FL MGUARD DM UNLIMITED Installation, Konfiguration und Benutzung des mGuard device manager (mdm 1.17.x)

Anwenderhandbuch

Anwenderhandbuch

FL MGUARD DM UNLIMITED –– Installation, Konfiguration und Benutzung des mGuard device manager (mdm 1.17.x)

UM DE MDM 1.17, Revision 03 2025-01-29

Dieses Handbuch ist gültig für:

Bezeichnung	Artikel-Nr.
FL MGUARD DM UNLIMITED 1.17.x	2981974

111024_de_03

Phoenix Contact GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Inhaltsverzeichnis

1 Einleitung 7

1.1 MGUARD-Geräte verwalten 7

2 Installation 9

2.1 Systemanforderungen (mdm 1.17.x) 9

2.1.1 Microsoft Windows 9

2.1.2 Ubuntu Linux 9

2.1.3 mdm-VA (mit Ubuntu 22.04 LTS) 9

2.1.4 Ubuntu 22.04 LTS Server (nativ) 10

3 Vorkonfigurationen 13

3.1 Die mGuard-Geräte vorkonfigurieren 13

3.2 HTTPS Configuration-Pull-Server vorkonfigurieren 13

4 mdm-Server und mdm-Client 15

4.1 mdm-Server unter Ubuntu starten 15

4.2 mdm-Client unter Windows verwenden 15

5 mdm-Client – Übersicht 17

5.1 Anmeldung 17

5.2 mdm Hauptfenster 18

5.2.1 mdm Hauptmenü 19

5.2.2 mdm Symbolleiste 22

5.3 Protokollfenster 23

5.3.1 Kontextmenü 24

5.3.2 Persistent Event Log 25

5.3.3 Protokollieren von Ereignissen mit syslog 26

5.4 Hardwarekonfigurationen 26

5.4.1 FL MGUARD RS2000 26

6 mdm-Client – Konfigurationsaufgaben 29

6.1 Allgemeine Bemerkungen 29

6.1.1 Navigationsbaum 29

6.1.2 Wertetypen von Variablen 31

6.1.3 Anzeige einer ungültigen Eingabe 35

6.1.4 Anzeige geänderter Werte 36

6.1.5 Anzeige eines „None“-Werts oder eines erschöpften Pools 37

6.1.6 mGuard Tabellenvariablen ändern 38

6.1.7 Komplexe Tabellenvariablen ändern 40

6.1.8 Änderungen in die Konfiguration übernehmen 41

6.2 Standardwerte (Default values) 42

6.2.1 Vererbung von geänderten Standardwerten 42

6.2.2 Verhalten von geänderten Standardwerten (mGuard 10.x) 43
6.2.3 Verhalten von geänderten Standardwerten (mGuard 8.5/8.6) 43
6.3 Geräte konfigurieren 44
6.3.1 Geräte-Übersicht (Device overview table) 44
6.3.2 Geräte-Kontextmenü (Device context menu) 55
6.3.3 Geräte-Eigenschaften (Device properties dialog) 64
6.4 Templates konfigurieren 69
6.4.1 Template-Übersicht (Template overview table) 69
6.4.2 Template-Kontextmenü (Template context menu) 71
6.4.3 Template-Eigenschaften (Template properties dialog) 74
6.4.4 Template-Konfiguration 79
6.4.5 Mit Templates arbeiten 80
6.5 Pools konfigurieren 85
6.5.1 Poolwerte-Übersicht (Pool value overview table) 85
6.5.2 Pool-Kontextmenü (Pool context menu) 88
6.5.3 Pool-Eigenschaften (Pool properties dialog) 88
6.6 VPN-Gruppen konfigurieren 92
6.6.1 VPN-Gruppen-Übersicht (VPN group overview table) 92
6.6.2 VPN-Gruppe-Kontextmenü (VPN group context menu) 95
6.6.3 Mitgliedschaft von Geräten in VPN-Gruppen bearbeiten 97
6.6.4 VPN-Gruppe-Eigenschaften (VPN group properties dialog) – Vermaschte VPN-Netzwerke 99
6.7 VPN-Verbindungen konfigurieren 103

7 mdm-Client – Verwaltungsaufgaben 107
7.1 Konfigurationen in mGuard-Geräte hochladen 107
7.1.1 Upload-Methoden 107
7.1.2 Zeit für Upload (*Upload Time*) 110
7.1.3 Temporäres Upload-Passwort (*Temporary upload password*) 111
7.1.4 Upload history 111
7.2 Gerätelizenzen und Voucher verwalten 112
7.2.1 Voucher verwalten 112
7.2.2 Lizenzen anfordern/generieren 112
7.2.3 Gerätelizenzen verwalten 113
7.2.4 Lizenzen erneuern 114
7.3 Benutzer, Rollen und Berechtigungen verwalten 115
7.3.1 Benutzer verwalten 116
7.3.2 Rollen verwalten 116
7.3.3 Berechtigungen 118
7.3.4 Authentifizierung des Benutzers 119
7.4 X.509-Zertifikate verwalten 120
7.4.1 Maschinenzertifikate 120
7.4.2 CA-Zertifikate (mGuard ab Firmware 5.0) 122
7.4.3 Gegenstellenzertifikate (mGuard ab Firmware 5.0) 123

7.4.4 Verbindungszertifikate 123
7.5 X.509-Zertifikate verwenden (mGuard ab Firmware 5.0) 123
7.6 Firmware-Upgrades mit mdm verwalten 124
7.7 Rollback-Unterstützung 127
7.8 Redundanzmodus 127

8 Konfigurationsverlauf 129
8.1 Dialog Konfigurationsverlauf 129
8.2 Frühere Konfigurationen anzeigen 133
8.3 Frühere Konfigurationen vergleichen 133
8.4 Ein Gerät aus einer früheren Konfiguration wiederherstellen 135
8.5 Änderungsbericht 136

9 Zertifikate erstellen und verwalten 139
9.1 Zertifikate und Schlüssel für SSL 140
9.2 Zertifikate und Schlüssel für eine PKI 145
9.2.1 CA-Zertifikate erstellen 148
9.2.2 Schlüsselverzeichnisse erstellen 157
9.2.3 Anforderungen an Zertifikate 159

10 mdm- Server und mdm-CA-Server konfigurieren 161
10.1 mdm-Server (Datei *preferences.xml*) 161
10.2 mdm Zertifizierungsstelle (CA) 170
10.2.1 Übersicht 170
10.2.2 mdm CA-Server (Datei *ca-preferences.xml*) 172

11 Glossar 177

1 Einleitung

1.1 MGUARD-Geräte verwalten

Durch den mGuard device manager (mdm) wird das Verwalten der mGuard Security Appliances stark vereinfacht. Das Programm bietet einen Template-Mechanismus, mit dem Sie als Anwender Tausende mGuard-Geräte zentral konfigurieren und verwalten können.

Einfach per Mausklick werden die gewünschten Firewall-Regeln und NAT-Einstellungen generiert und über die Upload-Funktion auf alle mGuard-Geräte im Netzwerk geladen. Die gewünschten Gerätekonfigurationen werden so einfach und sicher auf allen Geräten umgesetzt.

mdm ist eine Client-Server-Anwendung, bei der der Client die volle Kontrolle aller mdm Funktionen ermöglicht. Der Server speichert die Konfiguration in einer Datenbank, generiert Konfigurationsdateien und lädt diese bei entsprechender Anfrage auf die Geräte.

Das vorliegende Dokument enthält Informationen zur Installation von mdm, zum effizienten Erstellen von Konfigurationen für Ihre mGuard-Geräte und zum Hochladen von Konfigurationen auf diese Geräte. Beachten Sie ebenfalls die Release Notes von mdm 1.17.x.

Systemanforderungen: Betriebssystem Ubuntu in der mdm-VA

mdm 1.17.x kann nicht mehr unter Windows, sondern ausschließlich unter dem Betriebssystem Ubuntu 22.04 LTS (Server) betrieben werden.

Dazu kann mdm 1.17.x in der von Phoenix Contact bereitgestellten virtuellen Maschine „mdm-VA“ (siehe Kapitel 2.1.3) oder unter einem nativen Betriebssystem Ubuntu Server installiert werden (siehe Kapitel 2.1.4).

FL MGUARD 1000-Geräte werden nicht mehr unterstützt

Ab **mdm 1.15.0** ist die Verwaltung der Geräte FL MGUARD 1102/1105 nicht mehr möglich.

FL MGUARD 2000/4000-Geräte werden vollständig unterstützt

Mit der Version **mdm 1.17.x** ist es möglich, mGuard-Geräte der FL MGUARD 2000/4000-Familie vollständig zu verwalten.

Variablen, die im Vergleich zu Geräten mit installierter mGuard 8/9-Firmware nicht vorhanden sind, müssen vor einem Import (aus einer ATV-Datei oder einem Template) auf den mGuard 8/9-Geräten deaktiviert bzw. auf Werkseinstellungen zurückgesetzt werden (siehe auch Anwenderhandbuch UM DE FW MGUARD10 - 110191_de_xx, als Download erhältlich unter phoenixcontact.com/products).

Das genaue Vorgehen bei der Gerätemigration wird im Anwenderhinweis 111259_de_xx (AH DE MGUARD MIGRATE 10) beschrieben.

Unterstützte Firmware-Versionen

mGuard device manager (mdm) 1.17.x unterstützt folgende Firmware-Versionen:

- mGuard 8.0 bis 9.0 (vollständig)
- mGuard 10.3 bis 10.5 (vollständig)
- mGuard 5.0 bis 7.6 (mit Einschränkungen)

Die Firmware mGuardNT wird nicht mehr unterstützt.

2 Installation

2.1 Systemanforderungen (mdm 1.17.x)

2.1.1 Microsoft Windows

Für mdm 1.17.x wird keine Version des „*mdm-Installers for Windows*“ bereitgestellt, sodass mdm 1.17.x nicht mehr auf einem Windows-System installiert werden kann.

Ein Update auf mdm1.17.x wird auf einem Windows-System ebenfalls nicht unterstützt.

Um mdm 1.17.x weiter auf einem Windows-System betreiben zu können, kann jedoch die von Phoenix Contact bereitgestellte virtuelle Maschine „mdm-VA“ mit einem vorinstallierten Ubuntu-Betriebssystem verwendet werden (VA = *Virtual Appliance*) (siehe Kapitel 2.1.3).

Ist mdm 1.16.x bereits in einer mdm-VA installiert, kann es innerhalb der mdm-VA auf die Version mdm 1.17.x upgedated werden.

2.1.2 Ubuntu Linux

mdm 1.17.x kann ausschließlich unter dem Betriebssystem Ubuntu 22.04 LTS (Server) installiert werden.

Dazu kann mdm 1.17.x entweder

– in der von Phoenix Contact bereitgestellten virtuellen Maschine „mdm-VA“ (siehe Kapitel 2.1.3) oder
– unter einem nativen Betriebssystem Ubuntu Server installiert werden (siehe Kapitel 2.1.4).

2.1.3 mdm-VA (mit Ubuntu 22.04 LTS)

Die virtuelle Maschine „mdm-VA“ wird als OVA-Datei bereitgestellt und mit einer Virtualisierungssoftware betrieben. Sie wird durch eine von Phoenix Contact bereitgestellte Konfigurations-Datei vorkonfiguriert und ermöglicht die einfache Installation von mdm 1.17.x.

Die in der mdm-VA verwendete Version des Ubuntu-Betriebssystems kann nicht verändert werden: Ubuntu 22.04 LTS (Server).

Grundsätzlich müssen folgende Schritte ausgeführt werden, um mdm 1.17.x in einer virtuellen Umgebung zu installieren und wie gewohnt zu verwenden:

1. *VirtualBox* herunterladen und unter Windows installieren
2. mdm-VA herunterladen und in *VirtualBox* importieren
3. Konfigurations-Datei herunterladen und zur mdm-VA hinzufügen
4. mdm-VA starten und mdm 1.17.x in der mdm-VA installieren
5. mdm-Datenbanken von mdm (1.13.x bis 1.16.x) nach mdm 1.17.x migrieren.

Die Installation und der Betrieb von mdm 1.17.x in der virtuellen Maschine wird im Anwenderhandbuch „mdm 1.17.x in der mdm-VA verwenden“ (UM DE MDM VA - 110903_de_xx) ausführlich beschrieben. (Download unter: phoenixcontact.net/product/2981974.)

Systemanforderungen der mdm-VA:

– Arbeitsspeicher (RAM): min. 4096 MB
– Festplattenspeicher: min. 10 GB

Systemanforderungen mdm-Client:

– Betriebssystem: Ubuntu / Windows
– Java-Plattform (JRE): *OpenJDK 11* oder neuer
– Arbeitsspeicher (RAM): min. 512 MB / Festplattenspeicher: min. 500 MB

2.1.4 Ubuntu 22.04 LTS Server (nativ)

Neben der Installation von mdm 1.17.x unter dem Betriebssystem Ubuntu in der mdm-VA (siehe Kapitel 2.1.3) ist es ebenfalls möglich, mdm 1.17.x unter dem nativen Betriebssystem Ubuntu 22.04 (Server) zu installieren.

Grundsätzlich müssen dazu folgende Schritte ausgeführt werden:

1. Ubuntu 22.04 (Server) herunterladen und installieren.
2. Benutzer *vadmin* anlegen.
3. Programm *sudo* verfügbar machen.
4. mdm-Repository verfügbar machen.
5. *mdm-cockpit* installieren.
6. mdm 1.17.x installieren.
7. mdm-Datenbanken von mdm (1.13.x bis 1.16.x) nach mdm 1.17.x migrieren.

Gehen Sie wie folgt vor (erfordert Root-Rechte):

Ubuntu 22.04 (Server) herunterladen und installieren

- Installieren Sie Ubuntu 22.04 (Server).
- Legen Sie nach Möglichkeit bereits während der Installation den Benutzer *vadmin* mit der *User-ID* 1000 an.
- Melden Sie sich auf dem Ubuntu-Betriebssystem an.
- Aktualisieren Sie das System:
  – `apt update && apt upgrade`

Benutzer „vadmin“ gegebenenfalls verfügbar machen (erfordert Root-Rechte)

- Prüfen Sie, ob der Benutzer *vadmin* bereits auf dem System vorhanden ist:
  – Melden Sie sich als Benutzer *vadmin* an.
  – Prüfen Sie die user ID des Benutzers *vadmin:*
    `id -a`
    Der Befehl müsste folgende Antwort zurückgeben: `uid=1000(vadmin)`
- Je nachdem, ob der Benutzer vorhanden ist, müssen Sie eine der folgenden Maßnahmen ausführen:

1. Wenn der Benutzer *vadmin* mit der *User-ID 1000* vorhanden ist, fahren Sie fort im Kapitel “Das Programm „sudo“ verfügbar machen” .
2. Wenn der Benutzer *vadmin* vorhanden ist, aber **nicht** die *User-ID* 1000 besitzt, weisen Sie ihm die *User-ID* 1000 wie folgt zu:
   – `usermod --uid 1000 vadmin`
   – Fahren Sie fort im Kapitel “Das Programm „sudo“ verfügbar machen” .

3. Wenn ein anderer Benutzer (example-user) mit der *User-ID* 1000 auf dem System vorhanden ist, führen Sie **eine** der folgenden Maßnahmen durch:
   a) Entfernen Sie den Benutzer.
   – Fahren Sie fort mit Punkt 4 (siehe unten).
   b) Oder ändern Sie die *User-ID* des Benutzers in eine andere als 1000:
   – `usermod --uid 2000 example-user`
   – Fahren Sie fort mit Punkt 4 (siehe unten).
   c) Oder benennen Sie den Benutzer in *vadmin* um:
   – `id example-user`
   `uid=1000(example-user)`
   – `usermod -d /home/vadmin -m -c vadmin -l vadmin example-user`
   – `id vadmin`
   `uid=1000(vadmin)`
   – Fahren Sie fort im Kapitel “Das Programm „sudo“ verfügbar machen” .
4. Wenn der Benutzer *vadmin* **nicht** auf dem System vorhanden ist, legen Sie ihn an:
   – `useradd --home-dir /home/vadmin --create-home --uid 1000 --user-group vadmin`
   – Fahren Sie fort im Kapitel “Das Programm „sudo“ verfügbar machen” .

Das Programm „sudo“ verfügbar machen

- Prüfen Sie, ob das Programm *sudo* installiert ist:
  – `dpkg -l sudo`
- Wenn *sudo* **nicht** installiert ist, gehen Sie wie folgt vor (Root-Rechte):
  – `apt install sudo`
  – `visudo`
  Fügen Sie folgenden Eintrag am Ende der Datei *sudoers* hinzu:
  ```
  # User rules for vadmin
  vadmin ALL=(ALL) NOPASSWD:ALL
  ```
  Speichern Sie die Datei.
  – Testen Sie, ob der Benutzer *vadmin* den Befehl *sudo* verwenden kann:
  `sudo cat /etc/sudoers` (als Benutzer *vadmin* anmelden und ausführen)

mdm-Repository verfügbar machen

- Melden Sie sich als Benutzer *vadmin* an.
- Erstellen Sie das Verzeichnis, in dem die Repository-Schlüssel abgelegt werden:
  – `sudo mkdir -p /etc/apt/keyrings`
- Machen Sie den mdm-Repository-Schlüssel auf dem System verfügbar:
  – `curl -s -S -O https://repositories.mguard.com/pubkey.gpg`
- Prüfen Sie den Fingerabruck des öffentlichen Schlüssels (*public key*):
  – `gpg -finger pubkey.gpg`
  – Der Fingerabdruck muss folgenden Wert haben:
  AD3E B1F9 473D 5CC7 2ED4 2D4C 0571 79A3 CC0F FA55
- Speichern Sie den öffentlichen Schlüssels (*public key*):
  `sudo gpg --dearmor --yes -o /etc/apt/keyrings/mdm.gpg pubkey.gpg`
- Machen Sie das mdm-Repository mit den Schlüsseln verfügbar:

- `echo "deb [signed-by=/etc/apt/keyrings/mdm.gpg] http://repositories.mguard.com/mdm <version>/" | sudo tee /etc/apt/sources.list.d/pxccs.list`

Basiskomponente und WBM für die mdm-VA „mdm-cockpit“ installieren

- Aktualisieren Sie die Software-Repositorys (Ubuntu und mdm):
  - `sudo apt update`
- Entfernen Sie alle Dateien im Verzeichnis */etc/netplan* oder ändern Sie jeweils deren Dateiendung von *.yaml* in eine andere Dateiendung.
- Installieren Sie die Basiskomponete *mdm-cockpit*:
  - `sudo apt install mdm-cockpit`
- Starten Sie das System neu:
  - `sudo reboot`

mdm 1.17.x unter Ubuntu 22.04.LTS (Server)

- Installieren Sie die gewünschten mdm-Komponenten wie im Anwenderhandbuch zur mdm-VA beschrieben (siehe 110903_de_xx unter phoenixcontact.net/product/2981974):
  - Zum Beispiel mit dem Befehl: `pxccs-install-mdm`

mdm-Datenbanken von mdm (mdm 1.13.x bis 1.16.x) nach mdm 1.17.x migrieren

- Gehen Sie vor, wie im Anwenderhandbuch 110903_de_xx beschrieben (siehe phoenixcontact.net/product/2981974).

3 Vorkonfigurationen

3.1 Die mGuard-Geräte vorkonfigurieren

Führen Sie zur Inbetriebnahme und Konfiguration des Geräts (IP-Adressen der Schnittstellen usw.) die im unter phoenixcontact.net/products verfügbaren Anwenderhandbuch „Installation und Inbetriebnahme der mGuard-Hardware“ beschriebenen Schritte durch.

Weiterführende Informationen finden Sie im Software-Referenzhandbuch „Konfigurieren der mGuard Security-Appliances“, das unter phoenixcontact.net/products zur Verfügung steht.

SSH-Zugang aktivieren

Der mdm installiert die Konfigurationsdateien auf den mGuards mittels SSH. Daher muss auf den mGuards der SSH-Zugang erlaubt werden, wenn der mdm zum Hochladen der Konfiguration die externe (nicht vertrauenswürdige) Schnittstelle verwendet.

Wählen Sie im Menü der Web-Benutzeroberfläche *Verwaltung >> Systemeinstellungen >> Shell-Zugang* und aktivieren Sie den *SSH-Fernzugang*. Weiterführende Informationen zum *SSH-Fernzugang (SSH Remote Access)* finden Sie in den *Referenzhandbüchern für mGuard*.

Achten Sie darauf, dass Sie bei der Aktivierung des Fernzugriffs für Standard-Admin und Root sichere Passwörter verwenden.

mdm verwendet zur Anmeldung am mGuard das Administratorpasswort. Ändern Sie bei lokaler Änderung des Passworts am Gerät die Passworteinstellung in mdm entsprechend über die Option **Set Current Device Passwords** im Kontextmenü der Geräte-Übersicht. Andernfalls kann sich mdm nicht am Gerät anmelden.

Das aktuelle Root-Passwort ist Bestandteil der Konfigurationsdatei. Ändern Sie bei lokaler Änderung des Passworts am Gerät die Passworteinstellung in mdm entsprechend. Andernfalls weist der mGuard die Konfiguration zurück.

3.2 HTTPS Configuration-Pull-Server vorkonfigurieren

Zur Übertragung von Informationen zum Konfigurationszustand eines mGuard muss der HTTPS-Pull-Server SYSLOG-Meldungen an den mdm-Server absenden (Rückmeldungen ziehen – *pull feedback*).

Achten Sie darauf, dass die Kommunikation zwischen HTTPS-Server und mdm-Server sowie zwischen HTTPS-Pull-Server und den mGuards nicht durch eine Firewall oder ein NAT-Gerät blockiert wird.

4 mdm-Server und mdm-Client

4.1 mdm-Server unter Ubuntu starten

	mdm 1.17.x in der mdm-VA / Ubuntu 22.04 LTS
Starten	
mdm-Server	`sudo systemctl start mdm-server`
mdm-CA-Server	`sudo systemctl start mdm-ca`
Stoppen	
mdm-Server	`sudo systemctl stop mdm-server`
mdm-CA-Server	`sudo systemctl stop mdm-ca`

4.2 mdm-Client unter Windows verwenden

Voraussetzung:

– Die Java-Laufzeitumgebung *OpenJDK 11* oder neuer ist auf dem Windows-System installiert.

– Die mdm-Komponente *mdm-clientdownload* ist in der mdm-VA installiert.

Um den mdm-Client auf einem Windows-System zu verwenden, gehen Sie wie folgt vor:

- Verbinden Sie sich mit dem mdm-Webserver unter der konfigurierten IP-Adresse:
  https://<IP-Adresse>/mdm
  – Die Datei *mdm-client.zip* wird zum Download angeboten.
- Entpacken Sie die zip-Datei auf dem Windows-System.
- Starten Sie den mdm-Client mit einem Doppelklick auf die Datei *mdm-client-1.17.x.jar*.
  Alternativ könne Sie das Programm mit folgendem Befehl über die Kommandozeile starten (z. B.): **`java -Xmx512m -jar mdm-client-1.17.0.jar`** .

5 mdm-Client – Übersicht

Der mdm-Client ist die grafische Benutzeroberfläche für den Zugriff auf alle Funktionen des mdm. Er dient der Erstellung und Verwaltung von Geräten, Templates, Pools und VPN-Gruppen sowie zum Hochladen von Konfigurationen auf Geräte und zum Export der Konfigurationsdateien in das Dateisystem.

Informationen zum Hochfahren und Anhalten des Clients siehe „mdm-Server und mdm-Client“ auf Seite 15.

5.1 Anmeldung

Bevor Sie sich mit dem Server verbinden können, müssen Sie sich im Anmeldefenster authentifizieren. Im Eingabefeld „Hostname“ müssen Sie die IP-Adresse/den Hostnamen des Servers (der mdm-VA) eingeben. Außerdem kann der vom Benutzer zu verwendende Server-Port im Anmeldefenster angegeben werden.

Bild 5-1 Anmeldefenster des mdm-Clients

Drei Benutzerkonten sind voreingestellt: *root*, *admin* und *audit*. Der Benutzer *root* hat Zugriff auf alle Einstellungen, *admin* kann standardmäßig alle Konfigurationseinstellungen ändern und Einstellungen in der Benutzerverwaltung lesen, während *audit* ab Werk nur über eine Leseberechtigung verfügt. Das heißt, ein *audit*-Benutzer kann keine Einstellungen außer dem eigenen Passwort ändern. Die Benutzerberechtigungen können geändert werden, falls dies gewünscht ist (siehe „Benutzer, Rollen und Berechtigungen verwalten“ auf Seite 115). Werkseitig ist für *admin* das Passwort **admin** eingerichtet, für *audit* das Passwort **audit** und für *root* lautet das Passwort **root**.

Es wird dringend empfohlen, die Standardpasswörter nach der Installation zu ändern (siehe hierzu auch „Benutzer, Rollen und Berechtigungen verwalten“ auf Seite 115).

Mehrere Clients verwenden

Die gleichzeitige Verwendung einer mdm-Serverinstanz durch mehrere mdm-Clients wird nur durch die Version *mdm Unlimited Edition* voll unterstützt. Alle übrigen verfügbaren Ausgaben sind noch auf die Verwendung von zwei Clients gleichzeitig beschränkt. Um zu verhindern, dass zwei Benutzer gleichzeitig die gleiche Variable bearbeiten, können

Entitäten gesperrt werden. Dies schließt Vererbungshierarchien ein (bei denen ein Benutzer auch eine Variable bearbeiten kann, die ein abstammendes Template oder ein Gerät erbt), allerdings keine synthetisierten VPN-Verbindungen (auf die im empfangenden Gerät nur Lesezugriff besteht). Versucht ein anderer Benutzer, das Gerät oder das Template zu öffnen, wird eine Fehlermeldung angezeigt. Öffnet ein Client einen *Template properties dialog* (Template-Eigenschaften), werden das Template und alle mit diesem Template verbundenen Geräte gesperrt und können durch andere Benutzer nicht geöffnet werden.

Das gleiche gilt auch für Pools und VPN-Gruppen.

Falls die Verbindung zwischen Client und Server unterbrochen ist und nicht ordnungsgemäß beendet werden kann, werden die von diesem Client gesperrten Geräte/Templates/Pools/VPN-Gruppen nach einer Zeitabschaltung wegen Inaktivität wieder freigegeben (kann in der Serverkonfiguration eingerichtet werden, siehe „mdm-Server (Datei *preferences.xml)“ auf Seite 161*, Schlüssel *maxInactiveInterval*). Bis diese Zeitabschaltung erfolgt, kann möglicherweise nicht auf alle Einstellungen zugegriffen werden, bis die Zeitabschaltung wirksam wird.

5.2 mdm Hauptfenster

Der nachfolgende Screenshot zeigt das mdm Hauptfenster:

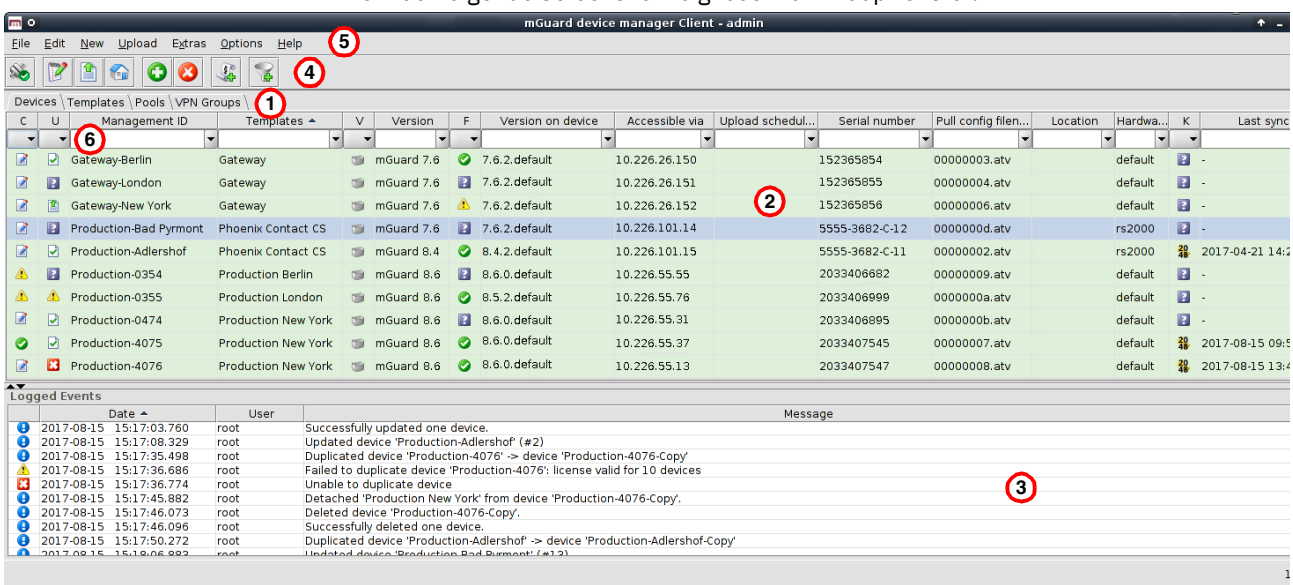


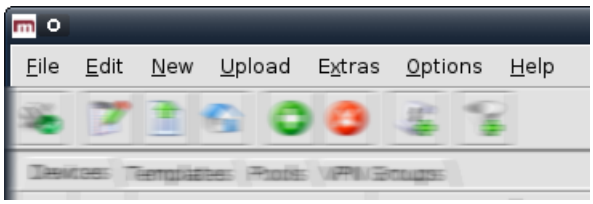
Bild 5-2 mdm Hauptfenster

Das mdm Hauptfenster gliedert sich in einen **Tab-Bereich** ① zum Öffnen der **Übersichtstabellen** für Geräte/Templates/Pool und VPN-Gruppen (z. B. ②) sowie ein **Protokollfenster** ③.

Darüber hinaus weist es eine **Symbolleiste** ④ und das **Hauptmenü** ⑤ auf. Nach entsprechender Aktivierung können die Einträge in den verschiedenen Spalten durch Eingabe eines beliebigen Terms in die Textfelder gespeichert werden⑥.

In den nächsten Kapiteln werden die einzelnen Bereiche und deren Funktionen beschrieben.

5.2.1 mdm Hauptmenü



Das mdm Hauptmenü weist folgende Menüpunkte auf.

Das mdm Hauptmenü		
File	**Connect to Server/Disconnect from Server**	Verbindung zum Server herstellen oder trennen.
	Exit	Client verlassen.
Edit	**Edit Item**	Den *Properties Dialog* für die Auswahl (Gerät, Template, Pool oder VPN-Gruppe) in der Übersichtstabelle öffnen.
	Web Configure	Webinterface für die in der Gerätetabelle ausgewählten Geräte öffnen. Nur aktiv, wenn in der Gerätetabelle mindestens ein Gerät ausgewählt wurde. Für diese Option ist der **Zugriff über Adresse** notwendig. Dieser kann unter **General settings** im *Device properties dialog* (Geräte-Eigenschaften) konfiguriert werden (siehe Kapitel 6.3.3).
	Cut	Markierten Text im aktiven Tabellenfilterfeld ausschneiden und in die Zwischenablage kopieren.
	Copy	Markierten Text im aktiven Tabellenfilterfeld in die Zwischenablage kopieren.
	Paste	Inhalt der Zwischenablage in das aktive Tabellenfilterfeld einfügen.
	Select All	Alle Einträge in der aktiven Übersichtstabelle markieren.
New	**Device**	Neues Gerät erstellen und *Device properties dialog* (Geräte-Eigenschaften) öffnen.
	Template	Neues Template erstellen und *Template properties dialog* (Template-Eigenschaften) öffnen.
	Pool	Neuen Pool erstellen und *Pool properties dialog* (Pool-Eigenschaften) öffnen.
	VPN Group	Neue VPN-Gruppe erstellen und *VPN group properties dialog* öffnen (VPN-Gruppe-Eigenschaften).

Das mdm Hauptmenü		

	Device Import	Fenster zur Auswahl einer Importdatei öffnen.
		
		Über Device Import können Sie eine automatisch (mittels Skript) generierte Gerätedatei importieren. Damit kann eine große Anzahl Geräte in mdm erstellt werden, ohne dass der Vorgang manuell durchgeführt werden muss.
		
		Für die Importdatei ist eine CSV-Formatierung (*comma-separated value*) erforderlich. Als Trennzeichen können Komma (,) oder Semikolon (;) verwendet werden. Jeder Eintrag (Zeile) in der Datei beschreibt ein einzelnes Gerät und besteht aus folgenden Feldern:
		
		Feld > Beschreibung
		
		#0 > Verwaltungs-ID
		
		#1 > Firmwareversion
		
		#2 > Name des Templates
		
		#3 > Erreichbar über" Adresse
		
		#4 > Seriennummer
		
		#5 > Flash-ID
		
		#6...#n > Variable Zuweisungen
		
		Verwaltungs-ID und Firmwareversion (Felder #0 und #1) sind Pflichtfelder, alle übrigen Felder sind optional. Bei einem leeren oder nicht vorhandenen Feld ist das entsprechende Attribut nicht gesetzt.
		
		Als Firmwareversion muss eine unterstützte Firmwareversion (ohne Patchlevel) angegeben werden, wie sie in der Versionsspalte der Geräte-Übersicht angezeigt wird, z. B. mGuard 6.1.
		
		Als Name des Templates muss entweder der Name eines vorhandenen Templates angegeben werden, das dem neuen Gerät zugewiesen ist, oder das Feld bleibt frei. In diesem Fall wird kein Template zugewiesen.
		
		Skalare Variablen (d.h. Variablen, die einen Einzelwert speichern und nicht in einer Tabelle enthalten sind) können in der folgenden Form mit einer Zuweisung gesetzt werden: *<VARIABLE_NAME>=<VALUE>*.
		
		Beispieleintrag:
		
		`My Device,mGuard 6.1,,192.168.2.3,17X46201,,`
		`ROUTERMODE=router,MY_LOCAL_IP=192.168.2.3`
		
		(Hinweis: Der Eintrag muss sich in einer einzigen Zeile befinden.)
		
		Ungültige Einträge werden übersprungen und führen zur Protokollierung einer Fehlermeldung.

Das mdm Hauptmenü		
	Import ATV & Create Device	Neues Gerät mit ausgewählter ATV-Konfiguration erstellen. Die Firmware-Version für das Gerät wird aus der ATV-Konfiguration übernommen.
	Import X.509 Certificates	Zertifikate importieren, die während der manuellen Zertifikatregistrierung erstellt wurden (nähere Informationen siehe „Maschinenzertifikate“ auf Seite 120).
Upload	Übersicht des Upload-Prozesses der Konfiguration und die verschiedenen Methoden zum Upload siehe „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107.	
	Selected	Konfigurationen in die in der Gerätetabelle ausgewählten Geräte hochladen.
	Changed	Konfigurationen in Geräte mit Konfigurationsstatus *out-of-date* hochladen.
	All	Konfigurationen in alle Geräte hochladen.
Extras	**Manage Device Licenses...**	Ihre Gerätelizenzen und Voucher verwalten.
	Manage License Vouchers...	Informationen zur Verwaltung von Lizenzen und Vouchern siehe „Gerätelizenzen und Voucher verwalten“ auf Seite 112.
	Manage Profile Keys	Ihre Profilschlüssel verwalten.
		Informationen zur Verwaltung von Profilschlüsseln siehe „Profilschlüssel verwalten“ auf Seite 110.
	Change Own Password	Dialog zum Ändern des eigenen Passworts durch den aktuellen Benutzer öffnen.
	Manage Users And Roles	Benutzer und Rollen verwalten.
		Informationen zur Verwaltung von Benutzern und Rollen siehe „Benutzer, Rollen und Berechtigungen verwalten“ auf Seite 115.
Options	**Default Browser**	Geben Sie eine Kommandozeile zur Verwendung für den Start des Browsers ein. Die Kommandozeile sollte mit dem kompletten Pfad und dem Namen der Binärdatei beginnen. Fügen Sie den String *{url}* hinzu, der durch die URL des mGuard ersetzt wird, geben Sie beispielsweise unter Windows Folgendes ein:
		C:\Program Files\Firefox\Firefox.exe {url}
	Default Firmware Version	Für die Erstellung eines neuen Geräts oder Templates verwendete Firmwareversion.
	Disable Filtering	Die Filter in den Tabellen für Gerät, Template, Pool und VPN-Gruppe aktivieren und deaktivieren.
Help	**About...**	Informationen zur aktuell installierten Version und enthaltenen Software von Drittanbietern anzeigen.
	mdm User Manual	Das *mdm Anwenderhandbuch* in einem Internetbrowser öffnen (Internetverbindung erforderlich).
	mdm Server License...	Installierte mdm Lizenz anzeigen.

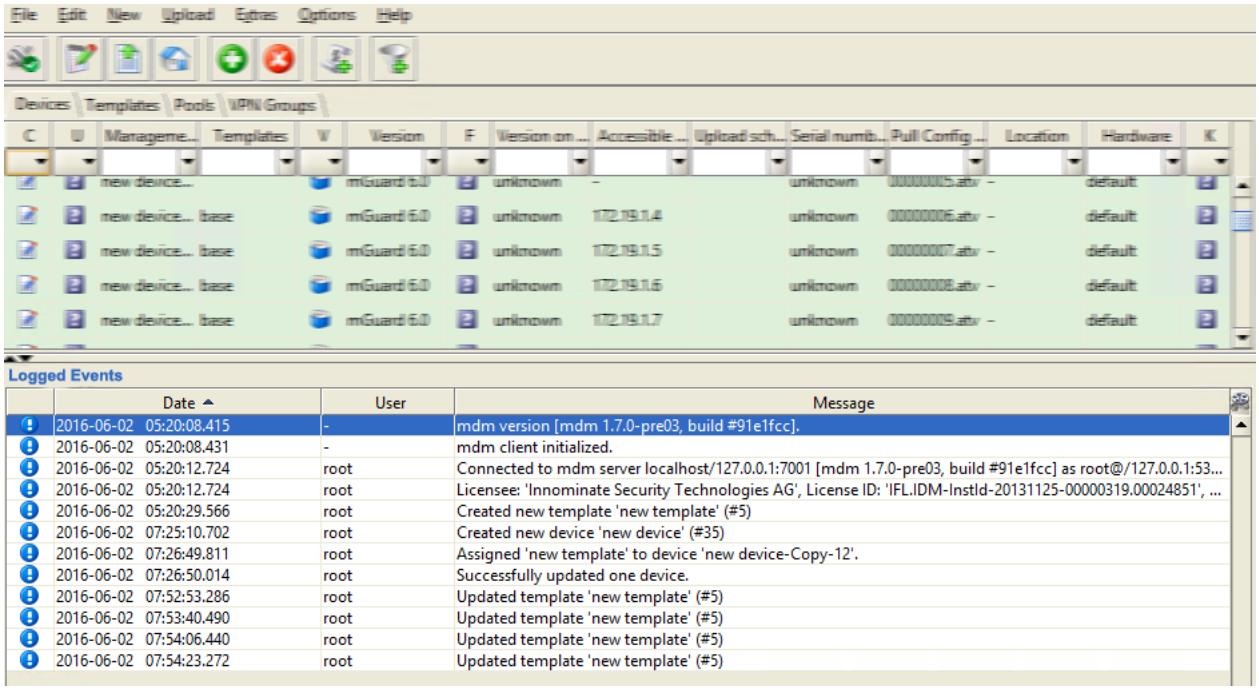
5.2.2 mdm Symbolleiste

Die Symbolleiste enthält Verknüpfungen zu einigen Funktionen des Hauptmenüs oder Kontextmenüs.

Die mdm Symbolleiste

	Keine Verbindung zum Server; Verbindung wird durch Anklicken hergestellt.
	Verbindung hergestellt; Verbindung wird durch Anklicken unterbrochen.
	Ausgewählten Eintrag bearbeiten (Gerät, Template, Pool oder VPN-Gruppe).
	Konfiguration in ausgewählte Geräte hochladen.
	Konfiguration in ausgewählte Geräte hochladen.
	Webinterface der in der Gerätetabelle ausgewählten Geräte öffnen.
	Aktuell ausgewählte Einträge löschen.
	Dialog öffnen, um Lizenzen vom Lizenzserver für die ausgewählten Geräte zu erstellen/anzufordern.
	Eintrag (Gerät, Template, Pool oder VPN-Gruppe) hinzufügen und entsprechenden *Properties Dialog* öffnen.
	Filter der aktuellen Übersichtstabelle (Gerät, Template, Pool oder VPN-Gruppe) ist aktiv. Filter wird durch Anklicken deaktiviert.
	Filter der aktuellen Übersichtstabelle (Gerät, Template, Pool oder VPN-Gruppe) ist nicht aktiv. Filter wird durch Anklicken aktiviert.

5.3 Protokollfenster



Im Protokollfenster werden verschiedene Ereignisse angezeigt, zum Beispiel:

- Ergebnisse von Uploads.
- Erstellen, Löschen, Ändern von Geräten, Templates, Pools, VPN-Gruppen, Benutzern oder Rollen.
- Verbindung zum Client herstellen oder trennen.

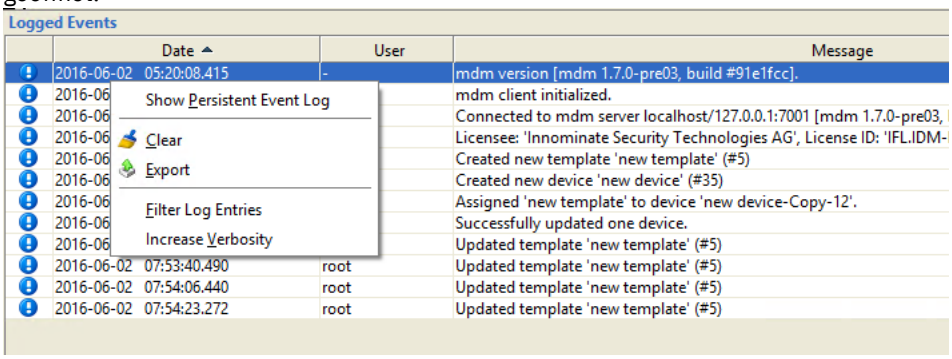
Für jedes Ereignis werden Schweregrad, Datum und Uhrzeit, Benutzername und eine Meldung protokolliert. Bei Ereignissen, die nicht auf Aktionen eines Benutzers zurückzuführen sind, wird anstelle des Benutzernamens „–“ protokolliert. Mit einem Doppelklick auf einen Protokolleintrag wird ein Fenster mit Detailinformationen geöffnet.

Tabelle sortieren

Mit der Kopfzeile der Tabelle können die Einträge sortiert werden. Durch Anklicken der Kopfzeile einer Spalte wird die (primäre) Sortierung anhand dieser Spalte aktiviert. Dies wird durch einen Pfeil in der Kopfzeile angezeigt. Durch einen zweiten Klick auf dieselbe Kopfzeile erfolgt die Sortierung in umgekehrter Reihenfolge. Durch Anklicken einer weiteren Spalte wird anhand dieser neuen Spalte sortiert, wobei die vorher aktive Spalte als Sekundärkriterium für die Sortierung herangezogen wird.

5.3.1 Kontextmenü

Das Kontextmenü wird durch Anklicken des Protokollfensters mit der rechten Maustaste geöffnet.



Sie können folgende Aktionen durchführen.

Kontextmenü Protokollfenster	
Show Persistent Event Log	Fenster „Persistent Event Log“ öffnen (siehe „Persistent Event Log“ auf Seite 25).
Clear	Protokolleinträge löschen. Dies gilt nur für den aktuellen mdm-Client, d. h. andere Clients sind nicht betroffen.
Export	Fenster zur Dateiauswahl öffnen und Protokolleinträge in eine XML-Datei exportieren.
Filter Log Entries	Filter für die Tabelle der Protokolleinträge aktivieren oder deaktivieren. Bei aktiviertem Filter wird in der ersten Tabellenzeile die Eingabe regulärer Ausdrücke akzeptiert (siehe Kapitel 11, *Regular expressions*), die zum effizienten Filtern der Tabelleneinträge verwendet werden können.
Increase Verbosity	Ausführliche Protokollierung aktivieren oder deaktivieren. Wenn die ausführliche Protokollierung (verbose logging) aktiviert ist, werden auch Ereignisse protokolliert, die nicht hilfreich sind und möglicherweise zu Verwirrung führen.

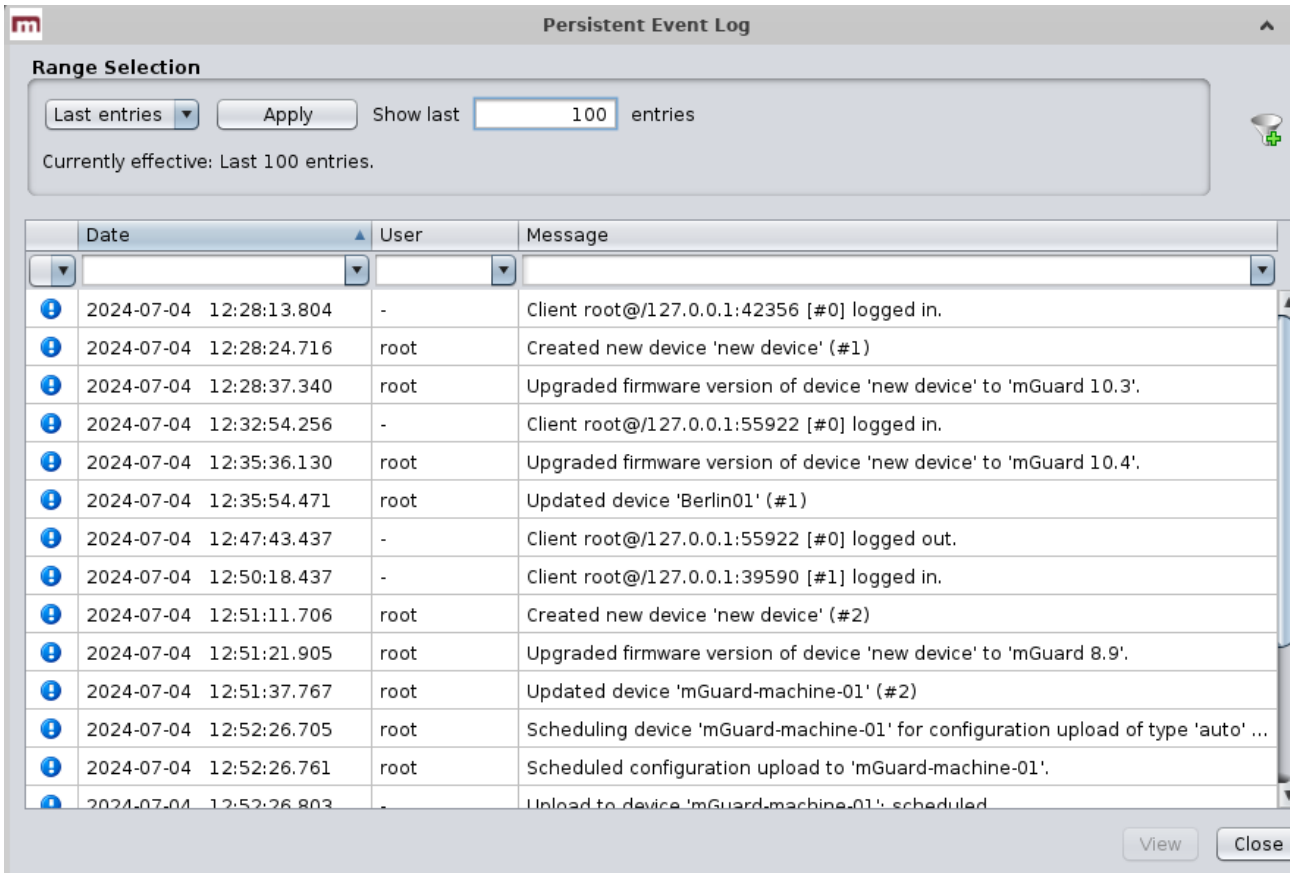
Auto-scrolling

Bei Protokollierung eines neuen Ereignisses erfolgt im Protokollfenster ein automatischer Bildlauf nach unten, sodass der neue Eintrag generell sichtbar ist. Der automatische Bildlauf kann durch Anklicken des Symbols in der  oberen rechten Ecke des Protokollfensters abgeschaltet und erneut aktiviert werden.

5.3.2 Persistent Event Log

Im Fenster „Persistent Event Log“ werden ausgewählte Ereignisse der letzten 200 Tage auf die gleiche Weise wie im Protokollfenster angezeigt. Im Gegensatz zu den Ereignissen im Protokollfenster werden die Einträge im Fenster „Persistent Event Log“ dauerhaft in der mdm Datenbank gespeichert, sie bleiben also auch nach einem Neustart des mdm-Servers erhalten.

Die Anzahl der Tage, nach der die Einträge in der Datenbank ablaufen (Standard: 200 Tage), kann in der Datei *preferences.xml* (Node *event*) konfiguriert werden.



Range selection

Da die Anzahl dauerhaft gespeicherter Protokolleinträge sehr hoch sein kann, werden beim Öffnen des Dialogfensters nicht alle Einträge automatisch vom mdm-Server geladen. Durch die Änderung der Kriterien unter „Range Selection“ und das Klicken auf „Apply“ werden die für die angegebenen Kriterien passenden Einträge geladen.

Mit der Werkseinstellung werden die letzten (also aktuellsten) 100 Einträge geladen.

Das Persistent Event Log		
	All Entries	Alle Protokolleinträge laden. Bei einer großen Anzahl von Einträgen (1000 oder mehr) kann das Laden der Einträge einige Zeit dauern.
	Time Range	Alle Einträge laden, die in einem bestimmten Zeitraum erstellt wurden. Dieser Zeitraum wird wie folgt angegeben: – Bei Angabe eines unteren, jedoch keines oberen Grenzwertes werden alle Einträge geladen, die aktueller als der untere Grenzwert sind. – Bei Angabe eines oberen, jedoch keines unteren Grenzwertes werden alle Einträge geladen, die älter als der obere Grenzwert sind. – Werden sowohl ein unterer als auch ein oberer Grenzwert angegeben, werden alle Einträge geladen, die in dem genannten Zeitraum erstellt wurden. Datumsangaben erfolgen im ISO-Format (JJJJ-MM-TT, wobei JJJJ das Jahr, MM den Monat dieses Jahres zwischen 01 und 12 und TT den Tag dieses Monats zwischen 01 und 31 bezeichnet). Optional kann eine ISO-Zeitangabe folgen (hh:mm:ss, wobei hh die Stunde im 24-Stunden-Format, mm die Minute und ss die Sekunde bezeichnet). Viertel fünf und 20 Sekunden am Nachmittag des 22. Dezember 2010 würde beispielsweise wie folgt dargestellt: 2010-12-22 16:15:20. Alternativ können Sie durch Anklicken des Symbols ein Datum aus dem Kalender auswählen.
	Last Entries	Letzte (neueste) Einträge laden. Die Anzahl der Einträge muss angegeben werden.

5.3.3 Protokollieren von Ereignissen mit syslog

Die gleichen Ereignisse, die im Dauerprotokoll (Persistent Log) protokolliert sind (siehe „Persistent Event Log“ auf Seite 25) oder eine nach Schweregrad ausgewählte Teilmenge können an einen syslog-Server übermittelt werden (siehe „mdm-Server (Datei *preferences.xml)“ auf Seite 161*).

5.4 Hardwarekonfigurationen

5.4.1 FL MGUARD RS2000

Die meisten mGuard-Geräte unterstützen unabhängig von der Hardware die gleichen Konfigurationsvariablen. Geräte der Serie FL/TC MGUARD (RS)2000 unterstützen jedoch nur einen begrenzten Satz Variablen. In mdm ist es möglich, diese Geräte über den Hard-

ware-Konfigurationsmechanismus *rs2000* zu verwalten. Wird die Hardwarekonfiguration *rs2000* und nicht *default* ausgewählt, werden Variablen, die von dieser Plattform nicht unterstützt werden, weggelassen.

Voraussetzungen: mGuard-Firmware-Version 7.5.0 oder höher muss installiert und die Funktion „Redundanz“ muss deaktiviert sein.

Templates verfügen nicht über eine Hardwarekonfiguration. Sie enthalten stets alle Variablen, die der Hardwarekonfiguration *default* entsprechen. Für Geräte mit der Hardwarekonfiguration *rs2000* gilt in diesem Fall:

Von einem Template geerbte Variablen, die von dem Gerät der Serie FL/TC MGUARD (RS)2000 nicht unterstützt werden, werden ignoriert.

Einige Variablen werden zwar auf FL/TC MGUARD (RS)2000-Geräten unterstützt, verfügen aber nur über einen begrenzten Bereich unterstützter Werte. Wird eine solche Variable durch ein auf die Konfiguration *rs2000* gesetztes Gerät geerbt und der geerbte Wert wird nicht unterstützt, so wird die Variable ungültig und muss im Konfigurationsdialog korrigiert werden, bevor sie auf das Gerät hochgeladen werden kann.

mdm 1.17.x unterstützt keine separate Hardwarekonfiguration für die Geräte der Serie TC MGUARD 2000, FL MGUARD RS2005 und FL MGUARD 2000. Bei diesen Geräten sollte die Hardwarekonfiguration *rs2000* im Netzwerkmodus „Router“ verwendet werden.

6 mdm-Client – Konfigurationsaufgaben

6.1 Allgemeine Bemerkungen

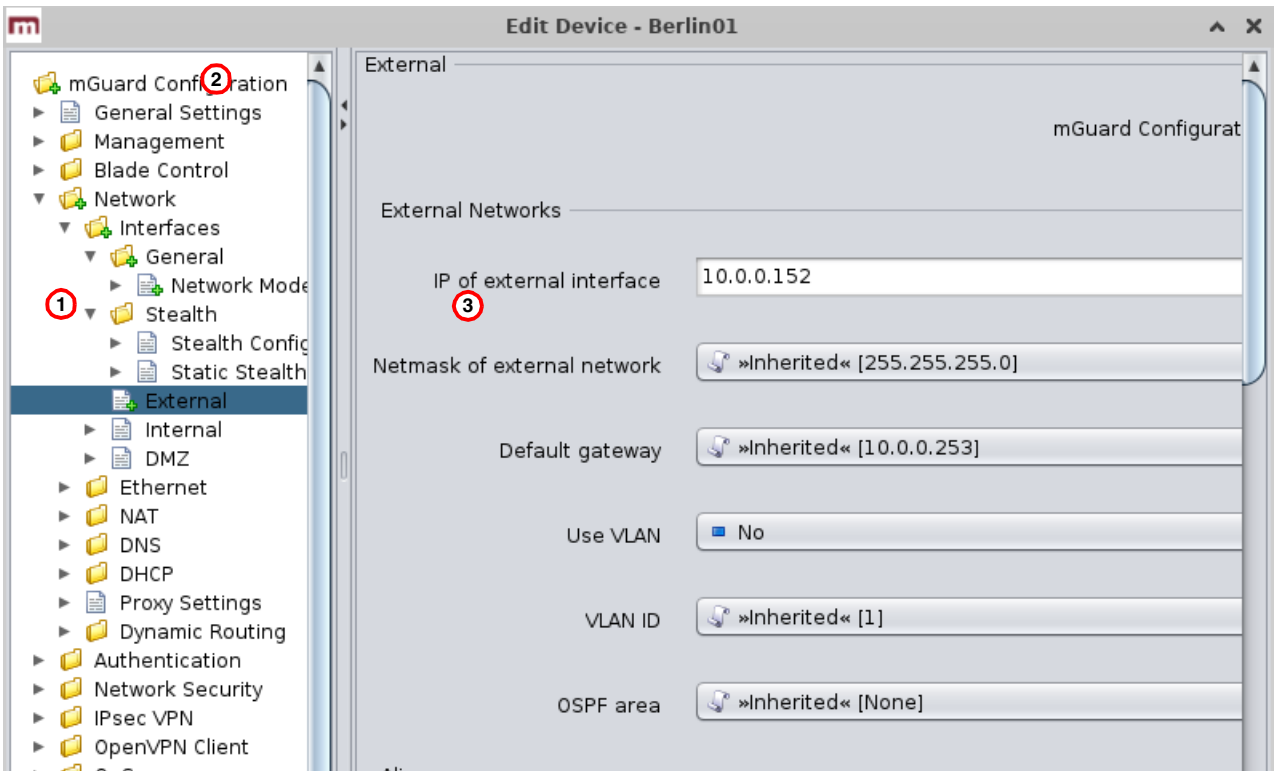
Der *Device properties dialog* (Geräte-Eigenschaften), der *Template properties dialog* (Template-Eigenschaften), der *Pool value properties dialog* (Pool-Eigenschaften), *sowie der VPN group properties dialog* (VPN-Gruppe-Eigenschaften) werden jeweils für die Konfiguration von Geräten, Templates, Pools bzw. VPN-Gruppen verwendet. Aufgrund der großen Ähnlichkeit des Geräte- und Template-Dialogs werden die gemeinsamen Teile in diesem Kapitel behandelt.

In Kapitel 6.3.3 und Kapitel 6.4.3 wird auf die Unterschiede zwischen den beiden Dialogen eingegangen. Die Konfiguration der Pools wird in Kapitel 6.5.3 beschrieben. Ausführliche Informationen zum Konzept von Template und Erbe finden Sie in Kapitel 6.4.5 („Mit Templates arbeiten“). Die Konfiguration der VPN-Gruppe wird in Kapitel 6.6.4 erläutert.

6.1.1 Navigationsbaum

Auf der linken Seite des Dialogs finden Sie den Navigationsbaum ①, der der Menüstruktur der Webinterface des mGuard ähnelt. Im Gegensatz zur Webinterface des mGuard enthält der Navigationsbaum jedoch zusätzlich den Eintrag **General Settings** ②, der Templates und Geräteparameter enthält, die ausschließlich in mdm verwendet werden.

