



FL MGuard DM UNLIMITED Upgrade auf Version mdm 1.13.x

Anwenderhinweis
AH DE MDM UPGRADE

Anwenderhinweis

FL MGuard DM UNLIMITED Upgrade auf Version mdm 1.13.x

AH DE MDM UPGRADE, Revision 08

2021-05-12

Dieser Anwenderhinweis ist gültig für das Produkt FL MGuard DM UNLIMITED.



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

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen
Geschäftsbedingungen finden Sie im Internet unter: phoenixcontact.com.

1 FL MGuard DM UNLIMITED auf Version 1.13.x upgraden



Dokument-ID: 107821_de_08
 Dokument-Bezeichnung: AH DE MDM UPGRADE
 © PHOENIX CONTACT 2021-05-12



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

Inhalt dieses Dokuments

In diesem Dokument wird beschrieben, wie Sie eine *mGuard device manager* (mdm) auf Version 1.13.x upgraden können.

1.1 Einleitung

1.1	Einleitung.....	1
1.2	Allgemeine Hinweise	2
1.3	Bekannte Probleme	3
1.4	Betriebssystem: Microsoft Windows	5
1.5	Betriebssystem: Ubuntu Linux	14
1.6	Batch-Dateien und Shell-Skripte	25
1.7	mdm 1.13.x Installer for Windows	26
1.8	Paketverwaltung von Ubuntu	31

Seit den mdm-Versionen 1.5.2 (Windows) und 1.7.0 (Windows und Ubuntu) können der *mGuard device manager* sowie Komponenten von mdm und Drittanbietern automatisch über den *mdm Installer for Windows* bzw. die Paketverwaltung von Ubuntu installiert und aktualisiert werden.

Sollte Ihr System die in Tabelle 1-1 und Tabelle 1-2 angegebenen System-Anforderungen nicht erfüllen, müssen von *mdm Server- und -CA-Serverdatenbanken* entweder Dumps erstellt und in ein neu installiertes mdm 1.13.x importiert werden, oder die installierte mdm-Version muss schrittweise auf mdm 1.13.x aktualisiert werden.

In den folgenden Kapiteln wird beschrieben,

- wie Sie Ihre mdm-Installation und Komponenten von Drittanbietern aktualisieren und
- wie Sie Ihre vorhandene mdm-Datenbank mittels Batch-Dateien und Shell-Skripten in Windows- und Linuxsysteme migrieren können (siehe Kapitel 1.6).

Mehr Informationen zur Installation, Konfiguration und Nutzung des *mGuard device manager* (mdm) 1.13.x finden Sie im mdm-Benutzerhandbuch (Version 1.13.x), das [online](https://phoenixcontact.net/produkt/2981974) oder als PDF-Version im PHOENIX CONTACT Webshop (phoenixcontact.net/produkt/2981974) erhältlich ist.

1.2 Allgemeine Hinweise



ACHTUNG: Sichern Sie wichtige Dateien und Datenbanken

Fertigen Sie von folgenden Dateien und Datenbanken Sicherheitskopien an, um Datenverlust während des Upgrade-Prozesses von mdm zu vermeiden:

- aktuelle mdm-Server- und mdm-CA-Server-Datenbanken
- *preferences.xml* und *ca-preferences.xml*

In diesen Dateien sind in der Regel individuelle Parameter konfiguriert, die nach erfolgtem Upgrade erneut übernommen werden sollen.

- *mdm-Lizenzdatei*

Sie benötigen die Lizenzdatei, um den mdm in vollem Umfang zu nutzen.



ACHTUNG: Inkompatibilität von PostgreSQL-Datenbanken

Das Upgrade von einer älteren Version auf mdm 1.13.x erfordert Änderungen an der unterstützten PostgreSQL-Datenbank, die nicht rückgängig gemacht werden können. Nach Durchführung dieser Änderungen kann mit älteren Versionen nicht mehr auf die Datenbank zugegriffen werden.



ACHTUNG: Java Runtime Environment (JRE) wird deinstalliert

Ab Version mdm 1.11.x verwendet mdm die Java-Plattform *OpenJDK* und nicht mehr das *Java Runtime Environment (JRE)*. Der *mdm 1.11.x Installer for Windows* installiert automatisch die benötigte Version von *OpenJDK* und **deinstalliert** vorhandene Versionen des *Java Runtime Environments*.



Die Migration der mdm-Installationen mittels **Batch-Dateien/Shell-Skripten** stellt lediglich die Datenbanken wieder her, von denen Dumps erstellt und importiert wurden. Jede andere Installationsdaten (z. B. Pull-Server-Zertifikat und Konfigurationsdateien) müssen von Hand in die neue Installation einkopiert werden.



Die mitgelieferten Batch-Dateien bzw. Shell-Skripte können nur bei mdm Standardinstallationen verwendet werden (überprüfen Sie die voreingestellten Bezeichnungen in den mitgelieferten Dateien *preferences.xml* und *ca-preferences.xml*).



Der mdm-Server (und der CA-Server) werden während der Erstellung des Datenbank-Dumps angehalten und neu gestartet.

1.3 Bekannte Probleme

1.3.1 CA-Datenbankmigration mittels gleicher CA-Zertifikatattribute

Problemstellung

Wenn die mdm CA-Datenbankmigration (mittels der mitgelieferten Skripte für Datenbank- und -import) in eine neu installierte mdm Version 1.13.x unter Windows

- von einem anderen Betriebssystem **oder**
- von einer installierten mdm Version < 1.12.0

unter Verwendung derselben CA-Zertifikatattribute in der neuen mdm 1.13.x-Installation durchgeführt wird, kann der mdm CA-Server nicht hochgefahren werden.

Lösung

Stellen Sie während der Installation von mdm 1.13.x nicht alle CA-Zertifikatattribute zur Verfügung, die mit den Attributen früherer Installation identisch sind (fügen Sie *Common Name* beispielsweise ein Suffix hinzu).

1.3.2 Verzeichnisstruktur und Passwortschutz des HTTP-Servers in Ubuntu und Windows verschieden

Problemstellung

Der *mdm Installer for Windows* und die Paketverwaltung von Ubuntu erstellen für den HTTP-Server unterschiedliche Verzeichnisstrukturen:

- Unter Windows ist der Zugriff auf den Server durch ein Passwort geschützt und es werden die Verzeichnisse „atv“, „crl“ und „fw“ verwendet, wobei „fw“ als Root-Verzeichnis definiert ist.
- Unter Ubuntu ist der Zugriff auf den Server **nicht** passwortgeschützt und das Root-Verzeichnis des Servers wird zum Speichern von Pull-Konfigurationsdateien, Firmware-Upgradepaketen und CRL-Dateien verwendet.

Lösung

Gehen Sie wie folgt vor, um den Zugriff unter Ubuntu durch ein Passwort zu schützen:

- a) Bearbeiten Sie die Datei „*/var/www/mdm/.htaccess*“, heben Sie die Auskommentierung der vorhandenen Zeilen auf und bearbeiten Sie diese:

```
AuthType Basic
AuthName "username"
AuthUserFile /etc/mdm/mdm-webbase/.htpasswd
Require valid-user
```

Setzen Sie unter „*username*“ den Benutzernamen ein, für den Sie den Zugriff gestatten wollen.

- b) Erstellen Sie in der Datei „*/etc/mdm/mdmwebbase/.htpasswd*“ mit dem Apache-Tool „*htpasswd*“ (als *sudo*) das gewünschte Benutzerpasswort:

```
sudo htpasswd -c /etc/mdm/mdm-webbase/.htpasswd username
```

Setzen Sie unter „*username*“ den Benutzernamen ein, für den Sie den Zugriff gestatten wollen. Sie werden zur Eingabe des gewünschten Passworts aufgefordert.

Gehen Sie wie folgt vor, um unter Ubuntu und Windows die gleiche Verzeichnisstruktur zu nutzen:

- a) Bearbeiten Sie die Datei „*/etc/apache2/sites-available/mdm-webbase-ssl.conf*“: Definieren Sie die Aliases „**atv**“ und „**crl**“. Beispielsweise:

```
Alias „/atv/“ „/var/www/mdm/“
Alias „/atv“ „/var/www/mdm/“
```

```
Alias „/crl“ „/etc/mdm/security/crl“  
Alias „/crl“ „/etc/mdm/security/crl“  
<Directory /etc/mdm/security/crl/>  
    Options +Indexes -FollowSymLinks +Multiviews  
    AllowOverride All  
    Require all granted  
</Directory>
```



Dadurch wird die tatsächliche Verzeichnisstruktur im System nicht verändert, aber bereits konfigurierte mGuards, die die Verzeichnisse **atv** und **crl** erwarten, können damit Pull-Konfigurationen und CRL-Dateien erfolgreich herunterladen.
Wenn Sie zusätzlich dieselbe Verzeichnisstruktur im System haben wollen, müssen Sie die entsprechenden Verzeichnisse erstellen und in **mdm-webbase-ssl.conf** die Zugriffsberechtigungen für jedes Verzeichnis erstellen.

