mGuard-Anwenderhinweise FL/TC MGUARD

Anwenderhinweis

AH DE MGUARD APPNOTES

PHOENIX CONTACT
INSPIRING INNOVATIONS

Anwenderhinweis

mGuard-Anwenderhinweise – FL/TC MGUARD

AH DE MGUARD APPNOTES , Revision 09 2024-10-17

Dieser Anwenderhinweis ist gültig für die folgenden mGuard-Security-Appliances:

Gerät	Bestellnummer
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

108391_de_09

Inhaltsverzeichnis

1 Zu Ihrer Sicherheit

Lesen Sie dieses Handbuch sorgfältig und bewahren Sie es für späteres Nachschlagen auf.

1.1 Kennzeichnung der Warnhinweise

Dieses Symbol mit dem Signalwort **ACHTUNG** warnt vor Handlungen, die zu einem Sachschaden oder einer Fehlfunktion führen können.

Hier finden Sie zusätzliche Informationen oder weiterführende Informationsquellen.

1.2 Qualifikation der Benutzer

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

- Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.
- Qualifizierte Anwendungsprogrammierer und Software-Ingenieure. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.

2 FL/TC MGUARD-Geräte updaten und flashen

Dokument-ID: 108250_de_12
Dokument-Bezeichnung: AH DE MGUARD UPDATE

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument wird beschrieben,

1. welche mGuard-Firmwareversionen auf mGuard 8.9.3 upgedatet werden können,
2. welche mGuard-Firmwareversionen auf mGuard 10.4.1 upgedatet werden können,
3. welche Dateien für ein Firmware-Update Ihres mGuard-Geräts benötigt werden,
4. wie ein Firmware-Update durchgeführt wird,
5. wie die Flash-Prozedur durchgeführt wird.

2.1 Einleitung

Die Firmware auf mGuard-Geräten kann auf unterschiedliche Weise aktualisiert werden:

1. Lokales Update
2. Online-Update (nicht verfügbar bei FL MGUARD 2000/4000 - mGuard 10.x)
3. Automatische Updates
4. Flashen der Firmware

Bei einem **Firmware-Update** bleibt die bestehenden Konfiguration des mGuard-Geräts in der Regel unverändert.

Das **Flashen** eines mGuard-Geräts löscht die bestehende Konfiguration inklusive aller Passwörter und setzt das Gerät in den Auslieferungsszustand (Werkseinstellungen) zurück.

Firmwareversion 8

Das Update auf die **Firmwareversion mGuard 8.9.3** wird für alle mGuard-Geräte in den Kapiteln 2.7 bis 2.17 ausführlich beschrieben. In Tabelle 2-1 werden die benötigten Update-Dateien kurz aufgeführt.

Firmwareversion 10

Das Update auf die **Firmwareversion mGuard 10.4.1** wird für alle mGuard-Geräte im Kapitel 2.18 ausführlich beschrieben. In Tabelle 2-3 werden die benötigten Update-Dateien kurz aufgeführt.

2.2 Update auf mGuard-Firmwareversion 8.9.3

Ein Update auf die **mGuard-Firmwareversion 8.9.3** ist ausschließlich von **mGuard-Firmwareversion 8.6.1** oder höher möglich.

Wenn Sie von einer **Firmwareversion < 8.6.1** updaten möchten, müssen Sie das Update in mehreren Schritten durchführen, indem Sie zunächst auf die Version 8.6.1 updaten (siehe Kapitel 2.3, „Update auf mGuard-Firmwareversion 8.6.1“). Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

Ein Update auf Firmware-Version 8.9.3 ist nur möglich, wenn die Funktion „**Verschlüsselter Zustandsabgleich**“ (Menü: *Redundanz*) zuvor deaktiviert wurde.

Der Name der zu verwendenden Update-Datei ist abhängig von der installierten Firmwareversion (Ausgangsversion):

– Ausgangsversion: 8.6.1 bis 8.7.x --> Bezeichnung: *8.{6-7}*
– Ausgangsversion: 8.8.0 bis 8.8.x --> Bezeichnung: *8.{8}*
– Ausgangsversion: 8.9.0 bis 8.9.x --> Bezeichnung: *8.{9}*

Das Update auf **mGuard-Firmwareversion 8.9.3** wird geräteabhängig in den Kapiteln 1.7 bis 1.17 ausführlich beschrieben (siehe „Inhalt dieses Dokuments“). In Tabelle 2-1 werden die je nach Ausgangs-Firmwareversion benötigten Update-Dateien kurz aufgeführt.

Tabelle 2-1 Update von mGuard-Firmwareversion ab **8.6.1** auf **8.9.3**: Benötigte Dateien

Geräte	Lokales Update	Flashen der Firmware
FL MGUARD RS2000 FL MGUARD RS4000 (TX/TX) (inkl. Varianten -B, -P, -M)	**Download-Datei**: *Update_MPC_v8.9.3.zip* **Update-Dateien**: *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*
FL MGUARD RS2005 FL MGUARD RS4004 (TX bzw. TX/DTX)	**Download-Datei**: *Update_MPC_v8.9.3.zip* **Update-Dateien**: *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*
FL MGUARD PCI(E)4000	**Download-Datei**: *Update_MPC_v8.9.3.zip* **Update-Dateien**: *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*
FL MGUARD SMART2	**Download-Datei**: *Update_MPC_v8.9.3.zip* **Update-Dateien**: *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*

Tabelle 2-1 Update von mGuard-Firmwareversion ab **8.6.1** auf **8.9.3**: Benötigte Dateien

FL MGUARD GT/GT	**Download-Datei**: *Update_MPC_v8.9.3.zip* **Update-Dateien**: *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_GTGT_v8.9.3* **Update-(Flash)-Dateien**: *jffs2.img.mpc83xx.p7s* *install.mpc83xx.p7s*
FL MGUARD DELTA TX/TX	**Download-Datei**: *Update_MPC_v8.9.3.zip* **Update-Dateien**: *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*
FL MGUARD CENTERPORT	**Download-Datei**: *Update_X86_v8.9.3.zip* **Update-Dateien**: *update-8.{6-7}-8.9.3.default.x86_64.tar.gz* *update-8.{8}-8.9.3.default.x86_64.tar.gz* *update-8.{9}-8.9.3.default.x86_64.tar.gz*	**Download-Datei**: *FW_X86_v8.9.3.zip* **Update-(Flash)-Dateien**: *firmware.img.x86_64.p7s* *install.x86_64.p7s*
TC MGUARD RS2000 3G VPN TC MGUARD RS4000 3G VPN	**Download-Datei**: *Update_MPC_TC3G_v8.9.3.zip* **Update-Dateien**: *gemalto.update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *gemalto.update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *gemalto.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_TC3G_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s* *pxs8_03001_0100617.usf.xz.p7s*
TC MGUARD RS2000 4G VPN TC MGUARD RS4000 4G VPN (Firmware-Update für Geräte mit **Gemalto-Engine** – ab Q3/2021)	**Download-Datei**: *Update_MPC_TC4G_G_v8.9.3.zip* **Update-Dateien**: *PLS8-E.update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *PLS8-E.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_TC4G_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s* *pls8-e_rev04.004_arn01.000.11.usf.xz.p7s*

Tabelle 2-1 Update von mGuard-Firmwareversion ab **8.6.1** auf **8.9.3**: Benötigte Dateien

TC MGUARD RS2000 4G VPN TC MGUARD RS4000 4G VPN (Firmware-Update für Geräte mit **Huawei-Engine** – bis Q3/2021)	**Download-Datei**: *Update_MPC_TC4G_H_v8.9.3.zip* **Update-Dateien**: *huaweigeneric.update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *huaweigeneric.update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *huaweigeneric.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_TC4H_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s* *ME909u-521_UPDATE_12.636.12.01.00.BIN.xz.p7s*
TC MGUARD RS2000/4000 4G VZW VPN	**Download-Datei**: *Update_MPC_TC4GVZW_v8.9.3.zip* **Update-Dateien**: *HL7518.update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *HL7518.update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *HL7518.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_TC4GVZW_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s* *RHL75xx.4.04.142600.201801231340.x7160_1_signed_dwl.dwl.xz.p7s*
TC MGUARD RS2000/4000 4G ATT VPN	**Download-Datei**: *Update_MPC_TC4GATT_v8.9.3.zip* **Update-Dateien**: *HL7588.update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz* *HL7588.update-8.{8}-8.9.3.default.mpc83xx.tar.gz* *HL7588.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_TC4GATT_v8.9.3.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s* *RHL75xx.A.2.15.151600.201809201422.x7160_3_signed_DWL.dwl.xz.p7s*

2.3 Update auf mGuard-Firmwareversion 8.6.1

Möglich ab **mGuard-Firmwareversion 7.6.0**.

Der Name der zu verwendenden Update-Datei ist abhängig von der installierten Firmwareversion (Ausgangsversion) und beinhaltet folgende Bezeichnungen:

- Ausgangsversion: 7.6.0 bis 7.6.x --> Bezeichnung: *7.{6}*
- Ausgangsversion: 8.0.0 bis 8.5.x --> Bezeichnung: *8.{0-5}*
- Ausgangsversion: 8.6.0 --> Bezeichnung: *8.{6}*

Das Update auf **mGuard-Firmwareversion 8.6.1** erfolgt analog zu den in den Kapiteln 1.7 bis 1.17 beschriebenen Verfahren (siehe „Inhalt dieses Dokuments“). In Tabelle 2-2 werden die je nach Ausgangs-Firmwareversion benötigten Update-Dateien kurz aufgeführt.

Tabelle 2-2 Update von mGuard-Firmwareversion **7.6.0 oder höher** auf **8.6.1**: Benötigte Dateien

Geräte	Lokales Update	Flashen der Firmware
FL MGUARD RS2000 FL MGUARD RS4000 (TX/TX) (inkl. Varianten -B, -P, -M)	**Download-Datei**: *Update_8.6.1_MPC.zip* **Update-Dateien**: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz* *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz* *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_8.6.1.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*
FL MGUARD RS2005 FL MGUARD RS4004 (TX bzw. TX/DTX)	**Download-Datei**: *Update_8.6.1_MPC.zip* **Update-Dateien**: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz* *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_8.6.1.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*
TC MGUARD RS2000 3G VPN TC MGUARD RS4000 3G VPN	**Download-Datei**: *Update_8.6.1_TC3G_MPC.zip* **Update-Dateien**: *gemalto.update-8.{4-5}-8.6.1.default.mpc83xx.tar.gz* *gemalto.update-8.{6}-8.6.1.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_TC3G_8.6.1.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s* pxs8_03001_0100617.usf.xz.p7s
TC MGUARD RS2000 4G VPN TC MGUARD RS4000 4G VPN	**Download-Datei**: *Update_8.6.1_TC4G_MPC.zip* **Update-Dateien**: *huaweigeneric.update-8.{4-5}-8.6.1.default.mpc83xx.tar.gz* *huaweigeneric.update-8.{6}-8.6.1.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_TC4G_8.6.1.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s* ME909u-521_UPDATE_12.636.12.01.00.BIN.xz.p7s
FL MGUARD PCI(E)4000	**Download-Datei**: *Update_8.6.1_MPC.zip* **Update-Dateien**: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz* *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz* *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_8.6.1.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*

Tabelle 2-2 Update von mGuard-Firmwareversion **7.6.0 oder höher** auf **8.6.1**: Benötigte Dateien

FL MGUARD SMART2	**Download-Datei**: *Update_8.6.1_MPC.zip* **Update-Dateien**: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz* *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz* *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_8.6.1.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*
FL MGUARD CENTERPORT	**Download-Datei**: *Update_8.6.1_x86.zip* **Update-Dateien**: *update-7.{6}-8.6.1.default.x86_64.tar.gz* *update-8.{0-5}-8.6.1.default.x86_64.tar.gz* update-8.{6}-8.6.1.*default.x86_64.tar.gz*	**Download-Datei**: *FW_X86_8.6.1.zip* **Update-(Flash)-Dateien**: *firmware.img.x86_64.p7s* *install.x86_64.p7s*
FL MGUARD GT/GT	**Download-Datei**: *Update_8.6.1_MPC.zip* **Update-Dateien**: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz* *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz* *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_GTGT_8.6.1.zip* **Update-(Flash)-Dateien**: *jffs2.img.mpc83xx.p7s* *install.mpc83xx.p7s*
FL MGUARD DELTA TX/TX	**Download-Datei**: *Update_8.6.1_MPC.zip* **Update-Dateien**: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz* *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz* *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*	**Download-Datei**: *FW_MPC_8.6.1.zip* **Update-(Flash)-Dateien**: *ubifs.img.mpc83xx.p7s* *install-ubi.mpc83xx.p7s*

2.4 Update auf mGuard-Firmwareversion 10.4.1

Ein Update auf die **mGuard-Firmwareversion 10.4.1** ist möglich von allen **mGuard-Firmwareversionen ab mGuard-Firmwareversion 10.0.0**.

Der Name der zu verwendenden Update-Datei ist abhängig von der installierten Firmwareversion (Ausgangsversion):

– Ausgangsversion: 10.0.x bis 10.4.x --> Bezeichnung: *10.{0-4}*

Das Update auf **mGuard-Firmwareversion 10.4.1** wird im Kapitel 2.18 ausführlich beschrieben (siehe „Inhalt dieses Dokuments“). In Tabelle 2-3 werden die je nach Ausgangs-Firmwareversion benötigten Update-Dateien kurz aufgeführt.

Tabelle 2-3 Update von mGuard-Firmwareversion ab **10.0.0** auf **10.4.1**: Benötigte Dateien

Geräte	Lokales Update	Flashen der Firmware
FL MGUARD 4302 FL MGUARD 4305 FL MGUARD 2102 FL MGUARD 2105 FL MGUARD 4102 PCI FL MGUARD 4102 PCIE	**Download-Datei**: *Update_mGuard-10.4.1.zip* **Update-Dateien**: *update-10.{0-4}-10.4.1.default.aarch64.tar.gz*	**Download-Datei**: *Firmware_mGuard-10.4.1.zip* **Update-(Flash)-Dateien**: *firmware.img.aarch64.p7s* *install.aarch64.p7s*

2.5 Migration der Konfiguration von mGuard-Firmwareversion 8.x nach 10.x

Die neue mGuard-Geräteplattform 3 wird mit der Firmwareversion mGuard 10.x betrieben. Ein Update von Firmwareversion 8.x auf 10.x ist nicht möglich.

Die Konfiguration von mGuard 8.x-Geräten kann jedoch auf Geräte mit installierter Firmwareversion mGuard 10.x migriert werden.

Das Vorgehen für die Migration nach mGuard 10.4.1 wird im Anwenderhinweis „Gerätetausch und Migration“ (AH DE MGUARD MIGRATE 10 – 111259_de_xx) beschrieben, verfügbar unter phoenixcontact.net/product/<artikel-nummer>.

2.6 Allgemeine Hinweise zu mGuard-Updates

2.6.1 PHOENIX CONTACT Web Shop

Die jeweils verfügbaren Update-Files werden für jedes mGuard-Gerät auf der Produktseite im PHOENIX CONTACT Web Shop zum Download zur Verfügung gestellt unter: phoenixcontact.net/products.

Je nach installierter Firmwareversion müssen unterschiedliche Dateien für ein Update verwendet werden.

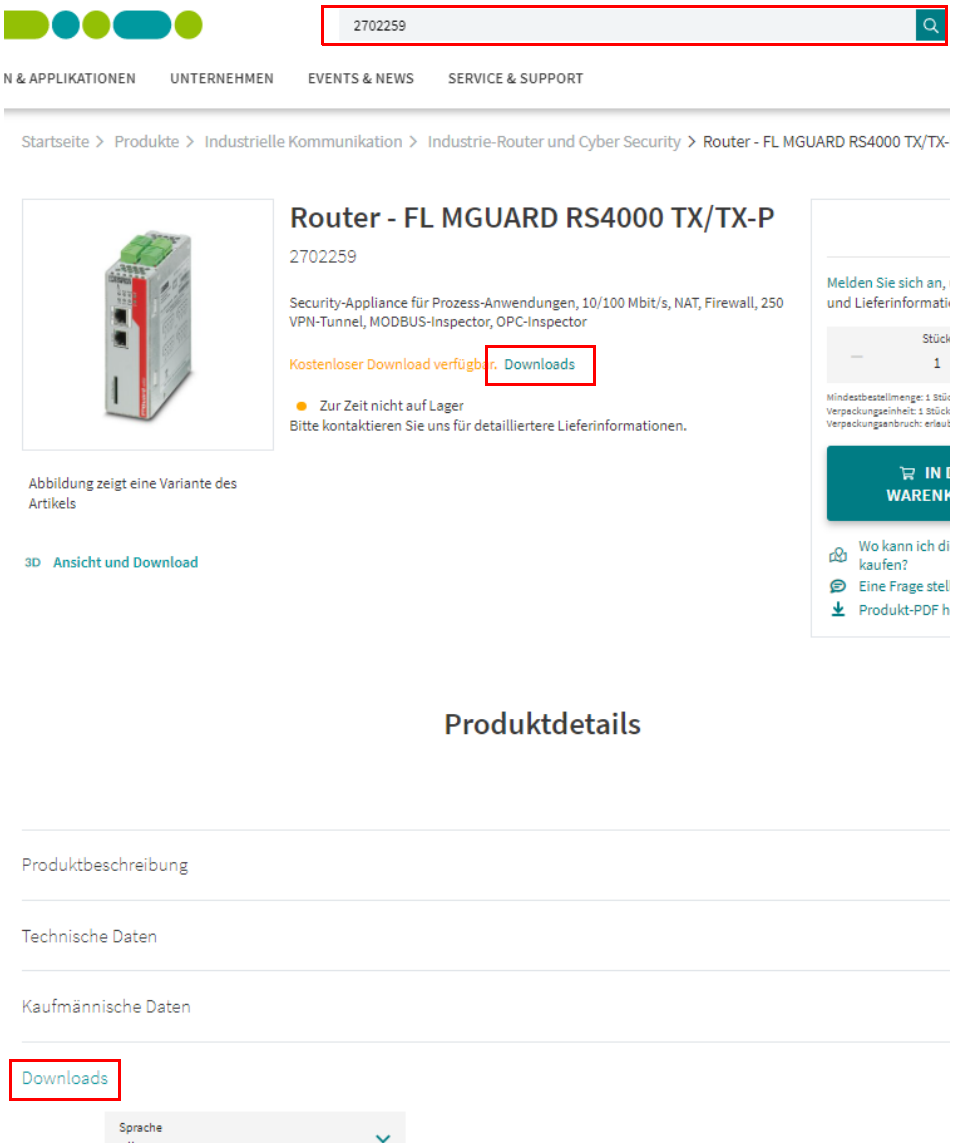


Bild 2-1 PHOENIX CONTACT Web Shop – Produktseite

2.6.2 Versionierung: Major-, Minor- und Patch-Releases

Bei der Versionierung der mGuard-Firmware werden folgende Bezeichnungen verwendet:

1. **Major-Release** (Hauptversionsnummer)

   Major-Releases ergänzen den mGuard um neue Eigenschaften und enthalten meist größere und grundsätzlichere Änderungen der mGuard-Firmware. Ihre Versionsnummer ändert sich in der ersten Stelle. Die Version **8**.6.1 ist z. B. ein Major-Release zur Version **7**.6.8.

2. **Minor-Release** (Nebenversionsnummer)

   Minor-Releases ergänzen den mGuard um neue Eigenschaften. Ihre Versionsnummer ändert sich in der zweiten Stelle. Die Version 8.**6**.0 ist z. B. ein Minor-Release zur Version 8.**4**.2.

3. **Patch-Release** (Schließen von Sicherheitslücken / allgemeine Fehlerbehebung)

   Patch-Releases beheben Fehler der vorherigen Versionen und haben eine Versionsnummer, welche sich in der dritten Stelle ändern. Die Version 8.6.**1** ist z. B. ein Patch-Release zur Version 8.6.**0**.

2.6.3 Bezeichnung der Update-Dateien (geschweifte Klammern)

Welche Datei für das Update Ihres mGuard-Geräts verwendet werden muss, ist abhängig von der installierten Firmwareversion auf dem Gerät.

Im Dateinamen der jeweiligen Update-Datei wird in **geschweiften Klammern** angegeben, welche Firmwareversionen sich mit dieser Datei aktualisieren lassen.

Beispiel „Lokales Update“ RS4000

Mit der Update-Datei „*update*-**8.{0-5}**-*8.6.1.default.mpc83xx.tar.gz*“ lassen sich die Firmwareversionen **8.0.0** bis **8.5.x** auf die Version 8.6.1 aktualisieren.

Die Download-Datei heißt in diesem Fall *„Update_8.6.1_MPC.zip“.*

Beispiel „Online-Update“ RS4000

Mit der Angabe des Package-Set-Namens *„update*-**7.{6}**-*8.6.1.default“* lassen sich die Firmwareversionen **7.6.0** bis **7.6.x** auf die Version 8.6.1 aktualisieren.

2.6.4 Beschreibung der Update-Verfahren

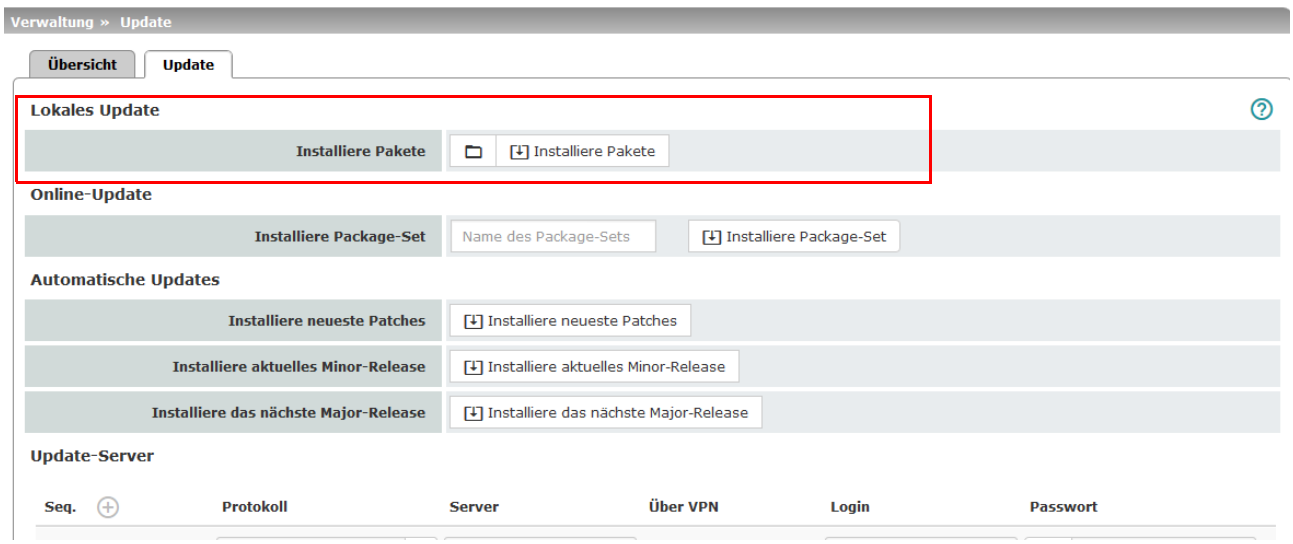
ACHTUNG: Unterbrechen Sie während des Updates nicht die Stromversorgung des mGuard-Geräts! Das Gerät könnte ansonsten beschädigt werden.

Weitere Informationen zu Installation, Betrieb und Update von mGuard-Geräten finden Sie im Firmware-Referenzhandbuch und im mGuard-Hardwarehandbuch (verfügbar im PHOENIX CONTACT Web Shop unter phoenixcontact.net/products oder unter help.mguard.com):

- mGuard 8.x: 105661_de_xx „UM DE MGUARD"
- mGuard 8.x: 105656_de_xx „UM DE MGUARD DEVICES"
- mGuard 10.x: 110191_de_xx „UM DE FW MGUARD10“
- mGuard 10.x: 110192_de_xx „UM EN HW FL MGUARD 2000/4000“

2.6.4.1 Lokales Update

Die Update-Datei (*tar.gz*-Format) wird vom lokal angeschlossenen Konfigurationsrechner auf das mGuard-Gerät geladen und über die mGuard-Weboberfläche installiert (**Verwaltung >> Update >> Update**).



Die Firmwareversionen, die mit der Update-Datei aktualisiert werden können, werden im Dateinamen der jeweiligen Update-Datei in geschweiften Klammern angegeben.

Beispiel (FL MGUARD RS4000):

Major-Release-Update: 7.6.8 auf 8.6.1:

- Download-Datei: *Update_8.6.1_MPC.zip*
- Update-Datei: *update-**7.{6}**-8.6.1.default.mpc83xx.tar.gz*

Minor-Release-Update: 8.**4**.2 auf 8.6.1:

- Download-Datei: *Update_8.6.1_MPC.zip*
- Update-Datei: *update-**8.{0-5}**-8.6.1.default.mpc83xx.tar.gz*

Patch-Release-Update: 8.6.**0** auf 8.6.1:

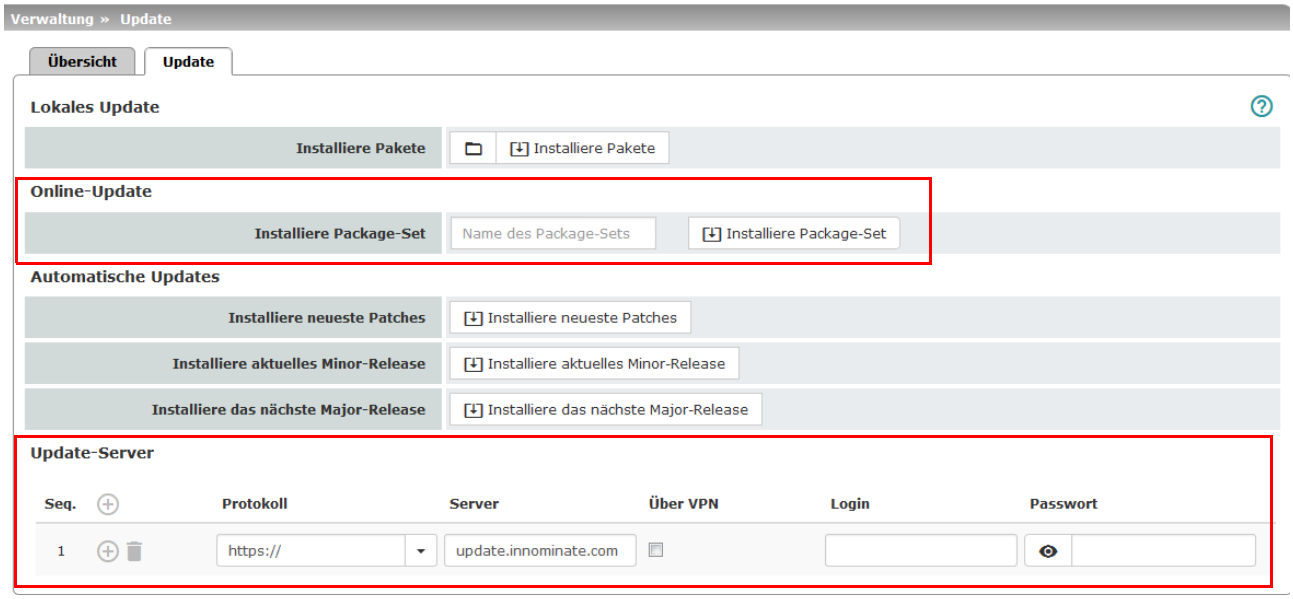
- Download-Datei: *Update_8.6.1_MPC.zip*
- Update-Datei: *update-**8.{6}**-8.6.1.default.mpc83xx.tar.gz*

2.6.4.2 Online-Update

Nicht verfügbar für FL MGUARD 2000/4000-Geräte mit installierter Firmwareversion 10.x.

Die Update-Datei wird von einem konfigurierbaren Update-Server geladen und installiert.

Die Initialisierung des Updates erfolgt durch die Anforderung eines **Package-Sets** auf der mGuard-Weboberfläche (**Verwaltung >> Update >> Update**).



Die Firmwareversionen, die über die Auswahl des Package-Set-Namens aktualisiert werden können, werden im jeweiligen Package-Set-Namen in geschweiften Klammern angegeben.

Beispiel (FL MGUARD RS4000):

Major-Release-Update: **7**.6.8 auf 8.6.1

– Package-Set-Name: *update*-**7.{6}**-*8.6.1.default*

Minor-Release-Update: 8.**4**.2 auf 8.6.1

– Package-Set-Name: *update*-**8.{0-5}**-*8.6.1.default*

Patch-Release-Update: 8.6.**0** auf 8.6.1

– Package-Set-Name: *update*-**8.{6}**-*8.6.1.default*

ACHTUNG: Online- oder Automatische Updates von der installierten Ausgangs-Firmwareversion **7.6.8** können zu einem Fehler führen (siehe Hinweis in Kapitel 2.20).

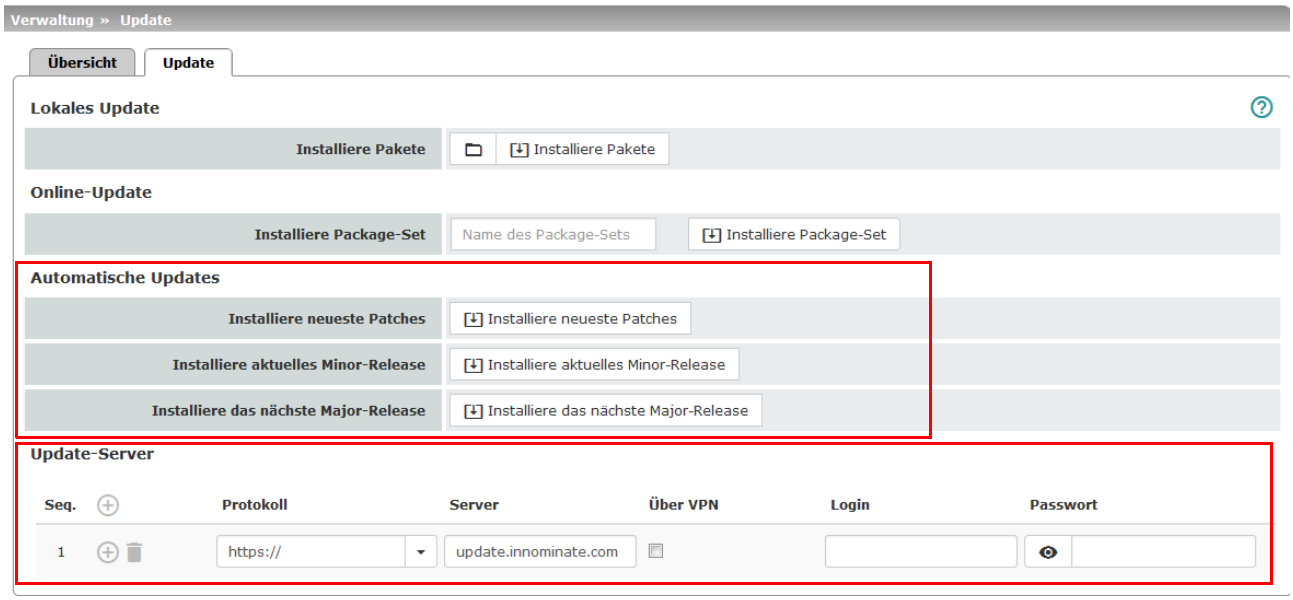
Die Login-Informationen (Login + Passwort) müssen nicht angegeben werden, wenn der werkseitig voreingestellte Update-Server (https://update.innominate.com) verwendet wird.

Ab Firmwareversion 10.3.0 kann die Authentizität eines Update-Server mittels X.509-Zertifikat sichergestellt werden.

2.6.4.3 Automatische Updates

Die Update-Datei wird abhängig von der ausgewählten Update-Option automatisch ermittelt und von einem konfigurierbaren Update-Server geladen und installiert.

Die Initialisierung des Updates erfolgt über die mGuard-Weboberfläche (**Verwaltung >> Update >> Update**) oder den mGuard-Kommandozeilenbefehl *„mg update“* .



Update-Optionen:

a) *Installiere neueste Patches*
b) *Installiere aktuelles Minor-Release*
c) *Installiere das nächste Major-Release*

ACHTUNG: Online- oder Automatische Updates von der installierten Ausgangs-Firmwareversion **7.6.8** können zu einem Fehler führen (siehe Hinweis in Kapitel 2.20).

Es kann vorkommen, dass von einer installierten Firmwareversion ein „**direktes**“ **Automatisches Update** auf das aktuelle Minor- oder das nächste Major-Release nicht möglich ist.

Führen Sie in diesem Fall zunächst ein oder mehrere Updates auf zugelassene Minor- oder Patch-Releases durch. Danach können Sie im letzten Schritt auf das aktuelle Minor- oder das nächste Major-Release updaten.

Die Login-Informationen (Login + Passwort) müssen nicht angegeben werden, wenn der werkseitig voreingestellte Update-Server (https://update.innominate.com) verwendet wird.

2.6.4.4 Flashen der Firmware

Die mGuard-Firmware wird von SD-Karte, USB-Flash-Speicher (beide mit vfat-Dateisystem) oder von einem TFTP-Update-Server geladen und auf dem mGuard-Gerät installiert.

Installierte Lizenzen bleiben nach dem Flashen auf dem Gerät erhalten (bei Geräten mit installierter Firmwareversion 5.0.0 oder höher).

Konfigurationsprofile und Lizenzen können während des Flash-Vorgangs mit installiert und aktiviert werden (siehe Kapitel 2.19, „mGuard Flash Guide“).

ACHTUNG: Das Flashen der Firmware löscht alle Daten, Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt. Eine vorhandene Konfiguration sollte vor dem Flashen als Konfigurationsprofil an einem sicheren Ort gespeichert werden.

ACHTUNG: Ein Downgrade der werkseitig vorinstallierten Firmwareversion wird nicht unterstützt.

Bei mGuard-Geräten, die ab Januar 2018 produziert wurden, kann ein *Downgrade* der werkseitig vorinstallierten Firmwareversion auf eine frühere Firmwareversion fehlschlagen. Flashen Sie in diesem Fall das Gerät erneut mit der ursprünglich installierten oder einer höheren Firmwareversion.

2.7 FL MGUARD RS2000/4000 TX/TX (inkl. -B, -P, -M)

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.7.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!*):

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*
– (Auf 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.7.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD RS4000).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.7.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.7.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-7.{6}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.7.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.7.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.7.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.7.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.7.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.7.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*

– *install-ubi.mpc83xx.p7s*

2.7.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD RS4000).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s*) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.7.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt, bis die LEDs *Stat, Mod* und *Sig* grün leuchten.
   – Das Gerät startet den Flash-Vorgang: Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach der entsprechenden Update-Datei gesucht. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.
2. Blinken die LEDs *Stat, Mod* und *Sig* gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen. (Blinkverhalten abweichend bei gleichzeitigem Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.8 FL MGUARD RS2005/4004 TX bzw. TX/DTX

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.8.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!*):

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*
– (Auf 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.8.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD RS4004).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.8.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon 🗀 **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.8.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion 8.6.1.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.)

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.8.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.8.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.8.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.8.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.8.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.8.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*

– *install-ubi.mpc83xx.p7s*

2.8.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD RS4004).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s*) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.8.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt, bis die LEDs *Stat, Mod* und *Info2* grün leuchten.
   – Das Gerät startet den Flash-Vorgang: Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach der entsprechenden Update-Datei gesucht. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.
2. Blinken die LEDs *Stat, Mod* und *Info2* gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen. (Blinkverhalten abweichend bei gleichzeitigem Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.9 TC MGUARD RS2000/4000 3G VPN

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

Ein **Lokales Update** auf mGuard-Firmwareversion **8.6.1** ist ab Version 8.4.0 möglich.

Online-Update und **Automatische Updates** auf mGuard-Firmwareversion 8.6.1 sind ab Version 8.0.0 möglich.

2.9.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_TC3G_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *gemalto.update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *gemalto.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *gemalto.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*
– (Auf 8.6.1: *gemalto.update-8.{4-5}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *gemalto.update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.9.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 3G).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_vTC3G_8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *gemalto.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.9.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *gemalto.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*.
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.9.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.9.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.9.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.9.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.9.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.9.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.9.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_TC3G_v8.9.3.zip*

Update-Dateien inklusive Modem-Firmware (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*
– *install-ubi.mpc83xx.p7s*
– *pxs8_03001_0100617.usf.xz.p7s*

2.9.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 3G).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_TC3G_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s* und *pxs8_03001_0100617.usf.xz.p7s*) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.9.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt, bis die LEDs *Stat, Mod* und *Info2* grün leuchten.
   – Das Gerät startet den Flash-Vorgang: Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach der entsprechenden Update-Datei gesucht. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.
2. Blinken die LEDs *Stat, Mod* und *Info2* gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen (abweichend bei Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.10 TC MGUARD RS2000/4000 4G VPN

Bestellnummer: 2903588 (RS2000) / 2903586 (RS4000)

Die benötigten Update-Dateien sind abhängig von dem verbauten Modem

Die Geräte 2903588 und 2903586 wurden abhängig von der Baureihe mit zwei unterschiedlichen Modems produziert:

– bis Q3/2021: Hersteller **Huawei**
– ab Q3/2021: Hersteller **Gemalto**

Je nach verbautem Modem benötigen Sie für ein Update auf die Firmwareversion 8.9.3 unterschiedliche Update- bzw. Download-Dateien (siehe Kapitel 2.10.1).