Weitere Informationen zu den **General Settings** finden Sie in den folgenden Kapiteln.



Navigationsbaum Kontextmenü

Der Navigationsbaum verfügt auch über ein Kontextmenü, dass durch Anklicken des Baums mit der rechten Maustaste geöffnet wird. Das Kontextmenü enthält verschiedene Einträge zum Auf-/Einklappen von Teilen des Baumes. Darüber hinaus zeigt das Kontextmenü die wichtigsten Verknüpfungen zum Zugriff auf Menüpunkte.

Navigationsbaum Kontextmenü		
Focus on Subtree	Nur der Subtree des ausgewählten Knotens wird vollständig erweitert. Alle anderen aktuell erweiterten Knoten/Subtrees werden eingeklappt.	
Collapse All Other Nodes	Alle Knoten, die momentan nicht ausgewählt sind, werden eingeklappt.	
Scroll to Active Node	Wenn der aktuell ausgewählte Knoten noch nicht sichtbar ist, wird auf ihn fokussiert.	
Collapse	**Collapse All Nodes**	Alle Knoten werden eingeklappt.
	Collapse Selected Subtree	Der ausgewählte Subtree wird eingeklappt.
	Collapse Selected Node	Der ausgewählte Knoten wird eingeklappt. Die derzeit erweiterten Subtrees des Knotens werden wieder erweitert, wenn der Knoten erneut erweitert wird.
Expand	**Expand All Nodes**	Alle Knoten werden vollständig erweitert.
	Expand Selected Subtree	Der ausgewählte Subtree wird vollständig erweitert.
	Expand Selected Node	Der ausgewählte Knoten wird erweitert (nur eine Ebene).
	Focus on Here Defined Nodes	Alle Knoten mit Werten, die nicht vererbt werden, werden erweitert (d.h. Wertetypen, die auf custom oder local festgelegt sind).
	Focus on Inherited Nodes	Alle Knoten mit vererbten Werten werden erweitert.
	Focus on Incomplete Nodes	Alle Knoten mit vererbten "None" -Werten oder nicht erfüllten Poolreferenzen werden erweitert.

mGuard-Konfiguration

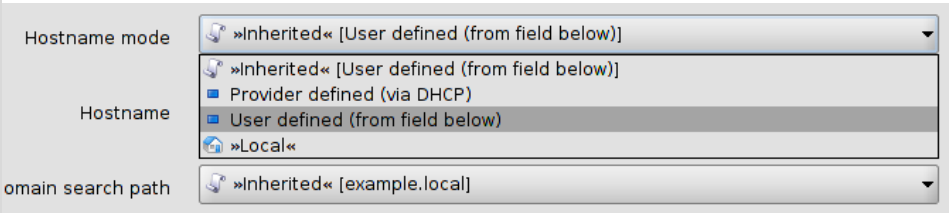
Mit dem Navigationsbaum kann bequem zwischen den Variablen des mGuard navigiert werden. Durch Anklicken eines „Blatts“ des Baumes werden die entsprechenden Variablen des mGuard sowie die dazugehörigen Einstellungen an der rechten Seite ③ des *Properties Dialogs* angezeigt.

6.1.2 Wertetypen von Variablen

Abhängig von der Variable können verschiedene Wertetypen ausgewählt werden (beispielhaft für den *Device properties dialog* (Geräte-Eigenschaften) dargestellt, siehe unten).

Verschiedene Wertetypen von Variablen

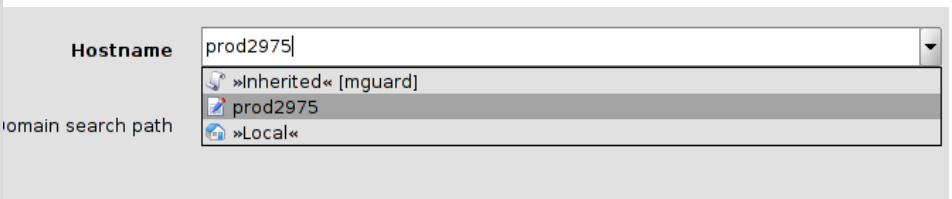
Variablen mit einem festen Wertesatz



Inherited	Setzen Sie die Variable auf den Standardwert oder auf den Wert, der in dem zugewiesenen Template (falls anwendbar) definiert ist. Auf die Verwendung von Templates und geerbten Werten wird in „Template-Eigenschaften (Template properties dialog)“ auf Seite 74 und „Mit Templates arbeiten“ auf Seite 80 eingegangen.
Local	Der mGuard unterstützt (unter anderem) zwei Rollen, den *Admin*, der alle Variablen des mGuard ändern kann, und den *Netadmin*, der nur lokale Variablen ändern kann. Der Wert für **Local** bestimmt, ob eine Variable lokal ist, d. h. ob sie durch den *Netadmin* am mGuard verwaltet werden kann. Zur Vermeidung von Konflikten zwischen mdm und dem *Netadmin* kann eine lokale Variable *nicht mehr durch mdm verwaltet* werden.
Fixed values	Eine Anzahl Fixed Values (feste Werte), die für diese Variable ausgewählt werden können. Welche Werte ausgewählt werden können, hängt von der Variablen ab. Im oben angegebenen Beispiel (siehe Abbildung) gibt es für die Variable **Hostname mode** die Fixed Values **Provider defined** und **User defined**.

Verschiedene Wertetypen von Variablen

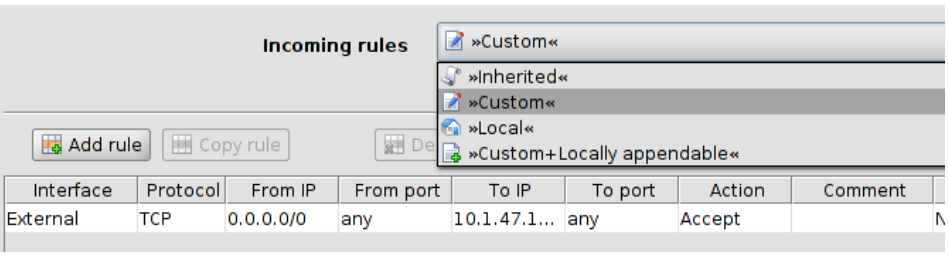
Variablen mit einem editierbaren Wert



Inherited	Siehe oben.
Local	Siehe oben.

Verschiedene Wertetypen von Variablen		
	Custom	Bei der Auswahl der Werteeingabe **Custom** wird die Combobox editierbar und Sie können einen spezifischen Wert für die Variable eingeben, beispielsweise **prod2975** im oben gezeigten Beispiel. Der eingegebene Wert wird daraufhin in der Combobox angezeigt und kann ausgewählt werden.

Verschiedene Wertetypen von Variablen		
Tabellenvariablen (z. B. Firewall-Regeln für eintreffende Daten)	Tabellenvariablen ermöglichen die folgenden Auswahlen (weitere Informationen zu Tabellen siehe „mGuard Tabellenvariablen ändern“ auf Seite 38).	



Inherited	Setzen Sie die Variable auf die Standardzeile oder auf die Zeile, die in dem zugewiesenen Template (falls anwendbar) definiert ist. Die geerbten Zeilen werden am Anfang der Tabelle in einer anderen Farbe dargestellt und können weder editiert noch ausgewählt werden. Auf die Verwendung von Templates und geerbten Werten wird in „Template-Eigenschaften (Template properties dialog)“ auf Seite 74 und „Mit Templates arbeiten“ auf Seite 80 eingegangen.
Local	Siehe oben. Wenn Sie eine Tabellenvariable auf **Local** setzen und mdm einen Fehler anzeigt, sollten Sie im Template (falls vorhanden) überprüfen, ob *May append* als Berechtigung eingerichtet ist. Ist *May append* im Template für die Tabelle als Berechtigung eingerichtet, können nur Zeilen im *Device Propterties Dialog* hinzugefügt werden. Die Auswahl von *Local* verursacht daher einen Fehler.

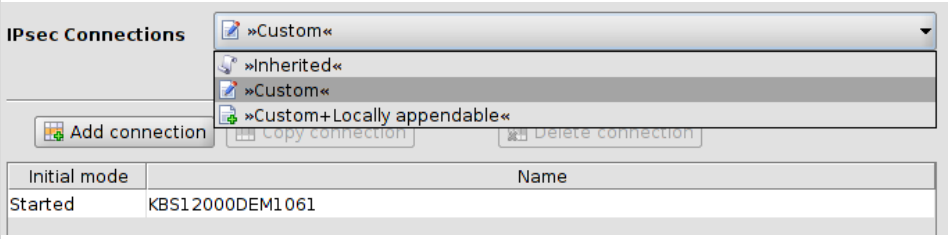
Verschiedene Wertetypen von Variablen		
	Custom	Bei Auswahl von **Custom** werden die Tabelle und die dazugehörigen Menüelemente aktiviert. In einem Template definierte Tabellenzeilen **können** vom Template in das Gerät kopiert werden. Sie können gelöscht oder editiert werden, oder neue Zeilen können im *Device properties dialog* (Geräte-Eigenschaften) hinzugefügt werden (gilt nur in bestimmten Fällen: siehe Punkt „Verhalten“ unten). Löschen oder Bearbeiten der Zeilen ändert nicht die Zeilen im Template. Sie können der Tabelle auch neue Zeilen hinzufügen. **Verhalten (Nur mit Berechtigung *May override*):** **Generell**: Normalerweise wird die Tabelle durch Umschalten von **Inherited** zu **Custom** vollständig überschrieben, d. h. der im Template definierte Tabelleninhalt wird auf dem Gerät *nicht behalten*, sondern es werden Standard-Tabellenzeilen eingerichtet (z. B. Firewall-Regeln für ausgehenden Datenverkehr). **Ausnahme**: Wenn die Tabelle nicht über eine Standardzeile verfügt (wenn sie z. B. leer ist), wird nach Wechseln von **Inherited** zu **Custom** der vom Template geerbte Tabelleninhalt der Einfachheit halber in die Tabelle **Custom** auf dem Gerät in Form neuer Zeilen kopiert (z. B. Firewall-Regeln für eingehenden Datenverkehr). **Workaround für den generellen Fall**: Im generellen Fall besteht die Möglichkeit, das Kopieren geerbter Tabellenzeilen zu erzwingen: Richten Sie die Tabelle als **Custom** ein, löschen Sie die Standard-Zeile(n), setzen Sie die Tabelle wieder auf **Inherited** und anschließend erneut auf **Custom**. In der damit erstellten **Custom**-Tabelle sind die Zeilen aus dem übergeordneten Template kopiert. Der Wechsel zwischen **Custom** und anderen Wertetypen ist ohne Datenverlust möglich. Wenn Sie jedoch von **Custom** auf, beispielsweise, **Inherited** wechseln und anschließend Ihre Einstellungen übernehmen und den Dialog verlassen, gehen alle eingegebenen Custom-Zeilen verloren.
	Custom + Locally appendable (nur *Device properties dialog* (Geräte-Eigenschaften))	Im Prinzip wie **Custom**, aber mit dieser Option kann der Benutzer *Netadmin* dem mGuard weitere Zeilen hinzufügen. (Die in mdm definierten Zeilen können nicht durch den Benutzer *Netadmin* am mGuard editiert oder gelöscht werden.)

Verschiedene Wertetypen von Variablen

Komplexe Tabellenvariablen (z. B. VPN-Verbindungen)

Anders als „normale“ Tabellenvariablen werden durch Hinzufügen oder Löschen von Zeilen von einer komplexen Tabellenvariablen zusätzlich Knoten am Navigationsbaum gelöscht oder hinzugefügt. Ein Beispiel für eine komplexe Tabellenvariable sind die VPN-Verbindungen: eine VPN-Verbindung wird durch eine Tabellenzeile in der Übersichtstabelle und einen zusätzlichen Knoten im Navigationsbaum dargestellt, in dem die Einstellungen für die Verbindung vorgenommen werden können. Hinweis: die Zellen komplexer Tabellen sind nicht editierbar, d. h. alle Einstellungen müssen in den Blättern der Knoten am Navigationsbaum vorgenommen werden.

Komplexe Tabellenvariablen ermöglichen die folgenden Auswahlen (weitere Informationen zu Tabellen siehe „mGuard Tabellenvariablen ändern“ auf Seite 38).



Inherited

Das Verhalten ist grundsätzlich das gleiche wie oben für die „normalen“ Variablen beschrieben. Wenn als komplexe Tabellenvariable **inherited** ausgewählt wird, sind alle Zeilen aus einem Template, die auch als Knoten im Navigationsbaum angezeigt werden, schreibgeschützt. Auf die Verwendung von Templates und geerbten Werten wird in „Template-Eigenschaften (Template properties dialog)“ auf Seite 74 und „Mit Templates arbeiten“ auf Seite 80 eingegangen.

Custom

Bei Auswahl von **Custom** werden die Tabelle und die dazugehörigen Menüelemente aktiviert. Im Gegensatz zu „normalen“ Tabellenvariablen werden die geerbten Tabellenzeilen beim Wechsel zu **Custom** *nicht* aus dem Template ins Gerät kopiert. Geerbte Zeilen können nicht gelöscht werden, aber nach Auswahl von **Custom** sind sie editierbar. Hinweis: Ändern oder Bearbeiten der Zeilen ändert nicht die Zeilen im Template. Sie können der Tabelle auch neue Zeilen (Knoten) hinzufügen.

Solange der *Properties Dialog* geöffnet ist, kann ohne Datenverlust zwischen **Custom** und anderen **Inherited** gewechselt werden. Wenn Sie jedoch von **Custom** auf **Inherited** wechseln und anschließend Ihre Einstellungen übernehmen und dann den Dialog verlassen, gehen alle eingegebenen Custom-Zeilen verloren.

Zusätzliche Konfiguration im Template

Im *Template properties dialog* (Template-Eigenschaften) finden Sie zusätzliche Einstellungen für die Variablen. Diese Einstellungen werden in „Template-Eigenschaften (Template properties dialog)“ auf Seite 74 erläutert.

6.1.3 Anzeige einer ungültigen Eingabe

Ungültige Eingaben werden sofort durch eine rote Bezeichnung der Variablen und Fehlersymbolen im Navigationsbaum angezeigt, wie in der folgenden Abbildung für die externe IP-Adresse dargestellt:

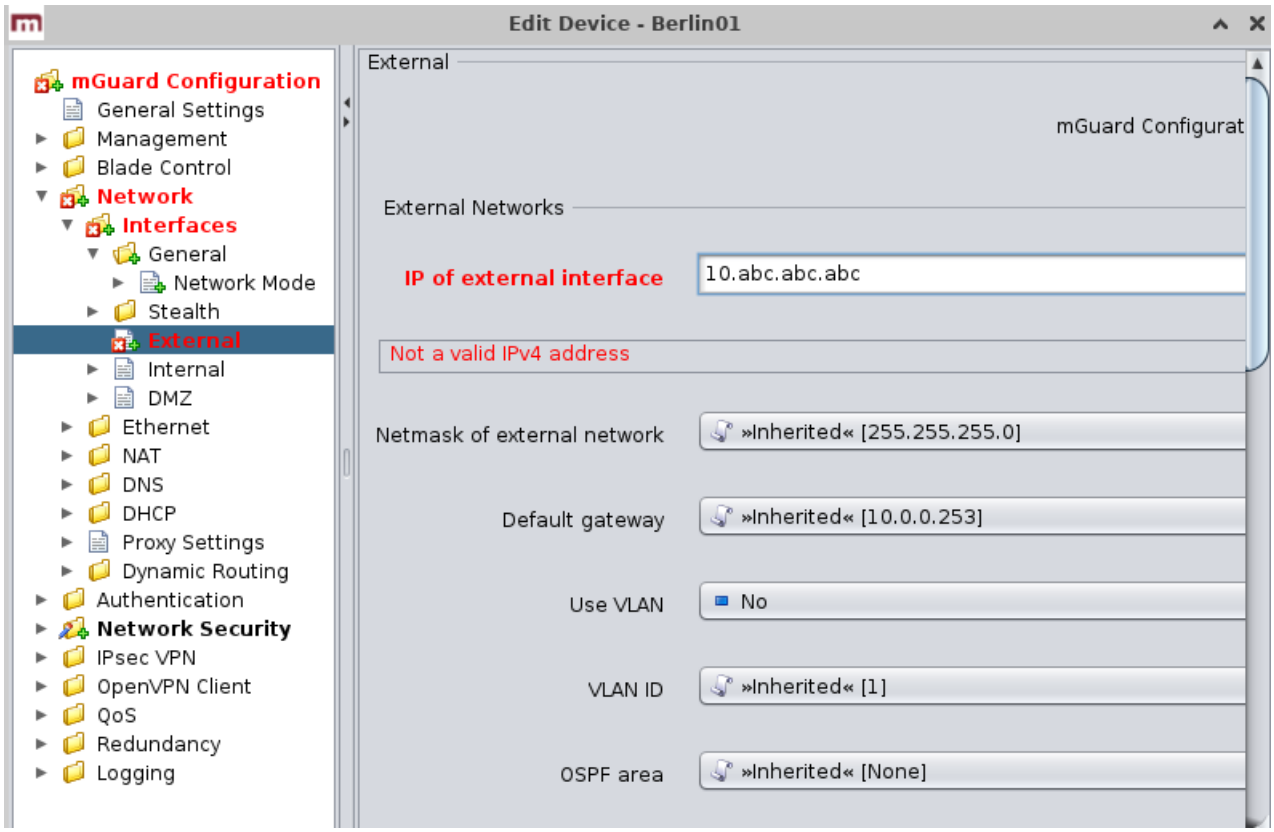


Bild 6-1 Prüfung der Eingabe/ungültige Eingabe

6.1.4 Anzeige geänderter Werte

Das Symbol in den Blättern des Navigationsbaumes (siehe folgende Abbildung) zeigt an, dass eine Variable in diesem Blatt geändert, diese Änderung aber noch nicht übernommen wurde.

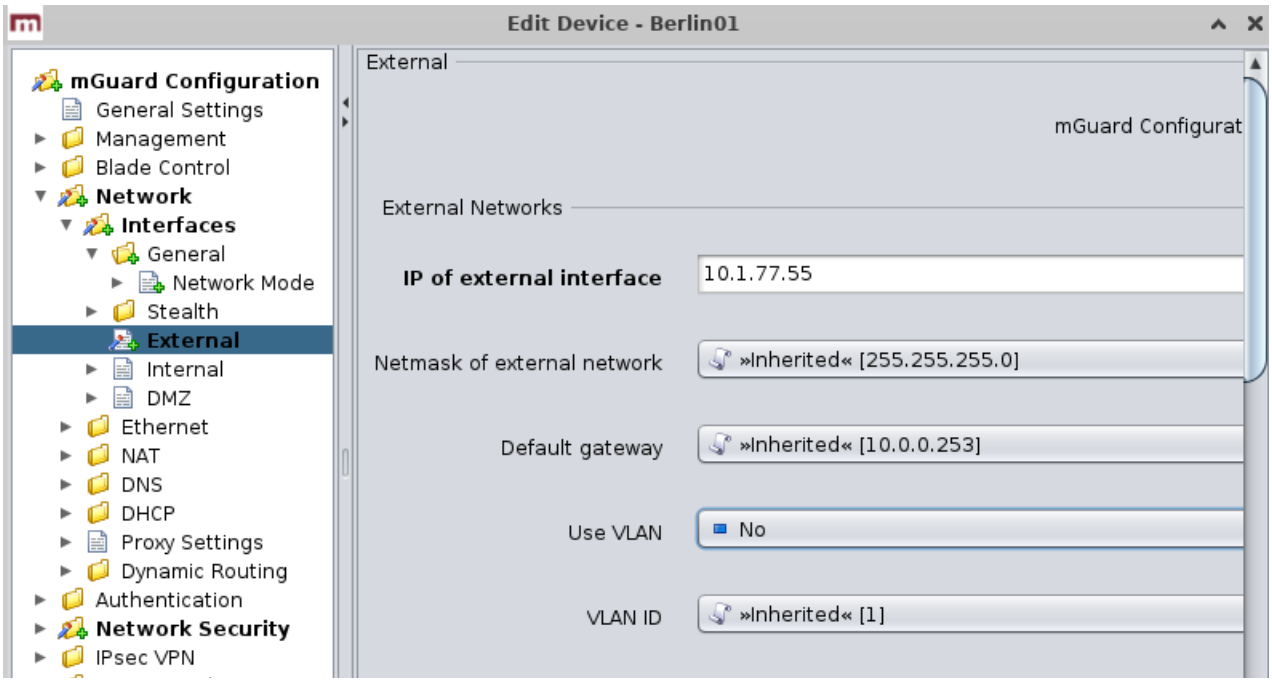


Bild 6-2 Anzeige nicht übernommener Änderungen

Das Symbol in den Blättern des Navigationsbaumes (siehe folgende Abbildung) zeigt an, dass Einstellungen in dem entsprechenden Blatt geändert und die Änderungen übernommen wurden.

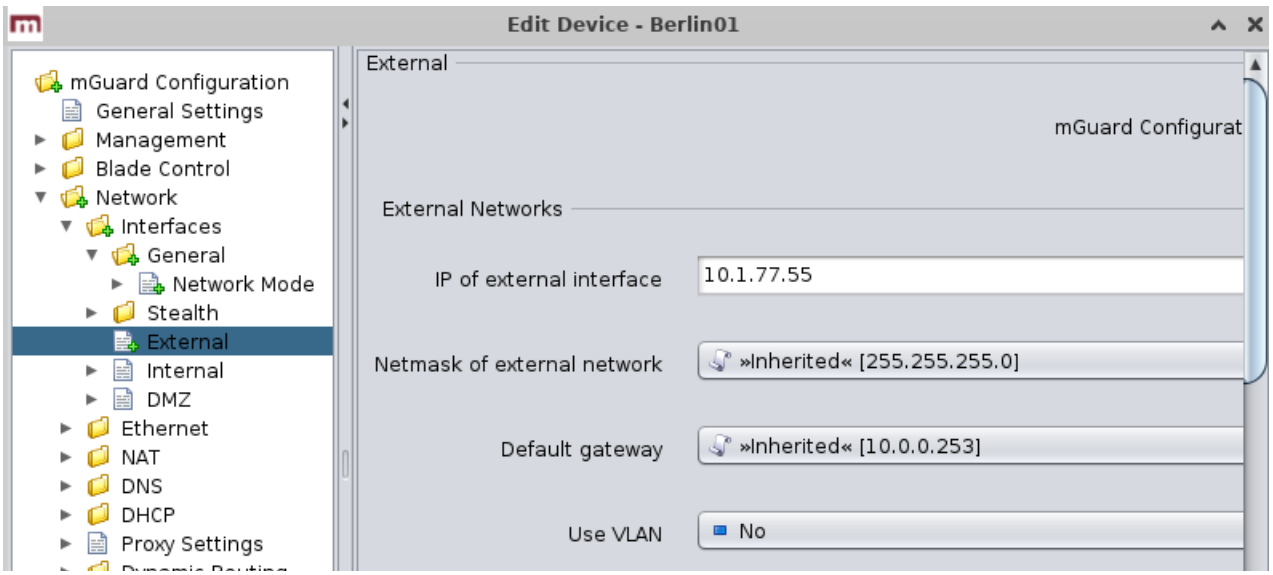


Bild 6-3 Anzeige übernommener Änderungen

6.1.5 Anzeige eines „None“-Werts oder eines erschöpften Pools

Das Symbol in den Blättern des Navigationsbaumes (siehe folgende Abbildung) zeigt entweder an,

– dass in einem der übergeordneten Templates ein „**None**“-Wert ausgewählt wurde, der noch nicht in der Templatehierarchie überschrieben (gesetzt) wurde oder
– das ein **erschöpfter (nicht ausreichend gefüllter) Pool** ausgewählt wurde.

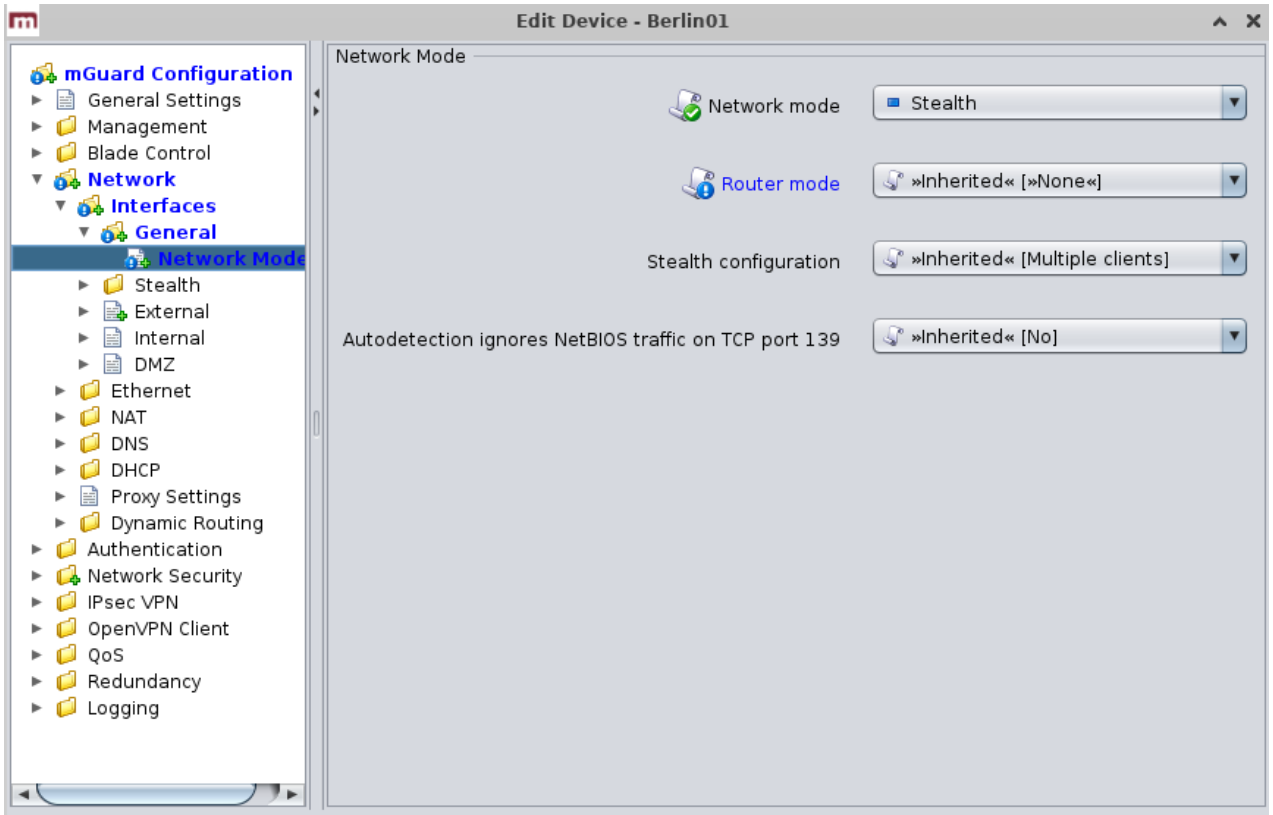


Bild 6-4 Anzeige eines *None*-Werts

6.1.6 mGuard Tabellenvariablen ändern

In der folgenden Abbildung ist ein Beispiel für eine Tabellenvariable dargestellt (Firewall-Regeln für eingehende Dateien):

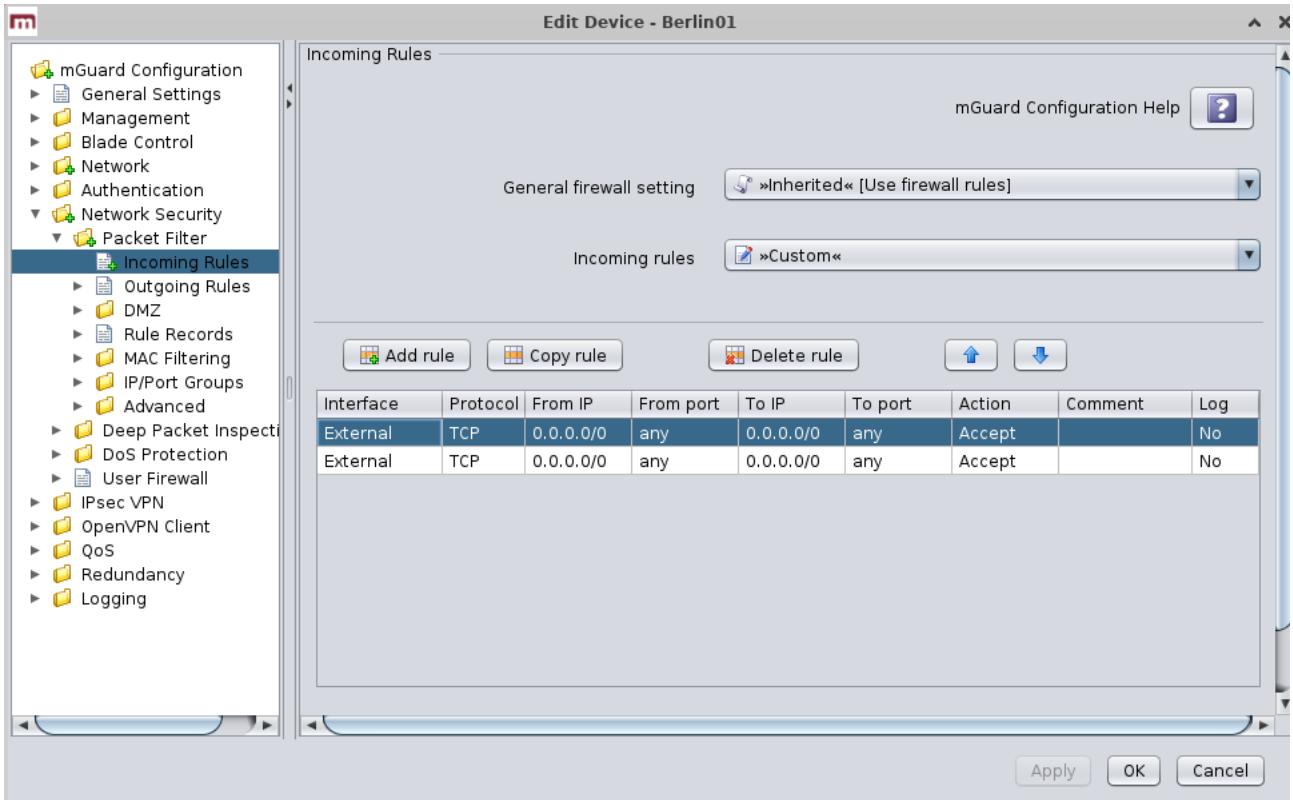


Bild 6-5 Ändern von Tabellenvariablen

Zeilen hinzufügen, löschen, kopieren oder verschieben

Mit den entsprechenden Schaltflächen können Sie Zeilen hinzufügen, löschen, kopieren oder verschieben.

Wenn keine Zeile markiert ist, klicken Sie auf die Schaltfläche **Add**, um eine Zeile zum Anfang der Tabelle hinzuzufügen. Sind bereits eine oder mehrere Zeilen markiert, wird die neue Zeile unter der letzten markierten Zeile eingefügt.

Die Schaltfläche **Delete** ist nur aktiv, wenn mindestens eine Zeile markiert ist. Mit dieser Schaltfläche werden die markierten Zeilen gelöscht.

Die Schaltfläche **Copy** ist nur aktiv, wenn mindestens eine Zeile markiert ist. Mit dieser Schaltfläche können markierte Zeilen kopiert und unter der letzten markierten Zeile eingefügt werden.

Die Schaltflächen **Move** sind nur aktiv, wenn mindestens eine Zeile markiert ist. Klicken Sie auf , um die aktuelle Auswahl um eine Zeile nach oben zu verschieben, und , um sie nach unten zu verschieben.

Die Schaltflächen **Add**, **Delete**, **Copy** und **Move** sind nur bei Auswahl von **Custom** oder **Custom + locally appendable** aktiv. Siehe Abschnitt *mGuard-Konfiguration* oben.

Tabellenzeilen markieren

Durch Anklicken einer Tabellenzeile mit der linken Maustaste können Sie diese Zeile markieren. Klicken Sie zum Markieren mehrerer zusammenhängender Zeilen mit der linken Maustaste auf die oberste und unterste Zeile der gewünschten Auswahl und halten Sie dabei die <*Umschalttaste*> gedrückt.

Durch Anklicken der linken Maustaste und gleichzeitigem Drücken der Taste <*Strg*> können Sie Zeilen zu Ihrer Auswahl hinzufügen oder daraus entfernen.

Tabellenzellen ändern

Führen Sie zum Bearbeiten einer Tabellenzelle mit der linken Maustaste einen Doppelklick darauf aus. (Mit einem einfachen Klick wird die Zeile markiert).

Ungültige Werte in Tabellen

Ein ungültiger Wert in einer Tabelle wird nicht im Navigationsbaum angezeigt, die Zelle wird jedoch rot markiert. Wenn Sie in eine Zelle einen ungültigen Wert eingeben und die Zelle anschließend verlassen, beispielsweise durch Anklicken eines anderen Knotens im Navigationsbaum, wird der ungültige Eintrag durch den letzten übernommenen (gültigen) Wert ersetzt.

In Firewall-Tabellen gilt: Wenn das gewählte Protokoll weder TCP noch UDP ist, wird der konfigurierte Port ignoriert. Die Zelle wird in diesen Fällen gelb markiert.

Zeilenfarben

Die Zeilen einer Tabelle können in verschiedenen Farben angezeigt werden, je nach Art der Zeile. Geerbte Reihen von einem übergeordneten Template werden in Rot, Grün oder Grau dargestellt:

- grüne Zeilen können bearbeitet werden,
- rote Zeilen können nicht bearbeitet oder gelöscht werden
- bei grauen Zeilen handelt es sich um geerbte Standardzeilen (die geändert werden können).

Um eine grüne oder graue Zeile ändern zu können, muss der Tabellenwert von **Inherited** zu **Custom** geändert werden.

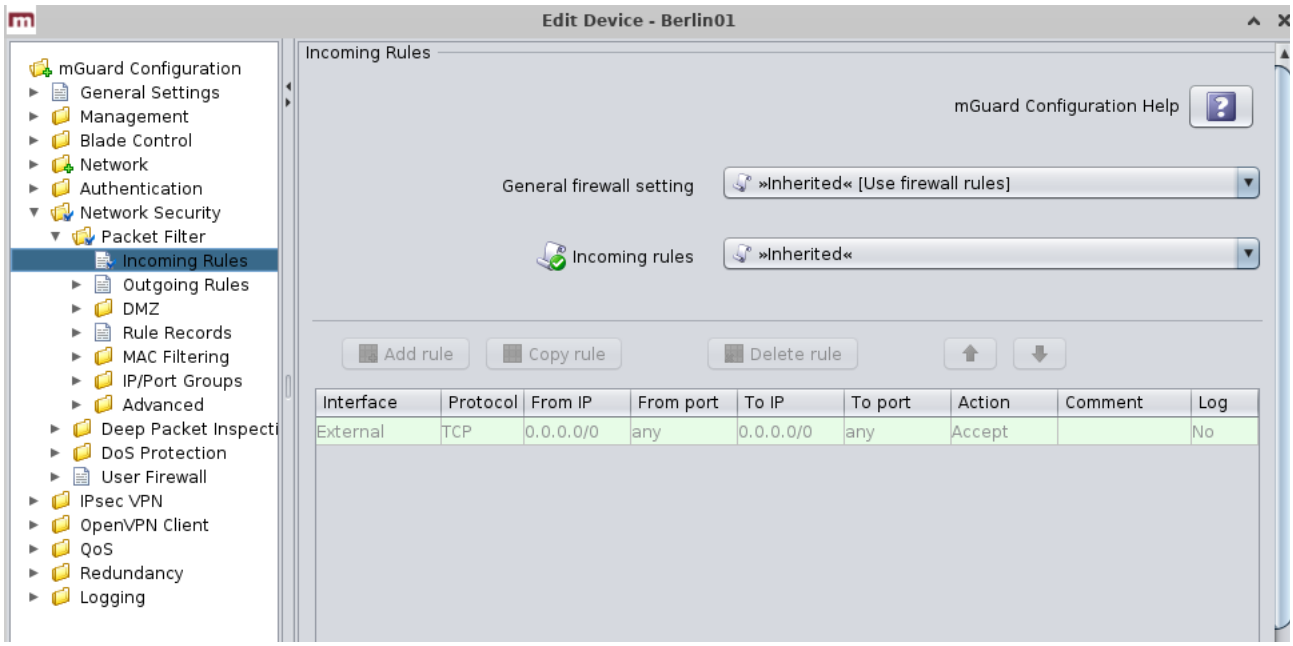


Bild 6-6 Farben von Tabellenzeilen

Kontextmenü

Tabellen können auch über das Kontextmenü bearbeitet werden. Klicken Sie die Tabelle mit der rechten Maustaste an. Das folgende Menü wird angezeigt:

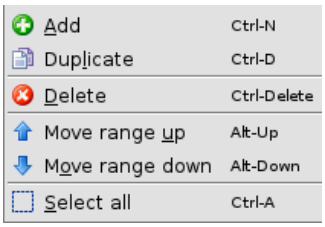


Bild 6-7 Kontextmenü

6.1.7 Komplexe Tabellenvariablen ändern

Definition einer komplexen Tabellenvariable siehe Abschnitt *mGuard-Konfiguration* oben. Grundsätzlich gilt der vorhergehende Abschnitt auch für komplexe Tabellenvariablen. Es bestehen jedoch einige Unterschiede, die der Benutzer kennen muss.

In der folgenden Abbildung ist ein Beispiel für eine komplexe Tabellenvariable dargestellt (VPN-Verbindungen):

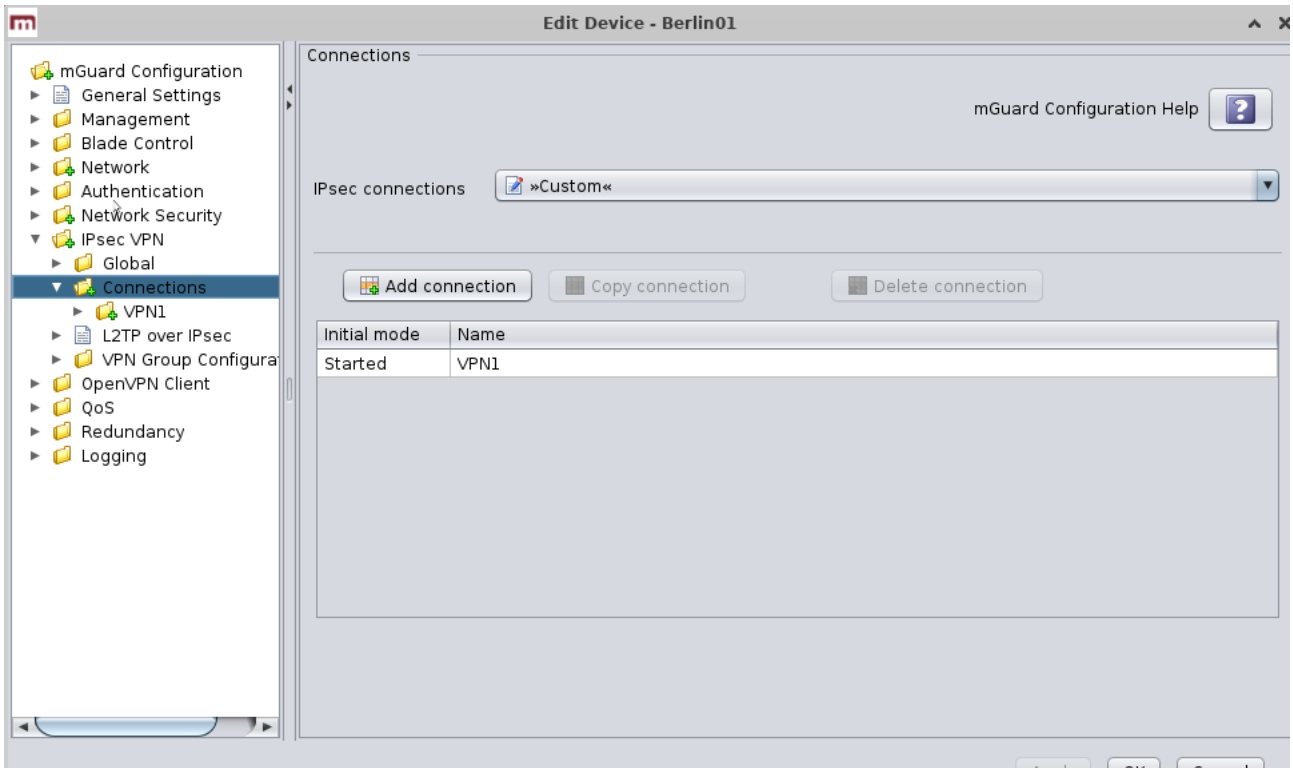


Bild 6-8 Ändern komplexer Tabellenvariablen

Bei einer komplexen Tabelle können die Zeilen nicht verschoben werden (hier fehlen die entsprechenden Schaltflächen). Darüber hinaus sind bei komplexen Tabellen die Zellen nicht editierbar. Durch das Hinzufügen einer Zeile zu einer komplexen Tabelle wird auch ein Knoten im Navigationsbaum hinzugefügt (siehe Bild 6-8).

Die Schaltflächen **Add, Copy** und **Delete** sind nur bei Auswahl von **Custom** oder **Custom + locally appendable** aktiv. Siehe Abschnitt *mGuard-Konfiguration* oben.

6.1.8 Änderungen in die Konfiguration übernehmen

An der Konfiguration vorgenommene Änderungen werden über die Schaltfläche **Apply** (am unteren Rand des Dialogs) dauerhaft gespeichert. Wenn Sie Änderungen vornehmen, ohne sie zu übernehmen, können Sie diese durch Schließen des Dialogs über die Schaltfläche **Cancel** verwerfen. Sie können Ihre Änderungen auch durch Schließen des Dialogs über die Schaltfläche **OK** übernehmen.

Die Konfiguration wird nach Übernahme einer Änderung **nicht** automatisch an den mGuard übertragen. Zur Übertragung der Konfiguration an einen mGuard müssen Sie die Konfigurationsdatei in den mGuard laden (siehe Kapitel 7.1).

6.2 Standardwerte (Default values)

Wird in der mGuard-Firmware ein Standardwert (*Default value*) geändert, so ist die Verwaltung dieses Wertes in mdm betroffen:

1. wenn die Firmware-Version eines verwalteten Geräts auf eine Firmwareversion mit geändertem Standardwert aktualisiert wird,
2. wenn ein erbendes „Kind“, das eine andere mGuard-Firmwareversion besitzt als seine Eltern, einen Wert mit einem anderen Standardwert erbt.

Das damit verbundene Verhalten von mdm wird nachfolgend beschrieben.

Wenn ein Gerät/Template auf eine mGuardFirmwareversion (8.5 oder 8.6) upgegradet wird und ein neuer Standardwert (*Default value*) vom alten Standardwert abweicht (siehe Tabelle oben), gilt Folgendes:

Wenn der Standardwert (*Default value*) in der Standardkonfiguration (Default configuration) ist und vererbt wird (entlang der gesamten Vererbungskette), wird der alte Standardwert nach dem Upgrade beibehalten. In diesem Fall wird der Wertetyp (der Tabelle) von „**Inherited**“ auf „**Custom**“ geändert (*Value type*).

6.2.1 Vererbung von geänderten Standardwerten

Die Vererbung geänderter Standardwerte (*Default values*) hängt von der installierten mdm-Version und der mGuard-Firmwareversion des betroffenen Gerätes/Templates ab.

Allgemeines Verhalten in mdm < 1.8.0:

Wenn sich die Standardwerte (Wertetyp = "*Inherited*" und nicht "*Local*" oder "*Custom*") des „Kindes“ von den Standardwerten der „Mutter“ (Wertetyp = "*Inherited*" entlang der vollständigen Vererbungskette) unterscheiden, verhält sich die Vererbung wie folgt:

1. Das „Kind“ behält die Standardwerte, die der Firmwareversion des „Kindes“ entsprechen. Der Wertetyp bleibt "***Inherited***".

Allgemeines Verhalten in mdm 1.8.0 oder höher:

Wenn sich die Standardwerte (Wertetyp = "*Inherited*" und nicht "*Local*" oder "*Custom*") des „Kindes“ von den Standardwerten der „Mutter“ (Wertetyp = "*Inherited*" entlang der vollständigen Vererbungskette) unterscheiden, verhält sich die Vererbung wie folgt:

1. Standardwerte, die in mGuard **Firmwareversionen < 8.5** geändert wurden:
   – Das „Kind“ behält die Standardwerte, die der Firmwareversion des „Kindes“ entsprechen. Der Wertetyp bleibt "***Inherited***".
2. Standardwerte, die in mGuard **Firmwareversion 8.5 oder höher** geändert wurden:
   – Das „Kind“ erbt die Standardwerte der „Mutter“. Der Wertetyp bleibt "***Inherited***".

6.2.2 Verhalten von geänderten Standardwerten (mGuard 10.x)

In **mGuard-Firmwareversion 10.x** wurden folgende Standardwerte (*Default values*) geändert (siehe Tabelle 6-1).

Tabelle 6-1 Geänderte **mGuard**-Standardwerte (*Default values*)

Geändert in Version	Pfad zum Wert in der mGuard-Weboberfläche	Alter Wert (mGuard < 10)	Neuer Wert (mGuard 10.x)
10.x	Network >> Interfaces >> General >> Network mode	Stealth	Router
Beschreibung / Auswirkung			
– Generell gilt: Ein Gerät/ein Template, das von Firmware-Version < 10 auf 10.x aktualisiert wird, verwendet weiterhin den konfigurierten Wert, wenn ein Wert in der Kette der Vorlagen (Gerät/Templates) vorhanden/konfiguriert ist.			
– Wenn der Netzwerkmodus in der Kette der Vorlagen (Gerät/Templates) oder im Gerät **nicht** konfiguriert ist, gilt: a) Ein Gerät/Template **ohne** übergeordnete Vorlage (Gerät/Template), das von der Firmware-Version < 10 auf 10.x aktualisiert wird, erhält den Netzwerkmodus "Stealth" (Wertetyp: **Custom**). b) Ein Gerät/Template **mit** übergeordneter Vorlage (Gerät/Template) < 10, das von Firmware-Version < 10 auf 10.x aktualisiert wird, erhält den Netzwerkmodus "Stealth" (Wertetyp: **Custom**). c) Ein Gerät/Template (Firmware-Version 10.x), das selbst von einer Vorlage (Template) mit Firmware-Version < 10 mit Standard-Netzwerkmodus erbt, erhält den Netzwerkmodus "Stealth" (Wertetyp: **Inherited**). – Ein Gerät/Template, das mit einer Firmware-Version < 10 erstellt wird, erhält den Netzwerkmodus "Stealth" (Wertetyp: **Inherited**). – Ein Gerät/Template, das mit einer Firmware-Version 10.x erstellt wird, erhält den Netzwerkmodus "Router" (Wertetyp: **Inherted**).			

6.2.3 Verhalten von geänderten Standardwerten (mGuard 8.5/8.6)

In **mGuard-Firmwareversion 8.5 und 8.6** wurden folgende Standardwerte (*Default values*) geändert (siehe Tabelle 6-2).

Tabelle 6-2 Geänderte mGuard-Standardwerte (*Default values*)

Geändert in Version	Pfad zum Wert in der mGuard-Weboberfläche	Alter Wert	Neuer Wert
8.5.0	IPsec VPN >> Connections >> EDIT >> IKE Options >> ISAKMP SA (Key Exchange)	3DES (Verschlüsselung)	AES-256
8.5.0	IPsec VPN >> Connections >> EDIT >> IKE Options >> IPsec SA (Data Exchange)	3DES (Verschlüsselung)	AES-256
8.6.0	CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Checking of Shares	SHA-1 (Hash)	SHA-256
8.6.0	OpenVPN Client -> Connections >> EDIT >> Tunnel Settings >> Data Encryption	Blowfish (Verschlüsselung)	AES-256
8.6.0	Redundancy >> Firewall Redundancy >> Redundancy >> Encrypted State Synchronization	3DES (Verschlüsselung)	AES-256
8.6.0		SHA-1 (Hash)	SHA-256
8.5.0	Network Security >> Packet Filter >> Incoming/Outgoing	Siehe mGuard-Firmwarehandbuch 8.5.x für weitere Informationen, verfügbar online oder unter phoenixcontact.net/products.	

6.3 Geräte konfigurieren

6.3.1 Geräte-Übersicht (Device overview table)

Klicken Sie auf die Registerkarte **Device**, um die Geräte-Übersicht (*Device overview table*) aufzurufen:

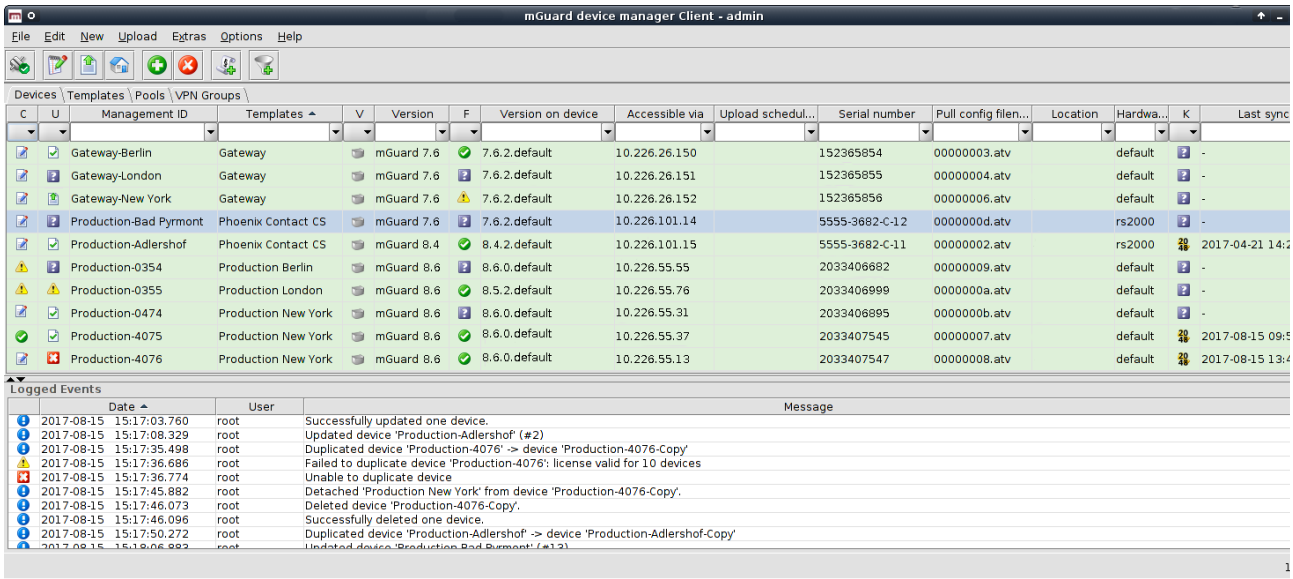


Bild 6-9 mdm Hauptfenster mit Gerätetabelle

Spalten der Gerätetabelle Die Geräte-Übersicht (*Device overview table*) enthält folgende Spalten (siehe unten).

Setzen Sie zum Ändern der Spaltenbreite den Cursor in die Kopfzeile der Tabelle an die Grenze zwischen zwei Spalten und ziehen Sie bei gedrückter linker Maustaste die Grenze in die gewünschte Richtung. Setzen Sie zum Verschieben einer Spalte den Cursor in die Kopfzeile der Tabelle und ziehen Sie bei gedrückter linker Maustaste die Spalte an den gewünschten Platz.

Geräte-Übersicht (Device table columns)		
Status *C*	Die mit ***C*** gekennzeichnete Spalte stellt den Konfigurationsstatus des Geräts dar und zeigt an, ob die Konfiguration des mGuard von der Konfiguration des Geräts in mdm abweicht. Der Konfigurationsstatus kann folgende Werte aufweisen.	
	Unknown	mdm kann nicht bestimmen, ob Ihr mGuard eine aktuelle Konfiguration aufweist.
	OK	Die Konfiguration in mdm ist mit der aktuellen Konfiguration Ihres mGuard identisch.
	Changed	Die Konfiguration in mdm weicht von der aktuellen Konfiguration Ihres mGuard ab, d. h. die mit mdm vorgenommenen Änderungen wurden noch nicht in das Gerät geladen.

Geräte-Übersicht (Device table columns)		
	Locked	Die Konfiguration ist derzeit durch einen anderen Benutzer gesperrt. Dies ist zum Beispiel der Fall, wenn der *Device properties dialog* (Geräte-Eigenschaften) oder der *Template properties dialog* (Template-Eigenschaften) eines zugewiesenen Templates durch einen anderen Benutzer geöffnet wurde.
		Änderungen an der Konfiguration, die nicht mit mdm vorgenommen wurden, können nicht erkannt werden, d. h. der Konfigurationsstatus wird nur dann korrekt angezeigt, wenn nur der Netadmin-Benutzer die Konfiguration des mGuard lokal am Gerät ändert.
		Bei Änderung eines Templates wird die Konfiguration **aller** mGuards, die dieses Template verwenden, auf *out-of-date* gesetzt, unabhängig davon, ob die Gerätekonfiguration von der Änderung des Templates betroffen ist.
		Informationen zum manuellen Zurücksetzen des Konfigurationsstatus zu *up-to-date* finden Sie in Kapitel 5.2.
Status *U*		Die mit ***U*** gekennzeichnete Spalte stellt den Upload-Status des Geräts dar und zeigt ein ausstehendes Upload bzw. das Ergebnis des letzten Uploads an. Informationen zum Hochladen von Konfigurationen in die Geräte finden Sie in „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107.
		Der Upload-Status kann folgende Werte aufweisen.
	Unknown	mdm konnte den Status noch nicht bestimmen, da kein Upload stattgefunden hat.
	Up to date	Die Konfiguration am Gerät wurde nicht geändert, da sie bereits auf dem neuesten Stand war.
	Updated	Die Gerätekonfiguration wurde aktualisiert.
	Configuration exported	Die Konfigurationsdateien wurden erfolgreich in das Dateisystem exportiert.
	Pull feedback received	Der mdm-Server hat eine Rückmeldung von einem Konfigurations-Pull (*Configuration Pull*) vom HTTPS-Server erhalten, aber es konnte nicht festgestellt werden, ob die Konfiguration am Gerät jetzt auf dem neuesten Stand ist. Dieser Status zeigt an, dass das Gerät eine Konfigurationsdatei gezogen, aber diese noch nicht übernommen hat, oder dass die Konfiguration veraltet ist, weil sie nach dem Export auf den HTTPS-Server in mdm geändert wurde.
	Device credential update	Zeigt an, dass der SSH-Host Key zurückgesetzt wurde.

Geräte-Übersicht (Device table columns)		
	Locked	Die Konfiguration ist derzeit durch einen anderen Benutzer gesperrt. Dies ist zum Beispiel der Fall, wenn der *Device properties dialog* (Geräte-Eigenschaften) oder der *Template properties dialog* (Template-Eigenschaften) eines zugewiesenen Templates durch einen anderen Benutzer geöffnet wurde.
		Änderungen an der Konfiguration, die nicht mit mdm vorgenommen wurden, können nicht erkannt werden, d. h. der Konfigurationsstatus wird nur dann korrekt angezeigt, wenn nur der Netadmin-Benutzer die Konfiguration des mGuard lokal am Gerät ändert.
		Bei Änderung eines Templates wird die Konfiguration **aller** mGuards, die dieses Template verwenden, auf *out-of-date* gesetzt, unabhängig davon, ob die Gerätekonfiguration von der Änderung des Templates betroffen ist.
		Informationen zum manuellen Zurücksetzen des Konfigurationsstatus zu *up-to-date* finden Sie in Kapitel 5.2.
Status *U*		Die mit ***U*** gekennzeichnete Spalte stellt den Upload-Status des Geräts dar und zeigt ein ausstehendes Upload bzw. das Ergebnis des letzten Uploads an. Informationen zum Hochladen von Konfigurationen in die Geräte finden Sie in „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107.
		Der Upload-Status kann folgende Werte aufweisen.
	Unknown	mdm konnte den Status noch nicht bestimmen, da kein Upload stattgefunden hat.
	Up to date	Die Konfiguration am Gerät wurde nicht geändert, da sie bereits auf dem neuesten Stand war.
	Updated	Die Gerätekonfiguration wurde aktualisiert.
	Configuration exported	Die Konfigurationsdateien wurden erfolgreich in das Dateisystem exportiert.
	Pull feedback received	Der mdm-Server hat eine Rückmeldung von einem Konfigurations-Pull (*Configuration Pull*) vom HTTPS-Server erhalten, aber es konnte nicht festgestellt werden, ob die Konfiguration am Gerät jetzt auf dem neuesten Stand ist. Dieser Status zeigt an, dass das Gerät eine Konfigurationsdatei gezogen, aber diese noch nicht übernommen hat, oder dass die Konfiguration veraltet ist, weil sie nach dem Export auf den HTTPS-Server in mdm geändert wurde.
	Device credential update	Zeigt an, dass der SSH-Host Key zurückgesetzt wurde.