1.4 Betriebssystem: Microsoft Windows

mdm 1.13.x kann nur auf unterstützten Microsoft Windows-Systemen installiert werden, wenn die notwendigen Voraussetzungen erfüllt sind (siehe Tabelle 1-1 auf Seite 6).



ACHTUNG: Windows Defender muss deaktiviert werden!

Vor der **Installation oder Aktualisierung (Upgrade)** von mdm **muss** der Microsoft *Windows Defender* auf dem Windows-System deaktiviert werden.

Bei aktiviertem Microsoft *Windows Defender* kann die bestehende mdm-Installation ansonsten irreparabel beschädigt werden.

Nachdem die Installation/das Upgrade von mdm erfolgreich abgeschlossen wurde, kann der Microsoft *Windows Defender* erneut aktiviert werden.



ACHTUNG: Fehlerhaft installiertes *Microsoft Visual C ++ 2017 Redistributable Package (x64)* kann die aktuelle mdm-Installation unbrauchbar machen

Vor der **Installation oder Aktualisierung (Upgrade)** von mdm muss *Microsoft Visual C ++ 2017 Redistributable Package (x64)* (oder neuer) erfolgreich auf dem Windows-System installiert worden sein.

Download: https://aka.ms/vs/16/release/VC_redist.x64.exe

HINWEIS: Es ist möglich, dass der angegebene Link nicht mehr gültig ist. Stellen Sie in jedem Fall sicher, dass die richtige Version verwendet wird!

Voraussetzung: Alle aktuellen Windows-Update-Packages müssen zunächst installiert werden.

Stellen Sie sicher, dass das Paket ohne Warnungen oder Fehlermeldungen installiert wurde.

Wenn das Paket erfolglos oder unvollständig installiert wurde, kann die mdm-Installation fehlschlagen und bestehende mdm-Installationen unbrauchbar machen.



ACHTUNG: Alle aktuellen Windows-Update-Pakete müssen installiert sein

Vor der **Installation oder Aktualisierung (Upgrade)** von mdm- oder Windows-Komponenten müssen alle verfügbaren Update-Pakete für das Windows-Betriebssystem **erfolgreich** installiert worden sein.

Achtung: Es könnte notwendig sein, wiederholt zu überprüfen, ob alle notwendigen Pakete installiert worden sind. In manchen Fällen werden einige der Pakete während der ersten oder sogar zweiten Windows-Update-Session nicht installiert.

Sollte Ihr System die in Tabelle 1-1 angegebenen System-Anforderungen nicht erfüllen, müssen von *mdm Server- und -CA-Serverdatenbanken* entweder Dumps erstellt und in ein neu installiertes mdm 1.13.x importiert werden, oder die installierte mdm-Version muss schrittweise auf mdm 1.13.x aktualisiert werden.

Systemanforderungen

Tabelle 1-1 Systemanforderungen (Microsoft Windows)

	mdm Client	mdm Server	mdm CA
Unterstütztes Betriebssystem	<ul style="list-style-type: none"> - Windows Server 2016 - Windows Server 2012 R2 - Windows 10 (nur mdm Client) - Windows 7 (nur mdm Client) 		
Hardware	<ul style="list-style-type: none"> - mindestens 512 MB RAM - 500 MB freier Festplattenspeicher - Farbmonitor mit einer Auflösung von mindestens 1280 x 1024 	<ul style="list-style-type: none"> - mindestens 4 GB RAM - 100 GB freier Festplattenspeicher 	<ul style="list-style-type: none"> - mindestens 512 MB RAM - 5 GB freier Festplattenspeicher
Software-Komponenten	<ul style="list-style-type: none"> - Komponenten von Drittanbietern (<i>PostgreSQL 10.16, Apache Webserver 2.4.46, OpenJDK 11.0.9, Python 3.8.3 und OpenSSL 1.1.1k</i>) werden über <i>mdm 1.13.x Installer for Windows</i> automatisch installiert. - <i>Apache Webserver</i> benötigt das installierte Paket <i>Microsoft Visual C ++ 2017 Redistributable Package (x64)</i> oder neuer. Download: https://aka.ms/vs/16/release/VC_redist.x64.exe HINWEIS: Es ist möglich, dass der angegebene Link nicht mehr gültig ist. Stellen Sie in jedem Fall sicher, dass die richtige Version verwendet wird! - mdm-Clients, die auf einem anderen als dem „Serversystem“ unabhängig laufen, erfordern für die Installation die Java-Plattform <i>OpenJDK 11</i>). 		
Voraussetzung	<ul style="list-style-type: none"> - wenn nicht über <i>mdm Installer for Windows</i> installiert: <i>OpenJDK 11</i> 	<ul style="list-style-type: none"> - mdm nicht installiert (oder mdm ab Version 1.12.0 installiert). - <i>PostgreSQL</i> nicht installiert (oder durch frühere Installationen von mdm installiert). - <i>Apache Webserver</i> nicht installiert <ul style="list-style-type: none"> - (oder installiert und horcht auf anderem Port als 443), - (oder durch frühere Versionen von mdm installiert). - <i>Microsoft Visual C ++ 2017 Redistributable Package (x64)</i> (oder neuer) installiert. 	

1.4.1 Upgrade auf unterstützten Windows-Systemen

Upgrade auf unterstützten Windows-Systemen

Von mdm Versionen ab 1.12.0

Verwenden Sie zum Upgrade von mdm 1.12.x unter Microsoft Windows den *mdm 1.13.x Installer for Windows* (siehe „mdm 1.13.x Installer for Windows“ auf Seite 26)

Die Deinstallation von mdm 1.12.x samt Komponenten ist nicht notwendig.

Der *mdm Installer for Windows* erstellt automatisch Datenbank-Dumps der aktuellen mdm 1.12.x-Installation.

Achtung: Im Fall von FL MGUARD 1000-Geräten (mGuard NT 1.3) werden Werte der Konfiguration größtenteils auf Werkseinstellungen von mGuard NT 1.4 zurückgesetzt.

Für weitere Informationen siehe [mdm-Benutzerhandbuch](#).

Von mdm-Versionen < 1.12.0

Für das Upgrade von installierten mdm-Versionen ab 1.5.2 auf unterstützten Windows-Systemen können zwei Verfahren gewählt werden:

1. **mdm Installer for Windows:** Führen Sie ein Upgrade der aktuellen mdm-Installation zur nächsten *Minor Version* schrittweise mit dem entsprechenden *mdm Installer for Windows* durch, bis mdm 1.13.x installiert ist (z. B. von mdm 1.5.2 >> 1.6.2 >> 1.7.0 >> 1.8.0 >> 1.9.0 >> 1.10.x >> 1.11.x >> 1.12.x auf mdm 1.13.x) **oder**
2. **Datenbank-Dumps:** Erstellen, exportieren und importieren Sie Datenbank-Dumps der *mdm-* und *CA-Server-Datenbanken* wie nachfolgend beschrieben:
 - erstellen Sie einen Dump und eine Sicherheitskopie der Datenbanken
 - entfernen Sie die komplette mdm-Installation
 - installieren Sie mit dem *mdm 1.13.x Installer for Windows* mdm 1.13.x
 - importieren Sie die erstellten Datenbank-Dumps



ACHTUNG: Unwiderruflicher Datenverlust

Die Daten Ihrer aktuellen mdm Server- und CA-Serverdatenbank werden gelöscht. Bewahren Sie Sicherheitskopien Ihrer aktuellen Datenbanken an einem sicheren Ort auf.



ACHTUNG: Inkompatibilität von mdm Datenbanken

Das Upgrade von einer älteren Version auf mdm 1.13.x erfordert Änderungen an der unterstützenden PostgreSQL-Datenbank, die nicht rückgängig gemacht werden können. Nach Durchführung dieser Änderungen kann mit älteren Versionen nicht mehr auf die Datenbank zugegriffen werden. Bewahren Sie Sicherheitskopien Ihrer aktuellen Datenbanken an einem sicheren Ort auf.

