1800"
// End of configuration profile
#sig MIIFcwYJKoZIhvcNAQcCoIIFZDCCBwACAQExDTALBg1ghkgBZQMEAgEwCwYJKoZI
#sig hvcNAQcBoIIC8DCCAuwggHUoAMCAQICCDVQ08u5bnJBMA0GCSqGSIB3DQEBcWUA
#sig MC0xCzAJBgNVBAYTAmRlMQ4wDAYDVQQLEwVlQlBDQTEOMAwGA1UEAxMFSA0Ew
#sig HhcNMjQwODI4MDkyNTAwWhcNMzQwODI4MDkyNTAwWjAtMQswCQYDVQQGEwJkZTEO
#sig MAwGA1UECxMFS0Igo0ExDjAMBGNVBAWBUtCIENBMBIIBIjANBgkqhkiG9w0BAQEF
#sig AA0CAQ8AMIIBCgKCAQEAjPzB1f6PwugA7an0+I1IS7TmrpDu3j63RGcIxahb8Yf
#sig 6SkogxzVvuQ9xz39G5ByERKjamW7AbgnmnPHEU08d0x1WSA9XMTkTD8cXh1ih4S
#sig /K8L2edSdAunEHUkY9anCY0eC+MoGOMVA1XJOFBa1wZump91dKdoRmUfF1N4Nf3N
#sig sKkqHwvR58d19G66ovVhpZtqxKx0eAhsB20vg15cEdnTC7GZrWUGBoXGe0bdvwf
#sig 3NePis9b8NkzGByISGfe5L8RqpSZtfdDH01zJzH10oBZtbK4iXa8YEUQagjG092D
#sig R7AHxCA44ViSp1yXPPutRmKTYv0JvjGU4oH03yGkbwIDAQABoxAwDjAMBGNVHRME
#sig BTADAQH/MA0GCSqGSIB3DQEBcWUA4IBAQCtTf/Y2gYjvznleUUCqq3G82cL9c
#sig 1EutiakDhHUT6+lvSSFYj4H9QMKHWRmD5B3nmeqqm6pwti93teol9VGQnD/5oQM
#sig c2mikMfah32lXwN0RiyAcki56ss0EAmhXcBBmgG4rbt7RRwy7KU8Ksrauxe0twP1
#sig aIAwg1luDnEEW0fYcOKCoYg7Z55pQHibfP9QYVApfJ/4w8nFKcyVloHZ2fSQNhpv
#sig azgZMU5cVugBU2cWd666amYQsb1FtEmKXD1J2iDK4MniUR2uedUxNwbaFYqBUGFQ
#sig WKMFTK+gLk10mjDx2TYjFaqT9qPCWdpD0z9zTURjTZ1Lk0UR3SyE3UcMYICSTCC
#sig AkUCAQEW0TAtMQswCQYDVQQGEwJkZTEOMAwGA1UECxMFS0Igo0ExDjAMBGNVBAW
#sig BUtCIENBAGglUNPLuw5yQTALBg1ghkgBZQMEAgGggeQwGAYJKoZIhvcNAQkDMQsG
#sig CSqGSIB3DQEHATAcBgkqhkiG9w0BCQUxDxcNMjUwMTA5MTMzNTU2WjAvBgkqhkiG
#sig 9w0BCQQxIgo0ExDjAMBGNVBAWBUtCIENBAGglUNPLuw5yQTALBg1ghkgBZQMEAg
#sig hvcNAQkPMwwajALBg1ghkgBZQMEASowCwYJYIZIAWUDBAEwMAsGCWCSAF1AwQB
#sig AjAKBggqhkig9w0DBzA0Bggqhkig9w0DAgICAIAwDQYIKoZIhvcNAwICAUAwBwYF
#sig Kw4DAGcwDQYIKoZIhvcNAwICASgwDQYJKoZIhvcNAQEBBQAEggEAFildP5txQr5S
#sig /7gkM6ORS4Ij2fHUd/+qGY6B1218o60/svduYBBIG2xGt40tBUAIoormCzScXdmT3
#sig rTBE113G6ec72qU1KpT0c+4eY+gdTVQLqp8qpaelU4sbFk4/SgpzyxT+M2pc0xD3
#sig Jik/yAYfkHuV/P4VsYNM0C0keK4Yb0XYUU85pAhStvCK8p4Fzkd+P9p0DCx4VB/
#sig aSozgxhzz37pa1bxSowCMFAhZRgUtgieMuLEyAjQ+C0EwRqZT/zHzFmD3r01721w
#sig ZAvPvZGFkGk/C7VSworTa4fQwZnmIn8axP7Sx8CC/kefrJ15DFtRY5xndB+WXsNh
#sig hvzQQxbnGQ==
```

### 3.4 Cases that require manual adjustment

Some functions available on the previous models (mGuard 8/9) are not supported by the new devices (mGuard 10) (see [Table 3-3](#)).

In the event of a migration via web-based management, a corresponding error message would be displayed when attempting to import such a configuration.

#### Upload configuration to profile

```
Either this configuration profile is inconsistent, or this device does not provide all the features to put the
Loading system configuration:
Error for QOS_INGRESS_LOCAL_ENABLE="yes": The value is not supported due to hardware restrictions.
```

Figure 3-1 Example of an error message when importing incompatible configurations

#### Functions not supported in mGuard 10.6

Table 3-3 Functions not supported in mGuard 10.6

<b>Network: Interfaces</b>
– PPPoE
– PPTP
– Secondary external interface
<b>Network: Serial interface</b>
<b>Network: GRE tunnel (generic routing encapsulation)</b>
<b>VPN redundancy</b>
<b>Quality of Service (QoS)</b>
<b>CIFS Integrity Monitoring</b>
<b>SEC stick</b>

#### What do you need to do?

Before you start the migration, you must manually reset the functions specified in to default settings on the old device (mGuard 8/9). If an error message is shown in the WBM (see above), you can use it as a guide if necessary.

Proceed as described in [Section 3.5](#) .

### 3.5 Resetting variables to the default settings

Management > Configuration Profiles

Configuration Profiles

Status	Name	Size	Action
	Factory Default	37544	
	Migration	50697	

Save current configuration to profile

*Please note:* Only applied changes will be saved.

Upload configuration to profile

The variables that are no longer available on the new device () must be reset to the default settings on the old device before migrating.

If this is not the case, an error message is displayed for an incompatible configuration from which you can ideally derive the variables to be customized.

Alternatively, you can compare the current configuration with the factory default settings of the device. This is done using the “Compare” function in the web interface.

Once you have identified the corresponding variables, you must manually reset them to the default settings.

To do this, proceed as follows:



**First, create a backup copy of your current configuration.**

To do this, save the configuration profile on the device and download it or save it to an SD card (see [Section 3.3](#)).

1. Log into the device via web-based management (WBM).
2. Open the menu “Management >> Configuration Profiles”.
3. Click on the “Edit profile” icon to the right of the “Factory Default” configuration profile.
- ↪ The “Factory Default” configuration profile is loaded, but not activated yet.
 

**NOTE:** Do not activate the profile because it will change the network settings of the device and the network access will be lost.
- ↪ All entries that contain changes to the configuration currently used are highlighted in green on the relevant page and in the associated menu path.
4. Identify using and, if necessary, the variables that must be reset to the default settings using error messages in the WBM. Note the relevant variables.
5. **IMPORTANT:** Now restore your **currently used configuration** by clicking on the “Reset” icon .
6. In your configuration currently used, only return the identified variables manually to the default settings.
7. Then click on the “Apply” icon .
8. If necessary, repeat steps 3 – 7.
- ↪ Once you have reset all relevant variables to the default settings, you can start the migration (see [Section 3.3](#)).

### 3.6 Device differences

For more information, see the UM EN HW FL MGuard 2000/4000 – 110192\_en\_xx device manual (available at [phoenixcontact.net/product/<Item number>](http://phoenixcontact.net/product/<Item number>)).

#### Network ports

Table 3-4 Designation of the network ports / switch ports

Network interfaces (mGuard 10)	Designation (on the device)	Designation (in the firmware)
<b>All FL MGuard devices</b>		
WAN	XF1	eth0
<b>FL MGuard 2102/4302/4102 PCI(E)</b>		
LAN	XF2	eth1
On the devices FL MGuard 2105 and 4305, eth1 acts as a software bridge, which combines all switch ports (with the exception of dmz0).		
<b>FL MGuard 2105/4305 (switch ports)</b>		
LAN1	XF2	swp0
LAN2	XF3	swp1
LAN3	XF4	swp2
<b>FL MGuard 2105 (switch port)</b>		
LAN4	XF5	swp3
<b>FL MGuard 4305 (DMZ port)</b>		
DMZ	XF5	dmz0

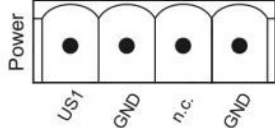
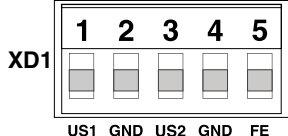
#### Switching inputs/switching outputs (I/Os)

Table 3-5 Switching inputs/switching outputs (I/Os) via Combicon connector

mGuard 8/9	mGuard 10
<b>Switching inputs</b>	
(Service 1) CMD1 (I1)	(XG1) CMD1 (I1)
(Service 2) CMD2 (I2)	(XG1) CMD2 (I2)
(Service) CMD3 (I3)	(XG1) CMD3 (I3)
<b>Switching outputs (signal outputs)</b>	
(Service) ACK1 (O1)	(XG2) ACK1 (O1)
(Service) ACK2 (O2)	(XG2) ACK2 (O2)
<b>Switching output (alarm output)</b>	
(Contact) FAULT (O4)	(XG2) O3

**Supply voltage**

Table 3-6 Power supply via Combicon connector

mGuard 8/9	mGuard 10 (Redundancy only for FL MGUARD 43xx)
	

### 3.6.1 Newly added functions

Variables have been added to the new device platform that are not available on the old device platform.

Table 3-7 Newly added functions / variables

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[Firewall Assistant]</b>  <b>Menu:</b>            Network Security &gt;&gt; Firewall Assistant &gt;&gt; Firewall Assistant            Network Security &gt;&gt; Firewall Assistant &gt;&gt; Alarms  <b>Section:</b>            Firewall Assistant            Alarms (Firewall Assistant)  <b>Variable:</b> Activate Firewall Assistant  <b>GAI variable:</b> FWASSIST_ENABLE</p>	<p>Data traffic unintentionally rejected by the firewall can be easily identified and permitted through the automated creation of corresponding firewall rules.</p> <p><b>Migration of older mGuard configurations</b>            No effect.</p>	<p><b>10.6.0</b></p>
<p><b>[IPsec VPN connections]</b>  <b>Menu:</b> IPsec VPN &gt;&gt; Connections  <b>Section:</b> Connections IKEv2 (beta)  <b>Variable:</b> The variables in the "Connections IKEv2 (beta)" section represent a subsection of the variables that are already available in the "Connections" section.  <b>GAI variable:</b> All GAI variables that contain the designation "IPSEC_CON".</p>	<p><b>NOTE: Can only be used in productive environments after successful testing in the customer application.</b></p> <p>Connections that are configured in the "Connections IKEv2 (beta)" section can also use the IKEv2 protocol in addition to the IKEv1 protocol.</p> <p>Support for the IKEv2 protocol for establishing VPN connections is currently in the beta phase and offers a limited range of functions.</p> <p>In productive use, IKEv2 connections should only be used after successful testing in the customer environment.</p> <p>In the IKEv2 connections, port 54500 is used to establish the connection, in deviation from the standard. Port 54500 must therefore also be configured on the remote side and must not be blocked by firewall settings.</p> <p><b>Migration of older mGuard configurations</b>            No effect.</p> <p>IPsec VPN connections that have already been configured remain unchanged.</p>	<p><b>10.6.0</b></p>

Table 3-7 Newly added functions / variables [...]

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[Update]</b>  <b>Menu:</b> n/a  <b>Section:</b> n/a  <b>Variable:</b> n/a  <b>GAI variable:</b> UPDATE_PASSWORD</p>	<p>A new user with the designation "update" is available.</p> <p>The "update" user is only authorized to perform firmware updates ("Local Update" or "Automatic Update").</p> <p>The "update" user can be created and its password (update password) can be changed.</p> <p>In the current version, the user cannot be configured via the WBM, but only via the <i>Generic Administration Interface</i> (GAI) and the <i>mGuard device manager</i> (FL MGUARD DM UNLIMITED).</p> <p><b>Migration of older mGuard configurations</b>                      No effects.</p>	<p><b>10.6.0</b></p>
<p><b>[Logging]</b>  <b>Menu:</b> n/a  <b>Section:</b> n/a  <b>Variable:</b> n/a  <b>GAI variable:</b> n/a</p>	<p>Remote logging uses the Syslog Message Format, compliant with „RFC 5424 - Ch. 6“.</p> <p><b>Migration of older mGuard configurations</b>                      No effects.</p>	<p><b>10.6.0</b></p>

Table 3-7 Newly added functions / variables [...]

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[Pull Configuration / Configuration Pull Server]</b>  <b>Menu:</b> Administration &gt;&gt; Central Management &gt;&gt; Configuration Pull  <b>Section:</b> Configuration Pull  <b>Variable:</b> Server certificate  <b>GAI variable:</b> GAI_PULL_HTTPS_CERT_REF</p>	<p>In addition to selecting a self-signed or root server certificate, the option "All installed certificates" can also be configured.</p> <p>This has the following advantage:</p> <p>During a planned replacement of the "Configuration Pull Server" certificate, the authentication of the server by the mGuard field devices can take place using either the "old" or the "new" server certificate.</p> <p>This is important if the corresponding server certificate of the field devices is or has been updated via a pull update. This is because the field devices sometimes do not maintain a permanent connection to the configuration pull server, which means that the server certificates are replaced on the field devices at different times.</p> <p>Updated and non-updated field devices can then access the configuration pull server, which uses the old certificate until further notice, regardless of the installed server certificate ("old" or "new").</p> <p>Only after all mGuard field devices have either loaded the new server certificate from the configuration pull server or installed it in another way (e.g. SSH upload or import via WBM) the "old" server certificate can be replaced with the "new" server certificate on the configuration pull server.</p> <p><b>Migration of older mGuard configurations</b></p> <p>No effects.</p> <p>Already configured variable values are adopted.</p>	<p><b>10.6.0</b></p>

Table 3-7 Newly added functions / variables [...]

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[Login via HTTPS/SSH]</b>  <b>Menu:</b> Administration &gt;&gt; System settings &gt;&gt; Host  <b>Section:</b> System  <b>Variable:</b> Control login via on/off switch (HTTPS/SSH)  <b>GAI variable:</b> LOGIN_CONTROL</p>	<p>The login of users on the mGuard device can be controlled via a connected on/off switch (service contact), i.e. activated (permitted) or deactivated (prohibited).</p> <p>This applies to login via the HTTPS (WBM) and SSH (command line) interfaces.</p> <p>The login of the following users is not affected by the function and cannot be controlled via an on/off switch:</p> <ul style="list-style-type: none"> <li>- User "user"</li> <li>- Firewall user</li> <li>- SNMP users via the SNMP interface.</li> </ul> <p><b>Migration of older mGuard configurations</b>                      No effects.</p>	<p><b>10.6.0</b></p>
<p><b>[Login of firewall users]</b>  <b>Menu:</b> Authentication &gt;&gt; Firewall Users &gt;&gt; Firewall Users  <b>Section:</b> Users  <b>Variable:</b> Enable/disable user firewall via on/off switch  <b>GAI variable:</b> USERFW_CONTROL</p>	<p>The user firewall of the mGuard device can be controlled, i.e. activated or deactivated, via a connected on/off switch (service contact).</p> <p>If the login of firewall users is controlled by an on/off switch, firewall users can only log in and use the functions of the user firewall if the switch has been activated.</p> <p><b>Migration of older mGuard configurations</b>                      No effect.</p>	<p><b>10.6.0</b></p>

Table 3-7 Newly added functions / variables [...]

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[SSH server] / [HTTPS-Server]</b>  <b>Menu:</b> Administration &gt;&gt; System Settings &gt;&gt; Shell Access  <b>Menu:</b> Administration &gt;&gt; Web Settings &gt;&gt; Access  <b>Section:</b> Shell &gt;&gt; Access  <b>Section:</b> HTTPS Web Access  <b>Variable:</b> Update SSH and HTTPS keys  <b>GAI variable:</b> n/a</p>	<p>Algorithms that are considered insecure are generally no longer supported by the mGuard device.</p> <p>If an SSH/HTTPS client uses outdated and therefore insecure hashing and encryption algorithms, the connection may be rejected by the mGuard. The mGuard only supports a defined selection of secure hash and encryption algorithms.</p> <p><b>Migration of older mGuard configurations</b>                      No effects.</p> <p>Under certain circumstances, some existing algorithms and SSH/HTTPS keys can initially continue to be used after a successful migration.</p> <p>However, newly created SSH/HTTPS keys only use the current algorithms.</p>	<p><b>10.6.0</b></p>
<p><b>[SNMPv3]</b>  <b>Menu:</b> Administration &gt;&gt; SNMP &gt;&gt; Query  <b>Section:</b> n/a  <b>Variable:</b> n/a  <b>GAI variable:</b> n/a</p>	<p>The MD5 and DES algorithms are no longer supported for newly created SNMP users.</p> <p>The SNMP server of the mGuard device generally only supports current encryption and hash algorithms that are considered secure.</p> <p>If a connection to the mGuard device is established via the SNMPv3 protocol, the hash algorithm SHA-1 (authentication) and the encryption algorithm AES must be used by the remote client.</p> <p><b>Migration from older mGuard configurations</b>                      No effects.</p> <p>Already configured variable values are adopted.</p> <p>The MD5/DES algorithms are still used for SNMPv3 users that have already been created.</p> <p>As soon as new credentials are configured for an SNMPv3 user, only the SHA-1/AES algorithms are used.</p>	<p><b>10.6.0</b></p>

Table 3-7 Newly added functions / variables [...]

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[TCP-Dump]</b>  <b>Menu:</b> Support &gt;&gt; Advanced &gt;&gt; TCP Dump  <b>Section:</b> TCP Dump  <b>Variable (Action):</b>                      (1) Starting tcpdump                      (2) Stopping and downloading tcpdump</p>	<p>A packet analysis (<i>tcpdump</i>) can be used to analyze the content of network packets that are sent or received via a selected network interface.</p> <p><b>Migration of older mGuard configurations</b>                      No effect.</p>	<p><b>10.5.0</b></p>
<p><b>[Logging]</b>  <b>Menu:</b> Logging &gt;&gt; Settings  <b>Section:</b> Data protection  <b>Variable:</b> Maximum retention period for log entries (0 = unlimited)  <b>GAI variable:</b> LOGGING_MAX_DAYS</p>	<p>In order to comply with basic data protection requirements, it is possible to save log entries on the device only for a limited period of time. After a configurable storage period has expired, log entries will be deleted automatically from the device.</p> <p><b>Migration of older mGuard configurations</b>                      No effect</p>	<p><b>10.5.0</b></p>
<p><b>[Configuration profiles]</b>  <b>Menu:</b> Management &gt;&gt; Configuration Profiles  <b>Section:</b> Configuration Profiles Signing  <b>Variables:</b>                      Enable signed configuration profiles                      Export certificate (machine certificate used to sign configuration profiles)                      Import certificate (certificate used to validate signature of configuration profiles)  <b>GAI variables:</b>                      PROFILE_SECURE_ONLY                      PROFILE_EXPORT_CERT                      PROFILE_IMPORT_CERT</p>	<p>Configuration profiles can be signed using certificates. On devices configured accordingly, it is then only possible to upload configuration profiles to the device that have been signed with valid certificates.</p> <p><b>Migration of older mGuard configurations</b>                      No effect</p>	<p><b>10.5.0</b></p>
<p><b>[OpenVPN Client]</b>  <b>Menu:</b> OpenVPN Client &gt;&gt; Connections &gt;&gt; Tunnel Settings  <b>Section:</b> Data Encryption  <b>Variable:</b> Encryption algorithm  <b>GAI variable:</b> OPENVPN_CONNECTION.x.VPN_ENCRYPTION</p>	<p><b>The "Blowfish" encryption algorithm is no longer supported.</b></p> <p>A total of six AES encryption algorithms can be selected instead of the previous three:                      AES-128-GCM / AES-192-GCM / AES-256-GCM / AES-128-CBC / AES-192-CBC / AES-256-CBC</p> <p><b>Migration of older mGuard configurations</b>                      After migrating a configuration from an older firmware version with the "Blowfish" encryption algorithm configured, the value of the variable is set to "AES-256-GCM".                      The following applies to all other algorithms:                      The value from the migrated configuration is adopted unchanged. The configured encryption algorithm will not be changed.</p>	<p><b>10.5.0</b></p>

Table 3-7 Newly added functions / variables [...]

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[HTTPS access]</b>  <b>Menu:</b> Management &gt;&gt; Web Settings &gt;&gt; Access  <b>Section:</b> HTTPS Web Access  <b>Variable:</b> Lowest supported TLS version  <b>GAI variable:</b> TLS_MIN_VERSION</p>	<p>Some functions of the mGuard device use TLS encryption, e.g.:</p> <ul style="list-style-type: none"> <li>– Web server (HTTPS access)</li> <li>– OpenVPN Client</li> </ul> <p>The used TLS version is negotiated between the remote peers. It is possible that a TLS version will be selected, that is no longer considered secure.</p> <p>To prevent this, it can be specified which TLS version will be accepted by the mGuard device as the lowest TLS version. Connections with lower TLS versions will be rejected by the mGuard device.</p> <p>Default: TLS 1.2</p> <p><b>Migration of older mGuard configurations</b></p> <p>The variable will be configured with the value TLS 1.0/1.1. All TLS versions from TLS 1.0 are accepted by the mGuard device.</p>	<p><b>10.5.0</b></p>
<p><b>[Web access via HTTPS / Server certificate]</b>  <b>Menu:</b> Management &gt;&gt; Web Settings &gt;&gt; Access  <b>Section:</b> HTTPS Web Access  <b>Variable:</b> HTTPS server certificate  <b>GAI variable:</b> HTTPS_SERVER_CERT_REF</p> <p>In previous firmware versions, the function was not officially available, but could be used as an unsupported expert function.</p>	<p>Instead of the self-signed web server certificate pre-installed on the mGuard device, a separate machine certificate can be uploaded to the device and used. The device can use this certificate to authenticate itself to requesting clients.</p> <p>The use of CA certificates in conjunction with a certificate chain of trust is possible.</p>	<p><b>10.5.0</b></p>
	<p><b>Migration of older mGuard configurations</b></p> <p>If an HTTPS server certificate is already in use, its use must be deactivated <b>before migrating the configuration or updating the device.</b></p> <p>Command on the command line:  <code>gaiconfig --set HTTPS_SERVER_CERT_REF ""</code></p> <p>You can now perform the migration/update again and use the certificate again (if it is valid).</p> <p>If no HTTPS server certificate is used, the following applies:          No effect.</p>	

Table 3-7 Newly added functions / variables [...]

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[Cellulink mode]</b>  <b>Menu:</b> Network &gt;&gt; Interfaces &gt;&gt; General  <b>Section:</b> Network Status / Network Mode  <b>Variable:</b> LINK mode  <b>GAI variable:</b> ROUTER_MODE_LINK</p>	<p>The mGuard device can use the device "CELLULINK" available from Phoenix Contact to establish a mobile data connection to other networks or the Internet (e.g. via the 4G network).</p> <p>If Cellulink mode is activated, a hyperlink to the web-based management of the device "CELLULINK" is displayed in the WBM area of the mGuard device.</p> <p><b>Migration of older mGuard configurations</b>                      No effect.</p>	<p><b>10.5.0</b></p>
<p><b>[OpenVPN Client]</b>  <b>Menu:</b> OpenVPN Client &gt;&gt; Connections &gt;&gt; Tunnel Settings  <b>Section:</b> Data Encryption  <b>Variable:</b> Hash algorithm (HMAC authentication)  <b>GAI variable:</b> OPENVPN_CONNECTION.x.VPN_AUTH_HMAC</p>	<p>The hash function used to calculate the checksum can be configured.</p> <p><b>Migration of older mGuard configurations</b>                      After migrating a configuration from an older firmware version, the value of the newly added variable is set to "SHA-1".</p>	<p><b>10.4.0</b></p>
<p><b>[Update Server]</b>  <b>Menu:</b> Management &gt;&gt; Update &gt;&gt; Update  <b>Section:</b> Update Servers  <b>Variable:</b> Server certificate  <b>GAI variable:</b> PSM_REPOSITORIES.x.REMOTE_CERT_REF</p>	<p>To ensure that a secure HTTPS connection is established to the configured update server, a server certificate for the update server can be installed on the mGuard device.</p> <p>This can be used by the mGuard device to check the authenticity of the update server.</p> <p><b>Migration of older mGuard configurations</b>                      After migrating a configuration from an older firmware version, the value of the newly added variable is set to "Ignore".</p>	<p><b>10.3.0</b></p>
<p><b>[Alarm Output]</b>  <b>Menu:</b> Management &gt;&gt; Service I/O &gt;&gt; Alarm Output  <b>Section:</b> Operation Supervision  <b>Variable:</b> Passwords not configured  <b>GAI variable:</b> PASSWORD_CHECK</p>	<p>A configurable alarm "Passwords not configured" for default passwords that have not been changed (<i>admin/root</i>) has been added to the device.</p> <p>The alarm triggers the alarm output via I/Os and the corresponding FAIL LED.</p> <p><b>Migration of older mGuard configurations</b>                      After migrating a configuration from an older firmware version, the value of the newly added variable is set to "Supervise".</p>	<p><b>10.3.0</b></p>

### 3.6.2 Changed default settings

In a few cases, the default settings of existing variables on the old and new device platform differ.

Table 3-8 Changed default settings

Function	Changed default settings / Impact of migration	Firmware
<p><b>[OpenVPN Client]</b>  <b>Menu:</b> OpenVPN Client &gt;&gt; Connections &gt;&gt; Tunnel Settings  <b>Section:</b> Data Encryption  <b>Variable:</b> Encryption algorithm  <b>GAI variable:</b> OPENVPN_CONNECTION.x.VPN_ENCRYPTION</p>	<p>In the default settings, the encryption algorithm "AES-256-GCM" is used instead of "AES-256-CBC" as before.</p> <p><b>Migration of older mGuard configurations</b></p> <p>After migrating a configuration from an older firmware version with the "Blowfish" encryption algorithm configured, the value of the variable is set to "AES-256-GCM".</p> <p>The following applies to all other algorithms:  The value from the migrated configuration is adopted unchanged. The configured encryption algorithm will not be changed.</p>	<p><b>10.5.0</b></p>
<p><b>[OpenVPN Client]</b>  <b>Menu:</b> OpenVPN Client &gt;&gt; Connections &gt;&gt; Tunnel Settings  <b>Section:</b> Data Encryption  <b>Variable:</b> Hash algorithm (HMAC authentication)  <b>GAI variable:</b> OPENVPN_CONNECTION.x.VPN_AUTH_HMAC</p>	<p>In the default settings, the hash algorithm "SHA-256" is used instead of "SHA-1" as before.</p> <p><b>Migration of older mGuard configurations</b></p> <p>The value from the migrated configuration is adopted unchanged. The configured hash algorithm will not be changed.</p>	<p><b>10.5.0</b></p>

Table 3-8 Changed default settings

Function	Changed default settings / Impact of migration	Firmware
<p><b>[E-Mail]</b>  <b>Menu:</b> Management &gt;&gt; System Settings &gt;&gt; E-Mail  <b>Section:</b> E-Mail  <b>Variable:</b> Encryption mode for the e-mail server  <b>GAI variable:</b> EMAIL_RELAY_TLS</p>	<p>In the default settings, the encryption algorithm "TLS Encryption" is used instead of "No encryption" as before.</p> <p><b>Migration of older mGuard configurations</b></p> <p>The value from the migrated configuration is adopted unchanged. The configured encryption mode will not be changed.</p>	<p><b>10.5.0</b></p>
<p><b>[Network Address Translation]</b>  <b>Menu:</b> Network &gt;&gt; NAT &gt;&gt; Masquerading  <b>Section:</b> Network Address Translation/IP Masquerading  <b>Variable:</b> Outgoing on interface / From IP</p>	<p>In default settings, a table row/rule with the following variable values is added:</p> <ul style="list-style-type: none"> <li>- Outgoing on interface: External</li> <li>- From IP: 0.0.0.0/0</li> </ul> <p>IP masquerading is thus activated for all packets that are routed from the internal network (LAN) to the external network (WAN) (LAN --&gt; WAN).</p> <p><b>Migration of older mGuard configurations</b></p> <p>The values from the migrated configuration are adopted unchanged. A new table row/rule will not be added.</p>	<p><b>10.3.0</b></p>
<p><b>[Network Settings]</b>  <b>Menu:</b> Network &gt;&gt; Interfaces &gt;&gt; General  <b>Section:</b> Network Mode  <b>Variable:</b> Network mode</p>	<p>All devices of the new device generation are delivered in the network mode "Router".</p> <p>The external WAN interface receives its IP configuration via DHCP. In the default setting, however, the firewall prevents remote access to the device via the WAN interface.</p> <p>The device can be accessed from the LAN network via the internal LAN interface under the network address 192.168.1.1/24. Devices connected to the LAN interface can obtain their IP configuration via the DHCP server of the mGuard device.</p> <p><b>Migration of older mGuard configurations</b></p> <p>The values from the migrated configuration are adopted unchanged. The configured network mode will not be changed.</p>	<p><b>10.3.0</b></p>

### 3.6.3 Changed variable values

In a few cases, variable values are no longer available on the new device platform and are replaced by other values.

Table 3-9 Changed variable values

Function	Changed variable values / Impact of migration	Firmware
<p><b>[OpenVPN Client]</b>  <b>Menu:</b> OpenVPN Client &gt;&gt; Connections &gt;&gt; Tunnel Settings  <b>Section:</b> Data Encryption  <b>Variable:</b> Encryption algorithm  <b>GAI variable:</b> OPENVPN_CONNECTION.x.VPN_ENCRYPTION</p>	<p><b>The "Blowfish" encryption algorithm is no longer supported.</b></p> <p>A total of six AES encryption algorithms can be selected instead of the previous three:  AES-128-GCM / AES-192-GCM / AES-256-GCM / AES-128-CBC / AES-192-CBC / AES-256-CBC</p> <p><b>Migration of older mGuard configurations</b></p> <p>After migrating a configuration from an older firmware version with the "Blowfish" encryption algorithm configured, the value of the variable is set to "AES-256-GCM".</p> <p>The following applies to all other algorithms:  The value from the migrated configuration is adopted unchanged. The configured encryption algorithm will not be changed.</p>	<p><b>10.5.0</b></p>
<p><b>[Shell access]</b>  <b>Menu:</b> Management &gt;&gt; System Settings &gt;&gt; Shell Access  <b>Section:</b> Maximum Number of Concurrent Sessions per Role  <b>Variable:</b> Admin / Netadmin / Audit  <b>GAI variables:</b>  SSH_ADMIN_LOGIN_ALLOWED_MAX  SSH_NETADMIN_LOGIN_ALLOWED_MAX  SSH_AUDIT_LOGIN_ALLOWED_MAX</p>	<p>The "Maximum Number of Concurrent Sessions per Role" is limited to 10.</p> <p><b>Migration of older mGuard configurations</b></p> <ul style="list-style-type: none"> <li>- Applies to all configured values <b>&lt;= 10</b>: <ul style="list-style-type: none"> <li>- The value from the migrated configuration is adopted unchanged. The configured maximum number of concurrent sessions per role will not be changed.</li> </ul> </li> <li>- The following applies to configured values <b>&gt; 10</b>: <ul style="list-style-type: none"> <li>- After the migration, the value of the variable "Maximum Number of Concurrent Sessions per Role" will be set to 10 in each case.</li> </ul> </li> </ul>	<p><b>10.5.0</b></p>

Table 3-9 Changed variable values[...]

Function	Changed variable values / Impact of migration	Firmware
<p><b>[Multicast]</b>  <b>Menu:</b> Network &gt;&gt; Ethernet &gt;&gt; Multicast  <b>Section:</b> General Multicast Configuration  <b>Variable:</b> IGMP snooping</p>	<p>To ensure that data in "Static multicast groups" is forwarded correctly to the configured ports, "IGMP snooping" must be activated</p> <p><b>Migration of older mGuard configurations</b></p> <p>After a migration, the value of the variable will be changed as follows:</p> <ul style="list-style-type: none"> <li>- <b>Enabled:</b> If "Static Multicast Groups" are configured.</li> <li>- <b>Enabled:</b> If "IGMP snooping" is enabled in the old configuration.</li> <li>- <b>Deactivated:</b> If no "Static Multicast Groups" are configured and "IGMP snooping" is deactivated in the old configuration.</li> </ul>	<p><b>10.3.0</b></p>

### 3.6.4 Added functions that were already available on the old device platform

Variables that were already present on the old device platform but had been removed in the meantime were added again on the new device platform.

Table 3-10 Newly added functions / variables / variable values

New function / variable / value	New function / Impact of migration	Firmware
<p><b>[Deep Packet Inspection / Modbus TCP]</b>  <b>Menu:</b> Network Security &gt;&gt; Deep packet Inspection &gt;&gt; Modbus TCP  <b>Section:</b> Rule Records  <b>Variable:</b> various  <b>GAI variable:</b>  MODBUS_RULESETS.x.FRIENDLY_NAME  MODBUS_RULESETS.x.SET.y.MODBUS_FUNCTION_CODE  MODBUS_RULESETS.x.SET.y.ADDRESS_RANGE  MODBUS_RULESETS.x.SET.y.TARGET  MODBUS_RULESETS.x.SET.y.COMMENT  MODBUS_RULESETS.x.SET.y.LOG  MODBUS_RULESETS.x.LOG_DEFAULT</p>	<p>The mGuard device can check packets of incoming and outgoing Modbus TCP connections (<i>Deep Packet Inspection</i>) and filter them if necessary.</p> <p><b>Migration of older mGuard configurations</b>  No effect.  Already configured variable values will be adopted.</p>	<b>10.5.0</b>
<p><b>[Deep Packet Inspection / OPC Inspector]</b>  <b>Menu:</b> Network Security &gt;&gt; Deep packet Inspection &gt;&gt; OPC Inspector  <b>Section:</b> OPC Inspector  <b>Variable:</b> various  <b>GAI variable:</b>  IP_CONNTRACK_OPC  IP_CONNTRACK_OPC_SANITY  IP_CONNTRACK_OPC_TIMEOUT</p>	<p>Until now, the <i>OPC Classic</i> network protocol could only be used across firewalls if large port ranges were opened.</p> <p>Activating the <i>OPC Classic</i> function allows this network protocol to be used easily without having to configure the mGuard device's firewall in an insecure way.</p> <p><b>Migration of older mGuard configurations</b>  No effect.  Already configured variable values will be adopted.</p>	<b>10.5.0</b>
<p><b>[Web access via HTTPS / Server certificate]</b>  <b>Menu:</b> Management &gt;&gt; Web Settings &gt;&gt; Access  <b>Section:</b> HTTPS Web Access  <b>Variable:</b> HTTPS server certificate  <b>GAI variable:</b> HTTPS_SERVER_CERT_REF</p> <p>In previous firmware versions, the function was not officially available, but could be used as an unsupported expert function.</p>	<p>Instead of the self-signed web server certificate pre-installed on the mGuard device, a separate machine certificate can be uploaded to the device and used. The device can use this certificate to authenticate itself to requesting clients.</p> <p>The use of CA certificates in conjunction with a certificate chain of trust is possible.</p>	<b>10.5.0</b>

## MGUARD 10

Table 3-10 Newly added functions / variables / variable values[...]

New function / variable / value	New function / Impact of migration	Firmware
	<p><b>Migration of older mGuard configurations</b></p> <p>If an HTTPS server certificate is already in use, its use must be deactivated <b>before migrating the configuration or updating the device.</b></p> <p>Command on the command line:  <code>gaiconfig --set HTTPS_SERVER_CERT_REF ""</code></p> <p>You can now perform the migration/update again and use the certificate again (if it is valid).</p> <p>If no HTTPS server certificate is used, the following applies:</p> <p>No effect.</p>	

### 3.6.5 Modified designation of GAI variables

The designation of some GAI variables will be changed after the migration from mGuard 8/9 to mGuard 10.3 or higher.

Table 3-11 Modified designations of GAI variables following migration

GAI variable (mGuard 8/9)	GAI variable (mGuard 10.3 or higher)
PORT_MIRROR_RECEIVER	MIRROR_RECEIVER
PHY_SETTING	SWITCHPORT
<b>STATIC_MULTICAST_GROUP</b>	MULTICAST_GROUP

## 4 mGuard 8.9/9.0 - Extended maintenance 2030



Document ID: 112009\_en\_00  
 Document name: AH EN LIC E MNT MDM  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation. It can be downloaded using the following link [phoenixcontact.com/products](https://phoenixcontact.com/products).

### Table of contents

4.1	Extended maintenance until the end of 2030 .....	113
4.2	Maintenance and Support .....	114
4.3	Firmware maintenance license .....	114

### 4.1 Extended maintenance until the end of 2030

The proven mGuard devices with firmware version 8.x installed were discontinued in 2024 after 15 years of availability.

The current firmware in this series will continue to be supported until the end of 2025 and will be supplied with regular free security updates.

Free support for these devices will be discontinued from 2026. However, it can be extended until the end of 2030 with a paid firmware maintenance license.

With this license, it is possible to install firmware version 9.0.x on the devices. These devices will be continuously supported with security updates until the end of support.

#### 4.1.1 List of affected devices

Device	Item No.	Device	Item No.
FL MGuard RS4000 TX/TX (VPN)	2700634 / (2200515)	FL MGuard CENTERPORT (special license)	2702547
FL MGuard GT/GT(VPN)	2700197 / (2700198)	FL MGuard CORE TX VPN	2702831
FL MGuard SMART2 (VPN)	2700640 / (2700639)	TC MGuard RS4000 3G VPN	2903440
FL MGuard RS2000 TX/TX VPN	2700642	TC MGuard RS2000 3G VPN	2903441
FL MGuard RS2000 TX/TX-B	2702139	TC MGuard RS4000 4G VPN	2903586
FL MGuard DELTA TX/TX (VPN)	2700967 / (2700968)	TC MGuard RS2000 4G VPN	2903588
FL MGuard PCI4000 VPN	2701275	TC MGuard RS4000 4G VZW VPN	1010461
FL MGuard PCIE4000 VPN	2701278	TC MGuard RS2000 4G VZW VPN	1010462
FL MGuard RS2005 TX VPN	2701875	TC MGuard RS4000 4G ATT VPN	1010463
FL MGuard RS4004 TX/DTX (VPN)	2701876 / (2701877)	TC MGuard RS2000 4G ATT VPN	1010464
FL MGuard RS4000 TX/TX-P	2702259		
FL MGuard RS4000 TX/TX VPN-M	2702465	<b>Customer-specific variants are also affected!</b>	

The successor products with installed firmware version mGuard 10.x are not affected. They will continue to receive free support and all necessary security updates.

## 4.2 Maintenance and Support

### Vulnerability check

Every day, specialized employees analyze up to 50 reported vulnerabilities (so-called CVE reports) and determine whether mGuard devices are affected by them (PSIRT process).

If this is the case, the respective vulnerability is evaluated according to defined criteria and a decision is then made as to whether the vulnerability will be closed in the next cyclical firmware release or in a timely interim release. Security for the customer is always the top priority.

### Obsolete software components

Further effort goes into evaluating the encryption algorithms used, which become outdated over time and must be kept up to date.

### Maintenance

The requirements for maintaining the current firmware are considerable. The necessary firmware changes affect the Linux kernel hardened by Phoenix Contact, public software libraries, inserted patches and different hardware versions.

### Support


Phoenix Contact is always aware of its responsibility for the customers. This applies in particular to network security devices, i.e. all available mGuard security routers.

For this reason, support for the affected devices can be extended until the end of 2030 for a fee.

## 4.3 Firmware maintenance license

All customers who wish to continue using their existing mGuard devices with firmware version 8.9.x installed can provide their devices with a maintenance license. This ensures that the devices will be supplied with security updates until the end of 2030.

To receive this support, appropriate licenses must be purchased and installed on the devices.

 Devices purchased from around June 2024 do not require the new license if the value „9“ is entered in the WBM as the "*Highest installable firmware major version*" under **Management >> Licensing >> Overview** (see below). These devices will be supported until the end of 2030.

Management > Licensing

Overview Install Terms of License

Feature License

Flash ID (Checksum)	Necec00770164
Serial number	2032415492

Licensed Features	
Feature	Installed
Firewall redundancy	✓
Highest installable firmware major version	9

OPC Inspector	
Feature	
OPC Classic DPI module	

### Available licenses

For all other devices, one of the following licenses must be purchased and installed or be available in order to receive support until the end of 2030:

– **1493074 - FL MGuard LIC FW MNT 2030**

Single license in the form of a license letter (voucher).


The license can be installed individually on one device at a time via web-based management.

– **1775935 - FL MGuard LIC-E FW MNT 2030**

Bulk license in electronic form (email).

The license vouchers can be installed on the devices via the mGuard Device Manager (FL MGuard DM UNLIMITED) or individually via web-based management.

– **2702552 - FL MGuard LIC LFS CENTER**

 "Firmware maintenance license" only for FL MGuard CENTERPORT.

– **2700184 - FL MGuard LIC LIFETIME FW**

Devices on which a "Lifetime Support" license has already been installed do not require an additional license.

## Product short description

---

## 5 Request and distribute mGuard licenses via MDM



Document ID: 112205\_en\_00  
 Document name: AH EN LIC E MNT MDM  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation. It can be downloaded using the following link [phoenixcontact.com/products](https://phoenixcontact.com/products).

### Table of contents

5.1	Introduction .....	117
5.2	Prerequisites .....	117
5.3	Procedure .....	118
5.4	Troubleshooting .....	124

### 5.1 Introduction

This document describes how firmware maintenance licenses can be generated using the mGuard device manager (MDM) and how they can be uploaded and installed on mGuard field devices. By installing the licenses, the devices are supported with security updates until the end of 2030.

### 5.2 Prerequisites

#### Supported mdm versions

FL MGUARD DM UNLIMITED (2981974) from version 1.13.1

#### Supported firmware maintenance licenses

- Single license: FL MGUARD LIC FW MNT 2030 (item number: 1493074)
- Bulk license: FL MGUARD LIC-E FW MNT 2030 (item number: 1775935)

#### Accessibility

The mGuard device manager (MDM) is connected to a network and can access the Internet.

The mGuard devices are online and can either

- be accessed by the MDM via the network/Internet, or
- reach the "Configuration Pull Server" via the network/Internet.

## 5.3 Procedure

### 5.3.1 Step 1: Check whether an initial connection has already been established between the MDM server and the mGuard device

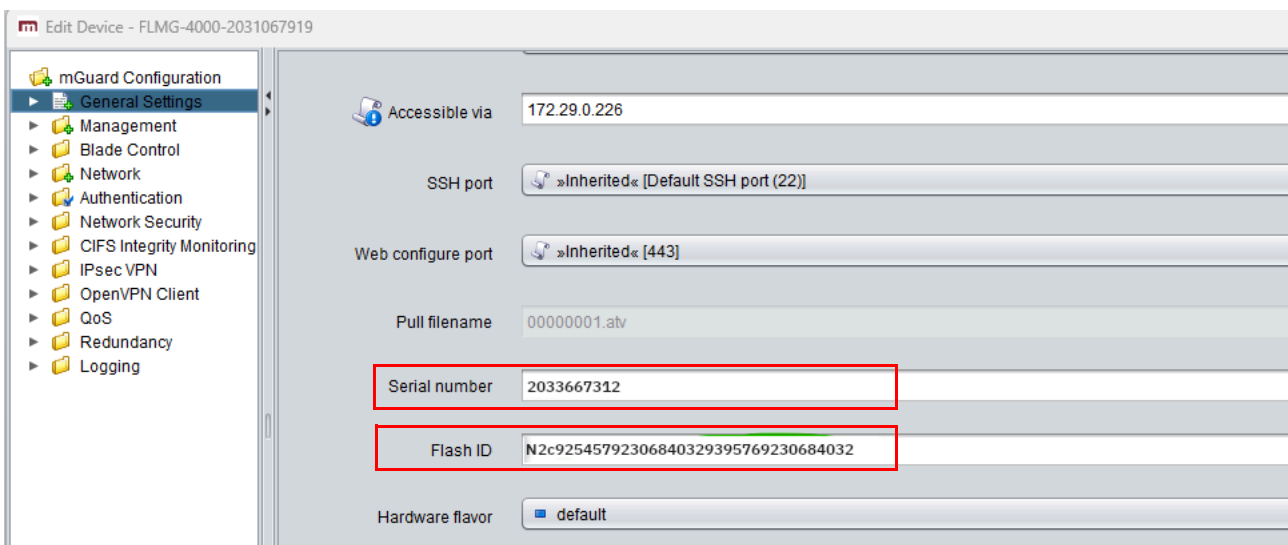
To be able to upload licenses to mGuard field devices using the MDM, the mGuard devices must either have a network connection to the MDM or to the "configuration pull server".

**i** For the unique assignment of licenses to mGuard devices, the "Serial number" and "Flash ID" of the devices must also be entered in the MDM.

**i** **As a rule**, if both the "Version on device" and "Serial number" fields are filled out in the MDM device table (*Device properties dialog*), there is already a connection between the mGuard device and MDM. The "Flash ID" is also entered in this case.

Check in the device table in the *Device properties dialog* under "General Settings" whether the values have already been entered for the corresponding mGuard devices ([Figure 5-1](#)).

Figure 5-1 Device properties dialog - Serial number and Flash ID



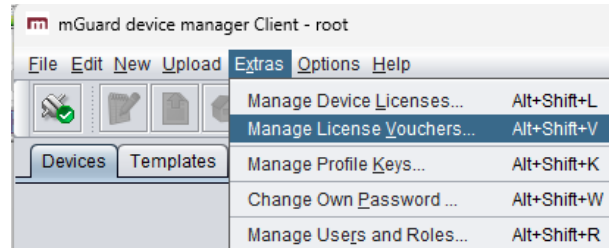
**i** If the "Serial number" was entered manually for commissioning the device, the "Flash ID" is not necessarily included. This is transmitted by the mGuard device each time a connection to the MDM is established. The "Version on device" is also transferred from the mGuard device to the MDM and entered automatically.

**i** Alternatively, the "Serial number" and "Flash ID" can also be retrieved via the web-based management (WBA) of the mGuard device, copied and entered manually in the *Device properties dialog* of the MDM. (Menu item: **Support >> Advanced >> Hardware**).

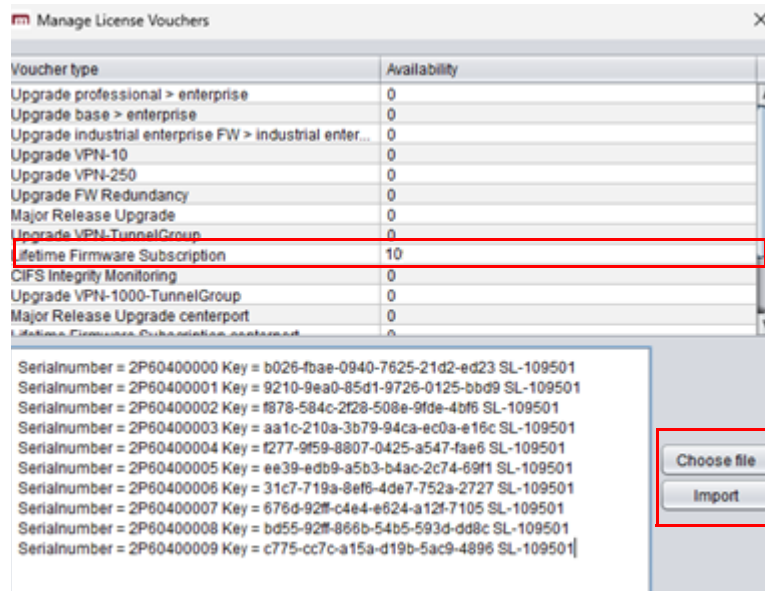
### 5.3.2 Step 2: Importing license vouchers

To make the licenses (purchased in the web shop) available in MDM, proceed as follows:

- Go to the menu item **Extras >> Manage License Vouchers**.



- Click on the "Choose file" button and upload the file with the corresponding license(s) to the MDM (e.g. the bulk license "FL MGUARD LIC\_E FW MNT 2030").
- You can also copy or enter individual vouchers (serial number and key) manually in the text field.



- Click on the "Import" button.
- ↳ The licenses are imported and made available in the MDM.
- ↳ The number of available licenses is then displayed (*Lifetime Firmware Subscription*>> *Availability*) is then displayed. These licenses can be assigned (generated) to selected mGuard devices, uploaded to them and installed.

### 5.3.3 Step 3: Assigning a license to a device and generating it

To assign simultaneously available licenses to selected mGuard devices, proceed as follows:

- Select the desired mGuard devices in the device table.

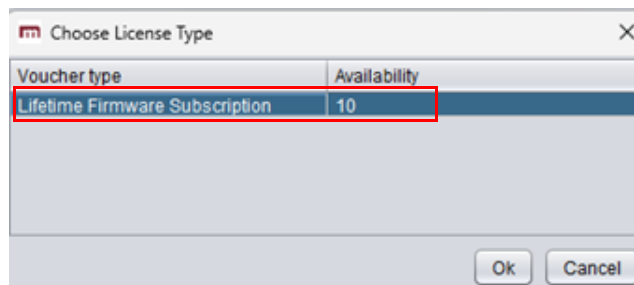
Devices							
C	U	Management ID	Templates	V	Version	F	Version on device
✓	✓	FLMG-4000-2031067919	Basic		mGuard 8.9	✓	8.9.4.default
✓	✓	FLMG-4000-2031067983	Basic		mGuard 8.9	✓	8.9.3.default
✓	✓	FLMG-4005-2032310564	Basic		mGuard 8.9	✓	8.9.4.default

- Right-click on the selected devices.

Devices							
C	U	Management ID	Templates	V	Version	F	
✓	✓	FLMG-4000-2031067919	Basic		mGuard 8.9	✓	
✓	✓	FLMG-4000-2031067983	Basic				
✓	✓	FLMG-4005-2032310564	Basic				

- ➕ Add Ctrl+N
- ✎ Edit Ctrl+E
- 📄 Duplicate Ctrl+D
- 📁 Upload/Import History... Ctrl+Shift+H
- 🔑 Set Current Device Credentials
- 📄 Device Replacement..
- 🏠 Set Redundancy Mode
- 🗨️ Generate Redundancy Passphrases
- 📄 Generate License Ctrl+Shift+L
- 🔄 Refresh License Ctrl+Shift+R
- 🔑 Get Profile Key Generate licen
- 🔒 Enable/Disable Profile Encryption Ctrl+Y
- 🔧 Firmware Upgrade








- Select "Generate License" from the expanded menu.
- ↳ The "Choose License Type" dialog box opens.



- Select the "Lifetime Firmware Subscription" entry and click "OK".
- ↳ The MDM server contacts the license server and transmits the corresponding license files (vouchers) with the associated data of the selected mGuard device(s) (identification parameters such as "Serial number", "Flash ID").

## Request and distribute mGuard licenses via MDM

- ↪ The license server generates the device-specific licenses and then automatically uploads them to the MDM.
- Check that the licenses have been created correctly in the MDM under "Logged events".

	2025-07-04	10:18:16.336	root	Generating 3 device licenses...
	2025-07-04	10:18:23.282	root	Generating license for device 'FLMG-4000-2031067919' failed.
	2025-07-04	10:20:10.194	root	Failed to generate license from voucher 2P60400009 c775-cc7
	2025-07-04	10:20:10.206	root	Error generating license for device FLMG-4000-2031067919
	2025-07-04	10:20:16.424	root	Generated device license LFS.2P60400009.00050600 (LFS).
	2025-07-04	10:20:19.411	root	Generated device license LFS.2P60400005.00050601 (LFS).
	2025-07-04	10:20:19.433	root	Generated 2 licenses.Failed to generate one license.

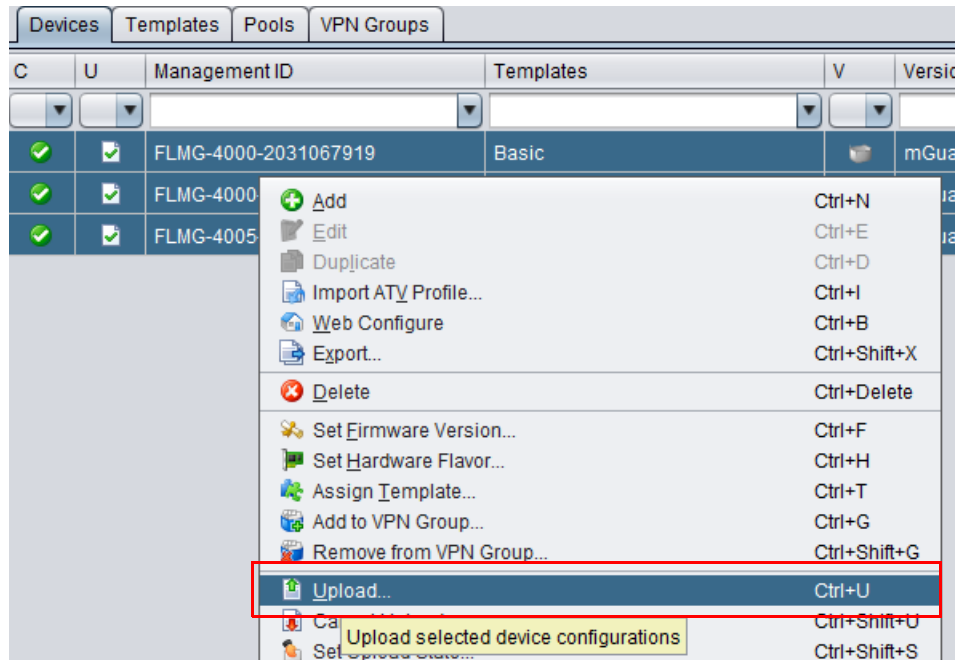
### 5.3.4 Step 4: Upload licenses to mGuard field devices

To upload the licenses generated and registered on the license server from the MDM to the mGuard field devices, proceed as follows:

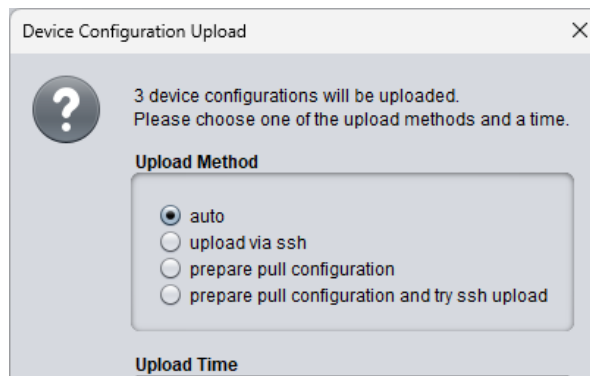
- Select the desired mGuard devices in the device table.

C	U	Management ID	Templates	V	Version	F	Version on device
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FLMG-4000-2031067919	Basic		mGuard 8.9	<input checked="" type="checkbox"/>	8.9.4.default
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FLMG-4000-2031067983	Basic		mGuard 8.9	<input checked="" type="checkbox"/>	8.9.3.default
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FLMG-4005-2032310564	Basic		mGuard 8.9	<input checked="" type="checkbox"/>	8.9.4.default

- Right-click on the selected devices.
- Select "Upload" from the expanded menu.



↪ The "Device Configuration Upload" dialog box opens.



## Request and distribute mGuard licenses via MDM

- Select an upload method. (As a rule, the default upload method "auto" can be retained).
- ↳ If the upload is carried out via SSH, the licenses are transferred to the mGuard devices together with the configuration currently available in the MDM.
- ↳ If the upload is carried out using "Pull Configuration", the licenses are transferred to the "Configuration Pull Server". The license is then transferred to the respective mGuard devices when they successfully connect to the "Configuration Pull Server".
- Check the creation of the licenses in the MDM under **Extras >> Manage License and Vouchers**.

License Id	License date	Flash Id	Device	Max version
LFS.2P60400005.00050601	2025-07-04T10:20:18	Necec00d3c57159343533532300505070b	FLMG-4005-2032310564	999
LFS.2P60400009.00050600	2025-07-04T10:20:15	N205d28323633152533a2d7cdc9cceedacc	FLMG-4000-2031067983	999

- ↳ The number of licenses (vouchers) subsequently available in the MDM is reduced accordingly and displayed in the "Manage License Vouchers" table.

Voucher type	Availability
Upgrade professional > enterprise	0
Upgrade base > enterprise	0
Upgrade industrial enterprise FW > industrial enter...	0
Upgrade VPN-10	0
Upgrade VPN-250	0
Upgrade FW Redundancy	0
Major Release Upgrade	0
Upgrade VPN-TunnelGroup	0
Lifetime Firmware Subscription	8
CIFS Integrity Monitoring	0

### Installed licenses in the WBM of the mGuard devices

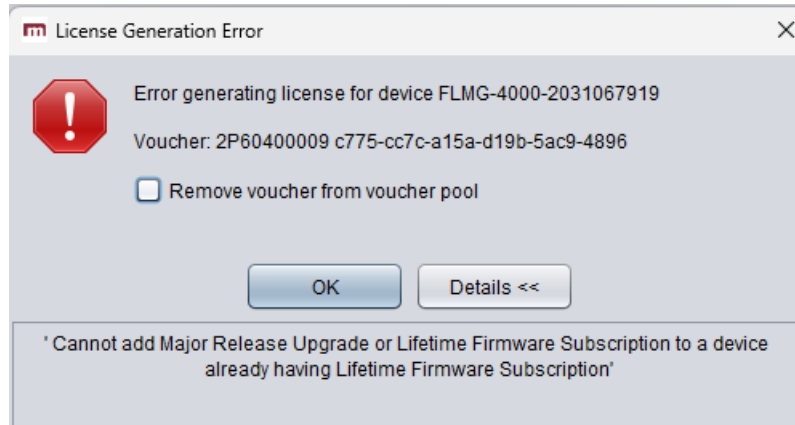
On the mGuard devices, the installed license is displayed as "Highest installable firmware major version = ∞" in the web-based management (WBM) under the menu item **Management >> Licensing**.

Feature	Installed
Firewall redundancy	✓
Highest installable firmware major version	∞
CIFS Integrity Monitoring	✓
Concurrent VPN connections	10
SecStick	✓
OPC Classic DPI module	⊘

## 5.4 Troubleshooting

### 5.4.1 License already installed

An mGuard device selected in the MDM already has a license installed.

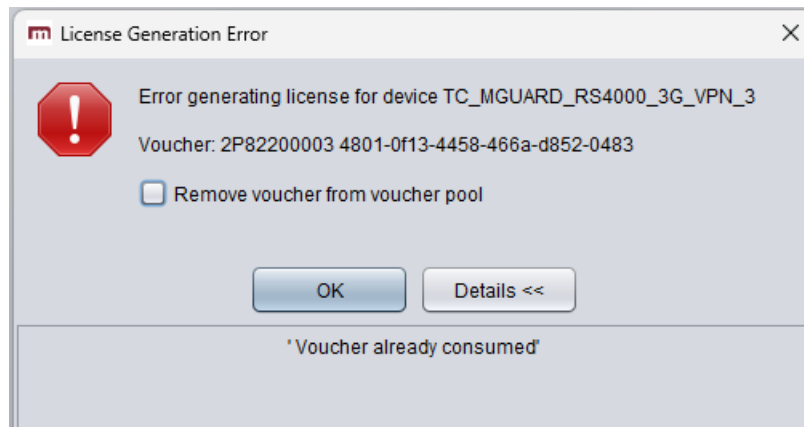


Further procedure:

- You do not need to do anything else, as the mGuard device in question already has a valid license.

### 5.4.2 Voucher already consumed

A purchased voucher has already been consumed on a device (e.g. via the WBM).

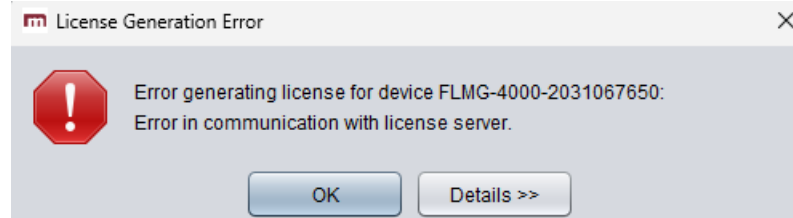


Further procedure:

- You must purchase a valid license (voucher) and make it available in MDM accordingly.
- You can remove the voucher that has already been used from the voucher pool in MDM. To do this, activate the "Remove voucher from voucher pool" checkbox.

### 5.4.3 No connection to the license server

The MDM server cannot resolve the DNS name of the license server or cannot establish a connection to the license server for other reasons.



2025-07-04 13:16:38.986	root	Successfully updated one device.
2025-07-04 13:17:13.986	root	Generating one device license ...
2025-07-04 13:17:34.147	root	Generating license for device 'FLMG-4000-2031067650' failed. (Error in communication with license server.)
2025-07-04 13:18:06.198	root	Failed to generate license from voucher 2P60400006 31c7-719a-8ef6-4de7-752a-2727; server said: Error in communication with license server.
2025-07-04 13:18:06.199	root	Error generating license for device FLMG-4000-2031067650
2025-07-04 13:18:06.211	root	Generated no licenses. Failed to generate one license.

Further procedure:

- Enter a correct address for the DNS server in MDM. (As of mdm version 1.16.0, the MDM cockpit can be used for this).
- Configure a correct network or internet connection from MDM to the license server.
- Test the accessibility of the license server (see below).

#### Test the accessibility of the license server

- Open a command line (terminal) on the MDM server.
  - (From mdm version 1.15.0, a command line can be opened via SSH).
  - As of mdm version 1.16.0, a command line can also be opened via the MDM cockpit under the "Terminal" menu item.

Enter the following command:

```
curl online.license.innominate.com
```

↪ The following output is displayed (in a similar or identical way):

```
vadmin@mdm:~$ curl online.license.innominate.com
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added,
yet.</p>
</body></html>
```

### 5.4.4 Flash ID not available


An mGuard device selected in the MDM only contains the "Serial number" but no "Flash ID".

C	U	Management ID	Templates	V	Version	F	Version on device	Accessible via	Upload scheduled at	Serial number
✓	✓	FLMG-4000-2031067919	Basic	✓	mGuard 8.9	✓	8.9.4.default	172.29.0.226		2031067919
✓	✓	FLMG-4000-2031067983	Basic	✓	mGuard 8.9	✓	8.9.3.default	172.29.0.225		2031067983
✓	✓	FLMG-4005-2032310564	Basic	✓	mGuard 8.9	✓	8.9.4.default	172.29.0.227		2032310564
✗	✗	FLMG-4000-2031067650	Basic	✗	mGuard 8.9	?	unknown	172.29.0.228		2031067650



Further procedure:

- Establish an initial connection between the mGuard device and the MDM server in order to transfer the "Flash ID" from the device to the MDM.
- The initial connection can be established using the following mechanisms:
  - a) Upload via SSH-Upload
  - b) Upload via Pull-Configuration
  - c) Importing an ATV profile from the mGuard device

 Alternatively, the "Serial number" and "Flash ID" can also be retrieved via the Web ased management (WBA) of the mGuard device, copied and entered manually in the *Device properties dialog* of the MDM.

Support » Advanced

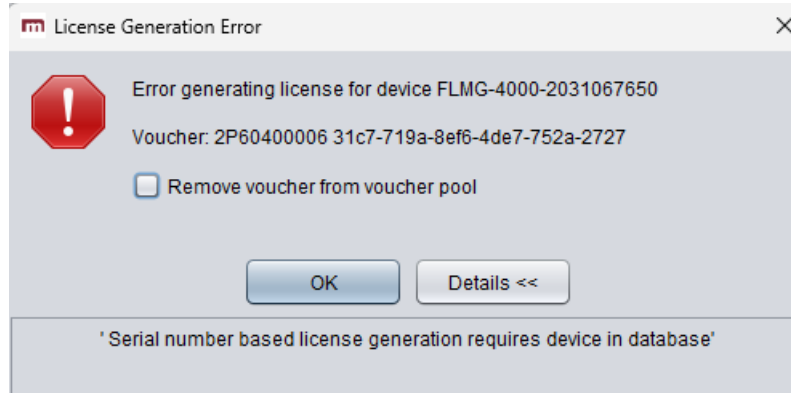
Tools Hardware Snapshot

**Hardware Information**

Property	Value
Uptime	5:08
Load average	0.08, 0.03, 0.04
No. of processes	295
Product	Innominate mGuard VirtualBox
Product code	BD-970010
CPU family	x86_64
CPU stepping	9
CPU clock speed	2807
RAM size	256 MB
User space memory	250048 kB
Factory supplied MAC addresses	4
First MAC address	00:0c:be:09:1d:e0
Serial number	1F711580
Flash ID	U1D6CE28A-CE06-1C3A-8397-000CBE0008C6

### 5.4.5 Incorrect serial number

An mGuard device selected in the MDM contains an incorrect "Serial number" that is not contained in the mGuard device database.



C	U	Management ID	Templates	V	Version	F	Version on device	Accessible via	Upload scheduled at	Serial number
		FLMG-4000-2031067919	Basic		mGuard 8.9	✓	8.9.4.default	172.29.0.226		2031067919
✓	✓	FLMG-4000-2031067983	Basic		mGuard 8.9	✓	8.9.3.default	172.29.0.225		2031067983
✓	✓	FLMG-4005-2032310564	Basic		mGuard 8.9	✓	8.9.4.default	172.29.0.227		2032310564
		FLMG-4000-2031067650	Basic		mGuard 8.9	?	unknown	172.29.0.228		2031067650

Further procedure:

- Correct the incorrect serial number in the MDM.



# 6 Logging / Firewall-Logging



Document-ID: 112008\_en\_00  
 Document-Description: AH EN MGUARD LOGGING  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
 It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

## Contents of this document

This document describes which events are logged in the log entries of mGuard devices and which abbreviations and log prefixes are used.

- 6.1 Introduction ..... 130**
- 6.2 Classification into log categories ..... 130**
- 6.3 Log entry (General) ..... 132**
  - 6.3.1 User login/logout ..... 132
  - 6.3.2 Change user password ..... 134
  - 6.3.3 Change configuration ..... 135
  - 6.3.4 Use configuration profiles (ATV / ECS) ..... 136
  - 6.3.5 Execute action ..... 137
  - 6.3.6 Create firewall user ..... 138
  - 6.3.7 Insert or remove ECS/SD card ..... 139
  - 6.3.8 Perform an update ..... 140
  - 6.3.9 Firewall redundancy ..... 141
  - 6.3.10 Remove / connect network cable ..... 142
  - 6.3.11 DHCP (Server) ..... 143
  - 6.3.12 DHCP (Client) ..... 144
  - 6.3.13 Rebooting the device ..... 145
  - 6.3.14 Uptime (time stamp) ..... 146
- 6.4 Log prefix (Firewall) ..... 147**
  - 6.4.1 Device and routing Firewall ..... 147
  - 6.4.2 Abbreviations ..... 148
  - 6.4.3 Log-Identifier ..... 150
  - 6.4.4 Limitation of access (fw-throttle) ..... 151
  - 6.4.5 Anti-Spoofing (fw-antispoofing) ..... 152
  - 6.4.6 Consistency check (fw-unclean) ..... 153
  - 6.4.7 Connection tracking (fw-invalid) ..... 154
  - 6.4.8 Remote access (fw-ssh-, fw-https-, fw-snmp-, fw-ntp-access) ..... 155
  - 6.4.9 Firewall (fw-incoming, fw-outgoing) ..... 156
  - 6.4.10 DMZ firewall (fw-dmz-incoming, fw-dmz-outgoing) ..... 157
  - 6.4.11 Firewall rule records (fw-ruleset) ..... 158
  - 6.4.12 User firewall (ufw) ..... 159
  - 6.4.13 IP- and Portforwarding (fw-portforwarding) ..... 160
  - 6.4.14 IPsec VPN firewall (fw-vpn-in, fw-vpn-out) ..... 161
  - 6.4.15 OpenVPN firewall, -forwarding (fw-openvpn-in, -out, -openvpn-portfw) ... 162
  - 6.4.16 DoS protection: SYN flood protection (fw-SYN-flood) ..... 163
  - 6.4.17 DoS protection: ICMP flood protection (fw-ICMP-flood) ..... 163
  - 6.4.18 Max. size „ICMP Echo Request packets“ (fw-ICMP-maxlen) ..... 164

## 6.1 Introduction

The mGuard device logs general system statuses, configuration changes and actions performed on or by the device.

This includes actions performed by the mGuard firewall, user logins and logouts and changes to the device configuration.

The log entries are identified by specific designations and log prefixes. This document briefly describes the log entries and the log prefixes. The aim is to facilitate the interpretation of log entries.

## 6.2 Classification into log categories

The log entries used on mGuard devices can be divided into categories to simplify matters. The following table provides an overview of important log categories and describes which events are logged in each case.

Table 6-1 Categories of log entries (examples)

Category	Detail
<b>Common</b>	
User (Login/Logout)	<ul style="list-style-type: none"> <li>- Login/logout (HTTPS / SSH / SNMP):                             <ul style="list-style-type: none"> <li>- Login of users</li> <li>- Login of firewall users</li> <li>- Login error</li> <li>- Manual logout / logout via timeout</li> </ul> </li> </ul>
User administration	<ul style="list-style-type: none"> <li>- Change password</li> <li>- Configure, change or delete user firewall template</li> <li>- Create, change or delete firewall user</li> </ul>
Change configuration / Configuration profiles	<ul style="list-style-type: none"> <li>- Change configuration (including parameters)</li> <li>- Create or delete configuration profile</li> <li>- Upload or download configuration profile</li> <li>- Apply configuration profile</li> <li>- Save configuration to SD card or load/apply from SD card.</li> </ul>
Certificates	<ul style="list-style-type: none"> <li>- Upload or delete certificates</li> </ul>
Hardware changes	<ul style="list-style-type: none"> <li>- Insert or remove SD card</li> <li>- Connect or disconnect network cable</li> </ul>
Connectivity	<ul style="list-style-type: none"> <li>- Network configuration received via DHCP</li> <li>- Network cable removed / connected</li> </ul>
Update	<ul style="list-style-type: none"> <li>- Perform firmware update</li> <li>- Add, change or delete update server</li> </ul>
Remote logging (syslog)	<ul style="list-style-type: none"> <li>- Configure, activate or deactivate remote syslog server connection</li> </ul>
Redundancy	<ul style="list-style-type: none"> <li>- Operate two mGuard devices in firewall redundancy mode</li> </ul>

Table 6-1 [...]Categories of log entries (examples)

Category	Detail
<b>Network Security</b>	
Firewall	<ul style="list-style-type: none"> <li>- Firewall rule applies and is applied (logging must be activated)</li> <li>- Firewall rule set is applied (logging must be activated)</li> <li>- Unknown connection attempt (logging must be activated)</li> <li>- Create, change or delete firewall rule</li> <li>- Configure, change or delete user firewall template</li> <li>- Anti-spoofing measures</li> <li>- DoS protection measures</li> <li>- Measures in the course of consistency checks</li> </ul>
<b>IPsec VPN</b>	
IPsec VPN	<ul style="list-style-type: none"> <li>- IPsec VPN connection is established or terminated</li> <li>- Connection (setup) error</li> </ul>
<b>OpenVPN Client</b>	
OpenVPN	<ul style="list-style-type: none"> <li>- OpenVPN connection is being established or terminated</li> <li>- Connection (setup) error</li> </ul>
<b>DHCP Server/Relay</b>	
DHCP	<ul style="list-style-type: none"> <li>- Network configuration assigned to a network client via DHCP</li> </ul>
<b>SNMP/LLDP</b>	
SNMP	<ul style="list-style-type: none"> <li>- Monitor or manage SNMP device via SNMP</li> </ul>
LDAP	<ul style="list-style-type: none"> <li>- Determine or send information about the network infrastructure via LLDP</li> </ul>
<b>Dynamic Routing</b>	
OSPF	<ul style="list-style-type: none"> <li>- Distribute OSPF routing information via OSPF protocol</li> </ul>

## 6.3 Log entry (General)

### 6.3.1 User login/logout

#### Web based management (web interface)

Log entry	Description
Webinterface action	<p>A user is logged on or off via the WBM. Authentication takes place on the mGuard device directly or via a RADIUS server.</p> <p>Unsuccessful login attempts and automatic logouts are also logged.</p> <p>If the user is logged in and authenticated using the RADIUS server, the user name configured on the RADIUS server appears as the user name.</p> <p>Unsuccessful login attempts and manual logout or logout after a session timeout are also logged.</p> <p>The logon and logoff of firewall users is also logged.</p>

#### Example:

2025-03-06_13:05:32.24439 <b>Webinterface</b> : Accepted login for 'user-bob' role 'admin' from 192.168.1.55 by Web
2025-03-06_13:06:32.24439 <b>Webinterface</b> : Logout for 'user-bob' role 'admin' from 192.168.1.55 by timeout
2025-03-06_13:07:32.24439 <b>Webinterface</b> : Failed login for '*****' role '*****' from 192.168.1.55 by Web
2025-05-05_10:23:19.72490 <b>action</b> : user-fred:admin performed the action 'userfw/login' via Webinterface
2025-05-05_10:23:19.72586 <b>Webinterface</b> : Accepted login for firewall user user-fred' from 192.168.1.55
2025-05-05_10:23:44.91426 <b>action</b> : Technician_Bob:admin performed the action 'userfw/logout' via Webinterface
2025-05-05_10:23:44.91568 <b>Webinterface</b> : Logout for firewall user 'user-fred' from 192.168.1.55

**Shell access (sshd)**

Log entry	Description
sshd	A user is logged on or off via the shell access of the mGuard device.
inno-sshdlimitd	Unsuccessful login attempts and manual logouts or logouts after a session timeout are also logged.

**Example:**

2025-03-06_13:21:03.24439 <b>sshd[28654]</b> : Accepted password for admin from 192.168.1.55 port 53721 ssh2
2025-03-06_13:21:04.00270 <b>inno-sshdlimitd</b> : accepting new connection at fd 6
2025-03-06_13:21:05.00315 <b>inno-sshdlimitd</b> : allow session 1 of maximum 4 for role admin (class 1) at fd 6
2025-03-06_13:21:09.00896 <b>sshd[28659]</b> : session start for user 'admin'
2025-03-06_13:24:10.00896 <b>sshd[28666]</b> : Closing connection for admin from 192.168.1.55 port 53716
2025-03-06_13:24:10.00896 <b>sshd[28766]</b> Failed password for admin from 192.168.1.55 port 53933 ssh2

### 6.3.2 Change user password

Log entry	Description
maid usermod	A user password is changed.

**Example:**