Geräte-Übersicht (Device table columns)		
	Locked	Die Konfiguration ist derzeit durch einen anderen Benutzer gesperrt. Dies ist zum Beispiel der Fall, wenn der *Device properties dialog* (Geräte-Eigenschaften) oder der *Template properties dialog* (Template-Eigenschaften) eines zugewiesenen Templates durch einen anderen Benutzer geöffnet wurde.
		Änderungen an der Konfiguration, die nicht mit mdm vorgenommen wurden, können nicht erkannt werden, d. h. der Konfigurationsstatus wird nur dann korrekt angezeigt, wenn nur der Netadmin-Benutzer die Konfiguration des mGuard lokal am Gerät ändert.
		Bei Änderung eines Templates wird die Konfiguration **aller** mGuards, die dieses Template verwenden, auf *out-of-date* gesetzt, unabhängig davon, ob die Gerätekonfiguration von der Änderung des Templates betroffen ist.
		Informationen zum manuellen Zurücksetzen des Konfigurationsstatus zu *up-to-date* finden Sie in Kapitel 5.2.
Status *U*		Die mit ***U*** gekennzeichnete Spalte stellt den Upload-Status des Geräts dar und zeigt ein ausstehendes Upload bzw. das Ergebnis des letzten Uploads an. Informationen zum Hochladen von Konfigurationen in die Geräte finden Sie in „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107.
		Der Upload-Status kann folgende Werte aufweisen.
	Unknown	mdm konnte den Status noch nicht bestimmen, da kein Upload stattgefunden hat.
	Up to date	Die Konfiguration am Gerät wurde nicht geändert, da sie bereits auf dem neuesten Stand war.
	Updated	Die Gerätekonfiguration wurde aktualisiert.
	Configuration exported	Die Konfigurationsdateien wurden erfolgreich in das Dateisystem exportiert.
	Pull feedback received	Der mdm-Server hat eine Rückmeldung von einem Konfigurations-Pull (*Configuration Pull*) vom HTTPS-Server erhalten, aber es konnte nicht festgestellt werden, ob die Konfiguration am Gerät jetzt auf dem neuesten Stand ist. Dieser Status zeigt an, dass das Gerät eine Konfigurationsdatei gezogen, aber diese noch nicht übernommen hat, oder dass die Konfiguration veraltet ist, weil sie nach dem Export auf den HTTPS-Server in mdm geändert wurde.
	Device credential update	Zeigt an, dass der SSH-Host Key zurückgesetzt wurde.

Geräte-Übersicht (Device table columns)		
	Locked	Die Konfiguration ist derzeit durch einen anderen Benutzer gesperrt. Dies ist zum Beispiel der Fall, wenn der *Device properties dialog* (Geräte-Eigenschaften) oder der *Template properties dialog* (Template-Eigenschaften) eines zugewiesenen Templates durch einen anderen Benutzer geöffnet wurde. Änderungen an der Konfiguration, die nicht mit mdm vorgenommen wurden, können nicht erkannt werden, d. h. der Konfigurationsstatus wird nur dann korrekt angezeigt, wenn nur der Netadmin-Benutzer die Konfiguration des mGuard lokal am Gerät ändert. Bei Änderung eines Templates wird die Konfiguration **aller** mGuards, die dieses Template verwenden, auf *out-of-date* gesetzt, unabhängig davon, ob die Gerätekonfiguration von der Änderung des Templates betroffen ist. Informationen zum manuellen Zurücksetzen des Konfigurationsstatus zu *up-to-date* finden Sie in Kapitel 5.2.
Status *U*		Die mit ***U*** gekennzeichnete Spalte stellt den Upload-Status des Geräts dar und zeigt ein ausstehendes Upload bzw. das Ergebnis des letzten Uploads an. Informationen zum Hochladen von Konfigurationen in die Geräte finden Sie in „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107. Der Upload-Status kann folgende Werte aufweisen.
	Unknown	mdm konnte den Status noch nicht bestimmen, da kein Upload stattgefunden hat.
	Up to date	Die Konfiguration am Gerät wurde nicht geändert, da sie bereits auf dem neuesten Stand war.
	Updated	Die Gerätekonfiguration wurde aktualisiert.
	Configuration exported	Die Konfigurationsdateien wurden erfolgreich in das Dateisystem exportiert.
	Pull feedback received	Der mdm-Server hat eine Rückmeldung von einem Konfigurations-Pull (*Configuration Pull*) vom HTTPS-Server erhalten, aber es konnte nicht festgestellt werden, ob die Konfiguration am Gerät jetzt auf dem neuesten Stand ist. Dieser Status zeigt an, dass das Gerät eine Konfigurationsdatei gezogen, aber diese noch nicht übernommen hat, oder dass die Konfiguration veraltet ist, weil sie nach dem Export auf den HTTPS-Server in mdm geändert wurde.
	Device credential update	Zeigt an, dass der SSH-Host Key zurückgesetzt wurde.

Geräte-Übersicht (Device table columns)		
	Locked	Die Konfiguration ist derzeit durch einen anderen Benutzer gesperrt. Dies ist zum Beispiel der Fall, wenn der *Device properties dialog* (Geräte-Eigenschaften) oder der *Template properties dialog* (Template-Eigenschaften) eines zugewiesenen Templates durch einen anderen Benutzer geöffnet wurde.
		Änderungen an der Konfiguration, die nicht mit mdm vorgenommen wurden, können nicht erkannt werden, d. h. der Konfigurationsstatus wird nur dann korrekt angezeigt, wenn nur der Netadmin-Benutzer die Konfiguration des mGuard lokal am Gerät ändert.
		Bei Änderung eines Templates wird die Konfiguration **aller** mGuards, die dieses Template verwenden, auf *out-of-date* gesetzt, unabhängig davon, ob die Gerätekonfiguration von der Änderung des Templates betroffen ist.
		Informationen zum manuellen Zurücksetzen des Konfigurationsstatus zu *up-to-date* finden Sie in Kapitel 5.2.
Status *U*		Die mit ***U*** gekennzeichnete Spalte stellt den Upload-Status des Geräts dar und zeigt ein ausstehendes Upload bzw. das Ergebnis des letzten Uploads an. Informationen zum Hochladen von Konfigurationen in die Geräte finden Sie in „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107.
		Der Upload-Status kann folgende Werte aufweisen.
	Unknown	mdm konnte den Status noch nicht bestimmen, da kein Upload stattgefunden hat.
	Up to date	Die Konfiguration am Gerät wurde nicht geändert, da sie bereits auf dem neuesten Stand war.
	Updated	Die Gerätekonfiguration wurde aktualisiert.
	Configuration exported	Die Konfigurationsdateien wurden erfolgreich in das Dateisystem exportiert.
	Pull feedback received	Der mdm-Server hat eine Rückmeldung von einem Konfigurations-Pull (*Configuration Pull*) vom HTTPS-Server erhalten, aber es konnte nicht festgestellt werden, ob die Konfiguration am Gerät jetzt auf dem neuesten Stand ist. Dieser Status zeigt an, dass das Gerät eine Konfigurationsdatei gezogen, aber diese noch nicht übernommen hat, oder dass die Konfiguration veraltet ist, weil sie nach dem Export auf den HTTPS-Server in mdm geändert wurde.
	Device credential update	Zeigt an, dass der SSH-Host Key zurückgesetzt wurde.

Geräte-Übersicht (Device table columns)	
Configuration invalid	mdm zeigt an, dass die aktuelle Konfiguration ungültig ist, z. B. ein **None**-Wert (siehe „Template-Konfiguration“ auf Seite 79) im Template nicht im Gerät überschrieben wurde.
Upload or export error	Ein permanenter Fehler ist aufgetreten und mdm kann diesen nicht beheben oder die maximale Anzahl an Versuchen für das Pushen der SSH/HTTPS-Konfiguration wurde erreicht, ohne dass auf den mGuard zugegriffen werden konnte. Die Ursache des Fehlers wird im Protokollfenster angezeigt. – **Host authentication failed** Dieser Fehler zeigt an, dass die Authentifizierung des SSH-Hosts fehlgeschlagen ist. Dies kann auf einen Angriff hinweisen, aber eine wahrscheinlichere Ursache ist der Austausch eines ausgefallenen Geräts. Vergewissern Sie sich vor der Durchführung der nächsten Schritte, dass die fraglichen Geräte wirklich ausgetauscht worden sind. Löschen Sie zum Fortfahren mit der Option Set Current Device Credentials im Kontextmenü der Tabelle Geräteübersicht den aktiven SSH-Hostkey (setzen Sie in das Kontrollkästchen **Reset SSH Host Key** ein Häkchen). Der neue SSH-Hostkey wird in der nächsten SSH-Verbindung gesetzt. – **User authentication failed** Dieser Fehler zeigt an, dass die Anmeldeinformationen (z. B. Benutzername *admin* und das in den Geräten abgelegte Passwort *active password*) nicht akzeptiert wurden. Er kann auch darauf hinweisen, dass die Authentifizierungsmethode *password* des SSH vom mGuard nicht akzeptiert wurde. – **I/O failed / Upload failed** Dieser Fehler weist auf eine Problem mit Ein-/Ausgabe (I/O) hin. Bei einem SSH-Upload ist dies möglicherweise ein transienter Fehler und ein neuer Versuch sollte angesetzt werden. Bei einer Dateisystem-Ausgabe (Pull-Konfiguration) ist der Fehler wahrscheinlich nicht transient und der Benutzer sollte die Ursache ermitteln. – **Concurrent configuration upload** Diese Meldung weist darauf hin, dass für das gleiche Gerät bereits ein anderer Upload durchgeführt wird. Ein Beispiel hierfür ist ein SSH-Upload, der ein laufendes Pull-Konfig-Skript erkennt. Die normale Vorgehensweise in diesem Fall ist eine Verschiebung des Uploads. – **Configuration rejected** Diese Meldung zeigt an, dass die Konfiguration vom Gerät als ungültig zurückgewiesen wurde.

Geräte-Übersicht (Device table columns)		
	Upload timeout	Diese Meldung zeigt an, dass die SSH-Verbindung zum Gerät aufgrund einer Zeitüberschreitung beendet wurde, d. h. das Gerät hat auf die vom mdm generierten Befehle innerhalb eines vorgegebenen (konfigurierbaren) Zeitrahmens nicht reagiert. Falls die Konfiguration sehr viele VPN-Verbindungen enthält, muss dieser Zeitrahmen möglicherweise erweitert werden, siehe Kapitel 10.1, Knoten *service » storage » update » ssh » deadPeerDetectionTimeout* (**„Key *deadPeerDetectionTimeout“ auf Seite 165***).
	License could not be installed	Diese Meldung weist darauf hin, dass eine mGuard Lizenzdatei nicht auf dem Gerät installiert werden konnte.
	Pull configuration rolled back	Diese Meldung zeigt an, dass die vom Gerät gezogene Konfiguration zurückgerollt wurde.
	Pull configuration blocked due to previous rollback	Diese Meldung weist darauf hin, dass eine Konfiguration aufgrund eines früheren Rollback blockiert ist.
	Saving configuration for rollback failed	Diese Meldung zeigt an, dass die Rollback-Konfiguration nicht gespeichert werden konnte, die Konfiguration wurde nicht übernommen.
	Pulled configuration invalid	Diese Meldung zeigt an, dass das Gerät eine ungültige Pull-Konfiguration erkannt hat und die Konfiguration daher nicht übernommen wurde.
	Firmware upgrade failed	Das geplante Firmware-Upgrade ist fehlgeschlagen.
	Queued for upload or export	Das Gerät befindet sich derzeit in der Warteschlange für einen Upload. Je nach den Einstellungen für *configuration push retries* und *waiting time between retries* kann sich das Gerät für einige Zeit in der Warteschlange befinden.
	Upload or export running	Der Zugriff auf das Gerät war erfolgreich und die Konfigurationsdatei wird gerade hochgeladen.
	Requeued for upload or export	Wenn nicht auf das Gerät zugegriffen werden kann, wird es erneut in die Warteschlange verschoben und nach *waiting time between retries* beginnt der Upload erneut. Wenn nach *configuration push retries* kein Zugriff auf das Gerät möglich ist, wird ein Fehler angezeigt. Dieses Symbol wird auch während eines laufenden Firmware-Upgrades angezeigt, da mdm vom Gerät in regelmäßigen Abständen das Ergebnis des Firmware-Upgrades abfragt.
Management ID	In dieser Spalte wird die Management-ID des Geräts angezeigt.	
Templates	In dieser Spalte wird eine durch Kommas getrennte Liste der übergeordneten Templates des Geräts angezeigt. Der erste Punkt auf der Liste ist das unmittelbar übergeordnete Template.	
Status *V*	In der mit ***V*** gekennzeichneten Spalte wird der VPN-Gruppenstatus angezeigt.	

Geräte-Übersicht (Device table columns)		
	Not a member of a VPN group **Member of exactly one VPN group** **Member of more than one VPN group**	Wird mit der Maus über die beiden letztgenannten Symbole gefahren, zeigt der Mauszeiger eine Quickinfo mit einer Aufzählung der VPN-Gruppen an, zu denen das Gerät gehört.
Version	In diese Spalte wird die aktuell in mdm für dieses Gerät ausgewählte Firmwareversion angezeigt.	
Status *F*	In der mit ***F*** gekennzeichneten Spalte wird der Firmwarestatus angezeigt.	
	Unknown	Der Status ist unbekannt.
	OK	Das Firmware-Upgrade war erfolgreich und die in mdm konfigurierte Firmwareversion entspricht der Firmwareversion des Geräts.
	Upgrade scheduled	Das Upgrade ist vorgesehen.
	Upgrade running	Das Upgrade läuft.
	Version mismatch	Die in mdm konfigurierte Firmwareversion und die Firmwareversion des Geräts stimmen nicht überein.
	Fehler	Während des Firmware-Upgrades ist ein Fehler aufgetreten.
Version on device	In dieser Spalte wird die aktuell auf dem Gerät installierte Firmwareversion angezeigt. Weitere Informationen finden Sie unter „Geräte-Eigenschaften (Device properties dialog)“ auf Seite 64. Wenn das Gerät im Redundanzmodus betrieben wird (nähere Informationen siehe „Redundanzmodus“ auf Seite 127), werden die Firmwareversionen beider Geräte mit Komma getrennt angezeigt.	
Accessible via	In dieser Spalte wird die IP-Adresse bzw. der Hostname angezeigt, der von mdm für den Zugriff auf das Gerät verwendet wird. Diese Adresse kann in den **General settings** des *Device properties dialogs* (Geräte-Eigenschaften) konfiguriert werden (siehe „Geräte-Eigenschaften (Device properties dialog)“ auf Seite 64). Ohne eine *Accessible via*-Adresse können weder Konfigurationen auf das Gerät geschoben, ATV-Konfigurationsprofile importiert, noch dessen Webinterface geöffnet werden. Hinweis: Diese Adresse entspricht möglicherweise nicht den internen oder externen Adressen des mGuard bei Verwendung von NAT. Wenn ein **SSH-Port** manuell unter **General settings** eingestellt wurde oder von dem konfigurierten Port (**Port for incoming SHH connections**) bezogen wird, wird er ebenfalls angezeigt. Wenn das Gerät im Redundanzmodus betrieben wird (nähere Informationen siehe „Redundanzmodus“ auf Seite 127), werden die *Accessible via*-Adressen beider Geräte mit Komma getrennt angezeigt.	
Upload scheduled at	In dieser Spalte werden Datum und Uhrzeit des nächsten für dieses Gerät geplanten Konfigurations-Upload angezeigt.	

Geräte-Übersicht (Device table columns)	
Serial number	In dieser Spalte wird die Seriennummer dieses Geräts angezeigt (siehe„Geräte-Eigenschaften (Device properties dialog)“ auf Seite 64). Wenn das Gerät im Redundanzmodus betrieben wird (nähere Informationen siehe „Redundanzmodus“ auf Seite 127), werden die Seriennummern beider Geräte mit Komma getrennt angezeigt.
Pull config filename	Bei einem Export der Konfiguration in das Dateisystem wird eine eindeutige ID als Name der Konfigurationsdatei verwendet. Der Dateiname der Konfiguration wird in dieser Spalte angezeigt.
Location	In dieser Spalte wird der Wert der SNMP Location Variable (SYS_LOCATION) angezeigt. Bei einem leeren Ort wird ein „–“ angezeigt. Wenn das Gerät im Redundanzmodus betrieben wird (nähere Informationen siehe „Redundanzmodus“ auf Seite 127) und für jedes physische Gerät unterschiedliche Orte eingestellt sind, werden die Standorte beider Geräte mit Komma getrennt angezeigt.
Hardware	In dieser Spalte wird die Hardwarekonfiguration des Geräts angezeigt. Weitere Informationen dazu erhalten Sie unter „Hardwarekonfigurationen“ auf Seite 26.
Status *K*	In der mit ***K*** gekennzeichneten Spalte werden die Größe der kryptografischen Schlüssel von *ssh* und *https* für den mGuard angezeigt. Die Größe wird bei jedem Zugriff des mdm auf den mGuard aktualisiert (nur wenn Firmwareversion ab 7.5 installiert ist). **mGuard-Geräte** mit einer früheren Firmwareversion als 7.5 aktualisieren diese Angaben nicht.  **Unknown** — Die Größe ist unbekannt.  **1024 bits** — Die Größe beträgt 1024 bit.  **2048 bits** — Die Größe beträgt 2048 bit.  **Key renewal scheduled** — Es wird empfohlen, Schlüssel mit 1024 bit zu erneuern (weiterführende Informationen siehe „Set Current Device Credentials“ auf Seite 61“).
Last sync	Die Spalte zeigt das Datum an, an dem jedes Gerät zuletzt erfolgreich mit mdm synchronisiert wurde. Synchronisierung bedeutet entweder ein Update via – SSH-Upload auf das Gerät (*upload via SSH*), – Pull-Export zum Gerät über einen HTTPS-Konfigurationspullserver + Rückmeldung (*prepare pull configuration*), – Online-Import von dem Gerät nach mdm (*Import ATV Profile*).  Wurde das Gerät per Pull-Export aktualisiert (*pull configuration*), zeigt *Last sync* diese Synchronisation nur an, wenn **alle** folgenden Punkte zutreffen: 1. Die Gerätekonfiguration in mdm hat sich seit dem geplanten Pull-Export nicht geändert. 2. Nach dem Pull-Export fand kein zusätzlicher SSH-Upload statt. 3. Der Pull-Export hat die Konfiguration auf dem mGuard-Gerät tatsächlich geändert. (Nachfolgende Pull-Feedback-Meldungen, bei denen keine Konfigurationsänderung stattfindet, werden nicht als Synchronisationsereignisse registriert.) Die Spalte kann durchsucht und chronologisch sortiert werden.

Tabelle filtern und sortieren

Mit der Kopfzeile der Tabelle können die Einträge sortiert werden. Durch Anklicken der Kopfzeile einer Spalte wird die (primäre) Sortierung anhand dieser Spalte aktiviert. Dies wird durch einen Pfeil in der Kopfzeile angezeigt. Durch einen zweiten Klick auf dieselbe Kopfzeile erfolgt die Sortierung in umgekehrter Reihenfolge. Durch Anklicken einer weiteren Spalte wird anhand dieser neuen Spalte sortiert, wobei die vorher aktive Spalte als zweites Kriterium für die Sortierung herangezogen wird.

In der ersten Tabellenzeile wird die Eingabe regulärer Ausdrücke akzeptiert (siehe „Glossar“ auf Seite 177, *Regular expressions*), die zum effizienten Filtern der Tabelleneinträge verwendet werden können. Bei Spalten, die keinen Text enthalten (Spalten **C**, **U, V** und **F**) kann nicht auf der Grundlage regulärer Ausdrücke gefiltert werden.

Der Filterverlauf wird für den aktuellen Benutzer gespeichert und kann über die Dropdown-Funktion der Filterfelder aufgerufen werden.

Geräte anlegen

Geräte können auf mehrere Arten angelegt werden:

1. Öffnen Sie das Kontextmenü durch einen Rechtsklick auf das Gerät. Klicken Sie im Kontextmenü auf **Add**, um den *Device properties dialog* (Geräte-Eigenschaften) für einen neuen mGuard zu öffnen.
2. Klicken Sie auf die Registerkarte **Device** und hier auf das Symbol in der Menüleiste und öffnen Sie den *Device properties dialog* für einen neuen mGuard.
3. Klicken Sie im Hauptmenü auf **New » Device,** um den *Device properties dialog* für einen neuen mGuard zu öffnen.
4. Klicken Sie im Hauptmenü auf **New » Device Import**, um mGuard-Geräte zu importieren.
5. Klicken Sie im Hauptmenü auf **New » Import ATV & Create Device**, um ein mGuard-Gerät mit einer ausgewählten ATV-Konfiguration zu erstellen.

Geräte bearbeiten

Ein Gerät kann auf mehrere Arten bearbeitet werden:

1. Führen Sie mit der linken Maustaste einen Doppelklick auf das Gerät in der Tabelle aus, um den *Device properties dialog* zu öffnen.
2. Wählen Sie mit der linken Maustaste das Gerät aus und öffnen Sie durch einen Rechtsklick das Kontextmenü. Öffnen Sie den *Device properties dialog* durch Klicken auf **Edit**.
3. Wählen Sie in der Gerätetabelle das zu ändernde Gerät. Klicken Sie im Hauptmenü auf **Edit » Edit Item,** um den *Device properties dialog* zu öffnen.

Der Menüpunkt **Edit** im Kontextmenü und die Schaltfläche **Edit** in der Symbolleiste sind nur aktiviert, wenn in der Gerätetabelle genau ein Gerät ausgewählt ist.

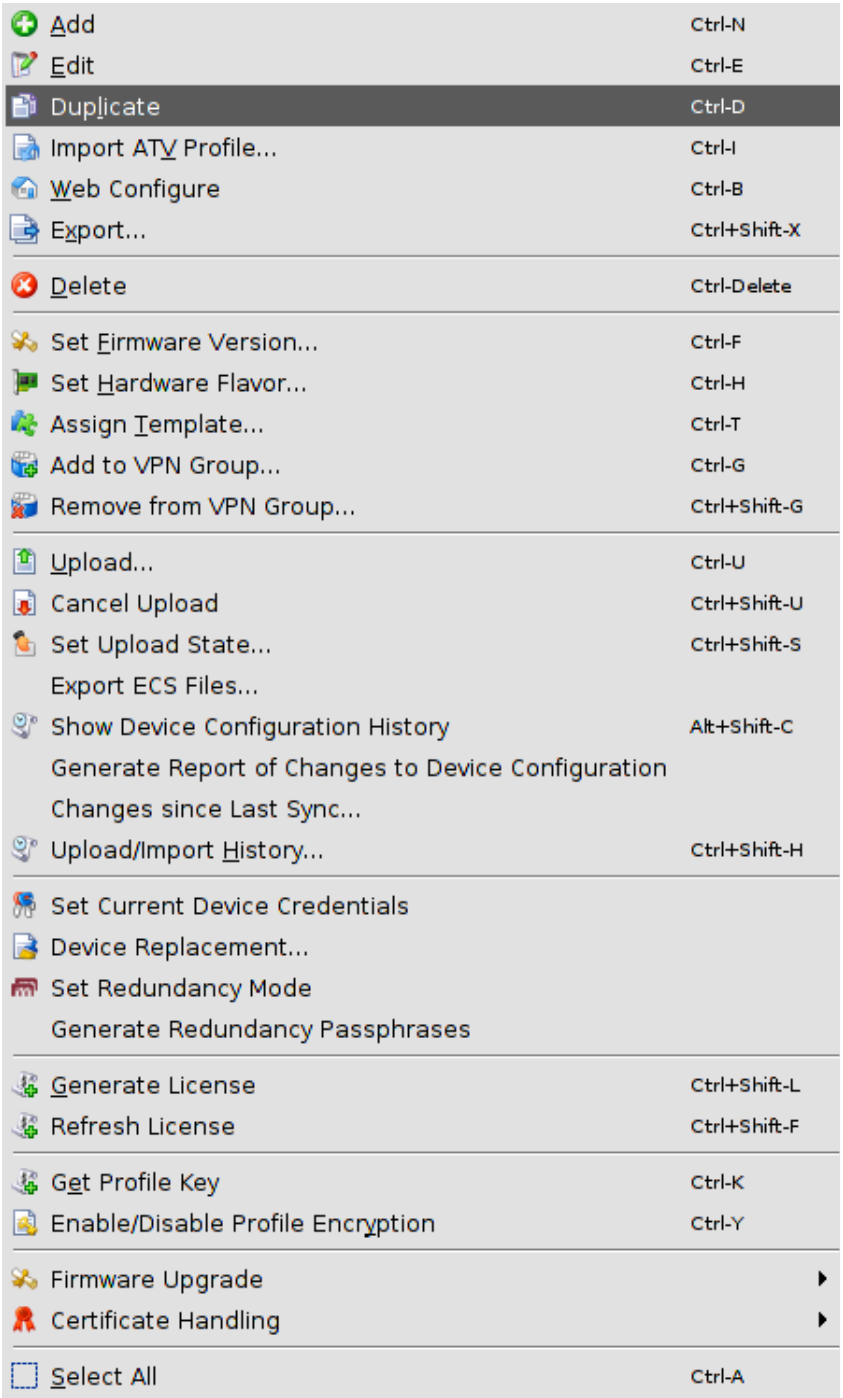
Geräte löschen

Geräte können auf mehrere Arten gelöscht werden:

1. Wählen Sie in der Gerätetabelle eines oder mehrere Geräte aus und öffnen Sie das Kontextmenü durch einen Klick mit der rechten Maustaste. Klicken Sie im Kontextmenü auf **Delete** um ein Gerät zu löschen.
2. Markieren Sie in der Tabelle die zu löschenden Geräte und klicken Sie in der Menüleiste auf das Symbol .

6.3.2 Geräte-Kontextmenü (Device context menu)

Das Geräte-Kontextmenü (*Device context menu*) enthält die folgenden Einträge (siehe unten).



Geräte-Kontextmenü (Device context menu)	
Add	Neues Gerät anlegen und den *Device properties dialog* (Geräte-Eigenschaften) des neuen Geräts öffnen.
Edit	Ausgewähltes Gerät bearbeiten (nur aktiv, wenn genau ein Gerät in der Übersichtstabelle markiert ist).
Duplicate	Öffnen Sie zum Erstellen einer Gerätekopie durch einen Klick mit der rechten Maustaste auf das Gerät in der Tabelle das Kontextmenü dieses Geräts. Klicken Sie im Kontextmenü auf **Duplicate**. mdm erstellt eine Kopie des Geräts und fügt zur Management-ID des neuen Geräts den String *_copy<n>* (<n> ist eine Zahl) hinzu. Hinweis: Der Menüeintrag **Duplicate** ist nur aktiviert, wenn in der Tabelle genau ein Gerät markiert ist.
Import ATV Profile	ATV-Profile in die ausgewählten Geräte importieren:

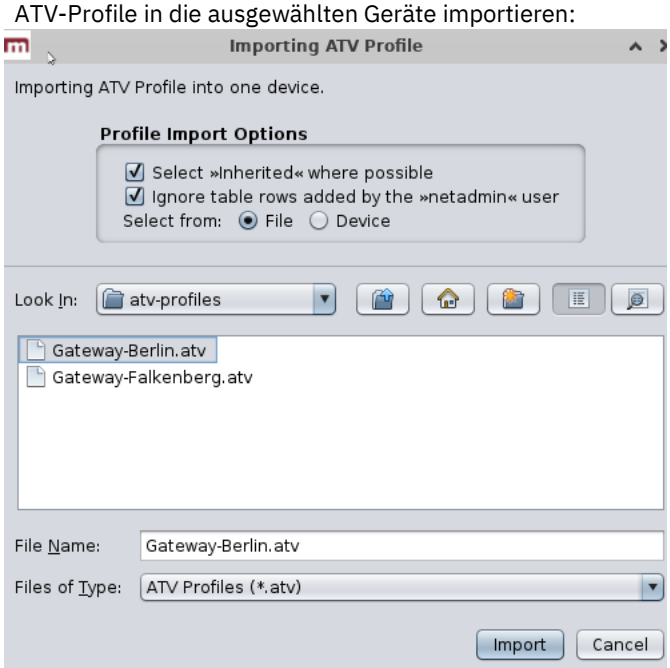


Bild 6-10 ATV-Import

Für den Import eines Profils stehen folgende Möglichkeiten zur Verfügung:

Select Inherited where possible

Bei Auswahl dieser Option werden die Variablen, für die der importierte Wert (d. h. der Wert im ATV-Profil) gleich dem geerbten Wert ist, auf Inherited gesetzt. Andernfalls werden alle im Profil enthaltenen Variablen ungeachtet ihres Werts auf Custom gesetzt.

Geräte-Kontextmenü (Device context menu)	
	Ignore table rows added by the netadmin user Vom lokalen **Netadmin**-Benutzer am mGuard erstellte Tabellenzeilen werden nicht importiert. **Select from File/Device** Bei Auswahl *File* wird das zu importierende ATV-Profil als Datei hochgeladen. Diese Möglichkeit steht nur zur Verfügung, wenn ein ATV-Import in ein Einzelgerät durchgeführt wird. Bei Auswahl *Device* lädt mdm das ATV-Profil vom mGuard herunter. Dafür muss sich mdm mit dem *ssh*-Protokoll am mGuard anmelden können; die **Accessible via**-Adresse muss gesetzt sein. Der zugehörige **SSH-Port** kann optional konfiguriert werden (siehe „Accessible via“ auf Seite 66). **Import into <A>/<B>** Wenn das Gerät im Redundanzmodus betrieben wird (weitere Informationen siehe „Redundanzmodus“ auf Seite 127), kann das Profil für das erste oder zweite physische Gerät in die Konfigurationsvariablen importiert werden. Einige Konfigurationsvariablen können nicht importiert werden und müssen ggf. manuell gesetzt werden: die Passwörter für Root- und Admin-Benutzer, die Passwörter der Firewallbenutzer und die Zertifikatssperrlisten (CRL). Von einem mGuard heruntergeladene ATV-Profile enthalten diese Variablen entweder überhaupt nicht oder nur in verschlüsselter Form (mit Hash). Hinweis: mdm importiert nicht das Passwort des Netadmin-Benutzers, wenn es im ATV-Profil gefunden wird. In einem von einem mGuard heruntergeladenen Profil ist es nicht enthalten.
Web Configure	Webinterface des Geräts öffnen, falls auf das Gerät zugegriffen werden kann (siehe auch **Accessible via**-Adresse in „Geräte-Eigenschaften (Device properties dialog)“ auf Seite 64). Jegliche Änderungen über das Webinterface werden vom nächsten mdm Konfigurations-Upload überschrieben (mit Ausnahme von Änderungen, die als Netadmin an lokalen Variablen vorgenommen wurden).
Export	Eine CSV-Datei mit den Grundeigenschaften (jedoch ohne die Konfigurationen) der markierten Geräte anlegen. Die Datei kann erneut in mdm importiert werden (siehe „mdm Hauptmenü“ auf Seite 19, Device Import.
Delete	Ausgewählte Geräte löschen.

Geräte-Kontextmenü (Device context menu)

Set Firmware Version

Firmware auf eine neue Version aktualisieren.

Da unterschiedliche Versionen der mGuard-Software über unterschiedliche Variablensätze verfügen, muss hier die zur auf dem mGuard installierten Firmware passende Firmware ausgewählt werden.

CAUTION: Unwiderrufliche Änderungen

Durch ein Upgrade der Firmwareversion des Geräts können sich die Werte der Standardvariablen in der Zielversion ändern.

Ein Downgrade zurück auf eine ältere Version ist nicht möglich. Daher ist bei einer Änderung der Firmwareversion größte Sorgfalt geboten. Weitere Informationen dazu erhalten Sie unter „Versionseinstellungen der Firmware und Vererbung“ auf Seite 84.

Prüfen Sie nach einem Upgrade alle Änderungen an den Variablen in der „Device Configuration History“ (siehe „Dialog Konfigurationsverlauf“ auf Seite 129).

ACHTUNG: Neue Standardwerte in mGuard-Firmware 8.5 und 8.6

Wird in der mGuard-Firmware ein Standardwert (*Default value*) geändert, so ist die Verwaltung dieses Wertes in mdm betroffen:

1. wenn die Firmware-Version eines verwalteten Geräts auf eine Firmwareversion mit einem geänderten Standardwert aktualisiert wird,
2. wenn ein erbendes „Kind“, das eine andere mGuard-Firmwareversion besitzt als sein Elternteil, einen Wert mit einem anderen Standardwert erbt.

Das damit verbundene Verhalten von mdm wird im Kapitel „Verhalten von geänderten Standardwerten (mGuard 8.5/8.6)“ auf Seite 43 beschrieben.

Weiterführende Informationen finden Sie unter „Firmware-Upgrades mit mdm verwalten“ auf Seite 124.

Set Hardware Flavor

Hardwarekonfiguration einrichten. Weiterführende Informationen finden Sie unter „Hardwarekonfigurationen“ auf Seite 26.

Assign Template

Dialog *Assign template* öffnen und den markierten Geräten ein Template zuweisen.

Add to VPN Group

Dialog öffnen, um die markierten Geräte zu einer VPN-Gruppe hinzuzufügen.

Geräte-Kontextmenü (Device context menu)	
Remove from VPN Group	Dialog öffnen, um die markierten Geräte aus einer VPN-Gruppe zu entfernen.
Upload	Upload-Dialog öffnen. Weiterführende Informationen finden Sie unter „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107.
Cancel Upload	Den für die ausgewählten Geräte vorgesehenen Upload abbrechen.
Set Upload State	Der Upload-Status wird nie automatisch auf *successfully uploaded* gesetzt, wenn kein Push-Upload durchgeführt wird und kein Pull-Feedback vom Konfigurationsserver eingeht (z. B. bei einem Verwendungsszenario, bei dem die exportierten Konfigurationsprofile manuell am Gerät installiert werden). Sie können mit dieser Option den Upload-Status von Hand auf *successfully uploaded* setzen. Wählen Sie in der Gerätetabelle eines oder mehrere Geräte aus, öffnen Sie das Kontextmenü durch einen Klick mit der rechten Maustaste und klicken Sie auf **Set upload state**.  Wenn aufgrund des Gerätezustands ein erfolgreicher Upload nicht möglich ist (beispielsweise wenn ein None-Wert nicht überschrieben wurde, siehe Kapitel 6.4.4), kann der Upload-Status nicht auf *successfully uploaded* gesetzt werden.
Export ECS Files	(verschlüsselte) ECS-Dateien für die ausgewählten Geräte herunterladen. ECS-Dateien werden standardmäßig verschlüsselt. Der Benutzer *root* und andere Benutzer mit der entsprechenden Berechtigung können die Verschlüsselung deaktivieren und unverschlüsselte ECS-Dateien herunterladen. (Vergabe von Rechten an autorisierte Benutzer siehe „Benutzer, Rollen und Berechtigungen verwalten“ auf Seite 115). ECS-Dateien können für die Konfiguration von mGuard Geräten verwendet werden, die diesen Mechanismus über SD-Karten unterstützen; weitere Informationen siehe mGuard firmware manual. Ein Dialog wird geöffnet, in dem das Verzeichnis zum Speichern der ECS-Dateien ausgewählt werden kann.  Die Voraussetzungen zum Erstellen verschlüsselter ECS-Dateien sind die gleichen wie die für verschlüsselte Profile. Siehe “„Profil verschlüsseln“ auf Seite 109”.
Show Device Configuration History	Dialog mit dem Konfigurationsverlauf öffnen. Weiterführende Informationen siehe „Dialog Konfigurationsverlauf“ auf Seite 129.

Geräte-Kontextmenü (Device context menu)

Generate Report of Changes to Device Configuration

Dialog zum Erstellen eines Berichts zu Änderungen an Gerätekonfigurationen öffnen. Weiterführende Informationen siehe „Änderungsbericht“ auf Seite 136.

Changes since last Sync

Ein Konfigurationsdialog öffnet sich und zeigt durchgeführte Änderungen seit der letzten Synchronisation an.

Synchronisierung bedeutet entweder ein Update via

- SSH-Upload auf das Gerät (*upload via SSH*),
- Pull-Export zum Gerät über einen HTTPS-Konfigurationspullserver + Rückmeldung (*prepare pull configuration*),
- Online-Import von dem Gerät nach mdm (*Import ATV Profile*).

Wurde das Gerät schon einmal erfolgreich synchronisiert, werden die Konfigurationsänderungen seit dem letzten Upload/Online-Import angezeigt.

Wurde das Gerät per Pull-Export aktualisiert (*pull configuration*), zeigt *Last sync* diese Synchronisation nur an, wenn **alle** folgenden Punkte zutreffen:

1. Die Gerätekonfiguration in mdm hat sich seit dem geplanten Pull-Export nicht geändert.
2. Nach dem Pull-Export fand kein zusätzlicher SSH-Upload statt.
3. Der Pull-Export hat die Konfiguration auf dem mGuard-Gerät tatsächlich geändert. (Nachfolgende Pull-Feedback-Meldungen, bei denen keine Konfigurationsänderung stattfindet, werden nicht als Synchronisationsereignisse registriert.)

Das Verhalten ähnelt dem Auswählen von zwei Historie-Einträgen im Dialog „Device Configuration History“ und dem Klicken auf „*Compare...*“ (siehe „Frühere Konfigurationen vergleichen“ auf Seite 133).

Wurde das Gerät noch nie synchronisiert, werden die Konfigurationsänderungen seit der Erstellung des Gerätes angezeigt.

Wenn es sich bei der aktuellen Konfiguration um die zuletzt synchronisierte Konfiguration handelt, wird im Konfigurationsdialog die aktuelle Konfiguration angezeigt.

Geräte-Kontextmenü (Device context menu)	
Upload/Import History	Zeigt eine Übersicht der letzten Synchronisierungen (Synchronization actions) an. Synchronisierung bedeutet entweder ein Update via – SSH-Upload auf das Gerät (*upload via SSH*), – Pull-Export zum Gerät über einen HTTPS-Konfigurationspullserver + Rückmeldung (*prepare pull configuration*), – Online-Import von dem Gerät nach mdm (*Import ATV Profile*).
Set Current Device Credentials	Dialog öffnen, in dem die Anmeldedaten des Geräts eingegeben werden können. Folgende Attribute können gesetzt werden: **Active root and admin passwords** Aktive Passwörter sind die aktuell für das Gerät gültige Passwörter. Sie können sich von den konfigurierten Passwörtern unterscheiden, wenn die aktuelle Konfiguration noch nicht in den mGuard hochgeladen oder davon gezogen wurde. mdm registriert alle aktiven Passwörter, da das Root-Passwort zum Setzen eines neuen Passworts und das Admin-Passwort für die Anmeldung am mGuard benötigt wird. **Reset SSH Host Key** mdm speichert den SSH-Schlüssel eines mGuard nach dem ersten Kontakt. Bei Austausch eines mGuard stimmen die SSH-Schlüssel nicht überein und mdm verweigert jegliche Verbindung mit dem ausgetauschten Gerät. Mit dieser Funktion kann der SSH-Schlüssel zurückgesetzt werden. **Renew Secure Key Length** Mit dieser Funktion generiert der mGuard *SSH*- und *HTTPS*-Schlüssel beim nächsten Upload oder Ziehen einer Konfiguration. Wenn noch Schlüssel mit 1024 Bit verwendet werden, wird die Erstellung neuer Schlüssel empfohlen.
Device Replacement	Alle gerätespezifischen Einstellungen werden auf die Werkseinstellung zurückgesetzt. Diese Funktion kann nach dem Austausch eines defekten Geräts verwendet werden. – Folgende Einstellungen werden zurückgesetzt: – Firmwareversion des Geräts – Serial Number – Flash ID – SSH Hostkey – Profile Encryption Key – Mit dem Gerät verbundene Lizenzen

Geräte-Kontextmenü (Device context menu)	
Set Redundancy Mode	Dialog öffnen, in dem der Redundanzbetrieb für die ausgewählten Geräte aktiviert oder deaktiviert werden kann.
Generate Redundancy Passphrases	Variablen der Redundanz-Passphrases in der Gerätekonfiguration auf zufällige Werte setzen.
Generate License	Weiterführende Informationen zur Lizenzverwaltung siehe „Gerätelizenzen und Voucher verwalten“ auf Seite 112.
Refresh License	Weiterführende Informationen zur Lizenzverwaltung siehe „Gerätelizenzen und Voucher verwalten“ auf Seite 112.
Get Profile Key	Profilschlüssel vom Lizenzserver abholen. Einzelheiten siehe Kapitel „Profil verschlüsseln“ auf Seite 109.
Enable/Disable profile encryption	Verschlüsselung der Konfigurationsprofile für die ausgewählten Geräte aktivieren oder deaktivieren. Einzelheiten siehe Kapitel „Profil verschlüsseln“ auf Seite 109.
Firmware Upgrade » Schedule upgrade to latest patches	Firmware-Upgrade für die aktuellsten verfügbaren Patches planen. Weiterführende Informationen finden Sie unter „Firmware-Upgrades mit mdm verwalten“ auf Seite 124.
Firmware Upgrade » Schedule upgrade to latest minor release	Firmware-Upgrade für die aktuellsten verfügbaren Minor Releases planen. Weiterführende Informationen finden Sie unter „Firmware-Upgrades mit mdm verwalten“ auf Seite 124.
Firmware Upgrade » Schedule upgrade to next major version	Firmware-Upgrade für das nächste Major Release planen. Weiterführende Informationen finden Sie unter „Firmware-Upgrades mit mdm verwalten“ auf Seite 124.
Firmware Upgrade » Unschedule upgrade	Firmware-Upgrade aus der Planung nehmen.
Certificate Handling » Request additional certificate	Maschinenzertifikat für das Gerät anfordern und der Liste der vorhandenen Maschinenzertifikate hinzufügen. Weiterführende Informationen finden Sie unter „Maschinenzertifikate“ auf Seite 120.
Certificate Handling » Request replacement certificate	Maschinenzertifikat für das Gerät anfordern und alle vorhandenen Maschinenzertifikate durch das neue ersetzen. Weiterführende Informationen finden Sie unter „Maschinenzertifikate“ auf Seite 120. Alle vorhandenen Maschinenzertifikate im Gerät werden gelöscht, auch wenn sie manuell importiert worden sind. Dies führt dazu, dass das Gerät nur noch über ein einziges Maschinenzertifikat (das neu angeforderte) verfügt. Daher ist diese Funktion für alle Geräte, die ein einzelnes Maschinenzertifikat enthalten, sehr hilfreich.
Certificate Handling » Issue and Export Certificate Requests	Zertifikatanfrage für die manuelle Zertifikatregistrierung generieren. Weiterführende Informationen siehe „Maschinenzertifikate“ auf Seite 120.

Geräte-Kontextmenü (Device context menu)		
	Select All	Alle nicht durch den Tabellenfilter ausgeschlossenen Geräte auswählen.

6.3.3 Geräte-Eigenschaften (Device properties dialog)

Im *Device properties dialog* können die Variablen des mGuard und deren zugehörige Einstellungen für das Gerät konfiguriert werden.

Informationen zum Anlegen, Löschen oder Bearbeiten von Geräten siehe „mdm Hauptfenster“ auf Seite 18.

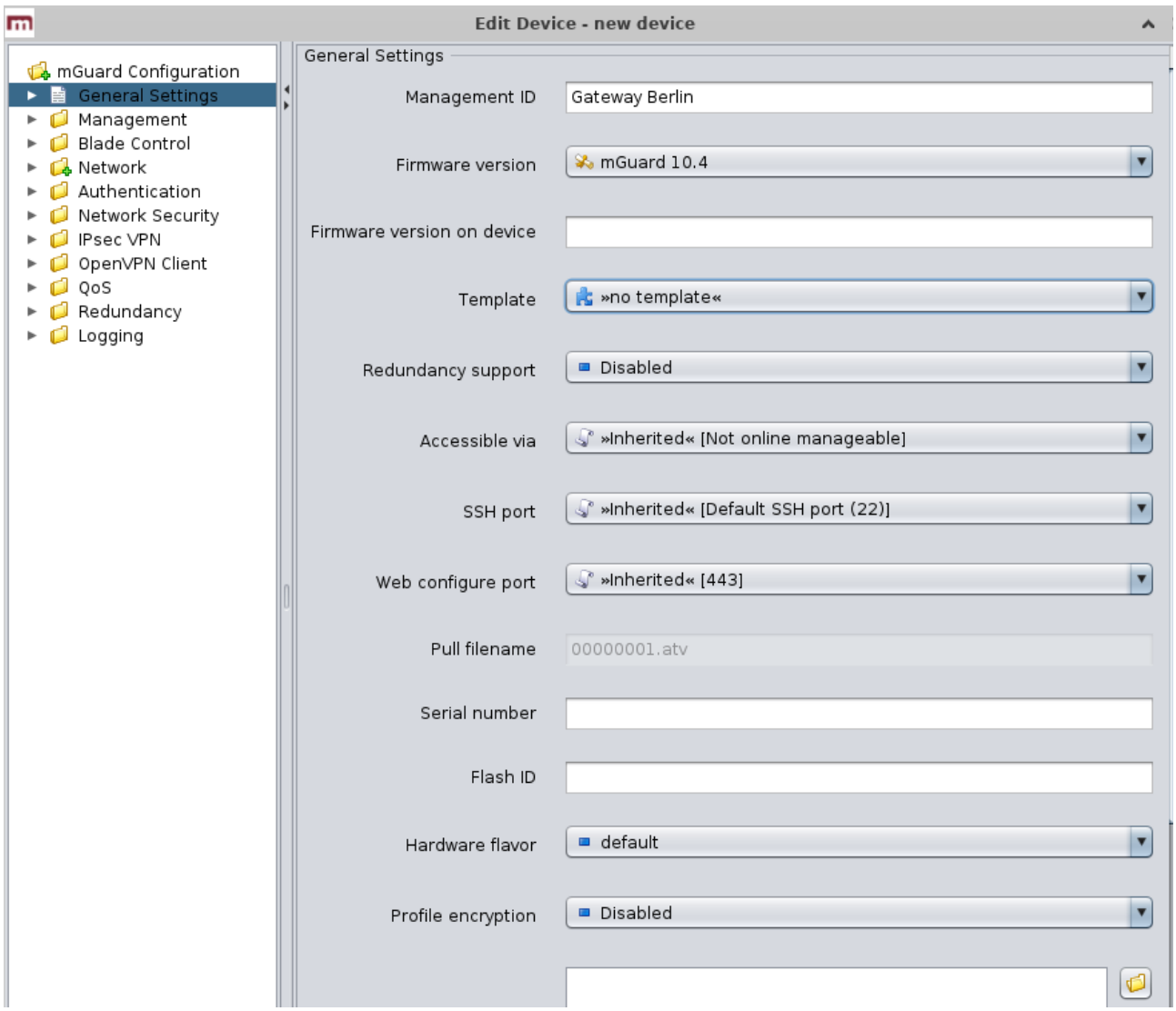


Bild 6-11 *Device properties dialog* (Geräte-Eigenschaften)

Ähnlich wie der *Template properties dialog* (Template-Eigenschaften) (siehe Kapitel 6.4.3) enthält auch der *Device properties dialog* auf der linken Seite einen Navigationsbaum, der der Menüstruktur der Webinterface des mGuard ähnelt. Mit dem Navigationsbaum kann bequem zwischen den Variablen des mGuard navigiert werden.

Der *Device properties dialog* enthält den Menüpunkt **General settings** zur Konfiguration zusätzlicher Parameter mit Bezug zu mdm. Die folgenden Parameter können in den **General settings** eingestellt werden.

Geräte-Eigenschaften (Device properties dialog)		
General Settings	**Management ID**	Anhand dieser ID wird das Gerät innerhalb des mdm erkannt. Die Management-ID muss eindeutig sein.
	Firmware Version	Firmware auf eine neue Version aktualisieren. Da unterschiedliche Versionen der mGuard-Software über unterschiedliche Variablensätze verfügen, muss hier die zur auf dem mGuard installierten Firmware passende Firmware ausgewählt werden.  **CAUTION: Unwiderrufliche Änderungen** Durch ein Upgrade der Firmwareversion des Geräts können sich die Werte der Standardvariablen in der Zielversion ändern. Ein Downgrade zurück auf eine ältere Version ist nicht möglich. Daher ist bei einer Änderung der Firmwareversion größte Sorgfalt geboten. Weitere Informationen dazu erhalten Sie unter „Versionseinstellungen der Firmware und Vererbung“ auf Seite 84. Prüfen Sie nach einem Upgrade alle Änderungen an den Variablen in der „Device Configuration History“ (siehe „Dialog Konfigurationsverlauf“ auf Seite 129).  **ACHTUNG: Neue Standardwerte in mGuard-Firmware 8.5 und 8.6** Wird in der mGuard-Firmware ein Standardwert (*Default value*) geändert, so ist die Verwaltung dieses Wertes in mdm betroffen: 1. wenn die Firmware-Version eines verwalteten Geräts auf eine Firmwareversion mit einem geänderten Standardwert aktualisiert wird, 2. wenn ein erbendes „Kind“, das eine andere mGuard-Firmwareversion besitzt als sein Elternteil, einen Wert mit einem anderen Standardwert erbt. Das damit verbundene Verhalten von mdm wird im Kapitel „Verhalten von geänderten Standardwerten (mGuard 8.5/8.6)“ auf Seite 43 beschrieben.  Weitere Informationen zur Verwaltung von Firmware-Upgrades Ihrer Geräte mit mdm siehe Kapitel 7.6.
	Firmware version on device	In diesem Feld wird die aktuell auf dem Gerät installierte Firmwareversion angezeigt. Sie kann manuell eingesetzt werden, wird aber bei jedem Push-Upload oder Pull-Feedback von dem Wert überschrieben, der auf dem Gerät gefunden wird.

Geräte-Eigenschaften (Device properties dialog)		
	Template	Das übergeordnete Template des Geräts.
	Redundancy support	Die Unterstützung für den Redundanzbetrieb des Geräts kann aktiviert oder deaktiviert werden.
	Accessible via	Dies ist die IP-Adresse oder der Hostname, über die der mdm-Server auf den mGuard zugreifen kann, um einen SSH-Push-Export oder einen ATV-Profilimport der Konfiguration durchzuführen oder das Web-Interface zu öffnen. Weitere Informationen zum Uploadvorgang finden Sie unter „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107. Die folgenden Werte können unter **Accessible via** ausgewählt werden (der **SSH-Port** und der **Web configuration port** können in den folgenden Feldern (siehe unten) angegeben werden. **Not online manageable** Das Gerät wird nicht über SSH-Push verwaltet. **Internal interface in auto stealth mode [1.1.1.1]** mdm verwendet für den Zugriff auf mGuard die Adresse 1.1.1.1 (Adresse der internen Schnittstelle im automatischen geschützten Modus). **Stealth management address** mdm greift im geschützten Modus auf die externe oder interne Schnittstelle des mGuard zu. **First external IP address** mdm greift im Router-Modus auf die externe Schnittstelle des mGuard zu. **First internal IP address** mdm greift im Router-Modus auf die interne Schnittstelle des mGuard zu. **Custom value** Für den Zugriff auf den mGuard in NAT-Szenarien ist möglicherweise ein benutzerspezifischer Wert (IP-Adresse oder Hostname) erforderlich.

Geräte-Eigenschaften (Device properties dialog)		
	SSH port	Dies ist die SSH-Portnummer, über die der mdm-Server auf den mGuard zugreifen kann, um einen SSH-Push-Export oder einen ATV-Profilimport der Konfiguration durchzuführen. In einigen Fällen kann es notwendig sein, den Standard-SSH-Port zu ändern, um eine Verbindung zum Gerät herzustellen (z. B. wenn das Gerät nicht mit dem Internet verbunden ist, sondern einen Port zugewiesen bekommt, der von der Firewall übermittelt wird). Wenn **Port for incoming SSH connections** ausgewählt ist, wird der unter *Management >> System Settings >> Shell Access >> Shell Access Options >> Port for incoming SSH connections* konfigurierte Port verwendet und in der Übersichtstabelle angezeigt. Weitere Informationen zum Uploadvorgang finden Sie unter „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107.
	Web configuration port	Dies ist die HTTPS-Portnummer, über die die grafische Weboberfläche des mGuard aufgerufen wird. In einigen Fällen kann es notwendig sein, den Standard-HTTPS-Port zu ändern, um eine Verbindung zur Weboberfläche herzustellen (z. B. wenn das Gerät einen Port zugewiesen bekommt, der von der Firewall übermittelt wird). Wenn **Remote HTTPS TCP port** ausgewählt ist, wird der Port verwendet, der unter *Management >> Web Settings >> Access >> HTTPS Web Access >> Remote HTTPS TCP port* ausgewählt ist.
	Pull filename (read only)	Bei einem Export der Konfiguration in das Dateisystem wird eine eindeutige, automatisch zugewiesene und unveränderliche ID als Name der Konfigurationsdatei verwendet. Der Dateiname wird in diesem Feld angezeigt. Optional können weitere Exportdateien mit einem anderen Benennungsschema generiert werden, weitere Informationen dazu siehe „mdm-Server (Datei *preferences.xml*)“ auf Seite 161.
	Serial number	Die Seriennummer des Geräts. Die Seriennummer wird für Lizenzangelegenheiten benötigt, vor allem zum **Anfordern und Aktualisieren von Lizenzen** (siehe „Lizenzen anfordern/generieren“ auf Seite 112). Sie kann manuell eingesetzt werden, wird aber bei jedem Push-Upload oder Pull-Feedback von dem Wert überschrieben, der auf dem Gerät gefunden wird. Wenn kein Push-Upload durchgeführt wird und kein Pull-Feedback eingeht (z. B. bei einem Verwendungsszenario, bei dem die exportierten Konfigurationsprofile manuell am Gerät installiert werden), muss die Seriennummer hier eingegeben werden, wenn Sie Dateinamen mit Seriennummer für die Pull-Konfiguration anlegen möchten.

Geräte-Eigenschaften (Device properties dialog)	
Flash ID	Die Flash-ID des Geräts. Die Flash-ID wird für Lizenzangelegenheiten benötigt, vor allem für die **Aktualisierung von Lizenzen** (siehe „Lizenzen erneuern“ auf Seite 114). Sie kann manuell eingesetzt werden, wird aber bei jedem Push-Upload oder Pull-Feedback von dem Wert überschrieben, der auf dem Gerät gefunden wird.
Comment	Optionale Anmerkungen.
Hardware flavor	Die Hardwarekonfiguration des Geräts (siehe „Hardwarekonfigurationen“ auf Seite 26). Bei Einstellung auf *rs2000* werden Variablen, die für diese Plattform nicht unterstützt werden, weggelassen.
Profile encryption	Verschlüsselung der Konfigurationsprofile für die ausgewählten Geräte aktivieren oder deaktivieren. Einzelheiten siehe Kapitel „Profil verschlüsseln“ auf Seite 109.
Additional ATV include	Dies ist ein Textfeld für zusätzliche Einstellungen, die in die Konfigurationsdatei des mGuard einzufügen sind. Die Eingabe muss sich an die Konventionen der mGuard Konfigurationsdatei halten. Durch Auswahl einer Datei mit dem Symbol *File Chooser* können Sie auch den Inhalt einer Textdatei in das Feld importieren.  Die enthaltene Konfiguration wird den generierten mdm Einstellungen hinzugefügt und daher überschreiben Einstellungen für dieselbe Variable im Feld Include die Einstellungen, die von mdm generiert wurden.

6.4 Templates konfigurieren

6.4.1 Template-Übersicht (Template overview table)

Klicken Sie auf die Registerkarte **Template**, um die Template-Übersicht (*Template overview table*) aufzurufen.

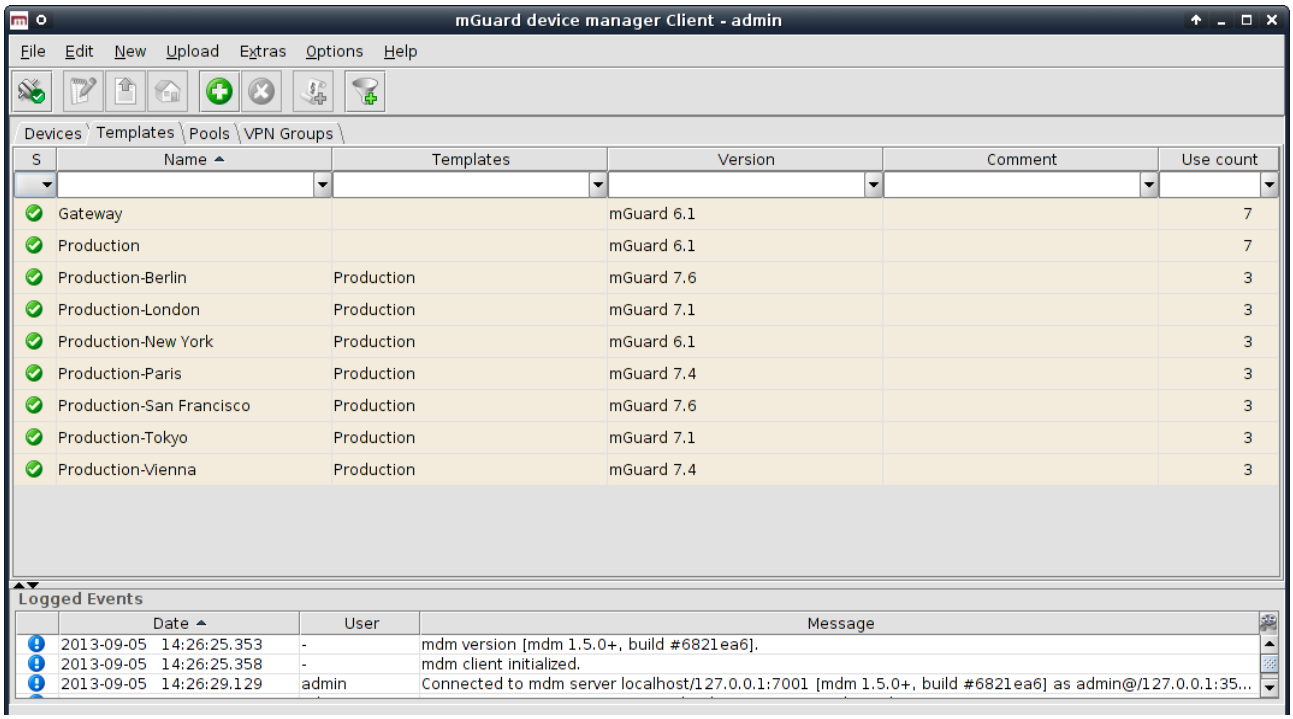


Bild 6-12 Template-Übersicht (*Template overview table*)

Spalten der Template-Übersicht (Template overview table)

Die Template-Übersicht (*Template overview table*) enthält folgende Spalten.