Gehen Sie zum Erstellen von Datenbank-Dumps und Sicherheitskopien wie folgt vor:

Upgrade auf unterstützten Windows-Systemen

A) Erstellen Sie Datenbank-Dumps der *mdm* und *mdm CA-Serverdatenbanken*

1. Kopieren Sie die erforderlichen Batch-Dateien in das Windows-System, in dem mdm installiert wird.
2. Führen Sie die Batch-Datei **export_mdm_server.bat** (als Administrator) aus.
3. Geben Sie einen Pfad zum Speichern des Datenbank-Dumps an (Standardeinstellung: *C:\Users\username\Documents\mdm-server.sql*).
4. Geben Sie den Pfad in das Installationsverzeichnis Ihres aktuellen mdm an (Standardeinstellung: *C:\Program Files\mGuard device manager*).
5. Geben Sie das Passwort des Datenbankbenutzers *innomms* an, falls erforderlich.
6. Wenn die Erstellung des Datenbank-Dumps abgeschlossen ist, können Sie die Eingabeaufforderung durch Drücken einer *beliebigen Taste* schließen.
7. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 6, **aber** führen Sie die Batch-Datei **export_mdm_ca.bat** aus, um einen Dump der *mdm CA-Serverdatenbank* zu erstellen (Standardeinstellung: *mdm_ca_server.sql*, Datenbankbenutzer = *mdmca*).

B) Erstellen Sie eine Sicherheitskopie der Datenbank-Dumps

1. Öffnen Sie das Verzeichnis, in dem die Datenbank-Dumps gespeichert sind.
2. Kopieren Sie die unter (A) erstellten Datenbank-Dumps an einen sicheren Ort (beispielsweise ein sicheres Backup-Verzeichnis auf einem anderen Server im Unternehmen).

C) (Falls erforderlich) Erstellen Sie eine Sicherheitskopie der Pull-Server-Konfiguration

1. Kopieren Sie zum Erstellen einer Sicherheitskopie der Webserverkonfiguration die folgende Datei an einen sicheren Speicherort:

<path to mdm installation>\apache\conf\extra\httpd-mdm.conf

- Suchen Sie nach den folgenden Einträgen (Ihre Einträge können von den nachfolgend angegebenen Standardeinstellungen des mdm Installers abweichen) und notieren Sie die Aliases des Pull-Konfig-Servers:

Verzeichnis für ATV-Profil (wie in preferences.xml eingestellt).

Alias /atv/ /var/apache-data/atv/

<Directory /var/apache-data/atv/>

Allas /atv/ „C:/Program Files/mGuard device manager/apache-data/atv/“

Allas /atv/ „C:/Program Files/mGuard device manager/apache-data/atv/“

- Wenn Sie einen Dienst so konfiguriert haben, dass das Pull-Feedback an mdm übermittelt wird, suchen Sie auch nach den folgenden Einträgen (CustomLog) und notieren Sie diese:

Pull Config-Feedback an den mdm Server (derzeit auskommentiert).

CustomLog „| /bin/nc -u -i1 127.0.0.1 7514“ common

<your feedback configuration>

2. Kopieren Sie zum Erstellen einer Sicherheitskopie des Zertifikats und der privaten Schlüssel die folgende Datei an einen sicheren Speicherort:

<path to mdm installation>\apache\conf\server.crt

<path to mdm installation>\apache\conf\server.key

D) Deinstallieren Sie die komplette mdm Installation vom Windows-System

1. Deinstallieren Sie die mdm Installation entweder mit dem integrierten Deinstallationsprogramm oder mit dem Standardverfahren unter Windows (e.g. *Control Panel\Programs\Programs and Features*).

Upgrade auf unterstützten Windows-Systemen

E) Installieren Sie mdm 1.13.x und die gewünschten Komponenten mit dem mdm 1.13.x Installer for Windows.

1. Verwenden Sie den *mdm 1.13.x Installer for Windows* wie in [Kapitel 1.7](#) beschrieben.



Stellen Sie nicht alle CA-Zertifikatattribute zur Verfügung, die mit den Attributen früherer Installation identisch sind (fügen Sie *Common Name* beispielsweise ein Suffix hinzu).

F) Importieren Sie die Datenbank-Dumps (mdm Server und mdm CA-Server)

1. Stellen Sie die Datenbank-Dumps auf dem System zur Verfügung, auf dem mdm 1.13.x installiert ist.
2. Führen Sie die Batch-Datei ***import_mdm_server.bat*** (als Administrator) aus.
3. Geben Sie einen Pfad zum Datenbank-Dump an (Standardeinstellung: *C:\Users\username\Documents\mdm-server.sql*).
4. Geben Sie den Pfad in das Installationsverzeichnis von mdm 1.13.x an (Standardeinstellung: *C:\Program Files\mGuard device manager*).
5. Geben Sie das Passwort des Datenbankbenutzers *innomms* an, falls erforderlich.
6. Wenn der Datenbankimport abgeschlossen ist, können Sie die Eingabeaufforderung durch Drücken einer *beliebigen Taste* schließen.
7. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 6, **aber** führen Sie die Batch-Datei ***import_mdm_ca.bat*** aus, um den Dump der *mdm CA-Serverdatenbank* zu importieren (Standardeinstellung: *mdm_ca_server.sql*, Datenbankbenutzer = *mdmca*).
8. mdm startet automatisch neu und verbindet sich mit den importierten Datenbanken.

G) (Falls erforderlich) Aktualisieren Sie das Firmwareupgrade/die Pull-Server-Konfiguration

1. Öffnen Sie den *Apache HTTP Server Monitor* (in der mdm Installation enthalten) und **stoppen** Sie den Dienst ***ApacheMDM***.
2. Vergleichen Sie die Konfigurationsdatei des Webservers mit der im Schritt (C) gespeicherten Sicherheitskopie:


```
<path to mdm installation>\apache\conf\extra\httpd-mdm.conf
```

 - Vergleichen Sie die Aliases des Pull-Konfig-Servers. Ändern Sie bei einer Abweichung der früheren Einstellungen von den Standardeinstellungen des mdm Installers (nachfolgend angegeben) die Standardeinstellungen entsprechend Ihren Einstellungen (z. B. ***Alias /my_company_atv/***):


```
Alias /atv/ „C:/Program Files/mGuard device manager/apache-data/atv/“
```

```
Alias /atv „C:/Program Files/mGuard device manager/apache-data/atv/“
```
 - Aktualisieren Sie die Rückmeldung der Pull-Konfiguration an den mdm Server, sofern dies konfiguriert werden muss:


```
# Pull Config-Feedback an den mdm Server (derzeit auskommentiert).
```

```
# CustomLog „|/bin/nc -u -i1 127.0.0.1 7514“ common
```

```
<your feedback configuration>
```
3. Kopieren Sie die in Schritt (C) angefertigten Sicherheitskopien von Zertifikat und privatem Schlüssel auf


```
<path to mdm installation>\apache\conf\server.crt
```

```
<path to mdm installation>\apache\conf\server.key
```
4. Öffnen Sie den *Apache HTTP Server Monitor* und **starten** Sie den Dienst ***ApacheMDM***.

1.4.2 Upgrade von nicht unterstützten Windows-Systemen

Upgrade von nicht unterstützten Windows-Systemen

Alle mdm Versionen

mdm-Versionen, die auf nicht unterstützten Windows-Systemen installiert sind, können nicht auf Version mdm 1.13.x aktualisiert werden.

Um die Datenbanken dieser mdm-Versionen auf unterstützten Windows-Systemen weiterzuverwenden, müssen Sie:

- Dumps und Sicherheitskopien der Datenbanken erstellen
- mit dem *mdm 1.13.x Installer for Windows* mdm 1.13.x auf einem unterstützten System installieren (siehe Kapitel 1.7)
- die Datenbank-Dumps importieren

Gehen Sie zum Erstellen der Dumps und zum Importieren der *mdm Serverdatenbank* und der *mdm CA-Serverdatenbank* wie oben beschrieben vor („Von mdm-Versionen < 1.12.0“ auf Seite 7).

1.4.3 Upgrade von Linux-Systemen

Upgrade von Linux-Systemen

Alle mdm Versionen

Um die Datenbanken von mdm-Versionen, die auf Linux-Systemen installiert sind, auf unterstützten Windows-Systemen weiterzuverwenden, müssen Sie:

- Dumps und Sicherheitskopien der Datenbanken erstellen
- mit dem *mdm 1.13.x Installer for Windows* mdm 1.13.x auf einem unterstützten System installieren (siehe Kapitel 1.7)
- die Datenbank-Dumps importieren



ACHTUNG: Inkompatibilität von mdm Datenbanken

Das Upgrade von einer älteren Version auf mdm 1.13.x erfordert Änderungen an der unterstützenden PostgreSQL-Datenbank, die nicht rückgängig gemacht werden können. Nach Durchführung dieser Änderungen kann mit älteren Versionen nicht mehr auf die Datenbank zugegriffen werden. Bewahren Sie Sicherheitskopien Ihrer aktuellen Datenbanken an einem sicheren Ort auf.