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.10.1 Lokales Update auf 8.9.3

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– Firmware-Update für Geräte mit **Huawei**-Engine:
  – *Update_MPC_TC4G_H_v8.9.3.zip* (siehe unten)
– Firmware-Update für Geräte mit **Gemalto**-Engine (ab Q3/2021):
  – *Update_MPC_TC4G_G_v8.9.3.zip* (siehe unten)

Huawei:
Update_MPC_TC4G_H_v8.9.3.zip

Update-Dateien (= entpackte Zip-Datei):

– *huaweigeneric.update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *huaweigeneric.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *huaweigeneric.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*
– (Auf 8.6.1: *huaweigeneric.update-8.{4-5}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *huaweigeneric.update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.10.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 4G).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_TC4G_H_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *huaweigeneric.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.10.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *huaweigeneric.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

Gemalto:
Update_MPC_TC4G_G_v8.9.3.zip

Update-Dateien (= entpackte Zip-Datei):
– *PLS8-E.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *PLS8-E.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.10.1.3 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 4G).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_TC4G_G_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *PLS8-E.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.10.1.4 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *PLS8-E.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.10.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-8.{4-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.10.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.10.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.10.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.10.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.10.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.10.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_TC4G_v8.9.3.zip*

Update-Dateien inkl. Modem-Firmware (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*
– *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

2.10.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 4G VPN).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_TC4G_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s,* pls8-e_rev04.004_arn01.000.11.usf.xz.p7s und ME909u-521_UPDATE_12.636.12.01.00.BIN.xz.p7s) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.10.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt, bis die LEDs *Stat, Mod* und *Info2* grün leuchten.
   – Das Gerät startet den Flash-Vorgang: Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach der entsprechenden Update-Datei gesucht. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.
2. Blinken die LEDs *Stat, Mod* und *Info2* gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen (abweichend bei Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.11 TC MGUARD RS2000/4000 4G VZW VPN

Bestellnummer: 1010462 (RS2000) / 1010461 (RS4000)

2.11.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_TC4GVZW_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *HL7518.update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *HL7518.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *HL7518.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.11.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 4G VZW VPN).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_TC4GVZW_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *HL7518.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.11.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon 🗀 **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *HL7518.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.11.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

– *update-8.{6-7}-8.9.3.default*
– *update-8.{8}-8.9.3.default*
– *update-8.{9}-8.9.3.default*

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.11.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.11.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   – z. .B. Minor-Update: *update-8.{8}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.11.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.11.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.11.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.11.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_TC4GVZW_v8.9.3.zip*

Update-Dateien inkl. Modem-Firmware (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*
– *install-ubi.mpc83xx.p7s*
– *RHL75xx.4.04.142600.201801231340.x7160_1_signed_dwl.dwl.xz.p7s*

2.11.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 4G VZW VPN).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_TC4GVZW_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s* und RHL75xx.4.04.142600.201801231340.x7160_1_signed_dwl.dwl.xz.p7s) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.11.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt, bis die LEDs *Stat, Mod* und *Info2* grün leuchten.
   – Das Gerät startet den Flash-Vorgang: Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach der entsprechenden Update-Datei gesucht. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.
2. Blinken die LEDs *Stat, Mod* und *Info2* gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen (abweichend bei Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.12 TC MGUARD RS2000/4000 4G ATT VPN

Bestellnummer: 1010464 (RS2000) / 1010463 (RS4000)

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.
Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.12.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_TC4GATT_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *HL7588.update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *HL7588.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *HL7588.update-8.{9}-8.9.3.default.mpc83xx.tar.gz*

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.12.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 4G ATT VPN).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_TC4GATT_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *HL7588.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.12.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon 🗀 **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *HL7588.update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.12.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!***):**

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

– *update-8.{6-7}-8.9.3.default*
– *update-8.{8}-8.9.3.default*
– *update-8.{9}-8.9.3.default*

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.12.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.12.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   – z. .B. Minor-Update: *update-8.{8}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.12.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.12.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.12.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.12.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_TC4GATT_v8.9.3.zip*

Update-Dateien inkl. Modem-Firmware (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*
– *install-ubi.mpc83xx.p7s*
– *RHL75xx.A.2.15.151600.201809201422.x7160_3_signed_DWL.dwl.xz.p7s*

2.12.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. TC MGUARD RS4000 4G ATT VPN).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_TC4GATT_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s* und RHL75xx.A.2.15.151600.201809201422.x7160_3_signed_DWL.dwl.xz.p7s) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.12.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt, bis die LEDs *Stat, Mod* und *Info2* grün leuchten.
   – Das Gerät startet den Flash-Vorgang: Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach der entsprechenden Update-Datei gesucht. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.
2. Blinken die LEDs *Stat, Mod* und *Info2* gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen (abweichend bei Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.13 FL MGUARD PCI(E)4000

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.13.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*
– (Auf 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.13.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD PCI4000).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.13.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.13.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-7.{6}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.13.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.13.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.13.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.13.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.13.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.13.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*

– *install-ubi.mpc83xx.p7s*

2.13.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD PCI4000).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s*) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.13.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt: Die beiden WAN LEDs und die obere LAN LED leuchten gleichzeitig grün. Lassen Sie während dieser grünen Leuchtphase die Reset-Taste los.
   – Das Gerät startet den Flash-Vorgang: Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach der entsprechenden Update-Datei gesucht. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.
2. Blinken die beiden WAN LEDs und die obere LAN LED gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen. (Blinkverhalten abweichend bei gleichzeitigem Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.14 FL MGUARD SMART2

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.14.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*
– (Auf 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.14.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD SMART2).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.14.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.14.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-7.{6}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.14.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.14.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.14.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.14.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.14.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.14.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*

– *install-ubi.mpc83xx.p7s*

2.14.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD SMART2).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s*) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server.

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.14.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt, bis alle drei LEDs grün leuchten.
   – Das Gerät startet den Flash-Vorgang: Das Gerät sucht über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden vom TFTP-Server geladen und installiert.
2. Blinken alle drei LEDs gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen. (Blinkverhalten abweichend bei gleichzeitigem Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.15 FL MGUARD CENTERPORT

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.15.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_X86_v8.9.3zip*

Update-Dateien (= entpackte Zip-Datei):

– *update-8.{6-7}-8.9.3.default.x86_64.tar.gz*
– *update-8.{8}-8.9.3.default.x86_64.tar.gz*
– *update-8.{9}-8.9.3.default.x86_64.tar.gz*
– (Auf 8.6.1: *update-7.{6}-8.6.1.default.x86_64.tar.gz*)
– (Auf 8.6.1: *update-8.{0-5}-8.6.1.default.x86_64.tar.gz*)
– (Auf 8.6.1: *update-8.{6}-8.6.1.default.x86_64.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.15.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD CENTERPORT).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_X86_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.x86_64.tar.gz* .

2.15.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.x86_64.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.15.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-7.{6}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.15.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.15.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.15.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.15.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.15.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.15.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_X86_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *firmware.img.x86_64.p7s*

– *install.x86_64.p7s*

2.15.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD CENTERPORT).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_X86_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*firmware.img.x86_64.p7s, install.x86_64.p7s*) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte oder dem USB-Flash-Laufwerk).

2.15.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte / USB-Flash-Laufwerk geladen. Nur wenn keine SD-Karte/kein USB-Flash-Laufwerk gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Schließen Sie eine USB-Tastatur und einen Monitor an das Gerät an.
2. Starten Sie das Gerät neu.
3. Sobald das Gerät bootet, drücken Sie auf der USB-Tastatur mehrmals eine der Pfeiltasten: ↑, ↓, ← oder → bis der Bootvorgang unterbrochen wird.
4. Das Boot-Menü wird angezeigt.

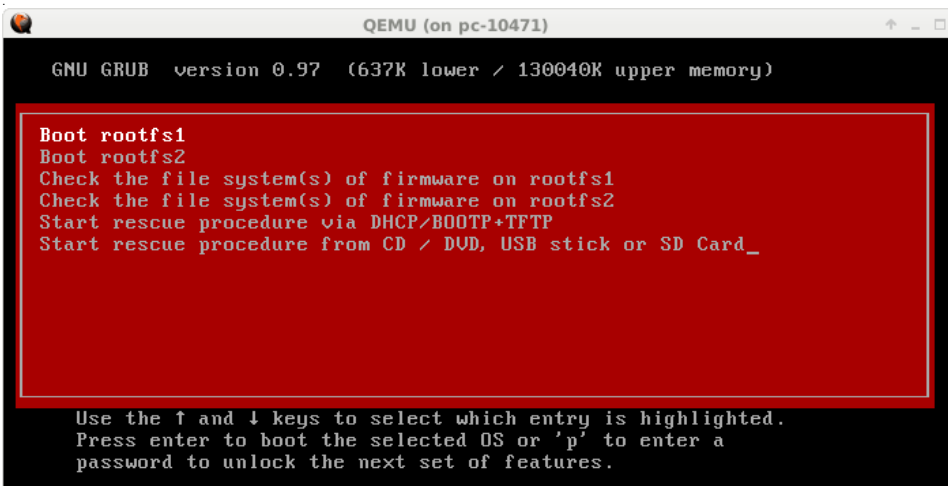


Bild 2-2 Boot-Menü

5. Wählen Sie mit den Pfeiltasten ↓ bzw. ↑ eine der beiden Optionen zur Durchführung der Flash-Prozedur (Rescue-Prozedur) aus:

– **Start rescue procedure via DHCP / BOOTP+TFTP**

– **Start rescue procedure from CD / DVD, USB stick or SD Card**

Drücken Sie zum Inkraftsetzen der Auswahl die **Enter**-Taste.

Start rescue procedure via DHCP / BootP+TFTP

Wirkung: Das Gerät lädt die notwendigen Dateien vom TFTP-Server:

– *install.x86_64.p7s*

– *firmware.img.x86_64.p7s*

Nach Abschluss des Flash-Vorgangs befindet sich das Gerät im Auslieferungszustand (werkseitige Voreinstellung).

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

Allgemeine Voraussetzungen:

1. Ein an den USB-Port angeschlossenes CD/DVD-Laufwerk oder
2. ein an den USB-Port angeschlossener USB stick (USB-Flash-Laufwerk) oder
3. eine in das SD-Card-Laufwerk eingesetzte SD-Speicherkarte.
4. Die notwendigen Update-Dateien wurde auf dem Installationsmedium in folgende Verzeichnisse kopiert:
   – */Firmware/install.x86_64.p7s*
   – */Firmware/firmware.img.x86_64.p7s*

Wirkung: Nach dem Starten des Flash-Vorgangs durch drücken der Enter-Taste werden die notwendigen Daten von dem ausgewählten Medium geladen. Nach Abschluss des Flash-Vorgangs befindet sich das Gerät im Auslieferungszustand (werkseitige Voreinstellung).

2.16 FL MGUARD GT/GT

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.16.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*
– (Auf 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.16.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD GT/GT).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.16.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon 🗀 **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.16.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!***):**

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-7.{6}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.16.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.16.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.16.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.16.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wähle Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.16.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wähle Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.16.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_GTGT_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *jffs2.img.mpc83xx.p7s*

– *install.mpc83xx.p7s*

2.16.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD GT/GT).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_GTGT_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*jffs2.img.mpc83xx.p7s, install.mpc83xx.p7s*) aus dem Verzeichnis *GTGT* ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server.

2.16.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein.

1. Starten Sie den Flash-Vorgang, indem Sie die Mode-Taste drücken (siehe „Kapitel 2.16.4.3, „Funktionsauswahl mittels Mode-Taste (Smart-Mode)““.
   – Das Gerät sucht über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden vom TFTP-Server geladen und installiert.
2. Wird im Display die **05** angezeigt und blinken die LEDs gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen. (Blinkverhalten abweichend bei gleichzeitigem Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.16.4.3 Funktionsauswahl mittels Mode-Taste (Smart-Mode)

Smart-Mode aktivieren

Über die Mode-Taste wird der Smart-Mode aufgerufen/verlassen und die gewünschte Funktion gewählt. Die drei Mode-LEDs zeigen, welche Einstellung aktuell ist und beim Verlassen des Smart-Mode berücksichtigt wird.

Smart-Mode aufrufen

- Trennen Sie das Gerät von der Spannungsversorgung.
- Halten Sie unmittelbar nach dem Einschalten der Versorgungsspannung die Mode-Taste **länger als zehn Sekunden** gedrückt. Die drei Mode-LEDs blinken dreimal kurz und zeigen, dass der Smart-Mode aktiviert ist.
- Zu Beginn des Smart-Modes befindet sich das Gerät zunächst im Zustand „Verlassen ohne Änderung“ („51“ im Display).

Gewünschten Einstellung auswählen

- Um die unterschiedlichen Einstellungen zu wählen, wird die Mode-Taste kurz gedrückt und die gewünschte Betriebsart mit Hilfe eines binären Leuchtmusters der Mode-LEDs und eines Codes auf dem 7-Segment-Display ausgewählt.

Smart-Mode verlassen und Auswahl aktivieren

- Zum Verlassen halten Sie die Mode-Taste mindestens fünf Sekunden gedrückt und die zuletzt gewählte Funktion wird ausgeführt.

Mögliche Funktionen im Smart-Mode

Das Gerät unterstützt die Auswahl der folgenden Funktionen im Smart-Mode (siehe auch nachfolgendes Beispiel):

Tabelle 2-4 Funktionen im Smart-Mode

Funktion	7-Segment-Display	ACT LED 1	SPD LED 2	FD LED 3
Verlassen des Smart-Mode ohne Änderung	51	Aus	Aus	**Ein**
Aktivieren der Recovery-Prozedur	55	**Ein**	Aus	**Ein**
Aktivieren der Flash-Prozedur	56	**Ein**	**Ein**	Aus
Customized-Default-Profil anwenden	57	**Ein**	**Ein**	**Ein**

2.17 FL MGUARD DELTA TX/TX

Ein Update auf mGuard-Firmwareversion 8.9.3 ist ab Version 8.6.1 möglich.

Führen Sie gegebenenfalls das Update in zwei Schritten durch, indem Sie die Version < 8.6.1 zunächst auf die Version 8.6.1 updaten. Im nächsten Schritt können Sie diese Version auf Version 8.9.3 updaten.

2.17.1 Lokales Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *update-8.{6-7}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
– *update-8.{9}-8.9.3.default.mpc83xx.tar.gz*
– (Auf 8.6.1: *update-7.{6}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz*)
– (Auf 8.6.1: *update-8.{6}-8.6.1.default.mpc83xx.tar.gz*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.17.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD DELTA).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_MPC_v8.9.3.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*

2.17.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *update-8.{8}-8.9.3.default.mpc83xx.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.17.2 Online-Update auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

Zu verwendender Package-Set-Name (*abhängig von installierter Firmwareversion!*):

Ein Package-Set-Name beschreibt, von welchen Firmwareversionen auf die aktuelle Firmwareversion upgedatet werden kann.

- *update-8.{6-7}-8.9.3.default*
- *update-8.{8}-8.9.3.default*
- *update-8.{9}-8.9.3.default*
- (Auf 8.6.1: *update-7.{6}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{0-5}-8.6.1.default*)
- (Auf 8.6.1: *update-8.{6}-8.6.1.default*)

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen unter Angabe des Package-Set-Namens aktualisiert werden können (siehe Kapitel 2.6.3).

2.17.2.1 Online-Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.17.2.2 Online-Update durchführen

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Geben Sie in Sektion **Online Update** unter **Installiere Package-Set** den Namen des gewünschten Package-Sets ein:
   - z. .B. Minor-Update: *update-8.{6-7}-8.9.3.default*
4. Klicken Sie auf die Schaltfläche **Installiere Package-Set**, um das Update zu starten.

2.17.3 Automatische Updates auf 8.9.3

Möglich ab installierter Firmwareversion **8.6.1**.

2.17.3.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.17.3.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.17.4 Firmwareversion 8.9.3 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *FW_MPC_v8.9.3.zip*

Update-Dateien (= entpackte Zip-Datei):

– *ubifs.img.mpc83xx.p7s*

– *install-ubi.mpc83xx.p7s*

2.17.4.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD DELTA).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *FW_MPC_v8.9.3.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie alle entpackten Dateien (*ubifs.img.mpc83xx.p7s, install-ubi.mpc83xx.p7s*) aus dem Verzeichnis *mpc* in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *ubifs.img.mpc83xx.p7s* und *install-ubi.mpc83xx.p7s* können zum Flashen aller in diesem Dokument beschriebenen Geräte verwendet werden, mit Ausnahme von FL MGUARD CENTERPORT und FL MGUARD GT/GT.

2.17.4.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

1. Halten Sie die Reset-Taste des Geräts gedrückt, bis die drei unteren LEDs auf der linken Seite (ERR, FAULT, INFO) grün leuchten.
   – Das Gerät startet den Flash-Vorgang: Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach der entsprechenden Update-Datei gesucht. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen. Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.
2. Blinken die drei unteren LEDs auf der rechten Seite (ERR, FAULT, INFO) gleichzeitig grün, wurde der Flash-Vorgang erfolgreich abgeschlossen. (Blinkverhalten abweichend bei gleichzeitigem Hochladen eines Konfigurationsprofils).
3. Starten Sie das Gerät neu.

2.18 FL MGUARD 2102/2105, 4302/4305, 4102 PCI(E)

Ein Update auf mGuard-Firmwareversion 10.4.1 ist ab Version 10.0.0 möglich.

2.18.1 Lokales Update auf 10.4.1

Benötigte Dateien (*abhängig von installierter Firmwareversion!***):**

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Update_mGuard-10.4.1.zip*

Update-Dateien (= entpackte Zip-Datei):

– *update-10.{0-4}-10.4.1.default.aarch64.tar.gz*

Die geschweifte Klammer gibt an, welche installierten Ausgangs-Firmwareversionen mit der Update-Datei aktualisiert werden können (siehe Kapitel 2.6.3).

2.18.1.1 Update-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD 4305).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die **Download-Datei** *Update_mGuard-10.4.1.zip* herunter.
6. Entpacken Sie die Zip-Datei.
7. Verwenden Sie die **Update-Datei**, die für die auf Ihrem Gerät installierte Firmwareversion vorgesehen ist (siehe Kapitel 2.6.3):
   – z. B. Minor-Update: *update-10.{0-4}-10.4.1.default.aarch64.tar.gz*

2.18.1.2 Lokales Update installieren

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in der Sektion **Lokales Update** unter **Installiere Pakete** auf das Icon **Keine Datei ausgewählt.**
4. Selektieren Sie die heruntergeladene **Update-Datei**:
   – z. B. Minor-Update: *update-10.{0-4}-10.4.1.default.aarch64.tar.gz*
5. Klicken Sie auf die Schaltfläche **Installiere Pakete**, um das Update zu starten.

2.18.2 Automatische Updates auf 10.4.1

2.18.2.1 Automatische Updates vorbereiten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Stellen Sie sicher, dass in Sektion **Update-Server** mindestens ein gültiger Update-Server eingetragen ist.

2.18.2.2 Automatische Updates starten

1. Melden Sie sich als Benutzer *admin* auf der Weboberfläche des mGuard-Geräts an.
2. Wählen Sie **Verwaltung** >> **Update** >> **Update**.
3. Klicken Sie in Sektion **Automatische Updates** auf die Schaltfläche des gewünschten Update-Verfahrens, um das Update zu starten:
   a) Installiere neueste Patches
   b) Installiere aktuelles Minor-Release
   c) Installiere das nächste Major-Release

2.18.3 Firmwareversion 10.4.1 flashen

Benötigte Dateien:

Download-Datei auf der gerätespezifischen Produktseite im Phoenix Contact Web Shop:

– *Firmware_mGuard-10.4.1.zip*

Update-Dateien (= entpackte Zip-Datei):

– *firmware.img.aarch64.p7s*

– *install.aarch64.p7s*

2.18.3.1 Flash-Datei herunterladen

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter: phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD 4305).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie folgende **Download-Datei** herunter: *Firmware_mGuard-10.4.1.zip*
6. Entpacken Sie die Zip-Datei.
7. Kopieren Sie die entpackten Dateien (*firmware.img.aarch64.p7s, install.aarch64.p7s*) in ein beliebiges Verzeichnis (z. B. *mGuard-Firmware*) auf Ihrem TFTP-Server oder in das Verzeichnis *Firmware* auf der SD-Karte).

Die Dateien *firmware.img.aarch64.p7s* und *install.aarch64.p7s* können zum Flashen aller in diesem Kapitel beschriebenen Geräte verwendet werden (Geräte der Plattform 3 mit installierter Firmwareversion 10.x).

2.18.3.2 mGuard-Gerät flashen

ACHTUNG: Das Flashen der Firmware löscht alle Passwörter und Konfigurationen auf dem mGuard-Gerät. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Der TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein.

Beschädigung des Geräts bei vorzeitigem Abbruch

Starten Sie das Gerät erst dann neu, wenn die Flash-Prozedur vollständig abgeschlossen wurde. (Dauer: ca. 2 Minuten).

FL MGUARD 2102/4302
FL MGUARD 2105/4305

Flash-Prozedur ausführen (Tragschienen-Geräte)

- Halten Sie die Mode-Taste des Geräts mindestens 9 Sekunden gedrückt, bis die **LEDs PF1–5** grün leuchten.
- Lassen Sie die Mode-Taste los. Ansonsten wird das Gerät neu gestartet.

⇒ Die Flash-Prozedur wird ausgeführt.

⇒ Nach ca. 20 Sekunden leuchten die LEDs **PF1-3** im Modus „Lauflicht/Running light“ (grün). Die LED **FAIL** leuchtet (rot):

– Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach den entsprechenden Update-Dateien gesucht.

– Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle (XF2) nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

⇒ Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.

⇒ Das Gerät wird während der Flash-Prozedur einmal automatisch neu gestartet.

Schalten Sie das Gerät auf keinen Fall vorzeitig aus. Warten Sie, bis die Flash-Prozedur **vollständig** beendet wurde.

⇒ Die LED **FAIL** leuchtet anschließend permanent (rot).

⇒ Nach weiteren ca. 60 Sekunden blinken die LEDs **PF1-3** (grün).

⇒ Die Flash-Prozedur wurde erfolgreich beendet. Dauer: ca. 2 Minuten.

- Starten Sie das Gerät neu, indem Sie kurz die Mode-Taste drücken oder das Gerät vorübergehenden von der Spannungsversorgung trennen.

⇒ Das Gerät ist betriebsbereit, wenn die LED **PF1** grün blinkt (Herzschlag).

FL MGUARD 4102 PCI(E) **Flash-Prozedur ausführen (PCI-Karten)**

- Halten Sie die Mode-Taste an der Frontblende des Geräts mindestens 9 Sekunden gedrückt, bis die **LED PF1** sowie die **LEDs der Ethernet-Buchsen** (XF1/2) grün leuchten.
- Lassen Sie die Mode-Taste los. Ansonsten wird das Gerät neu gestartet.

⇒ Die Flash-Prozedur wird ausgeführt.

  – Zunächst wird nach einer eingelegten SD-Karte und dort im Verzeichnis *Firmware* nach den entsprechenden Update-Dateien gesucht.
  – Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle (XF2) nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

⇒ Die benötigten Dateien werden von der SD-Karte oder dem TFTP-Server geladen und installiert.

⇒ Das Gerät wird während der Flash-Prozedur mehrmals automatisch neu gestartet.

⇒ Die LED **PF1/FAIL** leuchtet und blinkt grün und rot.

⇒ Nach weiteren ca. 60 Sekunden blinken die **SPD-LEDs** (XF1/2) zusätzlich grün.

⇒ Die Flash-Prozedur wurde erfolgreich beendet. Dauer: ca. 2 Minuten.

- Starten Sie das Gerät neu.

⇒ Das Gerät ist betriebsbereit, wenn die LED **PF1** grün blinkt (Herzschlag).

2.19 mGuard Flash Guide

2.19.1 mGuard-Geräte flashen

Die mGuard-Firmware wird von SD-Karte, USB-Flash-Speicher (beide mit vfat-Dateisystem) oder von einem TFTP-Update-Server auf das mGuard-Gerät geladen und installiert. Alle Daten, Passwörter und Konfigurationen auf dem Gerät werden gelöscht. Das Gerät wird auf seine werkseitige Voreinstellung zurückgesetzt.

Die Durchführung des Flash-Vorgangs wird in diesem Dokument für jedes mGuard-Gerät individuell beschrieben (siehe gerätespezifische Kapitel „*Firmwareversion x.x.x flashen*“).

ACHTUNG: Ein Downgrade der werkseitig vorinstallierten Firmwareversion wird nicht unterstützt.

Bei mGuard-Geräten, die ab Januar 2018 produziert wurden, kann ein *Downgrade* der werkseitig vorinstallierten Firmwareversion auf eine frühere Firmwareversion fehlschlagen. Flashen Sie in diesem Fall das Gerät erneut mit der ursprünglich installierten oder einer höheren Firmwareversion.

2.19.2 Probleme mit nicht kompatiblen SD-Karten

Wenn Sie das mGuard-Gerät von einer SD-Karte eines anderen Herstellers als PHOENIX CONTACT flashen, kann es vorkommen, dass der in diesem Dokument beschriebenen Flash-Vorgang fehlschlägt.

Um Probleme beim Flashen mit SD-Karten anderer Hersteller zu vermeiden, gehen Sie im Verlauf des jeweils beschriebenen Flash-Vorgangs wie folgt vor:

1. Stecken Sie die SD-Karte **locker** in den Steckplatz, ohne sie einrasten zu lassen.
2. Starten Sie den Flash-Vorgang wie beschrieben.
3. Halten Sie die Reset-Taste des Geräts gedrückt, bis die entsprechenden LEDs wie beschrieben leuchten.
4. Lassen Sie die Reset-Taste los.
5. Stecken Sie umgehend die SD-Karte **fest** in den Steckplatz ein, sodass sie einrastet.
6. Warten Sie, bis der Flash-Vorgang beendet wurde, und starten Sie das Gerät neu.

2.19.3 Konfigurationsprofil während des Flash-Vorgangs hochladen

Sie können ein erstelltes Konfigurationsprofil (ATV-Profil) während des Flash-Vorgangs automatisch auf das mGuard-Gerät hochladen und aktivieren.

Das Blinkverhalten der LEDs nach dem Beenden des Flash-Vorgangs ist in diesem Fall abweichend vom Standardblinkverhalten.

2.19.3.1 Vorbereitung

Erstellen Sie die Datei *preconfig.sh* mit folgendem Inhalt:

Für unverschlüsselte ATV-Profile

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

Für verschlüsselte ATV-Profile

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

Wenn Sie ein mit dem Gerätezertifikat verschlüsseltes Konfigurationsprofil hochladen wollen, sollten Sie die Datei von **.atv* in **.atv.p7e* umbenennen. Verschlüsselte und unverschlüsselte Konfigurationsprofile können so leichter auseinandergehalten werden.

Das mGuard-Gerät behandelt das ATV-Profil unabhängig von der Dateiendung gleich.

Während des Flash-Vorgangs sucht das Gerät nach folgenden Dateien und lädt sie hoch:

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

2.19.3.2 Konfigurationsprofil von SD-Karte laden

Um ein Konfigurationsprofil während des Flash-Vorgangs hochzuladen und zu aktivieren, gehen Sie wie folgt vor:

1. Erstellen Sie neben dem Verzeichnis *Firmware* das Verzeichnis *Rescue Config.*
2. Benennen Sie das gespeicherte Konfigurationsprofil um in *preconfig.atv oder <Seriennummer>.atv*.
3. Kopieren Sie das Konfigurationsprofil in das Verzeichnis *Rescue Config*.
4. Kopieren Sie die Datei *preconfig.sh* (UNIX-Format) in das Verzeichnis *Rescue Config*.
5. Führen Sie den Flash-Vorgang wie für Ihre Gerät beschrieben durch.

2.19.3.3 Konfigurationsprofil vom TFTP-Server laden

Um ein Konfigurationsprofil während des Flash-Vorgangs zu laden und zu aktivieren, siehe Beschreibung in Kapitel 2.19.5, „DHCP- und TFTP-Server einrichten“.

2.19.4 Lizenzdatei während des Flash-Vorgangs hochladen

Nicht bei Geräten der FL MGUARD 2000/4000-Serie mit installierter Firmwareversion mGuard 10.x.

Sie können eine Lizenzdatei während des Flash-Vorgangs auf das mGuard-Gerät hochladen und aktivieren (z. B. eine Lizenz für mehr VPN-Verbindungen *FL MGUARD LIC VPN-10* oder für ein Lifetime-Software-Update *FL MGUARD LIC LIFETIME FW*).

2.19.4.1 Von SD-Karte

Um eine Lizenzdatei während des Flash-Vorgangs hochzuladen und zu aktivieren, gehen Sie wie folgt vor:

1. Erstellen Sie auf dem Installationsmedium das Verzeichnis *Rescue Config.*
2. Kopieren Sie die Lizenzdatei in das Verzeichnis *Rescue Config.*
3. Benennen Sie die Lizenzdatei um in *license.lic oder <Seriennummer>.lic*.
4. Führen Sie den Flash-Vorgang wie für Ihre Gerät beschrieben durch.

2.19.4.2 Vom TFTP-Server

Um eine Lizenzdatei während des Flash-Vorgangs zu laden und zu aktivieren, siehe Kapitel 2.19.5, „DHCP- und TFTP-Server einrichten“.

2.19.5 DHCP- und TFTP-Server einrichten

Netzwerkprobleme

Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

Software von Drittanbietern

Phoenix Contact übernimmt keine Garantie oder Haftung bei der Verwendung von Produkten von Drittanbietern. Verweise auf Drittanbieter-Software stellen keine Empfehlung dar, sondern sind Beispiele für grundsätzlich verwendbare Programme.

2.19.5.1 Unter Windows

Falls Sie das Drittanbieter-Programm „*TFTPD32.exe*“ verwenden wollen, beschaffen Sie sich das Programm aus einer vertrauenswürdigen Quelle und gehen Sie wie folgt vor:

1. Wenn der Windows-Rechner an ein Netzwerk angeschlossen ist, trennen Sie ihn von diesem.
2. Erstellen Sie ein Verzeichnis auf dem Windows-Rechner, das Sie für den Flash-Vorgang von mGuard-Geräten verwenden wollen. Dieses Verzeichnis wird später als Root-Verzeichnis des TFTP-Servers ausgewählt. Während des Flash-Vorgangs werden alle benötigten Dateien aus diesem Verzeichnis geladen.
3. Kopieren Sie die gewünschten Firmware-Image-Datei(en) in das erstellte Verzeichnis.
4. **(Lizenzdatei hochladen)** Wenn eine **Lizenzdatei** während des Flash-Vorgangs auf das mGuard-Gerät hochgeladen und installiert werden soll, kopieren Sie die Datei in das erstellte Verzeichnis. Benennen Sie die Datei wie folgt:
   - *license.lic* oder
   - *<Seriennummer>.lic.*
5. **(Konfigurationsprofil hochladen)** Wenn eine Konfigurationsprofil während des Flash-Vorgangs auf das mGuard-Gerät hochgeladen und aktiviert werden soll, kopieren Sie das entsprechende **Rollout-Skript** (*rollout.sh*, siehe Kapitel 2.19.6, „Beispiel-Skript: rollout.sh“) und das **Konfigurationsprofil** in das erstellte Verzeichnis. Benennen Sie das Konfigurationsprofil wie folgt:
   - *preconfig.atv* (wenn alle mGuard-Geräte dieselbe Konfiguration erhalten sollen) oder
   - *<Seriennummer>.atv* (wenn jedes mGuard-Gerät eine individuelle Konfiguration erhalten soll).
6. Starten Sie das Programm *TFTPD32.exe*

   Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.
7. Klicken Sie die Schaltfläche **Browse**, um auf den Ordner zu wechseln, wo die mGuard-Image-Dateien gespeichert sind: (z. B. *install-ubi.mpx83xx.p7s, ubifs.img.mpc.p7s*).

8. Stellen Sie sicher, dass es sich um die Lizenzdatei handelt, die wirklich zum Gerät gehört (in der Weboberfläche unter „Verwaltung >> Update“).

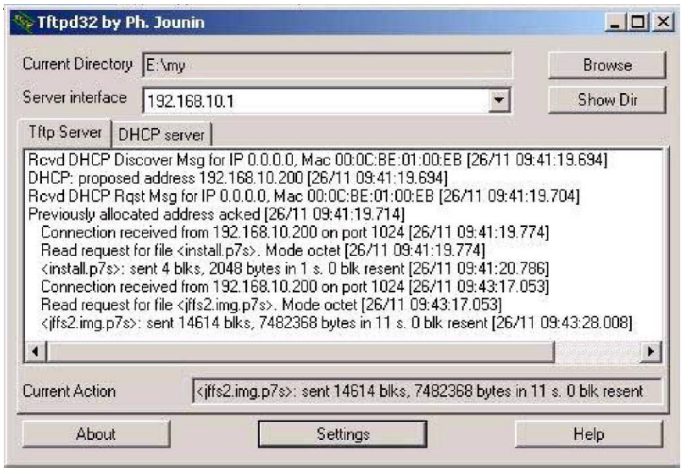
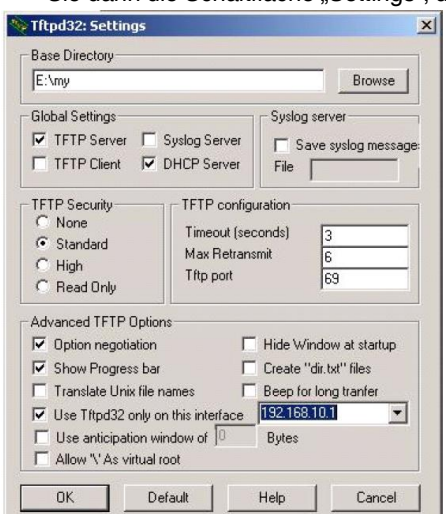


Bild 2-3 Host-IP eingeben

9. Wechseln Sie auf die Registerkarte „TFTP-Server“ bzw. „DHCP-Server“ und klicken Sie dann die Schaltfläche „Settings“, um die Parameter wie folgt zu setzen:



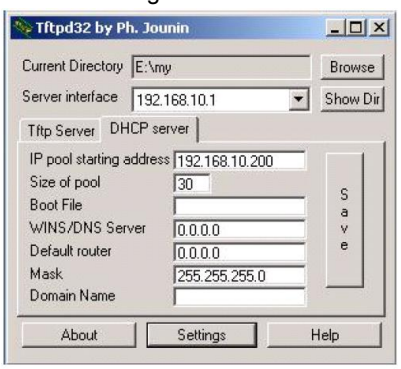


Bild 2-4 Settings

2.19.5.2 Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server.

1. Installieren Sie die entsprechenden Pakete nach der Anleitung der jeweiligen Distribution.
2. Konfigurieren Sie den DHCP-Server, indem Sie in der Datei */etc/dhcpd.conf* folgende Einstellungen vornehmen:
   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;}
   Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert: */etc/inetd.conf*

3. Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: */tftpboot*)
   tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
   Im Verzeichnis */tftpboot* müssen die mGuard-Imagedateien gespeichert sein:
   z. B. *install-ubi.mpx83xx.p7s, ubifs.img.mpc.p7s*.
4. **(Lizenzdatei hochladen)** Wenn eine **Lizenzdatei** während des Flash-Vorgangs auf das mGuard-Gerät hochgeladen und installiert werden soll, kopieren Sie die Datei in das Verzeichnis /*tftpboot*. Benennen Sie die Datei wie folgt:
   – *license.lic* oder
   – <*Seriennummer*>*.lic*.
5. **(Konfigurationsprofil hochladen)** Wenn eine Konfigurationsprofil während des Flash-Vorgangs auf das mGuard-Gerät hochgeladen und aktiviert werden soll, kopieren Sie das entsprechende **Rollout-Skript** (*rollout.sh*, siehe Kapitel 2.19.6, „Beispiel-Skript: rollout.sh“) und das *Konfigurationsprofil* in das Verzeichnis /*tftpboot*. Benennen Sie das Konfigurationsprofil wie folgt:
   – *preconfig.atv* (wenn alle mGuard-Geräte dieselbe Konfiguration erhalten sollen) oder
   – <*Seriennummer*>*.atv* (wenn jedes mGuard-Gerät eine individuelle Konfiguration erhalten soll).
6. Starten Sie dann den *inetd*-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
7. Wenn Sie einen anderen Mechanismus verwenden, z. B. *xinetd*, dann informieren Sie sich in der entsprechenden Dokumentation.

2.19.5.3 TFTP-Server: Fehlermeldungen

Während des Flash-Vorgangs sucht das mGuard-Gerät standardmäßig nach den Dateien *rollout.sh, license.lic* und *<Seriennummer>.lic*. Sind diese Dateien nicht vorhanden, wird eine entsprechende Fehlermeldung angezeigt:

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.

Die Fehlermeldung kann ignoriert werden, wenn keine Lizenzdatei hochgeladen bzw. das mGuard-Gerät nicht über das Skript *rollout.sh* vorkonfiguriert werden soll. Der Flash-Vorgang wird in diesen Fällen planmäßig fortgesetzt.

2.19.6 Beispiel-Skript: rollout.sh

Verwendung von Rollout-Skripten

Die Implementierung und Verwendung eines Rollout-Skripts ist kein von PHOENIX CONTACT unterstützter Bestandteil des mGuard-Produkts bzw. der mGuard-Firmware. Die Verantwortung für die Implementierung und Verwendung eines Rollout-Skripts liegt allein beim Kunden und nicht bei PHOENIX CONTACT.

Während des Flash-Vorgangs überprüft das mGuard-Gerät das Vorhandensein der Datei *rollout.sh*. Diese Datei muss sich im gleichen Verzeichnis wie die Firmware-Image-Datei auf dem TFTP-Server befinden. Wenn die Datei existiert, wird sie auf das mGuard-Gerät hochgeladen und dort ausgeführt.

Bei der Datei *rollout.sh* muss es sich um ein UNIX-Shell-Skript handeln. Mit dem Skript können die Konfigurationsdaten für das mGuard-Gerät vom TFTP-Server abgefragt und das Konfigurationsprogramm des mGuard-Geräts (*gaiconfig*) gestartet werden.

Das an dieser Stelle dokumentierte Rollout-Skript dient als Vorlage und kann nur in einer durch den Kunden individuell angepassten Form verwendet werden. Grundsätzlich kann der Rollout-Support auf zwei Arten implementiert werden, so dass

– „**alle**“ mGuard-Geräte die gleiche Konfiguration (**statisches TFTP**) erhalten, oder
– „**jeder**“ mGuard erhält seine eigene individuelle Konfiguration, abhängig von seiner Seriennummer (**dynamisches TFTP**).

2.19.6.1 Statisches TFTP (Standardkonfiguration für jedes mGuard-Gerät)

Im Folgenden wird ein Beispielskript *rollout.sh* dokumentiert, das über *tftp* eine Standardkonfigurationsdatei zur Installation auf mGuard-Geräten vom TFTP-Server herunterlädt. Der im Skript definierte Name der Konfigurationsdatei lautet: *preconfig.atv*.

```
#!/bin/sh -ex
# The IP address of the DHCP/TFTP server
# is supplied by install.p7s | install-ubi.mpc83xx.p7s | install.mpc83xx.p7s |
# 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 - -r "$cfg_name" "${server}" | dd bs=1M of=/bootstrap/preconfig.atv

# create a small configuration-script that installs the
# configuration fetched from ${server}

cat >/bootstrap/preconfig.sh <<EOF

#!/bin/sh

modprobe param_dev 2>/dev/null
gaiconfig --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
```

2.19.6.2 Dynamisches TFTP (individuelle Konfiguration für jedes mGuard-Gerät)

Im Folgenden wird ein Beispielskript *rollout. sh* dokumentiert, das über *tftp* eine gerätespezifische Konfigurationsdatei vom TFTP-Server herunterlädt. Der im Skript definierte Name der Konfigurationsdatei lautet: <*serialnumber*>.*atv*.

```
#!/bin/sh -ex

# The IP address of the DHCP/TFTP server
# is supplied by install.p7s | install-ubi.mpc83xx.p7s | install.mpc83xx.p7s |
# install.aarch64.p7s

server=$1
export PATH=/bin:/bootstrap
mount -t proc none /proc || : mount -t sysfs sysfs /sys || :
if test -f /proc/sys/mguard/parameter/oem_serial ; then SERIAL=`cat
/proc/sys/mguard/parameter/oem_serial`
else
SERIAL=`sysmguard param oem_serial`
fi

# This is the filename of the user supplied static configuration file
# on the host in the TFTP-server directory

cfg_name=${SERIAL}.atv

# 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

modprobe param_dev 2>/dev/null || :
gaiconfig --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
umount /proc umount /sys || :
```

2.20 mGuard-Firmware Update-Repositories einrichten

Bei Fragen wenden Sie sich bitte an den Support Ihrer PHOENIX CONTACT Landesgesellschaft.

Sie können zum Aktualisieren Ihrer mGuard-Geräte einen eigenen Update-Server betreiben (Unix- oder Windows-Server). Die notwendigen Update-Dateien können Sie auf den gerätespezifischen Produktseiten im Phoenix Contact Web Shop herunterladen.

Download-Datei:

- **FL MGUARD CENTERPORT**
  Unix- und Windows-Server: *mguard-firmware-repositories_x86_v8.9.3.zip*
- **Andere FL/TC MGUARD-Geräte (mGuard 8.x)**
  Unix- und Windows-Server: *mguard-firmware-repositories_mpc_v8.9.3.zip*
- **Andere FL MGUARD-Geräte (mGuard 10.x)**
  Unix- und Windows-Server: *mguard-firmware-repositories_10.4.1.zip*

Um einen eigenen Update-Server zu betreiben, gehen Sie wie folgt vor:

1. Öffnen Sie die Webseite des Phoenix Contact Web Shops unter:
   phoenixcontact.com/products.
2. Suchen Sie nach dem Produktnamen des Geräts (z. B. FL MGUARD RS4000).
3. Öffnen Sie die gewünschte Produktseite.
4. Wählen Sie den Menüpunkt *Downloads* und die Kategorie *Firmware-Update*.
5. Laden Sie die gewünschte **Download-Datei** herunter:
   z. B. *mguard-firmware-repositories_mpc_v8.9.3.zip*
6. Kopieren Sie den Inhalt des ZIP-Ordners auf Ihren Update-Server.
7. Tragen Sie den Update-Server auf der mGuard-Weboberfläche ein unter **Verwaltung >> Update >> Update** (siehe Kapitel 2.6.4.3, „Automatische Updates“).
8. Sie können nun **Online-Updates** oder **Automatische Updates** von Ihrem Update-Server durchführen.