Setzen Sie zum Ändern der Spaltenbreite den Cursor in die Kopfzeile der Tabelle an die Grenze zwischen zwei Spalten und ziehen Sie bei gedrückter linker Maustaste die Grenze in die gewünschte Richtung. Setzen Sie zum Verschieben einer Spalte den Cursor in die Kopfzeile der Tabelle und ziehen Sie bei gedrückter linker Maustaste die Spalte an den gewünschten Platz.

Status (*S*)	Das Status-Symbol zeigt an, ob das Template aktuell gesperrt ist.
Name	Der dem Template zugewiesene Name. Der Name kann unter **General Settings** im *Template properties dialog* (Template-Eigenschaften) eingetragen werden (siehe „Template-Eigenschaften (Template properties dialog)“ auf Seite 74).

Templates	In dieser Spalte wird eine durch Kommas getrennte Liste der übergeordneten Templates des Templates angezeigt. Der erste Punkt auf der Liste ist das unmittelbar übergeordnete Template.
Version	Für das Template verwendete Firmwareversion des mGuard.
Comment	Optionale Anmerkungen. Die Anmerkungen können unter **General Settings** im *Template properties dialog* (Template-Eigenschaften) eingetragen werden (siehe „Template-Eigenschaften (Template properties dialog)“ auf Seite 74).
Use count	In dieser Spalte wird die Anzahl der Geräte oder anderen Templates angezeigt, die dieses Template verwenden.

Tabelle filtern und sortieren

Mit der Kopfzeile der Tabelle können die Einträge sortiert werden. Durch Anklicken der Kopfzeile einer Spalte wird die (primäre) Sortierung anhand dieser Spalte aktiviert. Dies wird durch einen Pfeil in der Kopfzeile angezeigt. Durch einen zweiten Klick auf dieselbe Kopfzeile erfolgt die Sortierung in umgekehrter Reihenfolge. Durch Anklicken einer weiteren Spalte wird anhand dieser neuen Spalte sortiert, wobei die vorher aktive Spalte als zweites Kriterium für die Sortierung herangezogen wird.

In der ersten Tabellenzeile wird die Eingabe regulärer Ausdrücke akzeptiert (siehe Kapitel 11, *Regular expressions*), die zum effizienten Filtern der Tabelleneinträge verwendet werden können. Eine Spalte, die keinen Text enthält (d. h. Spalte **S**) kann nicht auf der Grundlage regulärer Ausdrücke gefiltert werden.

Das Filterkriterium **Use count** wird nicht als regulärer Ausdruck interpretiert, sondern als Liste von Zahlen oder Zahlenbereichen, die durch Komma getrennt sind (z. B. 0, 2 – 3).

Der Filterverlauf wird für den aktuellen Benutzer gespeichert und kann über die Dropdown-Funktion der Filterfelder aufgerufen werden.

Templates anlegen

Neue Templates können auf mehrere Arten angelegt werden:

1. Öffnen Sie das Kontextmenü durch einen Rechtsklick auf das Template. Klicken Sie im Kontextmenü auf **Add**, um den *Template properties dialog* (Template-Eigenschaften) für einen neuen Template zu öffnen.
2. Klicken Sie auf die Registerkarte **Template** und hier auf das Symbol  in der Menüleiste und öffnen Sie den *Template properties dialog* für ein neues Template.
3. Klicken Sie für ein neues Template im Hauptmenü auf **New » Template** und öffnen Sie den *Template properties dialog*.

Editing templates

Ein Template kann auf mehrere Arten bearbeitet werden:

1. Führen Sie mit der linken Maustaste einen Doppelklick auf das Template in der Tabelle aus, um den *Device properties dialog* (Geräte-Eigenschaften) zu öffnen.
2. Wählen Sie mit der linken Maustaste das Template aus und öffnen Sie durch einen Rechtsklick das Kontextmenü. Öffnen Sie den *Template properties dialog* durch Klicken auf **Edit**.

3. Wählen Sie in der Template-Tabelle das zu ändernde Template. Klicken Sie im Hauptmenü auf **Edit » Edit Item** um den *Template properties dialog* zu öffnen.

> Der Menüpunkt **Edit** im Kontextmenü und die Schaltfläche **Edit** in der Symbolleiste sind nur aktiviert, wenn in der Template-Tabelle genau ein Template ausgewählt ist.

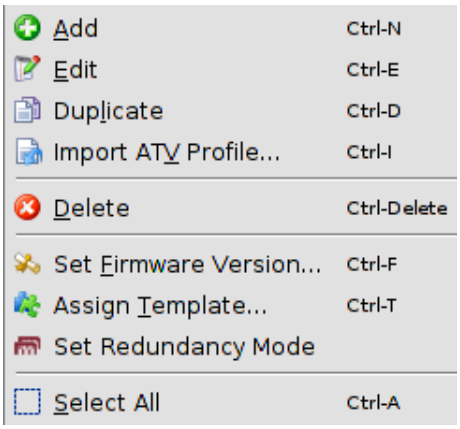
Deleting templates

Templates können auf mehrere Arten gelöscht werden:

1. Wählen Sie ein oder mehrere Templates aus und öffnen Sie das Kontextmenü durch einen Rechtsklick auf das Template. Klicken Sie im Kontextmenü auf **Delete** um ein Template zu löschen.
2. Markieren Sie in der Template-Tabelle die zu löschenden Templates und klicken Sie in der Menüleiste auf das Symbol .

> Templates, die noch Geräten oder anderen Templates zugewiesen sind, können nicht gelöscht werden.

6.4.2 Template-Kontextmenü (Template context menu)



Im Template-Kontextmenü stehen folgende Optionen zur Verfügung.

Template-Kontextmenü		
	Add	Neues Template anlegen und den *Template properties dialog* (Template-Eigenschaften) dieses Templates öffnen.
	Edit	Ausgewähltes Template bearbeiten (nur aktiv, wenn genau ein Template in der Übersichtstabelle markiert ist).
	Duplicate	Öffnen Sie zum Anlegen einer Template-Kopie durch einen Klick mit der rechten Maustaste auf das Template in der Tabelle das Template-Kontextmenü. Klicken Sie im Kontextmenü auf **Duplicate**. mdm erstellt eine Kopie des Templates und fügt zum Namen des neuen Templates den String *_copy<n>* (<n> ist eine Zahl) hinzu. Hinweis: Der Menüeintrag **Duplicate** ist nur aktiviert, wenn in der Tabelle genau ein Template markiert ist.

Template-Kontextmenü	
Import ATV Profile	Ein ATV-Profil in die ausgewählten Templates importieren. Dies funktioniert genauso wie der Import von ATV-Profilen in Geräte, nähere Informationen siehe „Geräte-Kontextmenü (Device context menu)“ auf Seite 55.
Delete	Ausgewählte Templates löschen.
Set Firmware Version	Firmware auf eine neue Version aktualisieren. Da unterschiedliche Versionen der mGuard-Software über unterschiedliche Variablensätze verfügen, muss hier die zur auf dem mGuard installierten Firmware passende Firmware ausgewählt werden. **CAUTION: Unwiderrufliche Änderungen** Durch ein Upgrade der Firmwareversion des Geräts können sich die Werte der Standardvariablen in der Zielversion ändern. Ein Downgrade zurück auf eine ältere Version ist nicht möglich. Daher ist bei einer Änderung der Firmwareversion größte Sorgfalt geboten. Weitere Informationen dazu erhalten Sie unter „Versionseinstellungen der Firmware und Vererbung“ auf Seite 84. Prüfen Sie nach einem Upgrade alle Änderungen an den Variablen in der „Device Configuration History“ (siehe „Dialog Konfigurationsverlauf“ auf Seite 129). **ACHTUNG: Neue Standardwerte in mGuard-Firmware 8.5 und 8.6** Wird in der mGuard-Firmware ein Standardwert (*Default value*) geändert, so ist die Verwaltung dieses Wertes in mdm betroffen: 1. wenn die Firmware-Version eines verwalteten Geräts auf eine Firmwareversion mit einem geänderten Standardwert aktualisiert wird, 2. wenn ein erbendes „Kind“, das eine andere mGuard-Firmwareversion besitzt als sein Elternteil, einen Wert mit einem anderen Standardwert erbt. Das damit verbundene Verhalten von mdm wird im Kapitel „Verhalten von geänderten Standardwerten (mGuard 8.5/8.6)“ auf Seite 43 beschrieben. Weiterführende Informationen finden Sie unter „Firmware-Upgrades mit mdm verwalten“ auf Seite 124.
Assign Template	Dialog *Assign template* öffnen und den markierten Templates ein übergeordnetes Template zuweisen.

Template-Kontextmenü		
	Set Redundancy Mode	Dialog öffnen, in dem der Redundanzbetrieb für die ausgewählten Templates aktiviert oder deaktiviert werden.
	Select All	Alle nicht durch den Tabellenfilter ausgeschlossenen Templates auswählen.

6.4.3 Template-Eigenschaften (Template properties dialog)

Mit Templates lassen sich sehr viele Geräte bequem und effizient konfigurieren und verwalten.

Durch die Zuweisung eines Templates zu einem Gerät (siehe „Geräte-Eigenschaften (Device properties dialog)“ auf Seite 64) erbt das Gerät die Template-Einstellungen und verwendet die im Template definierten Werte. Je nach Berechtigungseinstellungen können die Template-Einstellungen in der Gerätekonfiguration überschrieben werden.

In diesem Kapitel ist das Konzept der Templates beschrieben. Weiterführende Informationen zu Templates und Vererbung finden Sie unter „Mit Templates arbeiten“ auf Seite 80.

Informationen zum Anlegen, Löschen oder Bearbeiten von Templates siehe „mdm Hauptfenster“ auf Seite 18.

Im folgenden Screenshot ist der *Template properties dialog* (Template-Eigenschaften) abgebildet.

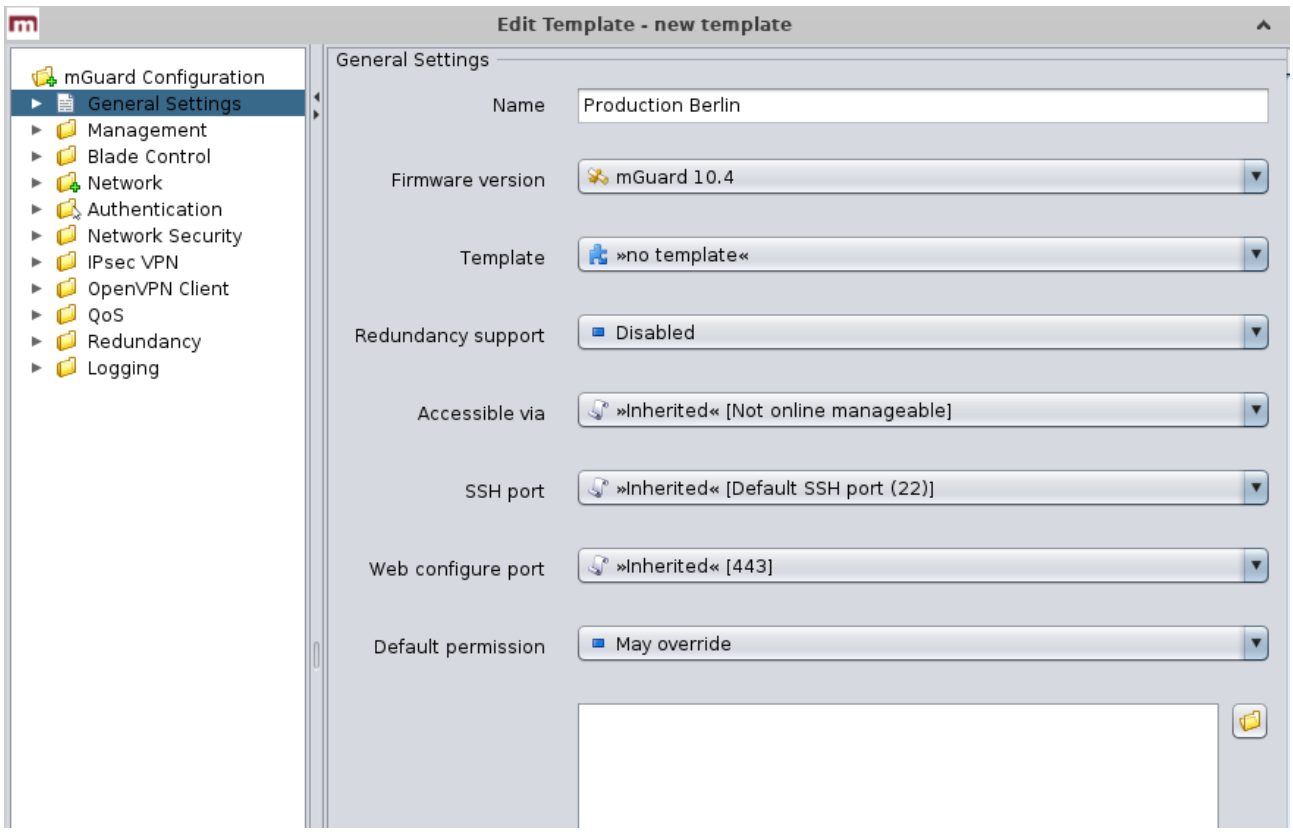


Bild 6-13 *Template properties dialog* (Template-Eigenschaften)

General settings

Ähnlich wie der *Device properties dialog* (siehe „Geräte-Eigenschaften (Device properties dialog)“ auf Seite 64) enthält auch der *Template properties dialog* (Template-Eigenschaften) auf der linken Seite ein Menü, das der Struktur der Webinterface des mGuard ähnelt.

Zusätzlich enthält der *Template properties dialog* den Menüpunkt **General settings** zur Konfiguration zusätzlicher Parameter mit Bezug zu mdm.

Dialog Template Properties

Name

Name des Templates.

Firmware version

Firmware auf eine neue Version aktualisieren.

Da unterschiedliche Firmwareversionen des mGuard über unterschiedliche Variablensätze verfügen, muss hier die vom Template zu verwendende Firmware (oder der Variablensatz) ausgewählt werden.

CAUTION: Unwiderrufliche Änderungen

Durch ein Upgrade der Firmwareversion des Geräts können sich die Werte der Standardvariablen in der Zielversion ändern.

Ein Downgrade zurück auf eine ältere Version ist nicht möglich. Daher ist bei einer Änderung der Firmwareversion größte Sorgfalt geboten. Weitere Informationen dazu erhalten Sie unter „Versionseinstellungen der Firmware und Vererbung“ auf Seite 84.

Prüfen Sie nach einem Upgrade alle Änderungen an den Variablen in der „Device Configuration History“ (siehe „Dialog Konfigurationsverlauf“ auf Seite 129).

ACHTUNG: Neue Standardwerte in mGuard-Firmware 8.5 und 8.6

Wird in der mGuard-Firmware ein Standardwert (*Default value*) geändert, so ist die Verwaltung dieses Wertes in mdm betroffen:

1. wenn die Firmware-Version eines verwalteten Geräts auf eine Firmwareversion mit einem geänderten Standardwert aktualisiert wird,
2. wenn ein erbendes „Kind“, das eine andere mGuard-Firmwareversion besitzt als sein Elternteil, einen Wert mit einem anderen Standardwert erbt.

Das damit verbundene Verhalten von mdm wird im Kapitel „Verhalten von geänderten Standardwerten (mGuard 8.5/8.6)“ auf Seite 43 beschrieben.

Weitere Informationen zur Verwaltung von Firmware-Upgrades Ihrer Geräte mit mdm siehe Kapitel 7.6.

Dialog Template Properties		
	Template	Das übergeordnete Template des Templates.
	Redundancy support	Die Unterstützung für den Redundanzbetrieb des Geräts kann aktiviert oder deaktiviert werden.
	Accessible via	Dies ist die IP-Adresse oder der Hostname, über die der mdm-Server auf den mGuard zugreifen kann, um einen SSH-Push-Export oder einen ATV-Profilimport der Konfiguration durchzuführen oder das Web-Interface zu öffnen. Weitere Informationen zum Uploadvorgang finden Sie unter „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107. Die folgenden Werte können unter **Accessible via** ausgewählt werden (der **SSH-Port** und der **Web configuration port** können in den folgenden Feldern (siehe unten) angegeben werden. **Not online manageable** Das Gerät wird nicht über SSH-Push verwaltet. **Internal interface in auto stealth mode [1.1.1.1]** mdm verwendet für den Zugriff auf mGuard die Adresse 1.1.1.1 (Adresse der internen Schnittstelle im automatischen geschützten Modus). **Stealth management address** mdm greift im geschützten Modus auf die externe oder interne Schnittstelle des mGuard zu. **First external IP address** mdm greift im Router-Modus auf die externe Schnittstelle des mGuard zu. **First internal IP address** mdm greift im Router-Modus auf die interne Schnittstelle des mGuard zu. **Custom value** Für den Zugriff auf den mGuard in NAT-Szenarien ist möglicherweise ein benutzerspezifischer Wert (IP-Adresse oder Hostname) erforderlich.

Dialog Template Properties		
	SSH port	Dies ist die SSH-Portnummer, über die der mdm-Server auf den mGuard zugreifen kann, um einen SSH-Push-Export oder einen ATV-Profilimport der Konfiguration durchzuführen. In einigen Fällen kann es notwendig sein, den Standard-SSH-Port zu ändern, um eine Verbindung zum Gerät herzustellen (z. B. wenn das Gerät nicht mit dem Internet verbunden ist, sondern einen Port zugewiesen bekommt, der von der Firewall übermittelt wird). Wenn **Port for incoming SSH connections** ausgewählt ist, wird der unter *Management >> System Settings >> Shell Access >> Shell Access Options >> Port for incoming SSH connections* konfigurierte Port verwendet und in der Übersichtstabelle angezeigt. Weitere Informationen zum Uploadvorgang finden Sie unter „Konfigurationen in mGuard-Geräte hochladen“ auf Seite 107.
	Web configuration port	Dies ist die HTTPS-Portnummer, über die die grafische Weboberfläche des mGuard aufgerufen wird. In einigen Fällen kann es notwendig sein, den Standard-HTTPS-Port zu ändern, um eine Verbindung zur Weboberfläche herzustellen (z. B. wenn das Gerät einen Port zugewiesen bekommt, der von der Firewall übermittelt wird). Wenn **Remote HTTPS TCP port** ausgewählt ist, wird der Port verwendet, der unter *Management >> Web Settings >> Access >> HTTPS Web Access >> Remote HTTPS TCP port* ausgewählt ist.
	Default Permission	Die Berechtigung, die von mdm für Variablen verwendet wird, die beim Beerben dieses Templates durch ein Gerät oder Template auf Inherited gesetzt sind. Folgende Berechtigungen können festgelegt werden: **May override** Variablen, die auf Inherited gesetzt sind, verfügen über die Berechtigung May override, d. h. sie können im erbenden Gerät oder Template gesetzt werden.

Dialog Template Properties		
		May append Tabellenvariablen, die auf Inherited gesetzt sind, verfügen über die Berechtigung May append, d. h. im erbenden Gerät oder Template können Zeilen hinzugefügt werden, aber Änderungen an vorhandenen Zeilen sind nicht möglich. Sonstige Variablen, die auf Inherited gesetzt sind, verfügen über die Berechtigung May override, d. h. sie können im erbenden Gerät oder Template gesetzt werden. **No override** Variablen, die auf Inherited gesetzt sind, verfügen über die Berechtigung No override, d. h. sie können nicht im erbenden Gerät oder Template gesetzt werden.
	Comment	Zusätzliche optionale Anmerkungen, die auch in der Template-Tabelle des Hauptfensters angezeigt werden.
	Additional ATV include	Dies ist ein Textfeld für zusätzliche Einstellungen, die in die Konfigurationsdatei des mGuard einzufügen sind. Die Eingabe muss sich an die Konventionen der mGuard Konfigurationsdatei halten. Durch Auswahl einer Datei mit dem Symbol *File Chooser* können Sie auch den Inhalt einer Textdatei in das Feld importieren. Die enthaltene Konfiguration wird den generierten mdm Einstellungen hinzugefügt und daher überschreiben Einstellungen für dieselbe Variable im Feld Include die Einstellungen, die von mdm generiert wurden.

6.4.4 Template-Konfiguration

Wie eingangs beschrieben, ähnelt der Navigationsbaum auf der linken Seite des *Template properties dialog* (Template-Eigenschaften) der Menüstruktur die dem Webinterface des mGuard ähnelt.

In Bild 6-14 ist ein Konfigurationsbeispiel für die interne Schnittstelle dargestellt.

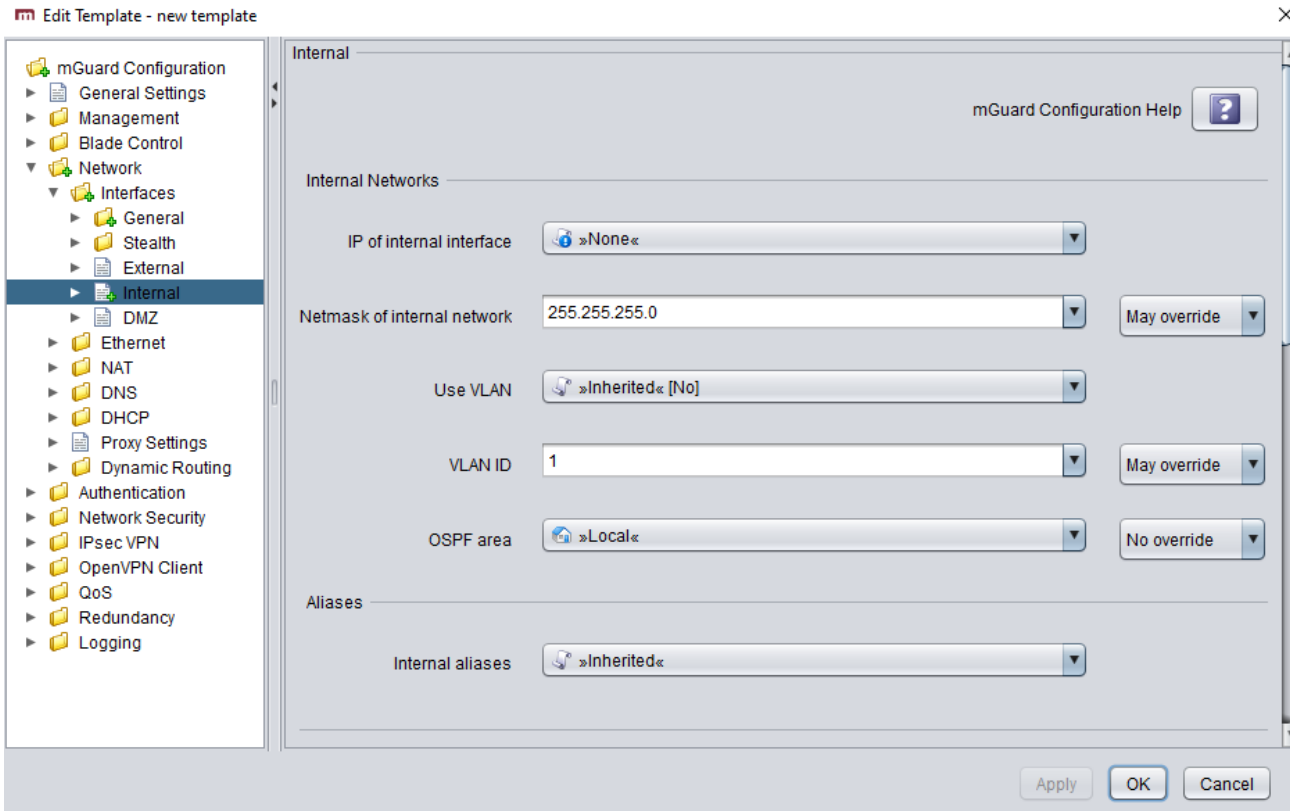


Bild 6-14 Template-Konfiguration

Im Vergleich zum *Device properties dialog* (Geräte-Eigenschaften) sind in der Template-Konfiguration zusätzliche Einstellungen enthalten, auf die in den folgenden Abschnitten eingegangen wird.

Ausführliche Informationen zum Konzept von Template und Erbe finden Sie in „Mit Templates arbeiten“ auf Seite 80.

Wertetyp None

Im Template kann der Wert **None** ausgewählt werden, wie in der Variablen **IP of internal interface** in Bild 6-14 dargestellt. Das bedeutet, dass der Ersteller des Templates keinen Wert im Template definieren möchte, aber dafür gesorgt hat, dass der Wert in einem erbenden Template oder Gerät überschrieben wird. Beim Versuch, ein Gerät hochzuladen, in dem ein None-Wert gar nicht oder durch einen lokalen Wert überschrieben wurde, erfolgt eine Fehleranzeige.

Einrichtung von Berechtigungen

In Bild 6-14 verfügt die Variable **Netmask of internal network** über die zusätzliche Möglichkeit zur Einrichtung von Berechtigungen. Diese Berechtigung kontrolliert, ob und wie ein erbendes Gerät oder Template die Einstellungen überschreiben kann. Die Berechtigungseinstellungen können pro Variable zugewiesen werden.

Bei Auswahl des Werts **Inherited** oder **None** wird die Combobox für Berechtigungen nicht angezeigt.

Folgende Berechtigungen können ausgewählt werden:

Template Configuration		
Permissions	**May override**	Der Wert kann durch ein erbendes Gerät oder Template geändert (überschrieben) werden.
	No override	Der Wert kann durch ein erbendes Gerät oder Template nicht geändert werden.
	May append	Der Einstellwert steht nur für Tabellen zur Verfügung (z. B. Firewall-Regeln). Ist die Tabellenvariable auf **May append** gesetzt, können in einem erbenden Gerät oder Template weitere Tabellenzeilen angefügt werden, die geerbten Zeilen können jedoch nicht geändert oder gelöscht werden. Wird der Wert **Local** und die Berechtigung **May append** ausgewählt, kann der Netadmin-Benutzer einem erbenden Gerät oder Template sowie dem mGuard neue Einträge hinzufügen.

6.4.5 Mit Templates arbeiten

Änderungen an einem Template wirken sich potenziell auf sehr viele Geräte oder Templates aus. Daher sollten Sie bei der Arbeit mit Templates stets die folgenden Regeln berücksichtigen:

- Prüfen Sie vor Änderungen an einer Variable oder einem Template, ob deren Auswirkungen auf die erbenden Templates bzw. Geräte wirklich erwünscht sind.
- Vor allem Änderungen an den mit einer Variable verbundenen Berechtigungen können an erbenden Geräten bzw. Templates irreversible Schäden verursachen. Wird beispielsweise eine Berechtigung von May override zu No override geändert wird der Wert der Variablen in allen erbenden Templates und Geräten verworfen.
- Templates, die noch Geräten oder anderen Templates zugewiesen sind, können nicht gelöscht werden.

In diesem Kapitel wird der Mechanismus der Templates ausführlich beschrieben.

Vererbung

Mit Templates lassen sich sehr viele Geräte effizient konfigurieren. Templates enthalten die gemeinsamen Aspekte einer Gruppe von Geräten bzw. untergeordneten Templates. Durch die Zuweisung eines Templates zu einem untergeordneten Element (Gerät oder anderes Template) „erbt“ dieses die Einstellungen des übergeordneten Templates und kann optional einige dieser Einstellungen überschreiben, sofern die Berechtigungen im übergeordneten Template dies zulassen. Jegliche Änderungen am übergeordneten Template wirken sich potenziell auf alle erbenden Templates und Geräte aus, je nach Einstellungen von Werten und Berechtigungen im übergeordneten Template.

Die Berechtigungseinstellung in einem Template begrenzt die Auswahl an erbenden Templates und Geräten.

Ob ein untergeordnetes Element die Einstellungen eines Vorgänger-Templates erbt, wird im *Properties Dialog* durch ein Symbol vor dem Namen der Variable angezeigt. Wenn kein Symbol angezeigt wird, ist kein Template zugewiesen bzw. die Variable ist in allen Vorgängertemplates auf den Wert **Inherited** gesetzt, d. h. es bestehen keine Einschränkungen für diese Variable.

Entsprechend den in „Template-Konfiguration“ auf Seite 79 aufgeführten Berechtigungen werden for dem Namen der Variablen folgende Symbole angezeigt:

May override.

No override.

May append (nur für Tabellen).

Kein Wert definiert (Wert = **None**), d. h. der Wert wurde im *Device properties dialog* (Geräte-Eigenschaften) oder in einem der dazwischenliegenden Templates gesetzt.

Der Mechanismus der Vererbung wird in der folgenden Abbildung dargestellt. Bild 6-15 zeigt die Einstellungen für *DHCP server options* im **übergeordneten (parent) Template**.

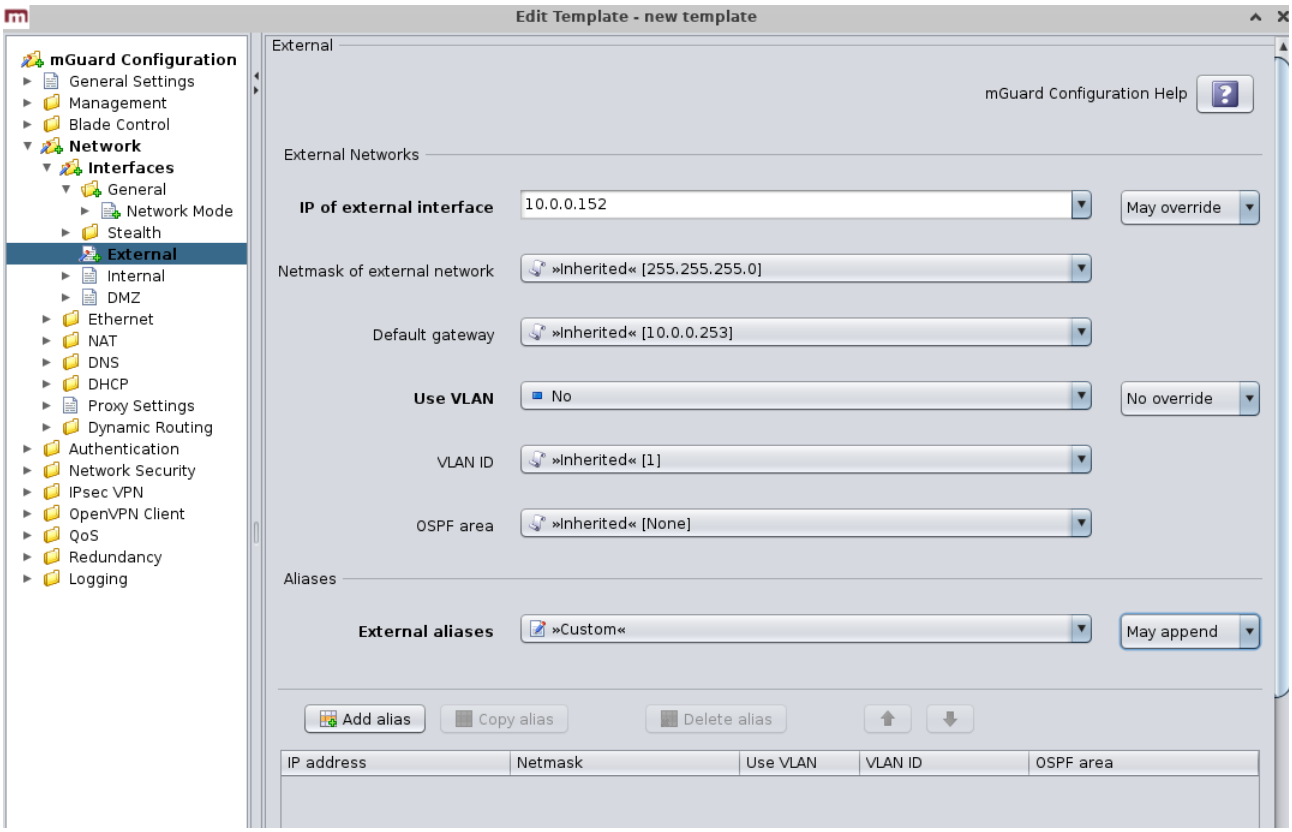


Bild 6-15 Einstellungen im übergeordneten Template

Bild 6-16 zeigt die Einstellungen in der **Gerätekonfiguration (child – untergeordnet)**. Diese beruhen auf vom übergeordneten Template geerbten Werten und Berechtigungen und von Änderungen am Gerät.

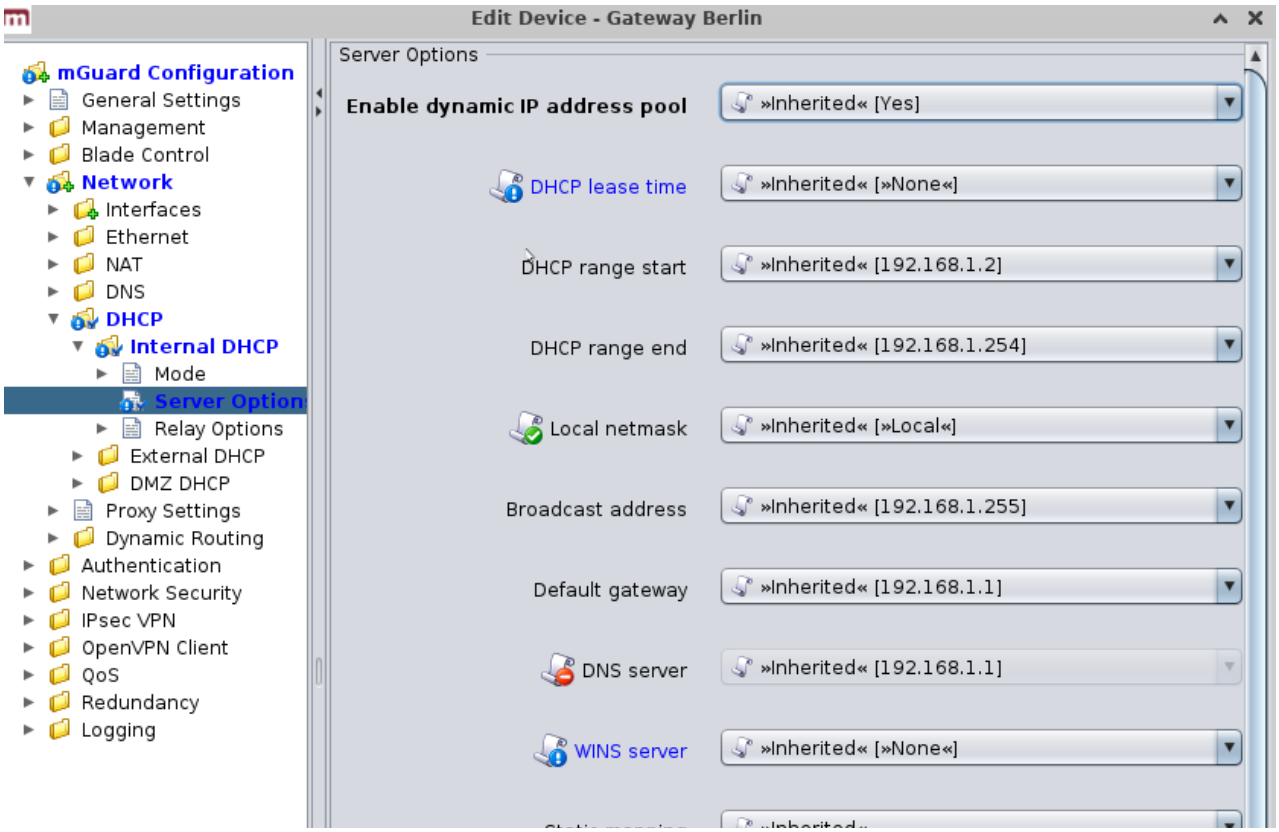


Bild 6-16 Einstellungen im erbenden Gerät

Einstellungen im erbenden Gerät	
Enable dynamic IP address pool	Diese Variable ist im Template auf **Yes** und die Berechtigung auf **No override** gesetzt. Daher kann der Wert der Variablen nicht in der Gerätekonfiguration geändert werden. Dies wird durch deaktivierte Steuerelemente und das Symbol vor dem Namen der Variablen im *Device properties dialog* (Geräte-Eigenschaften) angezeigt.
DHCP range start, DHCP range end	Diese Variablen sind auf **Local** und die Berechtigung auf **No override** gesetzt, d. h. die Einstellung **Local** kann in der Gerätekonfiguration nicht geändert werden. Diese Werte müssen durch den *netadmin* des mGuard gesetzt werden und können nicht von mdm verwaltet werden.

Einstellungen im erbenden Gerät		
	Local netmask, Broadcast address	Das fehlende Symbol vor dem Namen der Variablen im *Device properties dialog* (Geräte-Eigenschaften) weist darauf hin, dass für diese Variablen sind im Template keine Einschränkungen definiert sind. Im vorliegenden Beispiel entschied sich der Konfigurator des Geräts für die Verwendung eines benutzerdefinierten Werts für **Broadcast address** und den (geerbten) Standardwert für **Local netmask**.
	Default gateway	Der Wert dieser Variablen wird im Template gesetzt und die Berechtigung ist auf **May override** gesetzt. Daher kann der Wert der Variablen in der Gerätekonfiguration geändert werden. Dies wird durch aktivierte Steuerelemente und das Symbol  vor dem Namen der Variablen angezeigt. Im Beispiel wird der Wert aus dem Template durch einen benutzerdefinierten Wert überschrieben.
	DNS server	Der Wert dieser Variablen wird im Template gesetzt und die Berechtigung ist auf **May override** gesetzt. Daher kann der Wert der Variablen in der Gerätekonfiguration geändert werden. Dies wird durch aktivierte Steuerelemente und das Symbol  vor dem Namen der Variablen angezeigt. In diesem Beispiel wird der Wert aus dem Template in der Gerätekonfiguration durch einen benutzerdefinierten Wert überschrieben.
	WINS-Server	Der Wert dieser Variablen ist im Template auf **None** gesetzt. Dass bedeutet, dass in der Gerätekonfiguration ein Wert für diese Variable *zugewiesen werden muss*. Dies wird durch das Symbol  vor dem Namen der Variablen und eine blaue Markierung angezeigt. Wird ein Gerät hochgeladen, für das keine None-Werte zugewiesen sind, erscheint eine Fehlermeldung.
	Static mapping	Im Template ist die Tabelle **Static mapping** auf **Custom** und deren Berechtigung auf **May append** gesetzt. Wie in Bild 6-16 gezeigt, können nach der Änderung der Tabellenvariable auf **Custom** in der Gerätekonfiguration Zeilen angefügt werden. Vom Template geerbte Zeilen können nicht geändert werden.

Sonstiges

Komplexe Tabellenvariablen und Berechtigungen

Die Berechtigungseinstellungen für komplexe Tabellenvariablen (siehe „Allgemeine Bemerkungen“ auf Seite 29) im übergeordneten Template gelten für die Tabelle selbst, jedoch nicht für die Inhalte der Zeilen. Wenn die Tabelle auf **No Override** gesetzt ist, können keine Zeilen in der untergeordneten Konfiguration hinzugefügt oder gelöscht werden. Möglicherweise können jedoch die Werte der Variablen in den geerbten Zeilen der untergeordneten Tabelle geändert werden. Jede Variable einer Zeile (Knoten) verfügt über eine eigene Berechtigungseinstellung im übergeordneten Template, in der festgelegt ist, ob die Variable im untergeordneten Element überschrieben werden kann. Die Berechtigungseinstellung der Tabelle und die Berechtigungseinstellung einer einzelnen Variable innerhalb der Tabelle sind voneinander komplett unabhängig.

Versionseinstellungen der Firmware und Vererbung

In den **General Settings** des untergeordneten Elements und des übergeordneten Templates bestehen hinsichtlich der **Firmwareversion** gewisse Einschränkungen:

– Ein untergeordnetes Element kann nicht von einem übergeordneten Template erben, das eine neuere Firmwareversion als das untergeordnete Element selbst besitzt.
– Die Firmwareversion eines übergeordneten Templates kann nur auf eine neuere Version geändert werden, wenn alle untergeordneten Elemente, die von diesem übergeordneten Template erben, bereits auf die neuere Firmwareversion gesetzt sind.
– Die Vererbung der **geänderten Defaultwerte** hängt von der installierten mdm-Version und der mGuard-Firmwareversion des Device/Template ab (siehe unten).

Vererbung von geänderten Standardwerten

In mGuard**-Firmwareversion 8.5 und 8.6** wurden Standardwerte geändert.

Allgemeines Verhalten in mdm < 1.8.0:

Wenn sich die Standardwerte (Wertetyp = "*Inherited*" und nicht "*Local*" oder "*Custom*") des „Kindes“ von den Standardwerten der „Mutter“ (Wertetyp = "*Inherited*" entlang der vollständigen Vererbungskette) unterscheiden, verhält sich die Vererbung wie folgt:

1. Das „Kind“ behält die Standardwerte, die der Firmwareversion des „Kindes“ entsprechen. Der Wertetyp bleibt "***Inherited***".

Allgemeines Verhalten in mdm 1.8.0 oder höher:

Wenn sich die Standardwerte (Wertetyp = "*Inherited*" und nicht "*Local*" oder "*Custom*") des „Kindes“ von den Standardwerten der „Mutter“ (Wertetyp = "*Inherited*" entlang der vollständigen Vererbungskette) unterscheiden, verhält sich die Vererbung wie folgt:

1. Standardwerte, die in mGuard **Firmwareversionen < 8.5** geändert wurden:
   – Das „Kind“ behält die Standardwerte, die der Firmwareversion des „Kindes“ entsprechen. Der Wertetyp bleibt "***Inherited***".
2. Standardwerte, die in mGuard **Firmwareversion 8.5 oder höher** geändert wurden:
   – Das „Kind“ erbt die Standardwerte der „Mutter“. Der Wertetyp bleibt "***Inherited***".

6.5 Pools konfigurieren

6.5.1 Poolwerte-Übersicht (Pool value overview table)

Klicken Sie auf die Registerkarte **Pool**, um die Poolwerte-Übersicht (*Pool value overview table*) aufzurufen. Ein Pool definiert eine Reihe von Netzwerkadressen, die automatisch Variablen zugewiesen werden können. Weiterführende Informationen zu Pools und deren Verwendung finden Sie in „Pool-Eigenschaften (Pool properties dialog)“ auf Seite 88.

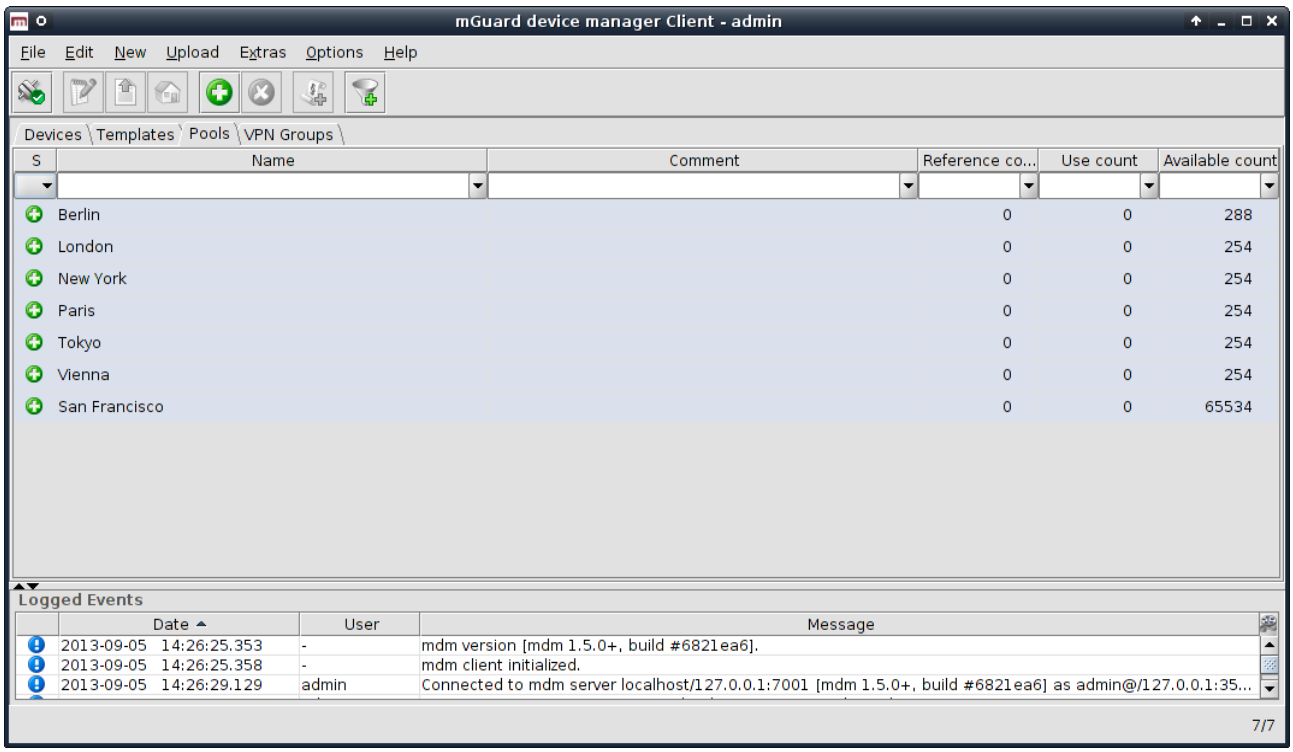


Bild 6-17 mdm Hauptfenster mit Pooltabelle

Spalten der Poolwerte-Übersicht (*Pool value overview table*)

Die Poolwerte-Übersicht (*Pool value overview table*) enthält folgende Spalten.

Setzen Sie zum Ändern der Spaltenbreite den Cursor in die Kopfzeile der Tabelle an die Grenze zwischen zwei Spalten und ziehen Sie bei gedrückter linker Maustaste die Grenze in die gewünschte Richtung. Setzen Sie zum Verschieben einer Spalte den Cursor in die Kopfzeile der Tabelle und ziehen Sie bei gedrückter linker Maustaste die Spalte an den gewünschten Platz.

Status (*S*)	Das Status-Symbol zeigt an, ob die Pooldefinition gültig ist.
Name	Der dem Pool zugewiesene Name.
Comment	Optionale Anmerkungen.

Reference count	In dieser Spalte wird angezeigt, wieviele Variablen sich auf diesen Pool beziehen (siehe „Pool-Eigenschaften (Pool properties dialog)“ auf Seite 88).
Use count	In dieser Spalte wird angezeigt, wieviele Werte aus diesem Pool verwendet wurden (siehe „Pool-Eigenschaften (Pool properties dialog)“ auf Seite 88).
Available count	Diese Zahl gibt an, wieviele Werte noch im Pool zur Verfügung stehen (siehe „Pool-Eigenschaften (Pool properties dialog)“ auf Seite 88).

Tabelle filtern und sortieren

Mit der Kopfzeile der Tabelle können die Einträge sortiert werden. Durch Anklicken der Kopfzeile einer Spalte wird die (primäre) Sortierung anhand dieser Spalte aktiviert. Dies wird durch einen Pfeil in der Kopfzeile angezeigt. Durch einen zweiten Klick auf dieselbe Kopfzeile erfolgt die Sortierung in umgekehrter Reihenfolge. Durch Anklicken einer weiteren Spalte wird anhand dieser neuen Spalte sortiert, wobei die vorher aktive Spalte als zweites Kriterium für die Sortierung herangezogen wird.

In der ersten Tabellenzeile wird die Eingabe regulärer Ausdrücke akzeptiert (siehe Kapitel 11, *Regular expressions*), die zum effizienten Filtern der Tabelleneinträge verwendet werden können. Eine Spalte, die keinen Text enthält (d. h. Spalte **S**) kann nicht auf der Grundlage regulärer Ausdrücke gefiltert werden.

Das Filterkriterium für die drei **count**-Spalten wird nicht als regulärer Ausdruck interpretiert, sondern als Liste von Zahlen oder Zahlenbereichen, die durch Komma getrennt sind (z. B. 0, 2 – 3).

Der Filterverlauf wird für den aktuellen Benutzer gespeichert und kann über die Dropdown-Funktion der Filterfelder aufgerufen werden.

Pools anlegen

Neue Pools können auf mehrere Arten angelegt werden:

1. Öffnen Sie das Kontextmenü durch einen Rechtsklick auf die Pool-Tabelle. Klicken Sie im Kontextmenü auf **Add**, um den *Pool properties dialog* (Pool-Eigenschaften) für einen neuen Pool zu öffnen.
2. Klicken Sie auf die Registerkarte **Pool** und hier auf das Symbol in der Menüleiste und öffnen Sie den *Pool properties dialog* für einen neuen Pool.
3. Klicken Sie im Hauptmenü auf **New » Pool** um den *Pool properties dialog* für einen neuen Pool zu öffnen.

Pools bearbeiten

Ein Pool kann auf mehrere Arten bearbeitet werden:

1. Führen Sie mit der linken Maustaste einen Doppelklick auf den Pool in der Tabelle aus, um den *Pool properties dialog* zu öffnen.
2. Wählen Sie mit der linken Maustaste den Pool aus und öffnen Sie durch einen Rechtsklick das Kontextmenü. Öffnen Sie den *Pool properties dialog* durch Klicken auf **Edit**.
3. Wählen Sie in der Pool-Tabelle den zu ändernden Pool. Klicken Sie im Hauptmenü auf **Edit » Edit Item** um den *Pool properties dialog* zu öffnen.

Der Menüpunkt **Edit** im Kontextmenü und die Schaltfläche **Edit** in der Symbolleiste sind nur aktiviert, wenn in der Pool-Tabelle genau ein Pool ausgewählt ist.

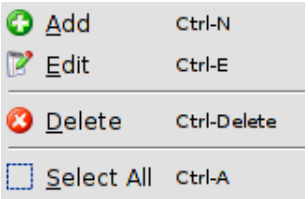
Pools löschen

Pools können auf mehrere Arten gelöscht werden:

1. Wählen Sie einen oder mehrere Pools aus und öffnen Sie das Kontextmenü durch einen Rechtsklick auf das Template. Klicken Sie im Kontextmenü auf **Delete** um einen Pool zu löschen.
2. Markieren Sie in der Pool-Tabelle die zu löschenden Pools und klicken Sie in der Menüleiste auf das Symbol  .

Pools, auf die sich noch Variablen beziehen, können nicht gelöscht werden.

6.5.2 Pool-Kontextmenü (Pool context menu)



Im Kontextmenü der Poolwerte-Übersicht (*Pool value overview table*) stehen folgende Optionen zur Verfügung.

Pool-Kontextmenü		
	Add	Neuen Pool anlegen und den *Pool properties dialog* (Pool-Eigenschaften) des neuen Pools öffnen.
	Edit	Ausgewählten Pool bearbeiten (nur aktiv, wenn genau ein Pool in der Übersichtstabelle markiert ist).
	Delete	Ausgewählte Pools löschen.
	Select All	Alle nicht durch den Tabellenfilter ausgeschlossenen Pools auswählen.

6.5.3 Pool-Eigenschaften (Pool properties dialog)

Der *Pool properties dialog* (Pool-Eigenschaften) ermöglicht die Definition von Wertepools, mit denen bestimmter Werte automatisch konfiguriert werden können (z. B. virtuelle Adressen für VPNs). Aktuell ermöglicht mdm die Definition von Adressbereichs-Pools (CIDR-Benachrichtigung), Beispiel siehe unten.

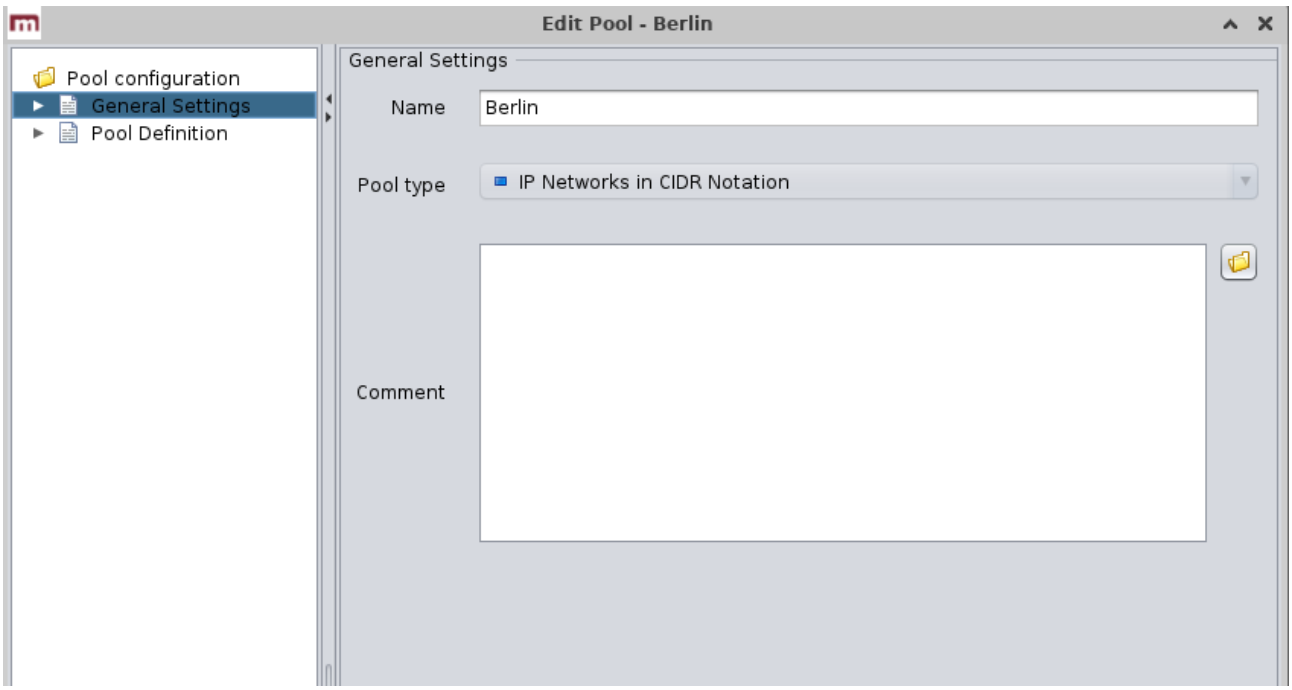


Bild 6-18 Der mdm Dialog Pool Properties

General settings Die folgenden Parameter des Pools können in den **General settings** eingestellt werden:

Dialog Pool Properties		
General settings	**Name**	Bezeichnung für den Pool. Diese Bezeichnung wird verwendet, wenn in einer Variablen Bezug auf den Pool genommen wird (siehe nachfolgenden Abschnitt *Verwendung von Pool-Werten* in Variablen).
	Pooltyp	Aktuell steht nur der Pooltyp *IP Networks in CIDR Notation* zur Verfügung.
	Comment	Anmerkungen (optional).

Pool definition

Über **Pool Definition** können der Wertebereich des Pools und der Adressbereich der dem Pool zu entnehmenden Werte definiert werden. Bild 6-19 zeigt ein Beispiel für eine Pool-Definition.

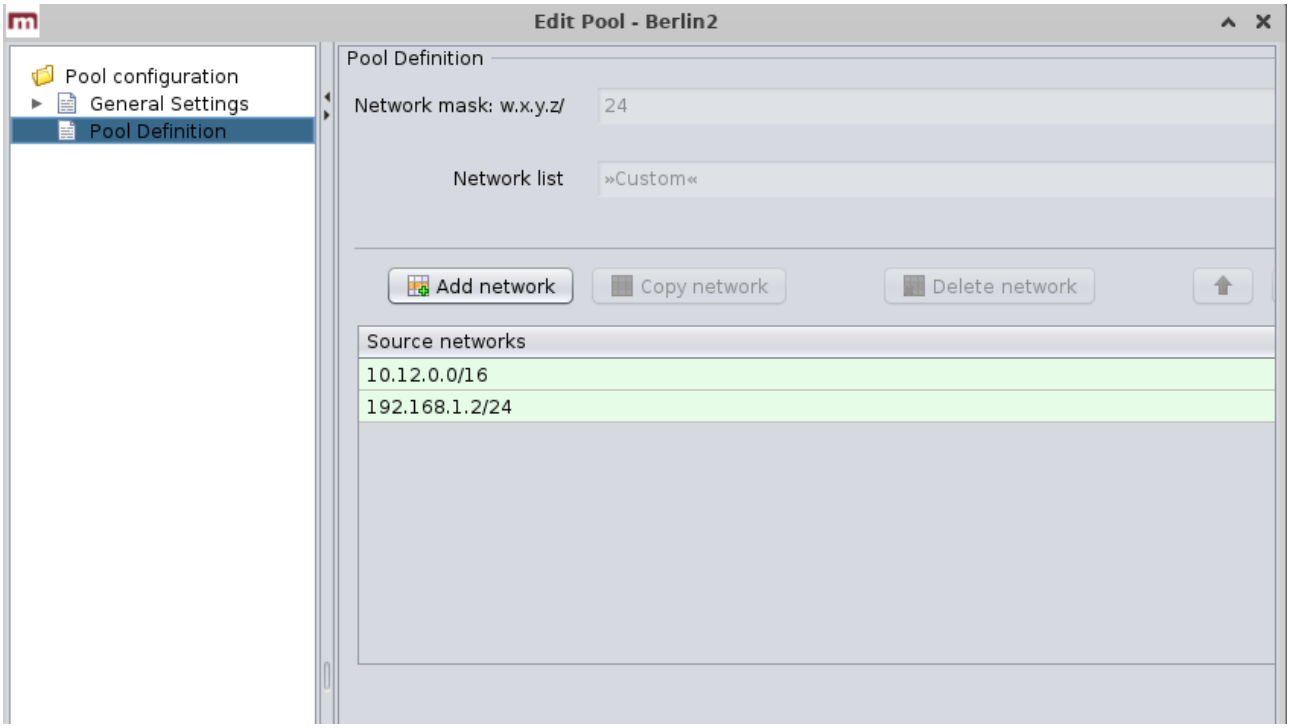


Bild 6-19 Definition eines CIDR-Pools

Der CIDR-Pool im Beispiel enthält alle in der Tabelle **Network List** definierten Adressen. Das Feld **Network Mask** definiert den Bereich der Einzelwerte, die dem Pool entnommen werden sollen, d. h. bei Verwendung des Pools in einer Variablen weist mdm dieser Variablen automatisch einen IP-Adressbereich mit einer Maske von 24 aus dem verfügbaren Source Networks zu.