Gehen Sie wie folgt vor:

A) Erstellen Sie Datenbank-Dumps der *mdm* und *mdm CA-Serverdatenbanken*

1. Kopieren Sie die benötigten Shell-Skript-Dateien auf das Linux-System, auf dem mdm installiert ist.
2. Führen Sie das Shell-Skript ***export_mdm_server.sh*** (als sudo) aus.
3. Geben Sie einen Pfad zum Speichern des Datenbank-Dumps an (Standardeinstellung: */tmp/mdm-server.sql*).
4. Geben Sie das Passwort des Datenbankbenutzers *innomms* an, falls erforderlich.
5. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 4, **aber** führen Sie das Shell-Skript ***export_mdm_ca.sh*** aus, um einen Dump der *mdm CA-Serverdatenbank* zu erstellen (Standardeinstellung: *mdm_ca_server.sql*, Datenbankbenutzer = *mdmca*).

B) Erstellen Sie eine Sicherheitskopie der Datenbank-Dumps

1. Öffnen Sie das Verzeichnis, in dem die Datenbank-Dumps gespeichert sind.
2. Kopieren Sie die unter (A) erstellten Datenbank-Dumps an einen sicheren Ort (beispielsweise ein sicheres Backup-Verzeichnis auf einem anderen Server im Unternehmen).

Upgrade von Linux-Systemen

C) (Falls erforderlich) Erstellen Sie eine Sicherheitskopie der Pull-Server-Konfiguration

1. Kopieren Sie zum Erstellen einer Sicherheitskopie der Webserverkonfiguration die folgende Serverkonfiguration an einen sicheren Speicherort. Wenn Sie beispielsweise Apache 2.x nutzen, können Sie Ihre Konfigurationsdatei unter `/etc/apache2/sites-available/your-server.conf` speichern.

- Falls Ihre Serverkonfiguration Aliases für das Verzeichnis der Pull-Konfiguration definiert, notieren Sie diese. Sie können wie folgt aussehen:

```
Alias /atv/ „/var/www/mdm pull/“
```

```
Alias /atv/ „/var/www/mdm-pull/“
```

2. Gehen Sie zur Erstellung einer Sicherheitskopie des Zertifikats und des privaten Schlüssels wie folgt vor:

- Überprüfen Sie die Konfiguration aus Schritt (1.) (z. B. `/etc/apache2/sites-available/your-server.conf`) und suchen Sie nach der von Ihrem Server verwendeten Zertifizierung. Wenn Sie beispielsweise Apache 2.x nutzen, können die Einträge wie folgt aussehen:

```
SSLCertificateFile /etc/mdm/mdm-pull-server/cert.pem
```

```
SSLCertificateKeyFile /etc/mdm/mdm-pull-server/key
```

- Kopieren Sie diese Dateien unter Verwendung der folgenden Dateinamen an einen sicheren Speicherort:

```
<path to certificate>/server.crt
```

```
<path to certificate>/server.key
```

D) Installieren Sie mdm 1.13.x und die gewünschten Komponenten mit dem mdm 1.13.x Installer for Windows.

1. Verwenden Sie den *mdm 1.13.x Installer for Windows* wie in [Kapitel 1.7](#) beschrieben.



Stellen Sie nicht alle CA-Zertifikatattribute zur Verfügung, die mit den Attributen früherer Installation identisch sind (fügen Sie *Common Name* beispielsweise ein Suffix hinzu).

E) Importieren Sie die Datenbank-Dumps (mdm Server und mdm CA-Server)

1. Stellen Sie die Datenbank-Dumps auf dem System zur Verfügung, auf dem mdm 1.13.x installiert ist.
2. Führen Sie die Batch-Datei **import_mdm_server.bat** (als Administrator) aus.
3. Geben Sie einen Pfad zum Datenbank-Dump an (Standardeinstellung: `C:\Users\username\Documents\mdm-server.sql`).
4. Geben Sie den Pfad in das Installationsverzeichnis von mdm 1.13.x an (Standardeinstellung: `C:\Program Files\mGuard device manager`).
5. Geben Sie das Passwort des Datenbankbenutzers *innomms* an, falls erforderlich.
6. Wenn der Datenbankimport abgeschlossen ist, können Sie die Eingabeaufforderung durch Drücken einer *beliebigen Taste* schließen.
7. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 6, **aber** führen Sie die Batch-Datei **import_mdm_ca.bat** aus, um den Dump der *mdm CA-Serverdatenbank* zu importieren (Standardeinstellung: `mdm_ca_server.sql`, Datenbankbenutzer = *mdmca*).
8. mdm startet automatisch neu und verbindet sich mit den importierten Datenbanken.

Upgrade von Linux-Systemen

F) (Falls erforderlich) Aktualisieren Sie das Firmwareupgrade/die Pull-Server-Konfiguration

1. Öffnen Sie den *Apache HTTP Server Monitor* (in der *mdm* Installation enthalten) und **stoppen** Sie den Dienst **ApacheMDM**.
2. Vergleichen Sie die Konfigurationsdatei des Webservers mit der im Schritt (C) gespeicherten Sicherheitskopie:

<path to mdm installation>\apache\conf\extra\httpd-mdm.conf

- Vergleichen Sie die Aliases des Pull-Konfig-Servers. Ändern Sie bei einer Abweichung der früheren Einstellungen von den Standardeinstellungen des *mdm* Installers (nachfolgend angegeben) die Standardeinstellungen entsprechend Ihren Einstellungen (z. B. **Alias /my_company_atv/**):
Alias /atv/ „C:/Program Files/mGuard device manager/apache-data/atv/“
Alias /atv „C:/Program Files/mGuard device manager/apache-data/atv/“
- Aktualisieren Sie die Rückmeldung der Pull-Konfiguration an den *mdm* Server, sofern dies konfiguriert werden muss:

Pull Config-Feedback an den mdm Server (derzeit auskommentiert).

CustomLog „|/bin/nc -u -i1 127.0.0.1 7514“ common

<your feedback configuration>

3. Kopieren Sie die in Schritt (C) angefertigten Sicherheitskopien von Zertifikat und privatem Schlüssel auf

<path to mdm installation>\apache\conf\server.crt

<path to mdm installation>\apache\conf\server.key

4. Öffnen Sie den *Apache HTTP Server Monitor* und **starten** Sie den Dienst **ApacheMDM**.

1.5 Betriebssystem: Ubuntu Linux



Die Versionen ab **mdm 1.11.x** können nur auf **Ubuntu (Server) 18.04 LTS** installiert werden.

Für das Upgrade älterer mdm-Versionen auf mdm 1.13.x müssen Sie zunächst Ubuntu 16.04 LTS über die Paketverwaltung auf Ubuntu 18.04 LTS upgraden.

Siehe:

- „Kurzanleitung: Ubuntu 16.04 auf 18.04 upgraden“ auf Seite 22
- „Kurzanleitung (Ubuntu): mdm 1.12.x auf 1.13.x upgraden“ auf Seite 23

Sollte Ihr System die in Tabelle 1-2 angegebenen System-Anforderungen nicht erfüllen, müssen von *mdm Server- und -CA-Serverdatenbanken* entweder Dumps erstellt und in ein neu installiertes mdm 1.13.x importiert werden, oder die installierte mdm-Version muss schrittweise auf mdm 1.13.x aktualisiert werden.



Datenschutzhinweis: Der Zugriff auf den *mdm-Repository-Server* wird protokolliert, um die Sicherheit und Stabilität des Dienstes zu gewährleisten. Für statistische Auswertungen werden nur anonymisierte Daten gespeichert.

Systemanforderungen

Tabelle 1-2 Systemanforderungen (Ubuntu Linux)

	mdm Client	mdm Server	mdm CA
Betriebssystem	- Ubuntu Desktop 18.04 LTS	- Ubuntu (Server) 18.04 LTS	
Hardware	- mindestens 512 MB RAM - 500 MB freier Festplattenspeicher - Farbmonitor mit einer Auflösung von mindestens 1280 x 1024	- mindestens 4 GB RAM - 100 GB freier Festplattenspeicher	- mindestens 512 MB RAM - 5 GB freier Festplattenspeicher
Software-Komponenten	- Komponenten von Drittanbietern (<i>PostgreSQL 10, Apache Webserver 2.4, OpenJDK 11, OpenSSL 1.1.x</i> und <i>Python 3.8</i>) werden über die Paketverwaltung von Ubuntu automatisch installiert.		
Voraussetzung	- Sofern nicht über die Paketverwaltung von Ubuntu installiert: <i>OpenJDK 11</i>	- mdm nicht installiert (oder mdm ab Version 1.12.0 installiert). - Die Komponenten früherer Installationen vor Version mdm 1.7.0 müssen vollständig entfernt sein.	