ACHTUNG: Online- oder Automatische Updates von der installierten Ausgangs-Firmwareversion **7.6.8** können zu einem Fehler führen, wenn der Update-Server mit neueren Versionen des Apache-Web-Servers (z. B. 2.4.18) betrieben wird.

Dieses Problem tritt nicht auf, wenn der werkseitig voreingestellte Update-Server von Phoenix Contact (https://update.innominate.com) verwendet wird.

Um das Problem zu vermeiden, können anstatt eines Apache-Web-Servers z. B. Update-Server wie *nginx* oder *fnord* verwendet werden.

3 X.509-Zertifikate mit OpenSSL erstellen

Dokument-ID: 108395_de_01
Dokument-Bezeichnung: AH DE X.509 CERT OPENSSL

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Kapitel wird die Erstellung von X.509-Zertifikaten mit dem Tool *OpenSSL* erläutert.

3.1 Einleitung

Die Registrierung von Zertifikaten erfordert eine Zertifizierungsstelle (Certification Authority; CA), die für einen bestimmten Zeitraum Public-Key-Zertifikate ausstellt. Eine CA kann eine private (interne) CA sein, die von Ihrer eigenen Organisation geführt wird, oder eine öffentliche CA. Eine öffentliche CA wird durch einen Drittanbieter geführt, dem Sie die Validierung der Identität der einzelnen Clients und Server, denen er ein Zertifikat ausstellt, anvertrauen.

Es stehen mehrere Tools zur Erstellung und Verwaltung von Zertifikaten zur Verfügung, wie z. B. *Microsoft Certification Authority (CA) Server*, *OpenSSL* und *XCA*.

Dieser Anwenderhinweis erläutert die Vorgehensweise zur Erstellung von X.509-Zertifikaten mit den Tools **OpenSSL** und **XCA**, um eine VPN-Verbindung mit den X.509-Zertifikaten als Authentifizierungsmethode einzurichten.

Dieses Dokument ist aufgrund des Umfangs nicht als vollständiges Benutzerhandbuch für die beschriebenen Tools geeignet. Dieses Dokument soll Ihnen helfen, mit den Tools vertraut zu werden und die benötigten Zertifikate in einem kurzen Zeitraum zu erstellen.

3.1.1 Einführung OpenSSL

OpenSSL ist für mehrere Plattformen erhältlich (Linux, UNIX, Windows) und kann im Internet heruntergeladen werden. Wir haben in diesem Fall *OpenSSL 1.1.0e* auf einer *Windows 7* Plattform verwendet. Weiterführende Informationen zu OpenSSL und die unterstützten Kommandozeilen-Optionen sind unter http://www.openssl.org zu finden.

OpenSSL bietet zahlreiche Möglichkeiten zur Festlegung der erforderlichen Optionen. Sie können sie in der Kommandozeile eingeben, sie in einer Konfigurationsdatei festlegen oder sie bei Aufforderung in einem bestimmten Fenster eingeben, wenn der Befehl *openssl* ausgeführt wird. Bei der Verwendung von Konfigurationsdateien können Sie entweder alle erforderlichen Parameter in einer Einzeldatei festlegen oder verschiedene Dateien verwenden, je nachdem, welche Art von Zertifikat Sie erstellen möchten. Die OpenSSL-Konfigurationsdatei, die bereits in OpenSSL vorhanden ist, hat die Bezeichnung *openssl.cnf*.

Bitte beachten: In Windows wird die Dateiendung *.cnf* ausgeblendet, selbst wenn Sie die Einstellung im *Windows Explorer* geändert haben sollten. Aus diesem Grund verwenden wir die Endung *.conf*.

In den folgenden Kapiteln werden wir erläutern, auf welche Weise OpenSSL eingerichtet werden muss, um die Funktion einer Zertifizierungsstelle (CA) zu erfüllen. Eine Zertifikatanfrage muss durch die CA signiert werden, um zu einem gültigen Zertifikat zu werden.

Sie können zum Erstellen der Zertifikate prinzipiell die Beispiele in den folgende Kapiteln anwenden. Sie müssen dazu lediglich die Anweisungen befolgen und die Parameter im Abschnitt *req_dn* der OpenSSL-Konfigurationsdatei *openssl.conf* (siehe Kapitel „OpenSSL-Konfigurationsdatei modifizieren“ auf Seite 88) an die Anforderungen Ihres Unternehmens entsprechend anpassen.

Es folgt eine kleine Legende mit **Dateiendungen**, die für die erstellten Dateien verwendet werden, sowie deren Bedeutung.

Dateiendung	Erläuterung
key	Privater Schlüssel Bei diesen Dateien müssen restriktive Berechtigungen gesetzt werden.
csr	Zertifikatanfrage (certificate request) Die Anfrage wird durch die CA signiert, um das Zertifikat zu erstellen. Im Anschluss wird diese Datei nicht mehr benötigt und kann gelöscht werden.
crt	Zertifikat Dieses Zertifikat kann öffentlich verbreitet werden.
p12	PKCS#12-Export des Zertifikats, der den zugehörigen privaten und öffentlichen Schlüssel enthält. Die Exportdatei wird durch ein Passwort geschützt, um den privaten Schlüssel vor unbefugter Nutzung zu schützen. Dieses Zertifikat **darf nicht** öffentlich verbreitet werden.

3.2 CA-Umgebung vorbereiten

Als Erstes muss eine Verzeichnisstruktur erstellt werden, in der sämtliche Zertifikatsangelegenheiten verwaltet werden. In den folgenden Beispielen wird **C:\CA** als Root-Verzeichnis verwendet. Folgende Unterverzeichnisse müssen erstellt werden:

Unterverzeichnis	Zweck
.\certs	Verzeichnis, in dem die Zertifikate abgelegt werden.
.\newcerts	Verzeichnis, in dem OpenSSL die erstellten Zertifikate im PEM-Format als *<cert serial number>.pem* (z. B. *07.pem*) ablegt. Dieses Verzeichnis wird von OpenSSL benötigt.
.\private	Verzeichnis zur Speicherung der privaten Schlüssel. Stellen Sie sicher, dass Sie bei diesem Verzeichnis restriktive Berechtigungen festlegen, sodass für Anwender mit den entsprechenden Privilegien ein Schreibschutz (*Read-Only*) besteht.

Neben dem Verzeichnisbaum müssen die folgenden zwei Dateien (*index.txt* und *serial*) erstellt werden:

- **index.txt**: Diese Datei wird von OpenSSL als Zertifikate-"Datenbank" verwendet. Um die diese Datei zu erstellen, gehen Sie wie folgt vor:
  - Öffnen Sie eine DOS-Eingabeaufforderung.
  - Wechseln Sie in das CA-Root-Verzeichnis (in unserem Beispiel: *C:\CA*).
  - Führen Sie folgenden Befehl aus: *copy NUL: index.txt*
    Dieser Befehl erstellt die leere Datei *index.txt*.
- **serial**: Diese Datei enthält den Zähler (*Counter*) für Zertifikatseriennummern. Dieser Zähler zählt durch OpenSSL automatisch hoch, wenn der entsprechende Wert zum Erstellen eines Zertifikats verwendet wurde. Um diese Datei zu erstellen, gehen Sie wie folgt vor:
  - Öffnen Sie eine DOS-Eingabeaufforderung.
  - Wechseln Sie in das CA-Root-Verzeichnis (in unserem Beispiel: *C:\CA*).
  - Führen Sie folgenden Befehl aus: *echo 0001 > serial*
    Dieser Befehl erstellt die Datei *serial* mit der anfänglichen Seriennummer 0001.

3.3 OpenSSL-Konfigurationsdatei modifizieren

Wir haben die OpenSSL-Konfigurationsdatei mit *openssl.conf* benannt und sie im CA-Root-Verzeichnis (in unserem Beispiel: *C:\CA*) abgelegt. Die OpenSSL-Konfigurationsdatei besteht aus mehreren Abschnitten. Jeder Abschnitt wird für einen anderen Zweck verwendet. Die Abschnitte umfassen die folgenden Positionen:

- **ca, CA_default**: Legt die Konfiguration der Zertifizierungsstelle fest.
- **policy_any**: Definiert die Richtlinien für Anfragen.
- **req, req_dn**: Definiert die Anfrage-Standardwerte.

In unserem Beispiel weist die Konfigurationdatei (*openssl.conf*) die folgenden Einträge auf:

```
[ 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                     = Länderkennung (2-stelliger Code)
countryName_default             = DE

organizationName                = Name der Organisation (Unternehmen)
organizationName_default        = PHOENIX CONTACT Cyber Security AG

organizationalUnitName          = Name der Organisationseinheit (Abteilung, Division)
organizationalUnitName_default  = Support

commonName                      = Common-Name (Hostname, IP oder Ihr Name)

# In unserem Beispiel nicht verwendet
#emailAddress                   = E-Mail-Adresse
#localityName                   = Name der Örtlichkeit (Stadt, Verwaltungsbezirk)
#stateOrProvinceName            = Name des Bundeslandes/Bundesstaats (vollständiger Name)

[ policy_any ]
countryName                     = supplied
organizationName                = supplied
organizationalUnitName          = optional
commonName                      = supplied
# In unserem Beispiel nicht verwendet
#emailAddress                   = optional
#localityName                   = optional
#stateOrProvinceName            = optional

[ req_ext ]
basicConstraints                = critical, CA:false

[ ca_ext ]
basicConstraints                = critical, CA:true, pathlen:0
keyUsage                        = critical, cRLSign, keyCertSign
```

Abschnitt	Option	Beschreibung
[req]	Dieser Abschnitt wird bei Anfrage nach einem Zertifikat abgerufen, indem der Befehl *openssl* mit der Option **req** aufgerufen wird.	
	prompt	Wenn dieser Wert auf **no** gesetzt wird, werden die Eingabeaufforderung für die Zertifikatsfelder deaktiviert und nur Werte aus der Konfigurationsdatei direkt übernommen. Sie müssen diese Option aktivieren, um in der Lage sein zu können, den *common name* einzugeben oder die Standardwerte des eindeutigen Namens des Zertifikats für jedes angefragte Zertifikat ändern zu können.
	default_bits	Dieser Eintrag legt die standardmäßige Schlüsselgröße in Bits fest. Bei einer fehlenden Angabe werden 512 Bits verwendet.
	distinguished_name	Dies bezeichnet den Abschnitt, der die eindeutigen Namensfelder enthält, die bei der Generierung eines Zertifikats oder einer Zertifikatanfrage per Eingabeaufforderung angezeigt werden. In unserem Beispiel wurde dieser Abschnitt **[req_dn]** benannt.
	x509_extensions	Dies bezeichnet den Abschnitt der Konfigurationsdatei, in dem eine Liste der Endungen zum Hinzufügen zum Zertifikat enthalten ist, welches durch Anwendung des **-x509**-Parameters erzeugt wird. Er kann durch den Kommandozeilen-Parameter **-extensions** übersteuert werden.
	string_mask	Diese Option blendet die Verwendung bestimmter Zeichenfolge-Typen in bestimmten Feldern aus. Wenn die Option **utf8only** eingesetzt wird, werden ausschließlich UTF8-Strings verwendet: dies ist die PKIX-Empfehlung in RFC2459 nach 2003.
[ca]	Dieser Abschnitt wird abgerufen, wenn Zertifikatanfragen durch Aufrufen des Befehls *openssl* mit der Option **ca** signiert werden.	
	default_ca	Wenn die Kommandozeilen-Option **-name** angewendet wird, wird damit der zu verwendende Abschnitt benannt. Andernfalls muss der zu verwendende Abschnitt in der Option **default_ca** des Abschnitts **ca** der Konfigurationdatei in unserem Beispiel **[CA_default]** benannt werden.

[CA_default]	Dieser Abschnitt wird abgerufen, wenn Zertifikatanfragen durch Aufrufen des Befehls *openssl* mit der Option **ca**, auf die die Option **default_ca** des Abschnitts **ca** Bezug nimmt, signiert werden.	
	dir	Root-Verzeichnis der CA-Umgebung. Wenn die Konfigurationsdatei in diesem Verzeichnis abgelegt wird und falls Sie sämtliche Befehle *openssl* aus diesem Verzeichnis ausführen, können Sie ganz einfach "dir = " angeben..
	certs	Zertifikate-Ausgabeverzeichnis.
	database	Die zu verwendende Text-Datenbankdatei (Pflichtparameter). Diese Datei muss vorhanden sein, selbst wenn sie zu Anfang leer ist.
	new_certs_dir	Hier wird das Verzeichnis festgelegt, in dem neue Zertifikate abgelegt werden. Pflichtangabe.
	certificate	Speicherort und Dateiname des CA-Zertifikats.
	serial	Eine Textdatei, in der die nächste Seriennummer zur Verwendung im Hex-Format enthalten ist. Pflichtangabe. Diese Datei muss vorhanden sein und eine gültige Seriennummer enthalten.
	private_key	Speicherort und Dateiname der Datei, in der der private Schlüssel der CA enthalten ist.
	default_md	Diese Option legt den zu verwendenden Digest-Algorithmus fest. Jeder Digest, der durch den OpenSSL-Befehl *dgst* unterstützt wird, kann verwendet werden.
	default_days	Die Standardanzahl an Tagen, die das Zertifikat gültig ist. Dieser Standardwert kann durch den Kommandozeilen-Parameter **-days** übersteuert werden.
	x509_extensions	Dies bezeichnet den Abschnitt der Konfigurationsdatei, in dem eine Liste der Endungen zum Hinzufügen zum Zertifikat enthalten ist, welches durch Anwendung des **-x509**-Parameters erzeugt wird. Er kann durch den Kommandozeilen-Parameter **-extensions** übersteuert werden.

[req_dn]	Dies bezeichnet die Parameter, die die eindeutigen Namensfelder enthalten, die bei der Generierung eines Zertifikats oder einer Zertifikatanfrage per Eingabeaufforderung angezeigt werden und auf die die Option **distinguished_name** des Abschnitts **req** Bezug nimmt. Wenn die Option **prompt** im Abschnitt **req** fehlt oder auf **yes** gesetzt ist, dann enthält der Abschnitt Informationen, die über Eingabeaufforderung den Feldern zugewiesen werden. <fieldname> bezeichnet den verwendeten Feldnamen, zum Beispiel *commonName* (oder CN).	
	<fieldname> = "prompt"	Die Zeichenfolge "prompt" dient dazu, den Anwender zur Eingabe der relevanten Details aufzufordern.
	<fieldname>_default ="default field value"	Wenn der Anwender nichts eingibt, wird der Standardwert verwendet; falls es keinen Standardwert gibt, wird das Feld ausgelassen.
[policy_any]	Diese Option legt die zu verwendende CA-"Richtlinie" fest und muss durch den Kommandozeilen-Parameter **–policy** spezifiziert werden. Dies ist ein Abschnitt in der Konfigurationsdatei, in dem entschieden wird, welche Felder Pflichtfelder sind oder mit dem CA-Zertifikat übereinstimmen müssen. Der Richtlinien-Abschnitt besteht aus einem Variablensatz, der den DN-Feldern des Zertifikats entspricht. Wenn der Wert "**match**" ist, muss der Feldwert mit dem gleichen Feld im CA-Zertifikat übereinstimmen. Wenn der Wert "**supplied**" ist, muss er im Feld vorhanden sein. Wenn der Wert "**optional**" ist, kann er im Feld vorhanden sein. Alle Felder, die im Richtlinien-Abschnitt nicht erwähnt werden, werden im Hintergrund und automatisch gelöscht.	
[…_ext]	Diese Abschnitte legen die X.509-Endungen fest und werden durch die Option **x509_extensions** innerhalb der Konfigurationsdatei (Abschnitt **[req]** und **[CA_default]**) referenziert. Sie können durch den Kommandozeilen-Parameter **-extensions** übersteuert werden.	
	basicConstraints	Dieser Flag dient zur Bestimmung, ob das Zertifikat als ein CA-Zertifikat verwendet werden kann.

3.4 CA-Zertifikat und Schlüssel erstellen

Nachdem nun alle anfänglichen Konfigurationen abgeschlossen wurden, kann ein selbstsigniertes Zertifikat erstellt werden, das als unser CA-Zertifikat verwendet werden wird. Mit anderen Worten: Wir werden dieses Zertifikat zum Signieren anderer Zertifikatanfragen verwenden.

Wechseln Sie in das CA-Root-Verzeichnis. Von diesem Verzeichnis aus können wir sämtliche **openssl-Befehle** erteilen, da unsere OpenSSL-Konfigurationsdatei (*openssl.conf*) hier abgelegt ist.

Syntax zum Erstellen von CA-Zertifikat und privatem Schlüssel:

```
openssl req -new  -config <filename> -x509 -extensions <section> -keyout
<filename> -out <filename> -days <nn>
```

Option	Beschreibung
req	Der *req*-Befehl dient in erster Linie zum Erstellen und Verarbeiten von Zertifikatanfragen. Er kann dafür selbstsignierte Zertifikate erstellen, wenn die Option **-x509** festgelegt wurde.
-new	Diese Option erzeugt eine neue Zertifikatanfrage.
-config <filename>	Dies ermöglicht die Festlegung einer alternativen Konfigurationsdatei.
-x509	Diese Option gibt ein selbstsigniertes Zertifikat statt einer Zertifikatanfrage aus.
-extensions <section>	Legt den Abschnitt in der openssl-Konfigurationsdatei (vorgegeben durch **-config <filename>**) fest, in dem die X.509-Zertifikatendungen definiert werden.
-keyout <filename>	Dateiname des privaten Schlüssels des CA. Obwohl dieser durch eine Passphrase geschützt ist, sollten Sie den Zugriff darauf beschränken, sodass nur autorisierte Anwender einen Lesezugriff haben.

Beispiel:

```
C:\CA>openssl req -new -config openssl.conf -x509 -extensions ca_ext -keyout
private/ca.key -out certs/ca.crt -days 3640
Erzeugt einen RSA-Private-Key mit 4096 Bit
.....++
.....++,
mit dem ein neuer privater Schlüssel unter 'private/ca.key' geschrieben wird
Enter PEM pass phrase: - geben Sie eine sichere Passphrase zur Verwendung mit diesem
Schlüssel ein
Verifying - Enter PEM pass phrase: - geben Sie die Passphrase zur Bestätigung erneut ein
-----
Sie werden aufgefordert werden, die Informationen einzugeben, die in
Ihre Zertifikatanfrage eingebunden werden.
Die Informationen, die Sie eingeben müssen, werden als "Distinguished Name"
(eindeutiger Name) oder DN bezeichnet.
Sie werden eine ganze Reihe an Feldern sehen, von denen Sie jedoch einige frei lassen
können.
Bei bestimmten Feldern gibt es einen Standardwert.
Wenn Sie '.' eingeben, bleibt das Feld leer.
-----
Country Name (2-stelliger Code) [DE]: - wir haben den Standardwert beibehalten
Organization Name (Unternehmen) [PHOENIX CONTACT Cyber Security AG]: - wir
haben den Standardwert beibehalten
Organizational Unit Name (Abteilung, Division) [Support]: - wir haben den Standardwert
beibehalten
Common Name (Hostname, IP oder Ihr Name) []:CA – wir haben den Common-Name für
das CA-Zertifikat eingegeben


C:\CA>
```

Es werden zwei Dateien erstellt:

– **certs/ca.crt**: Dies ist das Zertifikat der CA; es kann öffentlich zur Verfügung gestellt werden und ist selbstverständlich für alle lesbar.

– **private/ca.key**: Dies ist der private Schlüssel der CA. Obwohl dieser durch eine Passphrase geschützt ist, sollten Sie den Zugriff darauf beschränken, sodass nur autorisierte Anwender einen Zugriff erlangen können.

3.5 Zertifikatanfrage für den mGuard erstellen

Um ein gültiges mGuard-Zertifikat zu erhalten, müssen Sie zuerst eine Zertifikatanfrage erstellen und diese anschließend mit dem CA-Zertifikat signieren (erläutert in Kapitel „Zertifikatanfrage des mGuards mit dem CA signieren“ auf Seite 97).

Syntax zum Erstellen einer Zertifikatanfrage für den mGuard:

```
openssl req –new -config <filename> -keyout <filename> -out <filename> -days <nn>
```

Option	Beschreibung
req	Der *req*-Befehl dient in erster Linie zum Erstellen und Verarbeiten von Zertifikatanfragen.
-new	Diese Option erzeugt eine neue Zertifikatanfrage.
-config <filename>	Dies ermöglicht die Festlegung einer alternativen Konfigurationsdatei.
-keyout <filename>	Dateiname des privaten Schlüssels des mGuards. Obwohl dieser durch eine Passphrase geschützt ist, sollten Sie den Zugriff darauf beschränken, sodass nur autorisierte Anwender einen Lesezugriff haben.
-out <filename>	Dateiname des mGuard-Zertifikats.
-days <nn>	Die Anzahl der Tage, die das Zertifkat gültig bleiben soll.

Beispiel:

```
C:\CA>openssl req -new -config openssl.conf -keyout private/mGuard.key -out
mGuard.csr -days 364
Erzeugt einen RSA-Private-Key mit 4096 Bit
.....++
.....
+,
mit dem ein neuer privater Schlüssel unter 'private/mGuard.key' geschrieben wird.
Enter PEM pass phrase: - geben Sie eine sichere Passphrase zur Verwendung mit diesem
Schlüssel ein
Verifying - Enter PEM pass phrase: - geben Sie die Passphrase zur Bestätigung erneut ein
-----
Sie werden aufgefordert werden, die Informationen einzugeben, die in
Ihre Zertifikatanfrage eingebunden werden.
Die Informationen, die Sie eingeben müssen, werden als "Distinguished Name"
(eindeutiger Name) oder DN bezeichnet.
Sie werden eine ganze Reihe an Feldern sehen, von denen Sie jedoch einige frei lassen
können.
Bei bestimmten Feldern gibt es einen Standardwert.
Wenn Sie '.' eingeben, bleibt das Feld leer.
-----
Country Name (2-stelliger Code) [DE]: - wir haben den Standardwert beibehalten
Organization Name (Unternehmen) [PHOENIX CONTACT Cyber Security AG]: - wir
haben den Standardwert beibehalten
Organizational Unit Name (Abteilung, Division) [Support]: - wir haben den Standardwert
beibehalten
Common Name (Hostname, IP oder Ihr Name) []:mGuard – geben Sie den Common-
Name für das mGuard-Zertifikat ein


C:\CA>
```

Es werden zwei Dateien erstellt:

- **mGuard.csr**: Dies ist die Zertifikatanfrage, die durch das CA-Zertifikat signiert werden muss.
- **private/mGuard.key**: Dies ist der private Schlüssel, der nicht mit einer Passphrase geschützt wird.

3.6 Zertifikatanfrage des mGuards mit dem CA signieren

Die Zertifikatanfrage des mGuards muss durch die CA signiert werden, um ein gültiges Zertifikat zu werden.

Syntax zur Signierung der Zertifikatanfrage des mGuards mit dem CA:

```
openssl ca –config <filename> -out <filename> -infiles <filename>
```

Option	Beschreibung
ca	Der Befehl *ca* ist eine minimale CA-Anwendung. Mit ihm können Zertifikatanfragen auf vielfältige Weise signiert und CRLs (Zertifikatssperrlisten) erzeugt werden; er unterhält des Weiteren eine Textdatenbank mit ausgestellten Zertifikaten und deren Status.
-config <filename>	Dies ermöglicht die Festlegung einer alternativen Konfigurationsdatei.
-out <filename>	Dateiname des signierten mGuard-Zertifikats.
-infiles <filename>	Dateiname der Zertifikatanfrage des mGuard. Dies muss die letzte Option sein.

Beispiel:

```
C:\CA>openssl ca -config openssl.conf -out certs/mGuard.crt -infiles mGuard.csr
Verwendet die Konfiguration von openssl.conf
Enter pass phrase for C:/CA/private/ca.key: - geben Sie die Passphrase des privaten Schlüssels von CA ein
Stellen Sie sicher, dass die Anfrage mit der Signatur übereinstimmt
Signatur ist OK
Der "Distinguished Name" des Subjekts lautet wie folgt:
countryName           :PRINTABLE:'DE'
organizationName      :ASN.1 12:'PHOENIX CONTACT Cyber Security AG'
organizationalUnitName:ASN.1 12:'Support'
commonName            :ASN.1 12:'mGuard'
Das Zertfikat muss bis zum 7. Juli 2018, 09:02:23 GMT (365 Tage) ausgestellt werden
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>
```

Nachdem alle diese Schritte abgeschlossen wurden, werden zwei neue Dateien erstellt:

- **certs/mGuard.crt**: Dies ist das Zertifikat des mGuards, das öffentlich zur Verfügung gestellt werden kann.
- **newcerts/01.pem**: Dies ist genau das gleiche Zertifikat, jedoch mit der Seriennummer des Zertifikats (Hex-Zahl) als Dateiname. Bei nachfolgenden Anfragen wird die Zahl um 1 erhöht. Diese Datei wird nicht mehr benötigt und kann gelöscht werden.

Nun können Sie die Zertifikatanfrage des mGuards löschen (*mGuard.csr*). Diese wird nicht mehr benötigt.

3.7 PKCS#12-Datei von mGuard erstellen (Maschinenzertifikat)

Diese Datei kombiniert den privaten und öffentlichen Schlüssel und ist das Maschinenzertifikat des mGuards, das über das Menü **Authentifizierung >> Zertifikate >> Maschinenezertifikate** importiert werden muss. Es erscheint eine Eingabeaufforderung, in der Sie ein Passwort eingeben müssen, durch das der PKCS#12-Export des Zertifikats vor unbefugter Nutzung geschützt wird.

Es folgt die Syntax zum Erstellen des mGuard-Maschinenzertifikats:

```
openssl pkcs12 -export -in <filename> -inkey <filename> -out <filename>
```

Option	Beschreibung
pkcs12	Der *pkcs12*-Befehl ermöglicht das Erstellen und Zerteilen (Parsen) von PKCS#12-Dateien.
-export	Mit dieser Option wird festgelegt, dass eine PKCS#12-Datei erstellt und nicht zerteilt (geparst) wird.
-in <filename>	Der Dateiname, aus dem das Zertifikat ausgelesen wird. Das Format der Datei muss PEM sein. Dies ist das Zertifikat des mGuards, das Sie im vorherigen Schritt erstellt haben.
-inkey <filename>	Datei, aus der der private Schlüssel ausgelesen wird. Dies ist die Datei, in der der private Schlüssel des Zertifikats des mGuards enthalten ist.
-out <filename>	Der Dateiname, in den Zertifikate und private Schlüssel geschrieben werden. Sie werden alle im PEM-Format geschrieben.

Beispiel:

```
C:\CA>openssl pkcs12 -export -in certs/mGuard.crt -inkey private/mGuard.key -out
certs/mGuard.p12

Enter pass phrase for private/mGuard.key: - geben Sie das Passwort des privaten
Schlüssels von mGuard ein

Enter Export Password: - geben Sie eine sichere Passphrase zur Verwendung für diesen
Export ein

Verifying - Enter Export Password: - geben Sie zur Bestätigung erneut die Passphrase ein


C:\CA>
```

Dieser Befehl erstellt eine Datei mit der Bezeichnung **certs/mGuard.p12**, in der der öffentliche und private Schlüssel des mGuard-Zertifikats enthalten ist. Die Datei ist durch das eingegebene Passwort geschützt.

3.8 Beispiel: VPN-Verbindung zwischen zwei mGuard-Geräten

Wir gehen davon aus, dass Sie die CA-Umgebung bereits eingerichtet, die Konfigurationsdatei von OpenSSL (*openssl.conf*) konfiguriert sowie CA-Zertifikat und Schlüssel erstellt haben. (So wie in den vorherigen Kapiteln beschrieben.)

Schritt 1: Erstellen Sie eine Zertifikatanfrage für jeden 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
```

Schritt 2: Signieren Sie jede Zertifikatanfrage mit dem CA

mGuard 1

```
openssl ca -config openssl.conf -out certs/mGuard1.crt -infiles mGuard1.csr
```

mGuard 2

```
openssl ca -config openssl.conf -out certs/mGuard2.crt -infiles mGuard2.csr
```

Die zwei Zertifikate **certs/mGuard1.crt** und **certs/mGuard2.crt** werden erstellt. **mGuard1.crt** muss bei mGuard **2** als Verbindungszertifikat über das Menü **IPsec VPN >> Verbindungen >> Authentifizierung** importiert werden. **mGuard2.crt** dementsprechend bei **mGuard 1**.

Schritt 3: Erhalten Sie das Maschinenzertifikat für jeden 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
```

Die zwei Exporte **certs/mGuard1.p12** und **certs/mGuard2.p12** werden erstellt.

mGuard1.p12 muss bei mGuard **1** als Maschinenzertifikat über das Menü **Authentifizierung >> Zertifikate >> Maschinenzertifikate** importiert werden. **mGuard2.p12** dementsprechend bei mGuard **2**.

4 X.509-Zertifikate mit XCA erstellen

Dokument-ID: 108396_de_01
Dokument-Bezeichnung: AH DE X.509 CERT XCA

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument wird die Erstellung von X.509-Zertifikaten mit dem Tool *XCA* beschrieben.

XCA hat viel mehr Funktionalität zu bieten, als in diesem Dokument beschrieben wird. Weiterführende Informationen sind in der *XCA*-Dokumentation zu finden (http://xca.sourceforge.net/xca.html – 15.09.2017). Sie können das Tool *XCA* hier herunterladen: http://xca.sourceforge.net. Die Screenshots und Beschreibungen in diesem Kapitel beziehen sich auf *XCA* v1.3.2.

4.1 Einleitung

Die Registrierung von Zertifikaten erfordert eine Zertifizierungsstelle (Certification Authority; CA), die für einen bestimmten Zeitraum Public-Key-Zertifikate ausstellt. Eine CA kann eine private (interne) CA sein, die von Ihrer eigenen Organisation geführt wird, oder eine öffentliche CA. Eine öffentliche CA wird durch einen Drittanbieter geführt, dem Sie die Validierung der Identität der einzelnen Clients und Server, denen er ein Zertifikat ausstellt, anvertrauen.

Es stehen mehrere Tools zur Erstellung und Verwaltung von Zertifikaten zur Verfügung, wie z. B. *Microsoft Certification Authority (CA) Server*, *OpenSSL* und *XCA*.

Dieser Anwenderhinweis erläutert die Vorgehensweise zur Erstellung von X.509-Zertifikaten mit den Tools **OpenSSL** und **XCA**, um eine VPN-Verbindung mit den X.509-Zertifikaten als Authentifizierungsmethode einzurichten.

Dieses Dokument ist aufgrund des Umfangs nicht als vollständiges Benutzerhandbuch für die beschriebenen Tools geeignet. Dieses Dokument soll Ihnen helfen, mit den Tools vertraut zu werden und die benötigten Zertifikate in einem kurzen Zeitraum zu erstellen.

4.1.1 XCA - X Certificate and key management

XCA ist für die Erstellung und Verwaltung von X.509-Zertifikaten, Zertifikatsanforderungen (*Requests*), RSA-, DSA- und EC-Privatschlüsseln, Smartcards und CRLs vorgesehen. Alles, was für eine CA benötigt wird, ist implementiert. Alle CAs können Sub-CAs rekursiv signieren.

Für eine unternehmensweite Nutzung stehen Vorlagen (*Templates*) zur Verfügung, die für die Generierung von Zertifikaten oder Anfragen genutzt und angepasst werden können. Alle verschlüsselten Daten werden in einem portierbaren Dateiformat gespeichert.

4.2 XCA-Datenbank erstellen

Zum Erstellen von X.509-Zertifikaten und Schlüsseln unter Anwendung von *XCA* müssen Sie zuerst eine Datenbank erstellen. Gehen Sie wie folgt vor:

1. Klicken Sie auf **File >> New DataBase**.
2. Legen Sie Dateiname und Speicherort der Datenbank fest.
3. Klicken Sie auf **Save**.
4. Geben Sie ein Passwort ein, das die Datenbank vor unbefugter Nutzung schützt. Das Passwort wird jedes Mal abgefragt werden, wenn Sie die *XCA*-Datenbank öffnen.

4.2.1 XCA-Datenbank öffnen

Bei einem Neustart von *XCA* müssen Sie zuerst wieder eine Verbindung zur Datenbank herstellen. Um eine bereits erstellte Datenbank zu öffnen, gehen Sie wie folgt vor:

1. Klicken Sie auf **File >> Open DataBase**.
2. Wählen Sie die gewünschte Datenbank (Datei *.xdb) aus.
3. Klicken Sie auf **Open**.

4.2.2 Standard-Prüfsummen-Algorithmus festlegen

ACHTUNG: Phoenix Contact empfiehlt die Verwendung von sicheren und aktuellen Verschlüsselungen und Prüfsummen-Algorithmen gemäß den Angaben im mGuard Software-Referenzhandbuch, erhältlich unter phoenixcontact.net/products (Suchen Sie nach "UM EN MGUARD", wählen Sie ein Produkt und anschließend das Handbuch im Downloadbereich aus).

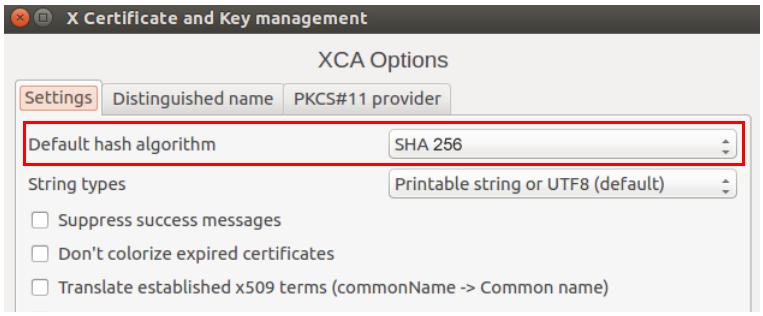
Bevor Sie mit dem Erstellen von Zertifikaten beginnen, müssen Sie den standardmäßigen Prüfsummen-Algorithmus auf **SHA 256** einstellen. Wenn Sie den Standard-Prüfsummen-Algorithmus nicht auf SHA 256 einstellen, müssen Sie diese Einstellung jedes Mal vornehmen, wenn Sie ein neues Zertifikat erstellen.

ACHTUNG: Nicht alle Geräte unterstützen die Funktionalität der SHA 2-Familie

Sollten Sie nicht sicher sein, ob alle Ihre Geräte die Funktionalität der SHA 2-Familie unterstützen, könnte stattdessen der nicht so sichere SHA 1-Algorithmus verwendet werden (wird von PHOENIX CONTACT nicht empfohlen und erfüllt nicht die Anforderungen der ANSSI-CSPN-2016-09).

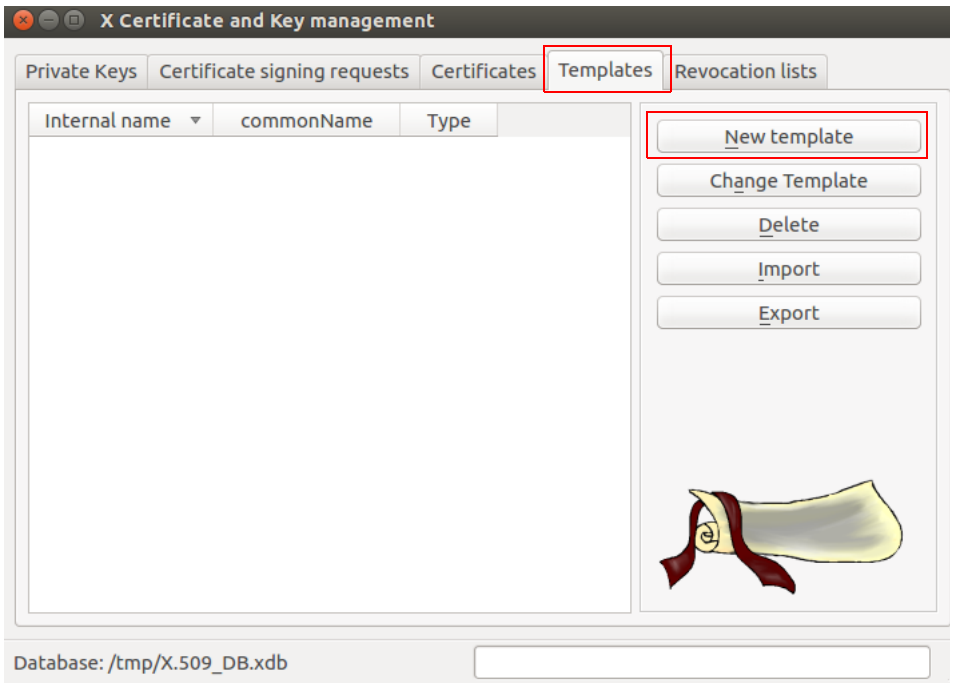
Gehen Sie wie folgt vor:

- Klicken Sie auf **File >> Options**, und setzen Sie den Standard-Prüfsummen-Algorithmus auf SHA 256 (oder den entsprechenden Algorithmus, den Sie bei Ihrer Einrichtung verwenden).



4.3 Zertifikatvorlage erstellen

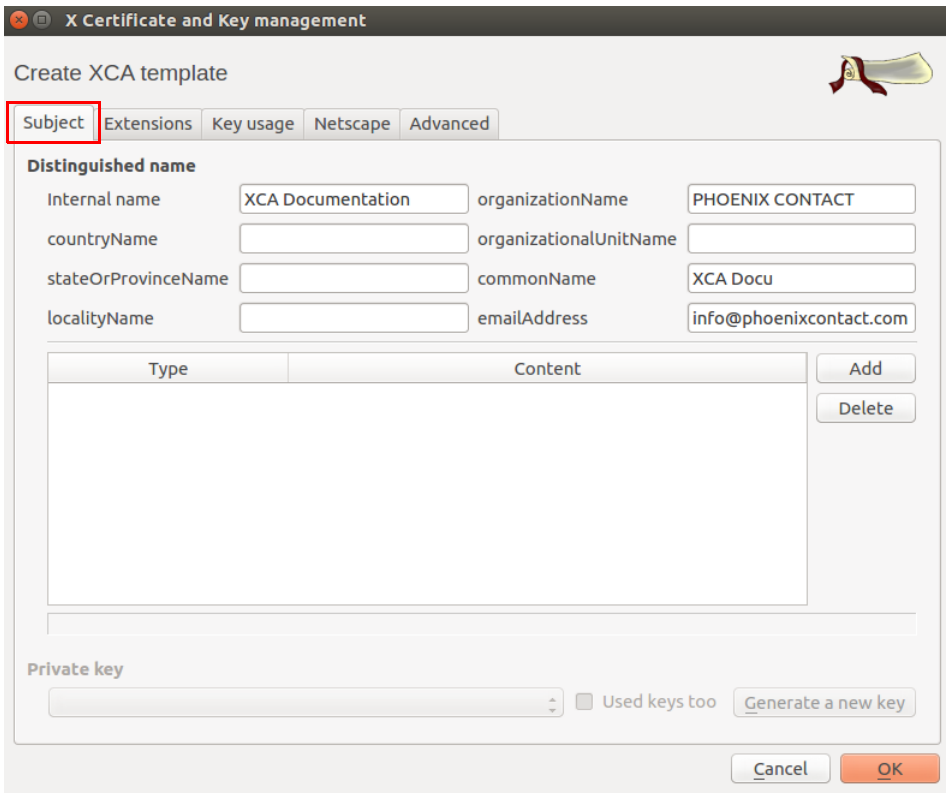
Falls Sie mehrere Zertifikate erstellen müssen, ist es hilfreich, aus Gründen der Konsistenz und für weniger Tastatureingaben eine Vorlage (Template) zu definieren. Diese Vorlage kann anschließend beim Erstellen der Zertifikate verwendet werden.



Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Templates**.
2. Klicken Sie auf **New template**.
3. Wählen Sie **Preset Template Values**, und klicken Sie auf **OK**.

4.3.1 XCA-Vorlage erstellen >> Registerkarte: Subject

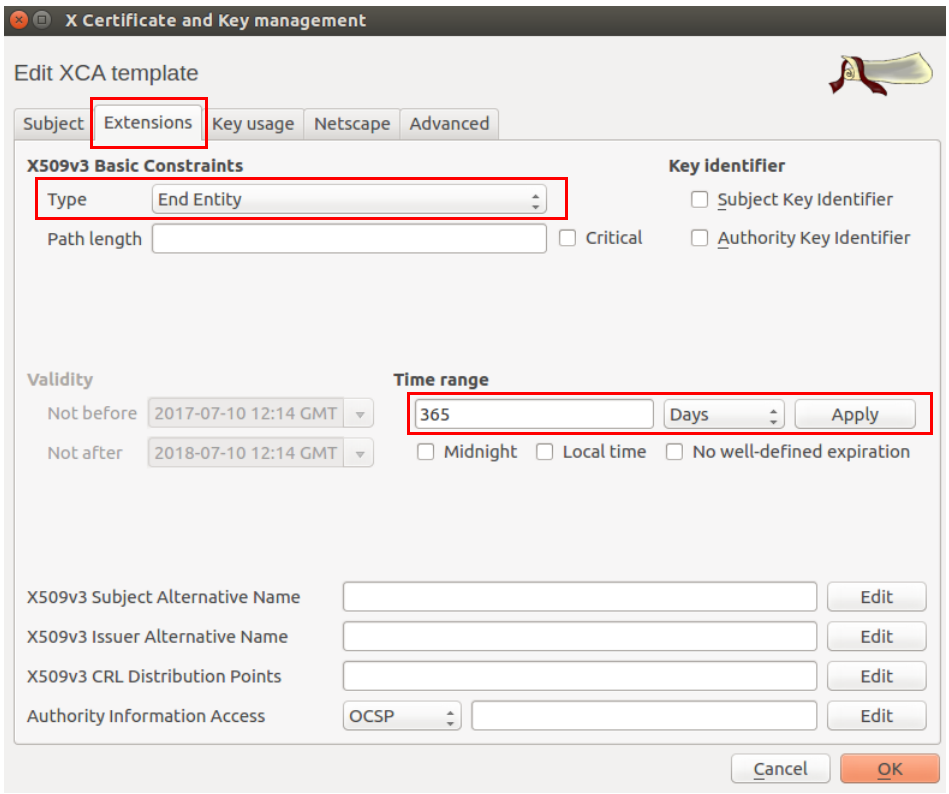


Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Subject.**
2. Verwenden Sie die Eingabefelder von **Internal name** bis **emailAddress,** um die identifizierenden Parameter einzugeben, die alle Zertifikate gemeinsam haben sollen.

   Die Vorlage wird in *XCA* unter **Internal name** gespeichert.
3. Wählen Sie die Registerkarte **Extensions**.

4.3.2 XCA-Vorlage erstellen >> Registerkarte: Extensions

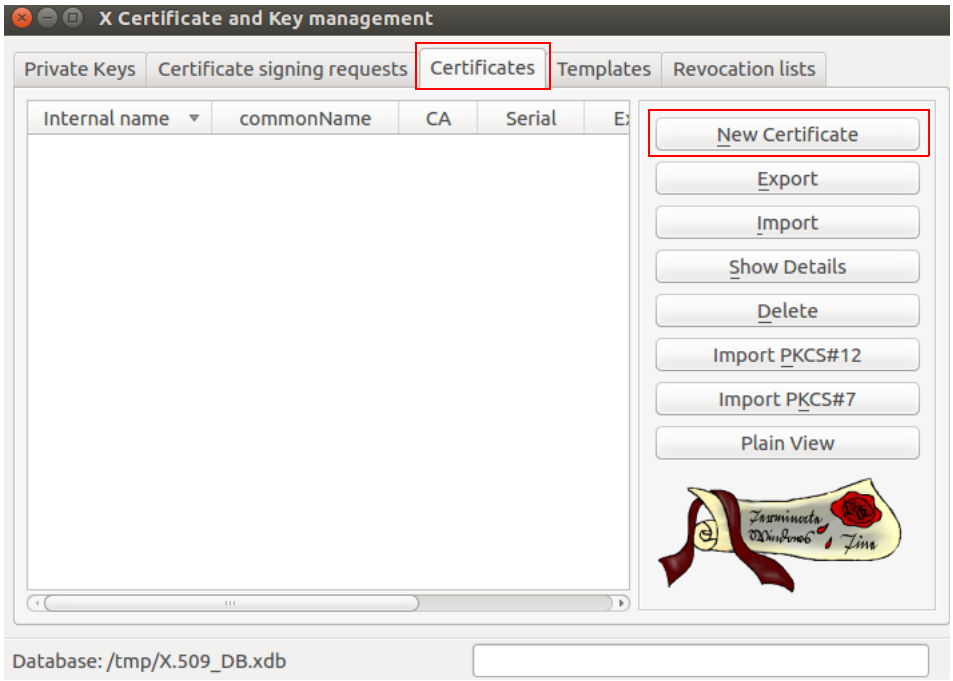


Gehen Sie wie folgt vor:

1. In Abschnitt **X509v3 Basic Constraints**:
   - Setzen Sie **Type** auf *End Entity*, wenn Sie die Vorlage zum Erstellen von Client-Zertifikaten verwenden möchten.
   - Setzen Sie **Type** auf *Certification Authority*, wenn die Vorlage zum Erstellen von CA-Zertifikaten verwendet werden soll.
2. Im Abschnitt **Time Range**:
   - Stellen Sie die Standard-Lebensdauer der Zertifikate ein, und klicken Sie auf **Apply**.
3. Klicken Sie zum Erstellen der Vorlage auf **OK**.

4.4 CA-Zertifikat erstellen

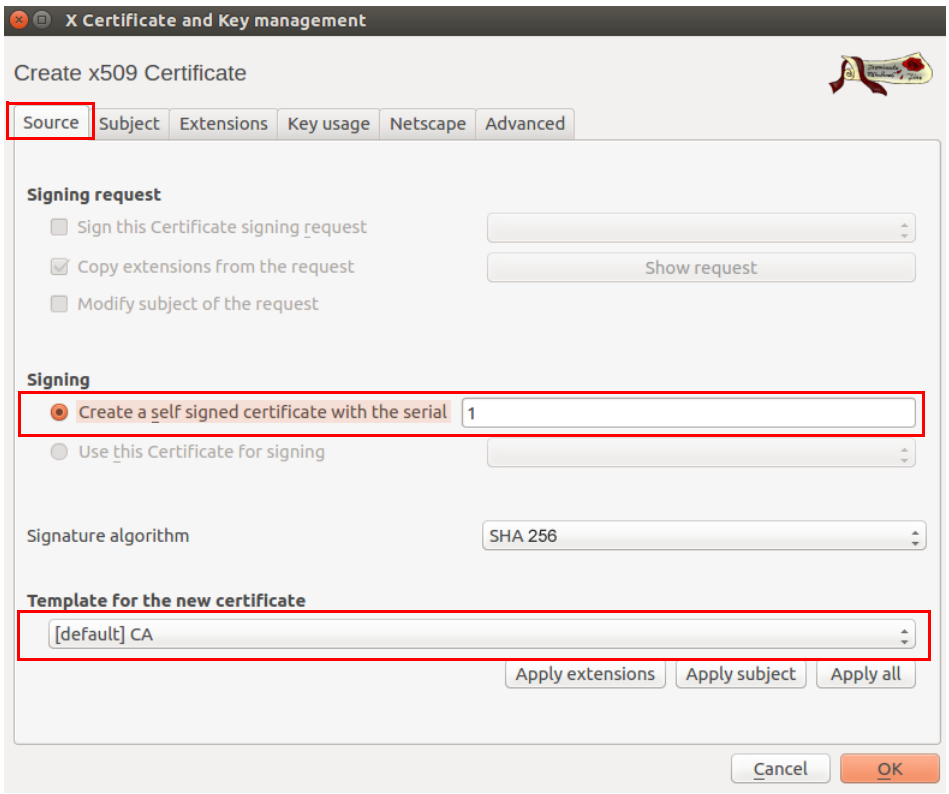
Falls Sie keine selbstsignierten Client-Zertifikate verwenden, muss ein Client-Zertifikat durch das CA-Zertifikat signiert werden, um zu einem gültigen Zertifikat zu werden. Aus diesem Grund müssen Sie zuerst das CA-Zertifikat erstellen, bevor Sie die Client-Zertifikate erstellen. Das CA-Zertifikat ist ein selbstsigniertes Zertifikat.



Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie auf **New Certificate**.

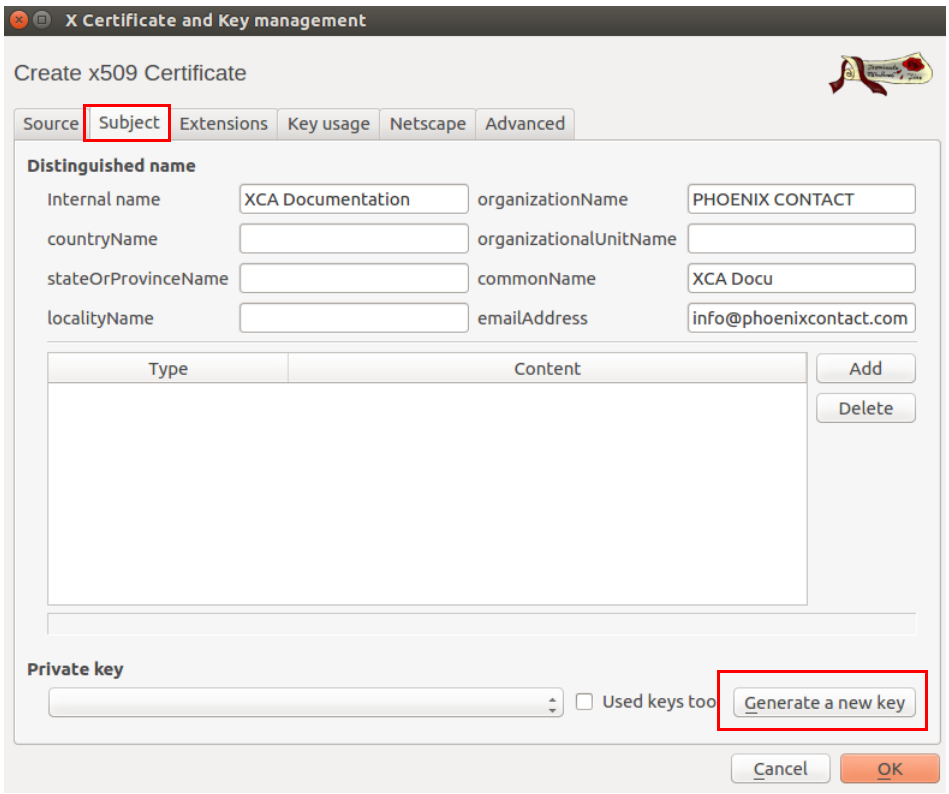
4.4.1 x509- (CA-) Zertifikat erstellen >> Registerkarte: Source



Gehen Sie wie folgt vor:

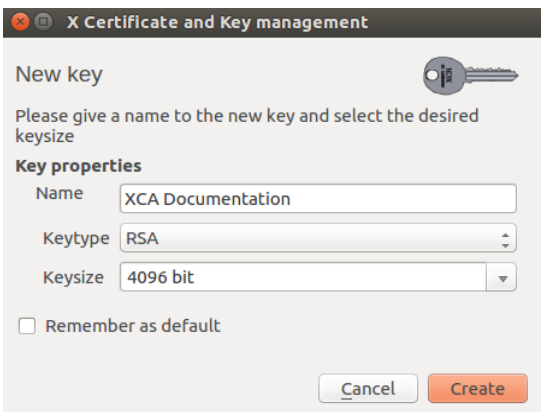
1. Wählen Sie die Registerkarte **Source**.
2. Im Abschnitt **Signing**: Stellen Sie sicher, dass **Create a self signed certificate with the serial** ausgewählt ist.
3. Sie können eine Seriennummer für das Zertifikat eingeben oder den Standardwert beibehalten.
4. Im Abschnitt **Template for the new certificate**: Wenn Sie eine Vorlage zum Erstellen von CA-Zertifikaten erstellt haben, können Sie diese nun auswählen und auf **Apply** klicken.
5. Wählen Sie die Registerkarte **Subject**.

4.4.2 x509- (CA-) Zertifikat erstellen >> Registerkarte: Subject



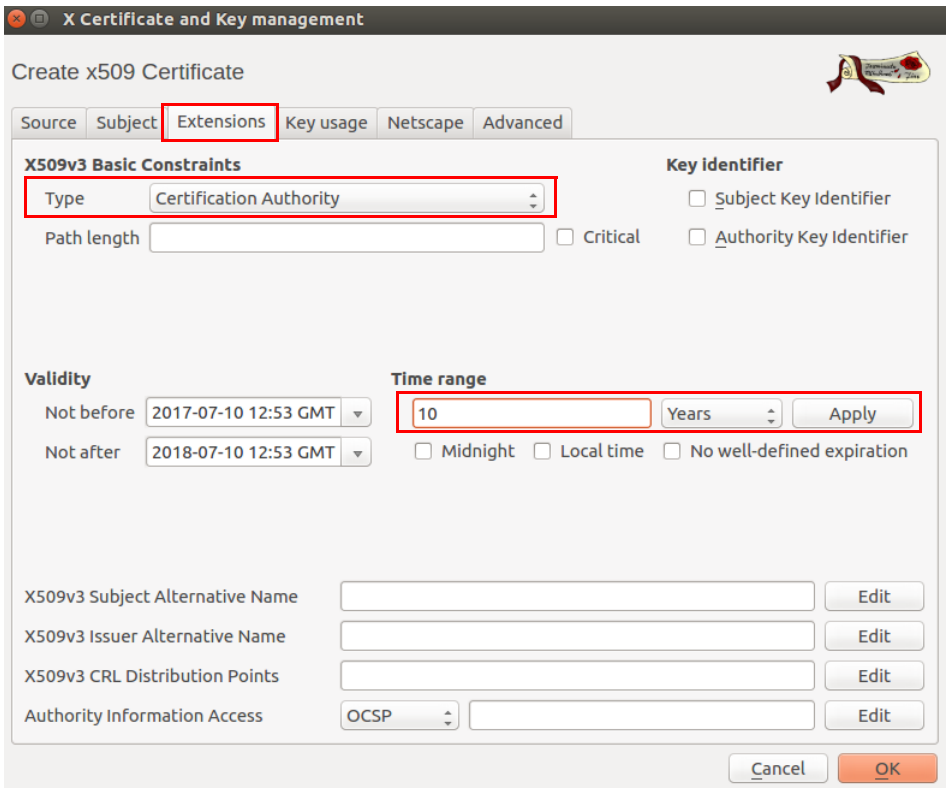
Gehen Sie wie folgt vor:

1. Im Abschnitt **Distinguished name**: Verwenden Sie die Eingabefelder von **Internal name** bis **emailAddress**, um die identifizierenden Parameter des CA-Zertifikats einzugeben.
2. Im Abschnitt **Private key**: Klicken Sie auf **Generate a new key**, um den privaten RSA-Schlüssel für das CA-Zertifikat zu erstellen.



3. Geben Sie einen **Namen** für den Schlüssel ein, legen Sie die gewünschten Werte für **Keytype** und **Keysize** fest, und klicken Sie auf **Create**.
4. Wählen Sie die Registerkarte **Extensions**.

4.4.3 x509- (CA-) Zertifikat erstellen >> Registerkarte: Extensions



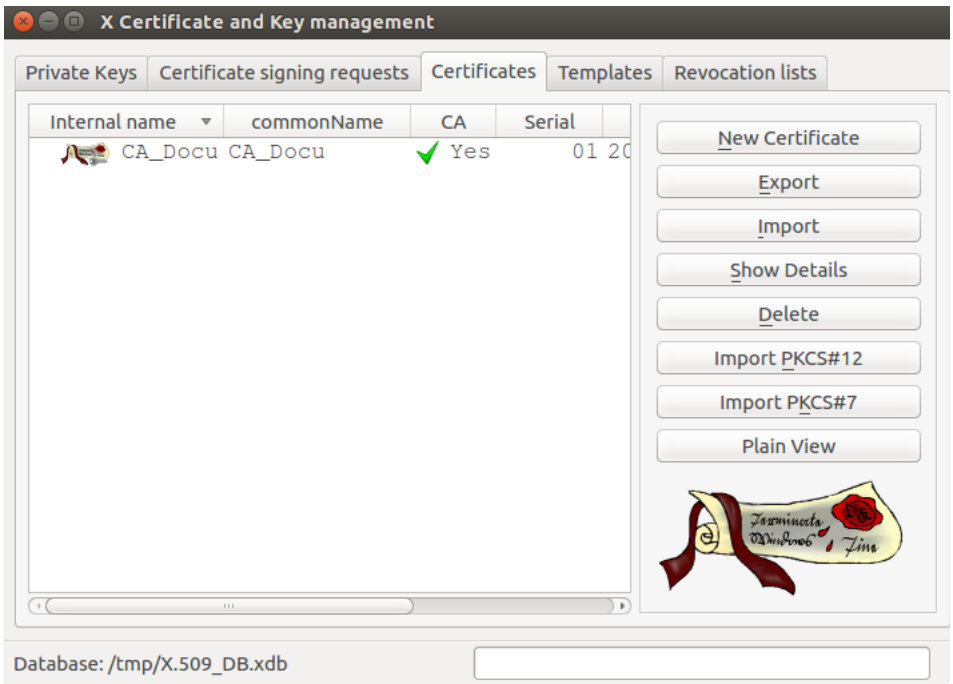
Gehen Sie wie folgt vor:

5. Im Abschnitt **X509v3 Basic Constraints**: Stellen Sie **Type** auf *Certification Authority* ein.
6. Im Abschnitt **Time Range**: Stellen Sie die Standard-Lebensdauer der Zertifikate ein, und klicken Sie auf **Apply**.
   Für ein CA-Zertifikat wünschen Sie sich unter Umständen eine längere Gültigkeit als für die Client-Zertifikate, sodass Sie die Zertifikate nicht so häufig erneut ausstellen müssen. Eine Lebensdauer von 10 Jahren ist im Allgemeinen ein guter Wert.
7. Klicken Sie auf **Apply**.
8. Klicken Sie zum Erstellen des Zertifikats auf **OK**.
   Das CA-Zertifikat wird auf der Registerkarte **Certificates** angezeigt.

4.5 Client-Zertifikat erstellen

Wenn Sie Client-Zertifikate erstellen möchten, müssen Sie zuerst ein CA-Zertifikat erstellen oder importieren, das anschließend zum Signieren des Client-Zertifikats verwendet wird. Das Client-Zertifikat erhält durch die Signatur des CA-Zertifikats seine Gültigkeit.

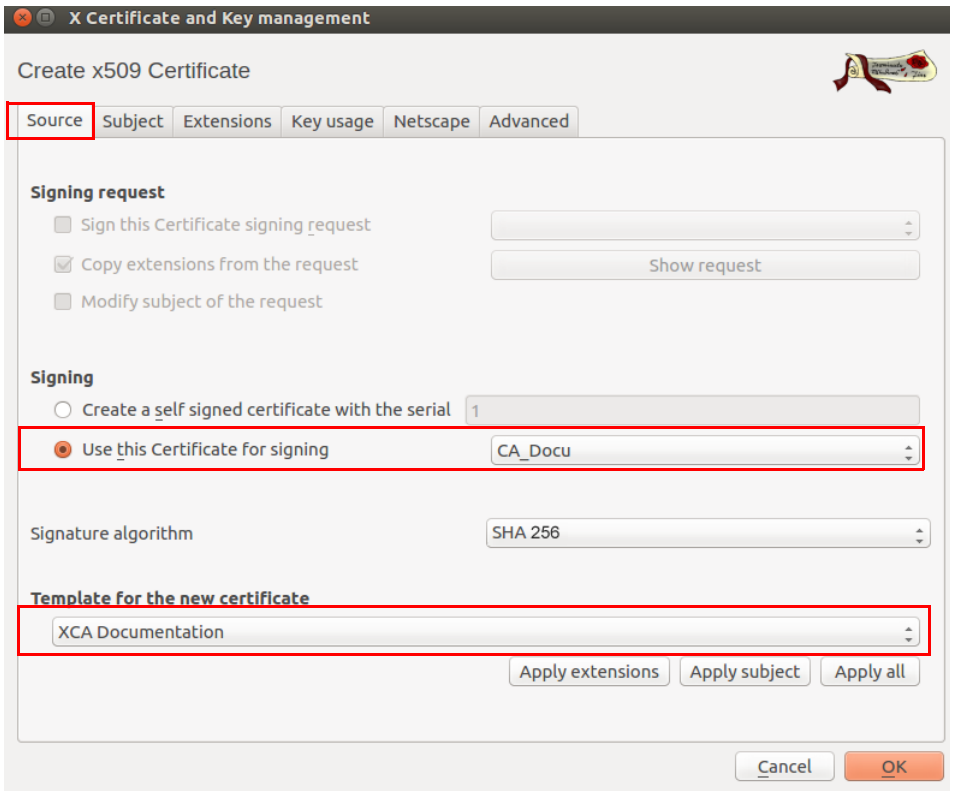
In der *XCA*-Datenbank muss ein CA-Zertifikat zum Signieren des Client-Zertifikats verfügbar sein. Sollte das CA-Zertifikat nicht verfügbar sein, muss es zuerst erstellt werden (siehe „CA-Zertifikat erstellen“ auf Seite 110).



Gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie auf **New Certificate**.

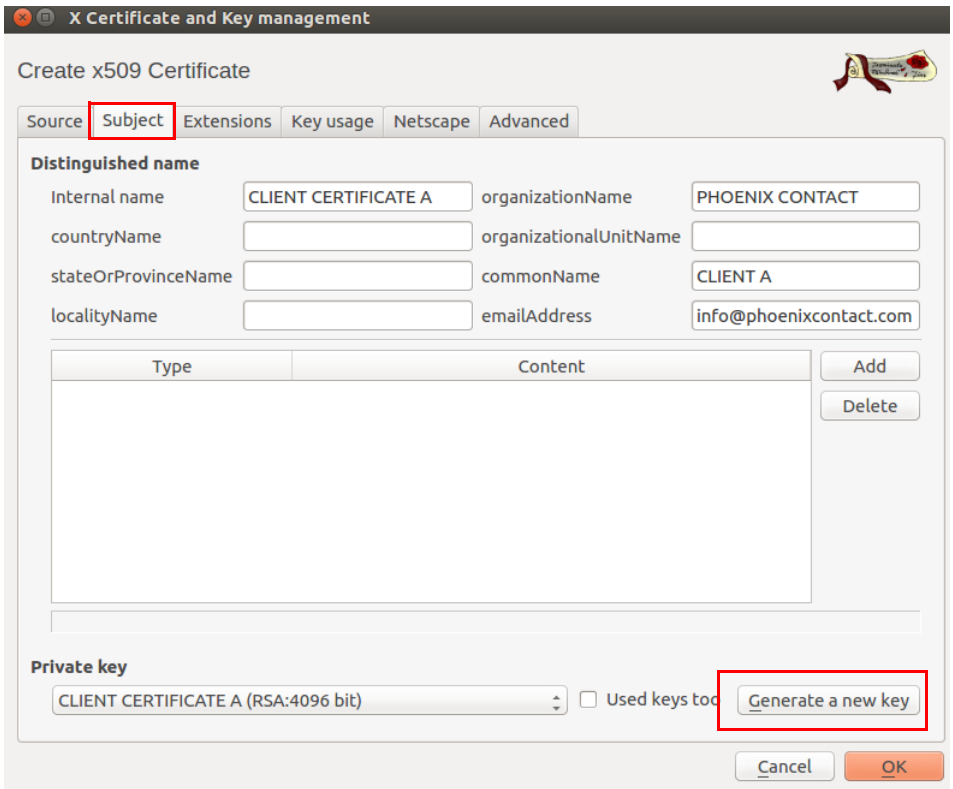
4.5.1 x509- (Client-) Zertifikat erstellen >> Registerkarte: Source



Gehen Sie wie folgt vor:

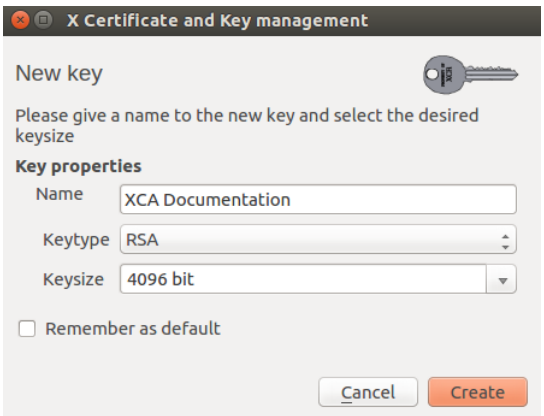
1. Wählen Sie die Registerkarte **Source**.
2. Im Abschnitt **Signing**: Stellen Sie sicher, dass das korrekte CA im Feld **Use this certificate for signing** ausgewählt ist.
3. Im Abschnitt **Template for the new certificate**: Wenn Sie eine Vorlage zum Erstellen von Client-Zertifikaten erstellt haben, können Sie diese nun auswählen und auf **Apply** klicken.
4. Wählen Sie die Registerkarte **Subject**.

4.5.2 x509- (Client-) Zertifikat erstellen >> Registerkarte: Subject



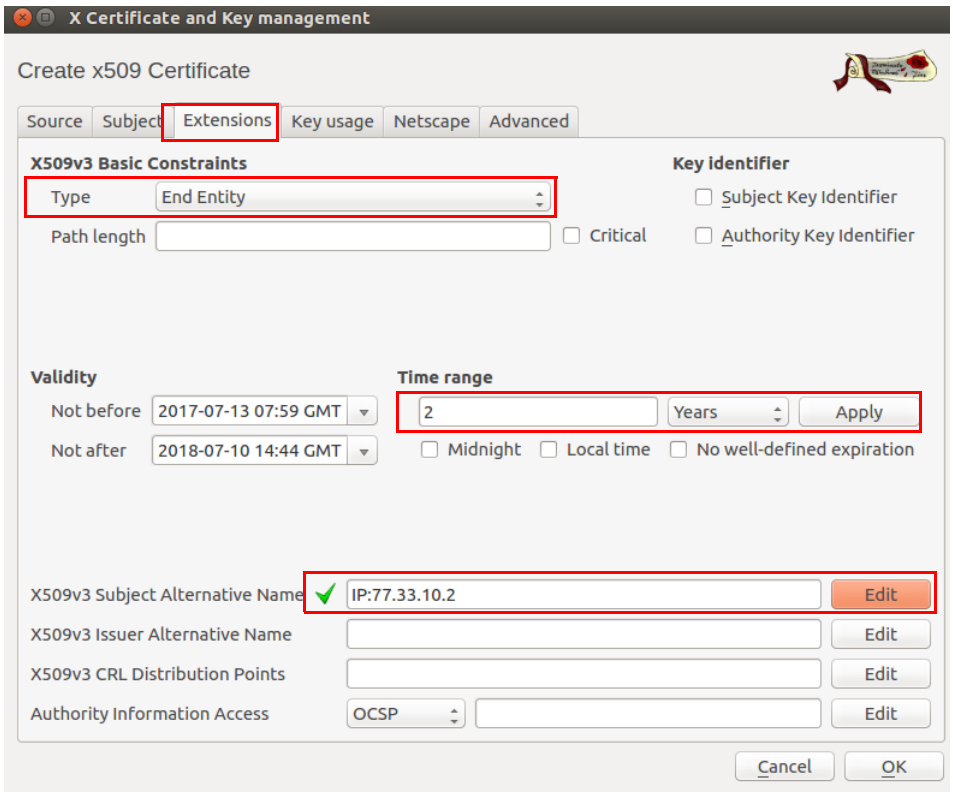
Gehen Sie wie folgt vor:

1. Im Abschnitt **Distinguished name**: Verwenden Sie die Eingabefelder von **Internal name** bis **emailAddress**, um die identifizierenden Parameter des Client-Zertifikats einzugeben.
2. Im Abschnitt **Private key**: Klicken Sie auf **Generate a new key**, um den privaten RSA-Schlüssel für das Zertifikat zu erstellen.



3. Geben Sie einen **Namen** für den Schlüssel ein, legen Sie die gewünschten Werte für **Keytype** und **Keysize** fest, und klicken Sie auf **Create**.
4. Wählen Sie die Registerkarte **Extensions**.

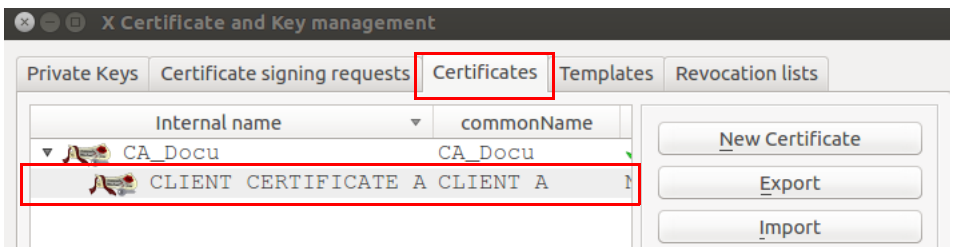
4.5.3 x509- (Client-) Zertifikat erstellen >> Registerkarte: Extensions



1. Im Abschnitt **X509v3 Basic Constraints**: Stellen Sie **Type** auf *End Entity* ein.
2. Im Abschnitt **Time Range**: Stellen Sie die Standard-Lebensdauer der Zertifikate ein, und klicken Sie auf **Apply**.
3. Der mGuard verwendet als standardmäßige VPN-Benennung den Subjektnamen des Zertifikats. Wenn Sie eine abweichende VPN-Benennung verwenden möchten (z. B. E-Mail-Adresse, Hostname oder IP-Adresse), muss diese Benennung als **subject alternative name** im Zertifikat vorhanden sein.

   Um eine weitere Benennung hinzuzufügen, klicken Sie in der Zeile **X509v3 Subject Alternative Name** auf **Edit**, wählen den Benennungstyp (E-Mail, DNS oder IP) aus, geben den Wert ein, klicken auf **Add** und anschließend auf **Apply**.
4. Klicken Sie zum Erstellen des Zertifikats auf **OK**.

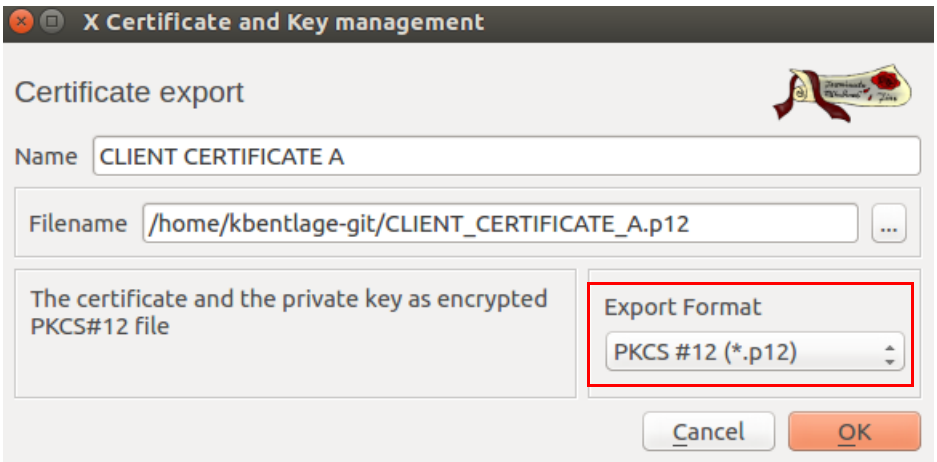
   Das Client-Zertifikat wird in der Registerkarte **Certificates** unterhalb des CA-Zertifikats angezeigt.



4.6 Zertifikat exportieren

Zum Exportieren eines Zertifikats, das mit *XCA* erstellt wurde, gehen Sie wie folgt vor:

1. Wählen Sie die Registerkarte **Certificates**.
2. Markieren Sie das Zertifikat, das exportiert werden soll.
3. Klicken Sie auf **Export**.



4. Wählen Sie das **Export Format** (PEM oder PKCS#12 – siehe Infobox unten).
5. Geben Sie den gewünschten **Filename** (Dateinamen) und den Ort an, an dem die Exportdatei gespeichert werden soll.
6. Klicken Sie auf **OK**.
7. Wenn Sie das Zertifikat als PKCS#12 exportieren, erscheint eine Eingabeaufforderung, in der Sie ein Passwort eingeben müssen, durch das der Export vor unbefugter Nutzung geschützt wird. Geben Sie das Passwort ein, und klicken Sie auf **OK**.

PKCS (Public Key Cryptography Standards)

PKCS #12: Personal Information Exchange Syntax v1.1 (Personaldaten-Austauschsyntax; definiert in **RFC 7292**)

PKCS #12 v1.1 beschreibt eine Übertragungssyntax für personenbezogene Identitätsinformationen, einschließlich der privaten Schlüssel, Zertifikate, verschiedener Geheimdaten und Erweiterungen. Maschinen, Applikationen, Browser, Internet-Kiosks usw., die diesen Standard unterstützen, ermöglichen einem Anwender den Import, Export und die Ausführung eines einzelnen Satzes aus personenbezogenen Identitätsinformationen. Dieser Standard unterstützt die direkte Übertragung personenbezogener Daten unter mehreren Privatsphäre- und Integritätsmodalitäten (RFC 7292).

PEM (Privacy-Enhanced Mail) (definiert in RFC 1421 bis 1424)

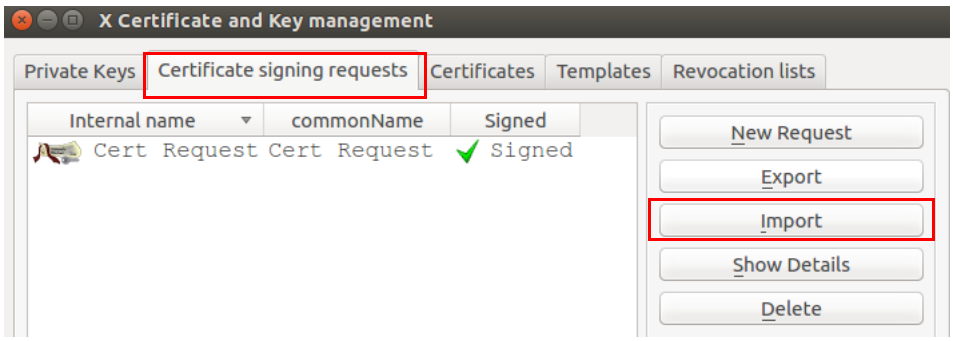
Ein PEM-Container kann nur das öffentliche Zertifikat oder eine gesamte Zertifikatskette enthalten (einschließlich des öffentlichen Schlüssels, privaten Schlüssels und der Root-Zertifikate).

PEM-Daten werden gewöhnlich in Dateien mit einem Suffix "**.pem**" oder "**.cer**" oder einem Suffix "**.crt**" (bei Zertifikaten) oder einem Suffix "**.key**" (bei öffentlichen oder privaten Schlüsseln) gespeichert.

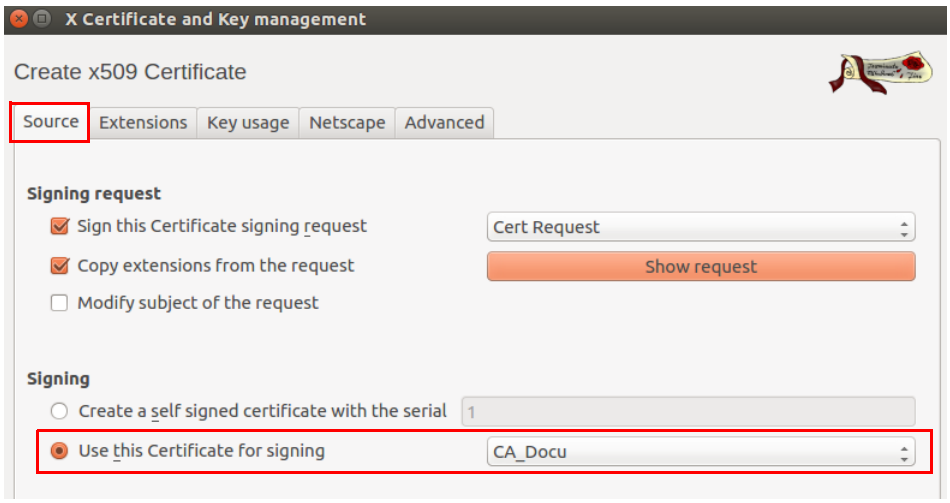
4.7 Zertifikatanfrage mit dem CA signieren

Gehen Sie zum Signieren eines Zertifikats wie folgt vor:

1. Wählen Sie die Registerkarte **Certificate signing requests**.
2. Klicken Sie auf **Import**.
3. Wählen Sie eine Zertifikatanfrage aus (PKCS#10-Datei), die durch die CA signiert werden soll, und klicken Sie auf **Open**.
4. Die importierte Zertifikatanfrage wird auf der Registerkarte **Certificate signing requests** angezeigt.



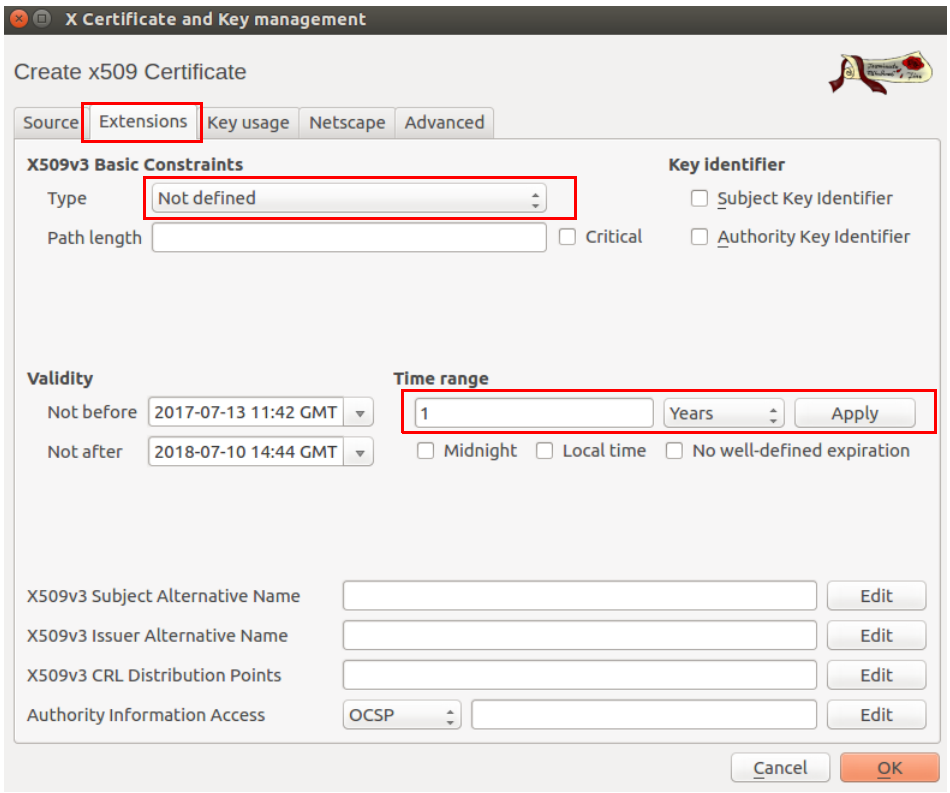
4.7.1 X-Zertifikat- und Schlüssel-Management >> Registerkarte: Source



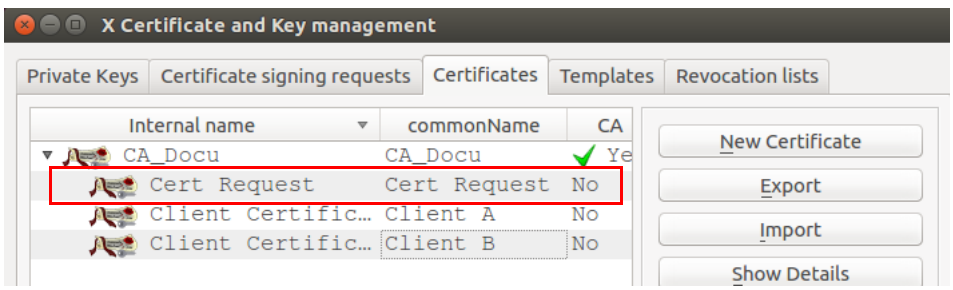
Gehen Sie zum Signieren der Zertifikatanfrage wie folgt vor:

1. Wählen Sie die Registerkarte **Certificate signing requests**.
2. Klicken Sie mit rechter Maustaste auf die Zertifikatanfrage, und wählen Sie im Kontextmenü **Sign**.
3. Im Abschnitt **Signing**: Stellen Sie sicher, dass das korrekte CA-Zertifikat im Feld **Use this certificate for signing** ausgewählt ist.
4. Wählen Sie die Registerkarte **Extensions**.