Wird der Pool beispielsweise (in einer VPN-Verbindung) für die Template-Variable **Remote network** verwendet, weist mdm der Variable **Remote network** bei allen Geräten, die das jeweilige Template nutzen, automatisch einen Wert zu. In der Tabelle Pool-Übersicht im Hauptfenster wird angezeigt, wieviele Variablen dem Pool entnommen wurden (*Use count*) und wieviele Werte im Pool noch zur Verfügung stehen (*Available count*).

Sind Netzwerkmaske und Quelladressbereiche des Pools einmal definiert, können sie nicht mehr geändert oder gelöscht werden, d. h. der Netzwerkbereich 10.12.0.0/16 bis 10.12.0.0/19 im oben angeführten Beispiel kann nicht mehr verringert werden. Dem Pool können lediglich weitere Bereiche hinzugefügt werden, d. h. der Wertebereich des Pools kann erweitert werden. Daher ist bei der Vorausplanung des Pools größte Sorgfalt geboten.

Poolwerte in Variablen verwenden

Poolwerte können nur in Templates verwendet werden. Bei bestimmten Variablen kann der gewünschte Pool aus einer Dropdown-Liste ausgewählt werden, z. B. stehen in Bild 6-20 eine Anzahl Pools (*London, New York, Paris usw.*) für die Verwendung mit der Variable *IP of external interface* zur Verfügung. In der Dropdown-Liste werden nur Pools angezeigt, die zur Variable passen (z. B. CIDR-Pool und Variable vom Typ IP-Adresse).

Bei Verwendung eines Pools in einem Template werden der jeweiligen Variablen keine Werte zugewiesen; auf den Pool wird zu diesem Zeitpunkt lediglich Bezug genommen. Daher wird der *Reference count* in der Pool-Tabelle um eins erhöht. Bei Zuweisung eines Wertes zu einer Variablen (erfolgt auf Geräteebene, nicht auf Template-Ebene) wird der *Use count* um eins erhöht.

Diese Zuweisung erfolgt automatisch, wenn Sie ein geerbtes Gerätetemplate durch Bezugnahme auf einen Pool von einer Variablen an das Template bearbeiten oder wenn Sie ein Template einem Gerät zuweisen, das bereits auf einen Pool Bezug nimmt.

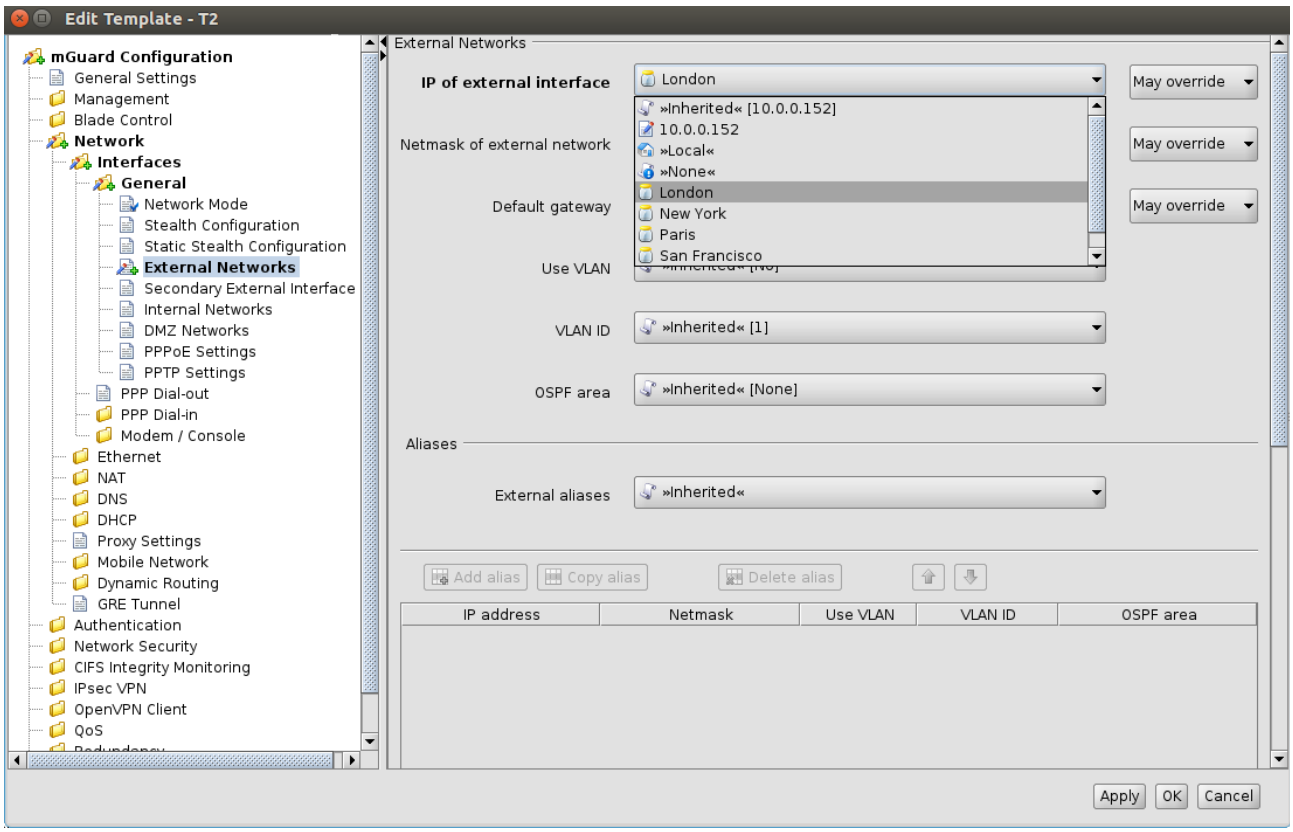


Bild 6-20 Verwendung von Pool-Werten

Bei der Arbeit mit Pools sollten Sie stets Folgendes beherzigen.

In einer Variable, die eine IP-Adresse (kein IP-Netzwerk) erfordert, kann nur auf Pools mit einer Netzwerkmaske von *32* Bezug genommen werden.

Wenn Sie sich dafür entscheiden, einen Pool-Wert im Gerät zu überschreiben, wird der zugewiesene Pool-Wert nicht an den Pool zurückgegeben (d. h. der *Use count* wird um eins verringert), sondern bleibt „im Hintergrund“ zugewiesen, falls Sie für die erneute Verwendung des geerbten Werts für notwendig erachten.

Pools müssen ausreichend groß sein, um einen Wert für jedes Gerät zur Verfügung zu stellen, das die Vorlage, in der auf diesen Pool Bezug genommen wird, beerbt. Dies gilt auch, wenn einige dieser Geräte ihren jeweiligen Pool-Wert überschreiben (siehe oben).

6.6 VPN-Gruppen konfigurieren

6.6.1 VPN-Gruppen-Übersicht (VPN group overview table)

Klicken Sie auf die Registerkarte **VPN Groups**, um die VPN-Gruppen-Übersicht (*VPN group overview table*) aufzurufen. Mit einer VPN-Gruppe können Geräte in einem vermaschten VPN-Netzwerk gruppiert werden. Weiterführende Informationen zu VPN-Gruppen und deren Verwendung finden Sie in „VPN-Gruppe-Eigenschaften (VPN group properties dialog) – Vermaschte VPN-Netzwerke“ auf Seite 99.

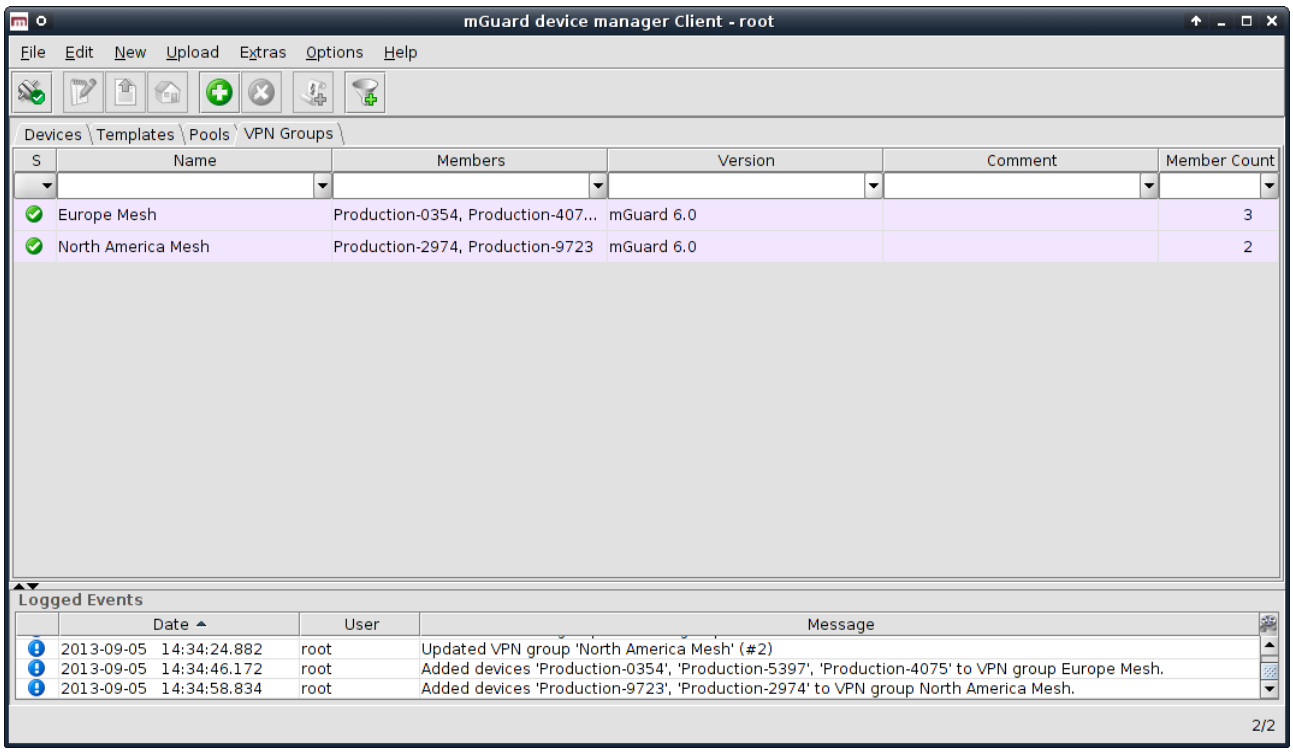


Bild 6-21 VPN-Gruppen-Übersicht (*VPN group overview table*)

Die VPN-Gruppen-Übersicht (*VPN group overview table*) enthält folgende Spalten.

Setzen Sie zum Ändern der Spaltenbreite den Cursor in die Kopfzeile der Tabelle an die Grenze zwischen zwei Spalten und ziehen Sie bei gedrückter linker Maustaste die Grenze in die gewünschte Richtung. Setzen Sie zum Verschieben einer Spalte den Cursor in die Kopfzeile der Tabelle und ziehen Sie bei gedrückter linker Maustaste die Spalte an den gewünschten Platz.

Spalten der VPN-Gruppen-Übersicht (VPN group table columns)	
Status (*S*)	Das Status-Symbol zeigt an, ob die VPN-Gruppe aktuell gesperrt ist.

Spalten der VPN-Gruppen-Übersicht (VPN group table columns)	
Name	Der der VPN-Gruppe zugewiesene Name. Der Name kann unter **General Settings** im *VPN group properties dialog* (VPN-Gruppe-Eigenschaften) eingetragen werden (siehe Kapitel 6.6.4).
Members	Liste, in der mit Komma getrennt die zur VPN-Gruppe gehörenden Geräte aufgeführt werden (d. h. die Teil des durch die VPN-Gruppe definierten vermaschten VPN-Netzwerks sind).
Version	Für die VPN-Gruppe verwendete Firmwareversion des mGuard.
Comment	Optionale Anmerkungen. Die Anmerkung kann unter **General Settings** im *VPN group properties dialog* (VPN-Gruppe-Eigenschaften) eingetragen werden (siehe Kapitel 6.6.4).
Member Count	In dieser Spalte wird die Anzahl der zur VPN-Gruppe gehörenden Geräte angezeigt.

Tabelle filtern und sortieren

Mit der Kopfzeile der Tabelle können die Einträge sortiert werden. Durch Anklicken der Kopfzeile einer Spalte wird die (primäre) Sortierung anhand dieser Spalte aktiviert. Dies wird durch einen Pfeil in der Kopfzeile angezeigt. Durch einen zweiten Klick auf dieselbe Kopfzeile erfolgt die Sortierung in umgekehrter Reihenfolge. Durch Anklicken einer weiteren Spalte wird anhand dieser neuen Spalte sortiert, wobei die vorher aktive Spalte als zweites Kriterium für die Sortierung herangezogen wird.

In der ersten Tabellenzeile wird die Eingabe regulärer Ausdrücke akzeptiert (siehe Kapitel 11, *Regular expressions*), die zum effizienten Filtern der Tabelleneinträge verwendet werden können. Eine Spalte, die keinen Text enthält (d. h. Spalte **S**) kann nicht auf der Grundlage regulärer Ausdrücke gefiltert werden.

Das Filterkriterium **Member count** wird nicht als regulärer Ausdruck interpretiert, sondern als Liste von Zahlen oder Zahlenbereichen, die durch Komma getrennt sind (z. B. 0, 2 – 3).

Der Filterverlauf wird für den aktuellen Benutzer gespeichert und kann über die Dropdown-Funktion der Filterfelder aufgerufen werden.

VPN-Gruppen anlegen

Neue VPN-Gruppen können auf mehrere Arten angelegt werden:

1. Öffnen Sie das Kontextmenü durch einen Rechtsklick auf die VPN-Gruppentabelle. Klicken Sie im Kontextmenü auf **Add**, um den *VPN group properties dialog* (VPN-Gruppe-Eigenschaften) für eine neue VPN-Gruppe zu öffnen.
2. Klicken Sie auf die Registerkarte **VPN-Gruppe** und hier auf das Symbol  in der Menüleiste und öffnen Sie den *VPN group properties dialog* für eine neue VPN-Gruppe.
3. Klicken Sie im Hauptmenü auf **New » VPN Group** um den *VPN group properties dialog* für eine neue VPN-Gruppe zu öffnen.

VPN-Gruppen bearbeiten

Eine VPN-Gruppe kann auf mehrere Arten bearbeitet werden:

1. Führen Sie mit der linken Maustaste einen Doppelklick auf die VPN-Gruppe in der Tabelle aus, um den *VPN group properties dialog* zu öffnen.
2. Wählen Sie mit der linken Maustaste die VPN-Gruppe aus und öffnen Sie durch einen Rechtsklick das Kontextmenü. Öffnen Sie den *VPN group properties dialog* durch Klicken auf **Edit**.

3. Wählen Sie in der Gerätetabelle das zu ändernde Gerät. Klicken Sie im Hauptmenü auf **Edit » Edit Item** um den *VPN group properties dialog* zu öffnen.

Der Menüpunkt **Edit** im Kontextmenü und die Schaltfläche **Edit** in der Symbolleiste sind nur aktiviert, wenn in der VPN-Gruppen-Übersicht (*VPN group overview table*) genau eine VPN-Gruppe ausgewählt ist.

VPN-Gruppen löschen

VPN-Gruppen können auf mehrere Arten gelöscht werden:

1. Wählen Sie in der VPN-Gruppentabelle eine oder mehrere VPN-Gruppen aus und öffnen Sie das Kontextmenü durch einen Klick mit der rechten Maustaste. Klicken Sie im Kontextmenü auf **Delete** um eine VPN-Gruppe zu löschen.
2. Markieren Sie in der Tabelle die zu löschenden VPN-Gruppen und klicken Sie in der Menüleiste auf das Symbol .

VPN-Gruppen, in denen noch Geräte Mitglied sind, können nicht gelöscht werden.

6.6.2 VPN-Gruppe-Kontextmenü (VPN group context menu)

Im VPN-Gruppe-Kontextmenü stehen folgende Optionen zur Verfügung.

VPN-Gruppe-Kontextmenü		
	Add	Neue VPN-Gruppe anlegen und den *VPN group properties dialog* (VPN-Gruppe-Eigenschaften) der neuen VPN-Gruppe öffnen.
	Edit	Ausgewählte VPN-Gruppe bearbeiten (nur aktiv, wenn genau eine VPN-Gruppe in der Übersichtstabelle markiert ist).
	Duplicate	Öffnen Sie zum Anlegen einer VPN-Gruppenkopie durch einen Klick mit der rechten Maustaste auf die VPN-Gruppe in der Tabelle das Kontextmenü dieser VPN-Gruppe. Klicken Sie im Kontextmenü auf **Duplicate**. mdm erstellt eine Kopie der VPN-Gruppe und fügt zum Namen der neuen VPN-Gruppe den String *_copy<n>* (<n> ist eine Zahl) hinzu. Hinweis: Der Menüeintrag **Duplicate** ist nur aktiviert, wenn in der VPN-Gruppentabelle genau eine VPN-Gruppe markiert ist.
	Delete	Ausgewählte VPN-Gruppen löschen.

VPN-Gruppe-Kontextmenü		
	Set Firmware Version	Da unterschiedliche Versionen der mGuard-Software über unterschiedliche Variablensätze verfügen, muss hier die zur auf dem mGuard installierten Firmware passende Firmware ausgewählt werden. Ein Gerät kann nur Mitglied einer VPN-Gruppe sein, wenn dessen Firmwareversion **gleichwertig oder aktueller** als die Firmwareversion der VPN-Gruppe ist. **CAUTION: Unwiderrufliche Änderungen** Ein Downgrade zurück auf eine ältere Version ist nicht möglich. Daher ist bei einer Änderung der Firmwareversion größte Sorgfalt geboten. Weitere Informationen dazu erhalten Sie unter „Versionseinstellungen der Firmware und Vererbung“ auf Seite 84. **ACHTUNG: Neue Standardwerte in mGuard-Firmware 8.5 und 8.6** Wenn eine vorhandene VPN-Guppe von mGuard-**Firmwareversion < 8.5** auf Version **8.5 oder 8.6** aktualisiert wird und die Tabelle *Algorithms* in "ISAKMP SA (Key Exchange)" sowie in "IPsec SA (Data Exchange)" die Standardkonfiguration haben, dann wird jeweils das bisherige Standard-Verschlüsselungsverfahren (3DES) beibehalten. In diesem Fall wird der Wertetyp der Tabelle von "***Inherited***" auf "***Custom***" geändert. Weitere Informationen zur Verwaltung von Firmware-Upgrades Ihrer Geräte mit mdm siehe Kapitel 7.6.
	Assign/Remove Member Devices	Geräte, die Mitglied einer oder mehrerer VPN-Gruppen sind, bearbeiten. Weiterführende Informationen finden Sie unter „Mitgliedschaft von Geräten in VPN-Gruppen bearbeiten“ auf Seite 97.
	Select All	Alle nicht durch den Tabellenfilter ausgeschlossenen VPN-Gruppen auswählen.

6.6.3 Mitgliedschaft von Geräten in VPN-Gruppen bearbeiten

Bei Anklicken von Assign/Remove Member Devices im Kontextmenü der VPN-Gruppe wird ein Dialog aufgerufen, der die Bearbeitung der Mitgliedschaft des Geräts in den ausgewählten VPN-Gruppen ermöglicht:

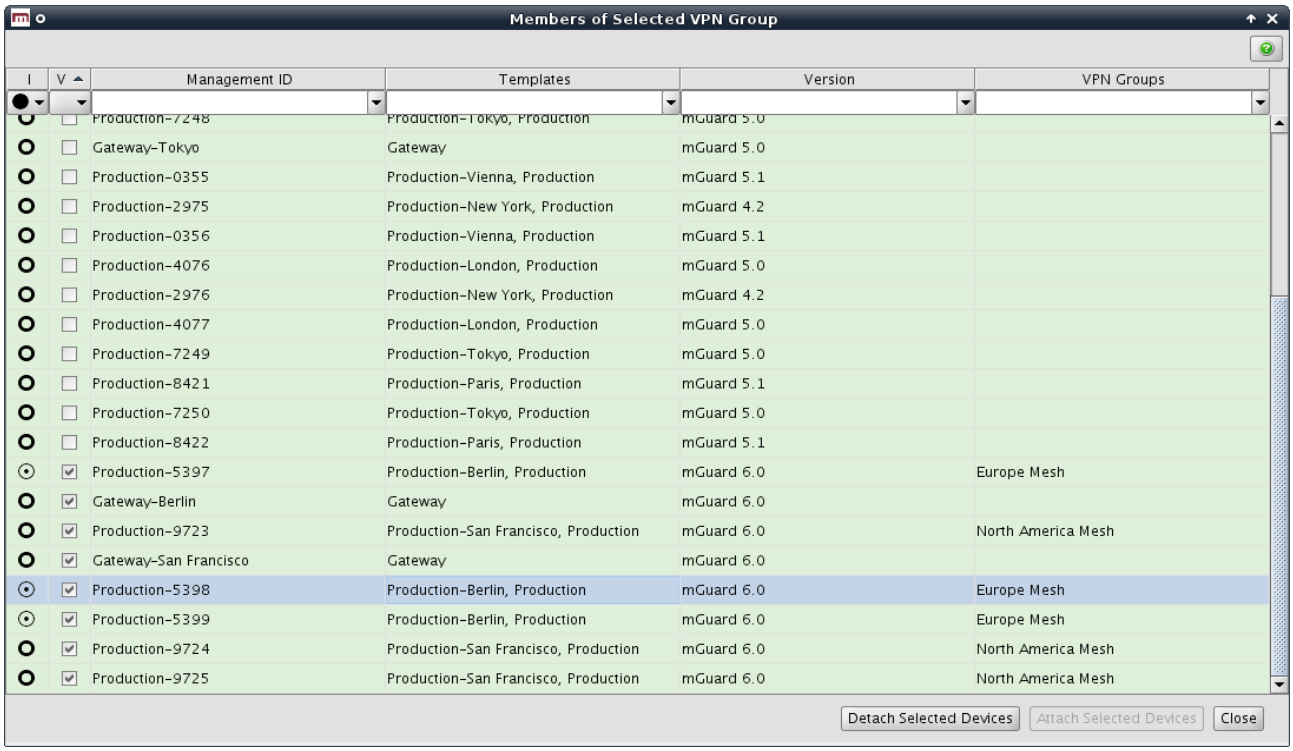


Bild 6-22 Dialog zur Bearbeitung der Mitgliedschaft von Geräten in VPN-Gruppen

Spalten der Tabelle VPN-Gruppenmitgliedschaft

Die Tabelle VPN-Gruppenmitgliedschaft enthält folgende Spalten.

Setzen Sie zum Ändern der Spaltenbreite den Cursor in die Kopfzeile der Tabelle an die Grenze zwischen zwei Spalten und ziehen Sie bei gedrückter linker Maustaste die Grenze in die gewünschte Richtung. Setzen Sie zum Verschieben einer Spalte den Cursor in die Kopfzeile der Tabelle und ziehen Sie bei gedrückter linker Maustaste die Spalte an den gewünschten Platz.

Spalten der Tabelle VPN-Gruppenmitgliedschaft	
Status *I*	Das Status-Symbol ***I*** zeigt an, ob ein Gerät Mitglied in einigen, allen oder keiner der ausgewählten VPN-Gruppen ist. Durch einen Klick auf das Symbol können Sie einen Dialog öffnen, in dem die zur Verfügung stehenden Symbole und deren Bedeutung beschrieben werden.
Status *V*	Das Status-Symbol ***V*** zeigt an, ob die Firmwareversion des Geräts zur Firmwareversion der ausgewählten VPN-Gruppen passt, d. h. ob sie gleichwertig oder aktueller ist.

Spalten der Tabelle VPN-Gruppenmitgliedschaft		
	Management ID	Management-ID des Geräts.
	Templates	Durch Kommas getrennte Liste der übergeordneten Templates des Geräts. Der erste Punkt auf der Liste ist das unmittelbar übergeordnete Template.
	Version	Firmwareversion der VPN-Gruppe.
	VPN Groups	Durch Kommas getrennte Liste der VPN-Gruppen, in denen das Geräts aktuell Mitglied ist.

Tabelle filtern und sortieren

Mit der Kopfzeile der Tabelle können die Einträge sortiert werden. Durch Anklicken der Kopfzeile einer Spalte wird die (primäre) Sortierung anhand dieser Spalte aktiviert. Dies wird durch einen Pfeil in der Kopfzeile angezeigt. Durch einen zweiten Klick auf dieselbe Kopfzeile erfolgt die Sortierung in umgekehrter Reihenfolge. Durch Anklicken einer weiteren Spalte wird anhand dieser neuen Spalte sortiert, wobei die vorher aktive Spalte als zweites Kriterium für die Sortierung herangezogen wird.

In der ersten Tabellenzeile wird die Eingabe regulärer Ausdrücke akzeptiert (siehe Kapitel 11, *Regular expressions*), die zum effizienten Filtern der Tabelleneinträge verwendet werden können. Bei Spalten, die keinen Text enthalten (Spalten **I und V**) kann nicht auf der Grundlage regulärer Ausdrücke gefiltert werden.

Geräte auswählen

Wählen Sie die Geräte aus, bei denen Sie die Mitgliedschaft in der VPN-Gruppe bearbeiten möchten:

- Markieren Sie ein Gerät durch Anklicken.
- Klicken Sie zur Auswahl eines Gerätebereichs ein Gerät an, halten Sie die Umschalttaste gedrückt und klicken Sie ein zweites Gerät an. Dadurch markieren Sie alle Geräte, die sich zwischen diesen beiden Geräten befinden.
- Um den Auswahlstatus eines Geräts umzukehren, klicken Sie bei gedrückter Strg-Taste das Gerät an.

VPN-Gruppenmitgliedschaft zuweisen oder aufheben

Klicken Sie zur Zuweisung der markierten Geräte zur ausgewählten VPN-Gruppe (d. h. die VPN-Gruppen wurden bei Öffnen des Dialogs in der VPN-Gruppentabelle ausgewählt) auf die Schaltfläche **Attach Selected Devices**. Klicken Sie analog zum Entfernen der markierten Geräte aus der ausgewählten VPN-Gruppe auf die Schaltfläche **Detach Selected Devices**.

Ein Gerät kann nur Mitglied einer VPN-Gruppe sein, wenn dessen Firmwareversion gleichwertig oder aktueller als die Firmwareversion der VPN-Gruppe ist.

Versuche, ein Gerät einer VPN-Gruppe hinzuzufügen, in der es bereits Mitglied ist, bzw. ein Gerät aus einer VPN-Gruppe zu entfernen, in der es kein Mitglied ist, werden nicht beachtet.

Das Hinzufügen von Geräten zu VPN-Gruppen oder das Löschen von Geräten aus VPN-Gruppen erfolgt im Hintergrund. Der Dialog kann bereits geschlossen werden, während dieser Vorgang noch läuft.

6.6.4 VPN-Gruppe-Eigenschaften (VPN group properties dialog) – Vermaschte VPN-Netzwerke

Die Geräte, die Mitglied einer VPN-Gruppe sind, bilden ein vermaschtes VPN-Netzwerk. Für jedes Mitglied legt mdm eine VPN-Verbindung (sog. VPN-Gruppenverbindung) zu jedem anderen Gerät an, das Mitglied dieser Gruppe ist. Ein Gerät kann Mitglied mehrerer VPN-Gruppen sein. Sollten dadurch mehrere VPN-Verbindungen zwischen denselben beiden Geräten entstehen, legt mdm nur eine derartige Verbindung an. VPN-Gruppen sind nicht für Firmwareversionen verfügbar, die älter sind als 6.0.

Mit dem *VPN group properties dialog* können gemeinsame, von allen VPN-Verbindungen innerhalb der Gruppe genutzte Variablen konfiguriert werden.

Informationen zum Anlegen, Löschen oder Bearbeiten von VPN-Gruppen und zum Hinzufügen oder Entfernen von Geräten aus diesen Gruppen siehe „VPN-Gruppen-Übersicht (VPN group overview table)“ auf Seite 92.

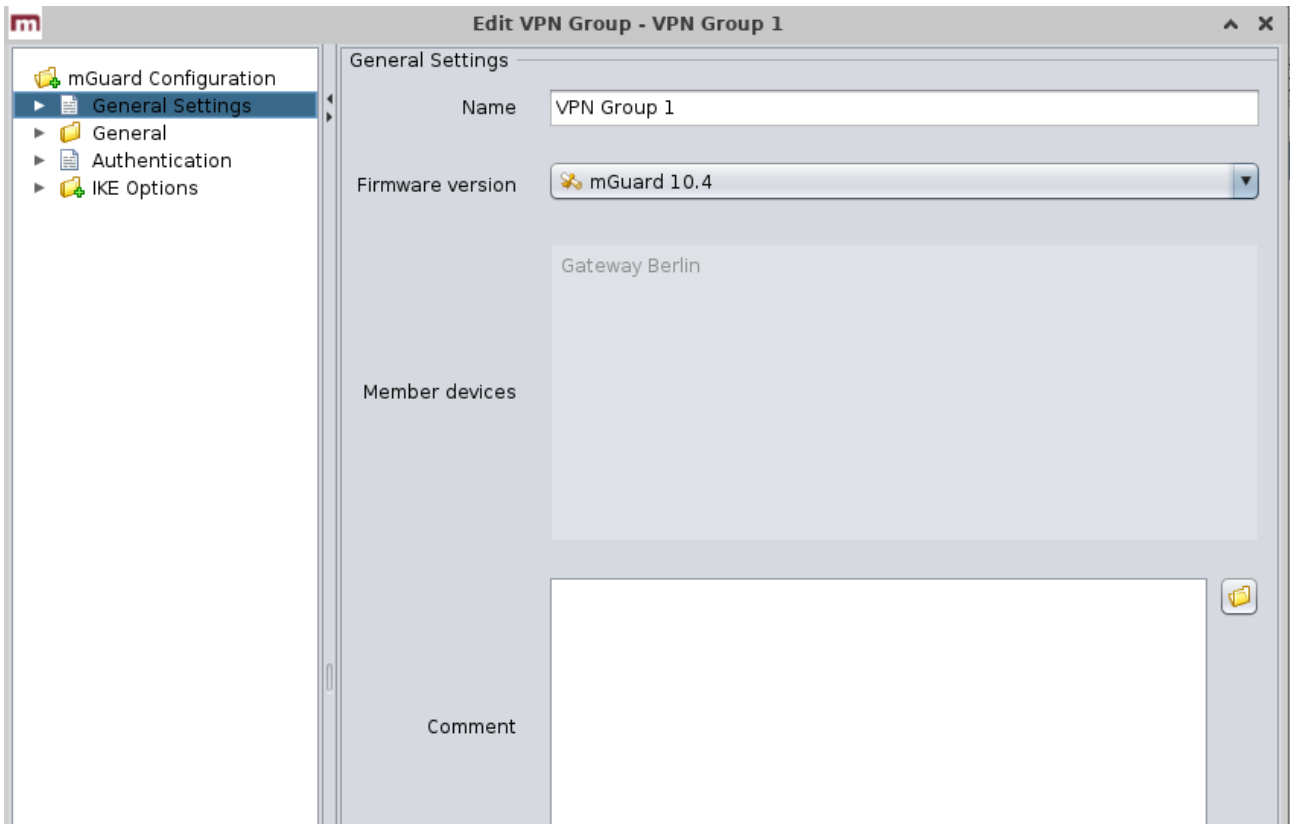


Bild 6-23 Der mdm Dialog VPN Group Properties

Ähnlich wie die *Dialoge Device bzw. Template Properties* enthält auch der *VPN group properties dialog* auf der linken Seite einen Navigationsbaum. Damit kann bequem zwischen den Variablen navigiert werden.

General settings

Der *VPN group properties dialog* enthält den Menüpunkt **General settings** zur Konfiguration zusätzlicher Parameter mit Bezug zu mdm. Die folgenden Parameter können in den **General settings** eingestellt werden.

VPN-Gruppe-Eigenschaften – VPN group properties dialog (Vermaschte VPN-Netzwerke)

General settings

Name

Mit dem Namen wird die VPN-Gruppe innerhalb des mdm erkannt. Der Name muss eindeutig sein.

Firmware Version

Da unterschiedliche Versionen der mGuard-Software über unterschiedliche Variablensätze verfügen, muss hier die zur auf dem mGuard installierten Firmware passende Firmware ausgewählt werden.

Ein Gerät kann nur Mitglied einer VPN-Gruppe sein, wenn dessen Firmwareversion **gleichwertig oder aktueller** als die Firmwareversion der VPN-Gruppe ist.

CAUTION: Unwiderrufliche Änderungen

Ein Downgrade zurück auf eine ältere Version ist nicht möglich. Daher ist bei einer Änderung der Firmwareversion größte Sorgfalt geboten. Weitere Informationen dazu erhalten Sie unter „Versionseinstellungen der Firmware und Vererbung“ auf Seite 84.

ACHTUNG: Neue Standardwerte in mGuard-Firmware 8.5 und 8.6

Wenn eine vorhandene VPN-Guppe von mGuard**-Firmwareversion < 8.5** auf Version **8.5 oder 8.6** aktualisiert wird und die Tabelle *Algorithms* in "ISAKMP SA (Key Exchange)" sowie in "IPsec SA (Data Exchange)" die Standardkonfiguration haben, dann wird jeweils das bisherige Standard-Verschlüsselungsverfahren (3DES) beibehalten.

In diesem Fall wird der Wertetyp der Tabelle von "***Inherited***" auf "***Custom***" geändert.

Weitere Informationen zur Verwaltung von Firmware-Upgrades Ihrer Geräte mit mdm siehe Kapitel 7.6.

Member devices (schreibgeschützt)

Die Geräte, die aktuell Mitglieder der VPN-Gruppe sind.

Comment

Optionale Anmerkungen.

VPN-Gruppenverbindungen

Beim Anlegen von VPN-Gruppenverbindungen kombiniert mdm die Variablen in der VPN-Gruppe mit zusätzlichen Variablen im Gerät. Während die Variablen in der VPN-Gruppe bei allen Verbindungen in dieser Gruppe gleich sind, sind die zusätzlichen Variablen gerätespezifisch, aber allen VPN-Gruppenverbindungen dieses Geräts gemeinsam.

Die VPN-Gruppe enthält folgende Variable:

- General VPN settings
- Protocol settings
- Authentication settings
- IKE options

Geräte und Templates enthalten Variablen unter dem **Gruppenkonfigurationsknoten IPsec VPN » VPN, die beim Hinzufügen von VPN-Gruppen zu einem Gerät durch mdm verwendet werden:**

- Tunnel settings
- NAT settings
- Firewall settings

Das lokale VPN-Netzwerk

Das für die VPN-Gruppenverbindungen zu verwendende lokale VPN-Netzwerk kann entweder im Template oder im Gerät angegeben werden (**IPsec VPN » VPN Group Configuration » Tunnel Settings » Local**) oder wird, wenn das Gerät im Routermodus betrieben wird, automatisch abgeleitet werden. Ist die Variable **IPsec VPN » VPN Group Configuration » Tunnel Settings » Use first internal address as local VPN network in router mode** auf Yes gesetzt, verwendet mdm die erste interne Adresse samt zugehöriger Netzmaske, sodass das entsprechende lokale Netzwerk durch den VPN-Tunnel sichtbar ist. Diese Einstellung wirkt sich im geschützten Modus nicht aus, d. h. wenn das Gerät im geschützten Modus verwendet wird, muss das lokale VPN-Netzwerk immer angegeben werden.

Local 1:1 NAT

VPN-Gruppenverbindungen können so konfiguriert werden, dass sie auf lokalen Adressen 1:1 NAT durchführen können. Keiner der anderen NAT-Mechanismen für VPN-Verbindungen ist in VPN-Gruppenverbindungen verfügbar.

Das lokale 1:1 NAT wird aktiviert, in dem man die Variable **IPsec VPN » VPN Group Configuration » NAT » Enable 1:1 NAT of local addresses** auf Yes setzt. Das lokale Netzwerk im Tunnel muss angegeben werden.

Das Netzwerk innerhalb Tunnel (d. h. Netzwerkadressen, wie sie von der Gegenstelle gesehen werden), wird durch die 1:1 NAT-Einstellungen angegeben. Dies ist der Unterschied zur Webinterface des mGuard, wo das Netzwerk außerhalb des Tunnels (d. h. die Netzwerkadressen, wie sie vom lokalen Netzwerk aus zu sehen sind) in den 1:1 NAT-Einstellungen angegeben wird.

Erweiterte Firewall-Regeln

In den Firewall-Regeln des Knotens **IPsec VPN » VPN Group Configuration** sind zusätzliche **Combine-**Felder enthalten, die mit den Adressen **From IP** und **To IP** oder Netzwerken verbunden sind. Ist ein Combine-Feld auf No gesetzt, wo wird die entsprechende Adresse bzw. das entsprechende Netzwerk ohne Änderung in der VPN-Gruppenverbindung verwendet.

Ist ein **Combine**-Feld auf **Yes** gesetzt, wird die in der Tabelle eingegebene Adresse bzw. das hier eingegebene Netzwerk mit dem lokalen oder Remote-VPN-Netzwerk verbunden, um das in der VPN-Gruppenverbindung genutzte Netzwerk zu berechnen.

- In den Firewall-Regeln für eingehenden Datenverkehr wird das Feld **From IP** mit dem Remote-VPN-Netzwerk und das Feld **To IP** mit dem lokalen VPN-Netzwerk kombiniert.
- In den Firewall-Regeln für ausgehenden Datenverkehr wird das Feld **From IP** mit dem lokalen VPN-Netzwerk und das Feld **To IP** mit dem Remote-VPN-Netzwerk kombiniert.

Der Wert des Feldes **From IP** oder **To IP** wird mit dem VPN-Netzwerk kombiniert, indem die Adressen oktettweise hinzugefügt werden, d. h. jedes Oktett wird einzeln hinzugefügt. Kommt es nach dem Hinzufügen zweier Oktetts zu einem Überlauf (d. h. es ist größer als 255), wird der Wert 256 subtrahiert (die Addition „wickelt sich also drumherum“). Die Netzwerkmaske des Werts des Feldes **From IP** oder **To IP** (oder 32 wenn das Feld keine Netzwerkmaske enthält) wird auf das Ergebnis angewendet.

Beispiele:

– Weist das Feld **From IP** oder **To IP** den Wert 0.0.78.0/24 auf und das VPN-Netzwerk ist 10.6.0.0/16, lautet der kombinierte Wert 10.6.78.0/24.
– Weist das Feld **From IP** oder **To IP** den Wert 0.1.78.0/24 auf und das VPN-Netzwerk ist 10.6.0.0/16, lautet der kombinierte Wert 10.7.78.0/24.

6.7 VPN-Verbindungen konfigurieren

Mit mdm lassen sich die Konfigurationen für eine große Anzahl von VPN-Tunneln problemlos anlegen. Generell gelten Angaben in Kapitel 6.1, Kapitel 6.3.3, Kapitel 6.4.3 und Kapitel 6.4.5 auch für die VPN-Konfiguration.

VPNs erfordern jedoch die Berücksichtigung einiger besonderer Einstellungen, beispielsweise die automatische Konfiguration der VPN-Gegenstelle. Im vorliegenden Abschnitt werden diese näher beschrieben. Die VPN-Konfiguration finden Sie im Knoten **IPsec VPN** des Navigationsbaumes.

VPN-Verbindungen hinzufügen und bearbeiten

Öffnen Sie zum Hinzufügen, Ändern oder Löschen von VPN-Verbindungen den Knoten **IPsec VPN » Connections**. Legen Sie zum Erstellen einer neuen Verbindung eine neue Tabellenzeile an (siehe „mGuard Tabellenvariablen ändern“ auf Seite 38). Sobald Sie eine Verbindung einrichten, erscheint diese als Knoten im Navigationsbaum. Öffnen Sie zum Bearbeiten einer Verbindung den Knoten dieser Verbindung im Navigationsbaum und navigieren Sie zu den gewünschten Einstellungen. Die Struktur des Verbindungsknotens ähnelt der Menüstruktur des mGuard.

Die Verbindungstabelle ist schreibgeschützt, d. h. wenn Sie Änderungen an der Verbindung vornehmen möchten, beispielsweise den Namen der Verbindung ändern oder eine Verbindung deaktivieren, müssen Sie zu dem jeweiligen Knoten navigieren.

Die Berechtigungseinstellungen der Verbindungstabelle in einem Template gilt nur für diese Tabelle, nicht jedoch für die Inhalte der Verbindung. Wenn Sie die Tabelle auf *No override* setzen, können die Einstellungen der VPN-Verbindung immer noch an dem Gerät, das das Template verwendet, modifiziert werden. Der Benutzer auf Geräteebene ist jedoch nicht berechtigt, weitere Verbindung zur Tabelle hinzuzufügen.

Automatische Konfiguration der VPN-Gegenstelle

Sie können die VPN-Verbindung für die Gegenstelle automatisch anlegen (siehe Bild 6-24). Setzen Sie dazu den Cursor in das Feld **Peer device** und drücken Sie die Pfeiltaste *Abwärts*. Eine Liste der verfügbaren Geräte wird angezeigt. Sie können die Anzahl der Geräte in der List begrenzen, indem Sie die ersten Zeichen der Management-ID des gewünschten Geräts eingeben. Bei Auswahl eines Geräts wird die VPN-Konfiguration für dieses Gerät automatisch erstellt.

Nicht alle Einstellungen der Gegenstelle können automatisch vorgenommen werden, daher müssen Sie Teile der Konfiguration manuell eingeben. Überprüfen Sie die Unterknoten der VPN-Verbindung für diese Einstellungen. Sie befinden sich in den entsprechenden Unterknoten und sind von den anderen Einstellungen durch den Text **Configuration of peer device** getrennt (Beispiel Bild 6-24).

Die automatisch angelegten VPN-Verbindungen werden schreibgeschützt in der Gegenstellen-Verbindungstabelle dargestellt, d. h. die Konfiguration auf Seiten der Gegenstelle kann nicht geändert werden.

Wenn die VPN-Gateways über unterschiedliche Firmwareversionen verfügen, kann eine Gegenstelle nur im *Device properties dialog* (Geräte-Eigenschaften) mit einer *älteren* Firmwareversion konfiguriert werden. Wenn Sie die Gegenstelle im *Device properties dialog* mit einer aktuellen Firmware als in der Verbindung vorhanden konfigurieren, wird Geräten mit einer älteren Firmware keine Verbindung hergestellt. Eine Fehlermeldung oder Warnung wird nicht angezeigt.

Die automatisch hergestellten VPN-Verbindungen können als Alternative zur Funktion mGuard *Tunnel Group* (mGuard ab Version 5.0) verwendet werden, siehe Anmerkungen im nachfolgenden Abschnitt *Hinweise für VPN-Verbindungen*.

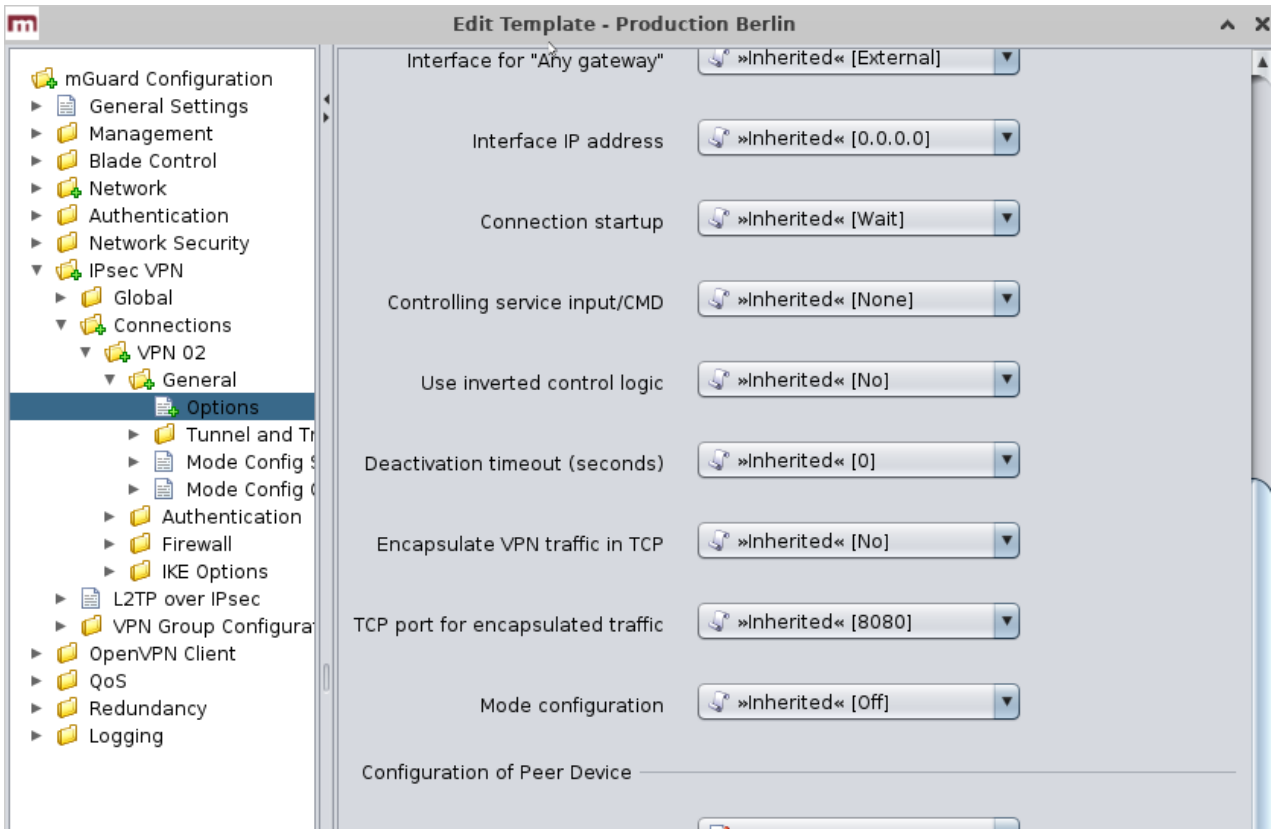


Bild 6-24 Automatische Konfiguration einer VPN-Gegenstelle

VPN-Kennungen automatisch einstellen

Das lokale und das Remote-Maschinenzertifikat sind mdm in zahlreichen typischen Verwendungsszenarien bekannt (wenn VPN-Konfigurationen für die Gegenstelle durch mdm angelegt werden). mdm kann diese Informationen zum automatischen Einrichten einer lokalen VPN-Kennung und der Remote-VPN-Kennung verwenden, d. h. Ableitung der Kennungen von den bekannten Zertifikaten. Bei der Verwendung von CA-Zertifikaten zur Authentifizierung von VPN-Verbindungen müssen diese Variablen gesetzt werden.

Zur Nutzung dieser Funktion **IPsec VPN » Connections » Connection Name » Authentication » VPN Identifiers node öffnen und Variable Set VPN Identifiers automatically auf Yes setzen. In diesen Knoten werden** die lokale VPN-Kennung und die Kennzeichnungsvariablen der Remote-VPN ignoriert, die Kennungen werden von den Zertifikaten abgeleitet.

Firewall-Regeln kopieren

Die Firewall-Tabellen innerhalb der VPN-Verbindungen enthalten eine Schaltfläche **Copy from Main**. Durch Anklicken dieser Schaltfläche wird der Inhalt der entsprechenden Firewall-Tabelle für Netzwerkverkehr außerhalb von VPN kopiert (d. h. wenn die aktuelle Firewall-Tabelle für eingehenden Datenverkehr bestimmt ist, wird die Firewall-Tabelle für eingehenden Datenverkehr außerhalb von VPN kopiert, analog wird für ausgehenden Datenverkehr verfahren).

Die kopierten Firewall-Regeln werden durch eine andere Hintergrundfarbe angezeigt. Die Hintergrundfarbe wird entfernt, wenn ein anderer Knoten des Navigationsbaumes geöffnet wird.

Hinweise für VPN-Verbindungen

Die folgenden Hinweise sind hilfreich, wenn die Tunnelgruppen-Funktion nicht verwendet wird und die VPN-Verbindungen explizit definiert sind.

Bei 1:N-VPN-Konfigurationen wird empfohlen, die VPN-Verbindung in einer Vorlage zu definieren und das zentrale Gerät im Feld **Peer device** auszuwählen (siehe obenstehenden *Abschnitt Automatische Konfiguration der VPN-Gegenstelle*). Wenn Sie dieses Template den Geräten zuweisen, legt mdm automatisch die Konfigurationen der N-Verbindung für das zentrale Gerät an.

Bei einer 1:N-VPN-Konfiguration ist es für die Konfiguration der Gegenstelle erforderlich, die Gateway-Adresse des aktuellen Geräts anzugeben (siehe Bild 6-24, **Configuration of peer device » Gateway address of peer**). Bei der Verwendung von Zertifikaten kann *%any* (siehe Bild 6-24) als Adresse im Template verwendet werden, aber als PSK-Authentifizierung ist *%any* nicht zulässig. Bei Verwendung der PSK-Authentifizierung muss für jedes Gerät die externe Adresse (wenn kein NAT verwendet wird) in das Feld **Configuration of peer device » Gateway address of peer** eingegeben werden.

7 mdm-Client – Verwaltungsaufgaben

7.1 Konfigurationen in mGuard-Geräte hochladen

7.1.1 Upload-Methoden

Einen Upload der Konfiguration auf die Geräte können Sie wie folgt einleiten:

- Öffnen Sie im Hauptmenü (Kapitel 5.2.1) das Menü **Upload** und wählen Sie die Geräte aus, die Sie hochladen möchten (**All**, **Selected** oder **Changed**, d. h. alle Geräte in mdm, die mit dem mGuard verbunden sind mit Konfigurationsstatus *out-of-date*).
- Klicken Sie im Kontextmenü (Rechtsklick auf die Gerätetabelle) auf **Upload**. Damit werden alle aktuell ausgewählten Geräte in der Gerätetabelle zum Hochladen vorgesehen.
- Klicken Sie auf das Symbol  in der Symbolleiste, um für die in der Tabelle aktuell ausgewählten Geräte einen Upload einzuleiten.

mdm bietet mehrere Methoden zum Hochladen der Konfigurationsdateien in den mGuard. Geben Sie nach Einleitung des Uploads die gewünschte Methode an.

Auto (*auto*)

Je nachdem, ob **Accessible via** in **General settings** eingerichtet ist, führt mdm entweder

- ein SSH-Push-Upload (siehe “einen Export der Konfiguration in das Dateisystem (siehe “Pull-Konfiguration vorbereiten (*prepare pull configuraton)”).”) oder
- einen Export der Konfiguration in das Dateisystem (siehe “Pull-Konfiguration vorbereiten (*prepare pull configuraton)”).

Upload über SSH (*upload via ssh*)

mdm versucht, alle vorgesehenen Geräte per SSH-Push-Upload zu versorgen.

Zur Durchführung eines SSH-Uploads müssen im *Device properties dialog* (Geräte-Eigenschaften) unter **General Settings** im Feld **Accessible via** eine IP-Adresse oder ein Hostname angegeben werden (siehe „Geräte-Eigenschaften (Device properties dialog)“ auf Seite 64). Wenn dies nicht der Fall ist, wird im Protokollfenster eine Fehlermeldung angezeigt und der Upload-Status wird auf *Fehler* gesetzt. Eine SSH-Portnummer (abweichend vom Standard-SSH-Port) kann optional konfiguriert werden.

Wenn sich mdm aufgrund falscher SSH-Authentifizierungsinformationen nicht am Gerät anmelden kann, wird ein Fehler im Protokollfenster angezeigt und der Upload-Status wird auf Fehler gesetzt.

Wenn nicht auf den mGuard zugegriffen werden kann, unternimmt mdm einen neuen Versuch zum Hochladen der Konfiguration. Nach dem die maximale Anzahl der Versuche erreicht ist, wird im Protokollfenster eine Fehlermeldung angezeigt und der Upload-Status wird auf Fehler gesetzt.

Der mdm-Server greift über ein SSH-Protokoll auf den mGuard zu. Anschließend wird die Konfigurationsdatei in das Gerät kopiert und eingesetzt. Jegliche im Upload-Prozess auftretenden Fehler werden im Protokollfenster angezeigt. Für den Einsatz dieser Methode müssen folgende Voraussetzungen erfüllt sein:

- Im *Device properties dialog* (Geräte-Eigenschaften) unter **General Settings** im Feld **Accessible via** eine IP-Adresse oder ein Hostname angegeben werden. Die SSH-Portnummer kann optional konfiguriert werden.

- Der mdm-Server muss über die Adresse **Accessible via** auf das mGuard zugreifen können, d. h. der Datenverkehr darf nicht durch eine Firewall blockiert werden, und ein NAT-Gerät im Kommunikationspfad muss so konfiguriert werden, dass es die Kommunikation zwischen dem mdm-Server und dem mGuard ermöglicht.
- Falls der Zugriff auf den mGuard über die externe Schnittstelle erfolgt, muss der SSH-Fernzugriff im mGuard aktiviert werden.
- Die Passwörter für den Gerätezugriff müssen korrekt gesetzt sein. Melden Sie sich als Benutzer ***admin*** an, wenn Sie eine Gerätekonfiguration in den mGuard laden können. Bei einer Passwortänderung sind zwei Passwörter im Einsatz: das alte Passwort für den Gerätezugriff und das neue Passwort, das nach der Anmeldung eingerichtet wird. Daher verfolgt mdm das aktive Passwort für den Gerätezugriff automatisch und verwendet *nicht* das im *Device properties dialog* (Geräte-Eigenschaften) für diesen Zweck konfigurierte Passwort. Wenn Sie das aktive Passwort manuell ändern möchten, können Sie die Option **Set Current Device Credentials** im Kontextmenü der Gerätetabelle verwenden.

Wenn auf ein Gerät nicht zugegriffen werden kann, versucht mdm nach einer bestimmten Wartezeit erneut, die Verbindung herzustellen. Sobald die maximale Anzahl Versuche erreicht ist, stellt mdm die Versuche zum Hochladen der Konfiguration ein und zeigt im Protokoll eine Fehlermeldung an.

Wenn die Änderung der Konfiguration einen Neustart des mGuards erfordert (z. B. wenn von geschützten auf Router-Modus gewechselt wird), wird mdm nicht sofort über die erfolgreiche Übernahme der Konfiguration informiert. Daher wird nach einer Wartezeit erneut auf das Gerät zugegriffen. Passen Sie die Einstellungen für **Accessible via**, **SSH Port** und **Web configuration port** nach dem initialen Upload an, falls diese erforderlich ist (siehe „Accessible via“ auf Seite 66). Übernehmen Sie ggf. die Einstellung Accessible via nach dem ersten Upload. Alternativ kann der Konfigurationszustand über die Option **Set Upload State** im Kontextmenü der Geräte-Übersicht (*Device overview table*) manuell eingestellt werden.

Wird das Passwort im *Device properties dialog* (Geräte-Eigenschaften) geändert und das Hochladen der Gerätekonfiguration schlägt im Anschluss fehl, wurde die Passwortänderung möglicherweise zwar am mGuard übernommen, aber mdm konnte die Erfolgreiche Änderung nicht nachverfolgen. In diesem Fall müssen Sie das aktive Passwort in mdm über die Option **Set Current Device Credentials** im Kontextmenü der Tabelle Geräteübersicht manuell einrichten, andernfalls kann sich mdm nicht für den nächsten Upload anmelden.

Aufgrund dieses potenziellen Problems wird empfohlen, Änderungen des Passworts getrennt von umfangreichen Änderungen an der Konfiguration zu übernehmen (hochzuladen).

Pull-Konfiguration vorbereiten (*prepare pull configuration*)

Die Konfiguration aller vorgesehenen Geräte wird in das Dateisystem exportiert.

Das Exportverzeichnis kann in der Präferenzdatei des Servers konfiguriert werden (siehe Kapitel 10.1).

Die Dateinamen aller Konfigurationsdateien werden im *Device properties dialog* (Geräte-Eigenschaften) unter **General Settings** und in der Gerätetabelle angezeigt.

Falls die Dateien nicht in das Datei geschrieben werden können (keine Berechtigung, kein ausreichender Speicherplatz, Exportverzeichnis nicht vorhanden usw.), zeigt mdm im Protokoll einen Fehler an und der Upload-Status wird auf Fehler gesetzt.

Die mGuards können Konfigurationsdateien von einem HTTPS-Server ziehen. mGuards ab Firmwareversion 5.0 können zusätzlich Lizenzdatei ziehen.