1.5.1 Upgrade auf unterstützten und nicht unterstützten Linux-Systemen

Upgrade auf unterstützten und nicht unterstützten Linux-Systemen	
<p>Von mdm-Versionen ab 1.12.0 (installiert auf Ubuntu Server 18.04 LTS)</p>	<p>Um mdm-Versionen ab mdm 1.12.0, installiert auf Ubuntu Server 18.04 LTS, upzugraden, müssen Sie:</p> <ul style="list-style-type: none"> – mdm über die Paketverwaltung upgraden: Aktualisieren Sie die installierte mdm-Version über die Paketverwaltung von Ubuntu 18.04 LTS auf Version mdm 1.13.x. Siehe „Kurzanleitung (Ubuntu): mdm 1.12.x auf 1.13.x upgraden“ auf Seite 23 <p>Achtung: Im Fall von FL MGUARD 1000-Geräten (mGuard NT 1.3) werden Werte der Konfiguration größtenteils auf Werkseinstellungen von mGuard NT 1.4 zurückgesetzt.</p> <p>Für weitere Informationen siehe mdm-Benutzerhandbuch.</p>
<p>Von mdm-Versionen ab 1.11.0 (installiert auf Ubuntu Server 18.04 LTS)</p>	<p>Um mdm-Versionen ab mdm 1.11.0, installiert auf Ubuntu Server 18.04 LTS, upzugraden, müssen Sie:</p> <ul style="list-style-type: none"> – mdm schrittweise über die Paketverwaltung upgraden: Aktualisieren Sie in zwei Schritten die installierte mdm-Version über die Paketverwaltung von Ubuntu 18.04 LTS zunächst auf Version mdm 1.12.x und anschließend auf Version mdm 1.13.x. Siehe „Kurzanleitung (Ubuntu): mdm 1.11.x auf 1.12.x upgraden“ auf Seite 23. Siehe „Kurzanleitung (Ubuntu): mdm 1.12.x auf 1.13.x upgraden“ auf Seite 23 <p>Für weitere Informationen siehe mdm-Benutzerhandbuch.</p>
<p>Von mdm-Versionen ab 1.10.0 (installiert auf Ubuntu Server 16.04 LTS)</p>	<p>Um mdm-Versionen ab mdm 1.10.0, installiert auf Ubuntu Server 16.04 LTS, upzugraden, müssen Sie:</p> <ul style="list-style-type: none"> – Ubuntu Server 16.04 LTS auf Ubuntu Server 18.04 LTS upgraden: Siehe „Kurzanleitung: Ubuntu 16.04 auf 18.04 upgraden“ auf Seite 22. – mdm schrittweise über die Paketverwaltung upgraden: Aktualisieren Sie in mehreren Schritten die installierte mdm-Version über die Paketverwaltung von Ubuntu 18.04 LTS zunächst auf Version mdm 1.11.x und anschließend in zwei Schritten über mdm 1.12.x auf 1.13.x. <ul style="list-style-type: none"> – Siehe „Kurzanleitung (Ubuntu): mdm 1.10.x auf 1.11.x upgraden“ auf Seite 23. – Siehe „Kurzanleitung (Ubuntu): mdm 1.11.x auf 1.12.x upgraden“ auf Seite 23. <p>Für weitere Informationen siehe mdm-Benutzerhandbuch.</p>
<p>Von mdm-Versionen ab 1.7.0 (installiert auf Ubuntu Server 16.04 LTS)</p>	<p>Um mdm-Versionen ab mdm 1.7.0, die auf Ubuntu Server 16.04 LTS installiert sind, upzugraden, müssen Sie schrittweise vorgehen:</p> <ol style="list-style-type: none"> 1. Aktualisieren Sie zunächst in mehreren Schritten die jeweils installierte mdm-Version über die Paketverwaltung von Ubuntu 16.04 LTS auf die nächstmöglich Version (mdm 1.7.x >> 1.8.x >> 1.9.x >> 1.10.x). 2. Upgraden Sie mdm 1.10.x auf mdm 1.11.x wie oben beschrieben („Von mdm-Versionen ab 1.10.0“). <p>Für weitere Informationen siehe mdm-Benutzerhandbuch.</p>

Upgrade auf unterstützten und nicht unterstützten Linux-Systemen

Von mdm-Versionen < 1.7.0

mdm-Versionen < 1.7.0 auf unterstützten und nicht unterstützten Linux-Systemen können nicht auf Version mdm 1.13.x aktualisiert werden.

Um die Datenbanken dieser mdm-Versionen auf unterstützten Linux-Systemen weiterzuverwenden, müssen Sie:

- Dumps und Sicherheitskopien der Datenbanken erstellen
- Ubuntu Server 18.04 LTS installieren
- mdm 1.13.x über die Paketverwaltung von Ubuntu Server 18.04 LTS installieren (siehe Kapitel 1.8)
- die Datenbank-Dumps importieren



ACHTUNG: Inkompatibilität von mdm Datenbanken

Das Upgrade von einer älteren Version auf mdm 1.13.x erfordert Änderungen an der unterstützenden PostgreSQL-Datenbank, die nicht rückgängig gemacht werden können. Nach Durchführung dieser Änderungen kann mit älteren Versionen nicht mehr auf die Datenbank zugegriffen werden. Bewahren Sie Sicherheitskopien Ihrer aktuellen Datenbanken an einem sicheren Ort auf.

Gehen Sie wie folgt vor:

A) Erstellen Sie Datenbank-Dumps der mdm und mdm CA-Serverdatenbanken

1. Kopieren Sie die benötigten Shell-Skript-Dateien auf das Linux-System, auf dem mdm installiert ist.
2. Führen Sie das Shell-Skript ***export_mdm_server.sh*** (als sudo) aus.
3. Geben Sie einen Pfad zum Speichern des Datenbank-Dumps an (Standardeinstellung: */tmp/mdm-server.sql*).
4. Geben Sie das Passwort des Datenbankbenutzers *innomms* an, falls erforderlich.
5. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 4, **aber** führen Sie das Shell-Skript ***export_mdm_ca.sh*** aus, um einen Dump der *mdm CA-Serverdatenbank* zu erstellen (Standardeinstellung: *mdm_ca_server.sql*, Datenbankbenutzer = *mdmca*).

B) Erstellen Sie eine Sicherheitskopie der Datenbank-Dumps

1. Öffnen Sie das Verzeichnis, in dem die Datenbank-Dumps gespeichert sind.
2. Kopieren Sie die unter (A) erstellten Datenbank-Dumps an einen sicheren Ort (beispielsweise ein sicheres Backup-Verzeichnis auf einem anderen Server im Unternehmen).

Upgrade auf unterstützten und nicht unterstützten Linux-Systemen

C) (Falls erforderlich) Erstellen Sie eine Sicherheitskopie der Pull-Server-Konfiguration

1. Kopieren Sie zum Erstellen einer Sicherheitskopie der Webserverkonfiguration die folgende Serverkonfiguration an einen sicheren Speicherort. Wenn Sie beispielsweise Apache 2.x nutzen, finden Sie Ihre Konfigurationsdatei möglicherweise unter:

/etc/apache2/sites-available/your-server.conf .

- Falls Ihre Serverkonfiguration Aliases für das Verzeichnis der Pull-Konfiguration definiert, notieren Sie diese. Sie können wie folgt aussehen:

Alias /atv/ „/var/www/mdm-pull/“

Alias /atv/ „/var/www/mdm-pull/“

2. Gehen Sie zur Erstellung einer Sicherheitskopie des Zertifikats und des privaten Schlüssels wie folgt vor:

- Überprüfen Sie die Konfiguration aus Schritt (1.) (z. B. */etc/apache2/sites-available/your-server.conf*) und suchen Sie nach der von Ihrem Server verwendeten Zertifizierung. Wenn Sie beispielsweise Apache 2.x nutzen, können die Einträge wie folgt aussehen:

SSLCertificateFile /etc/mdm/mdm-pull-server/cert.pem

SSLCertificateKeyFile /etc/mdm/mdm-pull-server/key

- Kopieren Sie diese Dateien unter Verwendung der folgenden Dateinamen an einen sicheren Speicherort:

<path to certificate>/cert.pem

<path to certificate>/key

D) Installieren Sie mdm 1.13.x und die gewünschten Komponenten über die Paketverwaltung von Ubuntu

1. Verwenden Sie die Ubuntu-Paketverwaltung wie in Kapitel 1.8 beschrieben.



Stellen Sie nicht alle CA-Zertifikatattribute zur Verfügung, die mit den Attributen früherer Installation identisch sind (fügen Sie *Common Name* beispielsweise ein Suffix hinzu).