```
2025-05-05_10:03:40.39609 maid[12436]: User 'admin' performed a configuration change with role 'admin':  
2025-05-05_10:03:40.39628 maid[12436]: WWW_PASSWORD_RAW set to '*****'  
2025-05-05_10:03:40.42302 usermod[23853]: change user 'admin' password
```

### 6.3.3 Change configuration

Log entry	Description
maid	<p>A user makes a configuration change. The changed parameters are logged.</p> <p>If the user is logged in and authenticated using the RADIUS server, the user name configured on the RADIUS server appears as the user name.</p>

**Example:**

```
2025-03-06_13:41:43.27927 maid[12341]: User 'admin' performed a configuration
change with role 'admin':
2025-03-06_13:41:43.27947 maid[12341]: NTP_SERVERS new row 0
2025-03-06_13:41:43.27984 maid[12341]: NTP_SERVERS:0.NTP_SERVER set to
'pool.ntp.org'
2025-03-06_13:41:43.27998 maid[12341]: NTP_SERVERS:0.PREFER_VPN set to
'no'
2025-03-06_13:41:43.28073 maid[12341]: NTP_SERVERS new row 1
2025-03-06_13:41:43.28087 maid[12341]: NTP_SERVERS:1.NTP_SERVER set to
'pool.ntp.net'
2025-03-06_13:41:43.28116 maid[12341]: NTP_SERVERS:1.PREFER_VPN set to
'no'
```

### 6.3.4 Use configuration profiles (ATV / ECS)

Log entry	Description
action service-ihald ECS-save	A configuration profile is created, uploaded, downloaded or applied.

#### Example:

##### As ATV profile

2025-05-05\_09:47:08.18954 **action:** admin:admin performed the action 'profile/save' via Webinterface

2025-05-05\_09:47:44.33517 **action:** admin:admin performed the action 'profile/download' via Webinterface

2025-05-05\_09:49:50.58022 **action:** admin:admin performed the action 'profile/upload' via Webinterface

2025-05-05\_09:50:18.32148 **action:** admin:admin performed the action 'profile/restore' via Webinterface

##### On ECS/SD card

###### *Create / Save*

2025-05-05\_12:38:43.92085 **service-ihald:** INFO: Writing the configuration to the external config storage.

2025-05-05\_12:38:47.00398 **syslog:** Generic SD card found.

2025-05-05\_12:38:47.03468 **ECS-save:** saved configuration

2025-05-05\_12:38:47.03918 **service-ihald:** INFO: Finished writing the configuration to the external config storage.

2025-05-05\_12:38:47.06146 **action:** admin:admin performed the action 'ecs/save' via Webinterface

###### *Hochladen / Anwenden*

2025-05-05\_12:42:03.69947 **service-ihald:** INFO: The configuration from the external config storage differs from the device.

2025-05-05\_12:42:03.71027 **ECS-load:** Configuration restored from external config storage.

2025-05-05\_12:42:03.82098 **action:** admin:admin performed the action 'ecs/load' via Webinterface

### 6.3.5 Execute action

Log entry	Description
action	An action is executed by a user with a specific user role (user name:role).  If the user is logged in and authenticated using the RADIUS server, the user name configured on the RADIUS server appears as the user name.

**Example:**

2025-03-06_13:44:29.56656 <b>action:</b> admin:admin performed the action 'tools/snapshot' via Webinterface
2025-03-06_13:45:09.97690 <b>action:</b> admin:admin performed the action 'tools/tcp-dump-start' via Webinterface
2025-05-05_10:26:34.81534 <b>action:</b> admin:admin performed the action 'update/patches' via Webinterface

### 6.3.6 Create firewall user

Log entry	Description
maid	A firewall user is configured or an already configured firewall user is changed or adapted.

#### Example:

```

2025-05-05_10:14:55.23385 maid[12435]: User 'admin' performed a configuration
change with role 'admin':
2025-05-05_10:14:55.23403 maid[12435]: USERFW_TEMPLATE new row 0
2025-05-05_10:14:55.23420 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_COMMENT set to ''
2025-05-05_10:14:55.23436 maid[12435]: USERFW_TEMPLATE:0.TEMPLATE_EN-
ABLED set to 'yes'
2025-05-05_10:14:55.23453 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_NAME set to 'Firewall-User-01'
2025-05-05_10:14:55.23467 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_RULE:0.COMMENT set to ''
2025-05-05_10:14:55.23483 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_RULE:0.DST_IP set to '0.0.0.0/0'
2025-05-05_10:14:55.23496 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_RULE:0.DST_PORT set to 'any'
2025-05-05_10:14:55.23512 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_RULE:0.LOG set to 'no'
2025-05-05_10:14:55.23526 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_RULE:0.PROTO set to 'all'
2025-05-05_10:14:55.23539 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_RULE:0.SRC_PORT set to 'any'
2025-05-05_10:14:55.23556 maid[12435]: USERFW_TEMPLATE:0.TEMPLATE_S-
SRC_IP set to '%authorized_ip'
2025-05-05_10:14:55.23570 maid[12435]: USERFW_TEMPLATE:0.TEMPLATE_TIM-
EOUT set to '28800'
2025-05-05_10:14:55.23651 maid[12435]: USERFW_TEMPLATE:0.TEM-
PLATE_TOUT_TYPE set to 'static'
2025-05-05_10:14:55.23667 maid[12435]: USERFW_TEMPLATE:0.TEMPLATE_US-
ERS:0.USERNAME set to 'Technician_01'
2025-05-05_10:14:55.23686 maid[12435]: USERFW_TEMPLATE:0.VPN_CONN_REF
set to ''

```

### 6.3.7 Insert or remove ECS/SD card

Log entry	Description
kernel service-ihald	An SD card is inserted or removed from the device.

#### Example:

2025-05-05_09:45:59.26220 <b>kernel:</b> [ 245.191375] mmc0: new high speed SDHC card at address 59b4
2025-05-05_09:45:59.26578 <b>kernel:</b> [ 245.193484] mmcblk0: mmc0:59b4 SDC 7.51 GiB
2025-05-05_09:45:59.26631 <b>kernel:</b> [ 245.195280] mmcblk0: p1
2025-05-05_09:46:00.71116 <b>service-ihald:</b> INFO: An external config storage medium was inserted.
2025-05-05_09:43:51.42165 <b>kernel:</b> [ 117.347900] mmc0: card 59b4 removed

### 6.3.8 Perform an update

Log entry	Description
action psm-sanitize	An update or attempt to update the firmware is carried out. Any errors that occur are also logged.

**Example:**

```
2025-05-14_07:09:14.96415 action: admin:admin performed the action 'update/major' via Webinterface
2025-05-14_07:09:15.03413 psm-sanitize: psm-sanitize: info: all packages installed completely.
2025-05-14_07:09:15.04755 psm-sanitize: psm-sanitize: info: installing new package set "10.6.0-pre19-beta06.default"...
2025-05-14_07:09:15.63286 psm-sanitize: psm-wget: download failed for URL https://***@update.innominat.com//aarch64/major/10.6.0.default: HTTP/1.1 404 Not Found
2025-05-14_07:09:15.64362 psm-sanitize: psm-install: fatal: download of package set "10.6.0.default" failed (107)
2025-05-14_07:09:15.65645 psm-sanitize: psm-sanitize: info: psm-install 10.6.0.default failed: 107
2025-05-14_07:09:15.66465 psm-sanitize: psm-sanitize: info: done.
2025-05-14_07:09:15.66947 psm-sanitize: psm-sanitize: info: running psm-clean...
2025-05-14_07:09:17.98191 psm-sanitize: psm-clean: info: done.
```

### 6.3.9 Firewall redundancy

Log entry	Description
ham-ssv / ham-vic ham-av-... contrackd pluto	An event occurs when two mGuard devices are used as a redundancy pair - with firewall redundancy activated (e.g. switching from one device of the redundancy pair to the other if the previously active device lacks connectivity).

#### Example:

```
[ ...]
2025-05-14_08:03:49.48428 ham-ssv: INFO transitioned from outdated to on_
standby because availability is failed totally, connectivity is successful, replication is
not unknown (outdated)
2025-05-14_08:03:49.48871 ham-ssv: INFO transitioned from on_standby to be-
comes_active because availability is failed totally, connectivity is not unknown (suc-
cessful), replication is not unknown (outdated)
2025-05-14_08:03:49.49177 ham-vic: INFO enabled IP forwarding and other condi-
tions
2025-05-14_08:03:49.49193 ham-ac-int: AC INFO ham-ac(5703,eth1) sending CARP
messages and listening to them
2025-05-14_08:03:49.49207 ham-ac-ext1: AC INFO ham-ac(5723,eth0) sending
CARP messages and listening to them
2025-05-14_08:03:49.50734 contrackd: [Wed May 14 08:03:49 2025] (pid=32161)
[notice] committing all external caches
2025-05-14_08:03:49.51356 contrackd: [Wed May 14 08:03:49 2025] (pid=32161)
[notice] Committed 115 new entries
2025-05-14_08:03:49.51376 contrackd: [Wed May 14 08:03:49 2025] (pid=32161)
[notice] commit has taken 0.006242 seconds
2025-05-14_08:03:49.52332 contrackd: [Wed May 14 08:03:49 2025] (pid=32161)
[notice] flushing caches
2025-05-14_08:03:49.53259 contrackd: [Wed May 14 08:03:49 2025] (pid=32161)
[notice] resync with master contrack table
2025-05-14_08:03:49.54625 contrackd: [Wed May 14 08:03:49 2025] (pid=32161)
[notice] sending bulk update
2025-05-14_08:03:49.84886 ham-ssv: INFO sigalrm (timeout)
2025-05-14_08:03:49.84905 ham-ssv: INFO transitioned from becomes_active to
active because replication is not 'received final' (outdated), timeout
2025-05-14_08:03:49.85119 ham-vic: INFO enabled virtual interface eth1.vif
2025-05-14_08:03:49.85238 pluto: pluto[21806]: HA: switching to 'active'
2025-05-14_08:03:49.85242 pluto: pluto[21806]: HA: I am active now
2025-05-14_08:03:49.87510 ham-vic: INFO Kernel Proxy ARP enabled
[ ...]
```

### 6.3.10 Remove / connect network cable

Log entry	Description
kernel service mauman	A network cable is removed from or connected to the device.

#### Example:

```
2025-06-10_09:50:19.27287 kernel: [ 5330.215135] mvneta d0030000.ethernet  
eth0: Link is Down  
2025-06-10_09:50:19.37295 service-mauman: [011] Running service loop because  
an interface changed  
2025-06-10_09:50:23.36572 kernel: [ 5334.308092] mvneta d0030000.ethernet  
eth0: Link is Up - 1Gbps/Full - flow control off  
2025-06-10_09:50:23.46578 service-mauman: [011] Running service loop because  
an interface changed
```

### 6.3.11 DHCP (Server)

Log entry	Description
dhcp-int dhcp-ext	A network configuration is assigned to a network client by the mGuard DHCP server via DHCP.

**Example:**

```
2025-06-11_09:19:06.72032 dhcp-int: udhcpd: started, v1.36.1
2025-06-11_09:19:14.35471 dhcp-int: udhcpd: sending OFFER to 192.168.100.223
2025-06-11_09:19:14.37093 dhcp-int: udhcpd: sending ACK to 192.168.100.223
```

### 6.3.12 DHCP (Client)

Log entry	Description
dhclient	The network configuration is requested from a DHCP server and received from it.

#### Example:

```
2025-06-11_09:00:41.65347 dhclient: udhcpc: Recieved a link-up event, exiting
2025-06-11_09:00:41.65351 dhclient:
2025-06-11_09:00:41.65953 dhclient: udhcpc: started, v1.36.1
2025-06-11_09:00:41.65957 dhclient: udhcpc: Will send DHCP requests.
2025-06-11_09:00:41.68587 dhclient: trigger: 'ifchange ext1'
2025-06-11_09:00:41.70078 dhclient: udhcpc: broadcasting discover
2025-06-11_09:00:41.75383 service-mauman: [011] Running service loop because
an interface changed
2025-06-11_09:00:41.81462 dhclient: udhcpc: broadcasting select for
192.168.178.38, server 192.168.100.1
2025-06-11_09:00:41.86462 dhclient: udhcpc: lease of 192.168.100.38 obtained
from 192.168.100.1, lease time 864000
2025-06-11_09:00:41.90523 dhclient: trigger: 'ifchange ext1'
```

### 6.3.13 Rebooting the device

Log entry	Description
ham-ssv	The device is restarted by a user or due to an error.  The complete log entries for this event can only be analyzed on the syslog server, as the events on the device are deleted after a re-start.

#### Example:

```
2025-06-11T15:21:52.145364+02:00 192.168.1.1 2025-06-11_15: 21:23.92907
<13>Jun 11 15:21:23 ham-ssv: INFO sigterm (request to terminate)
2025-06-11T15:21:52.145364+02:00 192.168.1.1 2025-06-11_15: 21:23.92959
<13>Jun 11 15:21:23 ham-ssv: INFO terminating
2025-06-11T15:21:52.146846+02:00 192.168.1.1 2025-06-11_15: 21:23.92997
<13>Jun 11 15:21:23 ham-ssv: INFO terminated
[...]
```

### 6.3.14 Uptime (time stamp)

To check on an external syslog server, for example, whether the transfer of log entries is taking place as desired and whether log entries are being transferred regularly, a log entry with the prefix "uptime-audit" is created approximately every 30 minutes and sent to the syslog server. The log entry shows the current time that has passed since the system start of the mGuard device (uptime).

Log entry	Description
uptime-audit	Automatic time stamp to check the logging function of the device.

**Example:**

2025-03-22_06:17:45.26984	<b>uptime-audit:</b> ----- UPTIME: 1 day, 23:51 -----
2025-03-22_06:46:45.27963	<b>uptime-audit:</b> ----- UPTIME: 2 days, 20 min -----
2025-03-23_09:50:45.81252	<b>uptime-audit:</b> ----- UPTIME: 3 days, 3:24 -----

## 6.4 Log prefix (Firewall)

### 6.4.1 Device and routing Firewall

Packets that are directed to the mGuard device or must pass through the firewall are checked in the following order:

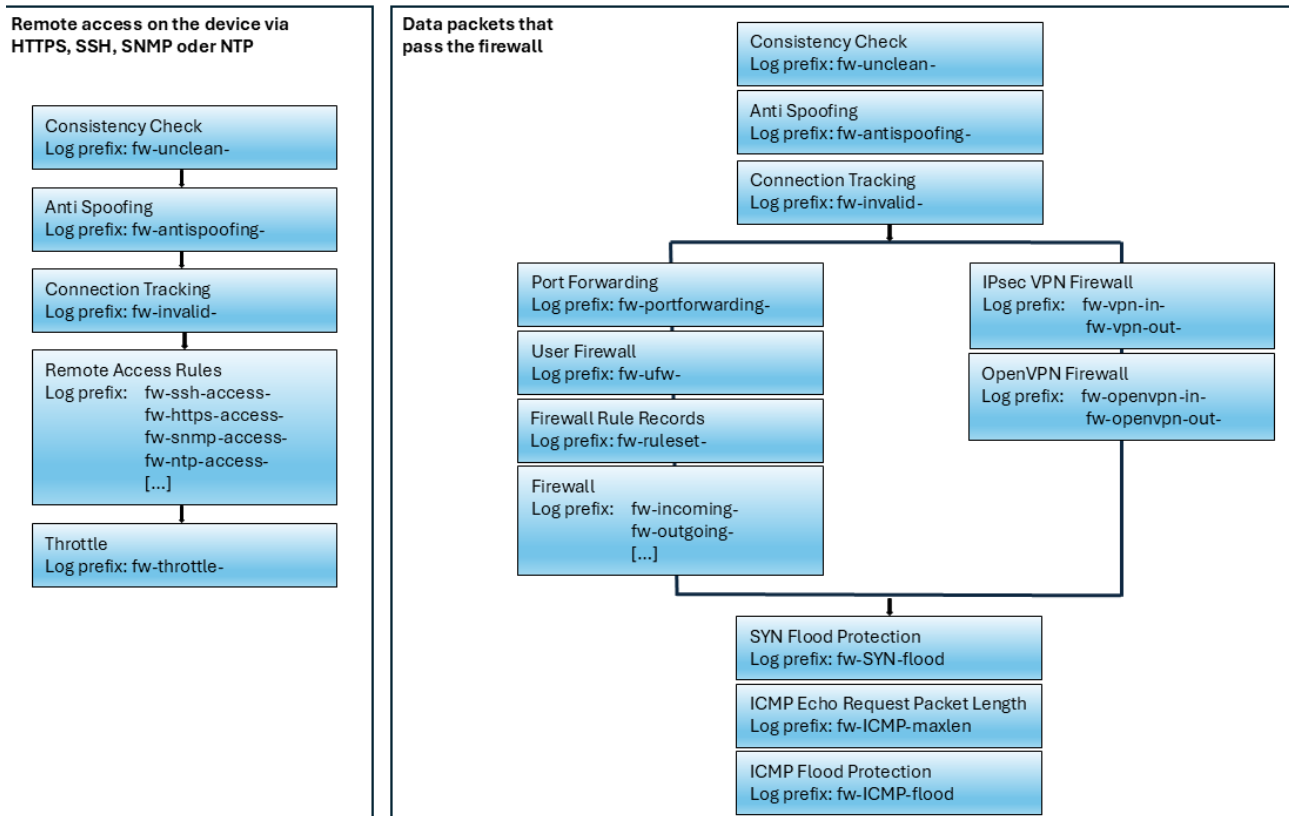


Figure 6-1 Packet inspection of packets that pass through a firewall  
Further details on package control are described in the following chapters.

## 6.4.2 Abbreviations

Table 6-2 Abbreviations used in log entries

Abbreviation	Description
IN (Router mode) PHYSIN (Stealth mode)	Incoming interface eth0: external interface / br0 (Stealth mode) eth1: internal interface / br0 (Stealth mode) tun(x): Interface for each active OpenVPN connection
OUT (Router mode) PHYSOUT (Stealth mode)	Outgoing interface eth0: external interface / br0 (Stealth mode) eth1: internal interface / br0 (Stealth mode) tun(x): Interface for each active OpenVPN connection
MAC	This information is always displayed, regardless of the protocol, if the MAC address of the remote station is known.
act	Action performed for package: DROP, REJECT or ACCEPT
SRC	Source IP address
DST	Destination IP address
LEN	Total length of the IP packet in bytes
TOS	Type of services , Field <i>Type</i>
PREC	Type of services , Field <i>Precedence</i>
TTL	Remaining lifetime (time to live) in hops
ID	Unique ID of the IP datagram, which is shared by all fragments if they are fragmented.
DF	Flag " <i>Don't fragment</i> " is active.
CE	Flag " <i>Reserved fragment</i> "
MF	Flag " <i>More fragments</i> " (reference to further following fragments of the same package)
PROTO	Name or number of the protocol (e.g. ARP or TCP, ICMP)
SPT	Source port (TCP and UDP)
DPT	Destination port (TCP and UDP)
WINDOW	The size of the <i>TCP Receive Window</i> . (Only for TCP)
[FLAGS]	If the TCP protocol is used, the TCP flags (e.g. SYN) are also displayed.
URG	URG = Urgent flag
ACK	ACK = Acknowledgement flag
PSH	PSH = Push flag
RST	RST = Reset flag
SYN	SYN = SYN flag (wird nur beim Aufbau von TCP-Verbindungen ausgetauscht)
FIN	FIN = FIN flag (wird nur bei der Trennung von TCP-Verbindungen ausgetauscht)
CWR	CWR = Peer has reduced "congestion window" (WINDOW)
ECE	ECE = Peer supports "explicit congestion notification" in the event of overload
SPI	Used SPI (only for ESP protocol)
URGP	The <i>Urgent Pointer</i> enables urgent data transmissions of the " <i>out of band</i> " type.
MARK	An internally used marker on the data packet.

Table 6-2 Abbreviations used in log entries

CTMARK	An internally used marker on the connection tracking entry belonging to the data packet.
SEQ	ID of the packet for ICMP Echo and Echo Reply (Ping)
CODE	ICMP code (only ICMP)
TYPE	ICMP type (only ICMP)
ROWID1 / ROWID2	IDs of the associated IPsec connection and the associated IPsec tunnel (if the packet goes into an IPsec tunnel or came out of one).
GATEWAY	Suggested gateway for ICMP " <i>Redirect</i> ".
MTU	Suggested MTU for ICMP " <i>Fragmentation Needed</i> ".
REQUEST	Request (ARP only)
REPLY	Response (ARP only)
NAK	<i>Negative acknowledgement</i> - The request could not be processed successfully (ARP only).
REPLY_MAC	Resolved MAC address (ARP only)
CODE	Other " <i>operation code</i> " for ARP, if it is neither REQUEST, nor REPLY, nor NAK. For example with reverse ARP.

### 6.4.3 Log-Identifier

Example of a firewall log entry:

```
2025-03-21_09:02:08.11705 firewall: fw-incoming-2-3189b8c7-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:15:17:20:df:7d SRC=10.1.80.200 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=26695 DF PROTO=TCP SPT=23695 DPT=5201 SEQ=107412944 ACK=0 WINDOW=65535 SYN URGP=0
```

Each log entry begins with the time stamp and the log identifier.

**Time stamp (Example):**

2025-03-08\_17:25:22.07497

**Log Identifier (Example):**

The Log Identifier consists of the following elements in the following format:

**<Log prefix>-<Rule number>-<Log ID>**

Example: **fw-incoming-1-3189b8c7-8002-1315-805d-a8741dfd1b11**

Log prefix	The log prefix indicates in which area or at which step an action took place during the analysis of the data traffic by the firewall.
Rule number	The rule number indicates which configured firewall rule caused the log entry. <Rule number> = 0 means that the log entry was caused by a standard firewall rule.
Log ID	Each type of configured firewall (e.g. incoming rules, outgoing rules, SSH or HTTPS remote access) has its own unique log ID.

The log identifier can be used in the "Logging>> View logs" menu to find the firewall rule that caused the log entry.



The time zone configured in the "Administration >> System settings >> Time and date" menu only affects the time stamps displayed in the web interface. If you use remote logging, the time stamp is displayed in UTC format on the remote syslog server. This makes it easier to compare the log entries if you are using a central syslog server to record and analyze the log entries of various devices located in different time zones.

#### 6.4.4 Limitation of access (fw-throttle)

This check is carried out for all packets that are received via the external interface.

Log prefix	Description
fw-throttle	The firewall limits the permitted connections for remote access to the mGuard device. The permitted number varies for different protocols. If the permitted number of connections is exceeded, new connections are rejected and the packets are discarded.

### 6.4.5 Anti-Spoofing (fw-antispoofing)

This check is carried out for all packets that are received via the external or DMZ interface. Packets are rejected and dropped if their sender IP address belongs to the network of an interface other than the one on which they were received.

(For example, if packets are received on the external interface whose sender IP is in the internal network).

The log prefix **fw-antispoofing-** is followed by the extensions *ext1* and *dmz* if the packet was received via the WAN or DMZ interface (*ext1*, *dmz*).

Log prefix	Description
fw-antispoofing	Packets are rejected and dropped if their sender IP address belongs to the network of an interface other than the one on which they were received.  (For example, if packets are received on the external interface whose sender IP is in the internal network).

#### Example:

```
2025-03-21_10:13:42.19680 firewall: fw-antispoofing-ext1-0- act=DROP IN=eth0  
MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=255.255.255.255 LEN=59  
TOS=0x00 PREC=0x00 TTL=128 ID=56636 PROTO=UDP SPT=1004 DPT=1003  
LEN=39 CTMARK=100000
```

### 6.4.6 Consistency check (fw-unclean)

The firewall performs a consistency check if the "Enable TCP/UDP/ICMP consistency checks" option is activated in the "Network security >> Packet filter>> Advanced" menu.

The consistency check is carried out for the IP headers of all IP packets. For the TCP, UDP and ICMP protocols, the headers of the respective protocol are also checked for invalid values (e.g. invalid checksum, ports or TCP flags).

Log prefix	Description
fw-unclean-input	Packet that was sent directly to an interface of the mGuard.
fw-unclean-output	Packet generated by the mGuard. This log prefix should not actually occur, but is included for the sake of completeness.
fw-unclean-forward	Packet that would pass through the firewall (routing).

#### Example:

```
2024-03-31_09:01:18.80548 firewall: fw-unclean-input-0- act=DROP IN=eth0
OUT= MAC=00:0c:be:02:20:27:00:13:20:48:d4:e6:08:00 SRC=10.1.0.64
DST=10.1.80.100 LEN=40 TOS=0x00 PREC=0x00 TTL=128 ID=1364 PROTO=TCP
SPT=1234 DPT=0 SEQ=0 ACK=0 WINDOW=1500 RES=0x00 SYN URGP=0
```

```
2025-03-21_08:41:17.97343 firewall: fw-unclean-forward-0- act=DROP IN=eth1
OUT=eth0 MAC=08:00:27:11:1e:6a SRC=192.168.1.100 DST=10.1.80.200 LEN=48
TOS=0x00 PREC=0x00 TTL=63 ID=292 PROTO=TCP SPT=40008 DPT=80
SEQ=811466752 ACK=0 WINDOW=512 SYN URGP=0
```

### 6.4.7 Connection tracking (fw-invalid)

*Connection tracking* is carried out for all packets.

fw-invalid occurs when the firewall discards a network packet for which no suitable connection is entered in the *connection tracking* table of the mGuard device. This means that the packet cannot be related to an existing connection.

In addition, the packet does not create a new entry in the *connection tracking* table, as the connection is blocked or dropped by a firewall rule.

If the packet belongs to an existing connection, TCP packets are also checked to see whether the set TCP flags meet expectations and whether the sequence number is within the currently accepted window. If one of these checks fails, the packet is discarded and an entry with the prefix *fw-invalid* is generated.

Log prefix	Description
fw-invalid-input	Packet that was sent directly to an interface of the mGuard device.
fw-invalid-output	Packet generated by the mGuard device. This log prefix should not actually occur, but is included for the sake of completeness.
fw-invalid-forward	Packet that would pass through the firewall.

#### Example:

```
2025-03-21_08:04:40.08134 firewall: fw-invalid-input-0- act=DROP IN=eth0
MAC=00:0c:be:04:00:58 SRC=10.1.80.123 DST=10.1.80.100 LEN=40 TOS=0x00
PREC=0x00 TTL=127 ID=54116 DF PROTO=TCP SPT=37645 DPT=5201
SEQ=3746596578 ACK=16777216 WINDOW=0 ACK RST URGP=0
```

```
2025-03-21_08:22:49.49289 firewall: fw-invalid-output-0- act=DROP OUT=eth0
MAC= SRC=10.1.80.100 DST=10.1.80.200 LEN=104 TOS=0x08 PREC=0x40 TTL=64
ID=54569 DF PROTO=TCP SPT=22 DPT=22841 SEQ=1343772416 ACK=16777216
WINDOW=501 ACK PSH URGP=0 UID=0 GID=0 MARK=800
```

```
2025-03-21_08:06:12.08142 firewall: fw-invalid-forward-0- act=DROP IN=eth1
OUT=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.123 LEN=40
TOS=0x00 PREC=0x00 TTL=127 ID=466 DF PROTO=TCP SPT=5201 DPT=37645
SEQ=584616543 ACK=16777216 WINDOW=53217 ACK FIN URGP=0
```

### 6.4.8 Remote access (fw-ssh-, fw-https-, fw-snmp-, fw-ntp-access)

Log entries with the prefixes **fw-ssh-**, **fw-https-**, **fw-snmp-** and **fw-ntp-access** are caused by remote access rules for SSH, HTTPS, SNMP and NTP access from the external network (if "Logging" has been enabled):

- **SSH remote access:** Menu "Administration>> System Settings>> Shell Access"
- **HTTPS remote access:** Menu "Administration>> Web Settings>> Access"
- **SNMP remote access:** Menu "Administration>> SNMP>> Query"
- **NTP remote access:** Menu "Administration>> System Settings>> Time and Date"

Log prefix	Description
fw-ssh-access	A remote access rule (shell access / SSH) applies to an incoming SSH connection that terminates on the device.
fw-https-access	A remote access rule (web access / HTTPS) applies to an incoming HTTPS connection that terminates on the device.
fw-snmp-access	A remote access rule (SNMP access / SNMP) applies to an incoming SNMP connection that terminates on the device.
fw-ntp-access	A remote access rule (NTP access / NTP) applies to an incoming NTP connection that terminates on the device.

#### Example:

```
2025-03-13_11:03:03.62955 firewall: fw-ssh-access-1-1dd08637-31d0-1f7f-b283-000cbe000d32 act=REJECT IN=eth0 MAC=d4:d8:53:b2:6d:62
SRC=192.168.178.32 DST=192.168.178.128 LEN=52 TOS=0x00 PREC=0x00
TTL=128 ID=60064 DF PROTO=TCP SPT=55219 DPT=22 SEQ=1601988361 ACK=0
WINDOW=65535 SYN URGP=0 CTMARK=100030
```

```
2025-03-13_11:04:38.28569 firewall: fw-https-access-1-1dd0864d-31d0-1f7f-b283-000cbe000d32 act=ACCEPT IN=eth0 MAC=d4:d8:53:b2:6d:62
SRC=192.168.178.32 DST=192.168.178.128 LEN=52 TOS=0x00 PREC=0x00
TTL=128 ID=60722 DF PROTO=TCP SPT=65104 DPT=443 SEQ=2949231819 ACK=0
WINDOW=65535 SYN URGP=0 CTMARK=100030
```