Wenn Sie die Konfigurations-Pull-Funktion (*Configuration Pull*) nutzen möchten, finden Sie im Abschnitt *Manual configuration upload* eine Beschreibung zum Export von Konfigurations- und Lizenzdateien. Darüber hinaus müssen folgende Voraussetzungen erfüllt sein:

– Ein *HTTPS Configuration-Pull-Server* muss konfiguriert sein (siehe Kapitel 3.2).
– Das Ziehen der Konfiguration muss am mGuard konfiguriert werden (siehe Software-Referenzhandbuch „Konfigurieren der mGuard Security-Appliances“ unter phoenixcontact.net/products).
  Darüber hinaus müssen die mGuards mit den beiden folgenden Befehlen ihre Konfiguration entsprechend der Namenskonvention für mdm Dateinamen konfiguriert werden:

```
gaiconfig --set GAI_PULL_HTTPS_DIR <your_directory>
gaiconfig --set GAI_PULL_HTTPS_FILE <identifier>.atv
```

– Falls der mdm-Server und der Konfigurationsserver auf verschiedenen Maschinen installiert sind, müssen Sie dafür sorgen, dass die mdm Exportdateien mit dem Dateisystem des Konfigurationsservers synchronisiert werden.
– Wenn mdm manuell installiert wurde, sind zusätzliche Schritte erforderlich, wenn Sie eine Rückmeldung erhalten möchten, ob die Übermittlung per Pull-Konfiguration erfolgreich war oder nicht.
– mdm kann Syslog-Meldungen an der Schnittstelle UDP 7514 (Standardeinstellung) empfangen, um den Konfigurationsstatus eines Geräts zu erkennen, wenn mdm in den Konfigurations-Servereinstellungen als Syslog-Server eingerichtet ist.

Die Pull-Anfrage enthält Angaben zum allgemeinen Konfigurationsstatus des mGuard. Diese Informationen werden als Syslog-Meldung vom Konfigurationsserver an mdm übermittelt. Die Schnittstelle, an der mdm auf Syslog-Meldungen horcht, kann in der Präferenzdatei des mdm-Servers konfiguriert werden (siehe Kapitel 10.1).

Profil verschlüsseln

Die vom mdm-Server exportierten Konfigurationsprofile können optional mit einem gerätespezifischen Schlüssel kodiert werden. Der mdm-Server lädt den Schlüssel vom Lizenzserver herunter. Nur der öffentliche (Kodierungs-) Schlüssel ist Phoenix Contact bekannt, der entsprechende private (Dekodierungs-) Schlüssel wird im mGuard in einem besonderen Hardwaremodul gespeichert und kann nicht extrahiert werden.

Die Profilverschlüsselung kann nur mit mGuard Hardware verwendet werden, die diese Funktion unterstützt. Hierfür ist eine Firmwareversion ab 7.6.0 erforderlich.

Da Profile mit einem speziellen Geräteschlüssel kodiert sind, kann nur der mGuard diesen Schlüssel lesen, für den das Profil verschlüsselt wurde.

Gehen Sie zum Verschlüsseln von Profilen wie nachfolgend beschrieben vor:

– Beim Kundendienst von Phoenix Contact erhalten Sie einen Benutzernamen und ein Kennwort zum Download von Profilschlüsseln. Konfigurieren Sie den mdm-Server für die Verwendung von „Benutzername“ und „Passwort“; siehe Kapitel 10.1, Knoten *license » licenseServer » reqUsername* **und** *license » licenseServer » reqPassword***.**
– Wählen Sie die Geräte aus, für die Sie in der Geräte-Übersicht (*Device overview table*) Profile verschlüsseln möchten.

– Wählen Sie im Kontextmenü *Get Profile Key* aus, um die Schlüssel auf den mdm-Server zu laden. Die Seriennummern und Flash-IDs der Geräte werden verwendet, um sie gegenüber dem Lizenzserver zu legitimieren und müssen daher mdm bekannt sein, tragen Sie diese daher ggf. ein.
– Wählen Sie zur Aktivierung der Profilverschlüsselung im Kontextmenü die Option *Enable/Disable profile encryption* aus.

Profilschlüssel verwalten

Die für die Profilverschlüsselung benötigten Profilschlüssel sind in der Tabelle aufgeführt. Neue Profilschlüssel können importiert werden. Vorhandene Profilschlüssel können gelöscht werden.

Pull-Konfiguration vorbereiten und SSH-Upload versuchen

(*prepare pull configuration and try ssh upload*)

Diese Methode kann verwendet werden, um Geräte zu aktualisieren, die online über SSH-Push-Upload verwaltet werden und ihre Pull-Konfiguration auf einmal aktualisieren (exportieren) können.

mdm führt folgende Aufgaben durch:

1. Vorbereitung der Pull-Konfiguration wie oben beschrieben (siehe “Pull-Konfiguration vorbereiten (*prepare pull configuraton)”*) für alle ausgewählten Geräte.
2. Prüfung, ob im *Device properties dialog* (Geräte-Eigenschaften) unter **General Settings** im Feld **Accessible via** (siehe „Geräte-Eigenschaften (Device properties dialog)“ auf Seite 64) für jedes der ausgewählten Geräte eine IP-Adresse oder ein Hostname angegeben ist.
3. Für diejenigen ausgewählten Geräte, für die eine IP-Adresse oder ein Hostname angegeben wurde, wird ein SSH-Push-Upload auf die ausgewählten Geräte durchgeführt (siehe “einen Export der Konfiguration in das Dateisystem (siehe “Pull-Konfiguration vorbereiten (*prepare pull configuraton)”).”).

Manueller Konfigurations-Upload

Falls nur einige Geräte konfiguriert werden sollen und kein Zugriff mit mdm möglich ist, können die Konfigurationsdateien in das Dateisystem exportiert und auf die Geräte über die Webinterface des jeweiligen Geräts manuell hochgeladen werden. Jedes Gerät wird durch eine eindeutige Benennung identifiziert, die durch mdm automatisch vergeben wird. Diese Benennung (8-stelliger Hex-String mit kleingeschriebenen Zeichen) wird für den Export als Dateiname verwendet. Die Konvention für die exportierte Konfigurationsdatei: *<identifier>.atv.* Die Dateinamen aller Konfigurationsdateien werden im *Device properties dialog* (Geräte-Eigenschaften) unter **General Settings** und in der Gerätetabelle angezeigt.
Für den Export der Konfigurationsdateien müssen folgende Voraussetzungen erfüllt sein:

– Ein Exportverzeichnis kann in der Präferenzdatei des mdm-Servers konfiguriert werden (siehe Kapitel 10.1). Hinweis: Diese Dateien können auf der Client-Seite nicht lokal exportiert werden. Die Dateien werden immer serverseitig in das Exportverzeichnis exportiert, das in der Präferenzdatei des Servers konfiguriert wurde.
– Der Server muss Schreibzugriff auf das Exportverzeichnis besitzen.
– Es muss ausreichend Speicherplatz für den Export der Dateien vorhanden sein.

7.1.2 Zeit für Upload (*Upload Time*)

Die Zeit, in der ein Upload durchgeführt werden sollte. Zeitangaben erfolgen im ISO-Format (JJJJ-MM-TT, wobei JJJJ das Jahr, MM den Monat dieses Jahres zwischen 01 und 12 und TT den Tag dieses Monats zwischen 01 und 31 bezeichnet). optional kann eine ISO-Zeitangabe folgen (hh:mm:ss, wobei hh die Stunde im 24-Stunden-Format, mm die

Minute und ss die Sekunde bezeichnet). Viertel fünf und 20 Sekunden am Nachmittag des 22. Dezember 2010 würde beispielsweise wie folgt dargestellt: 2010-12-22 16:15:20. Alternativ können Sie durch Anklicken des Symbols  ein Datum aus dem Kalender auswählen.

Wurde die aktuelle Zeit (Standardeinstellung) oder eine zurückliegende Zeit angegeben, dann erfolgt der Upload so schnell wie möglich.

Im Feld Upload within ... minutes after wird eine Obergrenze für den Zeitrahmen, in dem mdm den Upload versucht. Ist dieser Versuch innerhalb des angegebenen Zeitraums nicht erfolgreich, werden keine weiteren Versuche durchgeführt und der Upload wird als fehlgeschlagen gewertet.

7.1.3 Temporäres Upload-Passwort (*Temporary upload password*)

Wird in dieses Feld ein Passwort eingegeben und ein Push-Upload durchgeführt, verwendet mdm dieses Passwort bei der Anmeldung am mGuard über SSH. Das Passwort wird für alle Geräte verwendet. Bleibt dieses Feld frei (Standardeinstellung), verwendet mdm für jedes Gerät das bekannte Admin-Passwort.

Diese Funktion ist hilfreich, wenn der mGuard zur Authentifizierung der Anmeldeanfrage nicht das Admin-Passwort verwendet, beispielsweise wenn der mGuard keine RADIUS-Authentifizierung verwendet.

Wird ein temporäres Upload-Passwort verwendet, kann mdm für die Anmeldung am mGuard einen anderen Benutzernamen als Admin verwenden. Dieser Benutzername kann im *Device properties dialog* (Geräte-Eigenschaften) *oder im Template properties dialog* (Template-Eigenschaften) konfiguriert werden. Öffnen Sie den Knoten „**Authentication » Local Users » Temporary Upload User**“ im Navigationsbaum**.**

7.1.4 Upload history

Zeigt den Upload-Verlauf an. Der Upload-Verlauf enthält für jedes Gerät Informationen zum letzten Upload und deren Ergebnisse. Wählen Sie zur Ansicht des Upload-Verlaufs eines Geräts den mGuard in der Geräte-Übersicht (*Device overview table*) und öffnen Sie mit einem Rechtsklick das Kontextmenü. Öffnen Sie durch Klicken auf **Upload History** das Fenster mit dem Upload-Verlauf.

7.2 Gerätelizenzen und Voucher verwalten

Mit mdm können Sie Ihre Gerätelizenzen und Voucher zentral verwalten. Das Hauptmenü enthält zwei Menüpunkte: **Licenses » Manage Device Licenses** und **Licenses » Manage License Vouchers.** Diese werden in den folgenden Abschnitten genau erklärt.

7.2.1 Voucher verwalten

Klicken Sie zum Öffnen des *Voucher Management Window* im Hauptmenü auf **Licenses » Manage License Vouchers**.

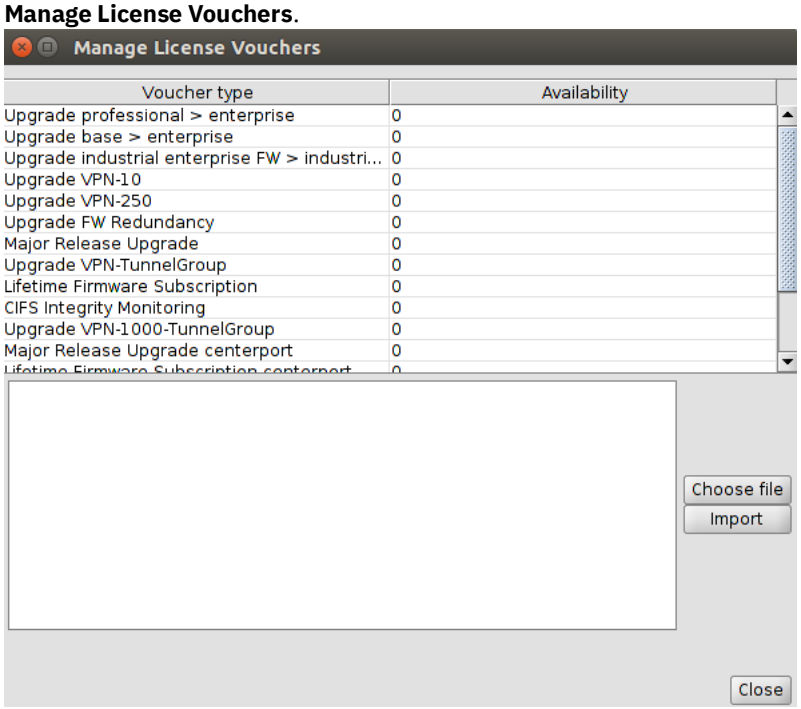


Bild 7-1 Fenster Voucher Management

In diesem Fenster werden die für jeden Vouchertyp verfügbaren Voucher angezeigt. Kopieren Sie zum Import eines Vouchers entweder die Voucher-Informationen in das Feld Import oder markieren Sie eine Datei mit den Voucher-Daten und klicken Sie auf *Import*. Das einzige unterstützte Importformat ist CSV, d. h. jede Zeile der Importdatei muss folgende Informationen enthalten:

<voucher number>,<voucher key>

7.2.2 Lizenzen anfordern/generieren

Bevor eine Gerätelizenz angefordert werden kann, muss mindestens ein Voucher des entsprechenden Typs (Major Release Upgrade, VPN usw.) in mdm importiert werden. Darüber hinaus wird für die Lizenzanforderung die Seriennummer benötigt, d. h. die Nummer muss in den **General Settings** des Geräts angegeben werden. Diese Identifikationsnummer kann entweder manuell eingegeben werden oder wird während des Push- oder Pull-Uploadvorgangs automatisch vom Gerät angefordert.

Markieren Sie zum Anfordern einer Lizenz die Geräte in der Geräte-Übersicht (*Device overview table*) und klicken Sei entweder auf das Symbol in der Symbolleiste oder wählen Sie im Kontextmenü **Generate License** aus. Die generierten Lizenzen werden anschließend im *License Management Window* und auf der Seite **Management » Licensing** im *Device properties dialog* (Geräte-Eigenschaften) angezeigt und mit dem nächsten Upload auf dem Gerät installiert. Das Ergebnis der Lizenzanforderung wird auch im Protokollfenster angezeigt.

mdm muss sich zum Generieren/Anfordern von Lizenzen mit dem Lizenzserver verbinden können.

7.2.3 Gerätelizenzen verwalten

Klicken Sie zum Öffnen des *License Management Window* im Hauptmenü auf **Licenses » Manage Device Licenses**. Im Fenster *License Management Window* werden alle von mdm verwalteten Lizenzen und die zugehörigen Daten angezeigt. Zusätzlich zu den durch das im vorhergehenden Abschnitt beschriebene Verfahren angeforderten/generierten Lizenzen können auch vorhandene Lizenzen importiert werden. Geben Sie zum Import von Lizenzen entweder die Namen der Lizenzdateien in das Feld *Import* ein oder kopieren Sie diese in dieses Feld (ein Dateiname pro Zeile) und klicken Sie anschließend auf Import, oder klicken Sie auf die Schaltfläche **Choose File** und markieren Sie im Dialog eine oder mehrere Dateien.

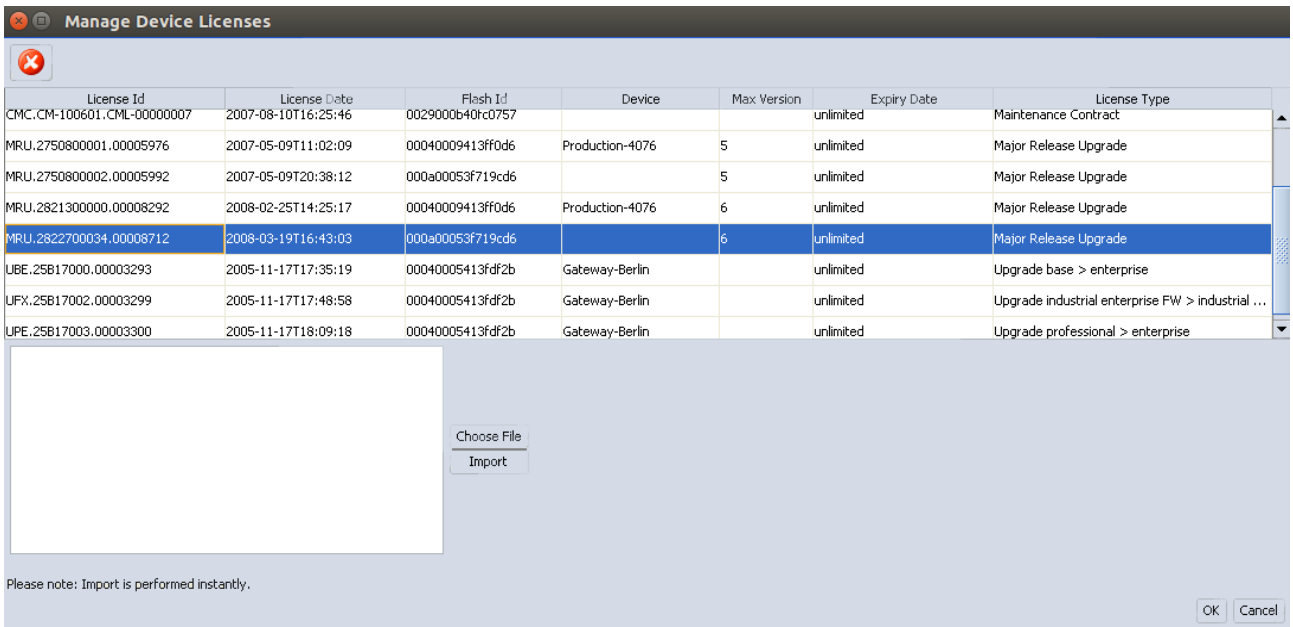


Bild 7-2 Fenster License Management

Der *Device properties dialog* (Geräte-Eigenschaften) einer Datei kann durch einen Doppelklick auf eine Lizenz (Zeile) in der Tabelle geöffnet werden, sofern vorhanden.

Alle durch mdm verwalteten Lizenzen werden bei jedem Upload auf den Geräten installiert.

Die Lizenzen werden automatisch den Geräten anhand der in der jeweiligen Lizenz enthaltenen Seriennummer zugewiesen, d. h. ohne eine Seriennummer in den *General settings* eines Geräts kann keine Lizenz zugewiesen werden.

7.2.4 Lizenzen erneuern

Zur Aktualisierung aller Lizenzen in mdm für ein Gerät können Sie im Kontextmenü der Geräte-Übersicht (*Device overview table*) die Option **Refresh Licenses** anklicken. Daraufhin kontaktiert mdm den Lizenzserver und holt alle für diese Gerät erworbenen Lizenzen ab. Die Lizenzen werden mit dem nächsten Konfigurations-Upload installiert. Diese Option können Sie nutzen, wenn Sie versehentlich Lizenzen in mdm gelöscht haben oder wenn Sie einen mGuard verwalten möchten, auf dem bereits Lizenzen installiert sind, die noch nicht durch mdm verwaltet werden.

7.3 Benutzer, Rollen und Berechtigungen verwalten

Die Berechtigungen zum Anmelden am mdm-Client und für die Ausführung bestimmter Operationen nach der Anmeldung werden über Benutzer und Rollen kontrolliert. Ein Benutzer entspricht einer Person, die sich am mdm-Client anmeldet. Jedem Benutzer sind eine oder mehrere Rollen zugewiesen und mit jeder Rolle sind bestimmte Berechtigungen verbunden. Die Gesamtheit aller mit den Rollen eines Benutzers verbundenen Berechtigungen bestimmt, welche Berechtigungen ihm gewährt werden.

Die Berechtigungen werden mit der Anmeldung des Benutzers gewährt und bleiben bis zur Abmeldung dieses Benutzers in Kraft. Daher wirken sich jedwede Änderungen an der Konfiguration von Benutzern, Rollen und Rechten nicht unmittelbar auf angemeldete Benutzer aus.

Verwaltung von Benutzern und Rollen

Die Verwaltung von Benutzern, Rollen und Berechtigungen erfolgt im Users and Roles Dialog, der über **Extras » Manage Users and Roles** geöffnet wird:

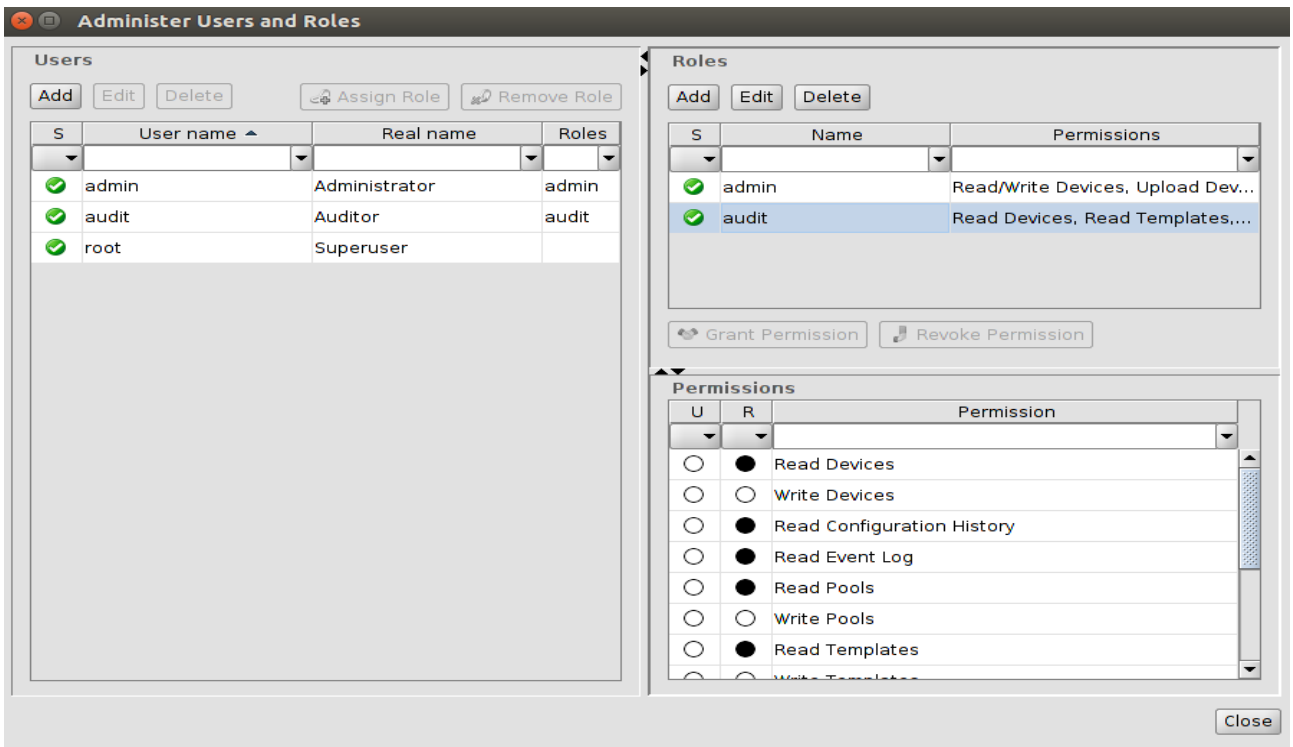


Bild 7-3 Der Dialog Users and roles

Der Dialog besteht aus den Bereichen Users, Roles und Permissions.

Der Bereich Users wird nicht angezeigt, wenn die RADIUS Authentifizierung verwendet wird, nähere Informationen finden Sie in Kapitel 7.3.4. Die Schaltflächen für die Änderung von Benutzern oder Rollen werden nur angezeigt, wenn der Benutzer, der diesen Dialog öffnet, über die Berechtigungen für die Änderung von Benutzern und Rollen verfügt.

7.3.1 Benutzer verwalten

Die Benutzerverwaltung erfolgt im Dialog *Users and Roles* im Bereich *Users*. Sie können über die Schaltfläche **Add** hinzugefügt, mit der Schaltfläche **Delete** gelöscht und mit der Schaltfläche **Edit** oder mit einem Doppelklick auf den Benutzer in der Tabelle bearbeitet werden. Für das Hinzufügen oder Bearbeiten eines Benutzers müssen folgende Daten angegeben werden:

Einmal angelegt, kann ein Benutzername (*Username*) nicht mehr geändert werden (*Edit*).

- **Username**: Der Benutzername mit dem sich der Benutzer am mdm-Client anmeldet. Benutzernamen müssen eindeutig sein.
- **Real Name**: Der Klarname (Real Name) hat keine technischen Auswirkungen, soll aber die Zuordnung eines Benutzers zu einer realen Person erleichtern.
- **Passwort**: Um sich am mdm-Client anmelden zu können, muss der Benutzer das korrekte Passwort eingeben.

Benutzerrollen zuweisen

Werden einer oder mehrere Benutzer im Bereich Users und eine oder mehrere Rollen im Bereich Roles ausgewählt, können die Rollen durch Klicken auf die Schaltfläche **Assign Role** den Benutzern zugewiesen oder durch Anklicken von **Remove Role** entzogen werden. Alle ausgewählten Rollen werden allen ausgewählten Benutzern zugewiesen oder entzogen.

Der Root-Superuser

Es besteht immer ein „Superuser“ mit dem Benutzernamen Root. Obwohl ihm keine Rollen zugewiesen sind, verfügt dieser über alle Berechtigungen (d. h. er wird von mdm anders behandelt). Der Superuser kann nicht gelöscht werden und ihm können auch keine Berechtigungen entzogen werden.

Ursprüngliche Benutzer

In einer neuen mdm-Installation sind drei Benutzer vorhanden: Root, Admin und Audit. Das ursprüngliche Passwort für diese Benutzer entspricht dem jeweiligen Benutzernamen.

Root-Passwort zurücksetzen

Wenn das Passwort für den Superuser *Root* verlorengeht, kann es mit dem folgenden psql-Befehl wieder zurückgesetzt werden (durchführen wenn der mdm-Server nicht läuft)

```
UPDATE mgnt_system_users SET "password" = 'WNd6PePC4QrGiz2zeKv6bQ==' WHERE "username" = 'root';
```

7.3.2 Rollen verwalten

Die Rollenverwaltung erfolgt im Dialog Users and Roles im Bereich Roles. Sie können über die Schaltfläche **Add** hinzugefügt, mit der Schaltfläche **Delete** gelöscht und mit der Schaltfläche **Edit** oder mit einem Doppelklick auf die Rolle in der Tabelle bearbeitet werden. Jeder Rolle ist ein Name zugeordnet, der eindeutig sein muss.

Rollen Berechtigungen zuweisen

Werden eine oder mehrere Rollen im Bereich Rolles und eine oder mehrere Berechtigungen im Bereich Permissions ausgewählt, können die Permissions durch Klicken auf die Schaltfläche **Grand Permission** den Rollen zugewiesen oder durch Anklicken von **Revoke Permission** entzogen werden. Alle ausgewählten Berechtigungen werden allen ausgewählten Rollen zugewiesen oder entzogen.

Ursprüngliche Rollen

In einer neuen mdm-Installation sind zwei Rollen vorhanden: Admin und Audit. Die Rolle Admin verfügt über alle Berechtigungen mit Ausnahme der Änderung von Benutzern und Rollen. Die Rolle Audit verfügt über Leseberechtigung, kann aber keine Änderungen vornehmen.

7.3.3 Berechtigungen

Im Dialog Users and Roles sind in der Tabelle Permissions im Bereich Permissions alle verfügbaren Berechtigungen aufgeführt. Mit den Berechtigungen können folgende Aktionen durchgeführt werden:

Berechtigung	Mögliche Aktionen
Read Devices	Liste der Geräte, Gerätekonfigurationen, Gerätelizenzen und Voucher ansehen.
Write Devices	Gerätekonfigurationen bearbeiten, hinzufügen, entfernen oder kopieren, Gerätelizenzen hinzufügen oder entfernen, Lizenz-Voucher hinzufügen. Wenn ein Benutzer über die Berechtigung Read Configuration History zusätzlich zu dieser Berechtigung verfügt: Geräte aus Einträgen im Geräte-Konfigurationsverlauf wiederherstellen.
Upload Device Configuration	Upload von Konfiguration in Geräte oder Export von Pull-Konfigurations-Dateien einleiten.
Read Configuration History	Einträge im Verlauf der Gerätekonfiguration ansehen und vergleichen. Wenn ein Benutzer über die Berechtigung Write Devices zusätzlich zu dieser Berechtigung verfügt: Geräte aus Einträgen im Geräte-Konfigurationsverlauf wiederherstellen.
Read Templates	Liste der Templates und Template-Konfigurationen ansehen.
Write Templates	Template-Konfigurationen bearbeiten, hinzufügen, entfernen oder kopieren.
Read Pools	Liste der Pools und Pool-Konfigurationen ansehen.
Write Pools	Pool-Konfigurationen bearbeiten, hinzufügen, entfernen oder kopieren.
Read VPN Groups	Liste der VPN-Gruppen und VPN-Gruppen-Konfigurationen ansehen.
Write VPN Groups	VPN-Gruppen-Konfigurationen bearbeiten, hinzufügen, entfernen oder kopieren.
Read Users and Roles	Benutzer, Rollen und Berechtigungen ansehen.
Write Users and Roles	Benutzer, Rollen und Berechtigungen verwalten (einschließlich der Berechtigung zum Einrichten von Passwörtern für andere Benutzer).
Read Event Log	Aktuelles Ereignisprotokoll ansehen.

Mindest-Berechtigungssatz

Die Berechtigungen Read Devices, Read Templates, Read Pools und Read VPN Groups bilden den Mindest-Berechtigungssatz. Diese Berechtigungen können einer Rolle nicht entzogen werden.

Berechtigungstabelle filtern und sortieren

In den Spalten U und R wird angezeigt, über welche Berechtigungen die aktuell ausgewählten Benutzer und Rollen verfügen. Sie können zum Filtern der Berechtigungstabelle genutzt werden.

In der Spalte U können folgende Symbole angezeigt werden:

○ Keiner der ausgewählten Benutzer verfügt über diese Berechtigung.

◐ Einige (aber nicht alle) der ausgewählten Benutzer verfügen über diese Berechtigung.

● Alle ausgewählten Benutzer verfügen über diese Berechtigung.

Die gleichen Symbole werden in der Spalte R verwendet, um die Zuweisung einer Berechtigung zu keiner, einigen oder allen der ausgewählten Rollen anzuzeigen.

7.3.4 Authentifizierung des Benutzers

Zur Authentifizierung von Benutzern, die sich am mdm-Client anmelden, unterstützt mdm zwei Mechanismen: die mdm Datenbank und RADIUS.

mdm Datenbank-Authentifizierung

Die Authentifizierung anhand der mdm Datenbank stellt den Standardmechanismus dar. Hier werden für die Authentifizierung der Benutzer die in der mdm Datenbank gespeicherten und im Users and Roles Dialog im Bereich Users konfigurierten Benutzernamen und Passwörter verwendet. Weiterführende Informationen finden Sie in Kapitel 7.3.1.

RADIUS-Authentifizierung

Remote Authentication Dial In User Service (RADIUS) ist ein Netzwerkprotokoll, dass eine Fernauthentifizierung ermöglicht. Wenn der mdm-Server für die Verwendung der RADIUS-Authentifizierung konfiguriert ist, werden die in der mdm Datenbank gespeicherten Benutzer nicht berücksichtigt. Will sich ein Besucher am mdm-Client anmelden, sendet der mdm-Server zur Authentifizierung des Benutzers eine Anfrage an einen oder mehrere RADIUS-Server. Die RADIUS-Antwort muss eines oder mehrere Filter-ID-Attribute enthalten, die der mdm-Server als Rollenbezeichnungen interpretiert. Wenn der Anmeldeversuch erfolgreich ist, wird der Benutzer einer der in den Filter-ID-Attributen angegebenen Rollen zugewiesen.

Bei Verwendung der RADIUS-Authentifizierung wird das Konzept Superuser von mdm nicht genutzt. Der Benutzername Root wird nicht besonders behandelt.

Weitere Informationen zur Konfiguration des mdm-Servers für die RADIUS-Authentifizierung finden Sie in Kapitel 10.1.

7.4 X.509-Zertifikate verwalten

Die Funktionalität der Zertitifkatverwaltung ist vom Release des mGuard abhängig. Ab mGuard Firmware 5.0 bestehen folgende Möglichkeiten:

- Verwaltung mehrerer Maschinenzertifikate (vor Version 5.0 wurde nur ein Maschinenzertifikat unterstützt)
- Verwaltung von CA-Zertifikaten (vor Version 5.0 wurden CA-Zertifikate nicht unterstützt)
- Verwaltung von Verbindungszertifikaten an einem zentralen Standort (vor Version 5.0 war das Verbindungszertifikat nur ein Teil der VPN-Verbindung; ab 5.0 können die Verbindungszertifikate zentral verwaltet und anschließend zur SSH- oder HTTPS-Authentifizierung referenziert werden)
- Verwaltung von CRLs (vor Version 5.0 wurden CA-CRLs nicht unterstützt)

Zertifikate exportieren

Zertifikate können exportiert werden, beispielsweise wenn Sie das Maschinenzertifikat als Verbindungszertifikat für eine VPN-Verbindung verwenden möchten. Navigieren Sie zum Export eines Zertifikats zur entsprechenden Zertifikatetabelle (weitere Informationen siehe unten) und klicken Sie auf die Schaltfläche **Export**. Sie können das Zertifikat in ein Verzeichnis Ihrer Wahl exportieren.

7.4.1 Maschinenzertifikate

Sie können ein Maschinenzertifikat (Datei PEM oder PKCS#2) importieren, ein Zertifikat der mdm CA anfordern, ein Zertifikat von einer beliebigen CA anfordern, die das Simple Certificate Enrollment Protocol (SCEP) unterstützt, oder Zertifikate manuell einsetzen.

In einem Template kann ein Maschinenzertifikat nicht angefordert oder importiert werden. (Es ist nur möglich, das Verbindungszertifikat der Gegenstelle zu importieren).

Importiert werden können Dateien im PEM-Format mit nicht kodiertem privatem Schlüssel und dem Zertifikat oder im Format PKCS#12 mit Passwort (die PKCS#12-Datei kann nur das Maschinenzertifikat enthalten, kein zusätzliches CA-Zertifikat). Der Dateityp wird automatisch erkannt. Beim Import einer PKCS#12-Datei wird ein Dialog mit Aufforderung zur Passworteingabe angezeigt.
Mit dem folgenden Befehl kann eine Datei von PKCS#12 in PEM umgewandelt werden:
`openssl pkcs12 -in` *inputfile.p12* `-nodes -out` *outputfile.pem* .

Bei Verwendung von SCEP muss der CA-Server zur sofortigen Ausgabe von Zertifikaten konfiguriert sein. Ausstehende Anfragen werden nicht unterstützt.

Maschinenzertifikat anfordern

Achten Sie vor dem Anfordern eines Zertifikats darauf, dass in den Feldern der Zertifikatattribute die richtigen Werte eingetragen sind (navigieren Sie für mGuard Firmware zu **IPsec VPN » Global » Machine certificate » Certificate attributes**, ab mGuard Firmware 5.0 zu **Authentication » Certificates » Certificate settings** und **Certificate attributes**).

Um von der mdm CA ein Zertifikat anfordern zu können, muss die CA-Komponente installiert sein (siehe „mdm-Server (Datei *preferences.xml)“ auf Seite 161*).

Markieren Sie zum Anfordern eines Zertifikats in der Geräte-Übersicht (*Device overview table*) eines oder mehrere Geräte und klicken Sie im Kontextmenü auf **Certificate Handling » Request Additional Certificate** oder **Certificate Handling » Request Replacement Certificate**. Der Unterschied besteht darin, dass bei **Request Additional Certifi-**

cate der Liste der vorhandenen Zertifikate ein neues Zertifikat hinzugefügt wird, während mit **Request Replacement Certificate** das vorhandene Zertifikat durch ein neues ersetzt wird, sodass das Gerät am Ende über ein einzelnes Maschinenzertifikat verfügt.

Der mdm-Server fordert Zertifikate von der CA an und weist sie den Geräten zu.

SCEP fordert für jede Zertifikatanfrage zur Eingabe eines Challenge-Passworts auf. Zertifikatanfragen können daher bei Verwendung von SCEP nur einmal durchgeführt werden. Der mdm-Client öffnet ein Dialogfenster für die Eingabe des Challenge-Passworts; Informationen zum Abholen des Passworts finden Sie in der Dokumentation Ihres CA-Servers.

OCSP und CRLs werden von mGuard nicht unterstützt. Wenn Sie dennoch Firmwareversionen nach mit CRL/OCSP-Unterstützung verwenden möchten, sollten Sie Werte für diese Attribute konfigurieren.

Maschinenzertifikat importieren (mGuard Firmware)

Navigieren Sie zum Import eines Zertifikats zu **IPsecVPN » Global » Machine certificate » Machine certificates** und klicken Sie auf **Import** (die Schaltfläche **Import** ist nur aktiviert, wenn **Custom** oder **Custom+Locally appendable** als Werte für die Tabelle der Maschinenzertifikate ausgewählt sind). Markieren Sie eine Datei mit Maschinenzertifikat und klicken Sie auf **Open**. Bei erfolgreichem Import wird das Maschinenzertifikat daraufhin in der Tabelle angezeigt; andernfalls erscheint eine Fehlermeldung.

Nur der erste Eintrag der Tabelle der Maschinenzertifikate wird als Maschinenzertifikat verwendet.

Maschinenzertifikat importieren (mGuard Firmware ab 5.0)

Navigieren Sie zum Import eines Zertifikats zu **Authentication » Certificates » Machine Certificates** und klicken Sie auf **Import** (die Schaltfläche **Import** ist nur aktiviert, wenn **Custom** oder **Custom+Locally appendable** als Werte für die Tabelle der Maschinenzertifikate ausgewählt sind). Markieren Sie eine Datei mit Maschinenzertifikat und klicken Sie auf **Open**. Bei erfolgreichem Import wird das Maschinenzertifikat daraufhin in der Tabelle angezeigt; andernfalls erscheint eine Fehlermeldung.

Maschinenzertifikate löschen

Navigieren Sie zum Löschen eines Zertifikats zu **Authentication » Certificates » Machine Certificates,** markieren Sie das Zertifikat in der Tabelle und klicken Sie auf die Schaltfläche **Delete certificate**.

Ein Zertifikat wird durch Löschen nicht automatisch widerrufen.

Maschinenzertifikate widerrufen

Navigieren Sie zum Wiederrufen eines Zertifikats zu **Authentication » Certificates » Machine Certificates,** markieren Sie das Zertifikat in der Tabelle und klicken Sie auf die Schaltfläche **Revoke certificate**. Diese Schaltfläche ist nur aktiv, wenn genau ein Maschinenzertifikat markiert ist. Nach dem Widerrufen eines Zertifikats wird automatisch der Text **** REVOKED **** im entsprechenden Feld in der Tabelle angezeigt. Bei jedem Widerruf eines Zertifikats exportiert die mdm CA eine neue Datei, die alle widerrufenen Zertifikate dieses Ausstellers enthält.

Für mehr Informationen zum Export der CRL-Dateien kontaktieren Sie bitte Phoenix Contact (phoenixcontact.com).

SCEP unterstützt das Widerrufen von Zertifikaten nicht.

CRLs werden erst ab mGuard Firmware 5.0 unterstützt.

Durch das Widerrufen eines Zertifikats wird es nicht aus der Tabelle gelöscht.

Zertifikate manuell registrieren

Für die Verwendung von Zertifikaten, die von einer CA ausgegeben wurden, aber nicht online (von der CA des mdm oder über SCEP) angefordert werden können, unterstützt mdm die manuelle Registrierung von Zertifikaten. Jede CA-Software oder Service kann verwendet werden. Gehen Sie zur manuellen Registrierung von Zertifikaten für mehrere Geräte wie folgt vor:

1. Markieren Sie in der Geräte-Übersicht (*Device overview table*) eines oder mehrere Geräte und klicken Sie im Kontextmenü auf **Certificate Handling » Issue and Export Certificate Requests**.
2. Ein Dialog zur Dateiauswahl wird geöffnet. Wählen Sie ein Verzeichnis aus und klicken Sie auf die Schaltfläche **Choose**.
3. mdm erstellt für die Geräte private Schlüssel und Zertifikatanforderungen. Die privaten Schlüssel sind (unsichtbar) mit den entsprechenden Geräten verbunden. Die Zertifikatanforderungen werden im ausgewählten Verzeichnis als PEM-verschlüsselte Dateien gespeichert (eine Anfrage pro Gerät).
4. Importieren Sie die Zertifikatanfragen in die CA und lassen Sie die CA die Zertifikate ausgeben. Weitere Informationen dazu finden Sie in der Dokumentation Ihrer CA-Software oder Service.
5. Klicken Sie im Hauptmenü auf New **»** Import X.509 Certificates.
6. Ein Dialog zur Dateiauswahl wird geöffnet. Markieren Sie die von der CA ausgegebenen Zertifikate.
7. Wählen Sie in den Import Settings aus, ob Sie Zertifikate hinzufügen oder in einem Gerät möglicherweise bereits vorhandene Zertifikate ersetzen möchten. Klicken Sie auf die Schaltfläche **Choose**.
8. mdm weist Zertifikate automatisch den richtigen Geräten zu und speichert diese in den Tabellen der Maschinenzertifikate.

Pro Gerät wird nur ein ausstehendes Zertifikat gespeichert. Wird das Certificate Handling **» Issue and Export Certificate Requests action** mehr als einmal aufgerufen, ohne dass die entsprechenden Zertifikate importiert werden, können nur die Zertifikate aus dem letzten Aufruf importiert werden.

7.4.2 CA-Zertifikate (mGuard ab Firmware 5.0)

CA-Zertifikate importieren

Ab mGuard Version 5.0 werden CA-Zertifikate (Root oder Intermediate) unterstützt. Navigieren Sie zum Import eines CA-Zertifikats zu **Authentication » Certificates » CA Certificates** und klicken Sie auf **Import** (die Schaltfläche **Import** ist nur aktiviert, wenn **Custom** oder **Custom+Locally appendable** als Werte für die Tabelle der CA-Zertifikate ausgewählt sind). Markieren Sie eine Datei mit CA-Zertifikat und klicken Sie auf **Open**. Bei erfolgreichem Import wird das CA-Zertifikat daraufhin in der Tabelle angezeigt; andernfalls erscheint eine Fehlermeldung.

7.4.3 Gegenstellenzertifikate (mGuard ab Firmware 5.0)

Gegenstellenzertifikate importieren

Navigieren Sie zum Import eines Gegenstellenzertifikats zu **Authentication » Certificates » Remote Certificates** und klicken Sie auf **Import** (die Schaltfläche **Import** ist nur aktiviert, wenn **Custom** oder **Custom+Locally appendable** als Werte für die Tabelle der Gegenstellenzertifikate ausgewählt sind). Markieren Sie eine Datei mit Gegenstellenzertifikat und klicken Sie auf **Open**. Bei erfolgreichem Import wird das Gegenstellenzertifikat daraufhin in der Tabelle angezeigt; andernfalls erscheint eine Fehlermeldung.

7.4.4 Verbindungszertifikate

Verbindungszertifikate importieren

Das Verbindungszertifikat kann nur in einer VPN-Verbindung importiert werden. Navigieren Sie zum Import des Zertifikats zu **IPsec VPN » Connections »** *Connection Name* **» Authentication.** Wählen Sie zum Import eines Zertifikats den Wert **Custom** für das **Remote X.509 certificate** aus und klicken Sie auf das Symbol  . Markieren Sie eine Datei mit Zertifikat und klicken Sie auf **Open**. Der Inhalt der Datei wird daraufhin im Zertifikat-Feld angezeigt. Die Gültigkeit der Daten wird bim Hochladen der Konfiguration in den mGuard überprüft.

7.5 X.509-Zertifikate verwenden (mGuard ab Firmware 5.0)

Die Zertifikate, die in den in Kapitel 7.4 beschriebenen Tabellen verwaltet werden, können für die Konfiguration von SSH- und HTTPS-Authentifizierung verwendet werden. Die Verwendung wird am Beispiel der SSH-Authentifizierung beschrieben. Navigieren Sie im *Device properties dialog* (Geräte-Eigenschaften) zu **Management » System settings » Shell access » X.509 authentication**. Wählen Sie zur Verwendung eines Zertifikats, beispielsweise eines CA-Zertifikats, für die Tabelle der CA-Zertifikate **Custom** aus und klicken Sie auf **Add certificate**. Geben Sie den *short name* des Zertifikats wie in der Tabelle CA-Zertifikate angegeben in **Authentication » Certificates » CA Certificates** ein. mdm prüft nicht nach, ob der *short name* des Zertifikats existiert.

7.6 Firmware-Upgrades mit mdm verwalten

mdm unterstützt die Verwaltung der Firmware Ihres mGuards. Die Firmware selbst wird nicht von mdm auf das Gerät geladen. mdm weist das Gerät beim Hochladen der Konfiguration an, das Upgrade-Paket der Firmware von einem Upgrade-Server herunterzuladen und zu übernehmen.

Voraussetzungen

- Ein Upgrade-Server muss eingerichtet sein und die benötigten Upgrade-Pakete müssen sich auf diesem Server befinden. Die Geräte (nicht zwingend mdm) benötigen Zugriff auf den Upgrade-Server.
- Der Server muss in der Gerätekonfiguration (oder in der Template-Konfiguration) konfiguriert sein. Navigieren Sie zum Hinzufügen Ihres Upgrade-Servers zur Konfiguration im *Properties Dialog* bei Geräten mit Version zu **Management » Firmware upgrade » Upgrade servers** und bei Geräten ab Version 5.0 zu **Management » Update » Firmware upgrade » Upgrade servers**.
- Achten Sie bei Verwendung des automatischen Firmware-Upgrades (siehe nachfolgenden Abschnitt) zusammen mit einem Pull-Upload darauf, dass das Feld **Firmware Version on Device** (siehe Kapitel 6.3.3) einen gültigen Wert aufweist. Der Wert kann manuell eingegeben werden. Alternativ kann mdm nach dem ersten Push-Upload oder Pull-Konfigurations-Feedback diese Angaben automatisch eintragen. Bei manueller Eingabe muss das Feld **Firmware Version on Device** *exakt* dem String entsprechen, der im Symbol in der oberen linken Ecke der Webinterface des mGuard angezeigt wird, z. B. *6.1.0.default*.

Firmware-Upgrade planen

Ein Firmware-Upgrade kann auf zwei Arten geplant werden:

- Explizite Angabe der Ziel-Firmware
  Navigieren Sie dazu im *Device properties dialog* (Geräte-Eigenschaften) zu **Management » Firmware upgrade » Schedule firmware upgrade** bei Geräten mit Version bzw. zu **Management » Update » Firmware upgrade » Schedule firmware upgrade** bei Geräten ab Version 5.0. Geben Sie im Feld **Package set name** den Namen des Pakets ein und setzen Sie **Install package set** auf **Yes**.
- Upgrade automatisch durchführen
  Wenn Sie das Upgrade automatisch durchführen möchten, navigieren Sie im *Device properties dialog* (Geräte-Eigenschaften) zu **Management » Firmware upgrade » Schedule firmware upgrade** bei Geräten mit Version bzw. zu **Management » Update » Firmware upgrade » Schedule firmware upgrade** bei Geräten mit Version 5.0. Wählen Sie in **Automatic upgrade** eine der folgenden Optionen:
  - Install latest patches
    Mit dieser Option aktualisieren Sie Ihr Gerät auf die letzte verfügbare Patch-Version, beispielsweise von Version .1 auf .3.
  - Install latest minor release
    Mit dieser Option aktualisieren Sie Ihr Gerät auf das letzte verfügbare Minor Release, beispielsweise von Version 5.0.1 auf 5.1.0.
  - Install next major version
    Mit dieser Option aktualisieren Sie Ihr Gerät auf das nächste Major Release, beispielsweise von Version .3 auf 5.1.0.
    Achten Sie vor der Einleitung eines Major Release-Upgrades darauf, dass für die Geräte Lizenzen für das Major Release in mdm vorhanden sind (siehe Kapitel 7.2).

Alternativ können Sie im Kontextmenü der Geräte-Übersicht (*Device overview table*) ein automatisches Firmware-Upgrade für eines oder mehrere Geräte planen. Öffnen Sie in der Gerätetabelle mit einem Klick auf die rechte Maustaste das Kontextmenü und wählen sie die gewünschte Möglichkeit zum Upgrade aus.

Um das Firmware-Upgrade endgültig zu starten, muss nach Durchführung der oben beschriebenen Schritte die Konfiguration in das Gerät geladen werden.

Geplantes Firmware-Upgrade abbrechen

Mit der Option **Unschedule upgrade** im Kontextmenü der Geräte-Übersicht (*Device overview table*) können Sie ein vorgesehenes Firmware-Upgrade aus der Planung nehmen.

Upgrade-Prozess

Bei einem Upgrade ist es wichtig, dass alle Schritte in der korrekten Reihenfolge durchgeführt werden.

Angenommen, Sie möchten ein Gerät von Version .3 auf 5.1.0 aktualisieren. Die in mdm (im *Device properties dialog* (Geräte-Eigenschaften) im Feld **Firmware Version**) konfigurierte Firmwareversion entspricht der Firmwareversion des Geräts, nämlich . Dies sollte in der Geräte-Übersicht (*Device overview table*) im Feld **Version on Device** angezeigt sein (siehe Kapitel 6.3.1). Achten Sie darauf, dass alle notwendigen Voraussetzungen (siehe Abschnitt *„Voraussetzungen“* oben) erfüllt sind und beginnen Sie mit dem Hochladen der Konfiguration für das Gerät (siehe Abschnitt *„Firmware-Upgrade planen“* oben). Das erste Symbol in der Spalte **Version on Device** wechselt zu und zeigt damit an, dass für den nächsten Upload ein Firmware-Upgrade vorgesehen ist. Nach Beginn des Konfigurations-Uploads ändert sich das Symbol zu und zeigt damit an, dass am Gerät ein Firmware-Upgrade läuft (das Symbol wird nur bei einem Push-Upload angezeigt). mdm fragt das Gerät regelmäßig ab, um eine Rückmeldung zum Ergebnis des Firmware-Upgrades zu erhalten. Dieses wird schließlich in der Geräte-Übersicht (*Device overview table*) im Feld **Version on Device** und der Spalte **U** angezeigt. Da das Gerät jetzt auf Version 5.1.0 aktualisiert wurde, die mdm Konfiguration für das Gerät jedoch noch auf Version gesetzt ist, sollte im Feld **Version on Device** jetzt eine Abweichung der Firmwareversionen angezeigt werden. Daher sollten Sie die Firmwareversion im Gerät entsprechend der aktuell installierten Firmware ändern. Dies kann allerdings erst *nach*

dem Firmwareupgrade am Gerät durchgeführt werden. Sie können die Firmwareversion im Feld **Firmware version** des *Device properties dialog* (Geräte-Eigenschaften) oder im Kontextmenü der Geräte-Übersicht (*Device overview table*) ändern.

CAUTION: Unwiderrufliche Änderungen

Durch ein Upgrade der Firmwareversion des Geräts können sich die Werte der Standardvariablen in der Zielversion ändern.

Ein Downgrade zurück auf eine ältere Version ist nicht möglich. Daher ist bei einer Änderung der Firmwareversion größte Sorgfalt geboten. Weitere Informationen dazu erhalten Sie unter „Versionseinstellungen der Firmware und Vererbung“ auf Seite 84.

Prüfen Sie nach einem Upgrade alle Änderungen an den Variablen in der „Device Configuration History“ (siehe „Dialog Konfigurationsverlauf“ auf Seite 129).

ACHTUNG: Neue Standardwerte in mGuard-Firmware 8.5 und 8.6

Wird in der mGuard-Firmware ein Standardwert (*Default value*) geändert, so ist die Verwaltung dieses Wertes in mdm betroffen:

1. wenn die Firmware-Version eines verwalteten Geräts auf eine Firmwareversion mit einem geänderten Standardwert aktualisiert wird,
2. wenn ein „Kind“, das eine andere mGuard-Firmwareversion besitzt als sein Elternteil, einen Wert mit einem anderen Standardwert erbt.

Das damit verbundene Verhalten von mdm wird im Kapitel „Verhalten von geänderten Standardwerten (mGuard 8.5/8.6)“ auf Seite 43 beschrieben.

Wenn Sie ein neues Device/Template mit der mGuard**-Firmwareversion 8.5** hinzufügen möchten, setzen Sie zuerst die Standard-Firmwareversion (*Default Firmware Version*) auf mGuard 8.5. In diesem Fall erfolgt kein Geräte-Upgrade und die Standardwerte, die der mGuard-Firmwareversion 8.5 entsprechen, werden gesetzt. Der Wertetyp bleibt "*Inherited*" (siehe „mdm Hauptmenü“ auf Seite 19 --> “Default Firmware Version”).

Sie können jetzt mit der Konfiguration der mit der neuen Firmwareversion eingeführten Funktionen beginnen.

Firmware-Upgrade überwachen

Der Fortschritt und das Ergebnis des Firmware-Upgrades werden durch das Symbol in der Spalte **Version on Device** in der Geräte-Übersicht (*Device overview table*) angezeigt. Weitere Informationen finden Sie unter Kapitel 6.3.1.

7.7 Rollback-Unterstützung

Für Geräte ab Firmwareversion 5.0 wird ein Rollback der Konfiguration unterstützt. Das Gerät führt ein Rollback durch, wenn es nach Übernahme einer Pull-Konfiguration nicht auf den *Configuration-Pull-Server* zugreifen kann (diese wird vom Gerät als Fehlkonfiguration gewertet). Navigieren Sie zur Aktivierung des Rollbacks für ein Gerät im *Properties Dialog* zu **Management » Configuration Pull** und setzen Sie die Option **Rollback misconfigurations** auf **Yes**.

7.8 Redundanzmodus

Wenn sich ein Gerät oder Template im Redundanzmodus befindet, stellt es ein Paar redundanter mGuards dar (also zwei physische Geräte). Einstellungen und Konfigurationsvariablen, die für die beiden Geräte eines Redundanzpaares verschieden sein können bzw. müssen, können separat vorgenommen werden.

In den Dialogen Device Properties und Template Properties werden im Navigationsbaum zusätzliche Knoten und Variablen angezeigt. Knoten und Variablen mit dem Präfix Device#2 werden für das zweite, Knoten und Variablen ohne Präfix für das erste Gerät verwendet.

Separate Einstellungen

Folgende Einstellungen sind für die physischen Geräte separat vorhanden, werden aber normalerweise nicht durch den Benutzer vorgenommen:

- **Firmware Version on Device**
- **Pull filename**
- **Serial Number**
- **Flash-ID**

Folgende Variablen müssen für die physischen Geräte auf unterschiedliche Werte gesetzt werden:

- Externe und interne Netzwerkeinstellungen im Router-Modus.
- Die Einstellungen für Stealth management address im geschützten Modus.
- Die IP-Einstellungen für die dezidierte Schnittstelle für die Synchronisierung des Redundanz-Status (falls diese Schnittstelle verwendet wird).

Folgende Variablen können für die physischen Geräte auf unterschiedliche Werte gesetzt werden:

- Host-Name
- SNMP-Systemname, Standort und Kontakt
- MTU-Einstellungen
- HTTP(S) Proxy-Einstellungen
- Passwörter der Benutzer des mGuard
- Einstellungen für Quality-of-Service
- Redundanz-Priorität
- Einstellungen für Redundanz-Konnektivitätsprüfung
- Anmeldeeinstellungen für Fernzugriff

Upload

Wenn der Upload eines redundanten Gerätepaars eingeleitet wird, werden beide Konfigurationen in die physischen Geräte hochgeladen. Die beiden Upload-Vorgänge in die mGuards, die ein Redundanzpaar bilden, werden nie gleichzeitig durchgeführt (aber kön-

nen gleichzeitig mit Uploads auf andere Geräte durchgeführt werden). Ein Upload auf ein Redundanzpaar gilt als erfolgreich, sobald der Upload auf beide physischen Geräte erfolgreich war.

Pull-Export

Durch einen Pull-Konfigurationsexport für ein redundantes Gerätepaar werden zwei Konfigurationsprofile angelegt. Dem Dateinamen des Profils für das zweite Gerät wird eine _2 hinzugefügt.

8 Konfigurationsverlauf

mdm speichert die mGuard Gerätekonfigurationen im Konfigurationsverlauf. Bei jeder Änderungen an einem Gerät, einem Template oder einer VPN-Gruppenkonfiguration wird für jedes Gerät, das sich daraufhin ändert, ein neuer Verlaufseintrag angelegt.

Jedes Gerät verfügt über seinen eigenen unabhängigen Verlauf. Mit dem Löschen eines Geräts wird auch dessen Verlauf gelöscht.

Im Verlauf werden Konfigurationen so gespeichert, wie sie in den mGuard geladen werden. Variable Berechtigungen und Erbbeziehungen von Templates gehören nicht zum Verlauf.

8.1 Dialog Konfigurationsverlauf

Wählen Sie zum Zugriff auf einen Konfigurationsverlauf das Gerät in der Tabelle **device overview table** aus und aktivieren Sie im Kontextmenü die Option **Show Device Configuration History**. Damit wird der Dialog Konfigurationsverlauf geöffnet, der eine Liste der Verlaufseinträge für das ausgewählte Gerät enthält.