4.7.2 X-Zertifikat- und Schlüssel-Management >> Registerkarte: Extensions



1. Im Abschnitt **X509v3 Basic Constraints**: Lassen Sie **Type** auf *Not defined* eingestellt. Andernfalls würde *XCA* die Zertifikaterweiterungen zwei Mal in das signierte Zertifikat kopieren.
2. Im Abschnitt **Time Range**: Stellen Sie die Standard-Lebensdauer für das neue Zertifikat ein, und klicken Sie auf **Apply**.
3. Klicken Sie auf **OK**.
4. Die signierte Zertifikatanfrage wird in der Registerkarte **Certificates** unterhalb des CA-Zertifikats angezeigt.



4.8 Zertifikatssperrliste (Certificate Revocation List; CRL) verwenden

4.8.1 Zertifikat sperren

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie mit rechter Maustaste auf das Client-Zertifikat, das gesperrt werden soll, und wählen Sie im Kontextmenü **Revoke**.
3. Bearbeiten Sie die Parameter, und klicken Sie auf **OK**.
4. Das gesperrte Zertifikat wird mit einem Kreuzsymbol gekennzeichnet  , und der Zustand **Trust state** ist *Not trusted*.

4.8.2 CRL-Erneuerungszeitraum festlegen

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie mit rechter Maustaste auf die CA, und wählen Sie im Kontextmenü **CA >> Properties**.
3. Geben Sie den gewünschten Erneuerungszeitraum im Feld **Days until next CRL issuing** ein.
4. Klicken Sie auf **OK**.

4.8.3 CRL erstellen

1. Wählen Sie die Registerkarte **Certificates**.
2. Klicken Sie mit rechter Maustaste auf die CA, und wählen Sie im Kontextmenü **CA >> Generate CRL**.
3. Bearbeiten Sie die Parameter, und klicken Sie auf **OK**.
4. Die CRL wird auf der Registerkarte **Revocation lists** angezeigt.

4.8.4 Informationen über eine CRL einholen

1. Wählen Sie die Registerkarte **Revocation lists**.
2. Markieren Sie die CRL, und klicken Sie auf **Show Details**.

4.8.5 CRL exportieren

1. Wählen Sie die Registerkarte **Revocation lists**.
2. Markieren Sie die CRL.
3. Klicken Sie auf **Export**.
4. Legen Sie Dateiname und Speicherort der CRL fest.
5. Wählen Sie das Exportformat (DER oder PEM).
6. Klicken Sie auf **OK**.

4.9 Beispiel: VPN-Verbindung zwischen zwei mGuard-Geräten

Um die benötigten Zertifikate für eine VPN-Verbindung zwischen zwei mGuard-Geräten zu erstellen und zu importieren, gehen Sie wie folgt vor:

CA-Zertifikat

- Erstellen Sie ein CA-Zertifikat gemäß der Beschreibung in Kapitel „CA-Zertifikat erstellen“ auf Seite 110.

Client-Zertifikat

- Erstellen Sie ein Client-Zertifikat für mGuard **#1** und ein Client-Zertifikat für mGuard **#2** (siehe die Beschreibung in Kapitel „Client-Zertifikat erstellen“ auf Seite 114).

Exportzertifikate

- Exportieren Sie die Zertifikate gemäß der Beschreibung in Kapitel „Zertifikat exportieren“ auf Seite 118.

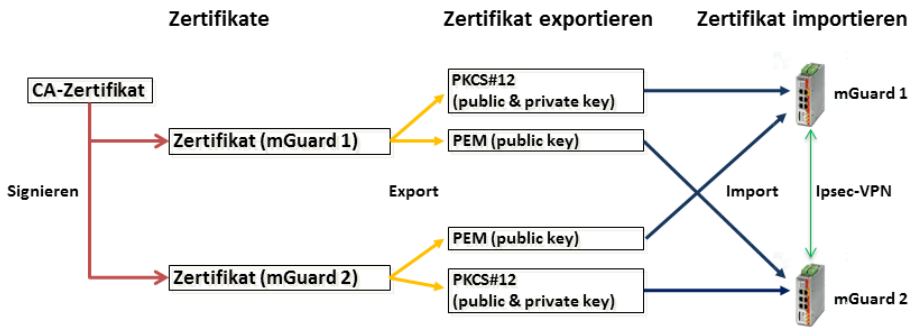
Die folgenden Exporte sind erforderlich:

– mGuard **#1** als PKCS#12: Dieser Export muss bei mGuard **#1** als *Maschinenzertifikat* importiert werden (Menü: Authentifizierung >> Zertifikate, Registerkarte *Maschinenzertifikate*).

– mGuard **#2** als PKCS#12: Dieser Export muss bei mGuard **#2** als *Maschinenzertifikat* importiert werden (Menü: Authentifizierung >> Zertifikate, Registerkarte *Maschinenzertifikate*).

– mGuard **#1** als PEM: Dieser Export muss bei mGuard **#2** als Verbindungszertifikat importiert werden (Menü: IPsec VPN >> Verbindungen >> (*Bearbeiten*), Registerkarte *Authentifizierung*).

– mGuard **#2** als PEM: Dieser Export muss bei mGuard **#1** als Verbindungszertifikat importiert werden (Menü: IPsec VPN >> Verbindungen >> (*Bearbeiten*), Registerkarte *Authentifizierung*).



5 IPsec-VPN-Verbindung zwischen iOS-Client und mGuard-Gerät herstellen

Dokument-ID: 108393_de_02

Dokument-Bezeichnung: AH DE MGUARD IOS SUPPORT

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument werden die notwendigen Schritte zur Konfiguration einer VPN-Verbindung zwischen einem iOS-Client (iPad oder iPhone mit iOS ab Version 8.0) und einem mGuard-Gerät (Server) beschrieben.

5.1 Einleitung

Das iOS-Gerät dient als Remote-Client zur Initialisierung der IPsec-VPN-Verbindung. Der mGuard übernimmt die Funktion des lokalen Servers sowie zur Konfiguration und Bereitstellung des lokalen Netzwerkes für die Clients über die XAuth/Mode-Config-Erweiterung.

Für die VPN-Verbindungen ist die Installation von X.509-Zertifikaten und Schlüsseln sowohl bei dem iOS-Client als auch dem mGuard-Gerät erforderlich

Anforderungen

- mGuard-Gerät mit installierter Firmware ab Version 8.5
- iOS-Gerät mit installierter Firmware ab Version 8.0
- Sämtliche erforderlichen und signierten Zertifikate

Wie erstelle ich X.509-Zertifikate?

Weiterführende Informationen zur Zertifikatsverwaltung finden Sie als Anwenderhinweis in dem Dokument „AH DE MGUARD APPNOTES“, verfügbar im PHOENIX CONTACT Webshop unter: phoenixcontact.net/products.

5.2 Zertifikate verwalten

Für den Aufbau einer IPsec-VPN-Verbindung zwischen einem iOS-Client und einem mGuard-Server müssen sich die Geräte über X.509-Zertifikate gegenseitig authentifizieren.

Tabelle 5-1 Erforderliche Zertifikate

Gerät	Erforderliches Zertifikat	Format
mGuard	CA-Zertifikat	**PEM / CER**
	mGuard-Maschinenzertifikat (von CA signiert)	**PKCS#12**
iOS-Client	CA-Zertifikat	**PEM / CER**
	iOS-Client-Zertifikat (von CA signiert)	**PKCS#12**

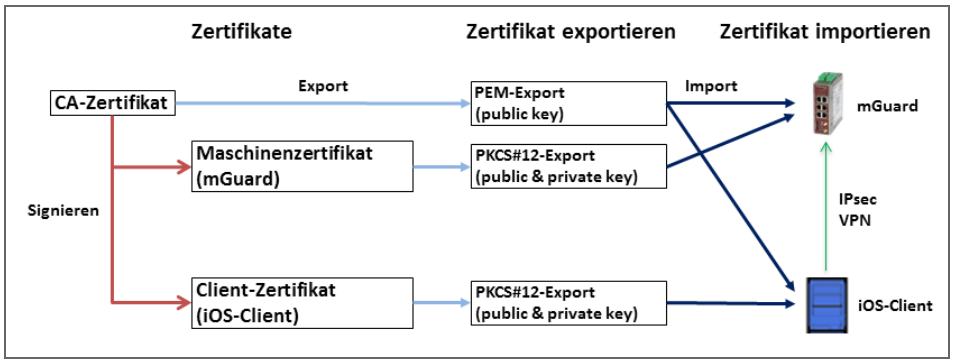


Bild 5-1 Zertifikatsverwaltung für Verbindungen mit Initialisierung durch **iOS-Clients**

5.2.1 Erforderliche Zertifikate auf dem mGuard-Gerät

Die folgenden Zertifikate müssen auf dem mGuard-Gerät installiert werden:

1. **CA-Zertifikat (PEM / CER)**

   Der mGuard überprüft die Echtheit des iOS-Clients auf Grundlage der CA-Signatur des vorgezeigten iOS-Client-Zertifikats.

2. **mGuard-Maschinenzertifikat (PKCS#12)**

   Der **iOS-Client** überprüft die Echtheit des mGuards auf Grundlage der CA-Signatur des mGuard-Maschinenzertifikats. Das signierende CA-Zertifikat muss daher auf dem iOS-Client installiert sein.

ACHTUNG: Die Netzwerkadresse des mGuard-Geräts muss im Zertifikat eingetragen werden

Bei der Erstellung des mGuard-Maschinenzertifikats muss an zwei Stellen die IP-Adresse (oder der Hostname/DNS-Name) eingetragen werden, die der iOS-Client zum Aufbau einer VPN-Verbindung mit dem mGuard-Gerät verwendet (in der Regel die externe Server-IP-Adresse des mGuard-Geräts):

1. **commonName (CN)** --> siehe Bild 5-2 und Bild 5-3
2. **X509v3 Subject Alternative Name** --> siehe Bild 5-4

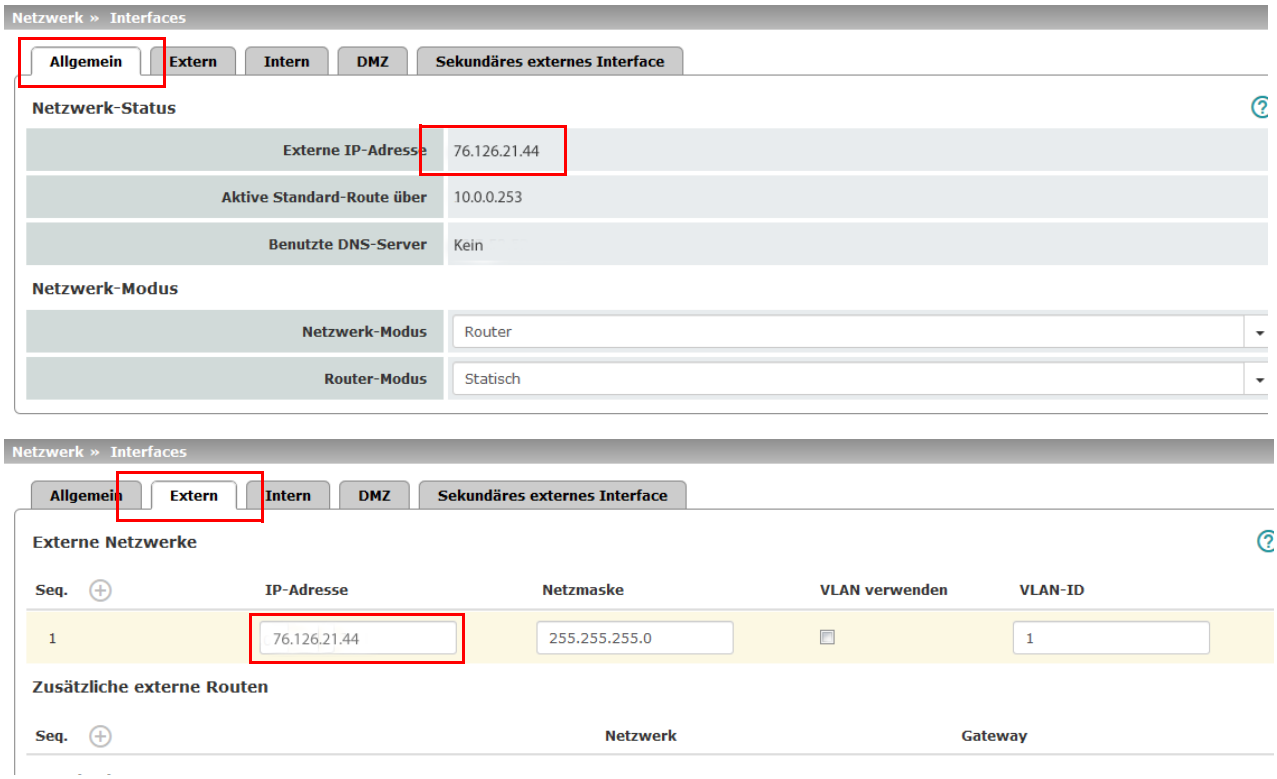


Bild 5-2 (Beispiel) Netzwerkeinstellungen am mGuard: Externe IP-Adresse hervorgehoben

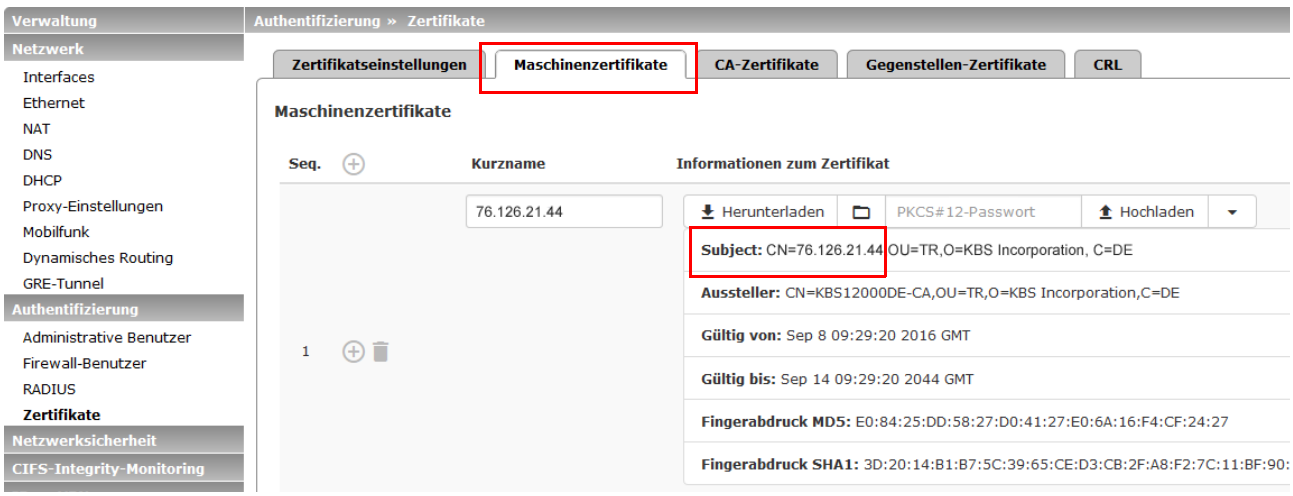


Bild 5-3 Maschinenzertifikat: CN = Externe IP-Adresse oder Hostname/DNS-Name des mGuards

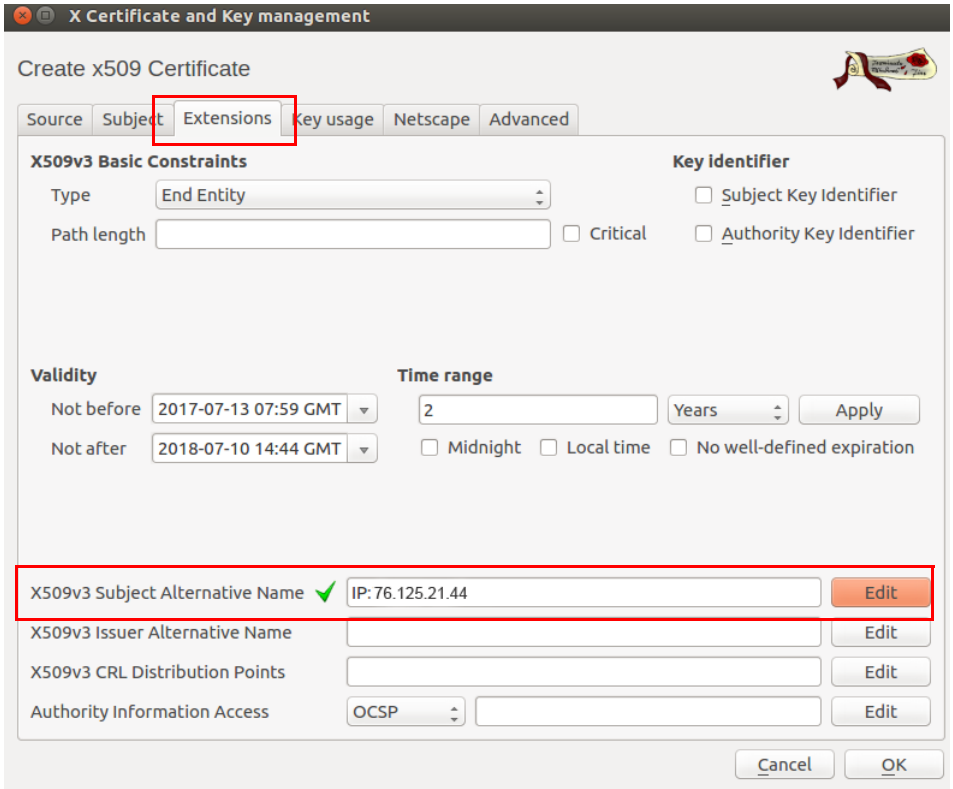


Bild 5-4 Maschinenzertifikat: Beispiel (XCA) – X509v3 Subject Alternative Name

5.2.2 Erforderliche Zertifikate auf dem iOS-Client

Die folgenden Zertifikate müssen auf dem iOS-Gerät installiert werden (siehe auch Seite 124):

1. **CA-Zertifikat (PEM/CER)**

   Der iOS-Client überprüft die Echtheit des mGuard-Servers auf Grundlage der CA-Signatur des vorgezeigten mGuard-Maschinenzertifikats.

2. **iOS-Client-Zertifikat (PKCS#12)**

   Der mGuard überprüft die Echtheit des iOS-Clients auf Grundlage der CA-Signatur des vorgezeigten iOS-Client-Zertifikats. Das signierende CA-Zertifikat muss daher auf dem mGuard installiert sein.

Da der iOS-Client die Schlüsselkette (*keychain*) einer PKCS#12-Datei ignoriert, muss das signierende CA-Zertifikat separat auf dem mGuard installiert werden.

5.2.3 Zertifikate auf dem mGuard-Gerät installieren

Maschinenzertifikat

Zum Hochladen des mGuard-Maschinenzertifikats auf den mGuard gehen Sie wie folgt vor:

1. Wählen Sie **Authentifizierung >> Zertifikate >> Maschinenzertifikate**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon 🗀.
4. Wählen Sie das Maschinenzertifikat aus (PKCS#12-Datei), und klicken Sie auf „Öffnen“.
5. Geben Sie das Passwort ein, mit dem der geheime Schlüssel des Zertifikats gesichert wurde.
6. Klicken Sie auf die Schaltfläche „Hochladen“.
   ► Das hochgeladene Zertifikat erscheint in der Zertifikate-Liste.
7. Klicken Sie auf das Icon 💾, um die Einstellungen zu speichern.
   ► Das mGuard-Maschinenzertifikat wurde hochgeladen und kann zur Authentifizierung gegenüber dem iOS-Client verwendet werden (siehe “mGuard konfigurieren” , „Registerkarte „Authentifizierung““).

CA-Zertifikat

Zum Hochladen des CA-Zertifikats auf den mGuard gehen Sie wie folgt vor:

1. Wählen Sie **Authentifizierung >> Zertifikate >> CA-Zertifikate**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon 🗀.
4. Wählen Sie das CA-Zertifikat aus (PEM- oder CER-Datei), und klicken Sie auf „Öffnen“.
5. Klicken Sie auf die Schaltfläche „Hochladen“.
   ► Das hochgeladene Zertifikat erscheint in der Zertifikate-Liste.
6. Klicken Sie auf das Icon 💾, um die Einstellungen zu speichern.
   ► Das CA-Zertifikat wurde hochgeladen und kann zur Authentifizierung des iOS-Client verwendet werden (siehe “mGuard konfigurieren” , „Registerkarte „Authentifizierung““).

5.2.4 Zertifikate auf dem iOS-Client installieren

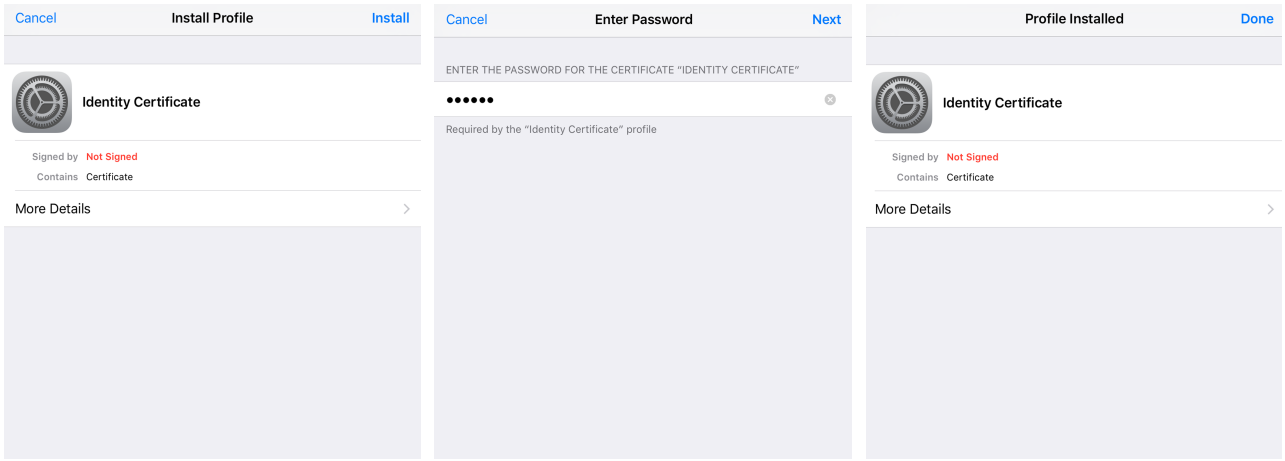


Bild 5-5 Installation der Client-Zertifikate

Bild 5-6 Installierte Zertifikate in der Zertifikate-Liste

Zur Installation des **iOS-Client-Zertifikats** oder des **CA-Zertifikats** auf dem iOS-Client gehen Sie wie folgt vor:

1. Stellen Sie das Zertifikat auf dem iOS-Client zur Verfügung.
2. Öffnen Sie die Datei.
   ► Das Fenster „Identitätszertifikat“ wird angezeigt.
3. Klicken Sie zwei Mal auf „Installieren“.
   ► Wenn das Zertifikat mit einem geheimen Schlüssel (PKCS#12-Dateien) gesichert wurde, wird das Fenster „Passwort“ angezeigt.
4. Geben Sie in diesem Fall das Passwort ein.
5. Klicken Sie auf „Weiter“.
   ► Das Fenster „Profil installiert“ wird angezeigt.
6. Klicken Sie auf „Fertig“, um die Installation des Zertifikats zu beenden.
   ► Das installierte Zertifikat erscheint in der Zertifikate-Liste.

5.3 VPN-Verbindungen konfigurieren

5.3.1 mGuard konfigurieren

Die IPsec-VPN-Verbindung zwischen iOS-Client und mGuard wird über die Erweiterung „XAuth/Mode Config“ hergestellt. Die Konfiguration des iOS-Clients erfolgt über den mGuard und wird dem iOS-Client mitgeteilt.

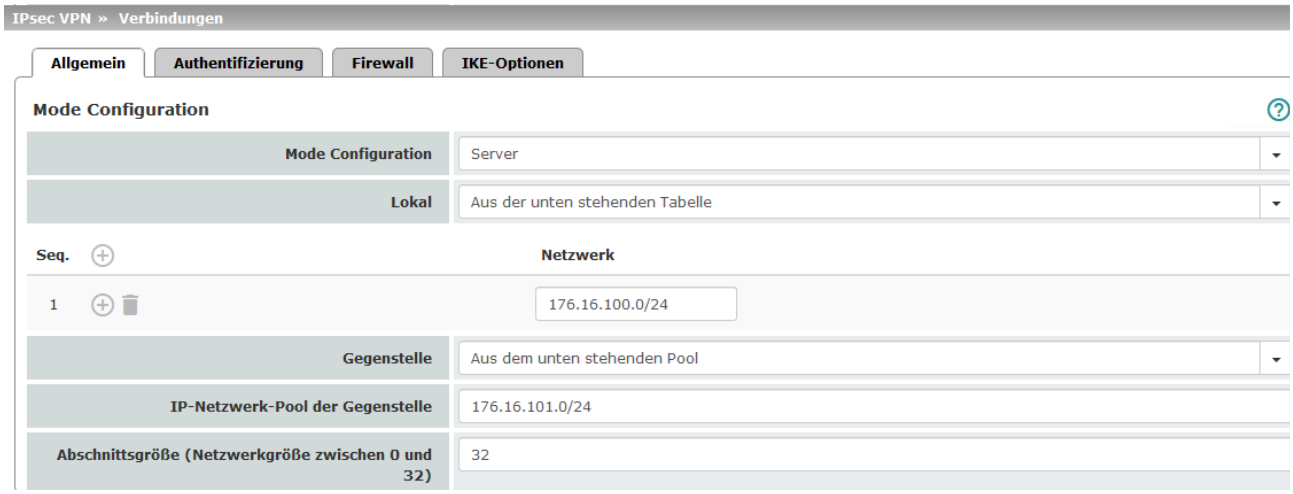


Bild 5-7 mGuard VPN-Konfiguration – Mode Configuration

5.3.1.1 Registerkarte „Allgemein“

Zur Konfiguration einer VPN-Verbindung zum iOS-Client auf dem mGuard gehen Sie wie folgt vor:

1. Wählen Sie **IPsec VPN >> Verbindungen >> Allgemein**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon ✎.
   ► Die Registerkarte „**Allgemein**“ erscheint.
4. Geben Sie einen beschreibenden Namen für die Verbindung ein, und ändern Sie optional weitere Einstellungen.

   Überprüfen Sie, ob das Eingabefeld „Adresse des VPN-Gateways der Gegenstelle“ den Wert „**%any**“ enthält und „Verbindungsinitiierung“ auf „**Warte**“ gesetzt ist (Standardwerte).

5. **Mode Configuration**: Wählen Sie die Option „**Server**“.
6. **Lokal**: Geben Sie alle lokalen Netzwerke (1 oder mehrere) auf Server-Seite (mGuard) ein, auf die über die VPN-Verbindung durch den iOS-Client zugegriffen werden soll.
   – **Fest**: Das *„Lokale IP-Netzwerk“* muss auf 0.0.0.0/0 gesetzt werden. In diesem Fall wird der gesamte Datenverkehr vom iOS-Client über die VPN-Verbindung übertragen.
   – **Aus der unten stehenden Tabelle**: Nur der Datenverkehr zu den in der *unten stehenden Tabelle* aufgelisteten Netzwerken wird über die VPN-Verbindung übertragen. Bei iOS-Clients wird bei Datenverkehr zu Netzwerken, die nicht in der *unten stehenden Tabelle* aufgelistet sind, die VPN-Verbindung umgangen (**Bypass**).

7. **Gegenstelle**: Definieren Sie den Netzwerk-Pool (**Aus dem unten stehenden Pool**), aus dem der mGuard einen variablen Abschnitt (**Abschnittsgröße**) zur Nutzung durch das Netzwerk des Remote-Clients zuweist.

5.3.1.2 Registerkarte „Authentifizierung“

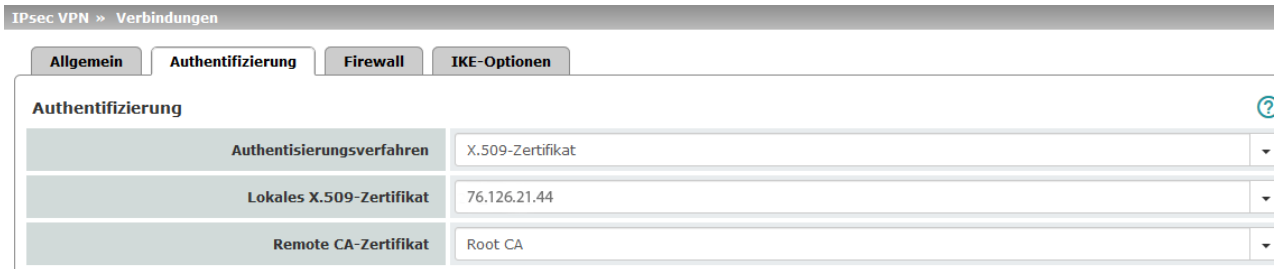


Bild 5-8 mGuard VPN-Konfiguration – Authentifizierung

Die VPN-Verbindung zwischen einem iOS-Client und dem mGuard muss durch X.509-Zertifikate autorisiert werden, die auf den entsprechenden Geräten installiert werden müssen (siehe „Zertifikate verwalten“ auf Seite 124).

Um der VPN-Verbindung die erforderlichen Zertifikate zuzuweisen, gehen Sie wie folgt vor:

1. Wählen Sie **IPsec VPN >> Verbindungen**.
2. Bearbeiten Sie die gewünschte VPN-Verbindung (Registerkarte „Authentifizierung“).
3. Wählen Sie „**Authentisierungsverfahren**: X.509 Certificate“.
4. Wählen Sie als *„Lokales X.509-Zertifikat“* das **mGuard-Maschinenzertifikat**.

   Der *Common Name* (CN) und der *Subject Alternative Name* des Zertifikats müssen mit der IP-Adresse (oder dem Hostnamen/DNS-Namen) des mGuard-Geräts übereinstimmen, die der iOS-Client zum Aufbau einer VPN-Verbindung mit dem mGuard-Gerät verwendet (siehe Kapitel 5.2.1).

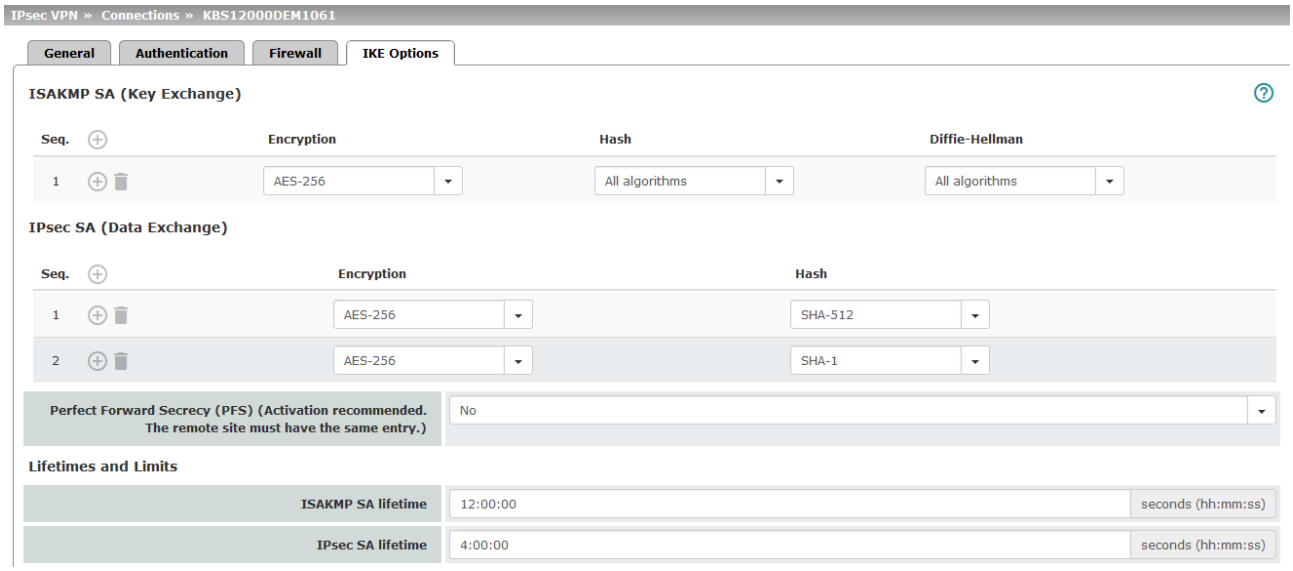
   Das lokale Zertifikat muss mit dem CA-Zertifikat signiert worden sein, das auf dem iOS-Client installiert wurde.
5. Wählen Sie als *„Remote CA-Zertifikat“* den Namen des CA-Zertifikats das zum Signieren des **iOS-Client-Zertifikats** verwendet wurde.
6. Klicken Sie auf auf das Icon , um die Einstellungen zu speichern.
   ► Die VPN-Verbindung wird nach einer Initialisierung durch den Client hergestellt.

5.3.1.3 Registerkarte „Firewall“

Die VPN-Firewall beschränkt den Zugriff über den VPN-Tunnel. Sie können die VPN-Firewall bei Bedarf konfigurieren.

In der werkseitigen Voreinstellung wird **jeglicher eingehender** und **ausgehender** Datenverkehr zugelassen**.**

5.3.1.4 Registerkarte „IKE-Optionen“



Die werkseitig voreingestellten IKE-Optionen müssen geändert werden:

1. Wählen Sie **IPsec VPN >> Verbindungen**.
2. Bearbeiten Sie die gewünschte VPN-Verbindung (Registerkarte „IKE-Optionen“).
3. Konfigurieren Sie die folgenden Einstellungen (und behalten Sie bei allen anderen Einstellungen die werkseitige Voreinstellung bei).

ISAKMP-SA (Schlüsselaustausch)

- Verschlüsselung: AES-256
- Prüfsumme: Alle Algorithmen
- Diffie-Hellman: Alle Algorithmen

IPsec-SA (Datenaustausch)

- Klicken Sie auf das Icon ⊕, um zwei Tabellenzeilen zu erzeugen und die folgenden Einstellungen zu verwenden:
  - (Zeile 1) Encryption: AES-256 | Hash: SHA-512
  - (Zeile 2) Encryption: AES-256 | Hash: SHA-1

5.3.2 iOS-Client konfigurieren

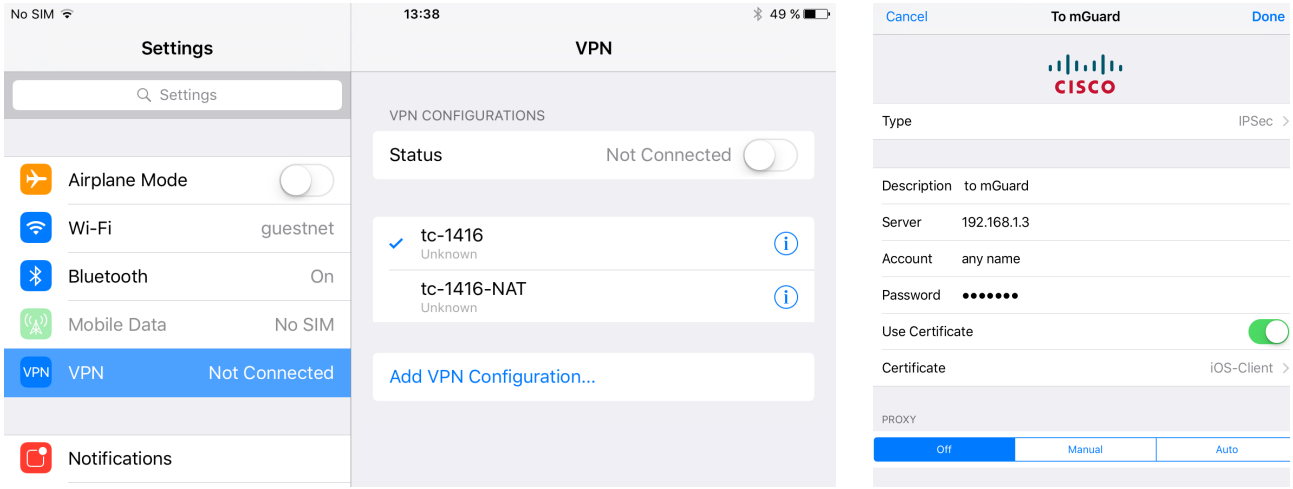


Bild 5-9 iOS-Client: VPN-Konfiguration

Um eine IPsec-VPN-Verbindung auf dem iOS-Client zu konfigurieren, gehen Sie wie folgt vor:

1. Wählen Sie „Einstellungen >> VPN“.
2. Klicken Sie auf „VPN hinzufügen“.
3. Klicken Sie auf „Typ“.
4. Wählen Sie „IPsec“, und wechseln Sie anschließend zur Konfigurations-Seite.
5. Füllen Sie folgende Eingabefelder aus:
   - *Beschreibung*: Ein beschreibender Name für die VPN-Verbindung
   - *Server*: Externe IP-Adresse oder Hostname/DNS-Name des mGuard-Servers

   Diese IP-Adresse bzw. dieser Hostname/DNS-Name muss mit dem *Common Name* (CN) und dem *Subject Alternative Name* des mGuard-Maschinenzertifikats übereinstimmen (siehe Kapitel 5.2.1).

   - *Account*: Die Authentifizierung von VPN-Gegenstellen ist von Zertifikaten abhängig. Daher werden der Name und das Passwort des Kontos **durch den mGuard ignoriert**. Geben Sie einen beliebigen Text ein, um weitere Anfragen zu vermeiden.
   - *Passwort*: Das Passwort wird **durch den mGuard ignoriert**. Geben Sie einen beliebigen Text ein.
   - *Zertifikat verwenden*: Aktivieren Sie den Schalter, um ein Zertifikat auszuwählen.
6. Klicken Sie auf „*Zertifikat*“.
   ► Eine Liste mit allen installierten Zertifikaten erscheint.
7. Wählen Sie das entsprechende Client-Zertifikat aus, und klicken Sie auf „Zurück“.
8. Klicken Sie auf „Fertig“, um die Konfiguration zu speichern.
   ► Die VPN-Verbindung ist nun gespeichert und kann gestartet werden.