```
2025-03-13_10:57:21.38954 firewall: fw-ntp-access-1-1dd08618-31d0-1f7f-b283-000cbe000d32 act=DROP IN=eth0 MAC=00:0c:be:00:10:fc
SRC=192.168.178.40 DST=192.168.178.128 LEN=76 TOS=0x18 PREC=0xA0 TTL=64
ID=20909 DF PROTO=UDP SPT=123 DPT=123 LEN=56 CTMARK=100030
```

### 6.4.9 Firewall (fw-incoming, fw-outgoing)

Log entries with the prefixes **fw-incoming** and **fw-outgoing** are caused by configured incoming and outgoing firewall rules (if "Logging" has been enabled).

- **Incoming rules:** Menu "Network Security>> Packet Filter>> Inbound Rules"
- **Outgoing rules:** Menu "Network Security>> Packet Filter>> Outgoing Rules"

Log prefix	Description
fw-incoming	An incoming rule applies to a connection that is established from external to internal (WAN --> LAN).
fw-outgoing	An outgoing rule applies to a connection that is established from internal to external (LAN --> WAN).

#### Example:

```
2025-03-21_09:01:46.32490 firewall: fw-incoming-1-3189b8c7-8002-1315-805d-
a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:15:17:20:df:7d
SRC=10.1.80.200 DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127
ID=26694 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=390
```

```
2025-03-21_09:02:08.11705 firewall: fw-incoming-2-3189b8c7-8002-1315-805d-
a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:15:17:20:df:7d
SRC=10.1.80.200 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127
ID=26695 DF PROTO=TCP SPT=23695 DPT=5201 SEQ=107412944 ACK=0 WIN-
DOW=65535 SYN URGP=0
```

```
2025-03-21_08:59:32.91681 firewall: fw-outgoing-1-3189b8c8-8002-1315-805d-
a8741dfd1b11 act=ACCEPT IN=eth1 OUT=eth0 MAC=08:00:27:11:1e:62
SRC=192.168.1.100 DST=10.1.80.200 LEN=60 TOS=0x00 PREC=0x00 TTL=127
ID=29288 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=39
```

```
2025-03-21_09:00:04.37373 firewall: fw-outgoing-2-3189b8c8-8002-1315-805d-
a8741dfd1b11 act=ACCEPT IN=eth1 OUT=eth0 MAC=08:00:27:11:1e:62
SRC=192.168.1.100 DST=10.1.80.200 LEN=52 TOS=0x00 PREC=0x00 TTL=127
ID=29291 DF PROTO=TCP SPT=51582 DPT=5201 SEQ=1243586400 ACK=0 WIN-
DOW=65535 SYN URGP=0
```

### 6.4.10 DMZ firewall (fw-dmz-incoming, fw-dmz-outgoing)

Log entries with the prefixes **fw-dmz-incoming-lan** and **fw-dmz-outgoing-lan** as well as **fw-dmzincoming-wan** and **fw-dmz-outgoing-wan** are caused by configured incoming and outgoing DMZ firewall rules (if "Logging" has been enabled)).

- **DMZ rules:** Menu "Network Security >> Packet Filter>> DMZ"

Log prefix	Description
fw-dmz-incoming-wan	A firewall rule applies to a connection (WAN --> DMZ).
fw-dmz-outgoing-wan	A firewall rule applies to a connection (DMZ --> WAN).
fw-dmz-incoming-lan	A firewall rule applies to a connection (LAN --> DMZ).
fw-dmz-outgoing-lan	A firewall rule applies to a connection (DMZ --> LAN).

#### Example:

```
2025-03-25_13:24:35.44775 firewall: fw-dmz-incoming-wan-1-38db7ed8-85b6-1760-a630-000cbe00105c act=ACCEPT IN=eth0 OUT=dmz0
MAC=d4:d8:53:b2:6d:62 SRC=192.168.100.32 DST=192.168.3.128 LEN=60
TOS=0x00 PREC=0x00 TTL=127 ID=29021 PROTO=ICMP TYPE=8 CODE=0 ID=1
SEQ=15028
```

```
2025-03-25_13:27:08.21530 firewall: fw-dmz-outgoing-wan-1-38db7eda-85b6-1760-a630-000cbe00105c act=ACCEPT IN=dmz0 OUT=eth0
MAC=00:0c:be:00:0d:32 SRC=192.168.3.128 DST=192.168.100.1 LEN=84
TOS=0x00 PREC=0x00 TTL=63 ID=27183 DF PROTO=ICMP TYPE=8 CODE=0
ID=17879 SEQ=4
```

```
2025-03-25_13:45:16.95125 firewall: fw-dmz-outgoing-lan-1-38db7edb-85b6-1760-a630-000cbe00105c act=ACCEPT IN=eth1 OUT=dmz0 PHYSIN=swp0
MAC=d4:d8:53:b2:6d:62 SRC=192.168.100.32 DST=192.168.3.128 LEN=60
TOS=0x00 PREC=0x00 TTL=127 ID=30850 PROTO=ICMP TYPE=8 CODE=0 ID=1
SEQ=16278
```

```
2025-03-25_13:46:39.31935 firewall: fw-dmz-outgoing-lan-1-38db7edb-85b6-1760-a630-000cbe00105c act=ACCEPT IN=eth1 OUT=dmz0 PHYSIN=swp0
MAC=d4:d8:53:b2:6d:62 SRC=192.168.100.32 DST=192.168.3.128 LEN=60
TOS=0x00 PREC=0x00 TTL=127 ID=30980 PROTO=ICMP TYPE=8 CODE=0 ID=1
SEQ=16366
```

### 6.4.11 Firewall rule records (fw-ruleset)

Log entries with the prefixes **fw-ruleset** are caused by configured firewall rules that have been defined in firewall rule records (if logging has been enabled in the corresponding incoming/outgoing firewall rule).

- **Rule records:** Menu "Network Security>> Packet Filter>> Rule Records"

Log prefix	Description
fw-ruleset	A rule that is defined in an active and corresponding firewall rule record applies to a connection.

#### Example:

```
2025-03-25_10:50:50.60941 firewall: fw-ruleset_MAIv167032083-1-108ee44b-c0c7-19cd-8938-000cbe00105c act=DROP IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=swp0 MAC=d4:d8:53:b2:6d:62 SRC=192.168.1.32 DST=192.168.1.128 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=9188 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=10364 MARK=c
2025-05-09_10:55:53.90349 firewall: fw-ruleset_MAIv226940804-1-1c55a7b6-c861-1037-a74f-000cbe00105c act=ACCEPT IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=swp0 MAC=bc:e9:2f:c3:60:06 SRC=192.168.1.37 DST=192.168.1.255 LEN=241 TOS=0x00 PREC=0x00 TTL=64 ID=25467 DF PROTO=UDP SPT=138 DPT=138 LEN=221 MARK=10000 CTMARK=100000
```

### 6.4.12 User firewall (ufw)

Log entries with the prefix **ufw** are caused by a configured user firewall (if "Logging" has been enabled).

Log prefix	Description
ufw	A user firewall rule applies to a connection.

#### Example:

```
2025-03-21_09:41:59.15695 firewall: fw-ufw_MAIv390774000-1-3189b901-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1
MAC=00:15:17:20:df:7d SRC=10.1.80.200 DST=192.168.1.100 LEN=60 TOS=0x00
PREC=0x00 TTL=127 ID=63856 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=398
MARK=10000

2025-03-21_09:42:36.18082 firewall: fw-ufw_MAIv390774000-1-3189b901-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1
MAC=00:15:17:20:df:7d SRC=10.1.80.200 DST=192.168.1.100 LEN=52 TOS=0x00
PREC=0x00 TTL=127 ID=63857 DF PROTO=TCP SPT=24482 DPT=5201
SEQ=1915233667 ACK=0 WINDOW=65535 SYN URGP=0 MARK=10000
```

### 6.4.13 IP- and Portforwarding (fw-portforwarding)

Log entries with the prefix **fw-portforwarding** are caused by configured IP and port forwarding rules (menu "Network >> NAT >> IP and Port Forwarding") (if "Logging" has been enabled).

Log prefix	Description
fw-portforwarding	An IP and port forwarding rule applies to a connection.

**Example:**

```
2025-03-21_08:00:29.71358 firewall: fw-portforwarding-1-3189b80a-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1 MAC=00:0c:be:04:00:58 SRC=10.1.80.123 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=126 ID=2146 DF PROTO=TCP SPT=37646 DPT=5201 SEQ=1731043981 ACK=0 WINDOW=65535 SYN URGP=0 CTMARK=1010
```

### 6.4.14 IPsec VPN firewall (fw-vpn-in, fw-vpn-out)

Log entries with the prefixes **fw-vpn-in** and **fw-vpn-out** are caused by configured incoming and/or outgoing VPN firewall rules (if "Logging" has been enabled).

Log prefix	Description
fw-vpn-in	An incoming rule applies to a connection established by the remote peer through the IPsec VPN tunnel.
fw-vpn-out	An outgoing rule applies to a locally established connection to the remote peer through the IPsec VPN tunnel.

#### Example:

```
2025-03-21_07:21:31.98537 firewall: fw-vpn-in_MAIv711498711-1-3189b7d8-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1
MAC=00:0c:be:04:00:58 SRC=192.168.27.100 DST=192.168.1.100 LEN=60
TOS=0x00 PREC=0x00 TTL=126 ID=239 PROTO=ICMP TYPE=8 CODE=0 ID=1
SEQ=376 CTMARK=800 ROWID1=MAIv711498711 ROWID2=MAIv144871511
```

```
2025-03-21_07:24:22.48150 firewall: fw-vpn-in_MAIv711498711-1-3189b7d8-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth0 OUT=eth1
MAC=00:0c:be:04:00:58 SRC=192.168.27.100 DST=192.168.1.100 LEN=52
TOS=0x00 PREC=0x00 TTL=126 ID=248 DF PROTO=TCP SPT=20703 DPT=5201
SEQ=1396473492 ACK=0 WINDOW=65535 SYN URGP=0 CTMARK=800 ROW-
ID1=MAIv711498711 ROWID2=MAIv144871511
```

```
2025-03-21_07:15:10.03337 firewall: fw-vpn-out_MAIv711498711-1-3189b7d9-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=eth0
MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=192.168.27.100 LEN=60
TOS=0x00 PREC=0x00 TTL=127 ID=6650 PROTO=ICMP TYPE=8 CODE=0 ID=1
SEQ=12 ROWID1=MAIv711498711 ROWID2=MAIv144871511
```

```
2025-03-21_07:15:49.55344 firewall: fw-vpn-out_MAIv711498711-1-3189b7d9-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=eth0
MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=192.168.27.100 LEN=52
TOS=0x00 PREC=0x00 TTL=127 ID=6654 DF PROTO=TCP SPT=51029 DPT=5201
SEQ=1008731145 ACK=0 WINDOW=65535 SYN URGP=0 ROWID1=MAIv711498711
ROWID2=MAIv144871511
```

### 6.4.15 OpenVPN firewall, -forwarding (fw-openvpn-in, -out, -openvpn-portfw)

Log entries with the prefixes **fw-openvpn-in** and **fw-openvpn-out** are caused by configured incoming and/or outgoing OpenVPN firewall rules (menu "OpenVPN Client >> Connections ((EDIT)) >> Firewall) (if "Logging" has been enabled).

Log entries with the prefixes **fw-openvpn-portfw** are caused by configured OpenVPN NAT rules (menu "IPsec VPN >> Connections ((EDIT)) >> NAT) (if "Logging" has been enabled).

Log prefix	Description
fw-openvpn-in	An incoming rule for the OpenVPN connection applies to an inbound connection.
fw-openvpn-out	An outgoing rule for the OpenVPN connection applies to an outgoing connection.
fw-openvpn-portfw	A port forwarding rule applies to a connection through the OpenVPN tunnel.

**Example:**

```

2025-03-21_07:02:39.24936 firewall: fw-openvpn-in_MAIv231480925-1-3189b7a5-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=tun0 OUT=eth1 MAC=SRC=11.8.0.1 DST=192.168.1.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=6909 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=361

2025-03-21_07:03:23.40939 firewall: fw-openvpn-in_MAIv231480925-1-3189b7a5-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=tun0 OUT=eth1 MAC=SRC=11.8.0.1 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=6913 DF PROTO=TCP SPT=20025 DPT=5201 SEQ=910850867 ACK=0 WINDOW=65535 SYN URGP=0

2025-03-21_06:22:47.05735 firewall: fw-openvpn-out_MAIv231480925-1-3189b7a6-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=tun0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=192.168.27.100 LEN=60 TOS=0x00 PREC=0x00 TTL=127 ID=21771 PROTO=ICMP TYPE=8 CODE=0 ID=1 SEQ=4

2025-03-21_06:23:06.76962 firewall: fw-openvpn-out_MAIv231480925-1-3189b7a6-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=eth1 OUT=tun0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=192.168.27.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=21775 DF PROTO=TCP SPT=50086 DPT=5201 SEQ=3770954720 ACK=0 WINDOW=65535 SYN URGP=0

2025-03-21_07:09:44.46552 firewall: fw-openvpn-portfw_MAIv231480925-1-3189b7b9-8002-1315-805d-a8741dfd1b11 act=ACCEPT IN=tun0 OUT=eth1 MAC=SRC=11.8.0.1 DST=192.168.1.100 LEN=52 TOS=0x00 PREC=0x00 TTL=127 ID=33661 DF PROTO=TCP SPT=20179 DPT=5201 SEQ=1909642899 ACK=0 WINDOW=65535 SYN URGP=0 CTMARK=1010
    
```

### 6.4.16 DoS protection: SYN flood protection (fw-SYN-flood)

The limit/threshold for new incoming and outgoing TCP connections (SYN flood protection) per second can be configured via the "Network Security >> DoS Protection" menu. If one limit is reached, a log entry with the log prefix **fw-SYN-flood** is recorded. These events are logged once per second.

Log prefix	Description
fw-SYN-flood	A limit for an incoming or outgoing TCP connection per second has been reached.

#### Example:

```
2025-03-21_08:56:51.06084 firewall: fw-SYN-flood act=DROP IN=eth1 OUT=eth0
MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.200 LEN=52 TOS=0x00
PREC=0x00 TTL=127 ID=29158 DF PROTO=TCP SPT=51564 DPT=8080
SEQ=408716129 ACK=0 WINDOW=64240 SYN URGP=0
```

### 6.4.17 DoS protection: ICMP flood protection (fw-ICMP-flood)

The maximum number of incoming and outgoing ICMP echo requests (ICMP flood protection) per second can be configured via the "Network Security >> DoS Protection" menu. If one of the limit is exceeded, a log entry with the log prefix **fw-ICMP-flood** is recorded. These events are logged once per second.

Log prefix	Description
fw-ICMP-flood	A limit for incoming or outgoing ICMP echo requests per second has been reached.

#### Example:

```
2025-03-21_08:51:10.64480 firewall: fw-ICMP-flood act=DROP IN=eth1 OUT=eth0
MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.200 LEN=60 TOS=0x00
PREC=0x00 TTL=254 ID=28715 PROTO=ICMP TYPE=8 CODE=0 ID=47114 SEQ=4
```

### 6.4.18 Max. size „ICMP Echo Request packets“ (fw-ICMP-maxlen)

The maximum size of the permitted ICMP echo request packets can be set via the "Network Security >> Packet Filter >> Advanced" menu. If an ICMP echo request packet exceeds this limit, a log entry with the log prefix **fw-ICMP-maxlen** is recorded.

Log prefix	Description
fw-ICMP-maxlen	The limit for the maximum size of an ICMP echo request has been reached.

**Example:**

```
2025-03-21_09:05:28.59680 firewall: fw-ICMP-maxlen act=DROP IN=eth1
OUT=eth0 MAC=08:00:27:11:1e:62 SRC=192.168.1.100 DST=10.1.80.200
LEN=2028 TOS=0x00 PREC=0x00 TTL=127 ID=49800 PROTO=ICMP TYPE=8 CODE=0
ID=1 SEQ=43
```

## 7 Create X.509 certificates with OpenSSL



Document-ID: 108395\_en\_01  
 Document-Description: AH EN X.509 CERT OPENSLL  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
 It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

### Contents of this document

This section explains briefly how to create X.509 certificates using the tool *OpenSSL*.

7.1	Introduction.....	165
7.2	Preparing the CA environment .....	167
7.3	Modifying the OpenSSL configuration file .....	168
7.4	Create the CA Certificate and Key .....	172
7.5	Create a Certificate Request for the mGuard .....	174
7.6	Sign the mGuard's Certificate Request with the CA .....	176
7.7	Creating the mGuard's PKCS#12 file (Machine Certificate) .....	178
7.8	Example: VPN connection between two mGuard devices .....	179

### 7.1 Introduction

The enrollment of certificates requires a certification authority (CA) which issues public key certificates for a specific period of time. A CA can be a private (in-house) CA, run by your own organization, or a public CA. A public CA is operated by a third party that you trust to validate the identity of each client or server to which it issues a certificate.

There are several tools available for creating and managing certificates, as for example *Microsoft Certification Authority (CA) Server*, *OpenSSL* and *XCA*.

This application note explains how to create X.509 certificates with the tools **OpenSSL** and **XCA** for setting up a VPN connection using X.509 certificates as authentication method.



The scope of this document is not to be a complete user's guide for the described tools. It shall help you getting familiar with them and to create the required certificates in a short term.

#### 7.1.1 Introduction OpenSSL

OpenSSL is available for several platforms (Linux, UNIX, Windows) and can be downloaded from the Internet. We have used *OpenSSL 1.1.0e* on a *Windows 7* platform. Please refer to <http://www.openssl.org> for getting further information about OpenSSL and the supported command line options.

OpenSSL provides various ways for specifying the required options. You can enter them at the command line, specify them in a configuration file or you'll be prompted to enter them when the *openssl* command is executed. When using configuration files, you can ei-

then specify all required parameters in one single file or use different ones, depending on which kind of certificate you want to create. The OpenSSL configuration file, which comes with OpenSSL, is called *openssl.cnf*.



Please note that Windows hides the file extension *.cnf*, even if you have configured the *Windows Explorer* not to do so. Therefore we use the extension *.cnf*.

In the following chapters we will explain how to setup OpenSSL to act as certification authority (CA). A certificate request must be signed by the CA to become a valid certificate.

Basically you can use the examples of the following chapters for creating the certificates. You only need to follow the instructions and adjust the parameters in the section *req\_dn* of the OpenSSL configuration file *openssl.cnf* (see chapter [“Modifying the OpenSSL configuration file” on page 168](#)) to your company needs.

Here is a small legend with **file extensions** we will use for the created files and their meaning.

File extension	Explanation
<b>key</b>	Private key Restrictive permissions should be set on these files.
<b>csr</b>	Certificate Request The request will be signed by the CA in order to create the certificate. After doing this, the file is not needed anymore and can be deleted.
<b>crt</b>	Certificate This certificate can be publicly distributed.
<b>p12</b>	PKCS#12 export of the certificate, containing its private and public key. The export file is secured by a password to protect the private key against unauthorized usage. This certificate may not be distributed publicly.

## 7.2 Preparing the CA environment

First of all we will create a directory structure where all certificate stuff will be kept. In the following examples we use **C:\CA** as root directory. The following subdirectories need to be created:

Subdirectory	Purpose
<b>.\certs</b>	Directory where the certificates will be placed.
<b>.\newcerts</b>	Directory where OpenSSL puts the created certificates in PEM format as <i>&lt;cert serial number&gt;.pem</i> (e.g. <i>07.pem</i> ). OpenSSL requires this directory.
<b>.\private</b>	Directory for storing the private keys. Ensure that you set restrictive permissions to this directory so that they can be read only by user with the appropriate privileges.

Apart of the directory tree, the following two files (*index.txt* and *serial*) need to be created:

- **index.txt:** This file is used as certificate “database” by OpenSSL. To create this file, proceed as follows:
  - Open a DOS prompt.
  - Switch to the CA root directory (in our example C:\CA).
  - Execute the command: *copy NUL: index.txt*  
This command creates the empty file *index.txt*.
- **serial:** This file contains the certificate serial number counter. This counter will be incremented automatically by OpenSSL when its value has been used for creating a certificate. To create this file, proceed as follows:
  - Open a DOS prompt.
  - Switch to the CA root directory (in our example C:\CA).
  - Execute the command: *echo 0001 > serial*  
This command creates the file *serial* with the initial serial number 0001.

## 7.3 Modifying the OpenSSL configuration file

We have named the OpenSSL configuration file *openssl.conf* and placed it into the CA root directory (in our example C:\CA). The OpenSSL configuration file has multiple sections. Each section is used for a different purpose. The sections include the following positions:

- **ca, CA\_default:** Defines certification authority configuration.
- **policy\_any:** Defines request policies.
- **req, req\_dn:** Defines request defaults.

In our examples the configuration file (*openssl.conf*) has the following entries:

```
[ req ]
prompt                = yes
default_bits          = 4096
distinguished_name    = req_dn
x509_extensions       = req_ext
string_mask           = utf8only

[ ca ]
default_ca            = CA_default

[ CA_default ]
dir                  = C:/CA
certs                = $dir/certs
database             = $dir/index.txt
new_certs_dir        = $dir/newcerts

certificate          = $dir/certs/ca.crt
serial               = $dir/serial
private_key          = $dir/private/ca.key

default_md           = sha256
default_days         = 365

x509_extensions     = req_ext
policy                = policy_any

[ req_dn ]
countryName          = Country Name (2 letter code)
countryName_default  = DE

organizationName     = Organization Name (company)
organizationName_default = PHOENIX CONTACT Cyber Security AG

organizationalUnitName = Organizational Unit Name (department, division)
organizationalUnitName_default = Support

commonName           = Common Name (hostname, IP, or your name)

# Not used in our example
#emailAddress         = Email Address
#localityName         = Locality Name (city, district)
#stateOrProvinceName = State or Province Name (full name)

[ policy_any ]
countryName          = supplied
organizationName     = supplied
organizationalUnitName = optional
commonName           = supplied
# Not used in our example
#emailAddress         = optional
#localityName         = optional
#stateOrProvinceName = optional

[ req_ext ]
basicConstraints     = critical, CA:false

[ ca_ext ]
basicConstraints     = critical, CA:true, pathlen:0
keyUsage             = critical, cRLSign, keyCertSign
```

Section	Option	Description
<b>[ req ]</b>		This section is called when requesting a certificate by calling the <i>openssl</i> command with the option <b>req</b> .
	<b>prompt</b>	If set to the value <b>no</b> this disables prompting of certificate fields and just takes values from the configuration file directly. You should enable this option for being able to enter the <i>common name</i> or to modify the default values of the certificate's distinguished name for each requested certificate.
	<b>default_bits</b>	This specifies the default key size in bits. If not specified then 512 is used.
	<b>distinguished_name</b>	This specifies the section containing the distinguished name fields to prompt for when generating a certificate or certificate request. In our example this section is called <b>[ req_dn ]</b> .
	<b>x509_extensions</b>	This specifies the configuration file section containing a list of extensions to add to certificate generated when the <b>-x509</b> switch is used. It can be overridden by the <b>-extensions</b> command line switch.
	<b>string_mask</b>	This option masks out the use of certain string types in certain fields. If the <b>utf8only</b> option is used then only UTF8Strings will be used: this is the PKIX recommendation in RFC2459 after 2003.
<b>[ ca ]</b>		This section is called when signing certificate requests by calling the <i>openssl</i> command with the option <b>ca</b> .
	<b>default_ca</b>	If the <b>-name</b> command line option is used, then it names the section to be used. Otherwise the section to be used must be named in the <b>default_ca</b> option of the <b>ca</b> section of the configuration file, in our example <b>[ CA_default ]</b> .

<p>[ CA_default ]</p>	<p>This section is called when signing certificate requests by calling the <i>openssl</i> command with the option <b>ca</b>, referenced by the <b>default_ca</b> option of the <b>ca</b> section.</p>	
	<p><b>dir</b></p>	<p>Root directory of the CA environment. If the configuration file is located in this directory and if you execute all <i>openssl</i> commands from this directory, you simply can specify "dir = .".</p>
	<p><b>certs</b></p>	<p>Certificates output directory.</p>
	<p><b>database</b></p>	<p>The text database file to use (mandatory parameter). This file must be present though initially it will be empty.</p>
	<p><b>new_certs_dir</b></p>	<p>It specifies the directory where new certificates will be placed. Mandatory.</p>
	<p><b>certificate</b></p>	<p>Location and filename of the CA certificate.</p>
	<p><b>serial</b></p>	<p>A text file containing the next serial number to use in hex. Mandatory. This file must be present and contain a valid serial number.</p>
	<p><b>private_key</b></p>	<p>Location and filename of the file which contains the CA's private key.</p>
	<p><b>default_md</b></p>	<p>This option specifies the digest algorithm to use. Any digest supported by the OpenSSL <i>dgst</i> command can be used.</p>
	<p><b>default_days</b></p>	<p>The default number of days the certificate will be valid. This default value can be overridden by the <b>-days</b> command line switch.</p>
	<p><b>x509_extensions</b></p>	<p>This specifies the configuration file section containing a list of extensions to add to certificate generated when the <b>-x509</b> switch is used. It can be overridden by the <b>-extensions</b> command line switch.</p>
<p>[ req_dn ]</p>	<p>This specifies the parameters containing the distinguished name fields to prompt for when generating a certificate or certificate request, referenced by the <b>distinguished_name</b> option of the <b>req</b> section. If the <b>prompt</b> option in the <b>req</b> section is absent or set to <b>yes</b> then the section contains field prompting information. &lt;fieldname&gt; is the field name being used, for example common-Name (or CN).</p>	
	<p>&lt;fieldname&gt; = "prompt"</p>	<p>The "prompt" string is used to ask the user to enter the relevant details.</p>
	<p>&lt;fieldname&gt;_default = "default field value"</p>	<p>If the user enters nothing then the default value is used if no default value is present then the field is omitted.</p>

<p><b>[ policy_any ]</b></p>	<p>This option defines the CA "policy" to use and needs to be specified by the –policy command line switch. This is a section in the configuration file which decides which fields should be mandatory or match the CA certificate. The policy section consists of a set of variables corresponding to certificate DN fields. If the value is <b>match</b> then the field value must match the same field in the CA certificate. If the value is <b>supplied</b> then it must be present. If the value is <b>optional</b> then it may be present. Any fields not mentioned in the policy section are silently deleted.</p>	
<p><b>[ ..._ext ]</b></p>	<p>Those sections specify the X.509 extensions and are referenced by the <b>x509_extensions</b> option within the configuration file (section <b>[ req ]</b> and <b>[ CA_default ]</b>). It can be overridden by the <b>-extensions</b> command line switch.</p>	
	<p>basicConstraints</p>	<p>This flag is used to determine whether the certificate can be used as a CA certificate.</p>

## 7.4 Create the CA Certificate and Key

Now, that all initial configuration is done, we may create a self signed certificate, that will be used as our CA certificate. In other words, we will use this to sign other certificate requests.

Switch to the CA root directory. From this directory we can issue all **openssl commands** because our OpenSSL configuration file (*openssl.conf*) is located here.

Syntax to create the CA certificate and private key:

```
openssl req -new -config <filename> -x509 -extensions <section> -keyout  
<filename> -out <filename> -days <nn>
```

Option	Description
<b>req</b>	The <i>req</i> command primarily creates and processes certificate requests. It can instead create self signed certificates when the option <b>-x509</b> is specified.
<b>-new</b>	This option generates a new certificate request.
<b>-config &lt;filename&gt;</b>	This allows an alternative configuration file to be specified.
<b>-x509</b>	This option outputs a self signed certificate instead of a certificate request.
<b>-extensions &lt;section&gt;</b>	Specifies the section in the openssl configuration file (specified by <b>-config &lt;filename&gt;</b> ) where the X.509 certificate extensions are defined.
<b>-keyout &lt;filename&gt;</b>	Filename of the CA's private key. Although it is protected with a pass phrase you should restrict access to it, so that only authorized users can read it.

**Example:**

```
C:\CA>openssl req -new -config openssl.conf -x509 -extensions ca_ext -keyout private/ca.key -out certs/ca.crt -days 3640
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to 'private/ca.key'
Enter PEM pass phrase: - enter a strong pass phrase to use for this key
Verifying - Enter PEM pass phrase: - reenter the pass phrase again for verification
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]: - we have kept the default value
Organization Name (company) [PHOENIX CONTACT Cyber Security AG]: - we have kept the default value
Organizational Unit Name (department, division) [Support]: - we have kept the default value
Common Name (hostname, IP, or your name) []: CA - we have entered the common name for the CA certificate

C:\CA>
```

Two files are created:

- **certs/ca.crt:** This is the CA's certificate and can be publicly available and of course world readable.
- **private/ca.key:** This is the CA's private key. Although it is protected with a pass phrase you should restrict access to it, so that only authorized users may have access to it.

## 7.5 Create a Certificate Request for the mGuard

For obtaining a valid mGuard certificate you need to create a certificate request first and then sign it with the CA certificate (explained in chapter [“Sign the mGuard’s Certificate Request with the CA”](#) on page 176).

Syntax for creating a certificate request for the mGuard:

```
openssl req -new -config <filename> -keyout <filename> -out <filename> -days <nn>
```

Option	Description
<b>req</b>	The <i>req</i> command primarily creates and processes certificate requests.
<b>-new</b>	This option generates a new certificate request.
<b>-config &lt;filename&gt;</b>	This allows an alternative configuration file to be specified.
<b>-keyout &lt;filename&gt;</b>	Filename of the mGuard private key. Although it is protected with a pass phrase you should restrict access to it, so that only authorized users can read it.
<b>-out &lt;filename&gt;</b>	Filename of the mGuard certificate.
<b>-days &lt;nn&gt;</b>	The number of days the certificate should be valid.

**Example:**

```
C:\CA>openssl req -new -config openssl.conf -keyout private/mGuard.key -out
mGuard.csr -days 364
Generating a 4096 bit RSA private key
.....++
.....
+
writing new private key to 'private/mGuard.key'
Enter PEM pass phrase: - enter a strong pass phrase to use for this key
Verifying - Enter PEM pass phrase: - reenter the pass phrase again for verification
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]: - we have kept the default value
Organization Name (company) [PHOENIX CONTACT Cyber Security AG]: - we have kept
the default value
Organizational Unit Name (department, division) [Support]: - we have kept the default
value
Common Name (hostname, IP, or your name) []:mGuard - enter the common name for
the mGuard certificate

C:\CA>
```

Two files are created:

- **mGuard.csr**: This is the certificate request which needs to be signed by the CA certificate.
- **private/mGuard.key**: This is the private key, which is not protected with a pass phrase.

## 7.6 Sign the mGuard's Certificate Request with the CA

The mGuard's certificate request needs to be signed by the CA to become a valid certificate.

Syntax for signing the mGuard's certificate request with the CA:

```
openssl ca -config <filename> -out <filename> -infiles <filename>
```

Option	Description
<b>ca</b>	The <i>ca</i> command is a minimal CA application. It can be used to sign certificate requests in a variety of forms and generate CRLs it also maintains a text database of issued certificates and their status.
<b>-config &lt;filename&gt;</b>	This allows an alternative configuration file to be specified.
<b>-out &lt;filename&gt;</b>	Filename of the signed mGuard certificate.
<b>-infiles &lt;filename&gt;</b>	Filename of the mGuard's certificate request. This must be the last option.

### Example:

```
C:\CA>openssl ca -config openssl.conf -out certs/mGuard.crt -infiles mGuard.csr
Using configuration from openssl.conf
Enter pass phrase for C:/CA/private/ca.key: - enter the pass phrase of the CA's private
key
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName      :PRINTABLE:'DE'
organizationName :ASN.1 12:'PHOENIX CONTACT Cyber Security AG'
organizationalUnitName:ASN.1 12:'Support'
commonName       :ASN.1 12:'mGuard'
Certificate is to be certified until Jul 7 09:02:23 2018 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\CA>
```

After all this is done two new files are created:

- **certs/mGuard.crt**: This is the mGuard's certificate, which can be made available publicly.
- **newcerts/01.pem**: This is exactly the same certificate, but with the certificate's serial number (hex number) as filename. For subsequent requests the number is incremented. This file is not needed anymore and can be removed.

Now you can delete the mGuard's certificate request (*mGuard.csr*). It's no longer needed.

## 7.7 Creating the mGuard’s PKCS#12 file (Machine Certificate)

This file combines the private and public key and is the mGuard’s machine certificate which needs to be imported through the mGuard menu **Authentication >> Certificates >> Machine Certificates**. You’ll be prompted to enter a password which protects the PKCS#12 export of the certificate against unauthorized usage.

Following is the syntax to create the mGuard machine certificate:

```
openssl pkcs12 -export -in <filename> -inkey <filename> -out <filename>
```

Option	Description
<b>pkcs12</b>	The <i>pkcs12</i> command allows PKCS#12 files to be created and parsed.
<b>-export</b>	This option specifies that a PKCS#12 file will be created rather than parsed.
<b>-in &lt;filename&gt;</b>	The filename to read the certificate from. The format of the file must be PEM. This is the mGuard’s certificate you have created in the previous step.
<b>-inkey &lt;filename&gt;</b>	File to read private key from. This is the file which contains the private key of the mGuard’s certificate.
<b>-out &lt;filename&gt;</b>	The filename to write certificates and private keys to. They are all written in PEM format.

**Example:**

```
C:\CA>openssl pkcs12 -export -in certs/mGuard.crt -inkey private/mGuard.key -out
certs/mGuard.p12
Enter pass phrase for private/mGuard.key: - enter the password of the mGuard’s private
key
Enter Export Password: - enter a strong pass phrase to use for this export
Verifying - Enter Export Password: - reenter the pass phrase again for verification
C:\CA>
```

This command will create a file called **certs/mGuard.p12**, containing the mGuard certificate public and private key. The file is protected by the entered password.

## 7.8 Example: VPN connection between two mGuard devices

We assume that you already have setup the CA environment, configured the OpenSSL's configuration file (*openssl.conf*) and created the CA certificate and key. (As described in the previous chapters.)

### Step 1: Create a certificate request for each mGuard

#### mGuard 1

```
openssl req -new -config openssl.conf -keyout private/mGuard1.key -out  
mGuard1.csr -days 364
```

#### mGuard 2

```
openssl req -new -config openssl.conf -keyout private/mGuard2.key -out  
mGuard2.csr -days 364
```

### Step 2: Sign each certificate request with the CA

#### mGuard 1

```
openssl ca -config openssl.conf -out certs/mGuard1.crt -infile mGuard1.csr
```

#### mGuard 2

```
openssl ca -config openssl.conf -out certs/mGuard2.crt -infile mGuard2.csr
```

The two certificates **certs/mGuard1.crt** and **certs/mGuard2.crt** are created. **mGuard1.crt** needs to be imported on mGuard 2 as connection certificate through the menu **IPsec VPN >> Connections >> Authentication**. **mGuard2.crt** on mGuard 1 correspondingly.

### Step 3: Obtain the machine certificate for each mGuard

#### mGuard 1