E) Importieren Sie die Datenbank-Dumps (mdm Server und mdm CA-Server)

1. Stellen Sie die Datenbank-Dumps auf dem System zur Verfügung, auf dem mdm 1.13.x installiert ist.
2. Führen Sie das Shell-Skript ***import_mdm_server.sh*** (als sudo) aus.
3. Geben Sie einen Pfad zum Speicherort des Datenbank-Dumps an (Standardeinstellung: */tmp/mdm-server.sql*).
4. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 3, **aber** führen Sie das Shell-Skript ***import_mdm_ca.sh*** aus, um den Dump der *mdm CA-Serverdatenbank* zu importieren (Standardeinstellung: *mdm_ca_server.sql*, Datenbankbenutzer = *mdmca*).
5. mdm startet automatisch neu und verbindet sich mit den importierten Datenbanken.

Upgrade auf unterstützten und nicht unterstützten Linux-Systemen

F) (Falls erforderlich) Firmwareupgrade/Pull-Server-Konfiguration aktualisieren

1. Halten Sie (als sudo) den Apache Webserver an: `service apache2 stop`
2. Wenn durch Ihre vorherige Konfiguration Aliases für die Pull-Konfiguration definiert wurden (überprüfen Sie die in Schritt (C) erstellte Sicherheitskopie), bearbeiten Sie die Apache-Konfigurationsdatei Ihrer neuen mdm Installation:
`/etc/mdm/mdm-webbase/30-configpull.conf`
 - Fügen Sie die Aliases Ihrer vorherigen Konfiguration hinzu (ändern Sie nicht das reale Exportverzeichnis: `/var/www/mdm/`). Beispielsweise:
`Alias /atv/ „/var/www/mdm/“`
`Alias /atv/ „/var/www/mdm/“`
3. Kopieren Sie die in Schritt (C) angefertigten Sicherheitskopien von Zertifikat und privatem Schlüssel auf
`/etc/mdm/mdm-webbase/cert.pem`
`/etc/mdm/mdm-webbase/key`
4. Starten Sie (als sudo) den Apache-Webserver: `service apache2 start`

1.5.2 Upgrade von Microsoft Windows-Systemen

Upgrade von Microsoft Windows-Systemen

Alle mdm Versionen

Um Datenbanken von mdm-Versionen, die auf Windows-Systemen installiert sind, auf Ubuntu Server 18.04 LTS weiterzuverwenden, müssen Sie:

- Dumps und Sicherheitskopien der Datenbanken erstellen
- Ubuntu Server 18.04 LTS installieren
- mdm 1.13.x über die Paketverwaltung von Ubuntu Server 18.04 LTS installieren (siehe Kapitel 1.8)
- die Datenbank-Dumps importieren



ACHTUNG: Unwiderruflicher Datenverlust

Das Upgrade von einer älteren Version auf mdm 1.13.x erfordert Änderungen an der unterstützenden PostgreSQL-Datenbank, die nicht rückgängig gemacht werden können. Nach Durchführung dieser Änderungen kann mit älteren Versionen nicht mehr auf die Datenbank zugegriffen werden. Bewahren Sie Sicherheitskopien Ihrer aktuellen Datenbanken an einem sicheren Ort auf.

Gehen Sie wie folgt vor:

A) Erstellen Sie Datenbank-Dumps der *mdm*- und *mdm-CA-Serverdatenbanken*

1. Kopieren Sie die erforderlichen Batch-Dateien in das Windows-System, in dem mdm installiert wird.
2. Führen Sie die Batch-Datei ***export_mdm_server.bat*** (als Administrator) aus.
3. Geben Sie einen Pfad zum Speichern des Datenbank-Dumps an (Standardeinstellung: *C:\Users\username\Documents\mdm-server.sql*).
4. Geben Sie den Pfad in das Installationsverzeichnis Ihres aktuellen mdm an (Standardeinstellung: *C:\Program Files\vmGuard device manager*).
5. Geben Sie das Passwort des Datenbankbenutzers *innomms* an, falls erforderlich.
6. Wenn die Erstellung des Datenbank-Dumps abgeschlossen ist, können Sie die Eingabeaufforderung durch Drücken einer *beliebigen Taste* schließen.
7. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 6, **aber** führen Sie die Batch-Datei ***export_mdm_ca.bat*** aus, um einen Dump der *mdm CA-Serverdatenbank* zu erstellen (Standardeinstellung: *mdm_ca_server.sql*, Datenbankbenutzer = *mdmca*).

B) Erstellen Sie eine Sicherheitskopie der Datenbank-Dumps

1. Öffnen Sie das Verzeichnis, in dem die Datenbank-Dumps gespeichert sind.
2. Kopieren Sie die unter (A) erstellten Datenbank-Dumps an einen sicheren Ort (beispielsweise ein sicheres Backup-Verzeichnis auf einem anderen Server im Unternehmen).

Upgrade von Microsoft Windows-Systemen

C) (Falls erforderlich) Erstellen Sie eine Sicherheitskopie der Pull-Server-Konfiguration

1. Kopieren Sie zum Erstellen einer Sicherheitskopie der Webserverkonfiguration die folgende Datei an einen sicheren Speicherort:

`<path to mdm installation>\apache\conf\extra\httpd-mdm.conf`

- Suchen Sie nach den folgenden Einträgen (Ihre Einträge können von den nachfolgend angegebenen Standardeinstellungen des mdm Installers abweichen) und notieren Sie die Aliases des Pull-Konfig-Servers:

`# Verzeichnis für ATV-Profile (wie in preferences.xml eingestellt).`

`# Alias /atv/ /var/apache-data/atv/`

`# <Directory /var/apache-data/atv/>`

`Alias /atv/ „C:/Program Files/mGuard device manager/apache-data/atv/“`

`Alias /atv „C:/Program Files/mGuard device manager/apache-data/atv/“`

2. Kopieren Sie zum Erstellen einer Sicherheitskopie des Zertifikats und der privaten Schlüssel die folgende Datei an einen sicheren Speicherort:

`<path to mdm installation>\apache\conf\server.crt`

`<path to mdm installation>\apache\conf\server.key`

D) Installieren Sie mdm 1.13.x und die gewünschten Komponenten über die Paketverwaltung von Ubuntu

1. Verwenden Sie die Ubuntu-Paketverwaltung wie in Kapitel 1.8 beschrieben.



Stellen Sie nicht alle CA-Zertifikatattribute zur Verfügung, die mit den Attributen früherer Installation identisch sind (fügen Sie *Common Name* beispielsweise ein Suffix hinzu).

E) Importieren Sie die Datenbank-Dumps (mdm Server und mdm CA-Server)

1. Stellen Sie die Datenbank-Dumps auf dem System zur Verfügung, auf dem mdm 1.13.x installiert ist.
2. Führen Sie das Shell-Skript **`import_mdm_server.sh`** (als sudo) aus.
3. Geben Sie einen Pfad zum Speicherort des Datenbank-Dumps an (Standardeinstellung: `/tmp/mdm-server.sql`).
4. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 3, **aber** führen Sie das Shell-Skript **`import_mdm_ca.sh`** aus, um den Dump der *mdm CA-Serverdatenbank* zu importieren (Standardeinstellung: `mdm_ca_server.sql`, Datenbankbenutzer = `mdmca`).
5. mdm startet automatisch neu und verbindet sich mit den importierten Datenbanken.

Upgrade von Microsoft Windows-Systemen

F) (Falls erforderlich) Firmwareupgrade/Pull-Server-Konfiguration aktualisieren

1. Halten Sie (als sudo) den Apache-Webserver an: `service apache2 stop`
2. Wenn durch Ihre vorherige Konfiguration Aliases für die Pull-Konfiguration definiert wurden (überprüfen Sie die in Schritt (C) erstellte Sicherheitskopie), bearbeiten Sie die Apache-Konfigurationsdatei Ihrer neuen mdm Installation:
`/etc/mdm/mdm-webbase/30-configpull.conf`
 - Fügen Sie die Aliases Ihrer vorherigen Konfiguration hinzu (ändern Sie nicht das reale Exportverzeichnis: `/var/www/mdm/`). Beispielsweise:
`Alias /atv/ „/var/www/mdm/“`
`Alias /atv/ „/var/www/mdm/“`
3. Kopieren Sie die in Schritt (C) angefertigten Sicherheitskopien von Zertifikat und privatem Schlüssel auf
`/etc/mdm/mdm-webbase/cert.pem`
`/etc/mdm/mdm-webbase/key`
4. Starten Sie (als sudo) den Apache-Webserver: `service apache2 start`

1.5.3 Kurzanleitung: Ubuntu 16.04 auf 18.04 upgraden

Versionen ab **mdm 1.11.0** können nur auf **Ubuntu (Server) 18.04 LTS** installiert werden.