5.4 VPN-Verbindungen auf dem iOS-Client starten

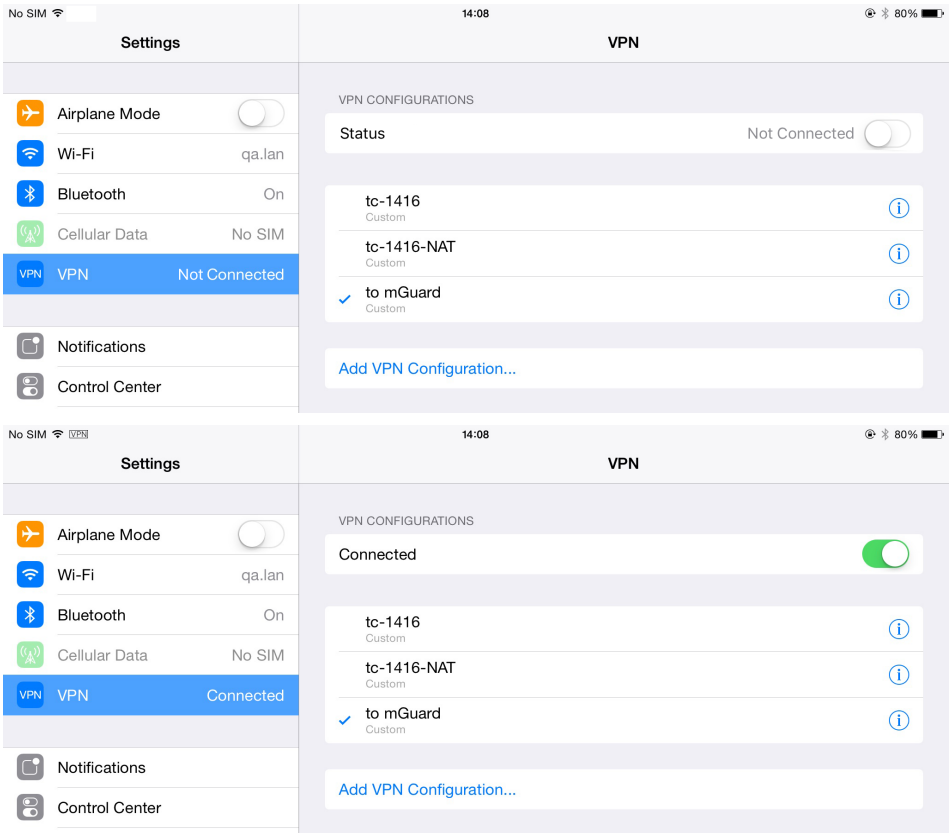


Bild 5-10 VPN-Verbindung auf dem iOS-Client starten

Zum Starten einer IPsec-VPN-Verbindung auf dem iOS-Client gehen Sie wie folgt vor:

1. Wählen Sie „Einstellungens >> VPN“.
2. Klicken Sie auf den Namen der entsprechenden VPN-Verbindung.
3. Klicken Sie im Bereich „VPN CONFIGURATIONEN“ auf die Schaltfläche „Nicht verbunden“.
   ► Die VPN-Verbindung wird hergestellt, und der Status ändert sich von „Nicht verbunden “ zu „Verbunden“.

Wenn die Verbindung fehlschlägt, klicken Sie auf das „Info“-Icon der VPN-Verbindung, um die Konfiguration auf Fehler oder den Status Ihrer Internetverbindung zu überprüfen.

5.5 VPN-Verbindungen auf dem mGuard überprüfen

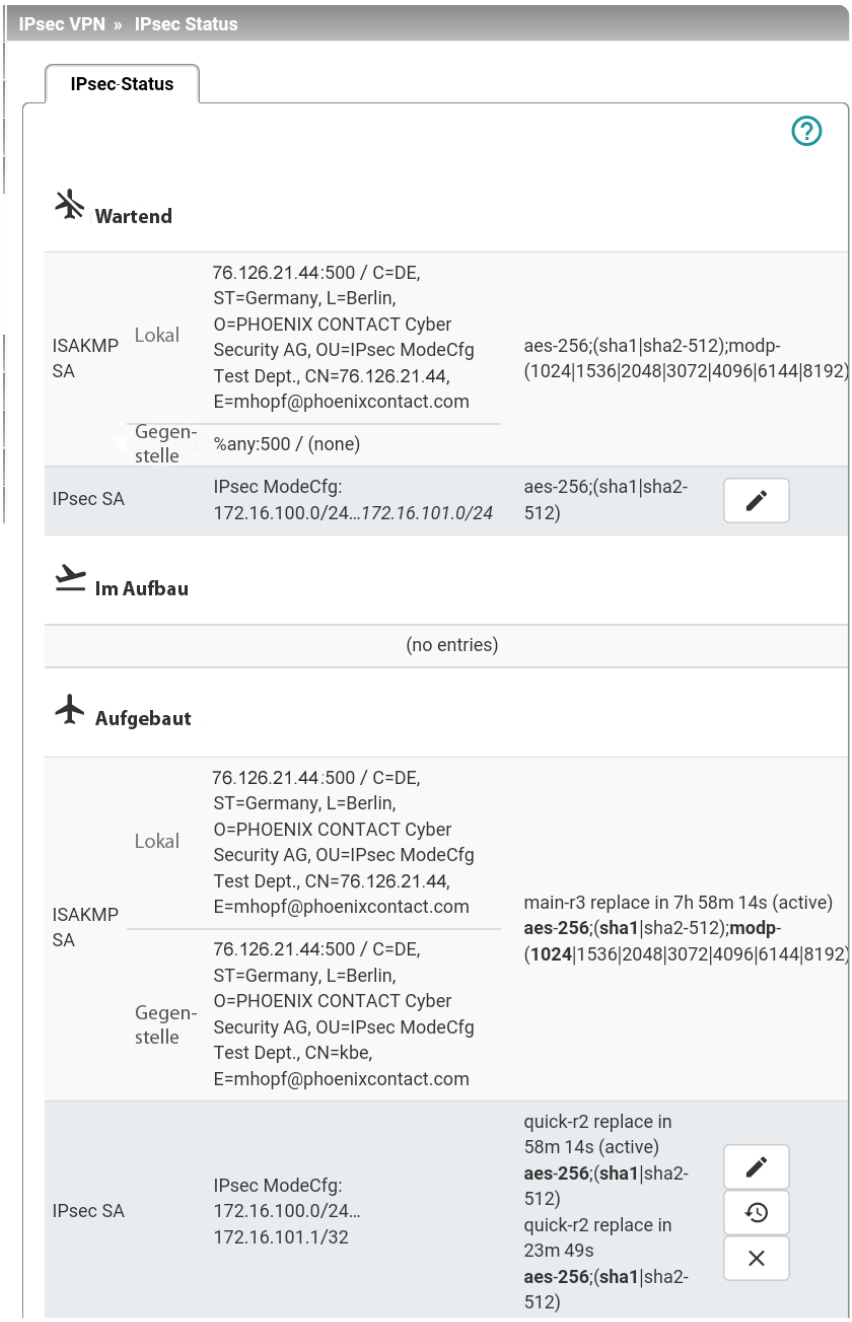


Bild 5-11 IPsec-VPN-Status

Zur Überprüfung des Status einer IPsec-VPN-Verbindung gehen Sie wie folgt vor:

- Wählen Sie **IPsec VPN >> IPsec-Status**.
  - ► Eine hergestellte IPsec-VPN-Verbindung wird im Bereich „Aufgebaut“ angezeigt.

6 IPsec-VPN-Verbindung zwischen Android-Client und mGuard-Gerät herstellen

Dokument-ID: 108394_de_01

Dokument-Bezeichnung: AH DE MGUARD ANDROID SUPPORT

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument werden die notwendigen Schritte zur Konfiguration einer VPN-Verbindung zwischen einem Android-Client (Tablet-PC oder Mobiltelefon mit Android OS Version 6.0) mit einem mGuard-Server beschrieben.

6.1 Einleitung

Das Android-Gerät dient als Remote-Client zur Initialisierung der IPsec-VPN-Verbindung. Der mGuard übernimmt die Funktion des lokalen Servers sowie zur Konfiguration und Bereitstellung des lokalen Netzwerkes für die Clients über die XAuth/Mode-Config-Erweiterung.

Für die VPN-Verbindungen ist die Installation von X.509-Zertifikaten und Schlüsseln sowohl bei dem Android-Client als auch dem mGuard-Gerät erforderlich.

Allgemeine Informationen zur Konfiguration von VPN-Verbindungen finden Sie unter „Software-Referenzhandbuch – mGuard-Firmware“, online verfügbar oder im PHOENIX CONTACT Webshop unter: phoenixcontact.net/products. Weiterführende Informationen zum Android-Client finden Sie auf den entsprechenden Webseiten des Herstellers.

Das Aussehen der Einstellungen und Bedienoberflächen unterscheidet sich deutlich bei Android-Geräten unterschiedlicher Modelle und Hersteller. Das vorliegende Dokument wurde auf Grundlage des Geräts *SAMSUNG SM-T580* mit installierter Android-Version 6.0.1 erstellt.

6.1.1 Anforderungen

- mGuard-Gerät mit installierter Firmware ab Version 8.5
- Android-Gerät mit installierter Firmware ab Version 6.0
- Sämtliche erforderlichen und signierten Zertifikate

Wie erstelle ich X.509-Zertifikate?

Weiterführende Informationen zur Zertifikatsverwaltung finden Sie als Anwenderhinweis in dem Dokument „AH DE MGUARD APPNOTES“, verfügbar im PHOENIX CONTACT Webshop unter: phoenixcontact.net/products.

6.1.2 Haftungsausschluss

Dieses Dokument stellt keinen Ersatz für die Anwenderhandbücher der betreffenden Produkte dar.

6.2 Zertifikate verwalten

Für den Aufbau einer IPsec-VPN-Verbindung zwischen einem Android-Client und einem mGuard-Server müssen sich die Geräte über X.509-Zertifikate gegenseitig authentifizieren.

Tabelle 6-1 Erforderliche Zertifikate

Gerät	Erforderliches Zertifikat	Format
mGuard	CA-Zertifikat	**PEM / CER**
	mGuard-Maschinenzertifikat (von CA signiert)	**PKCS#12**
Android-Client	mGuard-Maschinenzertifikat (von CA signiert)	**PEM / CER**
	Android-Client-Zertifikat (von CA signiert)	**PKCS#12**

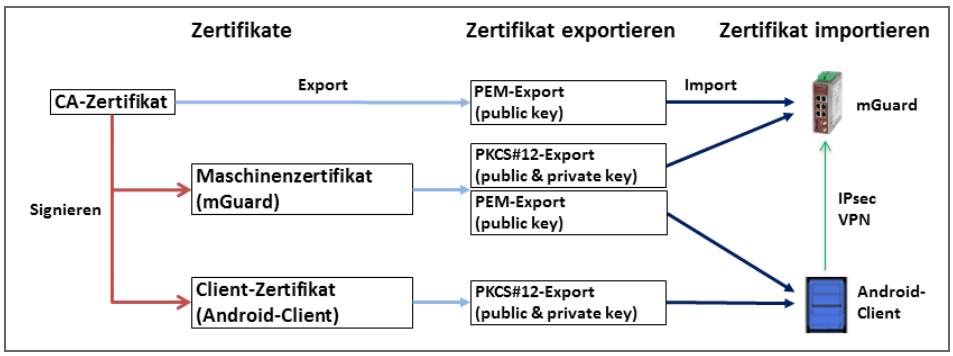


Bild 6-1 Zertifikathandhabung für Verbindungen mit Initialisierung durch **Android-Clients**

Die Begriffe „Maschinenzertifikat“ und „Client-Zertifikat“ bezeichnen ein X.509-Zertifikat und den zugehörigen privaten Schlüssel (*private key*), über den sich die Maschine bzw. der Client gegenüber den Gegenstellen identifiziert.

6.2.1 Erforderlichen Zertifikate auf dem mGuard-Gerät

Die folgenden Zertifikate müssen auf dem mGuard-Gerät installiert werden:

1. **CA-Zertifikat (PEM / CER)**

   Der mGuard überprüft die Echtheit des Android-Clients auf Grundlage der CA-Signatur des vorgezeigten Android-Client-Zertifikats.

2. **mGuard-Maschinenzertifikat (PKCS#12)**

   Der **Android-Client** überprüft die Echtheit des mGuards auf Grundlage des vorgezeigten mGuard-Maschinenzertifikats. Das mGuard-Maschinenzertifikat muss daher auch auf dem Android-Client installiert sein.

6.2.2 Erforderliche Zertifikate auf dem Android-Client

Die folgenden Zertifikate müssen auf dem Android-Gerät installiert werden (siehe auch Seite 139):

1. **mGuard-Maschinenzertifikat (PEM/CER)**
   Der Android-Client überprüft die Echtheit des mGuard-Servers auf Grundlage des vorgezeigten mGuard-Maschinenzertifikats.
2. **Android-Client-Zertifikat (PKCS#12)**
   Der mGuard überprüft die Echtheit des Android-Clients auf Grundlage der CA-Signatur des vorgezeigten Android-Client-Zertifikats. Das signierende CA-Zertifikat muss daher auf dem mGuard installiert sein.

6.2.3 Zertifikate auf dem mGuard-Gerät installieren

Maschinenzertifikat

Zum Hochladen des mGuard-Maschinenzertifikats auf den mGuard gehen Sie wie folgt vor:

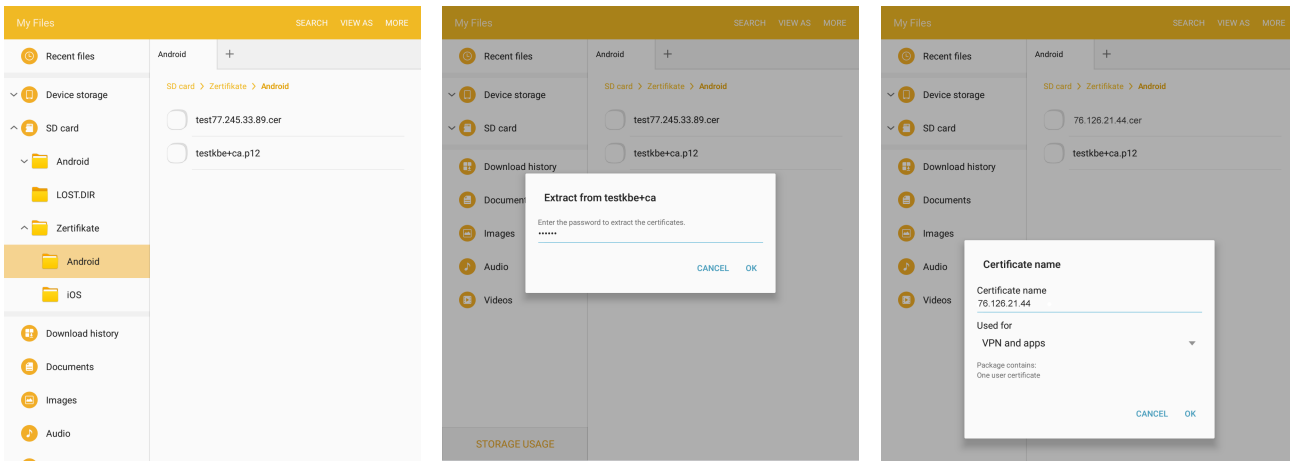
1. Wählen Sie **Authentifizierung >> Zertifikate >> Maschinenzertifikate**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon 🗀.
4. Wählen Sie das Maschinenzertifikat aus (PKCS#12-Datei), und klicken Sie auf „Öffnen“.
5. Geben Sie das Passwort ein, mit dem der geheime Schlüssel des Zertifikats gesichert wurde.
6. Klicken Sie auf die Schaltfläche „Hochladen“.
   ► Das hochgeladene Zertifikat erscheint in der Zertifikate-Liste.
7. Klicken Sie auf das Icon 💾, um die Einstellungen zu speichern.
   ► Das mGuard-Maschinenzertifikat wurde hochgeladen und kann zur Authentifizierung gegenüber dem Android-Client verwendet werden (siehe “mGuard konfigurieren” , Registerkarte „Authentifizierung“).

CA-Zertifikat

Zum Hochladen des CA-Zertifikats auf den mGuard gehen Sie wie folgt vor:

1. Wählen Sie **Authentifizierung >> Zertifikate >> CA-Zertifikate**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon 🗀.
4. Wählen Sie das CA-Zertifikat aus (PEM- oder CER-Datei), und klicken Sie auf „Öffnen“.
5. Klicken Sie auf die Schaltfläche „Hochladen“.
   ► Das hochgeladene Zertifikat erscheint in der Zertifikate-Liste.
6. Klicken Sie auf das Icon 💾, um die Einstellungen zu speichern.
   ► Das CA-Zertifikat wurde hochgeladen und kann zur Authentifizierung des Android-Client verwendet werden (siehe “mGuard konfigurieren” , Registerkarte „Authentifizierung“).

6.2.4 Zertifikate auf dem Android-Client installieren



Zur Installation des **Android-Client-Zertifikats** (PKCS#12-Datei mit signierendem CA-Zertifikat) und des **mGuard-Maschinenzertifikats** (PEM-/CER-Datei) auf dem Android-Client gehen Sie wie folgt vor:

1. Um die VPN-Funktion auf dem Android-Gerät nutzen zu können, müssen Sie das Bildschirm-Sperrmuster, den PIN oder das Passwort setzen.
2. Stellen Sie die Zertifikatsdateien auf dem Android-Client zur Verfügung.
3. Öffnen Sie die PKCS#12-Datei (**.p12),* um den Android-Client und die signierenden CA-Zertifikate zu extrahieren und zu installieren.
   ► Das Fenster „Zertifikat extrahiere“ erscheint.

   Falls das Fenster nicht erscheint und das Gerät stattdessen den Inhalt der Datei anzeigt, laden Sie die Datei in den Speicher Ihres Geräts herunter oder stellen sie über eine SD-Karte zur Verfügung. Öffnen Sie die Datei in dem entsprechenden Verzeichnis.

4. Geben Sie das Passwort ein, und klicken Sie auf „OK“.
   ► Das Fenster „Zertifikatsname“ erscheint.
5. Optional: Weisen Sie dem Zertifikat einen neuen Namen zu, um das Zertifikat einfacher in der Zertifikate-Liste finden zu können.
6. Klicken Sie auf „OK“, um die Installation des Android-Client-Zertifikats und des signierenden CA-Zertifikats zu beenden.
   ► Die installierten Zertifikate erscheinen in der Zertifikate-Liste des Anwenders (Einstellungen >> Gerätesicherheit >> Andere Sicherheitseinstellungen >> Benutzerzertifikate).
7. Öffnen Sie die PEM- oder CER-Datei (**.pem / *.cer*), um das mGuard-Maschinenzertifikat zu installieren.
   ► Das Fenster „Zertifikatsname“ erscheint.

   Falls das Fenster nicht erscheint und das Gerät stattdessen den Inhalt der Datei anzeigt, laden Sie die Datei in den Speicher Ihres Geräts herunter oder stellen sie über eine SD-Karte zur Verfügung. Öffnen Sie die Datei in dem entsprechenden Verzeichnis.

8. Klicken Sie auf „OK“, um die Installation des mGuard-Maschinenzertifikats zu beenden.

► Das installierte Zertifikat erscheint in der Zertifikate-Liste des Anwenders (Einstellungen >> Gerätesicherheit >> Andere Sicherheitseinstellungen >> Benutzerzertifikate).

6.3 VPN-Verbindungen konfigurieren

6.3.1 mGuard konfigurieren

Die IPsec-VPN-Verbindung zwischen Android-Client und mGuard wird über die Erweiterung „XAuth/Mode Config“ hergestellt.

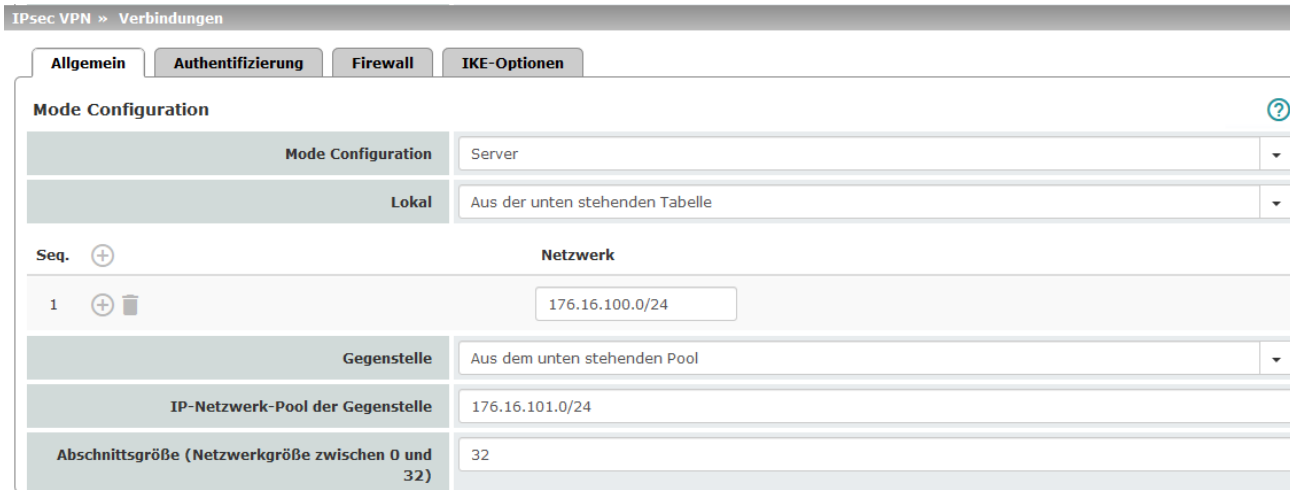


Bild 6-2 mGuard VPN-Konfiguration – Mode Configuration

6.3.1.1 Registerkarte „Allgemein“

Zur Konfiguration einer VPN-Verbindung zum Android-Client auf dem mGuard gehen Sie wie folgt vor:

1. Wählen Sie **IPsec VPN >> Verbindungen >> Allgemein**.
2. Klicken Sie auf das Icon ⊕, um eine neue Tabellenzeile zu erstellen.
3. Klicken Sie auf das Icon ✎.
   ► Die Registerkarte „**Allgemein**“ erscheint.
4. Geben Sie einen beschreibenden Namen für die Verbindung ein, und ändern Sie optional weitere Einstellungen.

   Überprüfen Sie, ob das Eingabefeld „Adresse des VPN-Gateways der Gegenstelle“ den Wert „**%any**“ enthält und „Verbindungsinitiierung“ auf „**Warte**“ gesetzt ist (Standardwerte).

5. **Mode Configuration**: Wählen Sie die Option „**Server**“.
6. **Lokal**: Geben Sie alle lokalen Netzwerke (1 oder mehrere) auf Server-Seite (mGuard) ein, auf die über die VPN-Verbindung durch den Android-Client zugegriffen werden soll.
   – **Fest**: Das *„Lokale IP-Netzwerk“* muss auf 0.0.0.0/0 gesetzt werden. In diesem Fall wird der gesamte Datenverkehr vom Android-Client über die VPN-Verbindung übertragen.

– **Aus der unten stehenden Tabelle**: Nur der Datenverkehr zu den in der *unten stehenden Tabelle* aufgelisteten Netzwerken wird über die VPN-Verbindung übertragen.

Bei Android-Clients wird die Funktion „*Aus der unten stehenden Tabelle*“ nicht vollständig unterstützt. **Datenverkehr** von Android-Clients zu Netzwerken, die nicht in der *unten stehenden Tabelle* definiert sind, **wird blockiert!**

7. **Gegenstelle**: Definieren Sie den Netzwerk-Pool (**Aus dem unten stehenden Pool**), aus dem der mGuard einen variablen Abschnitt (**Abschnittsgröße**) zur Nutzung durch das Netzwerk des Remote-Clients zuweist.

6.3.1.2 Registerkarte „Authentifizierung“

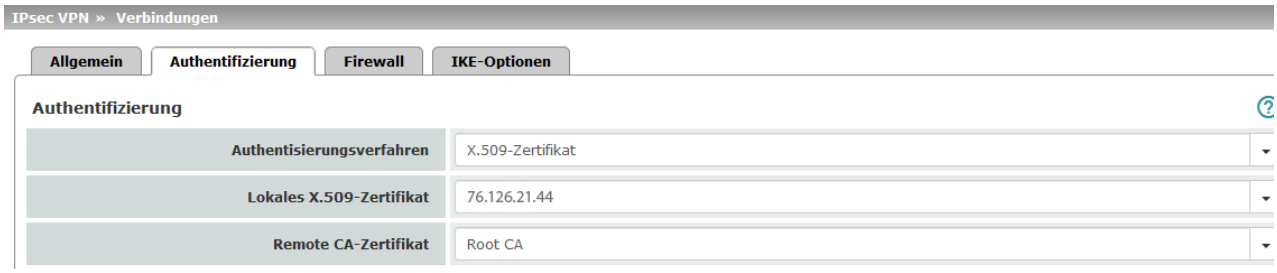


Bild 6-3 mGuard VPN-Konfiguration – Authentifizierung

Die VPN-Verbindung zwischen einem Android-Client und dem mGuard muss durch X.509-Zertifikate autorisiert werden, die auf den entsprechenden Geräten installiert werden müssen (siehe „Zertifikate verwalten“ auf Seite 139).

Um der VPN-Verbindung die erforderlichen Zertifikate zuzuweisen, gehen Sie wie folgt vor:

1. Wählen Sie **IPsec VPN >> Verbindungen**.
2. Bearbeiten Sie die gewünschte VPN-Verbindung (Registerkarte „Authentifizierung“).
3. Wählen Sie „**Authentisierungsverfahren**: X.509 Certificate“.
4. Wählen Sie als *„Lokales X.509-Zertifikat“* das **mGuard-Maschinenzertifikat**.

   Das lokale Zertifikat muss mit dem CA-Zertifikat signiert worden sein, das auf dem Android-Client installiert wurde.

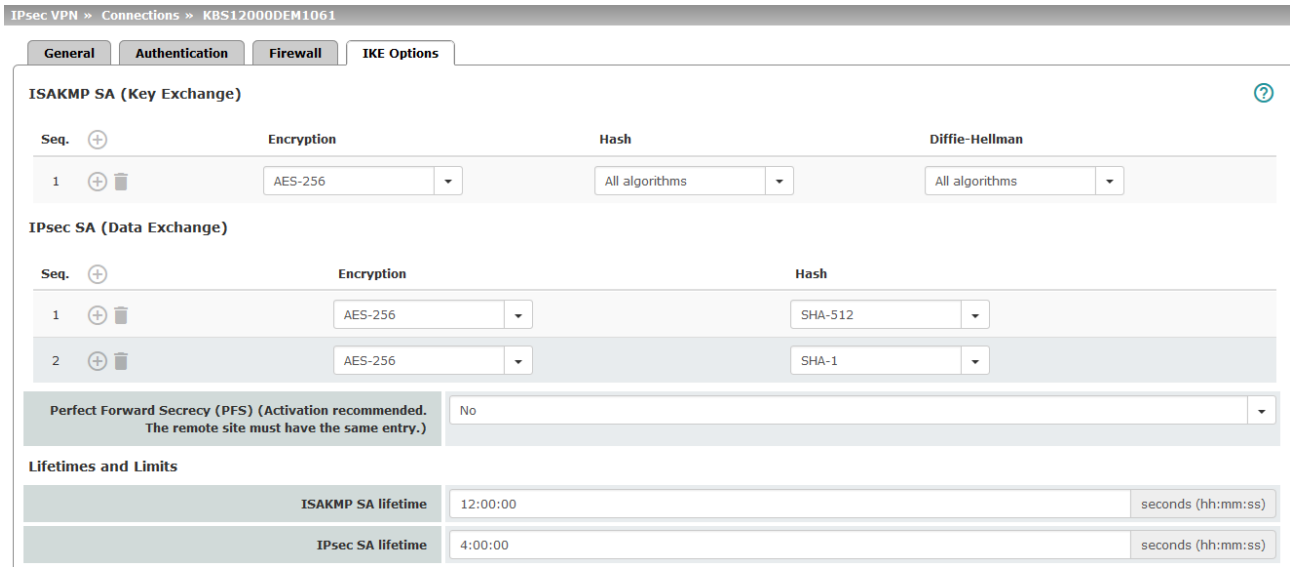
5. Wählen Sie als *„Remote CA-Zertifikat“* den Namen des CA-Zertifikats das zum Signieren des **Android-Client-Zertifikat** verwendet wurde.
6. Klicken Sie auf auf das Icon , um die Einstellungen zu speichern.
   ► Die VPN-Verbindung wird nach einer Initialisierung durch den Client hergestellt.

6.3.1.3 Registerkarte „Firewall“

Die VPN-Firewall beschränkt den Zugriff über den VPN-Tunnel. Sie können die VPN-Firewall bei Bedarf konfigurieren.

In der werkseitigen Voreinstellung wird **jeglicher eingehender** und **ausgehender** Datenverkehr zugelassen**.**

6.3.1.4 Registerkarte „IKE-Optionen“



Die werkseitig voreingestellten IKE-Optionen müssen geändert werden:

1. Wählen Sie **IPsec VPN >> Verbindungen**.
2. Bearbeiten Sie die gewünschte VPN-Verbindung (Registerkarte „IKE-Optionen“).
3. Konfigurieren Sie die folgenden Einstellungen (und behalten Sie bei allen anderen Einstellungen die werkseitige Voreinstellung bei).

ISAKMP-SA (Schlüsselaustausch)

- Verschlüsselung: AES-256
- Prüfsumme: Alle Algorithmen
- Diffie-Hellman: Alle Algorithmen

IPsec-SA (Datenaustausch)

- Klicken Sie auf das Icon ⊕, um zwei Tabellenzeilen zu erzeugen und die folgenden Einstellungen zu verwenden:
  - (Zeile 1) Encryption: AES-256 | Hash: SHA-512
  - (Zeile 2) Encryption: AES-256 | Hash: SHA-1

Perfect Forward Secrecy (PFS)

- Die PFS muss deaktiviert werden.

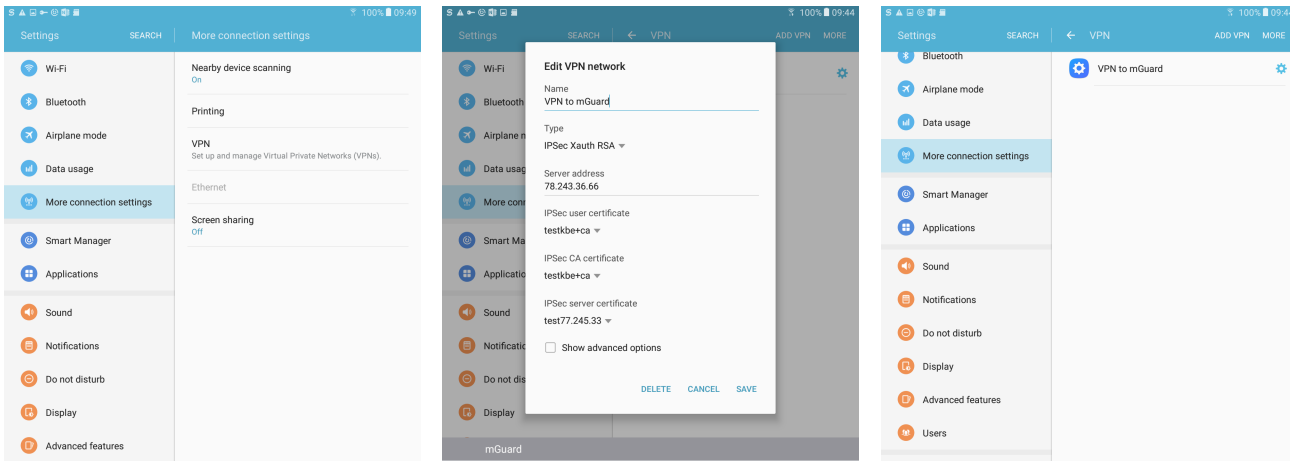
ISAKMP-SA-Lebensdauer

- 12:00:00 (hh:mm:ss)

IPsec-SA-Lebensdauer

- 04:00:00 (hh:mm:ss)

6.3.2 Android-Client konfigurieren



Um eine IPsec-VPN-Verbindung auf dem Android-Client zu konfigurieren, gehen Sie wie folgt vor:

1. Wählen Sie das „Einstellungen >> Weitere Verbindungseinstellungen >> VPN“.
2. Klicken Sie auf „VPN HINZUFÜGEN “ oder „+“.
   ► Das Fenster „VPN hinzufügen“ erscheint.
3. Konfigurieren Sie folgende Einstellungen:
   – *Name*: Ein beschreibender Name für die Verbindung
   – *Typ*: IPSec Xauth RSA
   – *Server-Adresse*: Die externe IP-Adresse oder der DNS-Name des mGuard-Servers
   – *IPSec-Benutzerzertifikat*: Wählen Sie den Namen, den Sie dem Android-Client-Zertifikat aus der PKCS#12-Datei zugewiesen haben.
   – *IPSec-CA-Zertifikate*: Wählen Sie den Namen, den Sie dem Android-Client-Zertifikat aus der PKCS#12-Datei zugewiesen haben.
   – *IPSec-Serverzertifikat*: Wählen Sie den Namen, den Sie dem mGuard-Maschinenzertifikat des mGuard-Servers (VPN-Gateway) zugewiesen haben.
4. Klicken Sie auf „SPEICHERN“, um die Konfiguration zu speichern.
   ► Die VPN-Verbindung ist nun gespeichert und kann gestartet werden.

6.4 VPN-Verbindungen auf dem Android-Client starten

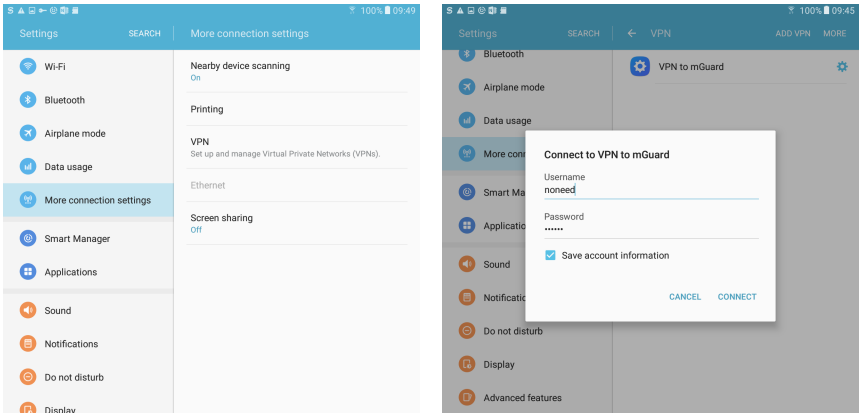


Bild 6-4 VPN-Verbindung auf dem Android-Client starten

Zum Starten einer IPsec-VPN-Verbindung auf dem Android-Client gehen Sie wie folgt vor:

1. Wählen Sie „Einstellungen >> Weitere Verbindungseinstellungen >> VPN“.
2. Klicken Sie auf den Namen der entsprechenden VPN-Verbindung.
   ► Das Fenster „Mit <Verbindungsname> verbinden“ erscheint.

Benutzername und Passwort für XAuth werden durch den mGuard ignoriert. Geben Sie eine kurze, beliebige Zeichenfolge ein, und speichern Sie die Kontoinformationen.

3. Klicken Sie auf „VERBINDEN“, um die Verbindung herzustellen.
   ► Die VPN-Verbindung wird hergestellt, und der Status ändert sich von „Nicht verbunden “ zu „Verbinden...“ und anschließend zu „Verbunden“.

Wenn die Verbindung fehlschlägt, klicken Sie auf das „Zahnrad“-Icon der VPN-Verbindung, um die Konfiguration auf Fehler oder den Status Ihrer Internetverbindung zu überprüfen.

6.5 VPN-Verbindungen auf dem mGuard überprüfen

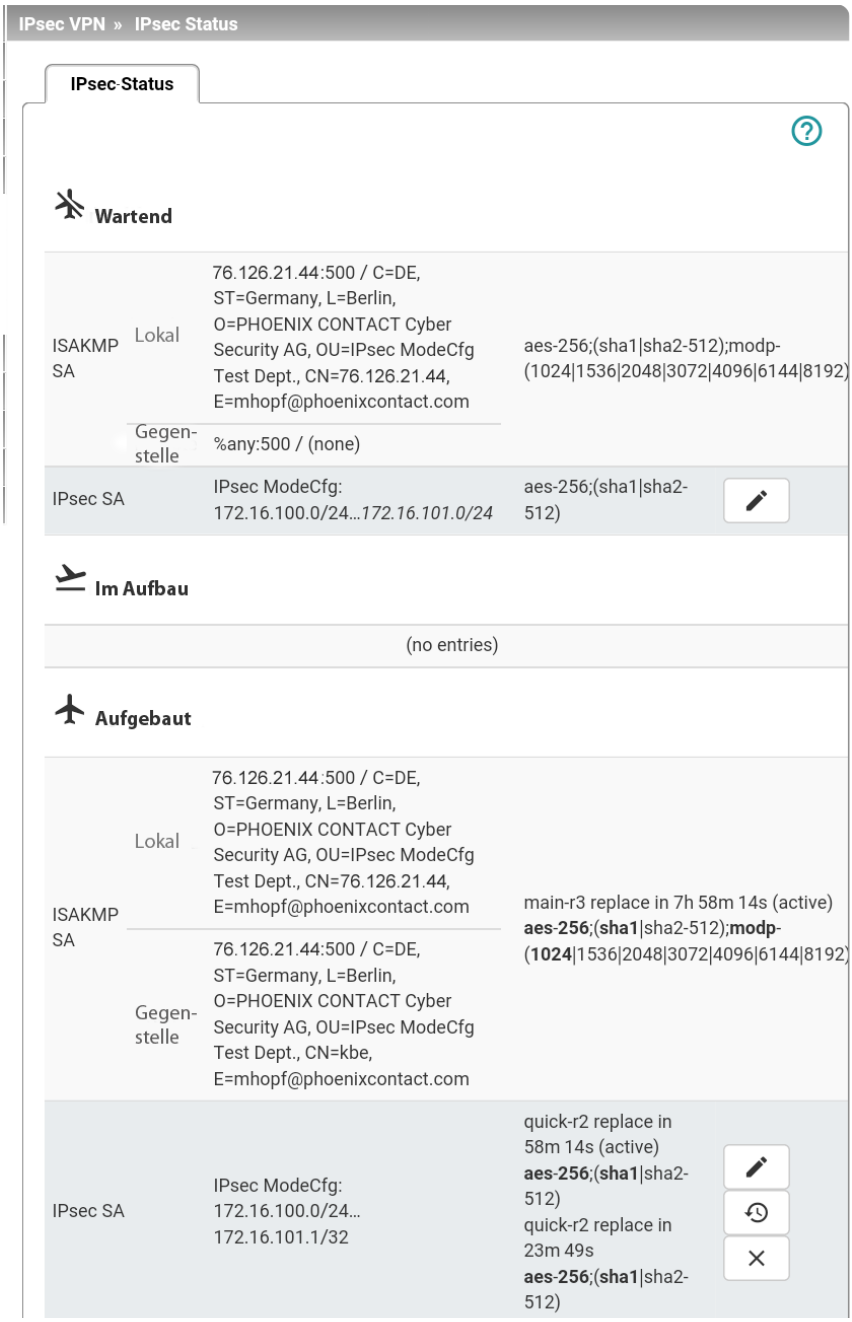


Bild 6-5 IPsec-VPN-Status

Zur Überprüfung des Status einer IPsec-VPN-Verbindung gehen Sie wie folgt vor:

- Wählen Sie **IPsec VPN >> IPsec-Status**.
  - ► Eine hergestellte IPsec-VPN-Verbindung wird im Bereich „Aufgebaut“ angezeigt.