```
openssl pkcs12 -export -in certs/mGuard1.crt -inkey private/mGuard1.key -out  
certs/mGuard1.p12
```

#### mGuard 2

```
openssl pkcs12 -export -in certs/mGuard2.crt -inkey private/mGuard2.key -out  
certs/mGuard2.p12
```

The two exports **certs/mGuard1.p12** and **certs/mGuard2.p12** are created.

**mGuard1.p12** needs to be imported on mGuard 1 as machine certificate through the menu **Authentication >> Certificates >> Machine Certificates**. **mGuard2.p12** on mGuard 2 correspondingly.



## 8 Create X.509 certificates with XCA



Document-ID: 108396\_en\_01  
 Document-Description: AH EN X.509 CERT XCA  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
 It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

### Contents of this document

This section explains briefly how to create X.509 certificates using the tool XCA.



XCA provides much more functionality than explained in this document. Please refer to the XCA documentation for further information (<http://xca.sourceforge.net/xca.html> – 15.09.2017). You can download XCA from <http://xca.sourceforge.net>. The screenshots and descriptions in this chapter are related to XCA v1.3.2.

8.1	Introduction.....	181
8.2	Create an XCA database .....	183
8.3	Create a certificate template .....	184
8.4	Create a CA Certificate .....	187
8.5	Create a Client Certificate .....	191
8.6	Export a certificate .....	195
8.7	Sign a Certificate Request with the CA .....	196
8.8	Using a Certificate Revocation List (CRL) .....	198
8.9	Example: VPN connection between two mGuard devices .....	199

### 8.1 Introduction

The enrollment of certificates requires a certification authority (CA) which issues public key certificates for a specific period of time. A CA can be a private (in-house) CA, run by your own organization, or a public CA. A public CA is operated by a third party that you trust to validate the identity of each client or server to which it issues a certificate.

There are several tools available for creating and managing certificates, as for example *Microsoft Certification Authority (CA) Server*, *OpenSSL* and *XCA*.

This application note explains how to create X.509 certificates with the tools **OpenSSL** and **XCA** for setting up a VPN connection using X.509 certificates as authentication method.



The scope of this document is not to be a complete user's guide for the described tools. It shall help you getting familiar with them and to create the required certificates in a short term.

#### 8.1.1 XCA - X Certificate and key management

XCA is intended for the creation and management of X.509 certificates, certificate requests, RSA, DSA and EC private keys, smart cards and CRLs. Everything that is required for a CA is implemented. All CAs can sign sub-CAs recursively.

## mGuard

---

For enterprise-wide use, templates are available that can be used and adapted to generate certificates or certificate request. All crypto data is stored in an endian-agnostic file format portable across operating systems.

## 8.2 Create an XCA database

To create X.509 certificates and keys using XCA you need to create a database first. Proceed as follows:

1. Click **File >> New DataBase**.
2. Specify the filename and the storage location of the database.
3. Click **Save**.
4. Enter a password which protects the database against unauthorized usage. The password will be requested every time you open the XCA database.

### 8.2.1 Open an XCA database

When restarting XCA, you need to reconnect to a database first. To open an already created database, proceed as follows:

1. Click **File >> Open DataBase**.
2. Select the desired database (file \*.xdb).
3. Click **Open**.

### 8.2.2 Set default hash algorithm



**NOTE:** Phoenix Contact recommends using secure and up to date encryption and hash algorithms, as stated in the mGuard Software Reference Manual, available at [phoenix-contact.net/products](https://phoenix-contact.net/products) (search for "UM EN MGuard", choose a product and select the manual in the download area).

Before you start creating certificates, you should set the default hash algorithm to **SHA 256**. If you don't set the default hash algorithm to SHA 256 you will need to do it every time creating a new certificate.

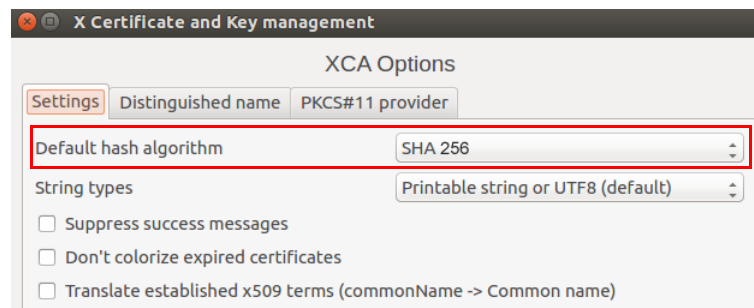


**NOTE: Not all appliances support the functionality of the SHA 2 family**

If you are unsure, if all of your appliances support the functionality of the SHA 2 family, the less secure SHA 1 algorithm might be used instead (not recommended by PHOENIX CONTACT and not in accordance with ANSSI-CSPN-2016-09).

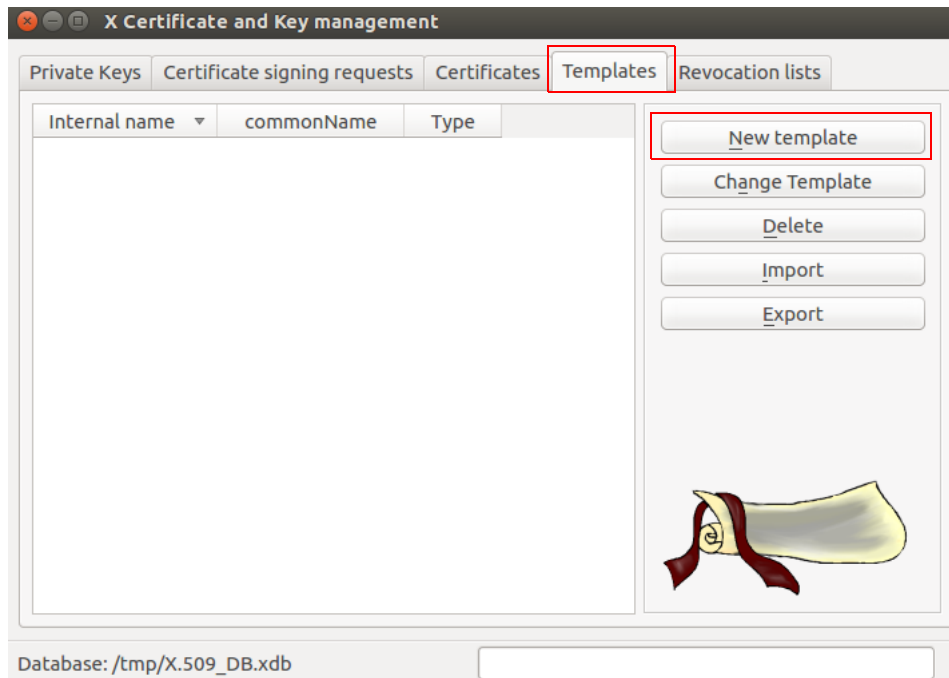
Proceed as follows:

- Click **File >> Options** and set the default hash algorithm to SHA 256 (or the algorithm you will use in your setup).



## 8.3 Create a certificate template

If you need to create more than one certificate it is useful to define a template for consistency reasons and less typing. This template can be used when creating the certificates.



Proceed as follows:

1. Move to the tab **Templates**.
2. Click **New template**.
3. Select the **Preset Template Values** and click **OK**.

### 8.3.1 Create XCA template >> Tab: Subject

The screenshot shows the 'Create XCA template' dialog box in XCA, with the 'Subject' tab selected. The dialog has a title bar 'X Certificate and Key management' and a close button. The main title is 'Create XCA template'. Below the title are tabs: 'Subject' (highlighted with a red box), 'Extensions', 'Key usage', 'Netscape', and 'Advanced'. The 'Distinguished name' section contains several input fields: 'Internal name' (XCA Documentation), 'organizationName' (PHOENIX CONTACT), 'countryName', 'organizationalUnitName', 'stateOrProvinceName', 'commonName' (XCA Docu), 'localityName', and 'emailAddress' (info@phoenixcontact.com). Below these fields is a table with columns 'Type' and 'Content', and buttons 'Add' and 'Delete'. At the bottom, there is a 'Private key' section with a dropdown menu, a checkbox 'Used keys too', and a 'Generate a new key' button. The dialog ends with 'Cancel' and 'OK' buttons.

Type	Content
------	---------

Proceed as follows:

1. Move to the tab **Subject**
2. Use the entry fields from **Internal name** to **emailAddress** for entering the identifying parameters that shall be common for all certificates.  
The template will be stored in XCA under the **Internal name**.
3. Move to the tab **Extensions**.

### 8.3.2 Create XCA template >> Tab: Extensions

The screenshot shows the 'Edit XCA template' dialog box with the following configuration:

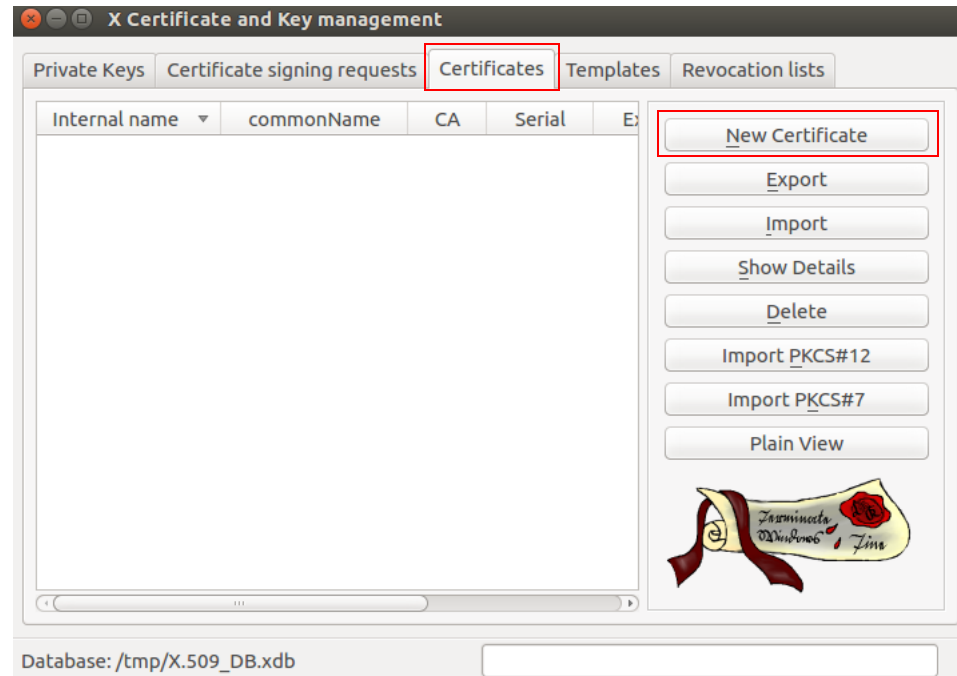
- Tab:** Extensions
- X509v3 Basic Constraints:**
  - Type: End Entity
  - Path length: (empty)
  - Critical:
- Key identifier:**
  - Subject Key Identifier:
  - Authority Key Identifier:
- Validity:**
  - Not before: 2017-07-10 12:14 GMT
  - Not after: 2018-07-10 12:14 GMT
- Time range:**
  - Value: 365
  - Unit: Days
  - Apply: (highlighted)
  - Midnight:
  - Local time:
  - No well-defined expiration:
- Other fields:**
  - X509v3 Subject Alternative Name: (empty)
  - X509v3 Issuer Alternative Name: (empty)
  - X509v3 CRL Distribution Points: (empty)
  - Authority Information Access: OCSP

Proceed as follows:

1. In Section **X509v3 Basic Constraints:**
  - Set the **Type** to *End Entity* if you want to use the template for creating client certificates.
  - Set the **Type** to *Certification Authority* if the template should be used for creating CA certificates.
2. In Section **Time Range:**
  - Set the default lifetime of the certificates and click **Apply**.
3. Click **OK** to create the template.

## 8.4 Create a CA Certificate

If you don't use self signed client certificates, a client certificate must be signed by the CA certificate to become a valid certificate. Therefore you need to create the CA certificate first before creating the client certificates. The CA certificate is a self signed certificate.



Proceed as follows:

1. Move to the tab **Certificates**.
2. Click **New Certificate**.

### 8.4.1 Create x509 (CA) Certificate >> Tab: Source

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

**Signing request**

Sign this Certificate signing request

Copy extensions from the request

Modify subject of the request

**Signing**

Create a self signed certificate with the serial 1

Use this Certificate for signing

Signature algorithm: SHA 256

**Template for the new certificate**

[default] CA

Apply extensions Apply subject Apply all

Cancel OK

Proceed as follows:

1. Move to the tab **Source**.
2. In Section **Signing**: Ensure that **Create a self signed certificate with the serial** is selected.
3. You may enter a serial number for the certificate or leave the default value.
4. In Section **Template for the new certificate**: If you have created a template for creating CA certificates, you may select it and click **Apply**.
5. Move to the tab **Subject**.

## 8.4.2 Create x509 (CA) Certificate >> Tab: Subject

X Certificate and Key management

Create x509 Certificate

Source **Subject** Extensions Key usage Netscape Advanced

**Distinguished name**

Internal name XCA Documentation organizationName PHOENIX CONTACT

countryName organizationalUnitName

stateOrProvinceName commonName XCA Docu

localityName emailAddress info@phoenixcontact.com

Type	Content

Private key

Used keys too **Generate a new key**

Cancel OK

Proceed as follows:

1. In Section **Distinguished name**: Use the entry fields from **Internal name** to **emailAddress** for entering the identifying parameters of the CA.
2. In Section **Private key**: Click **Generate a new key** for creating the private RSA key for the CA.

X Certificate and Key management

New key

Please give a name to the new key and select the desired keysize

**Key properties**

Name XCA Documentation

Keytype RSA

Keysize 4096 bit

Remember as default

Cancel Create

3. Enter a **Name** for the key, specify the desired **Keytype** and **Keysize** and click **Create**.
4. Move to the tab **Extensions**.

### 8.4.3 Create x509 (CA) Certificate >> Tab: Extensions

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Extensions' tab selected. The 'X509v3 Basic Constraints' section has 'Type' set to 'Certification Authority'. The 'Validity' section has 'Not before' set to '2017-07-10 12:53 GMT' and 'Not after' set to '2018-07-10 12:53 GMT'. The 'Time range' is set to '10' years. The 'Apply' button is highlighted.

Proceed as follows:

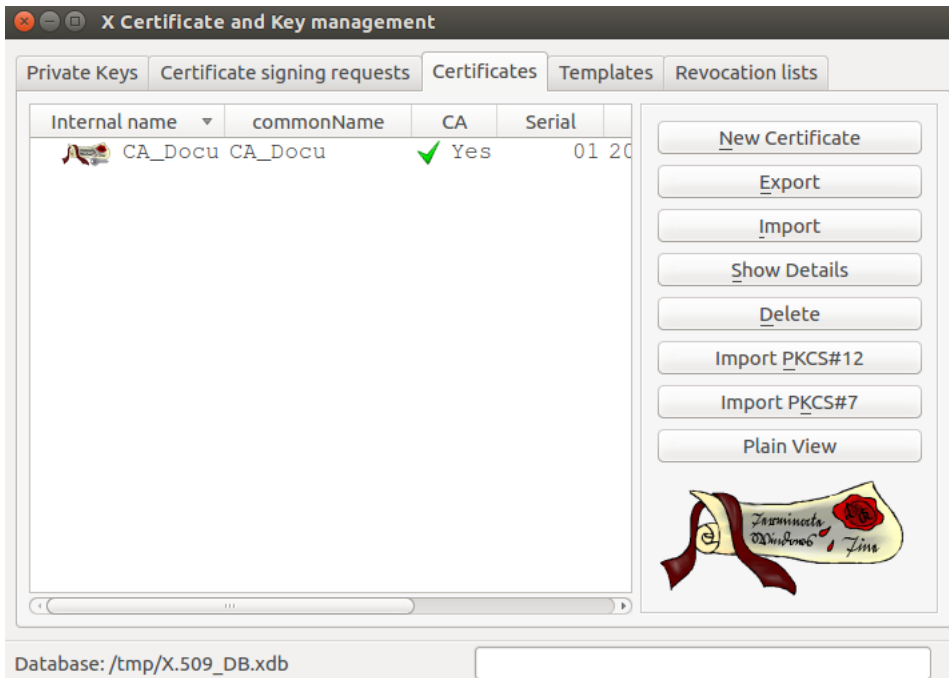
5. In Section **X509v3 Basic Constraints**: Set the **Type** to *Certification Authority*.
6. In Section **Time Range**: Set the default lifetime of the certificates and click **Apply**. For a CA certificate you may want it to last longer than the client certificates so that you do not have to reissue the certificates so often. A lifetime of 10 years might be a good value.
7. Click **Apply**.
8. Click **OK** to create the certificate.  
The CA certificate is displayed in the tab **Certificates**.

## 8.5 Create a Client Certificate

If you want to create client certificates, you have to create or import a CA certificate first, which will be used to sign the client certificate. By signing the client certificate with the CA certificate, it becomes valid.



A CA certificate to sign the client certificate must be available in the XCA database. If it is not available it has to be created first (see [“Create a CA Certificate”](#) on page 187).



Proceed as follows:

1. Move to the tab **Certificates**.
2. Click **New Certificate**.

### 8.5.1 Create x509 (Client) Certificate >> Tab: Source

X Certificate and Key management

Create x509 Certificate

Source Subject Extensions Key usage Netscape Advanced

**Signing request**

Sign this Certificate signing request

Copy extensions from the request

Modify subject of the request

**Signing**

Create a self signed certificate with the serial 1

Use this Certificate for signing CA\_Docu

Signature algorithm SHA 256

**Template for the new certificate**

XCA Documentation

Apply extensions Apply subject Apply all

Cancel OK

Proceed as follows:

1. Move to the tab **Source**.
2. In Section **Signing**: Ensure that the correct CA is selected in the field **Use this certificate for signing**.
3. In Section **Template for the new certificate**: If you have created a template for creating client certificates, you may select it and click **Apply**.
4. Move to the tab **Subject**.

## 8.5.2 Create x509 (Client) Certificate >> Tab: Subject

**Create x509 Certificate**

Source **Subject** Extensions Key usage Netscape Advanced

**Distinguished name**

Internal name: CLIENT CERTIFICATE A    organizationName: PHOENIX CONTACT  
 countryName:    organizationalUnitName:     
 stateOrProvinceName:    commonName: CLIENT A  
 localityName:    emailAddress: info@phoenixcontact.com

Type	Content

Private key: CLIENT CERTIFICATE A (RSA:4096 bit)     Used keys too    **Generate a new key**

Cancel    OK

Proceed as follows:

1. In Section **Distinguished name**: Use the entry fields from **Internal name** to **emailAddress** for entering the identifying parameters of the client certificate.
2. In Section **Private key**: Click **Generate a new key** for creating the private RSA key for the certificate.

**New key**

Please give a name to the new key and select the desired keysize

**Key properties**

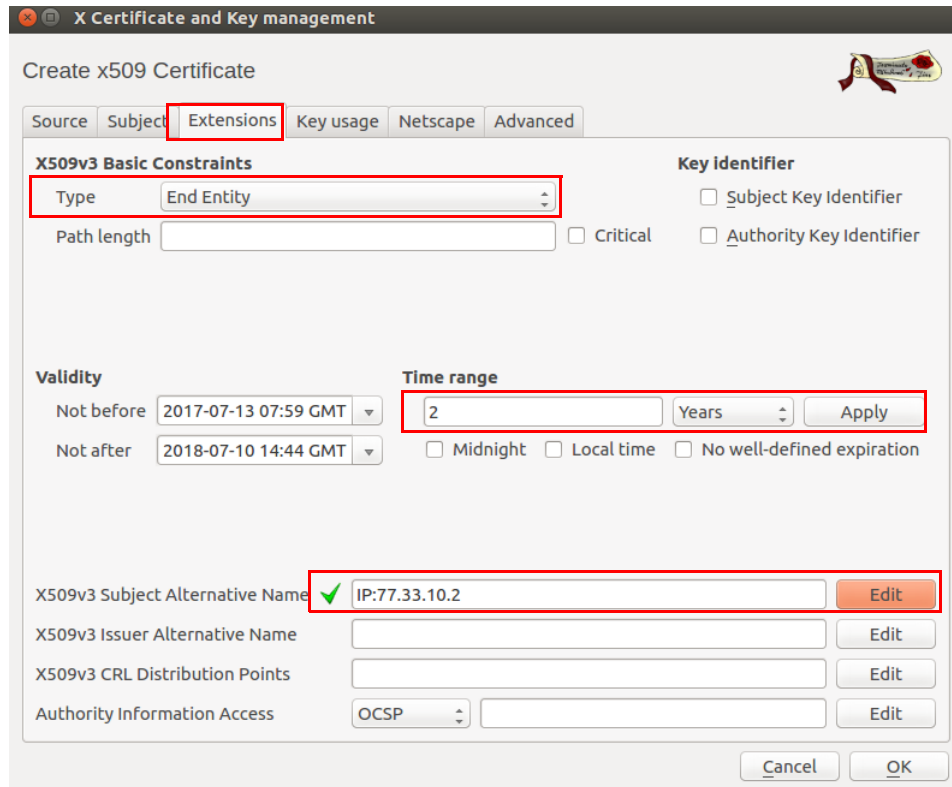
Name: XCA Documentation  
 Keytype: RSA  
 Keysize: 4096 bit

Remember as default

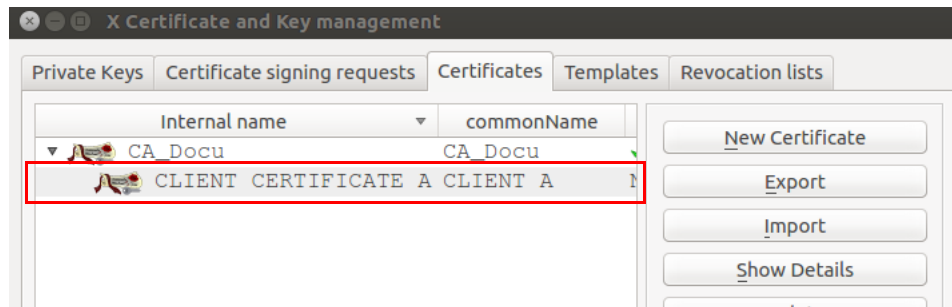
Cancel    Create

3. Enter a **Name** for the key, specify the desired **Keytype** and **Keysize** and click **Create**.
4. Move to the tab **Extensions**.

### 8.5.3 Create x509 (Client) Certificate >> Tab: Extensions



1. In Section **X509v3 Basic Constraints**: Set the **Type** to *End Entity*.
2. In Section **Time Range**: Set the default lifetime of the certificates and click **Apply**.
3. The mGuard uses as default VPN identifier the subject name of the certificate. If you want to use another VPN identifier (e. g. email address, hostname or IP address), this identifier must be present in the certificate as **subject alternative name**.  
To add another identifier, click **Edit** in the line **X509v3 Subject Alternative Name**, select the identifier type (email, DNS or IP), enter its value, click **Add** and then **Apply**.
4. Click **OK** to create the certificate.  
The client certificate will be displayed in the tab **Certificates** beneath the CA certificate.



## 8.6 Export a certificate

To export a certificate created with XCA, proceed as follows:

1. Move to the tab **Certificates**.
2. Highlight the certificate that shall be exported.
3. Click **Export**.



4. Select the **Export Format** (PEM or PKCS#12 – see info box below).
5. Specify the desired **Filename** and the location where the export should be stored.
6. Click **OK**.
7. If you export the certificate as PKCS#12 then you'll be prompted to enter a password which protects the export against unauthorized usage. Enter the Password and click **OK**.



### **PKCS (Public Key Cryptography Standards)**

PKCS #12: Personal Information Exchange Syntax v1.1 (defined in **RFC 7292**)

PKCS #12 v1.1 describes a transfer syntax for personal identity information, including private keys, certificates, miscellaneous secrets, and extensions. Machines, applications, browsers, Internet kiosks, and so on, that support this standard will allow a user to import, export, and exercise a single set of personal identity information. This standard supports direct transfer of personal information under several privacy and integrity modes (RFC 7292).



### **PEM (privacy-enhanced mail)** (defined in RFC's 1421 through 1424)

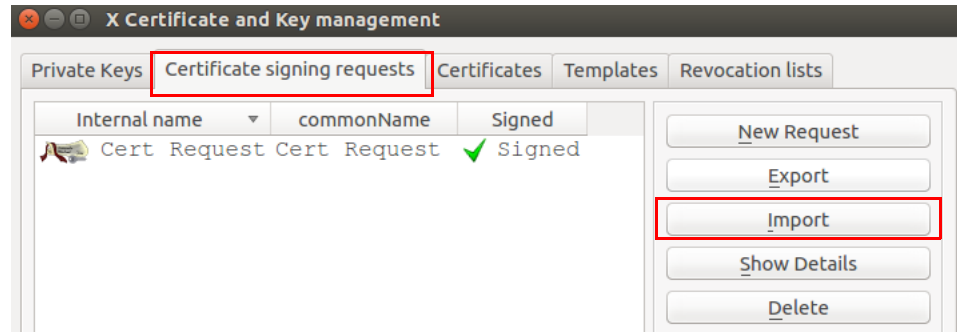
A PEM container may include just the public certificate or an entire certificate chain (including public key, private key, and root certificates).

PEM data is commonly stored in files with a **".pem"** or **".cer"** suffix or a **".crt"** suffix (for certificates), or a **".key"** suffix (for public or private keys).

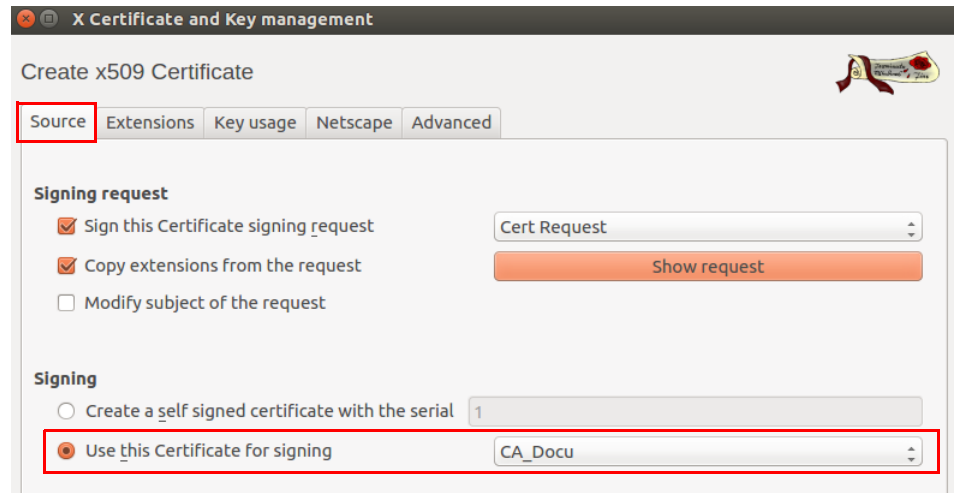
## 8.7 Sign a Certificate Request with the CA

To sign a certificate request, proceed as follows:

1. Move to the tab **Certificate signing requests**.
2. Click **Import**.
3. Select a certificate request (PKCS#10 file) which should be signed by the CA and click **Open**.
4. The imported certificate request is displayed in the tab **Certificate signing requests**.



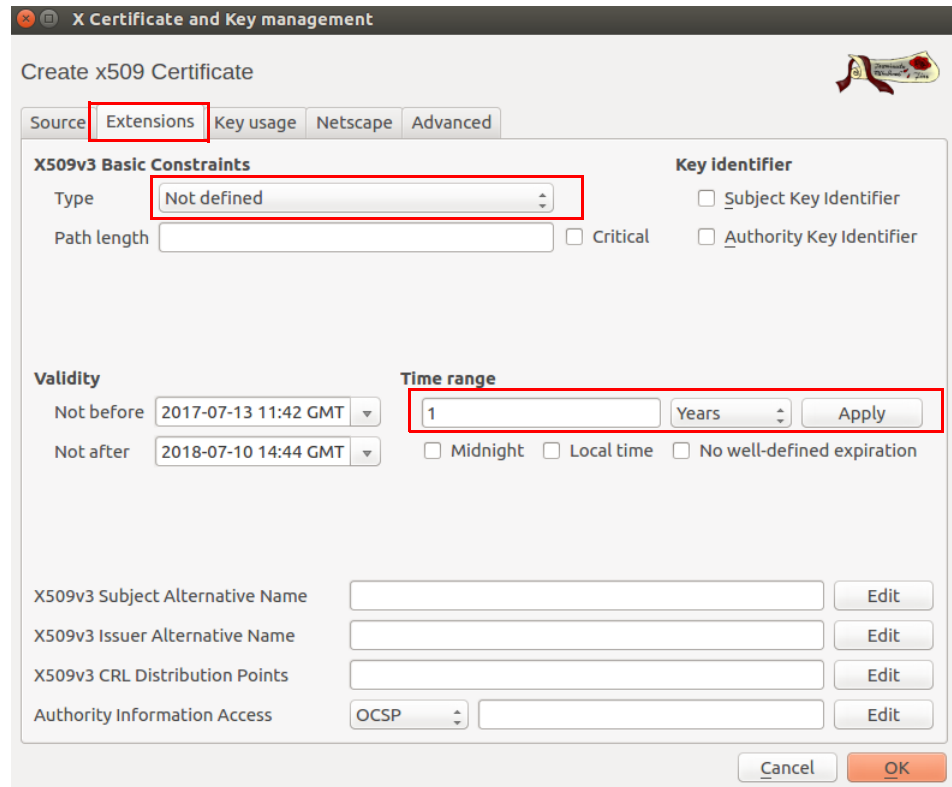
### 8.7.1 X Certificate and Key Management >> Tab: Source



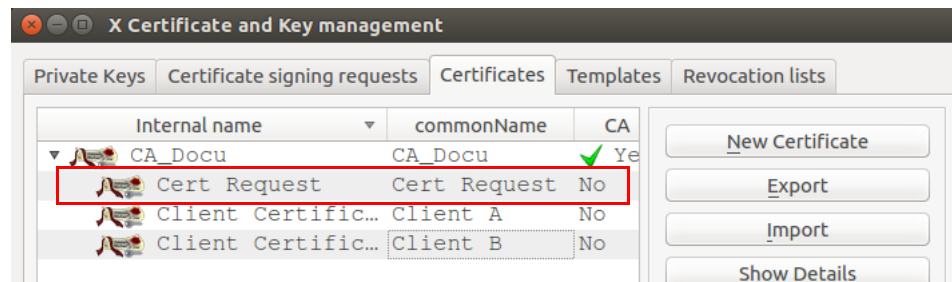
To sign the certificate request, proceed as follows:

1. Move to the tab **Certificate signing requests**.
2. Right click the certificate request and select **Sign** from the context menu.
3. In Section **Signing**: Ensure that the correct CA certificate is selected in the field **Use this certificate for signing**.
4. Move to the tab **Extensions**.

### 8.7.2 X Certificate and Key Management >> Tab: Extensions




1. In Section **X509v3 Basic Constraints**: Leave **Type** as *Not defined*. Otherwise XCA would copy the certificate extensions twice into the signed certificate.
2. In Section **Time Range**: Set the default lifetime for the new certificate and click **Apply**.
3. Click **OK**.
4. The signed certificate request is displayed in the tab **Certificates** beneath the CA certificate.



## 8.8 Using a Certificate Revocation List (CRL)

### 8.8.1 Revoke a certificate

1. Move to the tab **Certificates**.
2. Right click the client certificate that should be revoked and select **Revoke** from the context menu.
3. Edit the parameters and click **OK**.
4. The revoked certificate is marked with a cross icon  and the **Trust state** is *Not trusted*.

### 8.8.2 Specify the CRL renewal period

1. Move to the tab **Certificates**.
2. Right click the CA and select **CA >> Properties** from the context menu.
3. Enter the desired renewal period into the field **Days until next CRL issuing**.
4. Click **OK**.

### 8.8.3 Create the CRL

1. Move to the tab **Certificates**.
2. Right click the CA and select **CA >> Generate CRL** from the context menu.
3. Edit the parameters and click **OK**.
4. The CRL is displayed in the tab **Revocation lists**.

### 8.8.4 Obtain information about a CRL

1. Move to the tab **Revocation lists**.
2. Highlight the CRL and click **Show Details**.

### 8.8.5 Export of the CRL

1. Move to the tab **Revocation lists**.
2. Highlight the CRL.
3. Click **Export**.
4. Specify the filename and location for storing the CRL.
5. Chose the export format (DER or PEM).
6. Click **OK**.

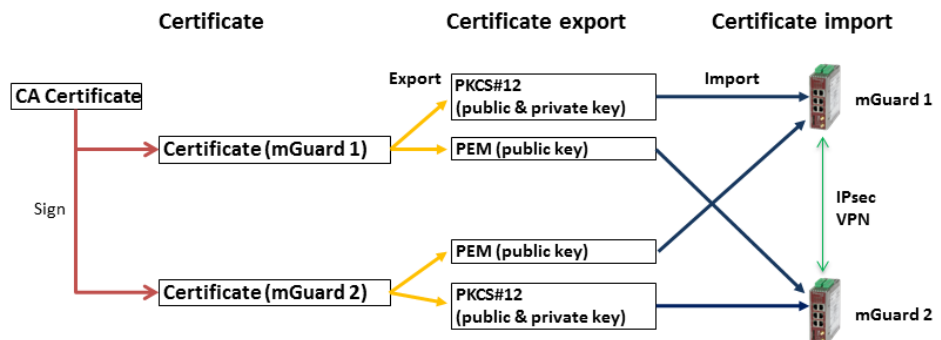
## 8.9 Example: VPN connection between two mGuard devices

To create and import the required certificates for a VPN connection between two mGuard devices, proceed as follows:

- CA Certificate**
  - Create a CA certificate as described in chapter “Create a CA Certificate” on page 187.
- Client Certificate**
  - Create a client certificate for **mGuard #1** and a client certificate for **mGuard #2** as described in chapter “Create a Client Certificate” on page 191.
- Export certificates**
  - Export the certificates as described in chapter “Export a certificate” on page 195.

The following exports are required:

- **mGuard #1** as PKCS#12: This export needs to be imported on **mGuard #1** as a *Machine Certificate* (menu: Authentication >> Certificates, tab *Machine Certificates*).
- **mGuard #2** as PKCS#12: This export needs to be imported on **mGuard #2** as a *Machine Certificate* (menu: Authentication >> Certificates, tab *Machine Certificates*).
- **mGuard #1** as PEM: This export needs to be imported on **mGuard #2** as connection certificate (menu: IPsec VPN >> Connections >> (Edit), tab *Authentication*).
- **mGuard #2** as PEM: This export needs to be imported on **mGuard #1** as connection certificate (menu: IPsec VPN >> Connections >> (Edit), tab *Authentication*).





## 9 Establish an IPsec VPN connection between iOS client and mGuard device



Document-ID: 108393\_en\_02  
 Document-Description: AH DE MGuard IOS SUPPORT  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
 It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

### Contents of this document

This document describes the required steps to configure a VPN connection between the mGuard server and an iOS client (iPad or iPhone with iOS version 8.0 or later).

9.1	Introduction.....	201
9.2	Manage certificates .....	202
9.3	Configure VPN connections .....	208
9.4	Start VPN connections on the iOS client .....	212
9.5	Check VPN connections on the mGuard .....	213

## 9.1 Introduction

The iOS device acts as a remote client that initiates the IPsec VPN connection. The mGuard acts as the local server and configures and provides the local network for the clients via the XAuth/Mode Config extension.

The VPN connections require the installation of X.509 certificates and keys both on the iOS client and the mGuard device.



For general information on how to configure VPN connections, please refer to the “Software Reference Manual – mGuard Firmware”, available [online](https://phoenixcontact.net/products) or in the PHOENIX CONTACT Webshop at: [phoenixcontact.net/products](https://phoenixcontact.net/products). For further information regarding the iOS client, please refer to the corresponding manufacturer's web page.

### 9.1.1 Requirements

- mGuard device with installed firmware 8.5 or later
- iOS device with installed firmware version 8.0 or later
- All required and signed certificates



#### How to obtain X.509 certificates?

For further information about certificate management please refer to the application note "AH EN MGuard APPNOTES“, available in the PHOENIX CONTACT Webshop at: [phoenixcontact.net/products](https://phoenixcontact.net/products).

## 9.2 Manage certificates

To establish an IPsec VPN connection between an iOS client and the mGuard server, the devices need to authenticate each other via X.509 certificates.

Table 9-1 Required certificates

Device	Required certificate	Format
mGuard	CA Certificate	PEM / CER
	mGuard Machine Certificate (signed by CA)	PKCS#12
iOS client	CA Certificate	PEM / CER
	iOS Client Certificate (signed by CA)	PKCS#12

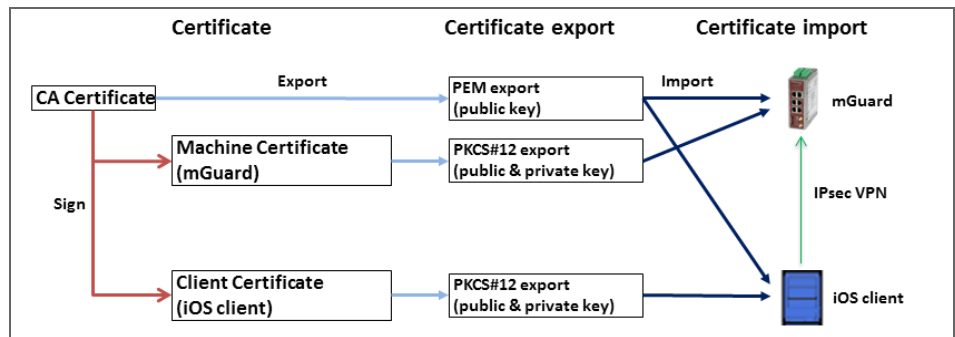


Figure 9-1 Certificate handling for connections initiated by iOS clients



The terms “Machine Certificate” and “Client Certificate” signify an X.509 certificate and it’s corresponding private key by which the machine/client identifies itself to it’s peers.

### 9.2.1 Required certificates on the mGuard device

The following certificates need to be installed on the mGuard device.

#### 1. CA Certificate (PEM / CER)

The mGuard verifies the iOS client on the basis of the iOS Client Certificate signed by the CA Certificate.

#### 2. mGuard Machine Certificate (PKCS#12)

The iOS client verifies the mGuard on the basis of the mGuard Machine Certificate signed by the CA Certificate. The CA Certificate must therefore be installed on the iOS client.



**NOTE: The network address of the mGuard device must be added in the certificate**

When creating the mGuard Machine Certificate, the IP address (or hostname/DNS name) that the iOS client uses to establish a VPN connection with the mGuard device (usually the external server IP address of the mGuard device) must be entered in two places:

- **commonName (CN)** --> see [Figure 9-2](#) and [Figure 9-3](#)
- **X509v3 Subject Alternative Name** --> see [Figure 9-4](#)

Establish an IPsec VPN connection between iOS client and mGuard device

Network » Interfaces

General External Internal DMZ Secondary External

Network Status

External IP address	76.126.21.44
Current default route	10.1.0.254
Used DNS servers	10.7.53.53

Network Mode

Network mode	Router
Router mode	Static

Network » Interfaces

General External Internal DMZ Secondary External

External Networks

Seq.	IP address	Netmask	Use VLAN	VLAN ID
1	76.126.21.44	255.255.255.0	<input type="checkbox"/>	1

Additional External Routes

Figure 9-2 (Example) Network settings on the mGuard: external IP address highlighted

Authentication » Certificates

Certificate Settings Machine Certificates CA Certificates Remote Certificates CRL

Machine Certificates

Seq.	Short name	Certificate details
1	76.126.21.44	<p>Download <input type="checkbox"/> PKCS#12 Password Upload</p> <p><b>Subject:</b> CN=76.126.21.44,O=Phoenix Contact CS,L=Berlin,ST=Germany,C=DE</p> <p><b>Issuer:</b> CN=CA.mGuard,O=Phoenix Contact CS,L=Berlin,ST=Germany,C=DE</p> <p><b>Valid from:</b> Oct 15 12:22:01 2015 GMT</p> <p><b>Valid until:</b> Oct 14 12:19:50 2016 GMT</p> <p><b>Fingerprint MD5:</b> 93:13:61:BA:AC:E2:5F:8D:D1:D9:B3:66:14:10:13:CC</p>

Figure 9-3 Machine Certificate: CN = mGuard's external IP address or DNS name

X Certificate and Key management

Create x509 Certificate

Source Subject **Extensions** Key usage Netscape Advanced

**X509v3 Basic Constraints**

Type: End Entity

Path length: 2

Critical

**Key identifier**

Subject Key Identifier

Authority Key Identifier

**Validity**

Not before: 2017-07-13 07:59 GMT

Not after: 2018-07-10 14:44 GMT

**Time range**

2 Years

Midnight  Local time  No well-defined expiration

X509v3 Subject Alternative Name ✓ IP: 76.125.21.44 Edit

X509v3 Issuer Alternative Name Edit

X509v3 CRL Distribution Points Edit

Authority Information Access OSCP Edit

Cancel OK

Figure 9-4 Machine Certificate: Example (XCA) – X509v3 Subject Alternative Name

### 9.2.2 Required certificates on the iOS client

The following certificates need to be installed on the iOS device (see [page 202](#)).

#### 1. CA Certificate (PEM/CER)

The iOS client verifies the mGuard server on the basis of the mGuard Machine Certificate signed by the CA.

#### 2. iOS Client Certificate (PKCS#12)

The mGuard verifies the iOS client on the basis of the iOS Client Certificate signed by the CA. The signing CA Certificate must therefore be installed on the mGuard.





Because the iOS client ignores the keychain of the PKCS#12 file, the signing CA Certificate must therefore be separately installed on the mGuard.

### 9.2.3 Install certificates on the mGuard device



#### Machine Certificate

To upload the mGuard Machine Certificate to the mGuard, proceed as follows:

1. Select the Menu “Authentication >> Certificate” (Tab “Machine Certificates”)
2. Click the icon  to create a new table row.
3. Click the icon .
4. Choose the Machine Certificate (PKCS#12 file) and click “Open”.
5. Enter the password, that has been used to protect the private key of the certificate.
6. Click the button “Upload”.
  - ▶ The uploaded certificate appears in the certificates list.
7. Click “Apply” to save the settings.
  - ▶ The mGuard Machine Certificate has been uploaded and can be used for authentication towards the iOS client (see „[Configure mGuard](#)“ , “[Tab “Authentication”](#)”).

#### CA Certificate

To upload the CA Certificate to the mGuard, proceed as follows:

1. Select the menu “Authentication >> Certificate” (Tab “CA Certificates”).
2. Click the icon  to create a new table row.
3. Click the icon .
4. Choose the CA Certificate (PEM or CER file) and click “Open”.
5. Click the button “Upload”.
  - ▶ The uploaded certificate appears in the certificates list.
6. Click “Apply” to save the settings.