ACHTUNG: Datenverlust durch Aktualisierung

Führen Sie vor dem Upgrade eine Datensicherung durch.

Sichern Sie die *mdm*- und *CA-Server-Datenbanken* der aktuellen mdm-Installation

1. Kopieren Sie die benötigten Shell-Skript-Dateien auf das Linux-System, auf dem mdm installiert ist.
2. Führen Sie das Shell-Skript ***export_mdm_server.sh*** (mit Administratorrechten) aus.
3. Geben Sie einen Pfad zum Speichern des Datenbank-Dumps an (Standardeinstellung: */tmp/mdm-server.sql*).
4. Geben Sie das Passwort des Datenbankbenutzers *innomms* an, falls erforderlich.
5. (Falls erforderlich) Wiederholen Sie Schritt 1 bis 4, **aber** führen Sie das Shell-Skript ***export_mdm_ca.sh*** aus, um einen Dump der *mdm-CA-Server-Datenbank* zu erstellen (Standardeinstellung: *mdm_ca_server.sql*, Datenbankbenutzer = *mdmca*).
6. Kopieren Sie die erstellten Datenbank-Dumps an einen sicheren Ort (beispielsweise ein sicheres Backup-Verzeichnis auf einem anderen Server im Unternehmen).

Führen Sie ein Upgrade von Ubuntu 16.04 auf Ubuntu 18.04 LTS durch

1. Laden Sie die Paketinformationen neu:

```
sudo apt update
```
2. Aktualisieren Sie die unter Ubuntu 16.04 LTS installierten Pakete:

```
sudo apt upgrade
```
3. Starten Sie das Upgrade auf Ubuntu 18.04 LTS:

```
sudo do-release-upgrade
```
4. Folgen Sie den Anweisungen auf dem Bildschirm oder drücken Sie gegebenenfalls die Enter-Taste, um das Upgrade fortzusetzen.

1.5.4 Kurzanleitung (Ubuntu): mdm 1.12.x auf 1.13.x upgraden



Wird mdm 1.13.x über die Kommandozeile aktualisiert, muss die Variable `DEBIAN_FRONTEND` mit dem Wert `readline` verwendet werden. Nur dann können die *Software License Terms* (SLT) angezeigt und akzeptiert werden.

1. Ändern Sie mit einem Text-Editor das *mdm software repository* in Ubuntu `/etc/apt/sources.list` von 1.12.x/ auf 1.13.x/:


```
sudo nano /etc/apt/sources.list
```
2. Alternativ können Sie das *mdm software repository* der Version 1.13.x auch mit folgendem Befehl zu Ihrer Paketverwaltung hinzufügen:


```
sudo apt-add-repository
„deb http://repositories.mguard.com/mdm 1.13.x/“
```
3. Laden Sie die Paketinformationen neu:


```
sudo apt update
```
4. Starten Sie das Upgrade auf mdm 1.13.x:


```
sudo DEBIAN_FRONTEND=readline apt upgrade
```
5. Bestätigen Sie die *Software License Terms* (SLT).

1.5.5 Kurzanleitung (Ubuntu): mdm 1.11.x auf 1.12.x upgraden

Gehe Sie prinzipiell so vor wie in Kapitel 1.5.4 beschrieben, wobei die Versionsangaben der Minor-Versionen jeweils um 1 reduziert werden müssen.

Repository: `deb http://repositories.mguard.com/mdm 1.12.x/`

1.5.6 Kurzanleitung (Ubuntu): mdm 1.10.x auf 1.11.x upgraden



Aktualisieren Sie Ihre mdm-Installation erst dann, wenn das Upgrade von Ubuntu 16.04 LTS auf **Ubuntu 18.04 LTS** vollständig und erfolgreich abgeschlossen wurde (siehe „Kurzanleitung: Ubuntu 16.04 auf 18.04 upgraden“ auf Seite 22).



Wird mdm 1.11.x über die Kommandozeile aktualisiert, muss die Variable `DEBIAN_FRONTEND` mit dem Wert `readline` verwendet werden. Nur dann können die *Software License Terms* (SLT) angezeigt und akzeptiert werden.

1. Ändern Sie mit einem Text-Editor das *mdm software repository* in Ubuntu `/etc/apt/sources.list` von 1.10.x/ auf 1.11.x/:


```
sudo nano /etc/apt/sources.list
```
2. Alternativ können Sie das *mdm software repository* der Version 1.11.x auch mit folgendem Befehl zu Ihrer Paketverwaltung hinzufügen:


```
sudo apt-add-repository
„deb http://repositories.mguard.com/mdm 1.11.x/“
```
3. Laden Sie die Paketinformationen neu:


```
sudo apt update
```
4. Starten Sie das Upgrade auf mdm 1.11.x:


```
sudo DEBIAN_FRONTEND=readline apt upgrade
```
5. Bestätigen Sie die *Software License Terms* (SLT).

1.5.7 PostgreSQL-Datenbanken (Cluster) updaten

Nach einem Upgrade von Ubuntu 16.04 LTS auf Ubuntu 18.04 LTS bleibt zunächst die Version *PostgreSQL 9.5* auf dem System installiert. Erst mit einem Upgrade der installierten mdm-Version auf mdm 1.11.x wird *PostgreSQL 10* installiert.

Die mit früheren mdm-Versionen erstellten *mdm-Server-* und *CA-Server-Datenbanken* wurden mit der *PostgreSQL 9.5* erstellt. Dies stellt allerdings kein Problem dar, da *PostgreSQL 10* abwärtskompatibel ist und mit älteren Versionen erstellte Datenbanken unterstützt.

Eine Anpassung der bestehenden *mdm-Server-* und *CA-Server-Datenbanken* ist daher für den Betrieb von mdm 1.11.0 und folgende mdm-Versionen nicht erforderlich!

1.6 Batch-Dateien und Shell-Skripte

Ein Dump und ein Import der Datenbanken kann mithilfe der von Phoenix Contact erstellten Batch-Dateien (Windows) und Shell-Skripten (Linux) ausgeführt werden, die über den PHOENIX CONTACT Webshop (phoenixcontact.net/produkt/2981974) erhältlich sind.



Die Migration der mdm-Installationen mittels **Batch-Dateien/Shell-Skripten** stellt lediglich die Datenbanken wieder her, von denen Dumps erstellt und importiert wurden. Jedwede anderen Installationsdaten (z. B. Pull-Server-Zertifikat und Konfigurationsdateien) müssen von Hand in die neue Installation einkopiert werden.



Die mitgelieferten Batch-Dateien bzw. Shell-Skripte können nur bei mdm Standardinstallationen verwendet werden (überprüfen Sie die voreingestellten Bezeichnungen der Datenbanken, Schnittstellen und Benutzernamen in den mitgelieferten Dateien *preferences.xml* und *ca-preferences.xml*).

Wenn mdm 1.13.x über den *mdm 1.13.x Installer für Windows* oder die Paketverwaltung von Ubuntu erfolgreich installiert wurde, wurden die Batch-Dateien/Shell-Skripte automatisch in folgenden Systemordnern installiert:

Microsoft Windows

mdm-Server und CA-Server: `<Pfad zur mdm-Installation>\data\db_migration\`

Ubuntu Linux

mdm-Server: `/usr/share/mdm-server/db_migration/`

mdm-CA-Server: `/usr/share/mdm-ca/db_migration/`

1.6.1 Batch-Dateien und Shell-Skripte

Tabelle 1-3 Windows Batch-Dateien

Name	Beschreibung
<i>export_mdm_server.bat</i>	Windows Batch-Datei zur Erstellung eines Dumps der mdm-Serverdatenbank
<i>export_mdm_ca.bat</i>	Windows Batch-Datei zur Erstellung eines Dumps der mdm-CA-Serverdatenbank
<i>import_mdm_server.bat</i>	Windows Batch-Datei zum Import des erzeugten Dumps der mdm-Serverdatenbank
<i>import_mdm_ca.bat</i>	Windows Batch-Datei zum Import des erzeugten Dumps der mdm-CA-Serverdatenbank

Tabelle 1-4 Linux Shell-Skripte

Name	Beschreibung
<i>export_mdm_server.sh</i>	Linux-Shell-Skript zur Erstellung eines Dumps der mdm-Serverdatenbank
<i>export_mdm_ca.sh</i>	Linux-Shell-Skript zur Erstellung eines Dumps der mdm-CA-Serverdatenbank
<i>import_mdm_server.sh</i>	Linux-Shell-Skript zum Import des erzeugten Dumps der mdm-Serverdatenbank
<i>import_mdm_ca.sh</i>	Linux-Shell-Skript zum Import des erzeugten Dumps der mdm-CA-Serverdatenbank

1.7 mdm 1.13.x Installer for Windows



Führen Sie das Installationsprogramm als **Lokaler Administrator** des Windows-Systems aus. Die Installation durch einen anderen Benutzer mit (**lediglich**) Administratorrechten kann zu einem Fehler führen.