7 mGuard-Konfiguration mittels Pull-Konfiguration aktualisieren

Dokument-ID: 108398_de_01
Dokument-Bezeichnung: AH DE MGUARD PULLCONFIG

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument wird beschrieben, wie Sie die Pull-Konfiguration (*pull configuration*) für Ihr mGuard-Gerät durchführen. Des Weiteren wird beschrieben, wie Sie ein Pull-Config-Feedback aus den Server-Logs beziehen können.

7.1 Einleitung

Ein mGuard-Gerät kann sich automatisch neue Konfigurationsprofile von einem Konfigurations-Pull-Server „holen“ (*pull configuration*), wenn dort entsprechende Profile (mit der Dateiendung *.atv*) abgelegt wurden.

Neue Konfigurationen können mittels mGuard device manager (mdm / FL MGUARD DM) erstellt und auf dem Pull-Server abgelegt werden. Auf dem mGuard-Gerät kann konfiguriert werden, in welchen Zeitabständen neue Konfigurationen vom Pull-Server „geholt“ werden.

7.2 Pull-Konfiguration auf dem mGuard-Gerät konfigurieren

Um die Pull-Konfiguration auf dem mGuard-Gerät zu konfigurieren, gehen Sie wie folgt vor:

1. Melden Sie sich auf der Web-Oberfläche des mGuard-Geräts an.
2. Gehen Sie zu **Verwaltung >> Zentrale Verwaltung** (siehe auch mGuard-Firmwarehandbuch).
3. Legen Sie einen Zeitplan fest, wann das mGuard-Gerät einen Anfrage an den Pull-Server senden soll (*pull request*).
4. Nehmen Sie gegebenenfalls weitere Einstellungen vor.

Das mGuard-Gerät wird zu den definierten Zeitpunkten versuchen, neue Konfiguration vom Pull-Server zu „holen“.

7.3 Pull-Konfiguration mittels mdm durchführen

Eine Methode, um die Konfigurationen oder die Firmwareversion eines mGuard-Geräts mithilfe des mGuard device managers (mdm / FL MGUARD DM) zu aktualisieren, ist die Pull-Konfiguration (*pull configuration*).

Die in mdm erstellten Konfigurationen werden dazu zunächst auf den Pull-Server exportiert und später vom mGuard-Gerät „geholt“ bzw. auf das Gerät hochgeladen (siehe auch mdm-Softwarehandbuch).

Das mGuard-Gerät sendet bei jeder Anfrage an den Pull-Server den Status seiner Konfiguration als HTTP(S)-Request. Um dem mdm-Server den Konfigurationsstatus des mGuard-Geräts mitzuteilen, versendet der Pull-Server wiederum SYSLOG-Meldungen an den mdm-Server (*pull feedback*).

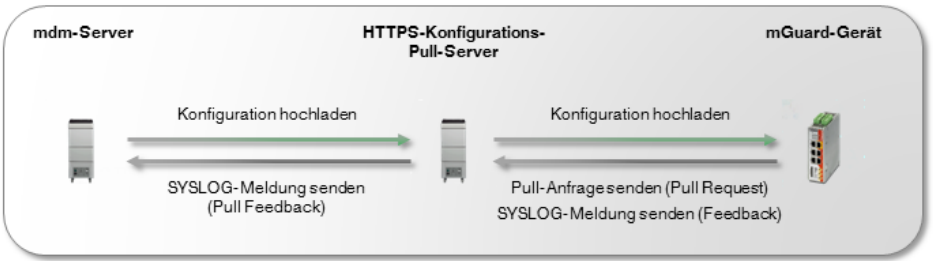


Bild 7-1 Pull-Konfiguration mittels mdm durchführen

Konfigurieren Sie den mdm-Server so, dass er SYSLOG-Meldungen vom HTTPS-Pull-Server empfangen kann.

Achten Sie darauf, dass die Netzwerkverbindung zwischen dem HTTPS-Pull-Server und dem mdm-Server sowie zwischen dem HTTPS-Pull-Server und dem mGuard-Gerät nicht durch eine Firewall oder einen NAT-Router blockiert wird.

7.4 Pull-Config-Feedback aus Server-Logs beziehen

Für den Fall, dass eine Kommunikation vom Konfigurations-Pull-Server zum mdm-Server aufgrund von Firewall- oder NAT-Einstellungen nicht möglich ist, kann der Status eines Konfigurations-Pulls (*configuration pull*) auch aus den Log-Einträgen des Pull-Servers ermittelt werden.

Holt ein mGuard-Gerät eine neue Konfiguration vom Pull-Server, werden bestimmte Parameter (z. B. der Status der Aktualisierung) als Pull-Config-Feedback (*pull feedback*) in Form einer URL vom mGuard-Gerät an den Pull-Server zurückgegeben (siehe nachfolgende Beispiele und Tabelle 7-1). Durch eine Auswertung der Pull-Server-Logs kann überprüft werden, ob ein Konfigurations-Pull erfolgreich war.

Beispiele

1. Konfiguration erfolgreich angewendet:

"GET
//atv//00000001.atv?**a**=8.6.0.default&**b**=N205414313033131033abebcecfccecefcc&**c**=2031420608&**d**=e2adce0a1edd2c72e1910303f9d86925&**e**=0&**f**=-&**g**=-&**k**=-&**i**=0&**j**=0&**z**=1670 HTTP/1.1"

2. Ungültige Konfiguration (aufgrund fehlender Lizenz für eine aktivierte Funktion**):**

"GET
//atv//00000001.atv?**a**=8.6.0.default&**b**=N205414313033131033abebcecfccecefcc&**c**=20
31420608&**d**=e2adce0a1edd2c72e1910303f9d86925&**e**=5&**f**=-&**g**=-&**k**=-
&**i**=0&**j**=0&**z**=71de HTTP/1.1"

Tabelle 7-1 Liste der HTTP(S)-Request-Parameter, die vom mGuard device mananger (mdm) ausgewertet werden

Parameter	Bedeutung	Status	Beschreibung
a	mGuard-Firmwareversion		Aktuell auf dem mGuard-Gerät installierte Firmwareversion
b	mGuard-Flash-ID		Flash-ID des mGuard-Geräts
c	mGuard-Seriennummer		Seriennummer des mGuard-Geräts
d	md5-Hash der mGuard-Konfiguration		md5-Hashwert der aktuell auf dem mGuard-Gerät angewendeten Konfiguration
e	Status der Aktualisierung der mGuard-Konfiguration (Konfiguration-Pull / *configuration pull*)	**0**	Die Konfiguration auf dem mGuard-Gerät wurde erfolgreich aktualisiert (upgedatet).
		1	Keine Aktualisierung: Die Konfiguration auf dem mGuard-Gerät befindet sich bereits auf dem aktuellen Stand.
e		**2**	Keine Aktualisierung: Die neue Konfiguration konnte auf dem mGuard-Gerät nicht angewendet werden. Die vorherige Konfiguration wurde wiederhergestellt (*rollback*).
		3	Keine Aktualisierung: Die neue Konfiguration wird vom mGuard geblockt, weil sie bei einem vorherigen Anwendungsversuch zu einer Wiederherstellung (*rollback*) führte.
		4	Keine Aktualisierung: Die alte Konfiguration konnte für eine möglicherweise später notwendige Wiederherstellung (*rollback*) nicht auf dem mGuard-Gerät zwischengespeichert werden.
		5	Keine Aktualisierung: Die Konfiguration, mit der das mGuard-Gerät aktualisiert werden sollte, ist ungültig.
		-	Keine Aktualisierung: Die Konfiguration auf dem Gerät sollte nicht aktualisiert werden.
f	Status des mGuard-Firmware-Updates	**0**	Das Firmware-Update auf dem mGuard-Gerät wurde erfolgreich durchgeführt.

Tabelle 7-1 Liste der HTTP(S)-Request-Parameter, die vom mGuard device mananger (mdm) ausgewertet werden

		-	Keine Aktualisierung: Ein Firmware-Update sollte auf dem Gerät nicht durchgeführt werden.
		beliebiges anderes Zeichen	Keine Aktualisierung: Firmware-Update fehlgeschlagen
g	Status des Lizenz-Downloads	**0**	Eine oder mehrere Lizenzen wurde erfolgreich auf dem mGuard-Gerät installiert.
		-	Es sollte keine Lizenz auf dem Gerät installiert werden.
		beliebiges anderes Zeichen	Installation der Lizenz fehlgeschlagen
k	Status der Schlüsselerneuerung (*key renewal*)	**0**	Die Schlüssel (*ssh* und *https*) auf dem mGuard-Gerät wurden erfolgreich erneuert.
		1	Die Schlüsselerneuerung ist fehlgeschlagen.
		2	Keine Schlüsselerneuerung durchgeführt Eine Erneuerung wird aber empfohlen, da der aktuelle Schlüssel eventuell nicht ausreichend sicher ist.
		-	Keine Schlüsselerneuerung durchgeführt

Weitere Parameter (derzeit nicht zugesichert)

- **h** = Geräte-Typ-Informationen, derzeit nur gesetzt für NAT-Router-Geräte. Auf anderen Geräten wird „h“ nicht übermittelt.
- **i** = Redundanz: Status des Passworts für die Verfügbarkeits-Prüfung (*availability check*).
- **j** = Redundanz: Status des Passworts für die Verschlüsselung des Netzwerkverkehrs zwischen synchronisierten mGuard-Geräten.
- **z** = 4 MSB (*Most Significant Bytes*) des md5-Hashwertes der Meta-Info – ohne das führende „?“ und das finale „&“ – aber mit einem angehängten Zeilenvorschubzeichen (0x0A).

8 Einen neuen Bootloader auf mGuard-Geräten installieren

Dokument-ID: 108042_de_02
Dokument-Bezeichnung: AH DE MGUARD BOOTLOADER

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

8.1 Einleitung

Durch die zunehmende Verkleinerung der Hardware-Strukturen bei Speicherbausteinen, ist es üblich, dass einige Speicherzellen nicht voll funktionsfähig sind und im Laufe der Zeit weitere Speicherzellen ihre Funktion einstellen. Diese Verringerung der Speicherkapazität wird durch Mehrkapazität bei der Produktion ausgeglichen, sodass im Laufe der Nutzungsdauer die gewünschte Kapazität nicht unterschritten wird.

Die mGuard-Geräte verfügen über Routinen, um mit den defekten Speicherzellen umzugehen. Diese Routinen werden mit der Installation eines neuen Bootloaders optimiert.

Falls Sie kein Update der Firmware-Version wünschen, können Sie nach dem Update des Bootloaders das Gerät auf die von Ihnen gewünschte Version downgraden. Die neu installierte Version des Bootloaders bleibt nach dem Downgrade der Firmware-Version erhalten. Phoenix Contact hingegen empfiehlt immer den Einsatz der aktuellen Firmware.

Geräte, die mit einer mGuard-Firmware-Version ab 8.7.0 produziert wurden, können nicht auf eine Firmwareversion < 8.7.0 geflasht werden (downgrade).

Mit einer aktuellen Firmware-Version ist eine optimierte Version des Bootloaders auf dem Gerät vorhanden. Bitte beachten Sie die Hinweise zum Firmware-Update im Handbuch der jeweiligen Geräte.

8.2 Bootloader prüfen

Falls Sie ein mGuard-Gerät haben, das nicht mehr bootet und Sie überprüfen wollen, ob der Bootloader die Ursache ist, nehmen Sie bitte die folgenden Schritte vor, um den Bootloader abzudaten.

1. Trennen Sie das Gerät von der Versorgungsspannung.
2. Verwenden Sie ein Tool zur Kommunikation über die serielle Schnittstelle auf Ihrem PC, z. B. „Putty“.
3. Stellen Sie die serielle Verbindung zwischen PC und mGuard-Gerät her.
4. Starten Sie das mGuard-Gerät durch anlegen der Versorgungsspannung. Das Gerät versucht zu booten.

Falls die folgende Fehlermeldung im Terminalfenster von Ihrem Tool erscheint, ist ein Update des Bootloaders erforderlich:

U-Boot 2009.11 (Dec 13 2013 - 08:34:06) MPC83XX

Neue Bootloader-Versionen werden ab den **Versionen 7.6.8** und **8.1.4** auf die mGuard-Geräte gebracht.

9 Das CGI-Interface verwenden

Dokument-ID: 108416_de_01
Dokument-Bezeichnung: AH DE MGUARD CGI INTERFACE

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument wird die Verwendung des CGI-Interface des mGuard-Geräts (eine zusätzliche HTTPS-Schnittstelle) beschrieben.

9.1 Einleitung

Die zusätzlichen HTTPS-Schnittstellen sind als CGI-Skripte (**C**ommon **G**ateway **I**nterface) umgesetzt und bieten folgende Merkmale und Funktionen:

Einige Befehle werden synchron ausgeführt: ihr Rückgabecode gibt Auskunft darüber, ob der Befehl erfolgreich ausgeführt wurde oder nicht. Beim Aufbau einer VPN-Verbindung wird der Fortschritt für jeden wichtigen Schritt angezeigt.

nph-vpn.cgi / nph-diag.cgi

- Zugriff von einem konventionellen HTTPS-Client.
- Aktivierung/Deaktivierung einer VPN-Verbindung.
- Ermittlung des Verbindungsstatus einer VPN-Verbindung.
- Ausführung eines "Download-Tests", um zu überprüfen, ob der mGuard die Konfigurationsdatei von dem angegebenen HTTPS-Server herunterladen kann.
- Ermittlung der Firmware-Version und Hardware-Revision des mGuards.
- Herunterladen eines Support-*Snapshots*.

nph-action.cgi / nph-status.cgi

Die CGI-Interfaces *nph-action.cgi* und *nph-status.cgi* bieten einen erweiterten Funktionsumfang (siehe Kapitel 9.6, "Interface nph.action.cgi" und Kapitel 9.7, "Interface nph.status.cgi").

9.2 Verwendung

Die CGI-Skripte auf dem mGuard können über HTTPS über die gleiche IP-Adresse und den gleichen Port erreicht werden, auf denen die Weboberfläche verfügbar ist. Sie müssen nur eine andere URL verwenden. Jeder Zugriff auf ein CGI-Skript führt einen bestimmten Befehl aus. Jeder Befehl antwortet mit einem UTF-8-Text im *Body* der HTTP-Antwort. Die Ausnahme bildet der Befehl *snapshot*, der binäre Daten zurückgibt. Einige Fehlerzustände werden im SSL in der jeweiligen HTTP-Antwort angezeigt. Der HTTP-Statuscode 401, zum Beispiel, zeigt eine fehlgeschlagene Autorisierung an.

9.2.1 Verfügbare Befehle

nph-vpn.cgi / nph-diag.cgi

Tabelle 9-1 Über CGI-Skripte verfügbare Befehle

CGI-Skript	Befehl	Zweck
nph-vpn.cgi	*synup*	Aktivierung einer VPN-Verbindung (synchroner Befehl)
	syndown	Deaktivierung einer VPN-Verbindung (synchroner Befehl)
	synstat	Bestimmung des Status einer VPN-Verbindung (synchroner Befehl)
	sysinfo	Ermittlung der Firmware-Version und Hardware-Revision auf dem mGuard
	up	Aktivierung einer VPN-Verbindung (asynchroner Befehl)
	down	Deaktivierung einer VPN-Verbindung (asynchroner Befehl)
	status	Bestimmung des Status einer VPN-Verbindung (asynchroner Befehl)
	clear	Löscht die Instanz einer VPN-Verbindung
nph-diag.cgi	*testpull*	Veranlasst einen "Download-Test" von einem HTTPS-Server
	snapshot	Herunterladen eines *Snapshots* vom mGuard

nph-action.cgi / nph-status.cgi

Für die Befehle, die über die CGI-Skripte *nph-action.cgi* und *nph-status.cgi* verfügbar sind, siehe Kapitel 9.6, "Interface nph.action.cgi" und Kapitel 9.7, "Interface nph.status.cgi".

9.2.2 Befehlssyntax

Die Verwendung des Kommandozeilen-Tools *wget* funktioniert nur im Zusammenspiel mit mGuard-Firmwareversionen < 8.4.0. Ab mGuard-Firmwareversion 8.4.0 kann das Kommandozeilen-Tool *curl* verwendet werden (Parameter und Optionen abweichend!).

Beispiel:

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"

Die Option --no-check-certificate (*wget*) bzw. --insecure (*curl*) sorgt dafür, dass das HTTPS-Zertifikat des mGuards nicht weiter geprüft wird.

Die Befehlszeile hat bei Verwendung des Dienstprogrammes *wget* folgende Syntax:

*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***'**

Bei Verwendung des Dienstprogrammes *curl* hat die Befehlszeile folgende Syntax:

*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***'**

Tabelle 9-2 Befehlssyntax

wget […] oder curl […]	Dienstprogramm zum Erstellen der HTTPS-Anfrage und der benötigten Argumente. Beachten Sie bitte das Handbuch zum Dienstprogramm.
MGUARD	IP-Adresse und Portnummer, auf denen der mGuard auf eingehende HTTPS-Anfragen horcht. Der IP-Adresse können Benutzername und Passwort vorangestellt werden. **[<Benutzername>:<Passwort>@]<IP-Adresse>[:<Port>]** Beispiel: admin:mGuard@192.168.1.254:443
CGI-SCRIPT	Name des aufzurufenden CGI-Skriptes, entweder *nph-vpn.cgi* oder *nph-diag.cgi*.
COMMAND	Auszuführender Befehl, auf den folgenden Seiten beschrieben.
VPN_NAME	Name der VPN-Verbindung, die aktiviert oder deaktiviert oder deren Status erfasst werden soll. Befehle: *synup, syndown, synstat, up, down, status*.
LNET_RNET	Lokales und Remote-VPN-Netzwerk. Befehle: status, clear.

Beispiele

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'

– Unter Linux und anderen UNIX-Betriebssystemen beginnt und endet der mit https:// beginnende String mit einem einfachen Anführungszeichen (‘). Unter anderen Betriebssystemen wie Windows können doppelte Anführungszeichen (") verwendet werden.
– Wenn der VPN-Name Sonderzeichen wie das Leerzeichen enthält, müssen diese entsprechend den URL-Kodierregeln in Anführungszeichen gesetzt werden.
– Beinhaltet die URL wie in den oben genannten Beispielen das Passwort, müssen Sie sich darüber im Klaren sein, dass ein Eindringling das Passwort aus der Prozessliste oder dem Verlauf der Befehlszeile auslesen kann. Es ist ratsam, den Benutzer mit dem Benutzernamen "*user*" zu verwenden. Dieser Benutzer hat die Rechte, eine VPN-Verbindung zu aktivieren oder deaktivieren oder ihren Status zu ermitteln, indem er die in diesem Dokument beschriebenen CGI-Skripte aufruft. Dieser Benutzer hat aber nicht das Recht, sich über HTTPS oder SSH auf dem mGuard einzuloggen oder Konfigurationsänderungen vorzunehmen.

9.2.3 Zugriffsrechte

Tabelle 9-3 Zugriffsrechte

Befehl	Benutzer				
	root	admin	user	netadmin	audit
up, down, synup, syndown	x	x	x	-	-
status, synstat, sysinfo	x	x	x	x	x
status & channel, clear (central VPN gateway)	x	x	-	-	-
testpull, snapshot	x	x	-	-	-

9.3 Voraussetzungen und Einschränkungen

Beim Ausführen der Skripte nph-vpn.cgi, nph-diag.cgi, nph-status.cgi und nph-action.cgi, dürfen nur folgende Zeichen für Benutzernamen, Passwörter und andere definierte Namen (z.B. die Benennung einer VPN-Verbindung) verwendet werden:

– Buchstaben: A - Z, a - z
– Ziffern: 0 - 9
– Sonderzeichen: - . _ ~

Andere Sonderzeichen, z. B. das Leerzeichen oder das Fragezeichen, müssen entsprechend codiert werden (URL-Kodierung).

Die Verwendung des Kommandozeilen-Tools *wget* funktioniert nur im Zusammenspiel mit mGuard-Firmwareversionen < 8.4.0. Ab mGuard-Firmwareversion 8.4.0 kann das Kommandozeilen-Tool *curl* verwendet werden (Parameter und Optionen abweichend!).

Beispiel:

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"

Die Option --no-check-certificate (*wget*) bzw. --insecure (*curl*) sorgt dafür, dass das HTTPS-Zertifikat des mGuards nicht weiter geprüft wird.

9.3.1 Voraussetzungen

Die Befehle *synup*, *syndown*, *up* und *down* können nur für das Auslösen einer VPN-Verbindung verwendet werden, wenn diese wie folgt konfiguriert ist:

1. Die VPN-Verbindung ist deaktiviert (Menü **IPsec VPN >> Verbindungen**).
2. Mindestens ein Tunnel der VPN-Verbindung ist aktiviert (Menü **VPN >> Verbindungen**, Registerkarte *Allgemein*, Abschnitt *Transport- und Tunneleinstellungen*).
3. Die Verbindungsinitialisierung muss auf *Initiiere* oder *Initiiere bei Datenverkehr* gestellt sein (Menü **VPN >> Verbindungen**, Registerkarte *Allgemein*, Abschnitt *Optionen*).

9.3.2 Einschränkungen

– Befehle, die über das CGI-Interface ausgeführt werden, können mit anderen Aktivitäten des mGuard sowie mit anderen über andere Schnittstellen ausgeführten Befehlen kollidieren.
– Eine VPN-Verbindung sollte entweder durch CMD-Kontakt oder über das CGI-Interface ausgelöst werden. Eine Kombination aus beiden Varianten wird nicht unterstützt.
– Die Befehle *synup*, *syndown*, *up* und *down* werden nicht für VPN-Verbindungen unterstützt, die auf eingehende VPN-Verbindungen warten (*Verbindungsinitiierung* = *Warte*).
– Das CGI sollte nicht während eines Firmware-Updates oder eines Neustarts des mGuard verwendet werden.

9.4 Interface nph-vpn.cgi

9.4.1 cmd=(up|down), name=<VPN-Name>

Diese Befehle aktivieren oder deaktivieren die angegebene VPN-Verbindung. Der Name der VPN-Verbindung muss mit dem Parameter *name* angegeben werden.

Aufgrund der asynchronen Ausführung dieser Befehle gibt der Rückgabewert keine Informationen über den Status der VPN-Verbindung. Daher sollte diesen Befehlen eine Ausführung des Befehls Status folgen, um den Status der VPN-Verbindung zu bestimmen.

Beispiele:

*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'*

Diese Befehle geben einen der folgenden Werte im HTTP-Antworttext zurück:

Rückgabewert	Bedeutung
unknown	Eine VPN-Verbindung mit dem angegebenen Namen existiert nicht.
void	Die VPN-Verbindung ist inaktiv, entweder aufgrund eines Fehlers oder weil sie nicht mithilfe des CGI-Interface aktiviert wurde.
ready	Die VPN-Verbindung ist bereit, selbst Tunnel aufzubauen oder eingehende Anfragen zum Tunnelaufbau zu erlauben.
active	Mindestens ein VPN-Tunnel der VPN-Verbindung ist für die Verbindung aufgebaut.

9.4.2 cmd=status, [name=(<VPN-Name>|*)]

Abhängig vom Parameter *name*, ermittelt dieser Befehl entweder den Status

1. einer angegebenen VPN-Verbindung (name=[VPN-Name]) oder
2. den aller konfigurierten VPN-Verbindungen (name=*), oder
3. den aller aktivierten oder über *synup* aktivierten VPN-Verbindungen (Parameter *name* nicht angegeben) samt zusätzlicher Informationen.

Im Falle von (1) oder (2) gibt der Befehl einen der folgenden Werte zurück:

Rückgabewert	Bedeutung
unknown	Eine VPN-Verbindung mit dem angegebenen Namen existiert nicht.
void	Die VPN-Verbindung ist inaktiv, entweder aufgrund eines Fehlers oder weil sie nicht mithilfe des CGI-Interface aktiviert wurde.
ready	Die VPN-Verbindung ist bereit, selbst Tunnel aufzubauen oder eingehende Anfragen zum Tunnelaufbau zu erlauben.
active	Mindestens ein VPN-Tunnel der VPN-Verbindung ist für die Verbindung aufgebaut.

9.4.2.1 cmd=status, name=<VPN-Name>

Dieser Befehl ermittelt den Status der angegebenen VPN-Verbindung.

Beispiel:

*wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?***cmd=status***&name=Service1'*

Rückgabewert
active

9.4.2.2 cmd=status, name=*

Dieser Befehl ermittelt den Status aller konfigurierten VPN-Verbindungen.

Beispiel:

*wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?***cmd=status***&name=*'*

Rückgabewert
Service 1: active
Service 2: void

9.4.2.3 cmd=status (ohne Parameter *name*)

Dieser Befehl ermittelt den Status aller aktivierten VPN-Verbindungen samt zusätzlicher Informationen.

Beispiel:

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=status'

(Parameter *name* nicht angegeben)

Rückgabewert	
fullname	Service1
name	MAI0003584192_1 instance
leftnet	192.168.1.0/24
leftgw	10.1.0.48
leftnatport	
leftid	O=Innominate, OU=Support, CN=mGuard 3
leftproto	
leftport	
rightnet	192.168.2.0/24
rightgw	77.245.33.67
rightnatport	
rightid	O=Innominate, OU=Support, CN=Central Gateway
rightproto	
rightport	

Rückgabewert	
isakmp	6
isakmp-txt	STATE_MAIN_I4 (ISAKMP-SA established)
isakmp-ltime	157s
isakmp-algo	3DES_CBC_192-MD5-MODP1536
ipsec	7
ipsec-txt	STATE_QUICK_I2 (sent QI2, IPsec-SA aufgebaut)
ipsec-ltime	25526s
ipsec-algo	3DES_0-HMAC_MD5

Der Status der VPN-Verbindung *Service2* wird in diesem Beispiel nicht zurückgegeben, da diese Verbindung nicht aktiviert ist.

9.4.3 cmd=(synup|synstat|syndown), name=<VPN-Name>

Diese Befehle aktivieren, deaktivieren oder ermitteln den Status der angegebenen VPN-Verbindung. Anders als die Befehle *-up*, *-down* und *-status* werden diese Befehle synchron ausgeführt, weshalb der Vorgang zurückgegeben wird, sobald ein bestimmter Status erreicht wurde.

Das erste Zeichen der Antwort gibt an, ob der Vorgang erfolgreich ausgeführt wurde. Dem Rest der Antwortzeile können weitere Informationen entnommen werden. Der Antworttext besteht nur aus einer Zeile, außer beim Befehl *synup*, der eine VPN-Verbindung aufbaut. Für diesen Befehl enthält der Antworttext Fortschrittsmeldungen bezüglich des Aufbaus der VPN-Verbindung sowie eine finale Meldung mit dem Gesamtergebnis.

9.4.3.1 Format der Antwortmeldung

Jede Meldung hat das Format: <TYP> <CODE> <MESSAGE BODY>

TYP	Meldungstyp, ein Zeichen: P, R oder F: **P** – Fortschrittsmeldung (nur für den Befehl *synup*) **R** – Finale Meldung, Vorgang erfolgreich abgeschlossen **F** – Finale Meldung, Vorgang abgeschlossen mit Fehler
CODE	Maximal 12 Zeichen, eine Abkürzung dessen, was in diesem Schritt getan wurde (für Fortschrittsmeldungen) oder des Endergebnisses (für finale Meldungen). Bitte beachten Sie das nächste Kapitel.
MESSAGE BODY	Eine Folge von Textfeldern, abgegrenzt durch Leerzeichen. Jedes Feld besteht aus einem Kennzeichner und einem Wert, getrennt durch ein Gleichheitszeichen. Zu Beginn des MESSAGE BODY steht oft das Feld "uptime=..." oder "tstamp=...". “uptime=” gibt die Betriebszeit des mGuard in Sekunden mit Nachkommastellen seit der letzten Inbetriebnahme an. “tstamp=” gibt das Datum und den Zeitpunkt an, zu der die Meldung generiert wurde.

9.4.3.2 Antwortcode

Die Antwort kann eine der folgenden Codes enthalten:

Antwortcode	Beschreibung
EAMBIGUOUS	Der angegebene Name der VPN-Verbindung war zweideutig, da mehrere VPN-Verbindungen den gleichen Namen haben.
EBUSY	Das gerufene GDI-Skript ist derzeit mit einer anderen Aufgabe beschäftigt oder ist aufgrund eines laufenden Firmware-Updates gesperrt.
ECONFPULL	Der Test-Download eines Konfigurationsprofils vom HTTPS-Servers ist fehlgeschlagen.
EINVAL	Der CGI-Befehl oder die Parameter enthalten Syntaxfehler.
EVLOOKUPGW	Der Hostname des Remote-VPN-Gateways konnte nicht in eine IP-Adresse aufgelöst werden.
EVLOOKUPROUT	Kein Pfad zur IP-Adresse des Remote-VPN-Gateways bekannt.
ENOENT	Das angegebene Objekt existiert nicht (z.B. existiert keine VPN-Verbindung mit dem angegebenen Namen).
ESYNVPN001	Die VPN-Verbindung wurde erfolgreich aufgebaut, wurde dann aber unterbrochen (z.B. aufgrund einer Netzwerkunterbrechung). Die Verbindung muss deaktiviert und neu aufgebaut werden. Verwenden Sie den Befehl *synstat*, um den Status der VPN-Verbindung zu ermitteln.
EVDIFFALG1	Während des Handshaking zu Beginn des Aufbaus der VPN-Verbindung (Negotiation von ISAKMP-SA) konnten sich die Geräte nicht auf die Stärke der Schlüssel oder die kryptographischen Algorithmen, die in der ersten Phase verwendet werden, einigen.
EVDIFFALG2	Während des Handshaking zu Beginn des Aufbaus der VPN-Verbindung (Negotiation von IPsec-SA) konnten sich die Geräte nicht auf die Stärke der Schlüssel oder die kryptographischen Algorithmen, die in der zweiten Phase verwendet werden, einigen.
EVIFDOWN	Die Netzwerkschnittstelle, über die die VPN-Verbindungen aufgebaut werden sollen, verfügt über keinen Uplink.
EVPEERNOENT1	Die Remote-VPN-Gegenstelle kennt keine VPN-Verbindung, die den Kriterien für die erste IKE-Phase (Negotiation von ISAKMP-SA) entspricht. Vermutlich ist die Konfiguration des mGuard oder der Gegenstelle nicht korrekt.
EVPEERNOENT2	Die Remote-VPN-Gegenstelle kennt keine VPN-Verbindung, die den Kriterien für die zweite IKE-Phase (Negotiation von IPsec-SA) entspricht. Vermutlich ist die Konfiguration des mGuard oder der Gegenstelle nicht korrekt.
EVTOUT1RESP	Der mGuard hat auf seine erste Meldung zum Aufbau der VPN-Verbindung keine Antwort der VPN-Gegenstelle erhalten.
EVTOUTWRESP	Der mGuard hat keine Antwort der Remote-VPN-Gegenstelle erhalten, nachdem diese auf mindestens eine Meldung geantwortet hatte.
OKCONFPULL	Der Test-Download eines Konfigurationsprofils vom HTTPS-Servers war erfolgreich.
OKVACT	Die VPN-Verbindung war beim Aufruf des Befehls *synup* bereits aufgebaut.
OKVDOWN	Die VPN-Verbindung wurde erfolgreich deaktiviert.
OKVNOTACT	Die VPN-Verbindung, die mit dem Befehl *syndown* deaktiviert werden sollte, war schon deaktiviert.
OKVST1	Der Status der angegebenen VPN-Verbindung wurde erfolgreich ermittelt.
OKVUP	Die VPN-Verbindung wurde erfolgreich aufgebaut.

9.4.3.3 cmd=synup

Dieser Befehl aktiviert eine VPN-Verbindung. Der Name der VPN-Verbindung muss mit dem Parameter *name* angegeben werden. Dieser Befehl wird synchron ausgeführt und gibt zurück, sobald ein bestimmter Status erreicht wurde. Der Antworttext enthält Fortschrittsmeldungen bezüglich des Aufbaus der VPN-Verbindung sowie eine finale Meldung mit dem Gesamtergebnis.

Beispiel: Aktivierung der VPN-Verbindung mit dem Namen Service

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synup&name=Service'

Antwort:

```
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.
```

Wenn der mGuard den Befehl *synup* ausführt, führt er folgende Schritte aus:

1. Auflösung des Namens des Remote-VPN-Gateways in eine IP-Adresse (falls erforderlich).
2. Bestimmung der Netzwerkschnittstelle, über die die VPN-Verbindung aufgebaut werden soll und ihrer Konnektivität.

Die Ergebnisse beider Schritte werden in den Zeilen *dnslookup* und *routeinfo* angezeigt. Nur wenn diese Schritte erfolgreich durchgeführt wurden, baut der mGuard die VPN-Verbindung weiter auf. Erhält der mGuard keine Antwort von der Remote-VPN-Gegenstelle, sendet er einen *IKE-Ping* um zu überprüfen, ob die Gegenstelle verfügbar ist, und gibt das Ergebnis aus.

Antwortmuster

Eine Antwort des Befehls *synup* besteht aus mehreren Fortschrittsmeldungen und einer finalen Meldung mit dem Gesamtergebnis. Folgende Struktur zeigt den Fall einer erfolgreich aufgebauten VPN-Verbindung.

Antwort bestehend aus Fortschrittsmeldungen *(pogress messages = P)* und einer finalen Meldung *(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.

Fortschrittsmeldungen

Die Antwort beginnt immer mit den fünf Fortschrittsmeldungen *synup, deviceinfo*, *vpnconn*, *dnslookup* und *routeinfo*:

synup	Zeigt den gegebenen Befehl *synup* mit seinem Parameter *name* an

<table>
<tr><td>deviceinfo</td><td colspan="4">Diese Meldung gibt Informationen zum mGuard. Das Format dieser Meldung ist:
P deviceinfo uptime=… tstamp=… serial=XXXX hostname=string
Die Bedeutung der Felder ist wie folgt:</td></tr>
<tr><td></td><td>uptime=</td><td colspan="3">Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32</td></tr>
<tr><td></td><td>tstamp=</td><td colspan="3">Datum und Zeitpunkt, zu dem die Meldung generiert wurde. Format: JJJJMMTThhmmssx, dem Datum folgen die Zeit (UTC) und ein Kleinbuchstabe. Die Bedeutung der Buchstaben ist wie folgt:</td></tr>
<tr><td></td><td></td><td>JJJJ</td><td colspan="2">4 Ziffern geben das Jahr an</td></tr>
<tr><td></td><td></td><td>MM</td><td colspan="2">2 Ziffern geben den Monat an</td></tr>
<tr><td></td><td></td><td>TT</td><td colspan="2">2 Ziffern geben den Tag im Monat an</td></tr>
<tr><td></td><td></td><td>hh</td><td colspan="2">2 Ziffern geben die Stunde des Tages an</td></tr>
<tr><td></td><td></td><td>mm</td><td colspan="2">2 Ziffern geben die Minute der Stunde an</td></tr>
<tr><td></td><td></td><td>ss</td><td colspan="2">2 Ziffern geben die Sekunde der Minute an</td></tr>
<tr><td></td><td></td><td>x</td><td colspan="2">Kleinbuchstaben geben den Status der Systemzeit und des Datums des mGuard an.</td></tr>
<tr><td></td><td></td><td></td><td>a</td><td>Systemzeit und -datum noch nicht synchronisiert.</td></tr>
<tr><td></td><td></td><td></td><td>b</td><td>Systemzeit wurde manuell eingestellt oder mittels eines unpräzisen Zeitstempels synchronisiert, der alle 2 Stunden im Dateisystem des mGuard gemeldet ist.</td></tr>
<tr><td></td><td></td><td></td><td>c</td><td>Die Systemzeit wurde mithilfe der gepufferten Echtzeituhr synchronisiert, die manuell oder einmalig über NTP synchronisiert wurde.</td></tr>
<tr><td></td><td></td><td></td><td>d</td><td>Systemzeit einmalig mit einem NTP-Server synchronisiert.</td></tr>
<tr><td></td><td></td><td></td><td>e</td><td>Systemzeit regelmäßig mit einem NTP-Server synchronisiert.</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">Trifft mehr als ein Fall zu, wird der letzte der alphabetischen Reihenfolge angezeigt.</td></tr>
<tr><td></td><td colspan="4">serial= Seriennummer des Gerätes. Leerzeichen werden durch Unterstriche ersetzt.</td></tr>
<tr><td></td><td colspan="4">hostname= Hostname des mGuard.</td></tr>
</table>

vpnconn	Spezielle Konfigurationseigenschaften der VPN-Verbindung. Das Format dieser Meldung ist wie folgt: **P vpnconn uptime=… id=vNNN gw=hostname/IP** Die Bedeutung der Felder ist wie folgt:		
	uptime=	Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32	
	id=	Der interne Name der VPN-Verbindung auf dem mGuard, unter dem die Verbindung aufrecht erhalten wird.	
	gw=	Remote-VPN-Gateway der VPN-Verbindung.	

dnslookup	Ergebnis der Auflösung des Hostnames der Remote-VPN-Gegenstelle in eine IP-Adresse. Das Format dieser Meldung ist wie folgt: **P dnslookup uptime=… ip=IP** Die Bedeutung der Felder ist wie folgt:		
	uptime=	Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32	
	ip=	IP-Adresse der VPN-Gegenstelle.	

routeinfo	Netzwerkschnittstelle, über die der mGuard versucht, die VPN-Verbindung und den Schnittstellenstatus aufzubauen. Das Format dieser Meldung ist wie folgt: **P routeinfo uptime=… via=IF(IP) ifstate=up/down/error** Die Bedeutung der Felder ist wie folgt:		
	uptime=	Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32	
	via=	Netzwerkschnittstelle, über die der mGuard versucht, die VPN-Verbindung aufzubauen. Mögliche Werte sind "ext1", "ext2", "int" "dmz0" und "dial-in".	
	ifstate=	Status der Netzwerkschnittstelle. Mögliche Werte sind:	
		up	Netzwerkschnittstelle betriebsbereit.
		down	Netzwerkschnittstelle wird betriebsbereit, sobald der Verkehr ankommt, der durch sie weitergeleitet werden soll.
		error	Netzwerkschnittstelle nicht betriebsbereit. In diesem Fall gibt der Befehl *synup* in der finalen Meldung EVIFDOWN zurück.

Der mGuard kann die Verbindung zur Remote-VPN-Gegenstelle nicht aufbauen, obwohl die vorherigen Schritte erfolgreich ausgeführt wurden; der mGuard prüft mithilfe eines IKE-Pings, ob die Remote-Site auf IKE-Meldungen antwortet. Die Prüfung wird ausgelassen wenn die IKE-Meldung schon während des Verbindungsaufbaus mit der Gegenstelle ausgetauscht wurde.

<table>
<tr><td rowspan="7">ikeping</td><td colspan="3">Ergebnis des IKE-Ping. Das Format dieser Meldung ist wie folgt:
P ikeping uptime=… to=IP:PORT via=IF response=yes|no|error
Die Bedeutung der Felder ist wie folgt:</td></tr>
<tr><td>uptime=</td><td colspan="2">Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Beispiel: uptime=75178.32</td></tr>
<tr><td>to=</td><td colspan="2">IP-Adresse und Portnummer des IKE-Ping-Ziels.</td></tr>
<tr><td>via=</td><td colspan="2">Netzwerkschnittstelle, über die der IKE-Ping gesendet wurde. Mögliche Werte sind: "ext1", "ext2", "int", "dmz0" und "dial-in".</td></tr>
<tr><td rowspan="4">response=</td><td colspan="2">Gibt Auskunft darüber, ob der mGuard rechtzeitig eine Antwort auf den IKE-Ping erhalten hat. Mögliche Werte:</td></tr>
<tr><td>yes</td><td>Der mGuard hat eine Antwort der VPN-Gegenstelle erhalten.</td></tr>
<tr><td>no</td><td>Der mGuard hat innerhalb eines bestimmten Zeitraums keine Antwort der VPN-Gegenstelle erhalten.</td></tr>
<tr><td>error</td><td>Der mGuard konnte keinen IKE-Ping senden.</td></tr>
</table>

Weitere Fortschrittsmeldungen werden während des Aufbaus der VPN-Verbindung angezeigt. Im Falle eines Versagens wird direkt eine finale Meldung angezeigt.