  - ▶ The CA Certificate has been uploaded and can be used to authenticate the iOS client certificate (see „[Configure mGuard](#)“ , “[Tab “Authentication”](#)”).

## 9.2.4 Install certificates on the iOS client

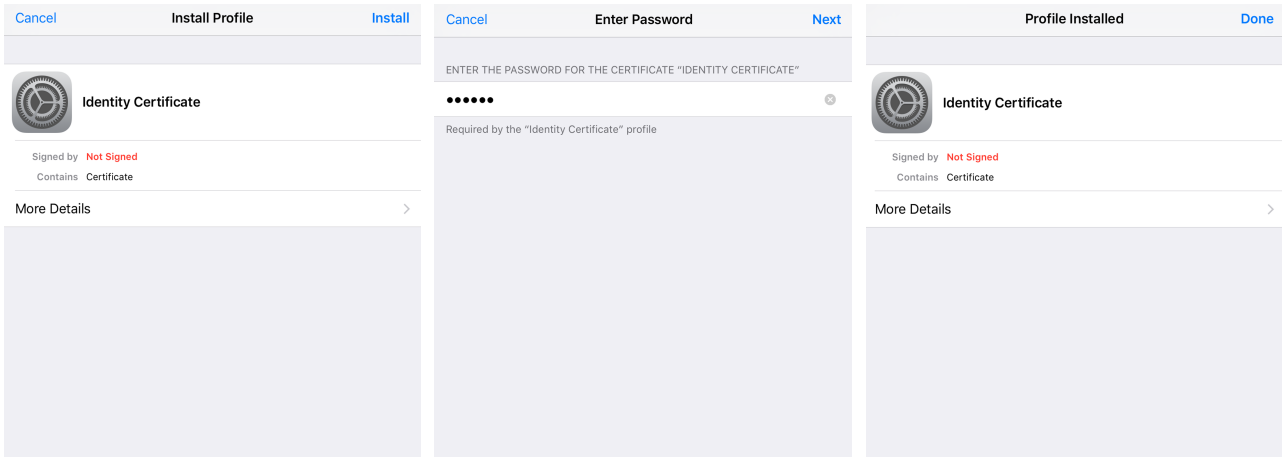


Figure 9-5 Installation of client certificates



Figure 9-6 Installed certificates in the certificate list

To install the iOS Client Certificate or the CA Certificate on the iOS client, proceed as follows:

1. Make the certificate file available on the iOS client.
2. Open the file.
  - ▶ The screen “Install Profile” appears.
3. Click twice on “Install”.
  - ▶ If the certificate has been secured with a secret key (PKCS#12 files), the screen “Enter Password” appears.
4. In this case, enter the password.
5. Click “Next”.
  - ▶ The screen “Profile Installed” appears.
6. Click “Done” to finish the installation of the certificate.
  - ▶ The installed certificate appears in the certificate list.

## 9.3 Configure VPN connections

### 9.3.1 Configure mGuard



The IPsec VPN connection between the iOS client and the mGuard will be established using the XAuth/Mode Config extension. The configuration of the iOS client will be configured by the mGuard and communicated to the iOS client.

The screenshot shows the 'IPsec ModeCfg' configuration page. It has four tabs: 'General', 'Authentication', 'Firewall', and 'IKE Options'. The 'General' tab is active. Under 'Mode Configuration', there are several fields: 'Mode configuration' set to 'Server', 'Local' set to 'From table below', 'Remote' set to 'From the pool below', 'Remote IP network pool' set to '172.16.101.0/24', and 'Tranches of size (network size between 0 and 32)' set to '32'. Below these fields is a table with one row. The table has two columns: 'Seq.' and 'Network'. The first row has '1' in the 'Seq.' column and '172.16.100.0/24' in the 'Network' column. There are plus and trash icons next to the '1' in the 'Seq.' column.

Figure 9-7 mGuard VPN configuration – Mode Configuration

#### 9.3.1.1 Tab “General”

To configure a VPN connection to an iOS client on the mGuard, proceed as follows:

1. Select the menu “IPsec VPN >> Connections”.
2. Click the icon  to create a new table row.
3. Click the icon  “Edit row”.
  - ▶ The tab “General” appears.
4. Enter a descriptive name for the connection and change further settings optionally.



Verify that the input field “Address of the remote site’s VPN gateway” contains the value “%any” and “Connection startup” is set to “Wait” (default values).

5. In section **Mode Configuration** select Mode configuration **Server**.
6. **Local:** Enter the local network(s) on the server side (mGuard) that shall be accessible by the iOS client via VPN connection.
  - **Fixed:** The *Local IP network* must be set to 0.0.0.0/0. In this case, all traffic from the iOS client will be sent over the VPN connection.
  - **From table below:** Only traffic to the *Networks* listed in the *table below* will be sent over the VPN connection. On iOS clients, traffic to networks not listed in the *table below* will bypass the VPN connection.
7. **Remote:** Define the network pool (**From the pool below**) from which the mGuard allocates a variable tranche (**Tranches of size**) to be used by the remote client’s network.

### 9.3.1.2 Tab “Authentication”

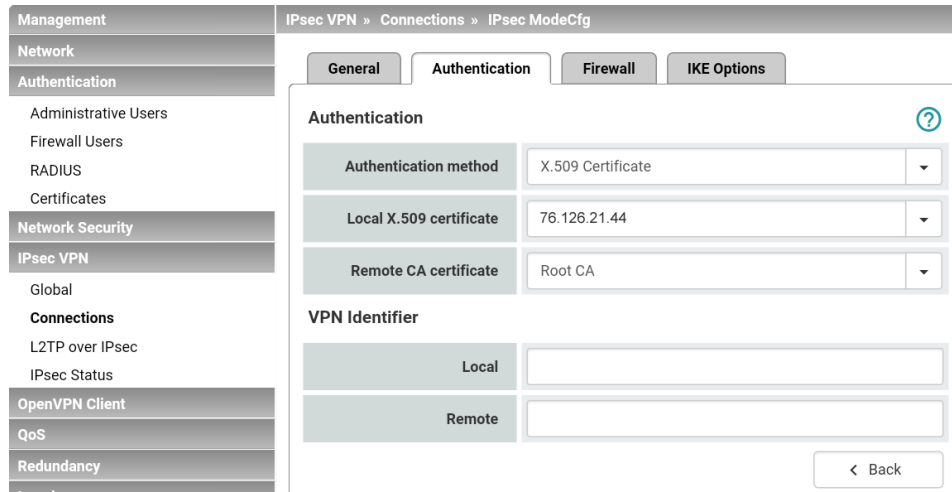


Figure 9-8 mGuard VPN configuration – Authentication

The VPN connection between an iOS client and the mGuard must be authorized by X.509 certificates, that have to be installed on the corresponding devices (see [“Manage certificates” on page 202](#)).

To assign the required certificates to a VPN connection, proceed as follows:

1. Select the menu “IPsec VPN >> Connections”.
2. Edit the desired VPN connection (Tab “Authentication”).
3. Select the **Authentication method** “X.509 Certificate”.
4. As the *Local X.509 certificate* select the **mGuard Machine Certificate**.



The *Common Name (CN)* and *Subject Alternative Name* of the certificate must match the IP address (or host name/DNS name) of the mGuard device that the iOS client uses to establish a VPN connection with the mGuard device (see [Section 9.2.1](#)).



The certificate must have been signed by the CA Certificate that has been installed on the iOS client.

5. As the *Remote CA certificate* select the **CA Certificate** that has been used to sign the **iOS Client Certificate**.
6. Click “Apply” to save the settings.
  - ▶ The VPN connection will be established after being initiated by the iOS client.

### 9.3.1.3 Tab “Firewall”

The VPN firewall restricts the access through the VPN tunnel. You may configure the VPN firewall if required.



By default, **any incoming** and **outgoing** traffic will be accepted.

### 9.3.1.4 Tab “IKE Options”

IPsec VPN » Connections » KBS12000DEM1061

General Authentication Firewall **IKE Options**

**ISAKMP SA (Key Exchange)** ?

Seq.	Encryption	Hash	Diffie-Hellman
1	AES-256	All algorithms	All algorithms

**IPsec SA (Data Exchange)**

Seq.	Encryption	Hash
1	AES-256	SHA-512
2	AES-256	SHA-1

Perfect Forward Secrecy (PFS) (Activation recommended. The remote site must have the same entry.) No

**Lifetimes and Limits**

ISAKMP SA lifetime	12:00:00	seconds (hh:mm:ss)
IPsec SA lifetime	4:00:00	seconds (hh:mm:ss)

It is necessary to change the default IKE options:

1. Select the menu “IPsec VPN >> Connections”.
2. Edit the desired VPN connection (Tab “IKE Options”).
3. Configure the following settings and leave all other settings on default.

#### ISAKMP SA (Key Exchange)

- Encryption: AES-256
- Hash: All algorithms
- Diffie-Hellman: All algorithms

#### IPsec SA (Data exchange)

- Click the icon **+** to create two table rows and use the following settings:
  - (Row 1) Encryption: AES-256 | Hash: SHA-512
  - (Row 2) Encryption: AES-256 | Hash: SHA-1

### 9.3.2 Configure iOS client

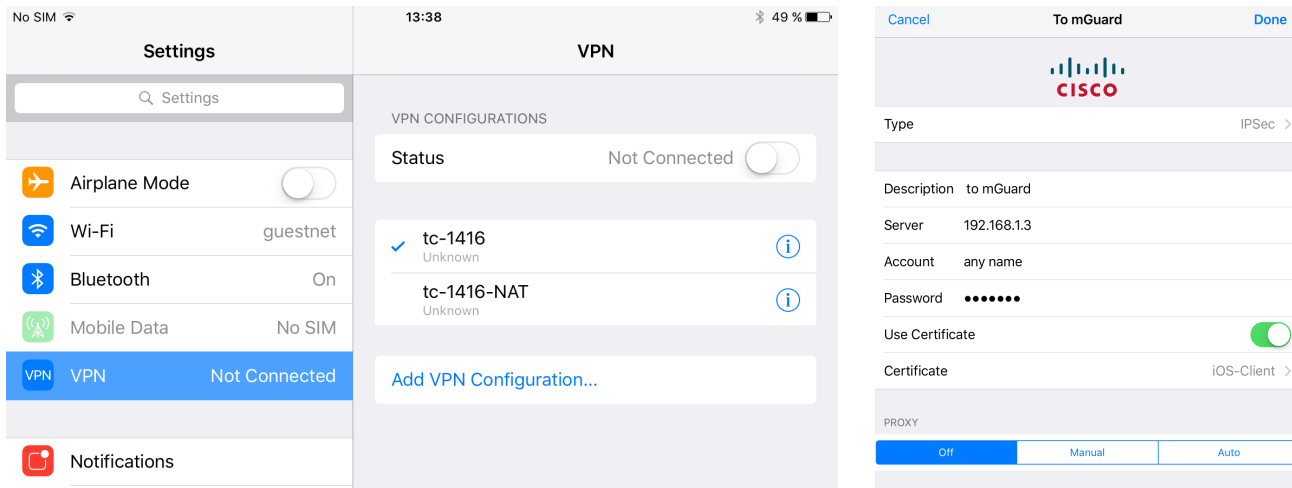


Figure 9-9 iOS client: VPN configuration

To configure an IPsec VPN connection on the iOS client, proceed as follows:

1. Select the menu “Settings >> VPN”.
  2. Click “Add VPN Configuration...”.
  3. Click “Type”.
  4. Select “IPSec” and click “Back”.
  5. Fill out the following input fields:
    - Description: A descriptive name for the connection
    - Server: The external IP address or the DNS name of the mGuard server
- i** This IP address or host name/DNS name must match the *Common Name (CN)* and *Subject Alternative Name* of the mGuard Machine Certificate (see [Section 9.2.1](#)).
- Account: The Authentication of VPN peers relies on certificates. Thus the account name and password will be **ignored by the mGuard**. To avoid ongoing requests, enter some random text.
  - Password: The password will be **ignored by the mGuard**. Enter random text.
  - Use Certificate: To select a certificate, activate the switch.
    6. Click “Certificate”.
      - ▶ A list with all installed certificates appears.
    7. Select the appropriate client certificate and click “Back”.
    8. Click “Done” to save the configuration.
      - ▶ The VPN configuration has been saved and is ready to be started.

## 9.4 Start VPN connections on the iOS client

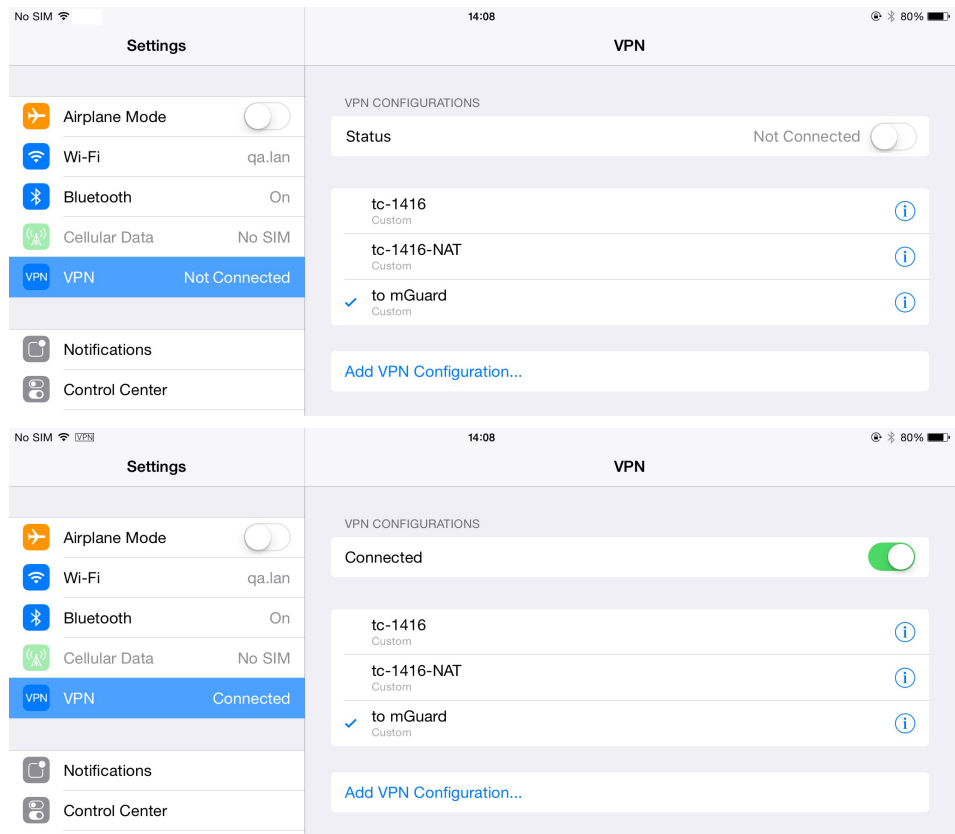


Figure 9-10 Start VPN connection on the iOS client

To start an IPsec VPN connection on the iOS client, proceed as follows:

1. Select the menu “Settings >> VPN”.
2. Click on the name of the appropriate VPN connection.
3. In the area “Status”, click the Button “Not Connected”.
  - ▶ The VPN connection will be established and the status changes from “Not Connected” to “Connected”.




If the connection fails, click the Info icon of the VPN connection to check for errors in the configuration or check your internet connection.


## 9.5 Check VPN connections on the mGuard


IPsec VPN » IPsec Status

**IPsec Status** ?


 **Waiting**

ISAKMP SA	Local	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=76.126.21.44, E=mhopf@phoenixcontact.com	aes-256;(sha1 sha2-512);modp-(1024 1536 2048 3072 4096 6144 8192)
	Remote	%any:500 / (none)	

IPsec SA	IPsec ModeCfg: 172.16.100.0/24...172.16.101.0/24	aes-256;(sha1 sha2-512)	
----------	--	-------------------------	---

 **Pending**

(no entries)

 **Established**

ISAKMP SA	Local	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=76.126.21.44, E=mhopf@phoenixcontact.com	main-r3 replace in 7h 58m 14s (active) <b>aes-256;(sha1 sha2-512);modp-(1024 1536 2048 3072 4096 6144 8192)</b>
	Remote	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=kbe, E=mhopf@phoenixcontact.com	




IPsec SA	IPsec ModeCfg: 172.16.100.0/24... 172.16.101.1/32	quick-r2 replace in 58m 14s (active) <b>aes-256;(sha1 sha2-512)</b>	
		quick-r2 replace in 23m 49s <b>aes-256;(sha1 sha2-512)</b>	
			

Figure 9-11 IPsec VPN status

To check the status of an IPsec VPN connection, proceed as follows:

- Select the menu “IPsec VPN >> IPsec Status”.
  - ▶ An established IPsec VPN connection appears in the area “Established”.



# 10 Establish an IPsec VPN connection between Android client and mGuard device



Document-ID: 108394\_en\_01  
Document-Description: AH DE MGuard ANDROID SUPPORT  
© PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

## Contents of this document

This document describes the required steps to configure a VPN connection between the mGuard server and an Android client (tablet PC or mobile phone with Android OS version 6.0).

10.1	Introduction.....	215
10.2	Manage certificates .....	216
10.3	Configure VPN connections .....	219
10.4	Start VPN connections on the Android client .....	224
10.5	Check VPN connections on the mGuard .....	225

## 10.1 Introduction

The Android device acts as a remote client that initiates the IPsec VPN connection. The mGuard acts as the local server and configures and provides the local network for the clients via the XAuth/Mode Config extension.

The VPN connections require the installation of X.509 certificates and keys both on the Android client and the mGuard device.



For general information on how to configure VPN connections, please refer to the “Software Reference Manual – mGuard Firmware”, available [online](https://phoenixcontact.net/products) or in the PHOENIX CONTACT Webshop at: [phoenixcontact.net/products](https://phoenixcontact.net/products). For further information regarding the Android client, please refer to the corresponding manufacturer's web page.



Settings and user interfaces may look different on different Android devices. They depend on the manufacturer's implementation. The present document was created on the basis of the following device: *SAMSUNG SM-T580* with installed Android version 6.0.1.

### 10.1.1 Requirements

- mGuard device with installed firmware 8.5 or later
- Android device with installed firmware version 6.0
- All required and signed certificates



#### How to obtain X.509 certificates?

For further information about certificate management please refer to the application note X.509 CERTIFICATES, available in the PHOENIX CONTACT Webshop at: [phoenixcontact.net/products](https://phoenixcontact.net/products).

## 10.2 Manage certificates

To establish an IPsec VPN connection between an Android client and the mGuard server, the devices need to authenticate each other via X.509 certificates.

Table 10-1 Required certificates

Device	Required certificate	Format
mGuard	CA Certificate	PEM / CER
	mGuard Machine Certificate (signed by CA)	PKCS#12
Android client	mGuard Machine Certificate (signed by CA)	PEM / CER
	Android Client Certificate (signed by CA)	PKCS#12

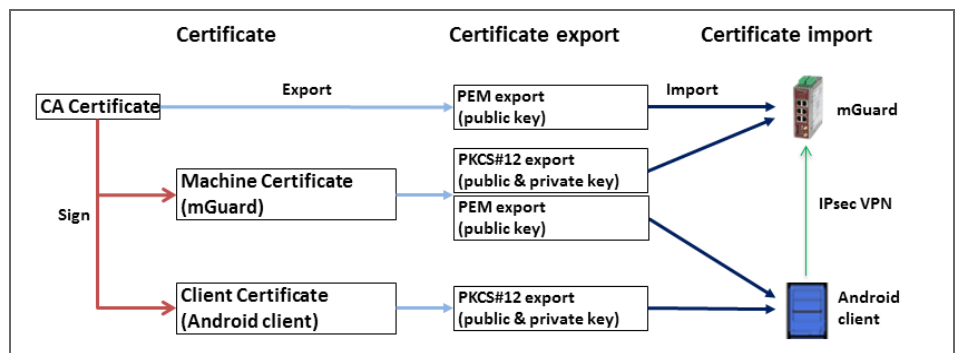


Figure 10-1 Certificate handling for connections initiated by Android clients



The terms “Machine Certificate” and “Client Certificate” signify an X.509 certificate and it’s corresponding private key by which the machine/client identifies itself to it’s peers.

### 10.2.1 Required certificates on the mGuard device

The following certificates need to be installed on the mGuard device.

#### mGuard Machine Certificate (PKCS#12)

The **Android client** verifies the mGuard on the basis of the mGuard Machine Certificate. The mGuard Machine Certificate must therefore be installed on the Android client.

### 10.2.2 Required certificates on the Android client

The following certificates need to be installed on the Android device (see [page 216](#)).

#### 1. mGuard Machine Certificate (PEM/CER)

The Android client verifies the mGuard server on the basis of the mGuard Machine Certificate.



#### 2. Android Client Certificate (PKCS#12)

The mGuard verifies the Android client on the basis of the Android Client Certificate signed by the CA. The signing CA Certificate must therefore be installed on the mGuard.

### 10.2.3 Install certificates on the mGuard device



#### Machine Certificate

To upload the mGuard Machine Certificate to the mGuard, proceed as follows:

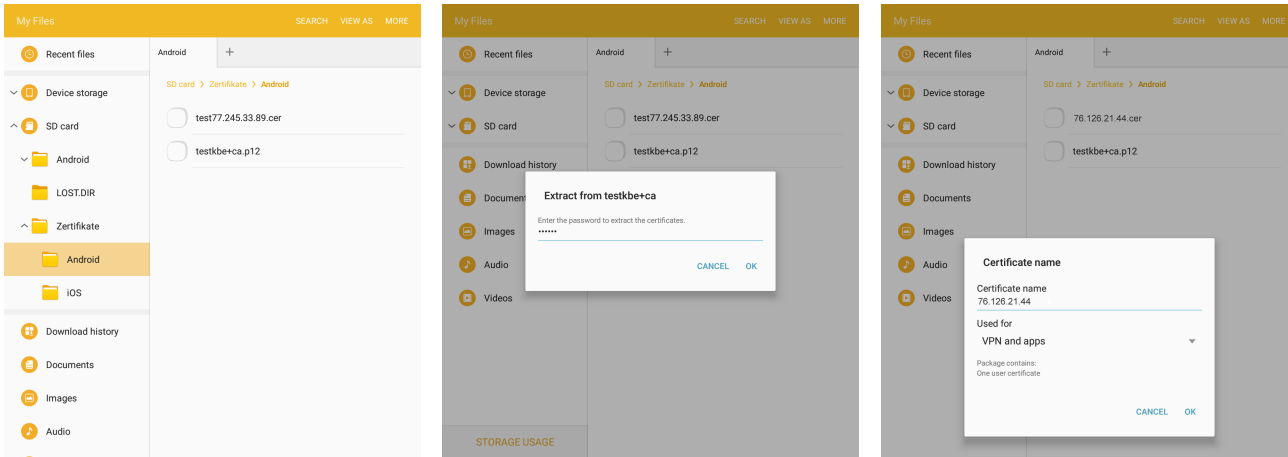
1. Select the menu **Authentication >> Certificates >> Machine Certificates**.
2. Click the icon  to create a new table row.
3. Click the icon .
4. Choose the Machine Certificate (PKCS#12 file) and click “Open”.
5. Enter the password, that has been used to protect the private key of the certificate.
6. Click the button “Upload”.
  - ▶ The uploaded certificate appears in the certificates list.
7. Click “Apply” to save the settings.
  - ▶ The mGuard Machine Certificate has been uploaded and can be used for authentication towards the Android client (see „[Configure the mGuard](#)“, “[Tab “Authentication”](#)”).

#### CA Certificate

To upload the CA Certificate to the mGuard, proceed as follows:

1. Select the menu **Authentication >> Certificates >> CA Certificates**.
2. Click the icon  to create a new table row.
3. Click the icon .
4. Choose the CA Certificate (PEM or CER file) and click “Open”.
5. Click the button “Upload”.
  - ▶ The uploaded certificate appears in the certificates list.
6. Click “Apply” to save the settings.
  - ▶ The CA Certificate has been uploaded and can be used to authenticate the Android client certificate (see „[Configure the mGuard](#)“, “[Tab “Authentication”](#)”).

## 10.2.4 Install certificates on the Android client



To install the **Android Client Certificate** (PKCS#12 file with signing CA certificate) and the **mGuard Machine Certificate** (PEM / CER file) on the Android client, proceed as follows:

1. To use the VPN feature on the Android device, you must set the screen lock type pattern, PIN, or password.
2. Make the certificate files available on the Android client.
3. Open the PKCS#12 file (\*.p12) to extract and install the Android Client and signing CA Certificates.
  - ▶ The screen “Extract from <certificate name>” appears.



If the screen does not appear and the device displays the content of the file instead, download the file to the storage of your device or make it available via SD card. Open the file from the corresponding directory.

4. Enter the password and click “OK”.
  - ▶ The screen “Certificate name” appears.
5. Optional: Assign a new name to the certificate to easily locate the certificate in the certificate list.
6. Click “OK” to finish the installation of the Android Client and signing CA Certificate.
  - ▶ The installed certificates appear in the user certificates list (Apps >> Settings >> Lock screen and security >> Other security settings >> User certificates).
7. Open the PEM or CER file (\*.pem / \*.cer) to install the mGuard Machine Certificate.
  - ▶ The screen “Certificate name” appears.



If the screen does not appear and the device displays the content of the file instead, download the file to the storage of your device or make it available via SD card. Open the file from the corresponding directory.

8. Click “OK” to finish the installation of the mGuard Machine Certificate.
  - ▶ The installed certificate appears in the user certificates list (Apps >> Settings >> Lock screen and security >> Other security settings >> User certificates).

## 10.3 Configure VPN connections

### 10.3.1 Configure the mGuard

The IPsec VPN connection between the Android client and the mGuard will be established using the XAuth/Mode Config extension. The configuration of the iOS client will be configured by the mGuard and communicated to the iOS client.

The screenshot shows the 'IPsec ModeCfg' configuration page. At the top, there are tabs for 'General', 'Authentication', 'Firewall', and 'IKE Options'. The 'General' tab is selected. Below the tabs, the 'Mode Configuration' section contains several fields: 'Mode configuration' is set to 'Server', 'Local' is set to 'From table below', and 'Remote' is set to 'From the pool below'. Below these fields is a table with one row: 'Seq.' 1 and 'Network' 172.16.100.0/24. Below the table, there are fields for 'Remote IP network pool' (172.16.101.0/24) and 'Tranches of size (network size between 0 and 32)' (32).

Figure 10-2 mGuard VPN configuration – Mode Configuration

#### 10.3.1.1 Tab “General”

To configure a VPN connection to an Android client on the mGuard, proceed as follows:

1. Select the menu “IPsec VPN >> Connections”.
2. Click the icon to create a new table row.
3. Click the icon “Edit row”.
  - ▶ The tab “General” appears.
4. Enter a descriptive name for the connection and change further settings optionally.



Verify that the input field “Address of the remote site’s VPN gateway” contains the value “%any” and “Connection startup” is set to “Wait” (default values).

5. In section **Mode Configuration** select Mode configuration **Server**.
6. **Local:** Enter the local network(s) on the server side (mGuard) that shall be accessible by the Android client via VPN connection.
  - **Fixed:** The *Local IP network* must be set to 0.0.0.0/0. In this case, all traffic from the Android client will be sent over the VPN connection.
  - **From table below:** Only traffic to the *Networks* listed in the *table below* will be send over the VPN connection.



Android clients do not fully support this feature. Traffic from Android clients to networks not defined in the *table below* **will be blocked!**

7. **Remote:** Define the network pool (**From the pool below**) from which the mGuard allocates a variable tranche (**Tranches of size**) to be used by the remote client's network.

### 10.3.1.2 Tab “Authentication”

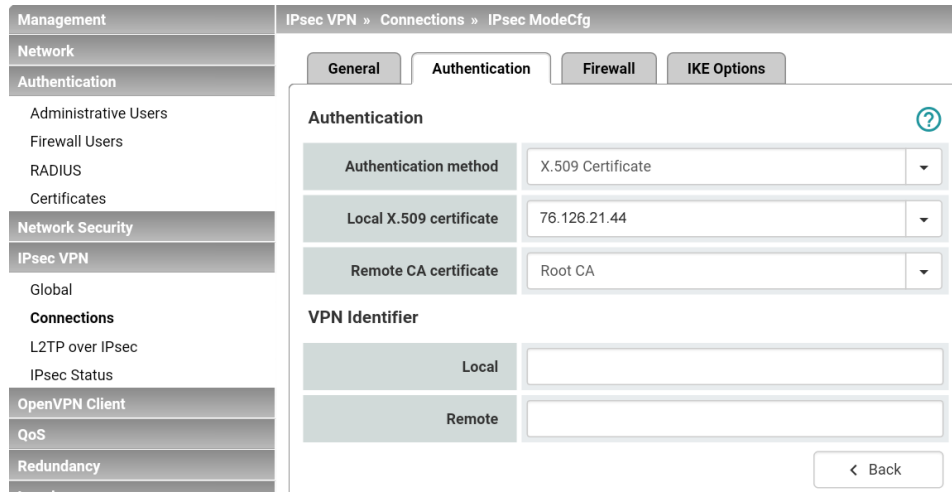


Figure 10-3 mGuard VPN configuration – Authentication

The VPN connection between an Android client and the mGuard must be authorized by X.509 certificates, that have to be installed on the corresponding devices (see [“Manage certificates” on page 216](#)).

To assign the required certificates to a VPN connection, proceed as follows:

1. Select the menu “IPsec VPN >> Connections”.
2. Edit the desired VPN connection (Tab “Authentication”).
3. Select the **Authentication method** “X.509 Certificate”.
4. As the *Local X.509 certificate* select the **mGuard Machine Certificate**.



**Only for connections from iOS clients:** The CN of the certificate must correspond with the external IP address or DNS name of the mGuard server.



The certificate must have been signed by the CA Certificate that has been installed on the Android client.

5. As the *Remote CA certificate* select the **CA Certificate** that has been used to sign the **iOS Client Certificate** and the **Android Client Certificate**.
6. Click “Apply” to save the settings.
  - ▶ The VPN connection will be established after being initiated by the Android client.

### 10.3.1.3 Tab “Firewall”

The VPN firewall restricts the access through the VPN tunnel. You may configure the VPN firewall if required.



By default, **any incoming** and **outgoing** traffic will be accepted.

### 10.3.1.4 Tab “IKE Options”

IPsec VPN » Connections » KBS12000DEM1061

General Authentication Firewall **IKE Options**

**ISAKMP SA (Key Exchange)** ?

Seq.	Encryption	Hash	Diffie-Hellman
1	AES-256	All algorithms	All algorithms

**IPsec SA (Data Exchange)**

Seq.	Encryption	Hash
1	AES-256	SHA-512
2	AES-256	SHA-1

Perfect Forward Secrecy (PFS) (Activation recommended. The remote site must have the same entry.) No

**Lifetimes and Limits**

ISAKMP SA lifetime	12:00:00	seconds (hh:mm:ss)
IPsec SA lifetime	4:00:00	seconds (hh:mm:ss)


It is necessary to change the default IKE options:

1. Select the menu “IPsec VPN >> Connections”.
2. Edit the desired VPN connection (Tab “IKE Options”).
3. Configure the following settings and leave all other settings on default.

#### ISAKMP SA (Key Exchange)

- Encryption: AES-256
- Hash: All algorithms
- Diffie-Hellman: All algorithms

#### IPsec SA (Data exchange)

- Click the icon  to create two table rows and use the following settings:
  - (Row 1) Encryption: AES-256 | Hash: SHA-512
  - (Row 2) Encryption: AES-256 | Hash: SHA-1

#### Perfect Forward Secrecy (PFS)

- The PFS must be set to **No**.  
(Even if set to **No**, iOS clients will still be able to use PFS.)

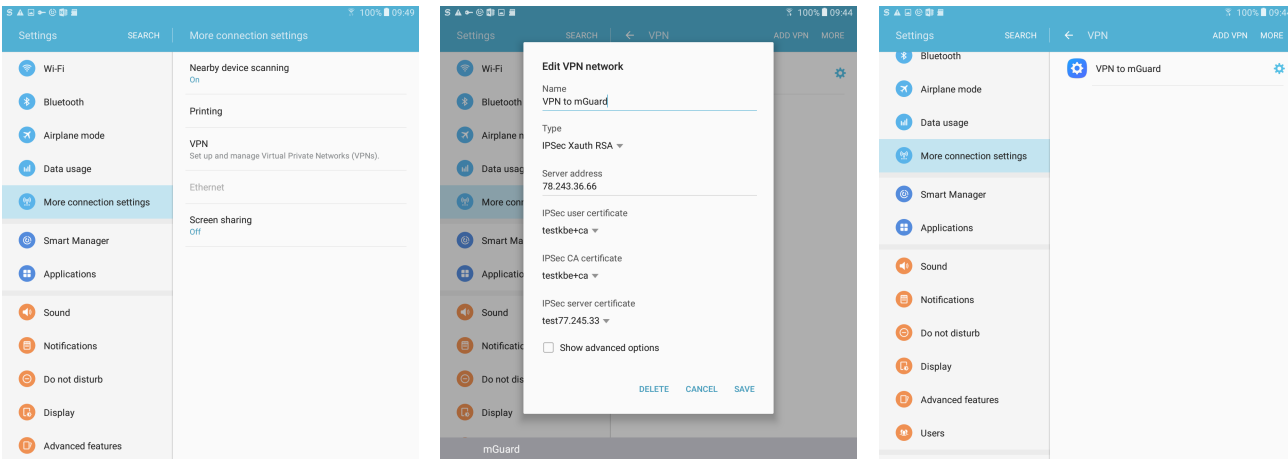
#### ISAKMP SA lifetime

- 12:00:00 (hh:mm:ss)

#### IPsec SA lifetime

- 04:00:00 (hh:mm:ss)

### 10.3.2 Configure the Android client



To configure an IPsec VPN connection on the Android client, proceed as follows:

1. Select the menu “Settings >> More connection settings >> VPN”.
2. Click “ADD VPN” or “+”.
  - ▶ The screen “Edit VPN network” appears.
3. Configure the following settings:
  - Name: A descriptive name for the connection
  - Type: IPsec Xauth RSA
  - Server address: The external IP address or the DNS name of the mGuard server
  - IPsec user certificate: Select the name you have assigned to the Android Client Certificate from the PKCS#12 file.
  - IPsec CA certificate: Select the name you have assigned to the Android Client Certificate from the PKCS#12 file.
  - IPsec Server certificate: Select the name you have assigned to the mGuard Machine Certificate of the mGuard server (VPN gateway).
4. Click “Save” to save the configuration.
  - ▶ The VPN configuration has been saved and is ready to be started.

## 10.4 Start VPN connections on the Android client

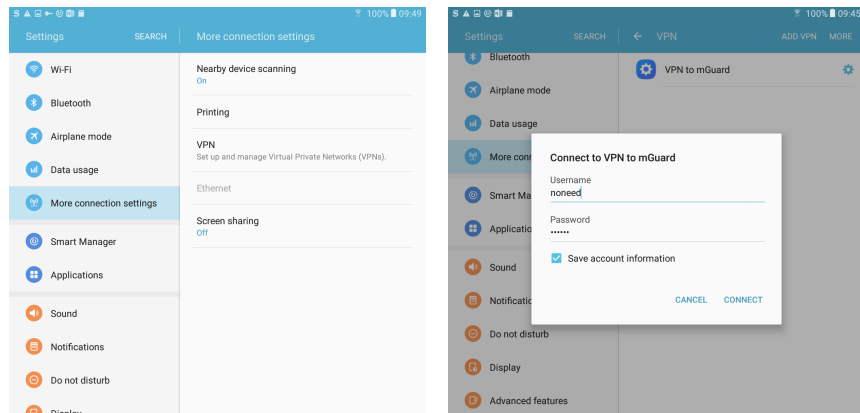


Figure 10-4 Start VPN connection on the Android client

To start an IPsec VPN connection on the Android client, proceed as follows:

1. Select the menu “Apps >> Settings >> More connection settings >> VPN”.
2. Click on the name of the appropriate VPN connection.
  - ▶ The screen “Connect to <connection name>” appears.



The username and password for Xauth will be ignored by the mGuard. Enter some random text and save the account information.

3. Click “CONNECT” to start the connection.
  - ▶ The VPN connection will be established and the status changes from “Not Connected” to “Connecting...” to “Connected”.





If the connection fails, click the “gear” symbol of the VPN connection to check for errors in the configuration or check your internet connection.


## 10.5 Check VPN connections on the mGuard

IPsec VPN » IPsec Status


**IPsec Status** ?

 **Waiting**

ISAKMP SA	Local	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=76.126.21.44, E=mhopf@phoenixcontact.com	aes-256;(sha1 sha2-512);modp-(1024 1536 2048 3072 4096 6144 8192)
	Remote	%any:500 / (none)	
IPsec SA		IPsec ModeCfg: 172.16.100.0/24...172.16.101.0/24	aes-256;(sha1 sha2-512) 

 **Pending**

(no entries)

 **Established**




ISAKMP SA	Local	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=76.126.21.44, E=mhopf@phoenixcontact.com	main-r3 replace in 7h 58m 14s (active) aes-256;(sha1 sha2-512);modp-(1024 1536 2048 3072 4096 6144 8192)
	Remote	76.126.21.44:500 / C=DE, ST=Germany, L=Berlin, O=PHOENIX CONTACT Cyber Security AG, OU=IPsec ModeCfg Test Dept., CN=kbe, E=mhopf@phoenixcontact.com	
IPsec SA		IPsec ModeCfg: 172.16.100.0/24... 172.16.101.1/32	quick-r2 replace in 58m 14s (active) aes-256;(sha1 sha2-512)  quick-r2 replace in 23m 49s aes-256;(sha1 sha2-512)  

Figure 10-5 IPsec VPN status

To check the status of an IPsec VPN connection, proceed as follows:

- Select the menu “IPsec VPN >> IPsec Status”.
  - ▶ An established IPsec VPN connection appears in the area “Established”.



# 11 Update the mGuard configuration using pull configuration



Document-ID: 108398\_en\_01  
 Document-Description: AH EN MGUARD PULLCONFIG  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
 It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

## Contents of this document

This document describes how to perform pull configuration for your mGuard device. It also describes how to obtain pull-config feedback from the server logs.

11.1	Introduction.....	227
11.2	Configure pull configuration on the mGuard device .....	227
11.3	Pull configuration using mdm .....	228
11.4	Obtain pull configuration feedback from server logs .....	228

## 11.1 Introduction

An mGuard device can automatically “retrieve” new configuration profiles from a configuration pull server (*pull configuration*), provided that the corresponding profiles (with file extension *.atv*) have been stored there.

New configurations can be created and stored on the pull server using the mGuard device manager (mdm / FL MGUARD DM). The intervals at which new configurations are “retrieved” from the pull server can be configured on the mGuard device.

## 11.2 Configure pull configuration on the mGuard device

Proceed as follows to configure pull configuration on the mGuard device:

1. Log on to the web interface of the mGuard device.
2. Open **Management >> Central Management** (see also [mGuard firmware manual](#)).
3. Specify a schedule for the mGuard device to send a request to the pull server (*pull request*).
4. Make other settings, if required.

At the specified intervals, the mGuard device will attempt to “retrieve” new configurations from the pull server.

## 11.3 Pull configuration using mdm

Pull configuration (*pull configuration*) is one method for updating the configurations or the firmware version of an mGuard device using the mGuard device manager (mdm / FL MGuard DM).

The configurations created in the mdm are first exported to the pull server and later “retrieved” by the mGuard device or uploaded to the device (see also [mdm software manual](#)).

The mGuard device sends the status of its configuration as a HTTP(S) request on every request to the pull server. The pull server then sends a SYSLOG message to the mdm server (*pull feedback*) in order to inform the mdm server about the configuration status of the mGuard device.

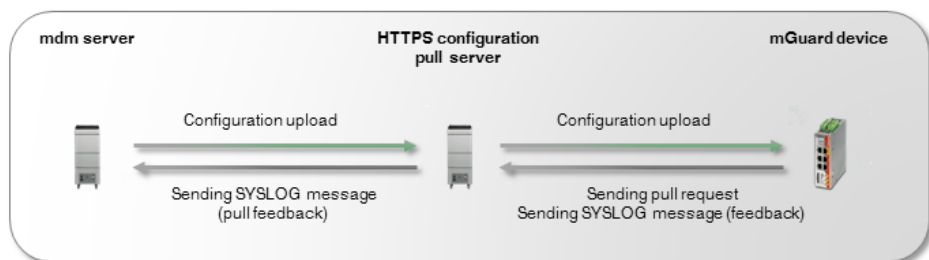


Figure 11-1 Pull configuration using mdm

Configure the mdm server to be able to receive SYSLOG messages from the HTTPS pull server.



Please make sure that neither the network connection between the HTTPS pull server and the mdm server nor the network connection between the HTTPS pull server and the mGuard device is blocked by a firewall or a NAT router.

## 11.4 Obtain pull configuration feedback from server logs

In the event that communication from the configuration pull server to the mdm server is blocked due to firewall or NAT settings, the status of a *configuration pull* can also be obtained from the log entries of the pull server.

When an mGuard device retrieves a new configuration from the pull server, the mGuard device returns specific parameters (e.g., update status) as pull configuration feedback (*pull feedback*) in the form of an URL to the pull server (see the following [Examples](#) and [Table 11-1](#)). The pull server logs can be evaluated to verify whether the configuration pull was successful.

### Examples

#### 1. Configuration applied successfully:

```
"GET
//atv//00000001.atv?a=8.6.0.default&b=N205414313033131033abebcefcfcecc&
c=2031420608&d=e2adce0a1edd2c72e1910303f9d86925&e=0&f=-&g=-&k=-
&i=0&j=0&z=1670 HTTP/1.1"
```

**2. Invalid configuration** (because of missing license for an activated function):

```
"GET
//atv//00000001.atv?a=8.6.0.default&b=N205414313033131033abebcefcfcefcfc&
c=2031420608&d=e2adce0a1edd2c72e1910303f9d86925&e=5&f=-&g=-&k=-
&i=0&j=0&z=71de HTTP/1.1"
```

Table 11-1 List of HTTP(S) request parameters evaluated by the mGuard device manager (mdm)

Parameter	Meaning	Status	Description
<b>a</b>	mGuard firmware version		Firmware version currently installed on the mGuard device
<b>b</b>	mGuard Flash ID		Flash ID of the mGuard device
<b>c</b>	mGuard device serial number		Serial number of the mGuard device
<b>d</b>	md5 hash of mGuard configuration		md5 hash value of the configuration currently used on the mGuard device
<b>e</b>	Update status of mGuard configuration ( <i>configuration pull</i> )	<b>0</b>	The configuration on the mGuard device has been successfully updated.
		<b>1</b>	No update: The configuration on the mGuard device already is up to date.
<b>e</b>		<b>2</b>	No update: The new configuration could not be applied on the mGuard device. The previous configuration was restored ( <i>rollback</i> ).
		<b>3</b>	No update: The mGuard blocks the new configuration because it was restored ( <i>rollback</i> ) during a previous application attempt.
		<b>4</b>	No update: It was not possible to buffer the old configuration on the mGuard device for restoring ( <i>rollback</i> ) it later, which might be required.
		<b>5</b>	No update: The configuration that was to be used to update the mGuard device is invalid.
		<b>-</b>	No update: The configuration on the device should not be updated.
<b>f</b>	Status of the mGuard firmware update	<b>0</b>	The firmware update on the mGuard device was executed successfully.
		<b>-</b>	No update: A firmware update should not be executed on the device.

Table 11-1 List of HTTP(S) request parameters evaluated by the mGuard device manager (mdm)

		<b>Any other character</b>	No update: Firmware update failed
<b>g</b>	Status of license download	<b>0</b>	One or more licenses have been successfully installed on the mGuard device.
		-	A license should not be installed on the device.
		<b>Any other character</b>	Installation of the license failed
<b>k</b>	Status of <i>key renewal</i>	<b>0</b>	The keys ( <i>ssh</i> and <i>https</i> ) on the mGuard device have been successfully renewed.
		<b>1</b>	Key renewal failed
		<b>2</b>	Key renewal has not been executed Renewal is recommended because the current key might not be appropriately secure.
		-	Key renewal has not been executed

**Further parameters (currently not guaranteed)**

- **h** = Device type information; currently only set for NAT router devices. “h” is not transmitted on other devices.
- **i** = Redundancy: status of the password for *availability check*.
- **j** = Redundancy: status of the password for encryption of the network traffic between synchronized mGuard devices.
- **z** = 4 MSB (*Most Significant Bytes*) of the md5 hash value of meta information – without leading “?” and final “&” – but with linefeed character (0x0A) appended.

## 12 Using the CGI Interface



Document-ID: 108416\_en\_01  
 Document-Description: AH EN MGuard CGI INTERFACE  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
 It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

### Contents of this document

This document describes the usage of the CGI interfaces (additional HTTPS interfaces) of the mGuard device.

12.1	Introduction.....	231
12.2	Usage.....	232
12.3	Preconditions and restrictions .....	235
12.4	Interface <code>nph-vpn.cgi</code> .....	236
12.5	Interface <code>nph-diag.cgi</code> .....	251
12.6	Interface <code>nph.action.cgi</code> .....	253
12.7	Interface <code>nph.status.cgi</code> .....	255

### 12.1 Introduction

The additional HTTPS interfaces are implemented as CGI (Common Gateway Interface) scripts, providing the following features and functionality.

Some commands are executed synchronously: they indicate the success or failure of their operation with their return code. When a VPN connection is to be established, also the progress is displayed with every significant step.

#### **`nph-vpn.cgi` / `nph-diag.cgi`**

- Accessible from a conventional HTTPS client.
- Enable/disable a VPN connection.
- Retrieve the connection status of a VPN connection.
- Triggering a "download test" in order to check whether the mGuard is able to download a configuration file from a specified HTTPS server.
- Retrieve firmware version and hardware revision of the mGuard.
- Download a support snapshot.

#### **`nph-action.cgi` / `nph-status.cgi`**

The CGI interfaces `nph-action.cgi` and `nph-status.cgi` provide an extended range of features and functionality (see [Section 12.6](#), "Interface `nph.action.cgi`" and [Section 12.7](#), "Interface `nph.status.cgi`").

## 12.2 Usage

The CGI scripts on the mGuard can be accessed via HTTPS through the same IP addresses and port on which the web interface is available. Only a different URL has to be used. Each access to a CGI script executes a single particular command. Each command responds with an UTF-8 text in the body of the HTTP reply, except for the command *snapshot*, which returns binary data. Some error conditions are signaled within the SSL respectively within the HTTP response. For example, an authorization failure is indicated by HTTP status code 401.

### 12.2.1 Available commands

#### nph-vpn.cgi / nph-diag.cgi

Table 12-1 Commands provided by the CGI scripts *nph-vpn.cgi* and *nph-diag.cgi*

CGI script	Command	Purpose
nph-vpn.cgi	<i>synup</i>	Activate a VPN connection (synchronous command)
	<i>syndown</i>	Deactivate a VPN connection (synchronous command)
	<i>synstat</i>	Determine the status of a VPN connection (synchronous command)
	<i>sysinfo</i>	Retrieve firmware version and hardware revision of the mGuard
	<i>up</i>	Enable a VPN connection (asynchronous command)
	<i>down</i>	Disable a VPN connection (asynchronous command)
	<i>status</i>	Determine the status of a VPN connection (asynchronous command)
	<i>clear</i>	Clears the instance of a VPN connection
nph-diag.cgi	<i>testpull</i>	Trigger a “download test” from an HTTPS server
	<i>snapshot</i>	Download a snapshot from the mGuard

#### nph-action.cgi / nph-status.cgi

For commands provided by the CGI scripts *nph-action.cgi* and *nph-status.cgi* see [Section 12.6, “Interface nph.action.cgi”](#) and [Section 12.7, “Interface nph.status.cgi”](#).

## 12.2.2 Command syntax



Using the command line tool *wget* only functions in combination with mGuard firmware versions < 8.4.0. From mGuard firmware Version 8.4.0, the command line tool *curl* can be used (parameters and options differ!).

Example:

```
wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"
curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"
```

The option `--no-check-certificate` (*wget*) or `--insecure` (*curl*) ensures that the HTTPS certificate on the mGuard does not undergo any further checking.

**The command line has the following syntax when using the utility *wget*:**

```
wget [...] 'https://MGUARD/CGI-SCRIPT?cmd=COMMAND'
wget [...] 'https://MGUARD/CGI-SCRIPT?cmd=COMMAND&name=VPN_NAME'
wget [...] 'https://MGUARD/CGI-SCRIPT?cmd=COMMAND&channel=LNET_RNET'
```

**The command line has the following syntax when using the utility *curl*:**

```
curl [...] 'https://MGUARD/CGI-SCRIPT?cmd=COMMAND'
curl [...] 'https://MGUARD/CGI-SCRIPT?cmd=COMMAND&name=VPN_NAME'
curl [...] 'https://MGUARD/CGI-SCRIPT?cmd=COMMAND&channel=LNET_RNET'
```

Table 12-2 Command syntax

wget [...] or curl [...]	Utility used to issue the HTTPS request and the required arguments. Please refer to the manual of the utility.
<b>MGUARD</b>	IP address and port number on which the mGuard listens for incoming HTTPS requests. The IP address may be preceded by username and password.  <b>[&lt;Username&gt;:&lt;Password&gt;@]&lt;IP Address&gt;[:&lt;Port&gt;]</b>  Example: admin:mGuard@192.168.1.254:443
<b>CGI-SCRIPT</b>	Name of the CGI script to be called, either <i>nph-vpn.cgi</i> or <i>nph-diag.cgi</i> .
<b>COMMAND</b>	Command to be executed, described in the following pages.
<b>VPN_NAME</b>	Name of the VPN connection to be enabled or disabled or which status is to be retrieved. Commands: <i>synup</i> , <i>syndown</i> , <i>synstat</i> , <i>up</i> , <i>down</i> , <i>status</i> .
<b>LNET_RNET</b>	Local and remote VPN network. Commands: <i>status</i> , <i>clear</i> .

### Examples

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synup&name=Service'
curl [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synup&name=Service'
```



- Under Linux and other UNIX operating systems the string beginning with https:// starts and ends with single quote ('). For other operating systems, like for example Windows, double quotes (") may be used.
- Special characters, like a space, must be quoted according to the URL encoding rules if the VPN name contains such characters.
- If the URL includes the password as shown in the examples above, be aware that an intruder may read the password from the process list or the command line history. It could be advisable to use the user with the username *user*. This user has the rights to enable or disable a VPN connection or to retrieve its status by calling the CGI scripts described in this document, but this user has neither the rights to log onto the mGuard via HTTPS or SSH, nor to apply changes to the configuration.

### 12.2.3 Access rights

Table 12-3 Access rights

Command	User				
	root	admin	user	netadmin	audit
<i>up, down, synup, syn-down</i>	x	x	x	-	-
<i>status, synstat, sysinfo</i>	x	x	x	x	x
<i>status &amp; channel, clear (central VPN gateway)</i>	x	x	-	-	-
<i>testpull, snapshot</i>	x	x	-	-	-

## 12.3 Preconditions and restrictions



When executing the CGI scrips *nph-vpn.cgi*, *nph-diag.cgi*, *nph-status.cgi* and *nph-action.cgi*, only the following characters may be used in user names, passwords, and other user-defined names (for example, the name of a VPN connection):

- Letters: A - Z, a - z
- Digits: 0 - 9
- Special characters: - . \_ ~

If other special characters, such as "space" or the "question mark", are used, they must be encoded accordingly (URL encoding).



Using the command line tool *wget* only functions in combination with mGuard firmware versions < 8.4.0. From mGuard firmware Version 8.4.0, the command line tool *curl* can be used (parameters and options differ!).

Example:

```
wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"
curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"
```

The option `--no-check-certificate` (*wget*) or `--insecure` (*curl*) ensures that the HTTPS certificate on the mGuard does not undergo any further checking.

### 12.3.1 Preconditions

The commands *synup*, *syndown*, *up* and *down* can only be used to trigger a VPN connection if it is configured as follows:

1. The VPN connection is disabled (menu **IPsec VPN >> Connections**).
2. At least one VPN tunnel of the VPN connection is enabled (menu **IPsec VPN >> Connections**, tab *General*, section *Transport and Tunnel Settings*).
3. Connection startup must be set to *Initiate* or *Initiate on traffic* (menu **IPsec VPN >> Connections**, tab *General*, section *Options*).

### 12.3.2 Restrictions

- Commands which are executed via the CGI interface may conflict with other activities of the mGuard and with other commands executed through different interfaces.
- A VPN connection should be triggered either by CMD contact or by the CGI interface. A combination of both is not supported.
- The commands *synup*, *syndown*, *up* and *down* are not supported for VPN connections which wait (*Connection startup = Wait*) for incoming VPN connections.
- The CGI interface should not be used during a firmware update or a restart of the mGuard.

## 12.4 Interface `nph-vpn.cgi`

### 12.4.1 `cmd=(up|down), name=<VPN name>`

These commands enable or disable the specified VPN connection. The name of the VPN connection must be specified with the parameter *name*.

The return value does not provide any information about the status of the VPN connection due to the asynchronous execution of these commands. Thus these commands should be followed by an execution of the command `status` to determine the status of the VPN connection.

#### Examples:

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=up&name=Service'
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=down&name=Service'
```

These commands return one of the following values in the HTTP reply:

Return value	Meaning
<i>unknown</i>	A VPN connection with the specified VPN name does not exist.
<i>void</i>	The VPN connection is inactive either due to an error or because it was not enabled using the CGI interface.
<i>ready</i>	The VPN connection is ready to establish tunnels or allow incoming queries regarding tunnel establishment.
<i>active</i>	At least one VPN tunnel of the VPN connection is established for the connection.

### 12.4.2 `cmd=status, [name=(<VPN name>|*)]`

This command retrieves, depending on the parameter *name*, the status either

1. of a specified VPN connection (`name=[VPN name]`), or
2. of all configured VPN connections (`name=*`), or
3. of all enabled or via *synup* activated VPN connections (parameter *name* not specified), providing also additional information.

In case of (1) and (2) the command returns one of the following values:

Return value	Meaning
<i>unknown</i>	A VPN connection with the specified VPN name does not exist.
<i>void</i>	The VPN connection is inactive either due to an error or because it was not enabled using the CGI interface.
<i>ready</i>	The VPN connection is ready to establish tunnels or allow incoming queries regarding tunnel establishment.
<i>active</i>	At least one VPN tunnel of the VPN connection is established for the connection.

**12.4.2.1 cmd=status, name=<VPN name>**

This command retrieves the status of the specified VPN connection.

**Example:**

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=status&name=Service1'
```

Return value
<i>active</i>

**12.4.2.2 cmd=status, name=\***

This command retrieves the status of all configured VPN connections.

**Example:**

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=status&name=*'
```

Return value
<i>Service 1: active</i>
<i>Service 2: void</i>

**12.4.2.3 cmd=status (without parameter name)**

This command retrieves the status of all enabled VPN connections, providing also additional information.

**Example:**

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=status'
```

(Parameter *name* not specified)

Return value	
<i>fullname</i>	Service1
<i>name</i>	MAI0003584192_1 instance
<i>leftnet</i>	192.168.1.0/24
<i>leftgw</i>	10.1.0.48
<i>leftnatport</i>	
<i>leftid</i>	O=Innominat, OU=Support, CN=mGuard 3
<i>leftproto</i>	
<i>leftport</i>	
<i>rightnet</i>	192.168.2.0/24
<i>rightgw</i>	77.245.33.67
<i>rightnatport</i>	
<i>rightid</i>	O=Innominat, OU=Support, CN=Central Gateway
<i>rightproto</i>	

Return value	
<i>rightport</i>	
<i>isakmp</i>	6
<i>isakmp-txt</i>	STATE_MAIN_I4 (ISAKMP SA established)
<i>isakmp-ltime</i>	157s
<i>isakmp-algo</i>	3DES_CBC_192-MD5-MODP1536
<i>ipsec</i>	7
<i>ipsec-txt</i>	STATE_QUICK_I2 (sent QI2, IPsec SA established)
<i>ipsec-ltime</i>	25526s
<i>ipsec-algo</i>	3DES_0-HMAC_MD5

The status of the VPN connection *Service2* is not returned in this example because this connection is not enabled.

### 12.4.3 cmd=(synup|synstat|syndown), name=<VPN name>

These commands enable, disable, or retrieve the status of the specified VPN connection. In contrast to the commands *up*, *down*, and *status*, these commands are executed synchronously which means that the operation returns once a certain status has been reached.

The first character of the response indicates whether the operation could be executed successfully. Further information is provided within the rest of the response line. The reply text consists of one line only, except for the command *synup*, which establishes a VPN connection. For this command the returned text contains progress messages about the establishment of the VPN connection and a final message with the overall result.

#### 12.4.3.1 Response message format

Each message has the format: <TYPE> <CODE> <MESSAGE BODY>

TYPE	Message type, one character: P, R or F: <b>P</b> – progress message (command <i>synup</i> only) <b>R</b> – final message, operation terminated successfully <b>F</b> – final message, operation terminated with a failure
CODE	Max. 12 characters, an abbreviation about what was done in this step (for progress messages) respectively what the final result was (for final messages). Please refer to the next chapter.
MESSAGE BODY	A sequence of text fields delimited by blanks. Each field consists of an identifier and a value, separated by an equal sign.  At the beginning of a MESSAGE BODY there is often the field “uptime=...” or “tstamp=...”.  “uptime=” indicates the operation time of the mGuard in seconds, with fractional digits since its last start up.  “tstamp=” indicates the date and time when the message was generated.

**12.4.3.2 Response code**

The response may contain one of the following codes:

<b>Response code</b>	<b>Description</b>
EAMBIGUOUS	The specified name of the VPN connection was ambiguous because there are several VPN connections having the same name.
EBUSY	The called CGI script is currently busy with another task or it is blocked due to a running firmware update.
ECONFPULL	The test download of a configuration profile from the HTTPS server failed.
EINVAL	The CGI command or the parameters contain syntactical errors.
EVLOOKUPGW	The host name of the remote VPN gateway could not be resolved into an IP address.
EVLOOKUPROUT	No route known to the IP address of the remote VPN gateway.
ENOENT	The specified object does not exist (e.g. a VPN connection with the specified name does not exist).
ESYNVPN001	The VPN connection was established successfully but then it was interrupted (e.g. due to a network outage). The connection should be deactivated and established again. Use the command <i>synstat</i> to determine the status of the VPN connection.
EVDIFFALG1	During the handshaking at the beginning of establishing the VPN connection (negotiation of the ISAKMP SA) the devices did not agree on the strength of the keys or the cryptographic algorithms to be used in the first phase.
EVDIFFALG2	During the handshaking at the beginning of the establishment of the VPN connection (negotiation of the IPsec SA) the devices did not agree on the strength of the keys or the cryptographic algorithms to be used in the second phase.
EVIFDOWN	The network interface, through which the VPN connections should be established, does not have an uplink.
EVPEERNOENT1	The remote VPN peer does not know a VPN connection matching the criteria for the first IKE phase (negotiation of the ISAKMP SA). Probably the mGuard's or the peer's configuration is not correct.
EVPEERNOENT2	The VPN peer does not know a VPN connection which matches the criteria for the second IKE phase (negotiation of the IPsec SA). Probably the mGuard's or the peer's configuration is not correct.
EVTOUT1RESP	The mGuard did not receive a response from the remote VPN peer to his first message for establishing the VPN connection.
EVTOUTWRESP	The mGuard did not receive a response from the remote VPN peer after it has responded at least to one message.
OKCONFPULL	The test download of a configuration profile from the HTTPS server succeeded.
OKVACT	The VPN connection was already established when the <i>synup</i> command was called.
OKVDOWN	The VPN connection was disabled successfully.
OKVNOTACT	The VPN connection, which should be disabled by the <i>syndown</i> command, was already disabled.
OKVST1	The status of the specified VPN connection could be retrieved successfully.
OKVUP	The VPN connection could be established successfully.

### 12.4.3.3 cmd=synup

This command enables a VPN connection. The name of the VPN connection must be specified with the parameter name. This command is executed synchronously and returns once a certain status has been reached. The returned text contains progress messages about the establishment of the VPN connection and a final message with the overall result.

**Example:** Activate the VPN connection with the name *Service*

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synup&name=Service'
```

Response:

```
P synup name=Service1
P deviceinfo uptime=9508.73 tstamp= 20120907095258a serial=2004010272 hostname=mguard
P vpnconn uptime=9508.79 id=MAI0003584192 gw=77.245.33.67
P dnslookup uptime=9508.83 ip=77.245.33.67
P routeinfo uptime=9508.87 via=ext1(10.1.0.48) ifstate=up
...
P IKEv1 uptime=9509.33 newstate=main-i2
...
P IKEv1 uptime=9509.88 newstate=main-i4
P IKEv1 uptime=9509.93 isakmp-sa=established id=#13
...
P IKEv1 uptime=9510.31 newstate=quick-i2 dpd=on
P IKEv1 uptime=9510.34 ipsec-sa=established id=#14 msg=IPsec SA 1 out of 1 is established on this side.
R OKVUP uptime=9510.36 msg=The connection is established on this side.
```

When the mGuard executes the command `synup`, it performs the following steps:

1. Resolve the name of the remote VPN gateway into an IP address (if required).
2. Determine the network interface through which the VPN connection should be established and its connectivity.

The results of both steps are reported in the lines *dnslookup* and *routeinfo*. Only if those steps were executed successfully, the mGuard continues establishing the VPN connection. If the mGuard did not receive any response from the remote VPN peer, it sends an *IKE ping* to check its availability and reports the result.

**Response pattern**

A response of the *synup* command consists of several progress messages and a final message with the overall result. The following structure reflects the case of a successful established VPN connection.

Response consisting of progress messages (*P*) and one final message (*R*).