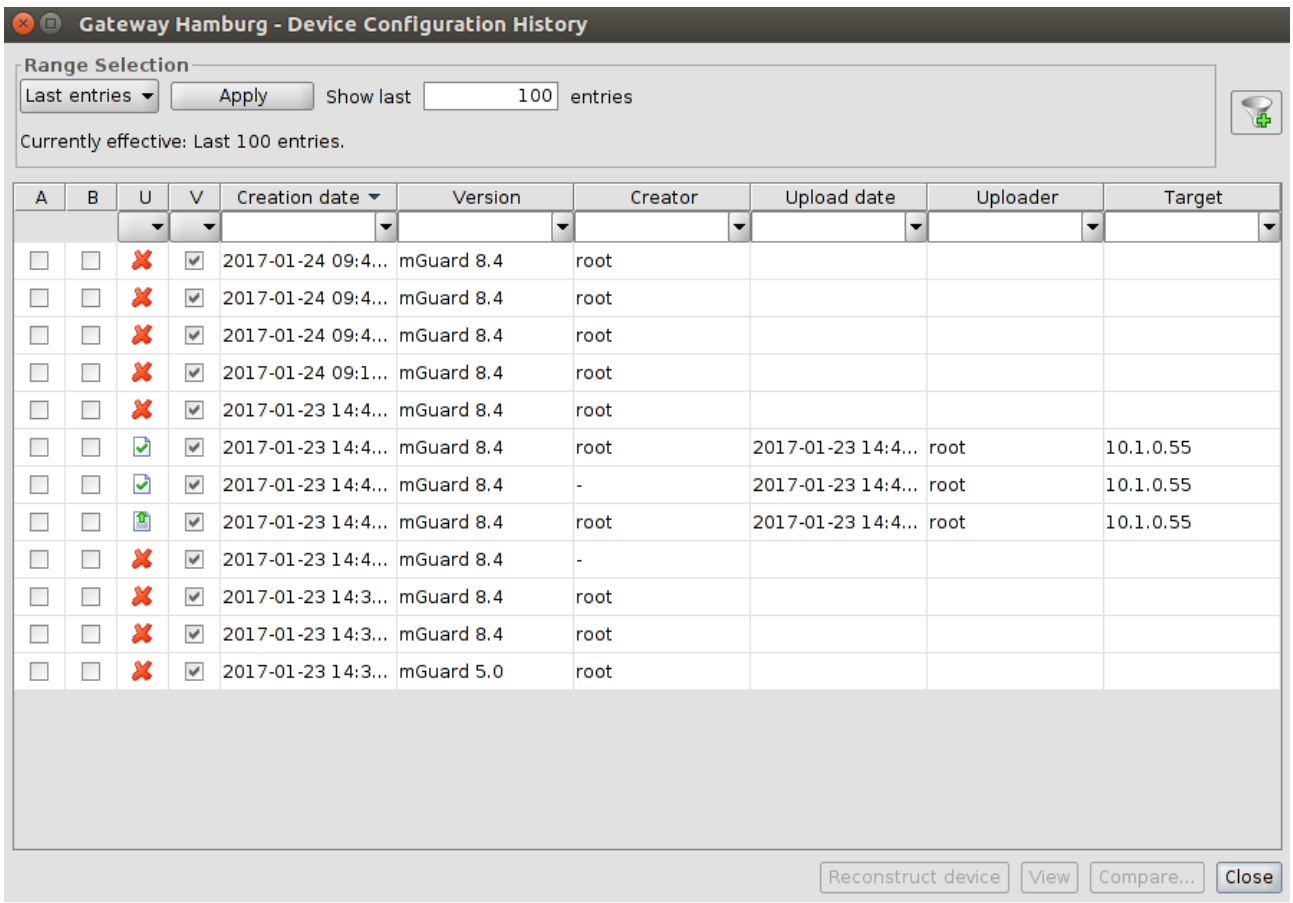


Bild 8-1 Dialog Konfigurationsverlauf

Dialog Konfigurationsverlauf	
Range selection	Da die Anzahl dauerhaft gespeicherter Verlaufseinträge für ein Gerät sehr hoch sein kann, werden beim Öffnen des Dialogfensters nicht alle Einträge automatisch vom mdm-Server geladen. Durch die Änderung der Kriterien unter „Range Selection“ und das Klicken auf „Apply“ werden die für die angegebenen Kriterien passenden Einträge geladen. Mit der Werkseinstellung werden die letzten (also aktuellsten) 100 Einträge geladen. **All Entries** — Alle mit dem Gerät verbundenen Verlaufseinträge laden. Bei einer großen Anzahl von Einträgen (1000 oder mehr) kann das Laden der Einträge einige Zeit dauern. **Time Range** — Alle Einträge laden, die in einem bestimmten Zeitraum erstellt wurden. Dieser Zeitraum wird wie folgt angegeben: – Bei Angabe eines unteren, jedoch keines oberen Grenzwertes werden alle Einträge geladen, die aktueller als der untere Grenzwert sind. – Bei Angabe eines oberen, jedoch keines unteren Grenzwertes werden alle Einträge geladen, die älter als der obere Grenzwert sind. – Werden sowohl ein unterer als auch ein oberer Grenzwert angegeben, werden alle Einträge geladen, die in dem genannten Zeitraum erstellt wurden. Datumsangaben erfolgen im ISO-Format (JJJJ-MM-TT, wobei JJJJ das Jahr, MM den Monat dieses Jahres zwischen 01 und 12 und TT den Tag dieses Monats zwischen 01 und 31 bezeichnet). Optional kann eine ISO-Zeitangabe folgen (hh:mm:ss, wobei hh die Stunde im 24-Stunden-Format, mm die Minute und ss die Sekunde bezeichnet). Viertel fünf und 20 Sekunden am Nachmittag des 22. Dezember 2010 würde beispielsweise wie folgt dargestellt: 2010-12-22 16:15:20. Alternativ können Sie durch Anklicken des Symbols ein Datum aus dem Kalender auswählen. **Last Entries** — Letzte (neueste) Einträge laden. Die Anzahl der Einträge muss angegeben werden.
Spalten der Tabelle Konfigurationsverlauf	Die Tabelle Konfigurationsverlauf enthält folgende Spalten (siehe unten). Setzen Sie zum Ändern der Spaltenbreite den Cursor in die Kopfzeile der Tabelle an die Grenze zwischen zwei Spalten und ziehen Sie bei gedrückter linker Maustaste die Grenze in die gewünschte Richtung. Setzen Sie zum Verschieben einer Spalte den Cursor in die Kopfzeile der Tabelle und ziehen Sie bei gedrückter linker Maustaste die Spalte an den gewünschten Platz.

Dialog Konfigurationsverlauf

Auswahl *A, B*

Mit den Kontrollkästchen in den Spalten ***A*** und ***B*** werden entweder einer oder zwei Verlaufseinträge „aktiviert“. Die aktivierten Verlaufseinträge werden verwendet, wenn eine Aktion durchgeführt wird; nähere Informationen finden Sie in den folgenden Abschnitten.

– Markieren Sie zur Aktivierung des entsprechenden Verlaufseintrags die Kontrollkästchen A und B in der gleichen Zeile.

Markieren Sie zur Aktivierung zweier Verlaufseinträge die Kontrollkästchen A und B in verschiedenen Zeilen.

Bei Aktivierung zweier unterschiedlicher Verlaufseinträge ist der in Spalte ***A*** markierte Eintrag immer älter als der in Spalte ***B*** markierte Eintrag. Immer wenn ein Kontrollkästchen markiert wird, entfernt mdm automatisch einige Kontrollkästchen, so dass die Reihenfolge nicht umgekehrt werden kann. Die Aktivierung zweier verschiedener Einträge geht am einfachsten vonstatten, wenn die Tabelle nach Erstelldatum sortiert wird.

Status *U*

In der Spalte ***U*** wird der Upload-Status angezeigt, wenn die mit dem Verlaufseintrag verbundene Konfiguration in einen mGuard geladen oder für eine Pull-Konfiguration exportiert wurde. Eine Liste der verfügbaren Upload-Status und deren Bedeutungen finden Sie in Kapitel 6.3.1. Ein zusätzlicher Upload-Status steht im Dialog Konfigurationsverlauf zur Verfügung:

Not uploaded

Die mit dem Verlaufseintrag verbundene Konfiguration wurde nicht in einen mGuard geladen oder für eine Pull-Konfiguration exportiert.

Wenn dieselbe Konfiguration zweimal oder häufiger hochgeladen oder exportiert wurde, wird der aktuellste Verlaufseintrag kopiert, sodass für jeden erfolgreichen oder nicht erfolgreichen Upload-Versuch ein Eintrag vorhanden ist.

Status *V*

Der Status ***V*** zeigt an, ob die mit dem Verlauf verbundene Konfiguration gültig ist. Eine Konfiguration ist ungültig, wenn ein None-Wert in einem Template nicht überschrieben wurde, sodass die Konfiguration nicht in einen mGuard hochgeladen werden kann. Weitere Informationen finden Sie unter Kapitel 6.1.

Ein Verlaufseintrag, der sich auf eine ungültige Konfiguration bezieht, kann nicht aktiviert werden.

Dialog Konfigurationsverlauf		
	Creation Date	Datum und Uhrzeit der Erstellung des Eintrags in den Konfigurationsverlauf.
	Version	Firmwareversion, die bei der Erstellung des Eintrags in den Konfigurationsverlauf im Gerät eingerichtet war.
	Creator	Der Benutzername des Benutzers, der die Änderung an einem Gerät, einem Template oder an einer VPN-Gruppe, aufgrund derer der Eintrag in den Konfigurationsverlauf angelegt wurde, durchführte.
	Upload Date	Das Datum und die Uhrzeit des Uploads der mit dem Verlaufseintrag verbundenen Konfiguration in einen mGuard oder des Exports für eine Pull-Konfiguration. Bleibt leer, wenn die Konfiguration nicht hochgeladen oder exportiert wurde.
	Uploader	Der Benutzername des Benutzers, der den Upload bzw. Export einleitete. Bleibt leer, wenn die Konfiguration nicht hochgeladen oder exportiert wurde.
	Target	– Wenn die Konfiguration hochgeladen wurde, die Adresse, zu der der Upload erfolgte. – Wenn die Konfiguration exportiert wurde, der Name der Datei, zu der der Export erfolgte. Andernfalls leer.

Tabelle filtern und sortieren

Mit der Kopfzeile der Tabelle können die Einträge sortiert werden. Durch Anklicken der Kopfzeile einer Spalte wird die (primäre) Sortierung anhand dieser Spalte aktiviert. Dies wird durch einen Pfeil in der Kopfzeile angezeigt. Durch einen zweiten Klick auf dieselbe Kopfzeile erfolgt die Sortierung in umgekehrter Reihenfolge. Durch Anklicken einer weiteren Spalte wird anhand dieser neuen Spalte sortiert, wobei die vorher aktive Spalte als zweites Kriterium für die Sortierung herangezogen wird.

In der ersten Tabellenzeile wird die Eingabe regulärer Ausdrücke akzeptiert (siehe Kapitel 11, *Regular expressions*), die zum effizienten Filtern der Tabelleneinträge verwendet werden können. Bei Spalten, die keinen Text enthalten (Spalten **U** oder **V**), kann nicht auf der Grundlage regulärer Ausdrücke gefiltert werden.

Da die Spalten **A** und **B** keine Informationen enthalten, jedoch für die Aktivierung von Verlaufseinträgen verwendet werden, können sie nicht zum Filtern oder Sortieren genutzt werden.

Detail Information

Mit einem Doppelklick auf eine Zeile im Dialog Konfigurationsverlauf wird ein Dialog mit ausführlichen Informationen über den Verlaufseintrag geöffnet. Vor allem nach dem Upload der Konfiguration werden die Meldungen vom mGuard angezeigt, die während der Übernahme der Konfiguration empfangen wurden.

8.2 Frühere Konfigurationen anzeigen

Bei Aktivierung eines einzelnen Verlaufseintrags im Dialog Konfigurationsverlauf wird die Schaltfläche **View** aktiviert. Durch Anklicken der Schaltfläche wird der Dialog History View geöffnet, der die frühere Konfiguration anzeigt.

Obwohl der Dialog History View in der Erscheinung dem Dialog Device Properties ähnelt, wird eine andere Art von Informationen angezeigt. Verlaufseinträge enthalten Konfigurationen, so wie sie in die mGuards geladen wurden, variable Berechtigungen und Erbverhältnisse bei Templates gehören nicht zum Verlauf.

Sonderwerte

Zusätzlich zu den variablen Werten (oder **Custom**, wenn Variablen nicht angezeigt werden können, z. B. Passwort-Variablen) werden zwei Sonderwerte verwendet:

- **Local** weist darauf hin, dass die Variable über keinen mdm bekannten Wert verfügt. Der Wert wird durch den Benutzer Netadmin am mGuard gesetzt.
- **Custom + Locally appendable** ist nur für Tabellenvariablen anwendbar. Der Wert zeigt an, dass der Benutzer Netadmin am mGuard über die Berechtigung zum Hinzufügen von Tabellenzeilen verfügt.

8.3 Frühere Konfigurationen vergleichen

Bei Aktivierung zweier Verlaufseinträge im Dialog Konfigurationsverlauf wird die Schaltfläche **Compare** aktiviert. Durch Anklicken der Schaltfläche wird der Dialog History Comparison geöffnet, der einen Vergleich zweier früherer Konfiguration anzeigt.

Obwohl der *Dialog History Comparison* in der Erscheinung dem *Dialog Device Properties* ähnelt, wird eine andere Art von Informationen angezeigt. Verlaufseinträge enthalten Konfigurationen, so wie sie in die mGuards geladen wurden, variable Berechtigungen und Erbverhältnisse bei Templates gehören nicht zum Verlauf

Navigationsbaum

Wann und wie sich die ältere und die aktuellere Konfiguration unterscheiden, wird durch unterschiedliche Symbole und Farben im Navigationsbaum angezeigt:

-  Unverändert (schwarze Markierung)
  Die ältere und die aktuellere Konfiguration sind im Teilbaum unter dem Knoten identisch.
-  Geändert (blaue Kennzeichnung)
  Im Teilbaum unter dem Knoten wurden Variablen zwischen der älteren und der aktuelleren Konfiguration geändert.
-  Hinzugefügt (grüne Kennzeichnung)
  Der Teilbaum wurde hinzugefügt, d. h. er ist in der aktuelleren, jedoch nicht in der älteren Konfiguration vorhanden.
-  Entfernt (rote Kennzeichnung)
  Der Teilbaum wurde entfernt, d. h. er ist in der älteren, jedoch nicht in der aktuelleren Konfiguration vorhanden.

Konfigurationsvariablen

Bei der Änderung einer Variablen von der älteren zur aktuelleren Konfiguration wird ihr Einzelwert angezeigt. Andernfalls wird bei der Änderung einer einfachen Variablen deren alter Wert über dem neuen Wert angezeigt. Wenn der Wert einer Variablen nicht ange-

zeigt werden kann (z. B. Passwortvariablen), wird stattdessen der Text Custom verwendet.

Wird der Einzelwert Custom für eine Passwortvariable angezeigt, weist dies darauf hin, dass sich das Passwort nicht geändert hat. Wird jedoch der Wert Custom zweimal angezeigt, hat sich das Passwort von der älteren zur neueren Konfiguration geändert.

Eine Änderung einer Tabellenvariable wird durch die Hintergrundfarbe der geänderten Zeile(n) und durch ein Zeichen in der Spalte „+/-“ angezeigt:

– Indikator „+“/grüner Hintergrund
  Die Zeile wurde eingefügt, d. h. sie ist in der aktuelleren, jedoch nicht in der älteren Konfiguration vorhanden.
– Indikator „+“/roter Hintergrund
  Die Zeile wurde gelöscht, d. h. sie ist in der älteren, jedoch nicht in der aktuelleren Konfiguration vorhanden.
– Indikator „M“/blauer Hintergrund
  Die Zeile wurde von der älteren zur aktuelleren Konfiguration verändert. Dieser Indikator wird nur für komplexe Tabellenvariablen verwendet (d. h. VPN-Verbindung), andernfalls wird eine geänderte Zeile wie eine gelöschte Zeile behandelt, wobei auf die älteren Inhalte eine eingefügte Zeile mit neuen Inhalten folgt.

Sonderwerte

Zusätzlich zu den Variablenwerten oder Custom werden zwei Sonderwerte verwendet:

– **Local** weist darauf hin, dass die Variable über keinen mdm bekannten Wert verfügt. Der Wert wird durch den Benutzer Netadmin am mGuard gesetzt.
– **Custom + Locally appendable** ist nur für Tabellenvariablen anwendbar. Der Wert zeigt an, dass der Benutzer Netadmin am mGuard über die Berechtigung zum Hinzufügen von Tabellenzeilen verfügt.

8.4 Ein Gerät aus einer früheren Konfiguration wiederherstellen

Bei Aktivierung eines einzelnen Verlaufseintrags im Dialog Konfigurationsverlauf durch Aktivieren der Kontrollkästchen in den Spalten A und B wird die Schaltfläche **Reconstruct Device** aktiviert. Durch das Anklicken dieser Schaltfläche wird ein neues Gerät erstellt, in dem alle Variablen entsprechend der früheren Konfiguration gesetzt sind, und der Dialog Device Properties für das wiederhergestellte Gerät wird geöffnet.

Sobald das neue Gerät erstellt ist, besteht keine Verbindung mehr zu dem Gerät, aus dem es wiederhergestellt wurde. Es ist ein unabhängiges Gerät mit einem unabhängigen Geräteverlauf.

Template zuweisen

Wurde das Gerät beim Anlegen eines Verlaufseintrags einem Template zugewiesen und ist dieses Template noch vorhanden und ist die Firmwareversion des Geräts bei Anlegen des Verlaufseintrags gleich oder neuer als die aktuelle Firmwareversion des Templates, dann kann das Template dem wiederhergestellten Gerät zugewiesen werden:

Bei Zuweisung des Templates zum Gerät werden die Variablen im Gerät auf Inherited gesetzt, sofern deren Wert (in der früheren Konfiguration) dem Wert im Template (in seinem aktuellen Zustand) entspricht.

Verwendet das Template die Berechtigung No override oder May append, kann die frühere Konfiguration möglicherweise nicht mehr exakt wiederhergestellt werden.

8.5 Änderungsbericht

Mit dem Änderungsbericht kann eine Übersicht erstellt werden, die über die Änderungen an mehreren Geräten zwischen zwei Zeitpunkten informiert. Wählen Sie in der Tabelle **device overview table** eines oder mehrere Geräte aus und aktivieren Sie im Kontextmenü die Option **Report of Changes to Device Configuration History**. Daraufhin wird der Dialog History Reporting geöffnet.

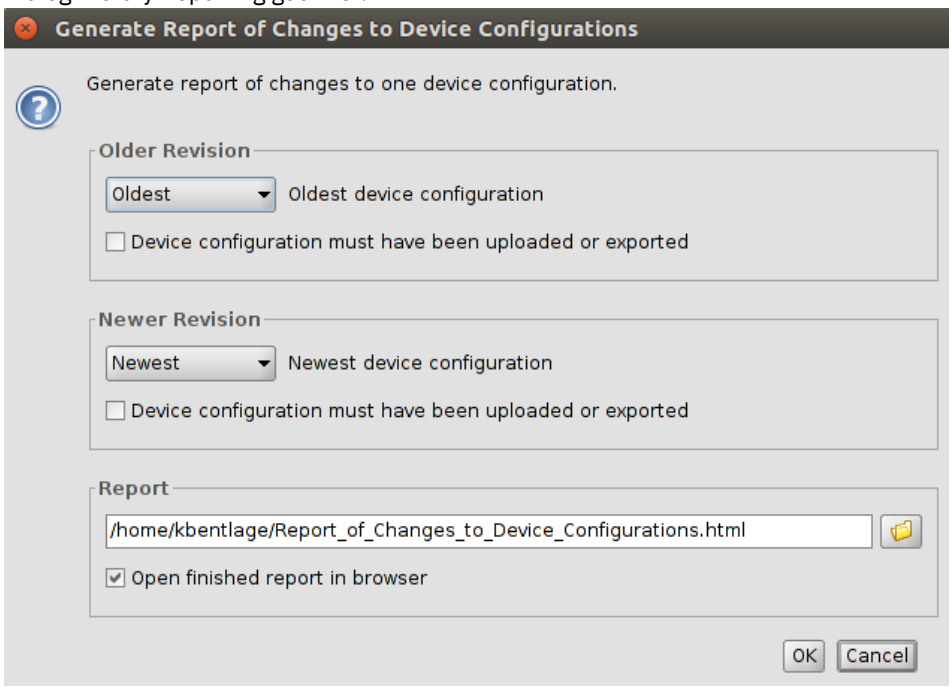


Bild 8-2 Dialog zum Erstellen eines Berichts zu Änderungen an Gerätekonfigurationen

Auswahlkriterien

Zur Auswahl der beiden zu vergleichenden früheren Konfigurationen werden zwei Auswahlkriterien, eines zur Auswahl der älteren Version und eines für die neuere Version, einzeln auf jedes ausgewählte Gerät angewandt. Folgende Kriterien stehen zur Auswahl:

Oldest

Die älteste Gerätekonfiguration.

Newest

Die neueste Gerätekonfiguration.

Newest Before

Die neueste Gerätekonfiguration vor einem bestimmten Zeitpunkt. Datum und Uhrzeit werden im ISO-Format angegeben (JJJJ-MM-TT, wobei JJJJ das Jahr, MM den Monat dieses Jahres zwischen 01 und 12 und TT den Tag dieses Monats zwischen 01 und 31 bezeichnet). Optional kann eine ISO-Zeitangabe folgen (hh:mm:ss, wobei hh die Stunde im 24-Stunden-Format, mm die Minute und ss die Sekunde bezeichnet). Viertel fünf und 20 Sekunden am Nachmittag des 22. Dezember 2010 würde beispielsweise wie folgt dargestellt: 2010-12-22 16:15:20.

Alternativ können Sie durch Anklicken des Symbols  ein Datum aus dem Kalender auswählen.

Device configuration must have been uploaded or exported

Das Kriterium kann mit den anderen kombiniert werden. Wird das Kontrollkästchen angeklickt, werden nur die Verlaufseinträge berücksichtigt, die sich auf Konfigurationen beziehen, welche auf einen mGuard hochgeladen oder zur Pull-Konfiguration exportiert wurden.

Bericht erstellen

Der Bericht besteht aus einer HTML-Datei, die mit jedem beliebigen Internetbrowser geöffnet werden kann. Der Name der Datei, in die der Bericht geschrieben werden soll, wird im Feld Report angegeben. Wenn das Kontrollkästchen Open finished Report in Browser aktiviert ist, öffnet mdm automatisch einen Internetbrowser und lädt den Report.

9 Zertifikate erstellen und verwalten

Es wird davon ausgegangen, dass der Leser über umfassende Kenntnisse über Zertifikate und Zertifikatserstellung sowie Verschlüsselung öffentlicher Schlüssel verfügt.

Erstellen Sie nur Zertifikate, wenn Sie die Zertifikatserstellung sicher beherrschen.

In diesem Kapitel wird die Erstellung von Zertifikaten mit *OpenSSL* beschrieben.

Wichtiger Hinweis: mdm erfordert zwei verschiedene Arten von Zertifikaten und Schlüsseln:

– Zertifikate und Schlüssel zur Sicherung der Kommunikation zwischen mdm Komponenten
– Zertifikate und Schlüssel für die PKI

Die Erstellung von Zertifikaten und Schlüsseln für die SSL-Kommunikation wird in Kapitel 9.1 beschrieben. Die in einer PKI verwendeten Zertifikate und Schlüssel werden in Kapitel 9.2 beschrieben.

Der in diesem Abschnitt beschriebene Prozess zur Erstellung von Zertifikaten stellt lediglich ein Beispiel für die Verwendung von OpenSSL dar. Sie können Ihre Zertifikate auch auf andere Art erstellen. Wenn Sie mit *OpenSSL* nicht vertraut sind, sollten sie die nachfolgende Anleitung *genau* befolgen.

Aus Sicherheitsgründen wird grundsätzlich die die Verwendung aktueller OpenSSL-Versionen ab Version 3 empfohlen.

Schlüsselspeicher

Zertifikate und Schlüssel werden in speziellen Datenbanken gespeichert, den sogenannten Schlüsselspeichern. Ein Schlüsselspeicher ist eine Datei, die kodierte Zertifikate und Schlüssel enthält. Für den Zugriff auf die Informationen in einem Schlüsselspeicher ist ein Passphrase erforderlich. Schlüsselspeicher können verschiedene Formate aufweisen, üblich sind beispielsweise PKCS#12 oder das proprietäre Format Java KeyStore (JKS). Der Kodierungsalgorithmus kann normalerweise beim Anlegen des Schlüsselspeichers ausgewählt werden. Empfohlen wird AES256.

Die *OpenSSL*-Konfigurationsdatei

OpenSSL verwendet Standardwerte, die in der Konfigurationsdatei *openssl.cnf* angegeben sind (in welchem Verzeichnis sich diese Datei befindet, hängt von Ihrer Verteilung ab, prüfen Sie beispielsweise das Verzeichnis */usr/ssl* oder */usr/lib/ssl*).

Wenn Sie obligatorische Argumente eines Befehls auslassen, verwendet OpenSSL die in der Konfigurationsdatei definierten Standardeinstellungen. Nach Möglichkeit sind alle obligatorischen Argumente in den nachfolgenden Beispielbefehlen explizit angegeben, wenn Sie beispielsweise die Befehle wie nachfolgend beschrieben verwenden, werden die wichtigen Informationen der Kommandozeile und nicht der Konfigurationsdatei entnommen. Wenn die Konfigurationsdatei für den jeweiligen Befehl benötigt wird, ist dies im Text ausdrücklich angeführt.

Weitere Informationen über Syntax und Inhalt der Konfigurationsdateien finden Sie in der Dokumentation von OpenSSL, vor allem im Handbuch auf den Seiten genrsa(1ssl), req(1ssl), ca(1ssl) und openssl(1ssl).

9.1 Zertifikate und Schlüssel für SSL

Für die Einrichtung einer sicheren Verbindung zwischen Entitäten (z. B. ET1, ET2) werden normalerweise folgende Komponenten benötigt:

- ein privater Schlüssel für jede an der Kommunikation beteiligte Entität:
  - $ET1_{key}$
  - $ET2_{key}$

  Der Begriff *privater Schlüssel* weist bereits darauf hin, dass diese Schlüssel vertraulich behandelt und an einem Ort abgelegt werden sollten, auf den nur der Administrator zugreifen kann.
- und die entsprechenden Zertifikate:
  - $ET1_{cert}$
  - $ET2_{cert}$

  Die Zertifikate enthalten unter anderem folgende Informationen
  - den öffentlichen Schlüssel der Entität
  - Informationen über die Entität, beispielsweise Name und/oder IP-Adresse
  - weitere Informationen zum Zertifikat, z. B. beabsichtigte Verwendung

  Das Zertifikat ist digital entweder mit dem privaten Schlüssel der jeweiligen Entität (selbstsigniert) oder mit einem CA-Schlüssel signiert.

  Die Zertifikate sind öffentlich und können durch jeden Teilnehmer an der Kommunikation verteilt werden.

ET1 verwendet den in $ET2_{cert}$ enthaltenen öffentlichen Schlüssel, um die an ET2 übermittelten Daten zu verschlüsseln. Damit ist gewährleistet, dass nur ET2 die Daten entschlüsseln kann. Wenn $ET2_{cert}$ selbstsigniert ist, dann ist gewährleistet, dass der in $ET2_{cert}$ enthaltene öffentliche Schlüssel $ET2_{key}$ entspricht. Wird $ET2_{cert}$ durch eine CA signiert, dann ist gewährleistet, dass der in $ET2_{cert}$ enthaltene öffentliche Schlüssel tatsächlich zu ET2 gehört (Authentifizierung).

Privaten Schlüssel erstellen

Zuerst ist mit dem folgendem Befehl ET_{key} zu erstellen:

```
openssl genrsa -aes256 -passout pass:yourSSLPW -out privkey.pem
2048
```

Erläuterung der Argumente:

Argument	Erläuterung
genrsa	*genrsa* weist *OpenSSL* an, einen RSA-Schlüssel zu erstellen.
-aes256	Zum Kodieren des Schlüssels AES256 verwenden.
-passout pass:*password*	Das zum Kodieren des privaten Schlüssels (im Beispiel: *yourSSLPW*) verwendete Passwort *yourSSLPW* ist lediglich ein Beispiel und sollte durch ein sicheres Passwort ersetzt werden.
-out *filename*	Name der Datei, die den ET_{key} enthält (im Beispiel: *privkey.pem*).
2048	Die Länge des Schlüssels.

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***privkey.pem***
  Diese Datei enthält den ET_{key} im PEM-Format. Der Schlüssel wird mit dem AES256-Algorithmus kodiert. Für den Zugriff auf den Schlüssel müssen Sie die oben angegebene Passphrase kennen (im Beispiel: *yourSSLPW*). Verwenden Sie zum Kodieren des privaten Schlüssels ein eigenes sicheres Passwort.

Manchmal ist die Erstellung eines nicht kodierten Schlüssels notwendig. Lassen Sie in diesem Fall die Optionen *-aes256* und *-passout* im Befehl oben einfach aus.

Zertifikat erstellen

Das Zertifikat wird mit folgendem Befehl erstellt:

```
openssl req -batch -new -x509 -key privkey.pem -keyform PEM
-passin pass:yourSSLPW -sha256 -outform PEM -out serverCert.pem
```

Erläuterung der Argumente:

Argument	Erläuterung
req	*req* weist *OpenSSL* an, eine Anforderung (Standard) für ein Zertifikat zu erstellen.
-batch	Kein interaktiver Modus.
-new	Neue Anfrage oder neues Zertifikat erstellen.
-x509	Selbstsigniertes Zertifikat statt einer Zertifikatanfrage erstellen.
-key *filename*	Der entsprechende private Schlüssel (im Beispiel: *privkey.pem*).
-keyform PEM	Der private Schlüssel weist das Format PEM auf.
-passin pass:*password*	Das für die Kodierung des privaten Schlüssels benötigte Passwort (im Beispiel: *yourSSLPW*).
-sha256	Mit dem Algorithmus SHA256 können Sie das Message Digest für die Signatur erstellen (empfohlen).
-outform PEM	Das Format der Ausgabedatei ist PEM.
-out *filename*	Der Name der Ausgabedatei, also das Zertifikat (im Beispiel *serverCert.pem*).

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***serverCert.pem***
  Diese Datei enthält das selbstsignierte Zertifikat ET_{cert}.

Schlüsselspeicher anlegen

Die Schlüssel und Zertifikate müssen in den Schlüsselspeichern enthalten sein. Die mdm-VA enthält das (proprietäre) Java-Tool *ImportKey* im Verzeichnis */etc/mdm/mdm-CA/demoCA*, das für das Anlegen und Verwalten von Schlüsselspeichern verwendet werden kann. Kopieren Sie die Datei *ImportKey.class* in Ihr Arbeitsverzeichnis.

Zuerst muss ET_{key} in das Format PKCS#8 umgewandelt und sowohl ET_{key} als auch ET_{cert} in den Schlüsselspeicher übernommen werden. In diesem Beispiel wird das Java KeyStore Format *JKS* verwendet. Dies kann mit dem Tool *ImportKey* abgeschlossen werden. *ImportKey* akzeptiert nur den (nicht kodierten) Schlüssel am Standardeingang, daher kann die Ausgabe des Befehls *pkcs8* wie folgt weitergereicht werden:

```
openssl pkcs8 -topk8 -in privkey.pem -passin pass:yourSSLPW
-inform PEM -nocrypt -outform DER |java -cp . ImportKey
-alias yourAlias -storetype JKS -keystore serverKeystore.jks
```

```
-storepass pass:yourSSLPW -keypass pass:yourSSLPW
-chain serverCert.pem
```

Erläuterung der ***openssl***-Argumente:

Argument	Erläuterung
pkcs8	Mit dem Befehl *pkcs8* werden private Schlüssel im Format PKCS#8 verarbeitet.
-topk8	Privaten Schlüssel im traditionellen Format verwenden und Schlüssel im Format PKCS#8 schreiben.
-in *filename*	Name und Speicherort der Eingabedatei (im Beispiel: *privkey.pem*).
-passin pass:*password*	Das für die Dekodierung der Eingabe benötigte Passwort (im Beispiel: *yourSSLPW*).
-inform PEM	Das Eingabeformat des Schlüssels ist PEM.
-nocrypt	Die Ausgabe (der Schlüssel) ist nicht kodiert.
-outform DER	Das Ausgabeformat ist DER.

Erläuterung der ***ImportKey***-Argumente:

Argument	Erläuterung
-alias *name*	Ein Schlüsselspeicher kann mehrere Einträge enthalten. Der Alias kennzeichnet den Eintrag und darf daher im Schlüsselspeicher nur einmal vorkommen. Aliases sind unabhängig von Groß- und Kleinschreibung.
-keystore *filename*	Die Datei, die den Schlüsselspeicher enthält (im Beispiel: *serverKeyStore.jks*).
-storetype JKS	Verwenden Sie für den Schlüsselspeicher das Format JKS.
-storepass pass:*password*	Das für die Dekodierung der Inhalte des Schlüsselspeichers benötigte Passwort (im Beispiel: *yourSSLPW*).
-keypass pass:*password*	Zusätzliches Passwort für die Dekodierung des privaten Schlüssels im Schlüsselspeicher.
-chain *filename*	Das Zertifikat (im Beispiel *serverCert.pem*).

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***serverKeyStore.jks***
  Dies ist der Schlüsselspeicher, der das Zertifikat und den privaten Schlüssel enthält.

Zertifikat importieren

Nach Anlegen des Schlüsselspeichers müssen zuweilen zusätzliche Zertifikate in den Schlüsselspeicher importiert werden. Dies kann mit dem folgenden Befehl erfolgen:

```
java -cp . ImportKey -alias yourAlias -storetype JKS
-file additionalCertificate.pem -storepass pass:yourSSLPW
-keystore serverKeystore.jks
```

Erläuterung der ***ImportKey***-Argumente:

Argument	Erläuterung
-alias *name*	Ein Schlüsselspeicher kann mehrere Einträge enthalten. Der Alias kennzeichnet den Eintrag und darf daher im Schlüsselspeicher nur einmal vorkommen. Aliases sind unabhängig von Groß- und Kleinschreibung.
-keystore *filename*	Die Datei, die den Schlüsselspeicher enthält (im Beispiel: *serverKeyStore.jks*).
-storetype JKS	Das Format des Schlüsselspeichers.
-storepass pass:*password*	Das für die Dekodierung der Inhalte des Schlüsselspeichers benötigte Passwort (im Beispiel: *yourSSLPW*).
-file *filename*	Das zu importierende Zertifikat (im Beispiel *serverCert.pem*).

9.2 Zertifikate und Schlüssel für eine PKI

Beim Ausrollen einer Private Key Infrastructure (PKI), das generell bei Verwendung des mdm CA beabsichtigt ist, sind zusätzlich zu den im vorherigen Abschnitt erwähnten Punkten weitere Voraussetzungen zu berücksichtigen. In diesem Kapitel werden zunächst die Grundlagen der PKI und anschließend die Verwendung von *OpenSSL* zum Ausrollen einer PKI erläutert.

Die in diesem Abschnitt beschriebenen Zertifikate werden nicht für SSL verwendet.

Die in diesem Abschnitt beschriebenen Zertifikate und Schlüssel werden nicht im SSL-Schlüsselspeicher des mdm CDA, sondern im CDA-Schlüsselspeicher abgelegt.

Grundlagen PKI

Gründe für die Verwendung einer PKI können unter anderem sein:

– **Authentifizierung**

  Bei der Kommunikation über Datennetzwerke kann die Entität auf der anderen Seite meist nicht „gesehen“ werden (Ausnahme: Videotelefonie), d. h. es besteht keine Sicherheit darüber, dass die Entität auf der anderen Seite auch wirklich die ist, die sie zu sein vorgibt. Durch die Verwendung einer PKI ist die Authentizität der miteinander kommunizierenden Entitäten gewährleistet.

– **Vertraulichkeit der Daten**

  Aus diesem Grund werden Daten mittels VPN ausgetauscht: Die Datenpakete werden „in der Öffentlichkeit“ (Internet) verschickt, aber nicht befugte Entitäten erhalten keinen Zugriff auf die in den Paketen enthaltenen Informationen.

– **Integrität der Daten**

  Die Sicherheit, dass die empfangenen Informationen den durch die andere Entität übermittelten Informationen entsprechen. Auf diese Weise wird verhindert, dass die Informationen durch eine nicht teilnahmeberechtigte Entität „in der Mitte“ geändert werden.

Die Beschreibung aller für eine komplette PKI notwendigen Komponenten und Interaktionen würde den Rahmen des vorliegenden Dokuments sprengen, daher sollen hier nur die wichtigsten genannt werden:

– **Zertifikate und private Schlüssel**

  Zertifikate sind ein Mittel einer PKI, um die Authentifizierung zu gewährleisten. Die Identität eines Zertifikatsinhabers wird durch eine CA anerkannt, die die Zertifikatanforderung des jeweiligen Inhabers signiert. Die Kodierung/Dekodierung der Daten erfolgt über öffentliche und private Schlüssel, sodass die Vertraulichkeit der Daten gewährleistet ist.

– **Zertifizierungsstelle (CA)**

  Eine *Zertifizierungsstelle* ist eine Komponente in einer PKI, die die Authentizität der teilnehmenden Entitäten durch Signieren von Zertifikatanfragen (d. h. die Ausstellung von Zertifikaten) gewährleistet. Normalerweise sind in einer PKI mehrere CAs in einer hierarchischen Struktur mit einer Root-CA an der Spitze organisiert.

– **CRL Distribution Points (CDP)**

  Siehe folgenden Abschnitt *Zertifikaterweiterungen*.

– **Miteinander kommunizierende Entitäten**

  Die Entitäten, die PKI verwenden, authentifizieren sich mit Zertifikaten und verwenden zum Kodieren/Dekodieren der ausgetauschten Daten den öffentlichen/privaten Schlüssel. Die Entitäten fordern die Zertifikate von der CA an. Normalerweise gehört

auch eine *Registration Authority* (RA) zu einer PKI. Die RA ist für die erstmalige Registrierung von Entitäten zuständig, die die PKI verwenden möchten. Im mdm Verwendungs-Szenario ist keine RA notwendig.

Inhalte eines Zertifikats

Wie im vorherigen Kapitel erwähnt, enthält ein Zertifikat folgende Informationen:

– den öffentlichen Schlüssel der Entität
– Informationen über die Entität, beispielsweise Name und/oder IP-Adresse
– weitere Informationen z. B. zum Zertifikat und der Infrastruktur

In den folgenden Kapiteln werden die Inhalte genauer beschrieben.

Der Subject Distinguished Name

Der *Subject Distinguished Name* ist eine eindeutige Benennung des Zertifikats und dessen Inhaber. Er besteht aus mehreren Komponenten:

Abkürzung	Name	Erläuterung
CN	Common Name	Identifiziert die Person oder das Objekt, zu der/dem das Zertifikat gehört. Beispielsweise: CN=server1
E	E-mail Address	Gibt die E-Mail-Adresse des Inhabers an.
OU	Organizational Unit	Kennzeichnet eine Einheit innerhalb des Unternehmens. Beispielsweise: OU=Research&Development
O	Organization	Kennzeichnet das Unternehmen. Beispielsweise: O=Innominate
L	Locality	Kennzeichnet den Ort, an dem die Entität sitzt. Der Ort kann eine Stadt sein: L=Berlin
ST	State	Kennzeichnet das Bundesland. Beispielsweise: ST=Berlin
C	Country	Code bestehend aus zwei Buchstaben, die das Land angeben. Beispielsweise: C=DE (Deutschland)

Entsprechend unseren Richtlinien sind nicht alle Komponenten obligatorisch, aber wenn die Erweiterung *Subject Alternative Name* nicht im Zertifikat enthalten ist, muss mindestens eine Komponente, die als Kennzeichnung dienen kann, angegeben werden. Dies ist normalerweise der *Common Name* (CN). Hinweis: die mdm CA kann aktuell Zertifikate mit der Erweiterung *Subject Alternative Name* nicht verarbeiten.

Zertifikaterweiterungen

In den sogenannten Erweiterungen oder Extensions sind Informationen über das Zertifikat oder die Infrastruktur enthalten. Im Grunde genommen kann jeder seine eigenen Erweiterungen festlegen, aber Standarderweiterungen (X.509version3) sind in RFC 3280 *Internet X.509 Public Key Infrastructure - Certificate and CRL Profile* definiert. Nachfolgend sind die für die mdm CA wichtigen Erweiterungen kurz beschrieben:

– **Critical Bit**

  Das *Critical Bit* ist keine Erweiterung, sondern wird verwendet, um die Verwendung von Erweiterungen im Zertifikat zu erzwingen. Das *Critical Bit* kann für jede Erweiterung im Zertifikat gesetzt werden. Anwendungen, die ein Zertifikat überprüfen, müssen eine Erweiterung mit *Critical Bit* interpretieren können. Wenn die Anwendung die Erweiterung nicht interpretieren kann, muss das Zertifikat zurückgewiesen werden.

– **Basic Constraints**

  Mit der Erweiterung *Basic Constraints* wird angezeigt, ob es sich bei einem Zertifikat um ein CA-Zertifikat handelt oder nicht. *Basic Constraints* besteht aus zwei Feldern:
  – Feld *cA* vom Typ BOOLEAN und
  – Feld *pathLenConstraint* (optional) vom Typ INTEGER

  Bei CA-Zertifikaten muss das Feld *cA* auf *true* gesetzt sein. *pathLenConstraint* wird nur verwendet, wenn das Feld *cA* auf True gesetzt ist und die Nummer der zulässigen CA-Ebenen unter dem Zertifikat angibt. *Basic Constraints* sollte immer als kritisch gekennzeichnet sein.

  Die Anforderungen hinsichtlich der Erweiterung *Basis Constraints* finden Sie in Kapitel 9.2.3.

– **Key Usage**

  Key Usage kontrolliert die beabsichtigte Verwendung der Schlüssel eines Zertifikats. Ein Schlüssel kann verwendet werden, um Zertifikatssperrlisten (CRL) zu signieren, Daten zu verschlüsseln oder Zertifikate zu signieren.

  Die Anforderungen hinsichtlich der Erweiterung *Key Esage Constraints* finden Sie in Kapitel 9.2.3.

– **Subject Alternative Name**

  Mit der Erweiterung *Subject Alternative Name* können weitere Kennzeichen hinzugefügt werden. *Subject Alternative Name* kann zum Beispiel E-Mailadressen, Domainnamen usw. enthalten. Es kann auch als Ersatz für das Feld *Subject* verwendet werden, das in diesem Fall nicht frei bleiben darf. Hinweis: die mdm CA kann aktuell Zertifikate mit der Erweiterung *Subject Alternative Name* nicht verarbeiten.

– **CRL Distribution Points (CDP)**

  Zertifikate können widerrufen werden, beispielsweise wenn ein privater Schlüssel beschädigt oder nicht mehr gültig ist. Normalerweise muss die Anwendung die Gültigkeit eines Zertifikats durch Kontrolle des Gültigkeitszeitraums und/oder durch Abholen des Widerrufs von einem CRL-Verteilungspunkt (CDP) überprüfen. Zum Abholen der Informationen kann entweder eine *Certificate Revocation Lists* (CRL) oder ein dezidiertes Protokoll wie OCSP verwendet werden. Das Zertifikat sollte jedoch Informationen dazu enthalten, welche CDP zu kontaktieren ist.

– **Authority Information Access**

  Authority Information Access ist keine Standarderweiterung von X.509, sondern eine Erweiterung, die durch die Arbeitsgruppe PKIX definiert wurde (http://www.ietf.org/html.charters/pkix-charter.html). *Authority Information Access* enthält Informationen über die Ausgabe einer CA, beispielsweise Richtlinien, weitere Root-Zertifikate oder Informationen zum Abholen höherwertiger Zertifikate in der Kette, wenn nicht die gesamte Kette im Zertifikat enthalten ist.

  Abhängig von den Einstellungen dieser Erweiterungen kann der Empfänger (nicht der Inhaber) eines Zertifikats die Kommunikation mit der Gegenstelle akzeptieren oder verweigern, sodass Missbrauch von Zertifikaten verhindert und eine höhere Sicherheitsstufe erreicht wird.

9.2.1 CA-Zertifikate erstellen

Abhängig von der vorhandenen Infrastruktur benötigt die mdm CA folgende Zertifikate:

– Ein selbstsigniertes Root-Zertifikat ($CA_{rootCert}$) mit dem passenden privaten Schlüssel ($CA_{rootKey}$).
  Wenn Sie über ein weiteres vorgeschaltetes (Root-) CA verfügen, besteht keine Notwendigkeit zur Erstellung des Root-Zertifikats und des passenden privaten Schlüssels.
  Das (selbstsignierte) Zertifikate wird an alle Entitäten verteilt, die an der Kommunikation teilnehmen. Es wird durch die Entitäten verwendet, um die Authentizität der Gegenstelle und jedweder zwischengeschalteter CAs in der Zertifikatskette zu überprüfen. Der private Schlüssel $CA_{rootKey}$ wird zum Signieren des selbstsignierten Root-Zertifikats verwendet.
– Ein CA-Zertifikat (CA_{cert}) mit dem passenden privaten Schlüssel (CA_{key}). Mit diesem Zertifikat authentifiziert sich die CA selbst gegenüber anderen Entitäten. Dieses Zertifikat muss mit dem privaten Root-Key signiert werden, d. h. entweder mit $CA_{rootKey}$ oder mit dem Schlüssel Ihrer bestehenden Root-CA. Mit dem privaten Schlüssel CA_{key} wird die vom mdm-Server übermittelte Zertifikatanfrage signiert, d. h. damit werden Zertifikate für die mGuards ausgegeben.
– Ein Template-Zertifikat ($CA_{templCert}$) das von der CA als Template bei der Ausgabe von End-Entitäts- (mGuard) Zertifikaten verwendet wird.
  In Bild 9-1 ist die Zertifikathierarchie dargestellt:

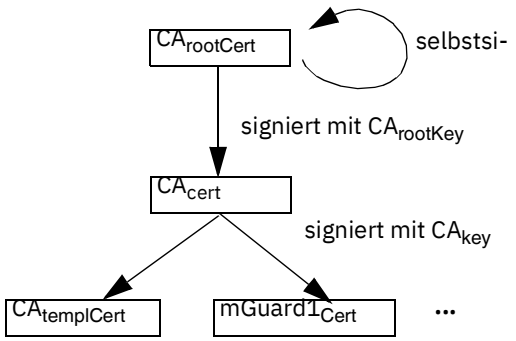


Bild 9-1 mdm CA-Zertifikathierarchie

Im Folgenden wird angenommen, dass keine andere Root-CA vorhanden ist und dass die mdm CA als Root-CA verwendet wird.

Achtung: Legen Sie den/die privaten Schlüssel an einem sicheren Speicherort ab. Dies ist vor allem für den privaten Schlüssel der Root-CA erforderlich.

Es wird empfohlen, im mdm-Installationsverzeichnis ein Arbeitsverzeichnis anzulegen, z. B. unter dem Namen *security*, in dem alle Zertifikate und Schlüssel während der folgenden Prozesse abgelegt werden.

Root-Zertifikat erstellen

Die folgenden *OpenSSL*-Befehle erfordern eine Eingabe von der *OpenSSL*-Konfigurationsdatei *openssl.cnf* (in welchem Verzeichnis sich diese Datei befindet, hängt von Ihrer Verteilung ab, prüfen Sie beispielsweise das Verzeichnis */usr/ssl* oder */usr/lib/ssl*). Anstatt

einer Änderung der Standard-Konfigurationsdatei Ihrer *OpenSSL*-Installation wird empfohlen, die in der mdm-VA im Verzeichnis */etc/mdm/mdm-ca/* vorhandenen Beispiel-Konfigurationsdateien zu verwenden und an die jeweiligen Anforderungen anzupassen. Sie können *OpenSSL* anweisen, anstelle der Standard-Konfigurationsdatei die zur Verfügung gestellten Konfigurationsdateien zu verwenden.

OpenSSL-Konfigurationsdatei anpassen

Kopieren Sie die Datei *rootCert.conf*, die in der mdm-VA im Verzeichnis */etc/mdm/mdm-CA/demoCA* zur Verfügung steht, in Ihr Arbeitsverzeichnis. Passen Sie den Bereich `[ root_dn ]` der Datei, in dem der *Subject Distinguished Name* Ihres Root-CA-Zertifikats enthalten ist, an:

```
[ root_dn ]
C= DE
O= Innominate Security Technologies AG
OU= Research & Development
CN= Test Root CA
```

Beachten Sie auch den Bereich `[ root_ext ]` der Konfigurationsdatei, der wichtig für die korrekte Erstellung des Root-Zertifikats ist (eine Erläuterung dazu finden Sie in Abschnitt *Certificate extensions*):

```
[ root_ext ]
keyUsage= cRLSign, keyCertSign
basicConstraints= critical, CA:true, pathlen:1
```

Privaten Schlüssel erstellen

Mit dem folgenden Befehl ist zunächst $CA_{rootKey}$ zu erstellen:

```
openssl genrsa -aes256 -passout pass:rootPW
-out rootKey.pem 2048
```

Erläuterung der Argumente:

Argument	Erläuterung
genrsa	*genrsa* weist *OpenSSL* an, einen RSA-Schlüssel zu erstellen.
-aes256	Zum Kodieren des Schlüssels AES256 verwenden.
-passout pass:*password*	Das zum Kodieren des privaten Schlüssels (im Beispiel: *rootPW*) verwendete Passwort *rootPW* ist lediglich ein Beispiel und sollte durch ein sicheres Passwort ersetzt werden.
-out *filename*	Name der Datei, die den $CA_{rootKey}$ enthält (im Beispiel: *rootKey.pem*).
2048	Die Länge des Schlüssels.

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***rootKey.pem***

Diese Datei enthält $CA_{rootKey}$ im PEM format. Der Schlüssel wird mit dem AES256-Algorithmus kodiert. Für den Zugriff auf den Schlüssel müssen Sie die oben angegebene Passphrase kennen (im Beispiel: *rootPW*). Verwenden Sie zum Kodieren des privaten Schlüssels ein eigenes sicheres Passwort.

Root-Zertifikat erstellen

Der OpenSSL-Befehl zur Erstellung von $CA_{rootCert}$ lautet:

```
openssl req -batch -new -config rootCert.conf -x509
-key rootKey.pem -keyform PEM -passin pass:rootPW -sha256 -days
5479 -outform PEM -out rootCert.pem
```

Erläuterung der Argumente:

Argument	Erläuterung
req	*req* weist *OpenSSL* an, eine Anforderung (Standard) für ein Zertifikat zu erstellen.
-batch	Kein interaktiver Modus.
-new	Neue Anfrage oder neues Zertifikat erstellen.
-config *filename*	Name und Speicherort der OpenSSL-Konfigurationsdatei (im Beispiel: *rootCert.conf*).
-x509	Selbstsigniertes Zertifikat statt einer Zertifikatanfrage erstellen.
-key *filename*	Der entsprechende private Schlüssel (im Beispiel: *rootkey.pem*).
-keyform PEM	Der private Schlüssel weist das Format PEM auf.
-passin pass:*password*	Das für die Kodierung des privaten Schlüssels benötigte Passwort (im Beispiel: *rootPW*).
-sha256	Mit dem Algorithmus SHA256 können Sie das Message Digest für die Signatur erstellen (empfohlen).
-days *5479*	Der Zeitraum, für den ein Zertifikat gültig ist.
-outform PEM	Das Format der Ausgabedatei ist PEM.
-out *filename*	Der Name der Ausgabedatei, also das Zertifikat (im Beispiel *rootCert.pem*).

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***rootCert.pem***
  Diese Datei enthält das selbstsignierte Root-Zertifikat $CA_{rootCert}$.

CA-Zertifikat erstellen

Das zwischengeschaltete CA-Zertifikat CA_{cert} ist zwar nicht selbstsigniert, wird aber durch die Root-CA ausgegeben (signiert). Daher müssen Sie zuerst einen privaten Schlüssel erstellen und eine entsprechende Zertifikatanforderung an die Root-CA „abschicken“. Die Root-CA gibt dann wiederum das CA_{cert} aus.

Zuerst muss die Konfigurationsdatei wie im vorhergehenden Abschnitt beschrieben an Ihre Bedürfnisse angepasst werden.

OpenSSL-Konfigurationsdatei und die Umgebung anpassen

Kopieren Sie die Datei *caCert.conf*, die in der mdm-VA im Verzeichnis */etc/mdm/mdm-CA/demoCA* enthalten ist, in Ihr Arbeitsverzeichnis. Passen Sie den Bereich [ca_dn] der Datei, in dem der *Subject Distinguished Name* Ihres Root-CA-Zertifikats enthalten ist, an:

```
[ ca_dn ]
C= DE
O= Innominate Security Technologies AG
OU= Research & Development
CN= Test CA
```

Passen Sie ebenfalls die Einträge `crlDistributionPoints` und `authorityInfoAccess` des Bereichs [ca_ext] der Konfigurationsdatei an (Erläuterung siehe Abschnitt *Certificate extensions*):

```
[ ca_ext ]
crlDistributionPoints=URI:http://ca.example.com/ca-ca.crl
authorityInfoAccess=OCSP;URI:http://ca.example.com/ocsp/ca-ca
```

Die Konfigurationsdatei enthält einige Parameter, die nicht in die Kommandozeile eingegeben werden können. Diese Einträge geben Dateien an, die im Dateisystem vorhanden sein *müssen*. Daher sind diese Dateien zuerst manuell zu erstellen (die Dateinamen werden ebenfalls in der Datei *caCert.con* verwendet, benutzen Sie daher genau die gleichen Dateinamen wie unten angegeben):

– Erstellen Sie in Ihrem Arbeitsverzeichnis ein Unterverzeichnis *archive*
(Linux: `mkdir ./archive`)
– Legen Sie im Unterverzeichnis *archive* eine Datei mit der Bezeichnung *serial* an, die die gültige Seriennummer für das Zertifikat enthält
(Linux: `echo 1234 > archive/serial`)
– Legen Sie eine leere Datei an, die als OpenSSL-Datenbank verwendet werden kann.
(Linux: `touch archive/index.txt`
Windows: `copy NUL: archive/index.txt`)

Privaten Schlüssel erstellen

Zuerst ist mit dem folgendem Befehl der private Schlüssel CA_{key} zu erstellen:

```
openssl genrsa -aes256 -passout pass:caPW -out caKey.pem 2048
```

Erläuterung der Argumente:

Argument	Erläuterung
genrsa	*genrsa* weist *OpenSSL* an, einen RSA-Schlüssel zu erstellen.
-aes256	Zum Kodieren des Schlüssels AES256 verwenden.

Argument	Erläuterung
-passout pass:*password*	Das zum Kodieren des privaten Schlüssels (im Beispiel: *caPW*) verwendete Passwort *caPW* ist lediglich ein Beispiel und sollte durch ein sicheres Passwort ersetzt werden.
-out *filename*	Name der Datei, die den privaten Schlüssel enthält (im Beispiel: *caKey.pem*).
2048	Die Länge des Schlüssels.

Mit diesem Befehl wird die Ausgabedatei erstellt:

– ***caKey.pem***
Diese Datei enthält den CA_{key} im PEM-Format. Der Schlüssel wird mit dem AES256-Algorithmus kodiert. Für den Zugriff auf den Schlüssel müssen Sie die oben angegebene Passphrase kennen (im Beispiel: *caPW*). Verwenden Sie zum Kodieren des privaten Schlüssels ein eigenes sicheres Passwort.

Zertifikatanfrage erstellen

Eine Zertifikatanfrage wird mit folgendem Befehl erstellt:

```
openssl req -batch -new -config caCert.conf
-key caKey.pem -keyform PEM -passin pass:caPW -sha256
-out caCertReq.pem -outform PEM
```

Erläuterung der Argumente:

Argument	Erläuterung
req	*req* weist *OpenSSL* an, eine Anforderung (Standard) für ein Zertifikat zu erstellen.
-batch	Kein interaktiver Modus.
-new	Neue Anfrage erstellen.
-config *filename*	Name und Speicherort der OpenSSL-Konfigurationsdatei (im Beispiel: *caCert.conf*).
-key *filename*	Der entsprechende private Schlüssel (im Beispiel: *caKey.pem*).
-keyform PEM	Der private Schlüssel weist das Format PEM auf.
-passin pass:*password*	Das für die Kodierung des privaten Schlüssels benötigte Passwort (im Beispiel: *caPW*).
-sha256	Mit dem Algorithmus SHA256 können Sie das Message Digest für die Signatur erstellen (empfohlen).
-outform PEM	Das Format der Ausgabedatei ist PEM.

Argument	Erläuterung
-out *filename*	Der Name der Ausgabedatei, also das Zertifikat (im Beispiel *caCertReq.pem*).

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***caCertReq.pem***
  Diese Datei enthält die Zertifikatanfrage.

CA-Zertifikat anfordern

Die Anfrage muss an die Root-CA übermittelt werden. Da die mdm CA im Beispiel die Root-CA ist, können Sie das Zertifikat mit folgendem Befehl ausgeben:

```
openssl ca -batch -config caCert.conf -days 3653
-in caCertReq.pem -cert rootCert.pem -keyfile rootKey.pem
-passin pass:rootPW-md sha256 -notext -out caCert.pem
-outdir .
```

Erläuterung der Argumente:

Argument	Erläuterung
ca	Der Befehl *ca* ist eine minimale CA-Anwendung. Mit ihm können Zertifikatanfragen signiert und CRLs erstellt werden.
-batch	Kein interaktiver Modus.
-config *filename*	Name und Speicherort der OpenSSL-Konfigurationsdatei (im Beispiel: *caCert.conf*).
-days *3653*	Der Zeitraum, für den ein Zertifikat gültig ist.
-in *filename*	Der Name der Datei, die die Zertifikatanfrage enthält (im Beispiel *caCertReq.pem*).
-cert *filename*	Der Name der Datei, die das Root-Zertifikat enthält (im Beispiel *rootCert.pem*).
-keyfile *filename*	Der Name der Datei, die den zum Signieren der Zertifikatanfrage verwendeten Schlüssel enthält (im Beispiel *rootKey.pem*).
-passin pass:*password*	Das für die Kodierung des privaten Schlüssels benötigte Passwort (im Beispiel: *rootPW*).
-md sha256	Mit dem Algorithmus SHA256 können Sie das Message Digest für die Signatur erstellen (empfohlen).