<table>
<tr><td>IKEv1</td><td colspan="3">Diese Meldung wird angezeigt wenn
– der mGuard ein IKEv1-Paket erhalten oder gesendet hat,
– eine Phase des Verbindungsaufbaus abgeschlossen ist.

Die Meldung kann mehrere Textfelder mit Werten enthalten. Einige von ihnen können die angebotenen oder ausgewählten Kryptoalgorithmen anzeigen.

Das Format dieser Meldung ist wie folgt:

P IKEv1 uptime=… newstate=state [key=value …] send=…

P IKEv1 uptime=… state=state [key=value …] rcvd=…

P IKEv1 uptime=… newstate=state

P IKEv1 uptime=… isakmp-sa=status id=NN info=… oder

P IKEv1 uptime=… ipsec-sa=established id=NN info=…

Die Bedeutung der Felder, die auftreten können, ist wie folgt:</td></tr>
<tr><td></td><td>uptime=</td><td colspan="2">Betriebszeit des mGuard seit der letzten Inbetriebnahme. Der Wert wird in Sekunden mit Nachkommastellen angezeigt. Zum Beispiel: uptime=75178.32</td></tr>
<tr><td></td><td>newstate=</td><td colspan="2">Statusänderung während des Aufbaus der VPN-Verbindung. Der Wert ist der Name des neuen Status.</td></tr>
<tr><td></td><td>state=</td><td colspan="2">Aktueller Status der VPN-Verbindung.</td></tr>
<tr><td></td><td>send=</td><td colspan="2">Details zu einem gesendeten Paket.</td></tr>
<tr><td></td><td>rcvd=</td><td colspan="2">Details zu einem erhaltenen Paket.</td></tr>
<tr><td></td><td rowspan="3">isakmp-sa=</td><td colspan="2">Abschlussstatus der ersten Phase. Mögliche Werte sind:</td></tr>
<tr><td></td><td>established</td><td>Eine neue ISAKMP Security Association (ISAKMP-SA) wurde aufgebaut.</td></tr>
<tr><td></td><td>reused</td><td>Eine geeignete ISAKMP-SA wurde bereits für eine andere VPN-Verbindung aufgebaut. Sie wurde für diese wieder verwendet.</td></tr>
<tr><td></td><td>ipsec-sa=</td><td colspan="2">Abschlussstatus der zweiten Phase. Der Wert ist immer "established" (aufgebaut).</td></tr>
<tr><td></td><td>id=</td><td colspan="2">Kennzeichner der ersten oder zweiten Phase. Diese Kennzeichner werden während der Laufzeit intern vom mGuard verwendet. Wird eine ISAKMP-SA wiederverwendet, kann der Kennzeichner für die Suche nach dem Befehl synup verwendet werden, der sie aufgebaut hat.</td></tr>
</table>

Finale Meldung

Wurde die VPN-Verbindung erfolgreich aufgebaut, gibt der Befehl entweder **OKVUP** oder **OKVACT** zurück.

Andernfalls wird einer der folgenden Werte zurückgegeben: **EINVAL, EAMBIGUOUS, ENOENT, ESYNVPN001, EBUSY, EVLOOKUPGW, EVLOOKUPROUT, EVIFDOWN, EVTOUT1RESP, EVTOUTWRESP, EVDIFFALG1, EVDIFFALG2, EVPEERNOENT1, EVPEERNOENT2.**

Erklärungen zu diesen Codes entnehmen Sie bitte „Antwortcode“ auf Seite 165.

9.4.3.4 cmd=synstat

Dieser Befehl ermittelt den Status einer VPN-Verbindung. Der Name der VPN-Verbindung muss mit dem Parameter *name* angegeben werden.

Beispiel: Ermittlung des Status der VPN-Verbindung mit dem Namen *Service*

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=synstat&name=Service'

Antwort:

```
R OKVST1 id=MAI0003584192 enabled=no activated=yes ike=OK ipsec=OK
```

Konnte der Status der VPN-Verbindung erfolgreich ermittelt werden, wird **OKVST1** mit folgender zusätzlicher Information zurückgegeben:

OKVST1	Der mGuard hat den Status der VPN-Verbindung erfolgreich ermittelt. Das Format dieser Meldung ist wie folgt: **R OKVST1 id=id enabled=yesno1 activated=yesno2 ike=stat1 ipsec=stat2** Die Bedeutung der Felder ist wie folgt:		
	id=	Interner Kennzeichner (*internal identifier*) der VPN-Verbindung, der während der Laufzeit vom mGuard verwendet wird. Dies ist nicht der konfigurierte Name der VPN-Verbindung.	
	enabled=	Zeigt an, ob die VPN-Verbindung auf dem mGuard als "*enabled*" (aktiviert) konfiguriert ist oder nicht. Mögliche Werte sind:	
		yes	VPN-Verbindung aktiviert.
		no	VPN-Verbindung deaktiviert.
	activated=	Zeigt an, ob die VPN-Verbindung "aushilfsweise aktiv" ist, was der Fall ist, wenn die VPN-Verbindung mit den Befehlen **synup** oder **up** durch das *CGI-Script nph-vpn.cgi* oder mit CMD-Kontakt aufgebaut wurde. Mögliche Werte sind:	
		yes	Aushilfsweise aktiv
		no	Nicht aushilfsweise aktiv
	ike=	Status der zu dieser VPN-Verbindung gehörenden ISAKMP Security Association (ISAKMP-SA). Dieses Feld ist nur vorhanden, wenn die VPN-Verbindung "aushilfsweise aktiv" ist. Mögliche Werte sind:	
		NAME	ISAKMP-SA wird aufgebaut. ISAKMP-SA hat den Status **NAME**. Der Wert von **NAME** unterscheidet sich von den anderen Werten "OK", "EXP" oder "DEAD".
		OK	ISAKMP-SA ist aufgebaut und kann verwendet werden.
		EXP	ISAKMP-SA abgelaufen. Wurde noch nicht erneuert.
		DEAD	ISAKMP-SA existiert nicht für diese VPN-Verbindung.
	ipsec=	Status der zu dieser VPN-Verbindung gehörenden IPsec ISAKMP Security Association (IPsec-SA). Wird nur angezeigt, wenn die VPN-Verbindung "aushilfsweise aktiv" ist. Mögliche Werte und ihre Bedeutungen:	
		NAME	IPsec-SA wird aufgebaut. IPsec-SA hat den Status **NAME**. Der Wert von **NAME** unterscheidet sich von den anderen Werten "OK", "EXP" oder "DEAD".
		OK	IPsec-SA ist aufgebaut und kann verwendet werden.
		EXP	IPsec-SA abgelaufen. Wurde noch nicht erneuert.
		DEAD	IPsec-SA existiert nicht für diese VPN-Verbindung.

Konnte der Status der VPN-Verbindung nicht erfolgreich ermittelt werden, wird einer der folgenden Werte zurückgegeben: **EINVAL, EAMBIGUOUS, ENOENT**.

Erklärungen zu diesen Codes entnehmen Sie bitte „Antwortcode“ auf Seite 165.

9.4.3.5 cmd=syndown

Dieser Befehl deaktiviert eine VPN-Verbindung. Der Name der VPN-Verbindung muss mit dem Parameter *name* angegeben werden.

Beispiel: Deaktivierung der VPN-Verbindung mit dem Namen *Service*

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=syndown&name=Service'

Antwort:

```
R OKVDOWN
```

Wurde die VPN-Verbindung erfolgreich deaktiviert, gibt der Befehl entweder **OKVDOWN** oder **OKVNOTACT** zurück.

Andernfalls wird einer der folgenden Werte zurück gegeben: **EINVAL, EAMBIGUOUS, ENOENT.**

Erklärungen zu diesen Codes entnehmen Sie bitte „Antwortcode“ auf Seite 165.

9.4.4 Zentrale VPN-Gateway-Befehle

Die in den vorhergehenden Kapitels erklärten Befehle werden auf Remote-mGuards verwendet, die VPN-Verbindungen zu einem zentralen VPN-Gateway aufbauen. Zwei weitere Befehle sind speziell für die Verwendung auf einem zentralen VPN-Gateway verfügbar, das das Feature *VPN-Tunnelgruppe* verwendet. *VPN-Tunnelgruppe* ermöglicht es vielen Remote-mGuards, eine VPN-Verbindung zu einer einzelnen konfigurierten VPN-Verbindung auf dem zentralen VPN-Gateway aufzubauen.

Eine *VPN-Tunnelgruppenverbindung* hat *%any* als Gegenstellenadresse und das angegebene VPN-Netzwerk ist ein großes Netzwerk (z.B. 192.168.0.0/16), inklusive aller Netzwerke der Remote-mGuards (z.B. 192.168.**1**.0/24, 192.168.**2**.0/24, 192.168.**3**.0/24 etc.).

Die VPN-Verbindung nimmt gleichzeitig ISAKMP-SAs von vielen unterschiedlichen Remote-mGuards an. Es wird erwartet, dass jeder Remote-mGuard eine oder mehrere IPsec-SAs im Tunnelmodus aufbaut, wo der Remote-mGuard ein eindeutiges Subnetz des konfigurierten Remote-Netzwerkes für jedes Tunnelende anfordert.

Hat das zentrale VPN-Gateway nur eine konfigurierte *VPN-Tunnelgruppe*, mit der sich alle Remote-mGuards verbinden, kann nicht ermittelt werden, ob eine aktive Verbindung zu einem einzelnen Remote-mGuard besteht. Natürlich kann *cmd=status* ohne Angabe des VPN-Verbindungsnamens verwendet werden (siehe Kapitel 9.4.2.3), aber dieser Befehl würde den Status aller Tunnel ermitteln, was für die Statusabfrage für einen einzelnen Tunnel nicht effizient ist.

Manchmal soll der Administrator des zentralen VPN-Gateways eine bestimmte VPN-Gegenstelle von der VPN-Verbindung löschen. Das ist besonders hilfreich, wenn die VPN-Gegenstelle aus welchen Interoperabilitätsgründen auch immer keinen neuen Tunnel aufbauen kann. IPsec ist ein Standard, aber manchmal erfüllen die Geräte anderer Anbieter nicht alle Anforderungen dieses Standards. Ohne die Option, eine spezifische VPN-Verbindung zu löschen, muss die gesamte *VPN-Tunnelgruppen*konfiguration neu gestartet werden. Das würde dazu führen, dass alle VPN-Tunnel verworfen und wieder aufgebaut werden müssen.

9.4.4.1 cmd=status, channel=<LNet:RNet>

Dieser Befehl ermittelt den Status des angegebenen VPN-Tunnels. *LNet* steht für das lokale VPN.Netzwerk, *RNet* für das VPN-Netzwerk der Gegenstelle.

Rückgabewert	Bedeutung
unknown	Dieser Rückgabewert kann zwei Ursachen haben: – Derzeit besteht kein passender Tunnel. Es besteht weder ein konfigurierter und aktiver Tunnel mit den angegebenen Netzwerken noch ein passender aufgebauter Tunnel einer *VPN-Tunnelgruppe*. – Ein passender Kanal ist aufgrund eines Fehlers inaktiv (zum Beispiel weil das externe Netzwerk gestört ist oder weil der Hostname der Gegenstelle nicht in eine IP-Adresse aufgelöst werden konnte (DNS)).
ready	Die Verbindung lässt eingehende Anfragen bezüglich des Tunnelaufbaus zu.
active	Der Tunnel ist aufgebaut.

Beispiel: *wget […] 'https://admin:mGuard@77.245.33.67/nphvpn.cgi?cmd=status& channel=10.1.0.0/16:192.168.23.0/24'*

Antwort:

```
active
```

9.4.4.2 cmd=clear, channel=<LNet:RNet>

Dieser Befehl löscht den angegebenen VPN-Tunnel. *LNet* steht für das lokale VPN-Netzwerk, *RNet* für das VPN-Netzwerk der Gegenstelle.

Rückgabewert	Bedeutung
unknown	Derzeit besteht kein passender Tunnel.
Deleting connection ...	Der Tunnel wird gelöscht.

Beispiel:

wget […] 'https://admin:mGuard@77.245.33.67/nph-vpn.cgi?cmd=clear&channel=10.1.0.0/16:192.168.23.0/24'

Antwort:

```
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
```

9.4.5 cmd=sysinfo

Dieser Befehl ermittelt die Softwareversion, den Hardwarenamen und die Hardware-Revision auf dem mGuard.

Beispiel:

wget […] 'https://admin:mGuard@192.168.1.1/nph-vpn.cgi?cmd=sysinfo'

Antwort:

```
mGuardProductName=mGuard smart2
mGuardHardware=MGUARD2
mGuardHardwareVersion=00003000
mGuardVersion=7.5.0.default
```

9.5 Interface nph-diag.cgi

9.5.1 cmd=snapshot

Der *Body* der durch den Befehl snapshot produzierten HTTP-Antwort hat binären Inhalt. Er sollte in eine Datei gespeichert werden, vorzugsweise als snapshot.tar.gz. Wird wget verwendet, nutzen Sie dafür die Option *output-document* (*wget … --output-document=snapshot.tar.gz …*).

Der Snapshot enthält die aktuelle Konfiguration des mGuard, seine Laufzeitparameter und alle Log-Einträge. Die Datei enthält außerdem die in diesem Dokument beschriebenen VPN-Diagnosemeldungen der letzten 100 (maximal) VPN-Verbindungsaufbauten, wenn die VPN-Verbindung durch CMD-Kontakt oder durch das Skript nph-vpn.cgi ausgelöst wurde und wenn die Optionen **Archiviere Diagnosemeldungen zu VPN-Verbindungen** (Menü **IPsec VPN >> Global**, Registerkarte *Optionen*) aktiviert sind. Diese Datei enthält keine privaten Informationen wie z. B. private Schlüssel oder Passwörter.

Beispiel: *wget […] 'https://admin:mGuard@192.168.1.1/nph-diag.cgi?cmd=snapshot'*

9.5.2 cmd=testpull

Der mGuard kann sich in einstellbaren Zeitintervallen neue Konfigurationsprofile von einem HTTPS Server holen, wenn der Server sie dem mGuard als Konfigurationsprofil (*.atv) zur Verfügung stellt. Unterscheidet sich eine neue mGuard-Konfiguration von der aktuellen Konfiguration, wird sie automatisch heruntergeladen und aktiviert. Diese Option wird über die Weboberflache im Menü **Verwaltung >> Zentrale Verwaltung** konfiguriert.

Mit diesem Befehl kann geprüft werden, ob eine Konfigurationsdatei vom Konfigurationsserver gemäß den aktuellen Einstellungen des mGuard heruntergeladen werden kann. Der mGuard wendet das Profil nicht an, wenn dieser Befehl erfolgreich ausgeführt wurde. Dieser Befehl gibt in der HTTP-Antwort einen der folgenden Werte zurück:

OKCONFPULL	Der mGuard hat die Konfiguration erfolgreich heruntergeladen. Das Format dieser Meldung ist: **R OKCONFPULL d=digest** Die Bedeutung der Felder ist wie folgt:	
	digest	Alphanumerischer String, den der mGuard an den IDM (MGUARD DM, MGUARD Device Manager) mit der HTTP-Anfrage schickt, um anzuzeigen, welche Version der Konfigurationsdatei heruntergeladen wurde.
ECONFPULL	Download der Konfigurationsdatei fehlgeschlagen. Das Format dieser Meldung ist wie folgt: **F ECONFPULL http-code=code msg=message** Die Bedeutung der Felder ist wie folgt:	
	code	Vom HTTPS-Server zurückgegebener HTTP-Statuscode. Leer, wenn der HTTP-Statuscode aufgrund eines Fehlers auf einem anderen Layer, z.B. auf dem Secure Socket Layer (SSL) nicht übertragen werden konnte.
	message	Diese Meldung gibt den Grund für den Fehler an und kann weitere Informationen enthalten. Sie enthält weiterhin die Fehlermeldung des HTTPS-Servers, wenn der HTTP-Statuscode unbekannt ist.

Beispiel: *wget […] 'https://admin:mGuard@192.168.1.1/nph-diag.cgi?cmd=testpull'*
Antwort:

```
R OKCONFPULL tstamp=20120515094007e d=d12851f0b9801e0df45c5794c7f392c5
```

9.6 Interface nph.action.cgi

Benutzer „root“ und „admin“

Die folgenden Befehle können durch die Benutzer **root** und **admin** ausgeführt werden.

Zeilenaktionen (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>

Tabelle 9-4 **Zeilenaktionen** – Parameter

Parameter	Beschreibung
name	Verbindungsname, Regelsätze, Integritätsprüfung
rowid	Eindeutige ID aus der Konfiguration (gaiconfig --goto VPN_CONNECTION:0 --get-rowid)

Tabelle 9-5 **Zeilenaktionen** – Aktion

Aktion	Beschreibung
fwrules/inactive	Deaktiviert einen Firewall-Regelsatz
fwrules/active	Aktiviert einen Firewall-Regelsatz
vpn/stop	Stoppt wie „nph-vpn.cgi“ ebenfalls eine IPsec-Verbindung, aber mit geringerer Komplexität
vpn/start	Startet wie „nph-vpn.cgi“ ebenfalls eine IPsec-Verbindung, aber mit geringerer Komplexität
openvpn/stop	Stoppt eine OpenVPN-Verbindung
openvpn/start	Startet eine OpenVPN-Verbindung
cifsim/validaterep	Validiert einen CIFS/IM-Scanbericht
cifsim/check-start	Startet eine CIFS/IM-Prüfung
cifsim/init-start	Erzeugt eine neue CIFS/IM-Integritätsdatenbank
cifsim/cancel	Beendet einen laufenden CIFS/IM-Job
cifsim/erase-db	Löscht die CIFS/IM-Datenbank
cifsim/access-scan	Startet die Zugriffsüberprüfung eines Netzlaufwerks

Benutzerfirewall-Logout

https://admin:mGuard@192.168.1.1/nph-action.cgi?action=userfw/logout&name=<NAME> &ip=<IP>

Tabelle 9-6 Benutzerfirewall-Logout – Parameter

Parameter	Beschreibung
name	Benutzerkennung des eingeloggten Benutzers der Benutzerfirewall
ip	Die aktuelle IP-Adresse des eingeloggten Benutzers der Benutzerfirewall

Tabelle 9-7 Benutzerfirewall-Logout – Aktion

Aktion	Beschreibung
userfw/logout	Meldet den angemeldeten Firewall-Benutzer ab (*Logout*)

Einfache Befehle

(Parameter *name* oder *ID* sind nicht erforderlich)

https://admin:mGuard@192.168.1.1/nph-action.cgi?action=<ACTION>

Tabelle 9-8 Einfache Befehle – Aktionen

Aktion	Beschreibung
switch/purge-arlt	Setzt die Address-Resolution-Tabelle des internen Switch zurück
switch/reset-phy-counters	Setzt den PHY-Zähler des internen Switch zurück

Benutzer „mobile“, „root“ und „admin“

Die folgenden Befehle können durch die Benutzer **mobile**, **root** und **admin** ausgeführt werden. Der Benutzer **mobile** ist ab Firmware-Version 8.3.0 verfügbar.

Mobile Aktionen (Benutzer: mobile / root / admin)

– **Nur mGuard-Firmwareversion 8.3:**
https://admin:mGuard@192.168.1.1/nph-action.cgi?action=gsm/call&dial=<NUMBER>&timeout=<TIMEOUT>

– **mGuard-Firmwareversion 8.3 und 8.4:**
https://admin:mGuard@192.168.1.1/nph-action.cgi?action=gsm/sms&dial=<NUMBER> &msg=<MESSAGE>

Tabelle 9-9 Mobile Aktionen – Parameter

Parameter	Beschreibung
dial	Ziel-Telefonnummer
timeout	Zeit bis zur Beendigung des Anrufs (in Sekunden)
msg	Inhalt der Kurznachricht (ohne Sonderzeichen und Umlaute)

Tabelle 9-10 Mobile Aktionen – Aktionen

Akion	Beschreibung
gsm/call	Startet einen Telefonanruf
gsm/sms	Sendet eine Textnachricht (SMS)

9.7 Interface nph.status.cgi

Die folgenden Befehle können durch die Benutzer **root** und **admin** ausgeführt werden.

Tabelle 9-11 CGI-Status

Parameter	Beschreibung
/network/modem/state	**Status des Modems**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/network/modem/state	
Antwort: *online* | *offline*	
/network/ntp_state	**Status der NTP-Zeitsynchronisation**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/network/ntp_state	
Antwort: *disabled* | *not_synced* | *synchronized*	
/system/time_sync	**Status der Systemzeitsynchronisation**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/system/time_sync	
Antwort: *not_synced* | *manually* | *stamp* | *rtc* | *ntp* | *gps* | *gpslost*	
/ecs/status	**Status des ECS-Speichers**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/ecs/status	
Antwort: "1" für nicht präsent, "2" für entfernt, "3" für präsent und in Synchronisation, "4" für nicht in Synchronisation und "8" für allgemeiner Fehler	
/vpn/con	**Status einer VPN-Verbindung**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/vpn/con&name=<Verbindungsname>	
Antwort: – */vpn/con/<rowid>/armed=[yes|no]* Zeigt an, ob die Verbindung gestartet wurde oder nicht. – */vpn/con/<rowid>/ipsec=[down|some|up]* Zeigt den IPsec-Status. – */vpn/con/<rowid>/isakmp=[up|down]* Zeigt den ISAKMP-Status. – */vpn/con/<rowid>/sa_count=<number>* Anzahl aufgebauter Tunnel – */vpn/con/<rowid>/sa_count_conf=<number>* Anzahl konfigurierter aktivierter Tunnel	
/fwrules	**Status eines Firewall-Regelsatzes**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/fwrules&name=<Regelsatz>	
Antwort: – */fwrules/<rowid>/expires=<seconds since 1.1.1970>* Ablaufzeit – 0 für keine Ablaufzeit – */fwrules/<rowid>/state=[inactive|active]* Aktivitätsstatus des Firewall-Regelsatzes	
/cifs/im	**Status eines Netzlaufwerks in Bezug auf CIFS**
https://admin:mGuard@192.168.1.1/nph-status.cgi?path=/cifs/im&name=<Netzlaufwerksname>	

Tabelle 9-11 CGI-Status

Parameter	Beschreibung
Antwort:	
Aktuell laufende Überprüfung	
– */cifs/im/<rowid>/curr/all=<number>* Anzahl der Dateien	
– */cifs/im/<rowid>/curr/end=<seconds>* Ablaufzeit der aktuell laufenden Überprüfung in Sekunden seit dem 1.1.1970	
– */cifs/im/<rowid>/curr/numdiffs=<number>* Aktuell gefundene Anzahl von Abweichungen.	
– */cifs/im/<rowid>/curr/operation=[none|suspend|check|idb_build]* Aktueller Vorgang	
– */cifs/im/<rowid>/curr/scanned=<number>* Anzahl aktuell überprüfter Dateien	
– */cifs/im/<rowid>/curr/start=<seconds>* Startzeit in Sekunden seit dem 1.1.1970	
Letzte abgeschlossene Überprüfung	
– */cifs/im/<rowid>/last/duration=<number>* Dauer der letzten Überprüfung in Sekunden	
– */cifs/im/<rowid>/last/numdiffs=<number>* Anzahl der Unterschiede, die bei der letzten Überprüfung gefunden wurden.	
– */cifs/im/<rowid>/last/start=<seconds> start time in seconds since 1.1.1970* Startzeitpunkt der letzten abgeschlossenen Überprüfung in Sekunden sei dem 1.1.1970	
– */cifs/im/<rowid>/last/result*=<siehe unten „Letzte Ergebnisse“>	
Log-Ergebnisse	
– */cifs/im/<rowid>/log/fname=<filename of the log file>*	
– */cifs/im/<rowid>/log/hash=<sha1 hash>*	
– */cifs/im/<rowid>/log/result*=<siehe unten „Log-Ergebnisse“>	

Tabelle 9-11 CGI-Status

Parameter	Beschreibung
Letzte Ergebnisse	
– *-1:* Das Netzlaufwerk wurde noch nie überprüft. Eine Integritätsdatenbank liegt wahrscheinlich nicht vor. – *0:* Die letzte Überprüfung wurde erfolgreich abgeschlossen. – *1:* Der Vorgang wurde aufgrund eines nicht erwarteten Ereignisses abgebrochen. Bitte prüfen Sie die Log-Dateien. – *2:* Die letzte Überprüfung wurde nach Ablauf eines Timeouts abgebrochen. – *3:* Die Integritätsdatenbank ist nicht vorhanden oder unvollständig. – *4:* Die Signatur der Integritätsdatenbank ist ungültig. – *5:* Die Integritätsdatenbank wurde mit einem anderen Prüfsummen-Algorithmus erstellt. – *6:* Die Integritätsdantenbank liegt in der falschen Version vor. – *7:* Das zu überprüfende Netzlaufwerk ist nicht verfügbar. – *8:* Das Netzlaufwerk, das als Prüfsummenspeicher verwendet werden soll, ist nicht verfügbar. – *11:* Eine Datei konnte aufgrund eines I/O-Fehlers nicht gelesen werden (siehe Prüfbericht). – *12:* Der Verzeichnisbaum konnte aufgrund eines I/O-Fehlers nicht vollständig durchlaufen werden (siehe Prüfbericht).	
Log-Ergebnisse	
– *unchecked* – Die Signatur wurde noch nicht verifiziert. – *valid* – Die Signatur ist gültig. – *Emissing* – FEHLER: Der Prüfbericht fehlt. – *Euuid_mismatch* – FEHLER: Der Prüfbericht gehört nicht zu diesem Gerät oder ist nicht aktuell. – *Ealgo_mismatch* – FEHLER: Der Prüfbericht wurde mit einem anderen Prüfsummenalgorithmus erstellt. – *Etampered* – FEHLER: Der Prüfbericht wurde verfälscht. – *Eunavail* – FEHLER: Der Prüfbericht ist nicht verfügbar. Prüfen Sie, ob das Netzlaufwerk eingebunden (mounted) ist. – *Eno_idb* – Eine Prüfbericht liegt aufgrund einer fehlenden Integritätsdatenbank nicht vor.	

10 LED-Statusanzeige und Blinkverhalten

Dokument-ID: 108400_de_00
Dokument-Bezeichnung: AH DE MGUARD LED SIGNALS

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der Adresse phoenixcontact.net/products zum Download bereit.

Inhalt dieses Dokuments

In diesem Dokument wird das Leucht- und Blinkverhalten der in mGuard-Geräten (FL/TC MGUARD RS2000/RS4000) verbauten LED-Dioden beschrieben.

10.1 Beschreibung der LEDs

Mithilfe von eingebauten LED-Dioden zeigen mGuard-Geräte verschiedene Systemzustände an. Dabei kann es sich um Status-, Alarm- oder Fehlermeldungen handeln.

Die Zustände werden durch permanentes oder temporäres Leuchten bzw. Blinken der LEDs angezeigt. Das angezeigte LED-Muster kann auch eine Kombination verschiedener Systemzustände darstellen.

ACHTUNG: Da mehrere Systemzustände nicht eindeutig, nur temporär oder in Kombination mit anderen Zuständen durch die LEDs angezeigt werden, müssen zusätzlich die Log-Dateien des mGuard-Geräts überprüft werden!

LED-Dioden der FL/TC MGUARD (RS200x/RS400x)-Geräte:

P1	Stat	Mod	Info2 (Sig)
●	●	●	●
●	●	●	●
P2	**Err**	**Fault**	**Info1**

P1 / P2

Die LEDs *P1* und *P2* zeigen an, welche der beiden Stromversorgungen angeschlossen ist (Geräte der FL/TC MGUARD RS2000-Serie: nur *P1* ist verfügbar).

Info2 / Info1 (die LED Sig wird nicht verwendet)

Über die LEDs *Info2* und *Info1* können aktive VPN-Verbindungen oder (ab Version 8.1) aktive Firewall-Regelsätze angezeigt werden. Die Aktivierung der LEDs durch eine bestimmte VPN-Verbindung oder einen bestimmten Firewall-Regelsatz wird auf der mGuard-Oberfläche im Menüpunkt **Verwaltung >> Servicekontakte** konfiguriert.

Die folgenden Zustände werden angezeigt:.

ON	Die VPN-Verbindung ist aufgebaut / der Firewall-Regelsatz ist geschaltet.
Blink	Die VPN-Verbindung wird auf- bzw. abgebaut oder wurde von der Gegenstellen gestoppt/deaktiviert.
OFF	Die VPN-Verbindung ist auf beiden Gegenstellen gestoppt/deaktiviert.

Stat / Mod / Err / Fault

Die LEDs *Stat*, *Mod*, *Err* und *Fault* zeigen Systemzustände (Status-, Alarm- oder Fehlermeldungen) an (siehe Tabelle 10-3).

Eine leuchtende **LED Fault** zeigt neben den Alarmmeldungen generell auch an, dass das Gerät aktuell nicht betriebsbereit ist.

LAN / WAN

Die LAN/WAN LEDs befinden sich in den LAN/WAN-Buchsen (10/100 und Duplex-

Anzeige).

Die LEDs zeigen den Ethernet-Status des LAN- bzw. WAN-Interface. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt ein kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerkpartner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.

Wenn alle LAN-/WAN-LEDs leuchten, bootet das System.

Bargraph und SIM 1/2 (Mobilfunk)

Tabelle 10-1 Anzeigen des TC MGUARD RS4000 3G und TC MGUARD RS2000 3G

LED	**Zustand und Bedeutung**					
Bar-graph	LED 3	Oben	Aus	Aus	Aus	Grün
	LED 2	Mitte	Aus	Aus	Grün	Grün
	LED 1	Unten	Aus	Gelb	Gelb	Gelb
	Signalstärke (dBm)		–113 ... 111	–109 ... 89	–87 ... 67	–65 ... 51
	Netzempfang		Sehr schlecht bis kein	Ausreichend	Gut	Sehr gut
SIM 1	Grün	ON Blink	SIM-Karte 1 aktiv Keine oder falsche PIN eingegeben			
SIM 2	Grün	ON Blink	SIM-Karte 2 aktiv Keine oder falsche PIN eingegeben			

10.2 Leucht- und Blinkverhalten der LEDs

Tabelle 10-2 Beschreibung des Leucht- und Blinkverhaltens der LED-Dioden

Heartbeat	Das Blinkverhalten ähnelt eine Herzschlag, bei dem zwei Schläge kurz hintereinander ausgeführt werden, gefolgt von einer kurzen Pause.
Running light	Drei Lichter bilden ein sich kontinuierlich wiederholendes Lauflicht von links nach rechts und wieder zurück.
Blink 50/1500	Blitzen mit 1500 ms Pause (50 ms an, dann 1500 ms aus)
Blink 50/800	Blitzen mit 800 ms Pause (50 ms an, dann 800 ms aus)
Blink 50/100	Blitzen mit 100 ms Pause (50 ms an, dann 100 ms aus)
Blink 500/500	Gleichmäßiges Blinken (500 ms an / 500 ms aus)
Morse code (. . . – – – . . .)	Das Blinkverhalten zeigt den *Morse-Code 'SOS'*, bei dem sich das Blinkverhalten "3x kurz, 3x lang, 3x kurz" fortlaufend wiederholt.
ON	Die Diode leuchtet permanent.
ON (n sec)	Die Diode leuchtet permanent für die angegeben Zeit (in Sekunden *n*)

10.3 Darstellung der Systemzustände

Die Systemzustände (Status-, Alarm- oder Fehlermeldungen), die über das Leucht- bzw. Blinkverhalten der LED-Dioden angezeigt werden, entnehmen Sie bitte Tabelle 10-3.

Tabelle 10-3 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände bei FL/TC MGUARD-Geräten

STAT	MOD	Info 2 (Sig)	ERR	FAULT	Beschreibung des Systemzustands
Heart-beat					Der Systemstatus ist OK.
			ON		Ein schwerer Fehler ist aufgetreten.
ON (12 sec)	ON (3 sec)		ON (12 sec)	ON (12 sec)	Das System bootet.
Morse code					Die Lizenz zur Verwendung der Firmware fehlt.
Morse code			**Morse code**		Der Austausch des Bootloaders ist aufgrund eines Hardwaredefekts fehlgeschlagen.
				ON	Ein Fehler bei der Stromversorgung wurde festgestellt.
				ON	Keine Konnektivität auf der WAN-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
				ON	Keine Konnektivität auf der LAN-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
				ON	Keine Konnektivität auf der LAN(1-4)-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
				ON	Keine Konnektivität auf der DMZ-Schnittstelle (Linküberwachung am Gerät konfigurierbar)
				ON	Spannungsversorgung 1 oder 2 ausgefallen (Alarm am Gerät konfigurierbar)
				ON	Temperatur zu hoch / zu niedrig (Alarm am Gerät konfigurierbar)

Tabelle 10-3 Durch das Leucht- und Blinkverhalten der LEDs dargestellte Systemzustände bei FL/TC MGUARD-Geräten

STAT	MOD	Info 2 (Sig)	ERR	FAULT	Beschreibung des Systemzustands
				ON	(Redundanz) Verbindungsprüfung fehlgeschlagen (Alarm am Gerät konfigurierbar)
				ON	(Modem) Verbindungsprüfung fehlgeschlagen (Alarm am Gerät konfigurierbar)
			ON (3 sec)		ECS: Das ECS ist inkompatibel.
			ON (3 sec)		ECS: Die Kapazität des ECS ist erschöpft.
			ON (3 sec)		ECS: Das Root-Passwort aus dem ECS stimmt nicht überein.
			ON (3 sec)		ECS: Die Konfiguration konnte nicht aus dem ECS geladen werden.
			ON (3 sec)		ECS: Die Konfiguration konnte nicht im ECS gespeichert werden.
	ON				PPPD: Das interne Modem hat eine Verbindung aufgebaut (eingestellt durch pppd).
	Blink 50/1500				PPPD: Das interne Modem ist aktiviert und erwartet eine Einwahl.
	Blink 500/500				PPPD: Das interne Modem wählt.
			ON (2 sec)		RECOVERY: Das Wiederherstellungsverfahren ist fehlgeschlagen.
ON (2 sec)					RECOVERY: Das Wiederherstellungsverfahren war erfolgreich.
ON				ON	FLASH-PROZEDUR: Die Flash-Prozedur wurde gestartet. Bitte warten.
Running light	Running light	Running light		ON	FLASH-PROZEDUR: Die Flash-Prozedur wird ausgeführt.
Blink 50/800	Blink 50/800	Blink 50/800		ON	FLASH-PROZEDUR: Die Flash-Prozedur war erfolgreich.
ON			ON		FLASH-PROZEDUR: Die Flash-Prozedur / der Produktionsvorgang ist fehlgeschlagen.
			Blink 50/100 (5 sec)		FLASH-PROZEDUR WARNUNG: Austausch des Rettungssystems. Schalten Sie das Gerät nicht aus. Wenn das Blinken aufhört, ist der Austausch des Rettungssystems beendet.
			ON		FLASH-PROZEDUR: Die DHCP/BOOTP-Anforderungen sind fehlgeschlagen.
			ON		FLASH-PROZEDUR: Das Einbinden (Mounten) des Datenspeichers (data storage device) ist fehlgeschlagen.
			ON		FLASH-PROZEDUR: Die Flash-Prozedur ist fehlgeschlagen.
			ON		FLASH-PROZEDUR: Das Löschen der Dateisystem-Partition ist fehlgeschlagen.
			ON		FLASH-PROZEDUR: Das Laden des Firmware-Images ist fehlgeschlagen.
			ON		FLASH-PROZEDUR: Die Signatur des Firmware-Images ist ungültig.
			ON		FLASH-PROZEDUR: Das Installationsskript konnte nicht geladen werden.
			ON		FLASH-PROZEDUR: Die Signatur des Installationsskripts ist ungültig.
			ON		FLASH-PROZEDUR: Das Rollout-Skript ist fehlgeschlagen.

Bitte beachten Sie folgende Hinweise

Hinweis zur Verwendung von Anwenderhinweisen

Die zur Verfügung gestellten Anwenderhinweise sind ein kostenloser Service von Phoenix Contact. Bei den dargestellten Beispielen und Lösungswegen handelt es sich nicht um kundenspezifische Lösungen, sondern um allgemeine Hilfestellungen bei typischen Anwendungsszenarien. Die Anwenderhinweise sind grundsätzlich unverbindlich und erheben keinen Anspruch auf Vollständigkeit.

Eine Qualitätsprüfung der Anwenderhinweise findet statt, ist jedoch nicht mit der Qualitätskontrolle kostenpflichtiger Produkte vergleichbar. Fehler, Funktions- und Leistungsmängel können nicht ausgeschlossen werden.

Zur Vermeidung von Fehlfunktionen/Fehlkonfigurationen und damit einhergehenden Schäden liegt die sachgemäße und sichere Verwendung des Produkts/der Software allein in der Verantwortung des Kunden und muss innerhalb der geltenden Vorschriften erfolgen.

Die beschriebenen Beispiele müssen vom Kunden auf ihre Funktion überprüft und an die individuellen, kundenspezifischen Anforderungen der Anlage bzw. des Einsatzszenarios angepasst werden.

Die IP-Einstellungen in den Anwenderhinweisen wurden beispielhaft gewählt. In einer echten Netzwerkumgebung müssen diese IP-Einstellungen grundsätzlich angepasst werden, um möglich Adresskonflikte zu vermeiden.

Die Angaben in den Anwenderhinweisen werden regelmäßig überprüft. Sollten Korrekturen notwendig sein, werden diese in der jeweils nachfolgenden Revision enthalten sein. Eine Benachrichtigung von Nutzern findet nicht statt.

Allgemeine Nutzungsbedingungen für Technische Dokumentation

Phoenix Contact behält sich das Recht vor, die technische Dokumentation und die in den technischen Dokumentationen beschriebenen Produkte jederzeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern, soweit dies dem Anwender zumutbar ist. Dies gilt ebenfalls für Änderungen, die dem technischen Fortschritt dienen.

Der Erhalt von technischer Dokumentation (insbesondere von Benutzerdokumentation) begründet keine weitergehende Informationspflicht von Phoenix Contact über etwaige Änderungen der Produkte und/oder technischer Dokumentation. Sie sind dafür eigenverantwortlich, die Eignung und den Einsatzzweck der Produkte in der konkreten Anwendung, insbesondere im Hinblick auf die Befolgung der geltenden Normen und Gesetze, zu überprüfen. Sämtliche der technischen Dokumentation zu entnehmenden Informationen werden ohne jegliche ausdrückliche, konkludente oder stillschweigende Garantie erteilt.

Im Übrigen gelten ausschließlich die Regelungen der jeweils aktuellen Allgemeinen Geschäftsbedingungen von Phoenix Contact, insbesondere für eine etwaige Gewährleistungshaftung.

Phoenix Contact behält sich das Recht vor, für die hier verwendeten Produktkennzeichnungen von Phoenix Contact-Produkten eigene Schutzrechte anzumelden. Die Anmeldung von Schutzrechten hierauf durch Dritte ist verboten.

Andere Produktkennzeichnungen können gesetzlich geschützt sein, auch wenn sie nicht als solche markiert sind.

So erreichen Sie uns

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen Geschäftsbedingungen finden Sie im Internet unter:
phoenixcontact.com.

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der folgenden Adresse zum Download bereit:
phoenixcontact.net/products.

Ländervertretungen

Bei Problemen, die Sie mit Hilfe dieser Dokumentation nicht lösen können, wenden Sie sich bitte an Ihre jeweilige Ländervertretung.
Die Adresse erfahren Sie unter phoenixcontact.com.

Herausgeber

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

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
tecdoc@phoenixcontact.com