```
P synup name=vpn_name
P deviceinfo uptime=... tstamp=... serial=XXXX hostname=string
P vpnconn uptime=... id=vNNN gw=hostname/IP
P dnslookup uptime=... ip=IP
P routeinfo uptime=... via=IF(IP) ifstate=up/down/error
P IKEv1 uptime=... newstate=status [key=value...] send=...
P IKEv1 uptime=... state=status [key=value ...] rcvd=...
P IKEv1 uptime=... newstate=status
P IKEv1 uptime=... newstate=status [key=value ...] send=...
P IKEv1 uptime=... state=status [key=value ...] rcvd=...
P IKEv1 uptime=... newstate=status
P IKEv1 uptime=... isakmp-sa=status [key=value ...] info=...
P IKEv1 uptime=... newstate=status [key=value...] send=...
P IKEv1 uptime=... state=status [key=value ...] rcvd=...
P IKEv1 uptime=... newstate=status
P IKEv1 uptime=... newstate=status [key=value ...] send=...
P IKEv1 uptime=... ipsec-sa=status [key=value ...] info=...
R OKVUP tstamp=... msg=VPN connection is established.
```

**Progress messages**

The response always starts with the five progress messages *synup*, *deviceinfo*, *vpnconn*, *dnslookup* and *routeinfo*:

<b>synup</b>	Displays the given <i>synup</i> command with its parameter <i>name</i>
--------------	--

<b>deviceinfo</b>	This message displays information about the mGuard. The format of this message is: <b>P deviceinfo uptime=... tstamp=... serial=XXXX hostname=string</b>			
	The meaning of the fields are:			
	uptime=	Operation time of the mGuard since its last start up. The value is displayed in seconds with fractional digits. Example: uptime=75178.32		
	tstamp=	Date and time when the message was generated. Format: YYYYMMDDhhmmssx The date is followed by the time (UTC), and a lowercase letter. The meaning of the letters is as follows:		
		YYYY	4 digits indicating the year	
		MM	2 digits indicating the month	
		DD	2 digits indicating the day in the month	
		hh	2 digits indicating the hour of the day	
		mm	2 digits indicating the minute of the hour	
		ss	2 digits indicating the second of the minute	
		x	Lowercase letter indicating the state of system time and date of the mGuard.	
			a	System time and date are not yet synchronized.
b			System time was set manually or synchronized by means of an imprecise timestamp recorded every 2 hours in the mGuard's file system.	
c	System time is synchronized by the battery buffered real time clock which had been synchronized manually or via NTP once.			
d	System time synchronized with an NTP server once.			
e	System time synchronized frequently with an NTP server.			
If more than one case applies, the last one of the alphabetical order is displayed.				
serial=	Serial number of the device. Spaces are substituted by underscores.			
hostname=	Hostname of the mGuard.			

<b>vpnconn</b>	Particular configuration properties of the VPN connection. The format of this message is as follows: <b>P vpnconn uptime=... id=vNNN gw=hostname/IP</b>	
	The meaning of the fields are:	
	uptime=	Operation time of the mGuard since its last start up. The value is displayed in seconds with fractional digits. Example: uptime=75178.32
	id=	mGuard's internal name of the VPN connection under which the connection is maintained.
	gw=	Remote VPN gateway of the VPN connection.

<b>dnslookup</b>	Result of resolving the host name of the remote VPN peer into an IP address. The format of this message is as follows: <b>P dnslookup uptime=... ip=IP</b>	
	The meaning of the fields are:	
	uptime=	Operation time of the mGuard since its last start up. The value is displayed in seconds with fractional digits. Example: uptime=75178.32
	ip=	IP address of the remote VPN peer.

<b>routeinfo</b>	Network interface, through which the mGuard will try to establish the VPN connection and interface status. The format of this message is as follows: <b>P routeinfo uptime=... via=IF(IP) ifstate=up/down/error</b>		
	The meaning of the fields are:		
	uptime=	Operation time of the mGuard since its last start up. The value is displayed in seconds with fractional digits. Example: uptime=75178.32	
	via=	Network interface, through which the mGuard will try to establish the VPN connection. Possible values are "ext1", "ext2", "int" "dmz0" and "dial-in".	
	ifstate=	Status of the network interface. Possible values are:	
		up	Network interface is ready for operation.
down		Network interface will become ready when traffic arrives that needs to be forwarded through it.	
	error	Network interface is not ready to operate. In this case the <i>synup</i> command will return EVIFDOWN in the final message.	

If the mGuard does not succeed to connect to the remote VPN peer although the previous steps were executed successfully, the mGuard checks with an IKE-ping, whether the remote site answers to IKE messages. The check will be skipped, if IKE messages had already been exchanged with the peer during the connection establishment.

<b>ikeping</b>	Result of the <i>IKE ping</i> . The format of this message is as follows: <b>P ikeping uptime=... to=IP:PORT via=IF response=yes no error</b>	
	The meaning of the fields are:	
	uptime=	Operation time of the mGuard since its last start up. The value is displayed in seconds with fractional digits. Example: uptime=75178.32
	to=	IP address and port number of the <i>IKE ping</i> target.
	via=	Network interface through which the <i>IKE ping</i> was sent. Possible values are: "ext1", "ext2", "int", "dmz0" and "dial-in".
	response=	Tells whether the mGuard has received a reply to the <i>IKE ping</i> in time. Possible values are:
	yes	The mGuard has received a reply from the remote VPN peer.
	no	The mGuard did not receive any reply from the remote VPN peer within a certain period of time.
	error	The mGuard failed to send an <i>IKE ping</i> .

Further progress messages are displayed during the establishment of the VPN connection. A final message will be displayed immediately upon failure.

<b>IKEv1</b>	This message is displayed if:	
	<ul style="list-style-type: none"> <li>– The mGuard has received or sent an IKEv1 packet.</li> <li>– A phase of the connection establishment has been completed.</li> </ul>	
	The message may contain several text fields with values. Some of them may indicate the crypto algorithms that are offered or selected.	
	The format of this message is as follows:	
	<b>P IKEv1 uptime=... newstate=state [key=value ...] send=...</b>	
	<b>P IKEv1 uptime=... state=state [key=value ...] rcvd=...</b>	
	<b>P IKEv1 uptime=... newstate=state</b>	
	<b>P IKEv1 uptime=... isakmp-sa=status id=NN info=... or</b>	
	<b>P IKEv1 uptime=... ipsec-sa=established id=NN info=...</b>	
	The meaning of the fields that may occur is as follows:	
uptime=	Operation time of the mGuard since its last start up. The value is displayed in seconds with fractional digits. For example: uptime=75178.32	
newstate=	Status change during the establishment of the VPN connection. The value is the name of the new status.	
state=	Current status of the VPN connection.	
send=	Details about a sent packet.	
rcvd=	Details about a received packet.	
isakmp-sa=	Completion status of the first phase. Possible values are:	
	established	A new ISAKMP Security Association (ISAKMP SA) has been established.
	reused	A suitable ISAKMP SA had already been established for another VPN connection. It was reused for this one.
ipsec-sa=	Completion status of the second phase. The value is always “ <i>established</i> ”.	
id=	Identifier of the first or the second phase. These identifiers are used by the mGuard internally during runtime. If an ISAKMP SA was reused, this identifier may be used to find the <i>synup</i> command, which established it.	

### Final message

If the VPN connection was established successfully, the command returns either **OKVUP** or **OKVACT**.

Otherwise one of the following values is returned: **EINVAL**, **EAMBIGUOUS**, **ENOENT**, **ESYNVPN001**, **EBUSY**, **EVLOOKUPGW**, **EVLOOKUPROUT**, **EVIFDOWN**, **EVTOUT1RESP**, **EVTOUTWRESP**, **EVDIFFALG1**, **EVDIFFALG2**, **EVPEERNOENT1**, **EVPEERNOENT2**.

Please refer to “[Response code](#)” on page 239 for an explanation about those codes.

#### 12.4.3.4 cmd=synstat

This command retrieves the status of a VPN connection. The name of the VPN connection must be specified with the parameter *name*.

**Example:** Retrieve the status of the VPN connection with the name *Service*

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synstat&name=Service'
```

Response:

```
R OKVST1 id=MAI0003584192 enabled=no activated=yes ike=OK ipsec=OK
```

If the status of the VPN connection could be retrieved successfully, **OKVST1** is returned with the following additional information:

<b>OKVST1</b>	The mGuard succeeded to determine the status of the VPN connection. The format of the message is as follows: <b>R OKVST1 id=id enabled=yesno1 activated=yesno2 ike=stat1 ipsec=stat2</b> The meaning of the fields are:		
	id=	Internal identifier of the VPN connection, which is used by the mGuard at runtime. It is not the configured name of the VPN connection.	
	enabled=	Indicates whether the VPN connection is configured on the mGuard as “enabled” or not. Possible values are:	
		yes	VPN connection is enabled.
		no	VPN connection is disabled.
	activated=	Indicates whether the VPN connection is “temporarily active”, which is the case if the VPN connection was established with the commands <b>synup</b> or <b>up</b> through the <i>CGI-script nph-vpn.cgi</i> or if it was established with the CMD contact. Possible values are:	
		yes	Temporarily active
		no	Not temporarily active
	ike=	Status of the ISAKMP Security Association (ISAKMP SA) which belongs to this VPN connection. The field is only present if the VPN connection is "temporarily active". Possible values are:	
		<b>NAME</b>	The ISAKMP SA is currently being established. The ISAKMP SA is in the state called <b>NAME</b> . The value of <b>NAME</b> differs from the other values “OK”, “EXP” or “DEAD”.
		OK	ISAKMP SA is established and can be used.
		EXP	ISAKMP SA expired. It has not yet been renewed.
		DEAD	ISAKMP SA does not exist for this VPN connection.
ipsec=	Status of the IPsec Security Association (IPsec SA) which belongs to this VPN connection. Displayed only if the VPN connection is "temporarily active". Possible values and their meaning are:		
	<b>NAME</b>	The IPsec SA is currently being established. The IPsec SA is in the state called <b>NAME</b> . The value of <b>NAME</b> differs from the other values “OK”, “EXP” or “DEAD”.	
	OK	IPsec SA is established and can be used.	
	EXP	IPsec SA is expired. It is not yet renewed.	
	DEAD	IPsec SA does not exist for this VPN connection.	

If the status of the VPN connection could not be retrieved successfully, one of the following values is returned: **EINVAL**, **EAMBIGUOUS**, **ENOENT**.

Please refer to “[Response code](#)” on [page 239](#) for an explanation about those codes.

#### 12.4.3.5 cmd=syndown

This command disables a VPN connection. The name of the VPN connection must be specified with the parameter *name*.

**Example:** Disable the VPN connection with the name *Service*

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=syndown&name=Service'
```

Response:

R OKVDOWN
-----------

If the VPN connection was disabled successfully, the command returns either **OKVDOWN** or **OKVNOTACT**.

Otherwise one of the following values is returned: **EINVAL**, **EAMBIGUOUS**, **ENOENT**, **EBUSY**.

Please refer to [“Response code” on page 239](#) for an explanation about those codes.

## 12.4.4 Central VPN gateway commands

The commands explained in the previous chapters are used on remote mGuards which initiate VPN connections to a central VPN gateway. Two more commands are available especially for using them on a central VPN gateway which uses the *VPN Tunnel Group* feature. The *VPN Tunnel Group* feature allows lots of remote mGuards to establish the VPN connection to one single configured VPN connection on the central VPN gateway.

A *VPN Tunnel Group* connection has *%any* as peer address and the specified remote VPN network is a large network (e.g. 192.168.0.0/16), including all networks of the remote mGuards (e.g. 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, etc.).

The VPN connection accepts ISAKMP SAs from many different remote mGuards at the same time. Each remote mGuard is expected to establish one or more IPsec SAs in tunnel mode where the remote mGuard requests a unique subnet of the configured remote network for each of its tunnel ends.

If the central VPN gateway has only one single *VPN Tunnel Group* configured, where all remote mGuards connect to, there is no way to determine whether there exists an active connection to an individual remote mGuard. Of course, *cmd=status* can be used without a specified VPN connection name (refer to [Section 12.4.2.3](#)) but this command would determine the status of all tunnels which is rather inefficient for querying the state of one single tunnel.

Sometimes it is also desired that the administrator of the central VPN gateway can clear the VPN connection of a specific remote VPN peer. This is in particular helpful if the remote VPN peer cannot establish a new tunnel for whatever interoperability reason. IPsec is a standard but sometimes other vendors are not fully compliant to it. Without an option to clear one specific VPN connection, it is only possible to restart the complete *VPN Tunnel Group* configuration. This would mean that all VPN tunnels are dropped and need to be reestablished.

### 12.4.4.1 *cmd=status, channel=<LNet:RNet>*

This command retrieves the status of the specified VPN tunnel. LNet stands for the local VPN network, RNet for the VPN network of the remote peer.

Return value	Meaning
<i>unknown</i>	This return value could have two reasons: <ul style="list-style-type: none"> <li>– A matching tunnel currently does not exist. There is neither a configured and active tunnel which has the specified networks nor a matching established tunnel of a <i>VPN tunnel group</i>.</li> <li>– A matching channel is inactive due to an error (e.g. the external network is down or the hostname of the remote peer could not be resolved to an IP address (DNS)).</li> </ul>
<i>ready</i>	A connection allows incoming queries regarding the tunnel establishment.
<i>active</i>	The tunnel is established.

**Example:** `wget [...] 'https://admin:mGuard@77.245.33.67/nphvpn.cgi?cmd=status&channel=10.1.0.0/16:192.168.23.0/24'`

Response:

```
active
```

#### 12.4.4.2 cmd=clear, channel=<LNet:RNet>

This command clears the specified VPN tunnel. *LNet* stands for the local VPN network, *RNet* for the VPN network of the remote peer.

Return value	Meaning
<i>unknown</i>	A matching tunnel currently does not exist.
<i>Deleting connection ...</i>	The tunnel is being deleted.

**Example:**

```
wget [...] 'https://admin:mGuard@77.245.33.67/nph-vpn.cgi?cmd=clear& channel=10.1.0.0/16:192.168.23.0/24'
```

Response:

```
002 "MAI1693250436_1"[2] 77.245.32.76: deleting connection
"MAI1693250436_1"[2] instance with peer 77.245.32.76 {isakmp=#0/ipsec=#0}
cleared
```

#### 12.4.5 cmd=sysinfo

This command retrieves the mGuard's software version, hardware name and hardware revision.

**Example:**

```
wget [...] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=sysinfo'
```

Response:

```
mGuardProductName=mGuard smart2
mGuardHardware=MGUARD2
mGuardHardwareVersion=00003000
mGuardVersion=8.6.1.default
```

## 12.5 Interface `nph-diag.cgi`

### 12.5.1 `cmd=snapshot`

The body of the HTTP response produced by the command `snapshot` is binary content. It should be saved to a file, preferable as `snapshot.tar.gz`. When using `wget`, use the option `output-document` to do so (`wget ... --output-document=snapshot.tar.gz ...`).

The snapshot contains the current configuration of the mGuard, the runtime parameters, and all log entries. The file also contains the VPN diagnostic messages described in this document of the last 100 VPN connection establishments at most, if the VPN connection is triggered by CMD contact or by the script `nph-vpn.cgi` and if the option **Archive diagnostic messages for VPN connections** (menu **IPsec VPN >> Global**, tab *Options*) is enabled. The file does not contain private information such as private keys or passwords.

**Example:** `wget [...] 'https://admin:mGuard@192.168.1.1/nph-diag.cgi?cmd=snapshot'`

### 12.5.2 `cmd=testpull`

The mGuard can retrieve new configuration profiles from a HTTPS server in configurable time intervals, provided that the server makes them available as configuration profile for the mGuard (\*.atv). When a new mGuard configuration differs from the current configuration, it will be downloaded and activated automatically. This option is configured through the web interface in the menu **Management >> Central Management**.

With this command it can be tested whether a configuration file can be downloaded from the configuration server according to the current settings of the mGuard. The mGuard does not apply the profile if execution of this command succeeded.

This command returns one of the following values in the HTTP reply:

OKCONFPULL	The mGuard succeeded in downloading the configuration. The format of the message is: <b>R OKCONFPULL d=digest</b>	
	The meaning of the fields are:	
	<b>digest</b>	Alphanumeric string the mGuard sends to the IDM (MGUARD DM, MGUARD Device Manager) with the HTTP request in order to indicate which version of the configuration file has been downloaded.
ECONFPULL	Downloading the configuration file failed. The format of the message is as follows: <b>F ECONFPULL http-code=code msg=message</b>	
	The meaning of the fields are:	
	<b>code</b>	HTTP status code returned by the HTTPS server. Empty, if the HTTP status code could not be transferred due to an error on another layer, e.g. on the Secure Socket Layer (SSL).
	<b>message</b>	This message indicates the cause of the error and may also contain further information. It contains also the error message of the HTTPS server if the HTTP status code is known.

**Example:** `wget [...] 'https://admin:mGuard@192.168.1.1/nph-diag.cgi?cmd=testpull'`

Response:

```
R OKCONFPULL tstamp=20120515094007e  
d=d12851f0b9801e0df45c5794c7f392c5
```

## 12.6 Interface `nph.action.cgi`

### User “root“ and “admin“

The following commands are executable by the users **root** and **admin**.

#### Row actions

`https://admin:mGuard@192.168.1.1/nph-action.cgi?action=<ACTION>&name=<NAME>`

`https://admin:mGuard@192.168.1.1/nph-action.cgi?action=<ACTION>&rowid=<ROWID>`

Table 12-4 Row actions – Parameters

Parameter	Description
<i>name</i>	Name of the connection, rule record, integrity check
<i>rowid</i>	Unique ID from the configuration. ( <code>gaiconfig --goto VPN_CONNECTION:0 --get-rowid</code> )

Table 12-5 Row actions – Actions

Action	Description
<i>fwrules/inactive</i>	Deactivates a firewall rule record
<i>fwrules/active</i>	Activates a firewall rule record
<i>vpn/stop</i>	Also stops an IPsec connection like "nph-vpn.cgi" but with less complexity
<i>vpn/start</i>	Also starts an IPsec connection like "nph-vpn.cgi" but with less complexity
<i>openvpn/stop</i>	Stops an OpenVPN connection
<i>openvpn/start</i>	Starts an OpenVPN connection
<i>cifsim/validaterep</i>	Validates the report of a CIFS/IM scan
<i>cifsim/check-start</i>	Starts a CIFS/IM check
<i>cifsim/init-start</i>	Intializes a new CIFS/IM integrity-database
<i>cifsim/cancel</i>	Cancel a running CIFS/IM job
<i>cifsim/erase-db</i>	Deletes the CIFS/IM database
<i>cifsim/access-scan</i>	Starts a quick file permission check of a share

#### User firewall logout

`https://admin:mGuard@192.168.1.1/nph-action.cgi?action=userfw/logout&name=<NAME> &ip=<IP>`

Table 12-6 User firewall logout – Parameters

Parameter	Description
<i>name</i>	Username of the logged in user of the user firewall
<i>ip</i>	The actual IP-Address of the logged in user of the user firewall

Table 12-7 User firewall logout – Actions

Action	Description
<i>userfw/logout</i>	Logs out the logged in firewall user

**Simple commands**

(Parameters *name* or *ID* not required)

*https://admin:mGuard@192.168.1.1/nph-action.cgi?action=<ACTION>*

Table 12-8 Simple commands – Actions

Action	Description
<i>switch/purge-arlt</i>	Resets the Address Resolution Table in the internal switch
<i>switch/reset-phy-counters</i>	Resets the PHY counters inside the switch

**User “mobile“, “root“ and “admin“**

The following commands are executable by the users **mobile**, **root** and **admin**. The user **mobile** is available since firmware version 8.3.0.

**Mobile actions (User: mobile / root / admin)**

– **Only mGuard firmware version 8.3:**

*https://admin:mGuard@192.168.1.1/nph-action.cgi?action=gsm/call&dial=<NUMBER> &time-out=<TIMEOUT>*

– **mGuard firmware version 8.3 and 8.4:**

*https://admin:mGuard@192.168.1.1/nph-action.cgi?action=gsm/sms&dial=<NUMBER> &msg=<MESSAGE>*

Table 12-9 Mobile actions – Parameters

Parameter	Description
<i>dial</i>	Telephone number of the destination
<i>timeout</i>	Time in seconds until the call is finished
<i>msg</i>	Content of the short message (should be cleaned of special characters like umlauts)

Table 12-10 Mobile actions – Actions

Action	Description
<i>gsm/call</i>	Starts a phone call
<i>gsm/sms</i>	Sends a text message (SMS)

## 12.7 Interface `nph.status.cgi`

The following commands are executable by the users **root** and **admin**.

Table 12-11 CGI status

Parameter	Description
<b>/network/modem/state</b>	<b>Modem state</b>
<a href="https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/network/modem/state">https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/network/modem/state</a>	
Answer: <i>online   offline</i>	
<b>/network/ntp_state</b>	<b>NTP time synchronization state</b>
<a href="https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/network/ntp_state">https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/network/ntp_state</a>	
Answer: <i>disabled   not_synced   synchronized</i>	
<b>/system/time_sync</b>	<b>State of the system time synchronization</b>
<a href="https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/system/time_sync">https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/system/time_sync</a>	
Answer: <i>not_synced   manually   stamp   rtc   ntp   gps   gpslost</i>	
<b>/ecs/status</b>	<b>State of the ECS</b>
<a href="https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/ecs/status">https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/ecs/status</a>	
Answer: "1" for not present, "2" for removed, "3" for present an in synchronization, "4" for not in synchronization and "8" for generic error	
<b>/vpn/con</b>	<b>State of a VPN connection</b>
<a href="https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/vpn/con&amp;name=&lt;Verbindungsname&gt;">https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/vpn/con&amp;name=&lt;Verbindungsname&gt;</a>	
Answer: <ul style="list-style-type: none"> <li>- <code>/vpn/con/&lt;rowid&gt;/armed=[yes no]</code> Shows whether the connection is started or not</li> <li>- <code>/vpn/con/&lt;rowid&gt;/ipsec=[down somelup]</code> Shows the IPsec state.</li> <li>- <code>/vpn/con/&lt;rowid&gt;/isakmp=[up down]</code> Shows the ISAKMP state.</li> <li>- <code>/vpn/con/&lt;rowid&gt;/sa_count=&lt;number&gt;</code> Number of configured tunnel</li> <li>- <code>/vpn/con/&lt;rowid&gt;/sa_count_conf=&lt;number&gt;</code> Number of configured enabled tunnel</li> </ul>	
<b>/fwrules</b>	<b>State of a firewall rule record</b>
<a href="https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/fwrules&amp;name=&lt;rule record &gt;">https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/fwrules&amp;name=&lt;rule record &gt;</a>	
Answer: <ul style="list-style-type: none"> <li>- <code>/fwrules/&lt;rowid&gt;/expires=&lt;seconds since 1.1.1970&gt;</code> Expiration date – 0 for no expiration</li> <li>- <code>/fwrules/&lt;rowid&gt;/state=[inactive active]</code> Activation state of the firewall rule record</li> </ul>	
<b>/cifs/im</b>	<b>State of a share in the context of CIFS</b>
<a href="https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/cifs/im&amp;name=&lt;WS_SHARE&gt;">https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/cifs/im&amp;name=&lt;WS_SHARE&gt;</a>	

Table 12-11 CGI status

Parameter	Description
Answer:	
<b>Actual check</b>	
- /cifs/im/<rowid>/curr/all=<number>	Number of files
- /cifs/im/<rowid>/curr/end=<seconds>	End time of the current check in seconds since 1.1.1970
- /cifs/im/<rowid>/curr/numdiffs=<number>	Currently found number of diffs.
- /cifs/im/<rowid>/curr/operation=[nonelsuspend check ldb_build]	Current operation
- /cifs/im/<rowid>/curr/scanned=<number>	Number of currently checked files
- /cifs/im/<rowid>/curr/start=<seconds>	Start time in seconds since 1.1.1970
<b>Last check</b>	
- /cifs/im/<rowid>/last/duration=<number>	Number of seconds of the last duration
- /cifs/im/<rowid>/last/numdiffs=<number>	Number of differences found during the last check
- /cifs/im/<rowid>/last/start=<seconds> start time in seconds since 1.1.1970	Start time in seconds since 1.1.1970
- /cifs/im/<rowid>/last/result=<see "Last Results" below">	
<b>Log results</b>	
- /cifs/im/<rowid>/log/fname=<filename of the log file>	
- /cifs/im/<rowid>/log/hash=<sha1 hash>	
- /cifs/im/<rowid>/log/result=<siehe "Log result" below">	

Table 12-11 CGI status

Parameter	Description
<b>Last results</b>	
- 1:	The share has not yet been checked. Probably no integrity database exists.
- 0:	Last check finished successfully.
- 1:	The process failed due to an unforeseen condition, please consult the logs.
- 2:	Last check was aborted due to timeout.
- 3:	The integrity database is missing or incomplete.
- 4:	The signature of the integrity database is invalid.
- 5:	The integrity database was created with a different hash algorithm.
- 6:	The integrity database is the wrong version.
- 7:	The share which is to be checked is not available.
- 8:	The share which is to be used as checksum memory is not available.
- 11:	A file could not be read due to an I/O failure. Please consult the report.
- 12:	The directory tree could not be traversed due to an I/O failure. Please consult the report.
<b>Log result</b>	
- <i>unchecked</i>	- The signature has not been verified, yet.
- <i>valid</i>	- The signature is valid.
- <i>Emissing</i>	- <i>ERROR: The report is missing.</i>
- <i>Euuid_mismatch</i>	- <i>ERROR: The report does not belong to this device or is not up to date.</i>
- <i>Ealgo_mismatch</i>	- <i>ERROR: The report was created with a different hash algorithm.</i>
- <i>Etampered</i>	- <i>ERROR: The report was tampered with.</i>
- <i>Eunavail</i>	- <i>ERROR: The report is not available. For example the share might not be mounted.</i>
- <i>Eno_idb</i>	- No report exists, because of a missing integrity database.



## 13 LED status indicator and blinking behavior



Document-ID: 108400\_en\_00  
 Document-Description: AH EN MGUARD LED SIGNALS  
 © PHOENIX CONTACT 2026-03-17



Make sure you always use the latest documentation.  
 It can be downloaded using the following link [phoenixcontact.net/products](https://phoenixcontact.net/products).

### Contents of this document

This document describes the lighting and blinking behavior of the LED diodes installed in mGuard devices (FL/TC MGUARD RS2000/RS4000).

13.1	Description of LEDs.....	259
13.2	LED lighting and blinking behavior .....	261
13.3	Representation of system states .....	261

### 13.1 Description of LEDs

With the help of built-in LED diodes, mGuard devices indicate different system states. This can be status, alarm or error messages.

The states are indicated by permanent or temporary lighting or blinking of the LEDs. The displayed LED pattern can also represent a combination of different system states.



**NOTE:** Since several system states are indicated by the LEDs not clearly, only temporarily or in combination with other system states, the log files of the mGuard device must also be checked!

LED diodes of FL/TC MGUARD (RS200x/RS400x) devices:

P1	Stat	Mod	Info2 (Sig)
P2	Err	Fault	Info1

#### P1 / P2

LEDs *P1* and *P2* indicate which of the two power supplies is connected (devices of the FL/TC MGUARD RS2000 series: only *P1* is available).

#### Info 2 / Info 1 (the LED Sig is not in use)

Active VPN connections or (as of Version 8.1) active firewall rule records can be indicated via the LEDs *Info2* and *Info1*. The activation of the LEDs by a certain VPN connection or a certain firewall rule record is configured on the mGuard interface in the menu item **Management >> Service Contacts**.

The following states will be indicated:

<b>ON</b>	The VPN connection is established / the firewall rule record is set.
<b>Blink</b>	The VPN connection will be established or released or has been stopped/disabled by the remote peer.
<b>OFF</b>	The VPN connection is stopped/disabled on both peers.

**Stat / Mod / Err / Fault**

The LEDs *Stat*, *Mod*, *Err* and *Fault* indicate system states (status, alarm or error messages) (see [Table 13-3](#)).

In addition to the alarm messages, an illuminated **Fault LED** generally also indicates that the device is currently not in operation mode.

**LAN / WAN**

The LAN/WAN LEDs are located in the LAN/WAN sockets (10/100 and duplex LED).

The LEDs indicate the ethernet status of the LAN or WAN port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN or WAN. When data packets are transmitted, the LED goes out briefly.

If all LAN/WAN LEDs are illuminated, the system is booting.

**Bar graph and SIM1/2 (Mobile)**

Table 13-1 LEDs on TC MGuard RS4000 3G and TC MGuard RS2000 3G

LED	State and Meaning					
<b>Bar graph</b>	LED 3	Top	Off	Off	Off	Green
	LED 2	Middle	Off	Off	Green	Green
	LED 1	Bottom	Off	Yellow	Yellow	Yellow
	Signal strength (dBm)		-113 ... 111	-109 ... 89	-87 ... 67	-65 ... 51
	Network reception		Very poor to none	Sufficient	Good	Very good
<b>SIM 1</b>	Green	On Blinking	SIM card 1 active No PIN or incorrect one entered			
<b>SIM 2</b>	Green	On Blinking	SIM card 2 active No PIN or incorrect one entered			

## 13.2 LED lighting and blinking behavior

Table 13-2 Description of the lighting and blinking behavior of the LED diodes

<b>Heartbeat</b>	The blinking behavior is similar to a heartbeat, in which two strokes are performed in quick succession, followed by a short break.
<b>Running light</b>	Three lights form a continuously repeating running light from left to right and back again.
<b>Blink 50/1500</b>	Flashing with 1500 ms break (50 ms on, then 1500 ms off)
<b>Blink 50/800</b>	Flashing with 800 ms break (50 ms on, then 800 ms off)
<b>Blink 50/100</b>	Flashing with 100 ms break (50 ms on, then 100 ms off)
<b>Blink 500/500</b>	Constant blinking (500 ms on / 500 ms off)
<b>Morse code (. . . - - - . . .)</b>	The blinking behavior shows the <i>Morse code</i> 'SOS', in which the blinking behavior "3x short, 3x long, 3x short" is repeated continuously.
<b>ON</b>	The diode lights up permanently.
<b>ON (n sec)</b>	The diode lights up permanently for the indicated time (in seconds n)

## 13.3 Representation of system states

The system states (status, alarm or error messages), which are displayed by the LED's lighting and blinking behavior, are shown in [Table 13-3](#).

Table 13-3 System states of FL/TC MGUARD devices represented by lighting and blinking behavior of the LEDs

STAT	MOD	Info 2 (Sig)	ERR	FAULT	Description of the system state
Heart-beat					The system status is OK.
			ON		A severe error has happened.
ON (12 sec)	ON (3 sec)		ON (12 sec)	ON (12 sec)	The system is booting.
<b>Morse code</b>					The license to operate this firmware is missing.
<b>Morse code</b>			<b>Morse code</b>		Bootloader replacement failed due to hardware error.
				ON	A power failure was detected.
				ON	No connectivity on WAN interface (link supervision configurable on device)
				ON	No connectivity on LAN interface (link supervision configurable on device)
				ON	No connectivity on LAN 1–4 interface (link supervision configurable on device)
				ON	No connectivity on DMZ interface (link supervision configurable on device)
				ON	Power supply 1 or 2 failed (alarm configurable on device)
				ON	Temperature too high / low (alarm configurable on device)
				ON	(Redundancy) Connectivity check failed (alarm configurable on device)
				ON	(Modem) Connectivity check failed (alarm configurable on the device)
			ON (3 sec)		ECS: The ECS is incompatible.
			ON (3 sec)		ECS: The capacity of the ECS is exhausted.

Table 13-3 System states of FL/TC MGUARD devices represented by lighting and blinking behavior of the LEDs

STAT	MOD	Info 2 (Sig)	ERR	FAULT	Description of the system state
			ON (3 sec)		ECS: The root password from the ECS does not match.
			ON (3 sec)		ECS: Failed to load the configuration from the ECS.
			ON (3 sec)		ECS: Failed to save the configuration to the ECS.
	ON				PPPD: The internal modem got a connect (set by pppd).
	Blink 50/1500				PPPD: The internal modem is armed and expecting a dial in.
	Blink 500/500				PPPD: The internal modem is dialing.
			ON (2 sec)		RECOVERY: The recovery procedure failed.
ON (2 sec)					RECOVERY: The recovery procedure succeeded.
ON				ON	FLASH PROCEDURE: The flash procedure has been started. Please wait.
Running light	Running light	Running light		ON	FLASH PROCEDURE: The flash procedure is currently executed.
Blink 50/800	Blink 50/800	Blink 50/800		ON	FLASH PROCEDURE: The flash procedure succeeded.
ON			ON		FLASH PROCEDURE: The flash/production procedure failed.
			Blink 50/100 (5 sec)		FLASH PROCEDURE WARNING: Replacing the rescue system. Do not power off. When the blinking stops, the replacement of the rescue system is over.
			ON		FLASH PROCEDURE: The DHCP/BOOTP requests failed.
			ON		FLASH PROCEDURE: Mounting the data storage device failed.
			ON		FLASH PROCEDURE: The flash procedure failed.
			ON		FLASH PROCEDURE: Erasing the file system partition failed.
			ON		FLASH PROCEDURE: Failed to load the firmware image.
			ON		FLASH PROCEDURE: The signature of the firmware image is not valid.
			ON		FLASH PROCEDURE: Failed to load the install script.
			ON		FLASH PROCEDURE: The signature of the install script is not valid.
			ON		FLASH PROCEDURE: The rollout script failed.

---

## Please observe the following notes

### **Note on the usage of Application Notes**

The provided Application Notes are a free service from Phoenix Contact. The examples and solutions shown are not customer-specific solutions, but general support for typical application scenarios. The Application Notes are not binding and do not claim to be complete.

A quality check of the Application Notes takes place but is not comparable with the quality assurance of commercial products. Errors, functional and performance deficiencies cannot be excluded.

To avoid malfunctions/misconfigurations and associated damage, the proper and safe use of the product/software is the sole responsibility of the customer and must comply with the applicable regulations. The customer must check the function of the examples described and adapt them to the individual, customer-specific requirements of the system or application scenario.

The IP settings in the Application Notes have been chosen as examples. In a real network scenario, these IP settings must always be adjusted to avoid address conflicts.

The information in the Application Notes is checked regularly. If corrections are necessary, they will be included in the subsequent revision. Users will not be notified.

### **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.

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

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](http://phoenixcontact.com)

Make sure you always use the latest documentation.

It can be downloaded at:

[phoenixcontact.net/products](http://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](http://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](mailto:tecdoc@phoenixcontact.com)