Argument	Erläuterung
-notext	*openssl* verfügt über die Möglichkeit, durch Benutzer lesbaren beschreibenden Text in das Zertifikat einzufügen. Dies würde jedoch im weiteren Prozessverlauf Probleme beim Anlegen der Schlüsselspeicher verursachen, daher sollte kein Text in das Zertifikat eingefügt werden.
-outdir *directoryName*	Das Ausgabeverzeichnis (im Beispiel das aktuelle Arbeitsverzeichnis ".").

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***caCert.pem***
Diese Datei enthält CA_{cert}.

Die Datei *caCertReq.pem* wird nicht länger benötigt und sollte gelöscht werden.

Zertifikatvorlage anlegen

Die CA dient der Ausgabe von Zertifikaten. Dazu benötigt die CA eine Anleitung zu den auszugebenden Zertifikaten, beispielsweise zu den benötigten Erweiterungen. Dazu kann der CA eine Zertifikatvorlage zur Verfügung gestellt werden ($CA_{templCert}$). $CA_{templCert}$ ist ein von der CA ausgegebenes Zertifikat. Zur Ausgabe eines Zertifikats müssen Sie zunächst wieder eine OpenSSL-Konfigurationsdatei anpassen.

OpenSSL-Konfigurationsdatei anpassen

Kopieren Sie die Datei *templateCert.conf*, die in der mdm-VA im Verzeichnis */etc/mdm/mdm-CA/demoCA* enthalten ist, in Ihr Arbeitsverzeichnis. Passen Sie die Einträge `crlDistributionPoints` und `authorityInfoAccess` des Bereichs [template_ext] der Konfigurationsdatei an (Erläuterung siehe Abschnitt *Certificate extensions*):

```
[ template_ext ]
crlDistributionPoints=URI:http://ca.example.com/ca-ee.crl
authorityInfoAccess=OCSP;URI:http://ca.example.com/ocsp/ca-ee
```

Die Konfigurationsdatei *templateCert.conf* erwartet, dass Dateien vorhanden sind, welche manuell angelegt werden müssen. (siehe vorherigen Abschnitt *CA-Zertifikat erstellen*, *Unterpunkt OpenSSL-Konfigurationsdatei und die Umgebung anpassen*).

Privaten Schlüssel erstellen

Zuerst ist mit dem folgendem Befehl der private Schlüssel zu erstellen:

```
openssl genrsa -aes256 -passout pass:caPW -out templateKey.pem
2048
```

Erläuterung der Argumente:

Argument	Erläuterung
genrsa	*genrsa* weist *OpenSSL* an, einen RSA-Schlüssel zu erstellen.
-aes256	Zum Kodieren des Schlüssels AES256 verwenden.
-passout pass:*password*	Das zum Kodieren des privaten Schlüssels (im Beispiel: *caPW*) verwendete Passwort *caPW* ist lediglich ein Beispiel und sollte durch ein sicheres Passwort ersetzt werden.
-out *filename*	Name der Datei, die den privaten Schlüssel enthält (im Beispiel: *templateKey.pem*).
2048	Die Länge des Schlüssels.

Mit diesem Befehl wird die Ausgabedatei erstellt:

– ***templateKey.pem***
  Diese Datei enthält einen kodierten privaten Schlüssel.

Zertifikatanfrage erstellen

Eine Zertifikatanfrage wird mit folgendem Befehl erstellt:

```
openssl req -new -batch -config templateCert.conf
-key templateKey.pem -keyform PEM -passin pass:caPW
-sha256 -outform PEM -out templateCertReq.pem
```

Erläuterung der Argumente:

Argument	Erläuterung
req	*req* weist *OpenSSL* an, eine Anforderung (Standard) für ein Zertifikat zu erstellen.
-batch	Kein interaktiver Modus.
-new	Neue Anfrage oder neues Zertifikat erstellen.
-config *filename*	Name und Speicherort der OpenSSL-Konfigurationsdatei (im Beispiel: *templateCert.conf*).
-key *filename*	Der entsprechende private Schlüssel (im Beispiel: *templateKey.pem*).
-keyform PEM	Der private Schlüssel weist das Format PEM auf.
-passin pass:*password*	Das für die Kodierung des privaten Schlüssels benötigte Passwort (im Beispiel: *caPW*).

Argument	Erläuterung
-sha256	Mit dem Algorithmus SHA256 können Sie das Message Digest für die Signatur erstellen (empfohlen).
-outform PEM	Das Format der Ausgabedatei ist PEM.
-out *filename*	Der Name der Ausgabedatei, also das Zertifikat (im Beispiel *templateCertReq.pem*).

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***templateCertReq.pem***
  Diese Datei enthält die Zertifikatanfrage.

Zertifikatvorlage anfordern

Die Anfrage muss an die (zwischengeschaltete) CA übermittelt werden. Sie können die Zertifikatanfrage mit dem folgenden Befehl signieren (das Zertifikat ausgeben):

```
openssl ca -batch -config templateCert.conf -days 1826
-md sha256 -in templateCertReq.pem -keyfile caKey.pem
-cert caCert.pem -passin pass:caPW -notext
-out templateCert.pem -outdir .
```

Erläuterung der Argumente:

Argument	Erläuterung
ca	Der Befehl *ca* ist eine minimale CA-Anwendung. Mit ihm können Zertifikatanfragen signiert und CRLs erstellt werden.
-batch	Kein interaktiver Modus.
-config *filename*	Name und Speicherort der OpenSSL-Konfigurationsdatei (im Beispiel: *templateCert.conf*).
-days *1826*	Der Zeitraum, für den ein Zertifikat gültig ist.
-in *filename*	Der Name der Datei, die die Zertifikatanfrage enthält (im Beispiel *templateCertReq.pem*).
-cert *filename*	Der Name der Datei, die das Root-Zertifikat enthält (im Beispiel *caCert.pem*).
-keyfile *filename*	Der Name der Datei, die den zum Signieren der Zertifikatanfrage verwendeten Schlüssel enthält (im Beispiel *caKey.pem*).
-passin pass:*password*	Das für die Kodierung des privaten Schlüssels benötigte Passwort (im Beispiel: *caPW*).

Argument	Erläuterung
-md sha256	Mit dem Algorithmus SHA256 können Sie das Message Digest für die Signatur erstellen (empfohlen).
-notext	*openssl* verfügt über die Möglichkeit, durch Benutzer lesbaren beschreibenden Text in das Zertifikat einzufügen. Dies würde jedoch im weiteren Prozessverlauf Probleme beim Anlegen der Schlüsselspeicher verursachen, daher sollte kein Text in das Zertifikat eingefügt werden.
-outdir *directoryName*	Das Ausgabeverzeichnis (im Beispiel das aktuelle Arbeitsverzeichnis ".").

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– ***templateCert.pem***
  Diese Datei enthält $CA_{templCert}$. Die Datei sollte in ihr endgültiges Zielverzeichnis kopiert werden; der Speicherort ist in *ca-preferences.xml* im Knoten *certificateFactory » certTemplate* zu konfigurieren.

Die Dateien *templateCertReq.pem* und *templateKey.pem* werden nicht mehr benötigt und sollten gelöscht werden.

9.2.2 Schlüsselverzeichnisse erstellen

Nach Durchführung der in Kapitel 9.2.1 beschriebenen Schritte sollten Sie in Ihrem Arbeitsverzeichnis die folgenden Dateien vorfinden:

– ***templateCert.pem***
  Diese Datei enthält $CA_{templCert}$, signiert mit CA_{key}.
– ***caCert.pem***
  Diese Datei enthält CA_{cert}, signiert mit $CA_{rootKey}$.
– ***caKey.pem***
  Diese Datei enthält CA_{key}.
– ***rootCert.pem***
  Diese Datei enthält das selbstsignierte Root-Zertifikat $CA_{rootCert}$.
– ***rootKey.pem***
  Diese Datei enthält den kodierten privaten Schlüssel $CA_{rootKey}$.

Einige dieser Dateien müssen in den Schlüsselspeichern enthalten sein. Die mdm-VA enthält im Verzeichnis */etc/mdm/mdm-CA/demoCA* das (proprietäre) Java-Tool *ImportKey*, das für das Anlegen und Verwalten von Schlüsselspeichern verwendet werden kann. Kopieren Sie die Datei *ImportKey.class* in Ihr Arbeitsverzeichnis.

Zuerst müssen das zwischengeschaltete CA-Zertifikat und das Root-Zertifikat in einer Datei zusammengeführt werden (eine Zertifikatskette erstellt werden):

```
cat caCert.pem rootCert.pem > caCertWithChain.pem
```

Dann muss der Key *caKey.perm* in das Format PKCS#8 umgewandelt und sowohl CA_{key} als auch die Zertifikatskette müssen in einen PKC#12-Schlüsselspeicher übernommen werden. Dies kann mit dem Tool *ImportKey* abgeschlossen werden. *ImportKey* akzeptiert nur den (nicht kodierten) Schlüssel am Standardeingang, daher kann die Ausgabe des Befehls *pkcs8* wie folgt weitergereicht werden:

```
openssl pkcs8 -topk8 -in caKey.pem -passin pass:caPW
-inform PEM -nocrypt -outform DER |
java -cp . ImportKey -alias ca -keystore ca-keystore.jks -
storetype JKS -storepass pass:caPW -keypass pass:caPW
-chain caCertWithChain.pem
```

Erläuterung der ***openssl***-Argumente:

Argument	Erläuterung
pkcs8	Mit dem Befehl *pkcs8* werden private Schlüssel im Format PKCS#8 verarbeitet.
-topk8	Privaten Schlüssel im traditionellen Format verwenden und Schlüssel im Format PKCS#8 schreiben.
-in *filename*	Name und Speicherort der Eingabedatei (im Beispiel: *caKey.pem*).
-passin pass:*password*	Das für die Dekodierung der Eingabe benötigte Passwort (im Beispiel: *caPW*).
-inform PEM	Das Eingabeformat des Schlüssels ist PEM.
-nocrypt	Die Ausgabe (der Schlüssel) ist nicht kodiert.
-outform DER	Das Ausgabeformat ist DER.

Erläuterung der ***ImportKey***-Argumente:

Argument	Erläuterung
-alias *name*	Ein Schlüsselspeicher kann mehrere Einträge enthalten. Der Alias kennzeichnet den Eintrag und darf daher im Schlüsselspeicher nur einmal vorkommen. Aliases sind unabhängig von Groß- und Kleinschreibung.
-keystore *filename*	Die Datei, die den Schlüsselspeicher enthält (im Beispiel: *ca-keyStore.jks*).
-storetype JKS	Verwenden Sie für den Schlüsselspeicher das Format JKS.
-storepass pass:*password*	Das für die Dekodierung der Inhalte des Schlüsselspeichers benötigte Passwort (im Beispiel: *caPW*).

Argument	Erläuterung
-keypass pass:*password*	Zusätzliches Passwort für die Dekodierung des privaten Schlüssels im Schlüsselspeicher.
-chain *filename*	Die Zertifikatskette mit dem Root-Zertifikat.

Mit dem Befehl oben wird die Ausgabedatei erstellt:

– *ca-keystore.jks*
  Dies ist der Schlüsselspeicher für Ihre CA, der die Zertifikatskette und den privaten CA-Schlüssel enthält. Kopieren Sie den Schlüsselspeicher in sein endgültiges Zielverzeichnis.
  – Der Dateiname mit dem absoluten oder relativen Pfad dieses Schlüsselspeichers muss in der Datei *ca-preferences.xml* im Knoten *certificateFactory » keyStore* konfiguriert werden.
  – Das Passwort für den Zugriff auf den Schlüsselspeicher (im Beispiel *caPW*) muss in der Datei *ca-preferences.xml* im Knoten *certificateFactory » keyStorePassword* konfiguriert werden.
  – Das Format dieses Schlüsselspeichers (Java KeyStore - JKS) muss in der Datei *ca-preferences.xml* im Knoten *certificateFactory » keyStoreType* konfiguriert werden.
  – Das Passwort für den Zugriff auf den privaten Schlüssel (im Beispiel *caPW*) muss in der Datei *ca-preferences.xml* im Knoten *certificateFactory » keyStorePassword* konfiguriert werden.
  – Der Alias (*ca*) des Schlüssels muss in der Datei *ca-preferences.xml* im Knoten *certificateFactory » keyAlias* konfiguriert werden.

Die Datei *caCertWithChain.pem* wird nicht länger benötigt und sollte gelöscht werden.

9.2.3 Anforderungen an Zertifikate

Für die einwandfreie Funktion der VPN-Zertifikate auch mit zukünftigen Versionen der mGuard-Firmware und des mdm müssen die Zertifikate folgende Anforderungen erfüllen:

1. Der private Schlüssel sollte eine Länge von mindestens 1024 Bit aufweisen. Phoenix Contact empfiehlt für die langfristige Sicherheit eine Schlüssellänge von 2048 Bit.
2. Alle Zertifikate müssen RFC 3280 entsprechen.
3. Alle Zertifikate müssen eine *Basic Constraints*-Erweiterung aufweisen, die als kritisch markiert ist und das Boolean-Feld *cA* muss auf *true* gesetzt sein.
4. Phoenix Contact empfiehlt dringend, das Feld *pathLenConstraint* in die *Basic Constraints*-Erweiterung aller Zertifikate einzubeziehen. Es muss auf eine Zahl unter der Anzahl der nachfolgenden Zertifikate gesetzt sein. Für ein typisches Szenario, bei dem eine Zertifikatskette aus einem Root-CA-Zertifikat, einem einzelnen zwischengeschaltetem CA-Zertifikat und einem End-Entitäts-Zertifikat (VPN-Zertifikat in diesem Fall) besteht, muss der *pathLenConstraint* eins (1) für das Root-CA-Zertifikat und Null für das zwischengeschaltete Zertifikat betragen.

5. Das Zertifikat des VPN-Templates muss über eine *Basic Constraints*-Erweiterung verfügen, die als kritisch markiert ist und das Boolean-Feld *cA* muss auf *false* gesetzt sein und ohne ein Feld *pathLenConstraint*.
6. Alle CA-Zertifikate müssen eine *Key Usage*-Erweiterung aufweisen, die als kritisch markiert ist und das Bit *keyCertSign* muss gesetzt sein. Es wird empfohlen, auch das Bit *cRLSign* zu setzen.
7. Das Zertifikat des VPN-Templates benötigt keine *Key Usage*-Erweiterung.
8. Ein zwischengeschaltetes CA-Zertifikat muss eine oder beide Erweiterungen *CRL Distribution Points* und *Authority Information Access* enthalten, wenn Sperrinformationen online mit einer zukünftigen Version von mdm und der mGuard-Firmware weitergeleitet werden sollen. Die Erweiterung muss als nicht-kritisch gekennzeichnet sein. Die frühere Erweiterung wird benötigt, wenn die Zertifikatssperrlisten (CRLs) in Zukunft verwendet werden sollen. Die letztere Erweiterung wird benötigt, wenn zukünftig die Verwendung des Online Certificate Status Protocol (OCSP, siehe RFC 2560) geplant ist. Jede der Erweiterungen darf nur HTTP-URLs enthalten.
9. Ein Template für ein VPN-Zertifikat sollte eine oder beide Erweiterungen *CRL Distribution Points* und *Authority Information Access wie oben* beschrieben enthalten, wenn Sperrinformationen online weitergeleitet werden sollen. Alternativ kann der mdm-Server angewiesen werden, diese in die Zertifikatanfrage einzufügen, die an die mdm CA übermittelt wurde. Das letztere ist flexibler, weil auf diese Art der Speicherort der Sperrinformationen (CRL) bzw. der Informationsdienst (OSCP) für Gerätegruppen und sogar für einzelne Geräte eingerichtet werden.
   Hinweis: Wenn das Template für das VPN-Zertifikat bereits eine dieser Erweiterungen enthält und der mdm angewiesen ist, dieses auch in die Zertifikatanforderung einzufügen, überschreibt die Erweiterung aus der Anfrage die im Template enthaltene Erweiterung. Das ausgegebene Zertifikat enthält die aus der Anfrage kopierte Erweiterung.
10. Der Schlüsselspeicher muss die komplette Zertifikatskette bis einschließlich des Root-Zertifikats enthalten.

10 mdm- Server und mdm-CA-Server konfigurieren

Für eine einwandfreie Funktion benötigt der mdm Server eine **XML preferences file** als Konfigurationsdatei, die beim Hochfahren des Servers angegeben werden kann (siehe „mdm-Server und mdm-Client“ auf Seite 15).

Eine Standard-Konfigurationsdatei (*preferences.xml*) ist in der mdm-VA im Verzeichnis */etc/mdm/mdm-server* enthalten.

In der Datei *preferences.xml* müssen mehrere Passwörter konfiguriert werden. Die entsprechenden *Keys* akzeptieren das Muster *ENV:VARNAME* als Wert, um das Passwort aus der Umgebungsvariable mit dem Namen *VARNAME* zu nehmen. Wenn Sie sich für dieses Muster entscheiden, sorgen Sie dafür, dass die jeweiligen *Environment Variablen vor* dem Hochfahren des Servers initialisiert werden.

10.1 mdm-Server (Datei *preferences.xml*)

Node *com*

Standardeinstellung (nicht ändern!)

Node *innominate*

Standardeinstellung (nicht ändern!)

Node *innomms*

Standardeinstellung (nicht ändern!)

Node *is*

Key *expertMode*

Wenn auf True gesetzt, werden einige nicht unterstützte Konfigurationsvariablen, die normalerweise verborgen sind, im Dialog Device and Template Properties aktiviert (Standardeinstellung: false). Darüber hinaus werden die mGuards so konfiguriert, dass nicht unterstützte Konfigurationsvariablen in deren Webinterface sichtbar werden. **Diesen Wert auf keinen Fall ändern!**

Key *defaultAdminPassword*

Das Passwort des Benutzers *admin* an neu angelegten mGuards (Standard: *mGuard*). Der Standardwert entspricht den Werkseinstellungen des mGuards. Wenn mGuard-Geräte vor ihrer Verwendung mit mdm vorkonfiguriert werden, kann ein anderes Standardpasswort für *admin* eingerichtet werden und die Datenbank muss mit dem folgenden Befehl aktualisiert werden:

```
java -Xmx1024m -jar mdm-server-1.17.x.jar update preferences.xml
```

Key *defaultRootPassword*

Das Passwort des Benutzers *root* an neu angelegten mGuards (Standard: *root*). Der Standardwert entspricht den Werkseinstellungen des mGuard. Wenn mGuard-Geräte vor ihrer Verwendung mit mdm vorkonfiguriert werden, kann ein anderes Standardpasswort für *root* eingerichtet werden und die Datenbank muss mit dem folgenden Befehl aktualisiert werden:

```
java -Xmx1024m -jar mdm-server-1.17.x.jar update preferences.xml
```

Node *license*

Key *licenseFile*

Name und Pfad der Lizenzdatei.

Node *device*

Node *licenseServer*

- **Key *proto***
  Das für den Zugriff auf den Lizenzserver zu verwendende Protokoll (Standard: *http*). Diesen Wert auf keinen Fall ändern!
- **Key *address***
  Die Adresse des Lizenzservers (Standard: *online.license.innominate.com*). Diesen Wert auf keinen Fall ändern!
- **Key *port***
  Der für den Zugriff auf den Lizenzserver zu verwendende Port (Standard: 80). Diesen Wert auf keinen Fall ändern!
- **Key *reqPage***
  Das zum Anfordern von Lizenzen aufzurufende CGI-Skript (Standard: cgi-bin/autoreq.cgi). Diesen Wert auf keinen Fall ändern!
- **Key *refPage***
  Das zum Aktualisieren von Lizenzen aufzurufende CGI-Skript (Standard: cgi-bin/autorefresh.cgi). Diesen Wert auf keinen Fall ändern!
- **Key *reqProfKey***
  Das zum Anfordern von Profilschlüsseln aufzurufende CGI-Skript (Standard: cgi-bin/autodevcert.cgi). Diesen Wert auf keinen Fall ändern!
- **Key *reqUsername***
  Der zum Anfordern von Profilschlüsseln benötigte Benutzername. Einen Benutzernamen erhalten Sie vom Kundendienst von Phoenix Contact.
- **Key *reqPassword***
  Das zum Anfordern von Profilschlüsseln benötigte Passwort. Einen Benutzernamen erhalten Sie vom Kundendienst von Phoenix Contact.
- **Key *retries***
  Die Anzahl der Versuche zum Kontaktieren des Lizenzservers (Standard: 3). Diesen Wert auf keinen Fall ändern!
- **Key *timeout***
  Die Zeitabschaltung in Sekunden beim Kontaktieren des Lizenzservers (Standard: 60). Diesen Wert auf keinen Fall ändern!

Node *connection*

- **Key *useProxy***
  Hier können Sie konfigurieren, ob ein Proxy für die Verbindung mit dem Lizenzserver benötigt wird (Standard: *false*).
- **Key *proxyAddress***
  Die Adresse des Proxy zum Kontaktieren des Lizenzservers (Standard: *127.0.0.1*).
- **Key *proxyPort***
  Der für den Zugriff auf den Lizenzserver zu verwendende Port des Proxy (Standard: *3128*).
- **Key *proxyRequiresAuthentication***
  Boolean, das festlegt, ob der Proxy eine Authentifizierung erfordert (Standard: *false*).
- **Key *proxyAuthenticationUsername***
  Key *proxyAuthenticationPassword*
  Key *proxyAuthenticationRealm*
  Die zu verwendenden Anmeldedaten für den Fall, dass der Proxy eine Authentifizierung erfordert (Standard: leer).

Node *service*

Key *address*

Die IP-Adresse, die die Netzwerkschnittstelle bezeichnet, an der der Server auf Client-Verbindungen horcht. Bei Angabe von *0.0.0.0,* lauscht der Server an allen Schnittstellen (Standard: *127.0.0.1*).

Key *port*

Die Nummer des Ports, an dem der Server auf Client-Verbindungen horcht (Standard: *7001*).

Key *backlog*

Anzahl der zu speichernde Protokolleinträge (Standard: *50*).

Key *storage*

Der zu verwendende Speicher (Standard: *database*).

Node *security*

Key *keyStore*

Name und Pfad der Schlüsselspeicherdatei.

Key *keyStoreType*

Format des Schlüsselspeichers, entweder *JKS* (Java KeyStore) oder *PKCS12* (OpenSSL).

Key *keyStorePassword*

Passwort für die Schlüsselspeicherdatei. Der Sonderwert *ENV:PASSWORD_SSL* veranlasst den mdm-Server, beim Hochfahren dieses Passwort von der *Environment Variable PASSWORD_SSL* zu lesen; die Bezeichnung *PASSWORD_SSL* ist lediglich ein Beispiel und kann auch geändert werden.

Key *trustStore*

Name und Pfad der Truststore-Datei.

Key *trustStoreType*

Format des Truststores, entweder *JKS* (Java KeyStore) oder *PKCS12* (OpenSSL).

Key *trustStorePassword*

Passwort für die Truststore-Datei. Der Sonderwert *ENV:PASSWORD_SSL* veranlasst den mdm-Server, beim Hochfahren dieses Passwort von der *Environment Variable PASSWORD_SSL* zu lesen; die Bezeichnung *PASSWORD_SSL* ist lediglich ein Beispiel und kann auch geändert werden.

Node *session*

Key *maxInactiveInterval*

Die maximale Dauer der inaktiven Phase (in Sekunden), für die der Server die Sitzung zwischen den Client-Zugriffen offen lässt.

Ein negativer Wert oder Null (Standard) weist darauf hin, dass es für eine Sitzung keine Zeitabschaltung gibt.

Diese Zeitabschaltung wird erst zurückgesetzt, wenn Interaktion zwischen Client und Server stattfindet. Lokale Aktionen am Client wie Bildlauf in einer Tabelle oder Wechsel zwischen den Tabs für Gerät, Template, Pool oder VPN-Gruppe setzen die Zeitabschaltung nicht zurück.

Key *maxConcurrentSessions*

Die maximale Zahl gleichzeitiger Sitzungen (=angeschlossene Clients). Ein negativer oder Nullwert (Standard) weist darauf hin, dass durch die Lizenz eine Obergrenze für die Anzahl gleichzeitiger Sitzungen festgelegt ist.

Node *storage*

- **Node *database***
  - **Key *host***
    Die IP-Adresse (oder der Hostname) mit dem sich mdm verbinden sollte, um Zugriff auf die mdm-Client-Datenbank zu erhalten (Standard: *127.0.0.1*).
  - **Key *port***
    Der Port, den mdm für den Zugriff auf die Datenbank verwenden sollte (Standard: *5432*).
  - **Key *name***
    Name der Datenbank (Standard: *innomms*).
  - **Key *user***
    Benutzer der Datenbank (Standard: *innomms).*
  - **Key *password***
    Das Passwort für die Verbindung mit der Datenbank (Standard: *ENV:PASSWORD_DB*). Der Sonderwert *ENV:PASSWORD_DB* veranlasst den mdm-Server, beim Hochfahren dieses Passwort von der *Environment Variable ENV:PASSWORD_DB* zu lesen; die Bezeichnung *ENV:PASSWORD_DB* ist lediglich ein Beispiel und kann auch geändert werden.

    Achten Sie darauf, dass die Werte für *port*, *name*, *user* und *password* den während der Installation von mdm-Client angegebenen Werten entsprechen.

  - **Key *ssl***
    Sichere Verbindung zwischen mdm-Server und mdm-Client-Server aktivieren/deaktivieren. Hinweis: Für die Aktivierung dieser Option sind zusätzliche Installationsschritte erforderlich (Standard: *false).*

- **Node *update***
  - **Node *scheduler***

    Key *tries*

    Die maximale Versuche für den Upload oder Export einer Gerätekonfiguration. Wenn dieses Maximum erreicht ist, stellt mdm alle Versuche zum Laden einer Konfiguration in das Gerät ein (Standard: *5*).

    Key *timeout*

    Die maximale Anzahl an Sekunden, die vergehen, bis das Hochladen der Gerätekonfiguration abgebrochen wird. Nachdem die Zeitabschaltung erreicht ist, stellt mdm alle Versuche zum Laden einer Konfiguration in das Gerät ein (Standard: *600*).

Key *rescheduleDelay*

Anzahl der Sekunden zwischen den Upload-Versuchen (Standard: *45*).

– **Node *firmwareUpgradeScheduler***

Key *tries*

Maximale Anzahl der Verbindungsversuche von mdm, um von einem Gerät eine Rückmeldung zum Ergebnis eines Firmware-Upgrades zu erhalten. Wenn dieses Maximum erreicht ist, stellt mdm alle Versuche zur Kontaktaufnahme mit dem Gerät ein (Standard: *5*).

Key *timeout*

Maximale Anzahl der Sekunden die vergehen, bis mdm die Kontaktaufnahme zu einem Gerät für Rückmeldungen zum Ergebnis eines Firmware-Upgrades einstellt. Nach Erreichen der Zeitabschaltung zeigt mdm an, dass das Firmware-Upgrade fehlgeschlagen ist (Standard: *3600*).

Key *rescheduleDelay*

Intervall in Sekunden zwischen zwei Versuchen, eine Rückmeldung zum Ergebnis eines Firmware-Upgrades zu erhalten (Standard: *300*).

– **Node *ssh***

Key *connectTimeout*

Zeitabschaltung für die erstmalige SSH-Verbindung zu einem Gerät (Standard: *60*).

Key *socketTimeout*

Zeitabschaltung für die SSH-Verbindung TCP/IP-Buchse, z. B. Verbindung verloren (Standard: *120*).

Key *deadPeerDetectionTimeout*

Diese Zeitabschaltung wird aktiviert, wenn ein Gerät nicht auf einen am Gerät gestarteten Befehl antwortet (Standard: *120*).

– **Node *pull***

Node *export*

Key *directory*

Das Basisverzeichnis für den Export auf dem Server, wohin die Konfigurationsdateien exportiert werden sollten (zum Beispiel um eine Konfiguration zu ziehen). Hinweis: Die Konfigurationsdateien werden immer durch den Server exportiert, nicht durch den Client, d. h. der Client hat auf die Dateien keinen Zugriff. Der angegebene Pfad zum Verzeichnis sollte das entsprechende Format für das jeweilige Betriebssystem aufweisen (Standard: voreingestelltes temporäres Verzeichnis Ihrer Installation, z. B. */tmp* für Linux).

Key *filenames*

Eine durch Komma getrennte Liste von Benennungsschemen für Pull-Konfigurations-Exporte.
dbid: Eine eindeutige ID (automatisch zugewiesen) wird als Dateiname verwendet und die Dateien werden in das Basisverzeichnis der Exportdatei geschrieben.
serial: Die Seriennummer wird als Dateiname herangezogen und die Dateien werden in das Unterverzeichnis *serial/* des Basisverzeichnisses für den Export geschrieben
mgntid: Die Management-ID wird als Dateiname verwendet und die

Dateien werden in das Unterverzeichnis *mgntid/* des Basisverzeichnisses für den Export geschrieben (Standard: *dbid,serial,mgntid*).

Node *feedback*

Key *port*
Die mGuards können ihre Konfigurationen von einem HTTPS-Server ziehen. Da es sich bei dem HTTPS-Server um eine separate Anwendung handelt, erhält mdm keine direkten Rückmeldungen zum Ergebnis des Konfigurations-Pulls (*Configuration Pull*). Um den Rückmeldemechanismus zu aktivieren, muss mdm in den HTTPS-Servereinstellungen als Syslog-Server konfiguriert werden. mdm kann dann die Syslog-Meldungen des HTTPS-Servers empfangen und analysieren und zeigt das Ergebnis des Konfigurations-Pulls am Client an.
Es wird empfohlen, einen nichtpriveligierten Port (größer 1024) zu verwenden, sodass der Server ohne Administrator-/Root-Rechte verwendet werden kann (Standard: *7514*).

Node *auth*

Node *radius*

- **Key *numServers***
  Setzen Sie diese auf die Anzahl der RADIUS-Server, um die RADIUS-Authentifizierung zu aktivieren. Weiterführende Informationen siehe „Authentifizierung des Benutzers“ auf Seite 119. Wenn auf 0 gesetzt, ist die RADIUS-Authentifizierung deaktiviert (Standard: 0).
- **Key *timeout***
  Die Anzahl der Sekunden, die der mdm-Server auf eine Antwort vom RADIUS-Server wartet. Wird nur verwendet, wenn die RADIUS-Authentifizierung aktiviert ist (Standard: 5).
- **Key *retries***
  Die Anzahl der vom mdm-Server versendeten Anfragen an die RADIUS-Server. Wenn innerhalb der festgelegten Zeit keine Antwort empfangen wurde, wird die Authentifizierungsanforderung als fehlgeschlagen gewertet. Wird nur verwendet, wenn die RADIUS-Authentifizierung aktiviert ist (Standard: 3).
- **Key *nasIdentifier***
  Die NAS-Benennung, die in den vom mdm-Server versendeten RADIUS-Anfragen enthalten ist. Einige RADIUS-Server ignorieren dies, der Standardwert kann in diesem Fall unverändert bleiben (Standard: nas.identifier.example).

Node *0, 1, ...* (bis zur Anzahl der RADIUS-Server minus eins)

Jeder nummerierte Node steht für einen einzelnen RADIUS-Server.

- **Key *host***
  Hostname oder IP-Adresse des RADIUS-Servers (Standard: localhost).
- **Key *port***
  Der Port, an dem der RADIUS-Server auf eingehende Anfragen horcht (Standard: 1812).
- **Key *sharedSecret***

Der gemeinsame geheime Schlüssel zur Authentifizierung der RADIUS-Anfrage. Der gemeinsame geheime Schlüssel muss im RADIUS-Server konfiguriert werden (Standard: secret).

Node *locale*

Länder- und sprachenspezifische Einstellungen.

Standards stehen lassen, da diese Einstellungen noch nicht voll unterstützt werden!

Key *language*
Key *country*
Key *variant*

Node *logging*

Node *syslog*

- **Key *numReceivers***
  Setzen Sie diesen *Key* auf die Anzahl der Syslog-Empfänger, zu denen mdm Protokollmeldungen versendet. Wenn auf 0 gesetzt, ist die Protokollierung über Syslot deaktiviert (Standard: 1).
- **Key *logLevel***
  Der Mindestschweregrad der Meldungen für die Protokollierung über Syslog. Meldungen mit einem Schweregrad unterhalb des angegebenen Wertes werden unterdrückt (Standard: INFO).
  Folgende Schweregrade können verwendet werden:
  - *SEVERE* (höchster Schweregrad)
  - *WARNING*
  - *INFO*
  - *CONFIG*
  - *FINE*
  - *FINER*
  - *FINEST* (geringster Schweregrad)
- **Node** *0, 1, ...* (bis zur Anzahl der Syslog-Server minus eins)
  Jeder nummerierte Node steht für einen einzigen Syslog-Server.
  - **Key *host***
    Hostname oder IP-Adresse des Syslog-Servers (Standard: localhost).
  - **Key *port***
    Der Port, an dem der Syslog-Server auf eingehende Protokollmeldungen horcht (Standard: 514).

Node *configurationHistory*

Key *expireAfterDays*

Einträge im Konfigurationsverlauf, die älter als die angegebene Anzahl Tage sind, gelten automatisch als abgelaufen (werden aus dem Verlauf gelöscht).

Wird der Wert 0 verwendet, laufen Einträge im Konfigurationsverlauf nicht ab (Standard: 14).

Der Höchstwert beträgt 365250 (1000 Jahre). Wenn der Wert < 0 oder > 365250 oder keine ganze Zahl ist, wird der Standardwert von 14 angenommen.

Genauere Informationen zu Einträgen im Konfigurationsverlauf finden Sie in „Konfigurationsverlauf“ auf Seite 129.

Node *event*

Key *cleanupDays*

Einträge im *Persistent event log*, die älter als die angegebene Anzahl Tage sind, gelten automatisch als abgelaufen (werden aus dem Verlauf gelöscht).

Wird der Wert 0 verwendet, laufen Einträge im *Persistent event log* nicht ab (Standard: 200).

Der Höchstwert beträgt 365250 (1000 Jahre). Wenn der Wert < 0 oder > 365250 oder keine ganze Zahl ist, wird der Standardwert von 200 angenommen.

Genauere Informationen zu Einträgen im *Persistent event log* finden Sie in „Persistent Event Log“ auf Seite 25.

Node *CA*

Diese Einstellungen werden nur benötigt, wenn eine CA verwendet wird.

Key *type*

Der Typ der zu verwendenden CA. Gültige Werte sind mdm-CA zur Verwendung der mdm CA oder SCEP für die Kommunikation mit einer CA über SCEP (Standard: mdm-CA). Weiterführende Informationen zu SCEP siehe „Maschinenzertifikate“ auf Seite 120.

Key *protocol*

Das für die Verbindung mit der mdm CA verwendete Protokoll. Gültige Werte sind http oder https (Standard: https). Bei Verwendung der mdm CA sollte nur *https* verwendet werden, da die mdm CA sich für die Authentifizierung auf die Sicherheit der Transportschicht verlässt. SCEP enthält Mechanismen zur Authentifizierung der Anwendungsschicht, sodass mit SCEP normalerweise http verwendet wird.

Key *host*

Hostname oder IP-Adresse des CA-Servers (Standard: *localhost*).

Key *port*

Der Port, an dem der CA-Server auf eingehende Anfragen lauscht (Standard: *7070*). Wird hier 0 angegeben, dann wird der Default-Port für https oder http verwendet.

Key *requestDirectory*

Der Pfad innerhalb der URL, den der mdm-Server für Zertifizierungsanfragen verwendet (Standard: request). Bei Verwendung der mdm CA muss request verwendet werden. Bei Verwendung von SCEP in der Dokumentation des CA-Servers nachschlagen. Wird beispielsweise der Microsoft Windows Server 2008 CA verwendet, sollte CertSrv/mscep/mscep.dll angegeben werden.

Key *revocationDirectory*

Der Pfad innerhalb der URL, den der mdm-Server für Zertifkatssperranfragen verwendet (Standard: revoke). Bei Verwendung der mdm CA muss revoke verwendet werden. Bei Verwendung von SCEP nicht anwendbar.

Key *rsaKeySize*

Größe des RSA-Modulus (in Bit), dass der mdm-Server zur Erstellung von RSA-Schlüsselpaaren verwendet (Standard: 2048).

Node *SCEP*

– **Key *name***

  Der in SCEP-Anfragen verwendete Name der Instanz (Standard: mdm). Hinweis: Einige CAs ignorieren den Namen der Instanz, verlangen aber trotzdem einen nichtleeren Wert.

Node *httpServer*

Diese Einstellungen sind nur erforderlich, wenn der mdm-Server als RESTful Server gestartet werden soll.

ACHTUNG: Unbefugter Zugriff über HTTP

Der RESTful-Server akzeptiert Anfragen ohne Authentifizierung oder Verschlüsselung.

Um einen unbefugten Zugriff auf den RESTful-Server über HTTP über die konfigurierte IP-Adresse und den Port zu vermeiden, konfigurieren Sie die Firewall entsprechend.

Key *start*

RESTful-Services des mdm-Servers können aktiviert (Wert: *true*) oder deaktiviert (Wert: *false*) werden. Standardwert: *false*.

Key *address*

Der Hostname oder die IP-Adresse, auf die der mdm RESTful-Server auf eingehende Anfragen lauscht (Standard: *127.0.0.1*).

Wenn Sie *0.0.0.0* angeben, lauscht der mdm RESTful-Server auf alle Schnittstellen.

Key *port*

Der Port, auf dem der mdm RESTful-Server auf eingehende Anfragen lauscht (Standard: *7080*).

10.2 mdm Zertifizierungsstelle (CA)

mdm stellt eine eigene Zertifizierungsstelle (CA) zur Verfügung. Die mdm CA ist eine separate Serverinstanz. Über die CA werden Maschinenzertifikate für den mGuard ausgegeben, zum Beispiel für die Verwendung von X.509-Authentifizierung für Ihre VPN-Tunnel. Informationen zur Anforderung von Zertifikaten für einen mGuard über die CA finden Sie in „VPN-Verbindungen konfigurieren“ auf Seite 103 und „X.509-Zertifikate verwalten“ auf Seite 120.

Wenn Sie die VPN-Tunnel nicht mit mdm konfigurieren oder wenn Sie Ihre eigene CA bzw. voreingestellte Schlüssel (PSK) verwenden möchten, wird die mdm CA nicht benötigt.

10.2.1 Übersicht

Die mdm CA dient der Ausgabe von Zertifikaten, die vom mdm-Server für die Verwendung als Maschinenzertifikate für mGuards angefordert werden.

Die mdm CA wird als eigenständiger Server implementiert. Dessen Schnittstelle mit dem mdm-Server ist ein servletbetriebener Webserver (HTTP), der mit SSL (HTTPS) gesichert werden und eine Authentifizierung des Clients erzwingen kann. Vor allem in Produktionsumgebungen empfiehlt Phoenix Contact nachdrücklich die Verwendung von HTTPS mit Client-Authentifizierung, da nur so gewährleistet ist, dass die mdm CA Zertifikate nur an authentifizierte Clients ausstellt.

Die Konfigurationsdatei des mdm CA-Servers ermöglicht die Konfiguration verschiedener Schlüsselspeicher (Isolation) für die Ausstellung von Zertifikaten (CA-Schlüsselspeicher) und für die SSL-Authentifizierung (SSL-Schlüsselspeicher, SSL-Truststore). Auf diese Weise ist gewährleistet, dass der private Schlüssel der CA (der zur Ausgabe von Maschinenzertifikaten vorgesehen ist) nicht versehentlich für die SSL-Authentifizierung benutzt wird.

Die mdm CA speichert alle benötigten Informationen in einer mdm-Client-Datenbank. Die Kommunikation zwischen der mdm CA und der Datenbank sollte ebenfalls über SSL abgesichert werden.

Alle benötigten Schlüssel zur Absicherung der Kommunikation zwischen mdm CA, mdm Server und der Datenbank müssen angelegt, im Dateisystem installiert und in der Datei *ca-preferences.xml* der CA-Komponente und auch in der Datei *preferences.xml* auf dem mdm-Server konfiguriert werden.

Für die Ausstellung und Verwaltung von Schlüsseln und Zertifikaten gibt es zahlreiche Werkzeuge. Im vorliegenden Dokument wird die Verwendung von *OpenSSL* -Werkzeugen beschrieben, die für Linux und Windows zur Verfügung stehen (z. B. als eigenständige

Binary oder als Teil des *cygwin*-Pakets). Die Werkzeuge zur Erstellung von Zertifikaten, Schlüsseln und Schlüsselspeichern brauche nicht auf dem Zielsystem der mdm CA installiert zu werden.

Aus Sicherheitsgründen wird grundsätzlich die Verwendung aktueller OpenSSL-Versionen ab Version 3 empfohlen.

Zertifikatssperrlisten (CRLs) werde nicht von mGuard , sondern erst ab mGuard Firmware 5.0 unterstützt. Bei Verwendung von mGuard wird empfohlen, Informationen zu CRL-Distribution Points (CDP) einzubeziehen, die beim Ausrollen einer PKI bereits im Zertifikat enthalten sind, da dann ein Austausch der Zertifikate bei der Aktualisierung auf eine neuere mGuard-Firmware nicht notwendig ist.

10.2.2 mdm CA-Server (Datei *ca-preferences.xml*)

In diesem Kapitel wird der Inhalt der Konfigurationsdatei *ca-preferences.xml* beschrieben. Passen Sie die *ca-preferences.xml* ggf. an Ihre Umgebung an.

Node *certificateFactory*

Key *validityPeriodDays*

Anzahl der Tage, an denen durch die mdm CA ausgegebene Zertifikate gültig sind (d. h. jedes Zertifikat ist für die angegebene Anzahl Tage gültig, beginnend am Tag der Ausgabe).

Key *certTemplate*

Name und Pfad einer Zertifikatdatei, die als Vorlage für neue VPN-Zertifikate der mdm CA verwendet werden soll.

Key *keyStore*

Name und Pfad der Schlüsselspeicherdatei (siehe Kapitel 10.2).

Key *keyStoreType*

Format des Schlüsselspeichers, entweder *JKS* (Java KeyStore) oder *PKCS12* (OpenSSL).

Key *keyStorePassword*

Passwort für die Schlüsselspeicherdatei (siehe Kapitel 10.2). Der Sonderwert *ENV:PASSWORD_CA* veranlasst den mdm-Server, beim Hochfahren dieses Passwort von der *Environment Variable PASSWORD_CA* zu lesen; die Bezeichnung *PASSWORD_CA* ist lediglich ein Beispiel und kann auch geändert werden.

Key *keyAlias*

Name des Eintrags im Schlüsselspeicher, in dem der private Schlüssel und das damit verbundene öffentliche Schlüsselzertifikat zu finden sind (der Schlüsselspeicher kann mehr als einen Eintrag enthalten) – der Standardeintrag passt zu dem aus den in Kapitel 10.2.2 beschriebenen Beispielskripten. Mit dem folgenden Befehl können die Alias-Namen in einer *.p12*-Datei gefunden werden:

```
openssl pkcs12 -in <filename>.p12 -nodes
```

Der Alias wird in der Ausgabe als *Friendly Name* dargestellt.

Mit dem folgenden Befehl können die Alias-Namen in einer *JKS*-Datei gefunden werden:

```
keytool -list <filename>
```

Key *keyPassword*

Passwort zur Dekodierung des im Schlüsselspeicher enthaltenen privaten RSA-Schlüssels (siehe Eintrag *keyAlias*), der Sonderwert *ENV:PASSWORD_CA* veranlasst die mdm CA, beim Hochfahren dieses Passwort von der *Environment Variable PASSWORD_CA* zu lesen; die Bezeichnung *PASSWORD_CA* ist lediglich ein Beispiel und kann auch geändert werden.

Key *crlExportDirectory*

Der Pfad zu dem Verzeichnis, das von der mdm CA für den Export der Dateien mit CRLs (Zertifikatssperrlisten) verwendet wird. Jede Datei enthält eine mit PEM codierte X.509 CRL der gesperrten Zertifikate einer einzigen Ausgabestelle. Der Name jeder CRL-Datei besteht aus dem Hashwert der Ausgabestelle mit einer *crl*-Erweiterung, z. B.

5E84D566026616ED32169580A913661499FA6B03.crl. Achten Sie darauf, dass auf die in diesem Verzeichnis gespeicherten Dateien von den mGuards aus zugegriffen werden kann. Navigieren Sie zur Konfiguration der CRL URL am mGuard im *Device* oder *Template properties Ddialog* (Geräte- oder Template-Eigenschaften) zu **Authentication » Certificates » CRLs** (nur mGuard ab Version 5.0) und fügen Sie in die CRL-Tabelle die korrekte URL ein. Weiterführende Informationen zum Sperren von Zertifikaten finden Sie in Kapitel 7.4.1 (Standard: *security/crl).*

Key *crlUpdatePeriodMinutes*

Zeitintervall für den Export der CRLs zum *crlExportDirectory* in Minuten. Bei Sperrung eines Zertifikats wird sofort eine CRL exportiert. Darüber hinaus werden CRLs regelmäßig entsprechend dem angegebenen Zeitintervalle exportiert.

Key nextUpdatePeriodDays

Die im Feld *Next Update* in exportierte CRLs eingetragene Anzahl der verbleibenden Tage. Dieses Feld teilt dem mGuard, der die CRL herunterlädt, mit, wann diese als veraltet zu betrachten ist. Sie sollte daher deutlich höher sein als *crlUpdatePeriodMinutes* (beachten, dass *crlUpdatePeriodMinutes* in Minuten und *nextUpdatePeriodDays* in Tagen angegeben wird).

Node *storage*

- **Node *database***
  - **Key *host***
    Die IP-Adresse (oder der Hostname), mit der/m sich die mdm CA verbinden sollte, um Zugriff auf die mdm-Client-Datenbank zu erhalten (Standard: *127.0.0.1*).
  - **Key *port***
    Der Port, den die CA mdm für den Zugriff auf die Datenbank verwenden sollte (Standard: *5432*).
  - **Key *name***
    Name der Datenbank (Standard: *mdmca*).
  - **Key *user***
    Benutzer der Datenbank (Standard: *mdmca).*
  - **Key *password***
    Das Passwort für die Verbindung mit der Datenbank. Der Standardwert *ENV:PASSWORD_DB* veranlasst den mdm CA-Server, beim Hochfahren dieses Passwort von der *Environment Variable ENV:PASSWORD_DB* zu lesen; die Bezeichnung *ENV:PASSWORD_DB* ist lediglich ein Beispiel und kann auch geändert werden.

Achten Sie darauf, dass die Werte für *port*, *name*, *user* und *password* den während der Datenbankinitialisierung angegebenen Werten entsprechen.

  - **Key *ssl***
    Sichere Verbindung zwischen mdm CA und mdm-Client-Server aktivieren/deaktivieren. Für die Aktivierung sicherer Verbindungen den Wert *true* verwenden.
  - **Key *logLevel***
    Nur für interne Verwendung. Diesen Wert nicht ändern (Standard: *0*).
  - **Node *security***

    Key *trustStore*

    Name und Pfad der Truststore-Datei, die das vertrauenswürdige Zertifikat des Datenbankservers enthält.

Key *trustStoreType*

Format des Truststores, entweder *JKS* (Java KeyStore) oder *PKCS12* (OpenSSL).

Key *trustStorePassword*

Passwort für die Truststore-Datei (siehe Kapitel 10.2). Der Sonderwert *ENV:PASSWORD_SSL* veranlasst den mdm-Server, beim Hochfahren dieses Passwort von der *Environment Variable PASSWORD_SSL* zu lesen; die Bezeichnung *PASSWORD_SSL* ist lediglich ein Beispiel und kann auch geändert werden.

Node *certificationRequest-Handler*

Key *maxRequestLength*

Anzahl der Bytes, die Zertifikatanfragen PKCS#10 höchstens haben dürfen; werden zur Verteidigung gegen einfache DoS-Angriffe abgewiesen (Standard: *102400*).

Node *revocationRequest-Handler*

Key *maxRequestLength*

Anzahl der Bytes, die Sperranfragen maximal haben dürfen; werden zur Verteidigung gegen einfache DoS-Angriffe abgewiesen (Standard: *10240*).

Node *httpServer*

Key *host*

IP-Adressen oder Hostnamen der Ports, an denen mit der Servlet-Schnittstelle der CA gehorcht wird; Wert *0.0.0.0* bedeutet Horchen an jedem Port (Standard: *127.0.0.1*).

Key *port*

Die Nummer des Ports, an dem der Server auf ankommende Verbindung horchen soll (Standard: *7070*).

Key *minThreads*

Mindestanzahl der instanziierten HTTP-Serverthreads, die die mdm CA in ihrem Pool halten kann (Standard: *2*).

Key *lowThreads*

Nur für interne Verwendung. Nicht ändern.

Key *maxThreads*

Höchstzahl der instanziierten HTTP-Serverthreads, die die mdm CA in ihrem Pool halten kann (Standard: *5*).

Key *protocol*

Das von der Servlet-Schnittstelle der mdm CA zu verwendende Protokoll, entweder *http* oder *https.* Um eine sichere Kommunikation zu ermöglichen sollte *https* verwendet werden.

Node *https*

Die Konfiguration in diesem Node wird nur verwendet, wenn das *Protokoll* im Node *httpServer https* ist.

– **Key *keyStore***
  Name und Pfad der Schlüsselspeicherdatei.
– **Key *keyStoreType***

Format des Schlüsselspeichers, entweder *JKS* (Java KeyStore) oder *PKCS12* (OpenSSL).

– **Key *keyStorePassword***

  Passwort für die Schlüsselspeicherdatei. Der Sonderwert *ENV:PASSWORD_SSL* veranlasst den mdm-Server, beim Hochfahren dieses Passwort von der *Environment Variable PASSWORD_SSL* zu lesen; die Bezeichnung *PASSWORD_SSL* ist lediglich ein Beispiel und kann auch geändert werden.

– **Key *keyPassword***

  Das zum Dekodieren des privaten SSL-Schlüssels im Schlüsselspeicher für den HTTPS-Server verwendete Passwort.

– **Key *clientAuth***

  Boolescher Wert, *true* bedeutet, dass sich die Clients ebenfalls (nicht nur der Server) über SSL authentifizieren müssen, *false* bedeutet, dass die Clients sich nicht zu authentifizieren brauchen. Dieser Wert sollte auf *true* gesetzt sein.

– **Key *trustStore***

  Name und Pfad der Truststore-Datei, die vertrauenswürdige Zertifikate für die SSL-Verbindung von den Clients enthält.

– **Key *trustStoreType***

  Format des Truststores, entweder *JKS* (Java KeyStore) oder *PKCS12* (OpenSSL).

– **Key *trustStorePassword***

  Passwort für die Truststore-Datei (siehe Kapitel 10.2). Der Sonderwert *ENV:PASSWORD_SSL* veranlasst den mdm-Server, beim Hochfahren dieses Passwort von der *Environment Variable PASSWORD_SSL* zu lesen; die Bezeichnung *PASSWORD_SSL* ist lediglich ein Beispiel und kann auch geändert werden.

Node *logging*

Key *file*

Der Basisname der von der mdm CA erstellten rotierten Protokolldatei, der Dateiname kann mit einer relativen oder absoluten Pfadbezeichnung verwendet werden. Das Suffix *n.log* wird an den Basisnamen angefügt, wobei *n* für einen nicht-negativen Integer steht.

Key *limit*

Maximale Anzahl an Bytes, die eine Log-Datei der mdm CA erreichen kann. Wenn sie über diese Zahl hinauswächst, wird sie rotiert.

Key *count*

Maximale Anzahl rotierter Log-Dateien, die die mdm CA halten kann.

Key *level*

Definiert die Granularität der Protokollmeldungen, die die mdm CA produzieren kann. Akzeptable Werte sind:

– *OFF*
– *SEVERE* (höchster Wert)
– *WARNING*
– *INFO*
– *CONFIG*
– *FINE*
– *FINER*
– *FINEST* (niedrigster Wert)
– *ALL*

11 Glossar

Admin/Netadmin (am mGuard)

Der Benutzer *admin* (mGuard-Benutzer) kann alle Einstellungen am mGuard ändern, der Benutzer *netadmin* kann dagegen nur lokale Variablen ändern.

AIA

Die Zertifikaterweiterung Authority Information Access (AIA) zeigt an, wie auf CA-Informationen und Leistungen für den Aussteller des Zertifikats, in dem die Erweiterung erscheint, zugegriffen werden kann. Mit einer solchen Erweiterung wird der OSCP-Server identifiziert, der die Informationen zum aktuellen Sperrstatus des Zertifikats bereitstellt. mdm unterstützt die Einbeziehung einer AIA-Erweiterung, die die URL eines Einzel-OSCP-Servers enthält. Ausführliche Informationen zur AIA-Erweiterung siehe RFC-3280.

CDP

Die Zertifikaterweiterung CRL Distribution Points (CDP) gibt an, wie CRL-Informationen für das Zertifikat, in dem die Erweiterung enthalten ist, abgeholt werden. mdm unterstützt die Erstellung von Zertifikaten mit der CDP-Erweiterung mit einer einzigen *http://*-URL, die dort enthalten ist. Die URL gibt das Download-Verzeichnis der eigentlichen CRL an. Weiterführende Informationen zu CRL Distribution Poins siehe RFC 3280.

CRL

Eine Zertifikatssperrliste (CRL) wird durch eine Zertifizierungsstelle (CA) ausgegeben, um (öffentlichen) Zugriff auf den Sperrstatus der von ihr ausgegebenen Zertifikate zu ermöglichen. Eine CRL ist eine Liste der gesperrten Zertifikate, die durch ihre Seriennummer gekennzeichnet sind. Sobald ein Zertifikat gesperrt ist, wird es als ungültig gewertet. Eine Sperrung ist insbesondere dann notwendig, wenn damit zusammenhängende private Schlüssel beschädigt sind. Weiterführende Informationen zu CRLs siehe RFC 3280.

Lokale (mGuard) Variablen

Lokale mGuard-Variablen werden nicht durch mdm, sondern nur lokal durch den *Netadmin* am mGuard verwaltet. In mdm (im *Template properties dialog* – Template-Eigenschaften oder dem *Device properties dialog* – Geräte-Eigenschaften) kann jede Variable durch Auswahl von **Local** als Wert als lokale Variable definiert werden.

Geerbter Wert

Geräte oder Templates, die ein übergeordnetes Template verwenden, „erben“ die im übergeordneten Template festgelegten Werte. Ob der geerbte Wert in den erbenden Geräten und Templates überschrieben werden kann, hängt von den Berechtigungseinstellungen ab.

Management-ID

Eine eindeutige lokale, von der physischen Hardware unabhängige Benennung für jedes einzelne Gerät, im Gegensatz zu einer Kennzeichnung am eigentlichen, physischen Gerät wie der Seriennummer.

OCSP

Das Onlinezertifikats-Statusprotokoll (OSCP) gibt das Meldungsformat für einen Dienst an, der auf Anfrage mit Informationen zum tatsächlichen Sperrstatus zu einzelnen Zertifikaten antwortet. Ein solcher Dienst ist konventionell in einem HTTP-Server eingebettet.

OSCP-Server müssen daher HTTP als Transportschicht für die OSCP-Meldungen verwenden. Ein solcher OSCP-Server wird durch einige Zertifizierungsstellen als Alternative zu oder Ersatz für CLRs betrieben. Weiterführende Informationen zu OCSP siehe RFC 2560.

Berechtigungen

Die Berechtigungen eines Templates bestimmen, ob der Benutzer, der ein erbendes Gerät oder Template konfiguriert, Einstellungen des übergeordneten Templates ändern/überschreiben kann.

Reguläre Ausdrücke

Reguläre Ausdrücke sind Text-Strings, die zu Teilen eines Feldes mit Zeichen, Zahlen, Wildcards und Metazeichen passen. In mdm können reguläre Ausdrücke zum Filtern von Geräte-, Template- oder Pool-Tabellen verwendet werden. Weiterführende Informationen zu regulären Ausdrücken siehe *www.regular-expressions.info* (2017-01-30).

Template

Ein Satz mGuard-Variablen mit den entsprechenden Werten und Berechtigungen. Das Template kann durch ein Gerät oder ein anderes Template verwendet (d. h. geerbt) werden. Eine Änderung am Template wirkt sich auf alle erbenden Geräte und Templates aus, je nach Zugriffsberechtigungen. Das Template wird nur in mdm, nicht am mGuard verwendet. Siehe auch *„Geerbter Wert“* und *„Berechtigungen“*.

X.509-Zertifikate

Digitale Zertifikate sind nach der Norm X.509 der ITU-T anzugeben. Ein Profil dieser Norm wurde als RFC 3280 veröffentlicht. Derartige Zertifikate bestätigen die Identität einer Entität. Das Zertifikat enthält den öffentlichen Schlüssel der Entität und eine elektronische Signatur von der Zertifizierungsstelle (CA). X.509-Zertifikate sind hierarchisch organisiert: Eine Root-CA erstellt einen selbstsignierten Vertrauensanker, der als solcher für Anwendungen konfiguriert werden muss, die digitale Signaturen oder Zertifikate überprüfen. Die Identität und Vertrauenswürdigkeit der zwischengeschalteten CAs wird mit einem CA-Zertifikat bestätigt, das von der Root-CA bzw. der davorliegenden zwischengeschalteten CA ausgegeben worden ist. Die Identität der End-Entitäten wird mit Zertifikaten bestätigt, die von der untersten CA ausgegeben worden sind. Jedes Zertifikat kann Erweiterungen für die Einbeziehung arbiträrer zusätzlicher Informationen enthalten. mdm unterstützt die Erstellung von End-Entitätszertifikaten für Endpunkte von VPN-Verbindungen und die optionale Einbeziehung der CDP- und AIA-Erweiterungen. Weiterführende Informationen zu digitalen Zertifikaten siehe RFC 3280.

Bitte beachten Sie folgende Hinweise

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.com/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

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
Email: info@phoenixcontact.com
phoenixcontact.com

111024_de_03
Item No. –03