Wenn Sie den mdm-Server, den Datenbankserver PostgreSQL und den mdm-CA-Server (falls zutreffend) auf einem einzigen Microsoft Windows System verwenden möchten, kann das automatische Installationsprogramm benutzt werden.

Das Installationsprogramm kann zusätzlich den Server als Pull-Server für die Konfiguration (siehe „Konfigurationen in mGuard-Geräte hochladen“ im [mdm-Benutzerhandbuch](#)) oder als Firmware-Upgrade-Server einrichten (siehe „Firmware-Upgrades mit mdm verwalten“ im [mdm-Benutzerhandbuch](#)).

Voraussetzungen

Es gelten die folgenden Systemanforderungen und Voraussetzungen (siehe Tabelle 1-1 auf Seite 6).

Lizenzdatei installieren

Kopieren Sie die Lizenz in ein Verzeichnis Ihrer Wahl. Während der Installation werden Sie nach der Datei gefragt. Der Pfad der Lizenzdatei kann anschließend in der Datei *preferences.xml* konfiguriert werden (siehe „mdm-Server (Datei preferences.xml)“ im [mdm-Benutzerhandbuch](#)). Installieren Sie die Lizenzdatei vor dem Hochfahren des Servers.



Wenn während der Installation keine Lizenzdatei angegeben wird, startet der mdm-Server im **Evaluierungsmodus** (Evaluation License) mit einer Anzahl von zehn verwendbaren Geräten und zwei gleichzeitig angeschlossenen Clients. Eine Lizenz können Sie im Webshop von PHOENIX CONTACT auf der Seite phoenixcontact.net/product/2981974 erwerben.

Installation mdm

Gehen Sie zur Installation von mdm auf einem unterstützten Microsoft Windows-System wie folgt vor:

1. Stellen Sie sicher, dass die Systemanforderungen aus Tabelle 1-1 erfüllt sind.
2. Installieren Sie das Paket *Microsoft Visual C++ 2015-2019 Redistributable Package (x64)* (oder neuer).

Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14....

Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29325

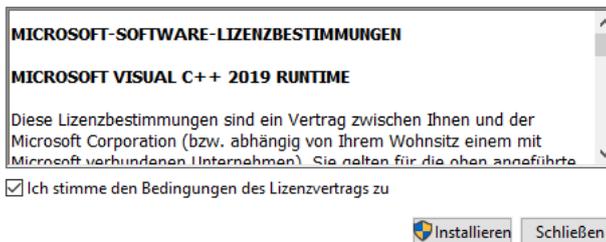


Bild 1-1 *Microsoft Visual C++ 2015-2019 Redistributable Package (x64)* installieren

3. Führen Sie den *mdm Installer for Windows* als **Lokaler Administrator** des Windows-Systems aus.
4. Klicken Sie auf dem Startbildschirm auf die Schaltfläche **Next >** und akzeptieren Sie auf den folgenden Bildschirmen die Softwarelizenzen für mdm und Drittanbieter.

- Wählen Sie ein Verzeichnis zur Installation von mdm aus. Normalerweise braucht das als Standard verwendete Zielverzeichnis nicht geändert zu werden.

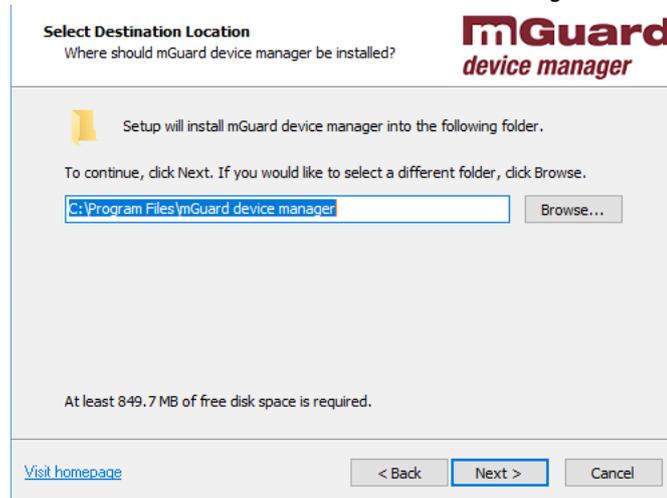


Bild 1-2 Zielverzeichnis auswählen

- Wählen Sie, welche Komponenten von mdm Sie installieren möchten.
Hinweis: Die Benachrichtigung, dass ein Upload auf ein FL MGUARD 1000-Gerät erfolgreich durchgeführt wurde oder fehlgeschlagen ist, kann nur an den mdm zurückgemeldet und dort angezeigt werden, wenn die Option „*mdm Windows Pull Feedback*“ ausgewählt wurde.

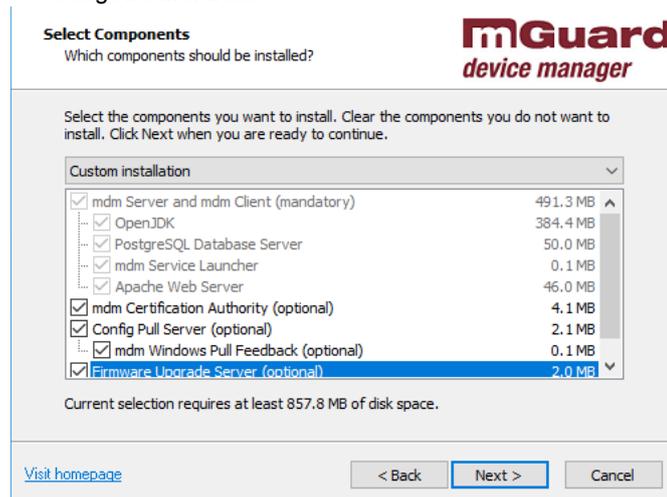


Bild 1-3 mdm Komponenten installieren

Der mdm-Server, OpenJDK, PostgreSQL Database Server, mdm Service Launcher (zur Ausführung des mdm-Servers als Service) und Apache Webserver werden immer installiert. Die mdm Certification Authority (CA) ist eine Option. Optional kann der Apache Webserver auch als *Configuration-Pull-Server* und Server für Firmware-Upgrades eingerichtet werden.



Der mdm-Client steht über den Webserver anderen Hosts zur Verfügung. Die Hosts müssen Java 11 unterstützen (systemweit oder mittels lokalem Java-Binary). Zum Ausführen des Clients die ZIP-Datei vom Webserver herunterladen, entpacken und die Datei `mdm-client-1.13.x.jar` starten.

7. Geben Sie eine Lizenzdatei für den mdm-Server an oder überspringen Sie die Installation der Lizenzdatei, um mdm im Evaluierungsmodus auszuführen.

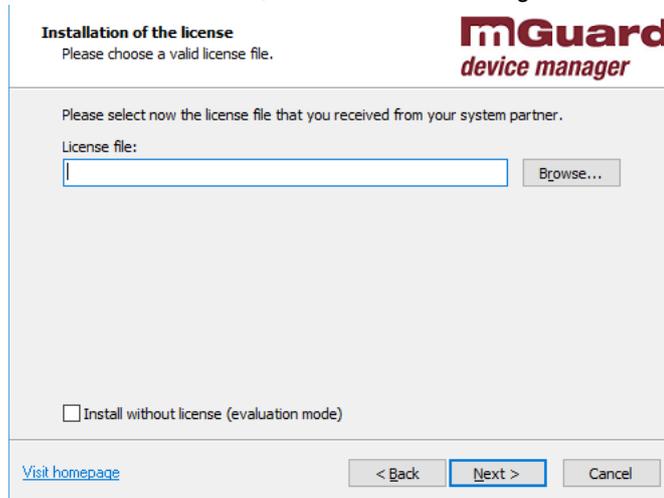


Bild 1-4 Installation der Lizenz

8. Das Installationsprogramm erstellt ein selbstsigniertes X.509-Zertifikat und einen passenden privaten Schlüssel zur Verwendung durch den HTTPS-Webserver. Geben Sie die für das Zertifikat zu verwendenden Attribute ein.

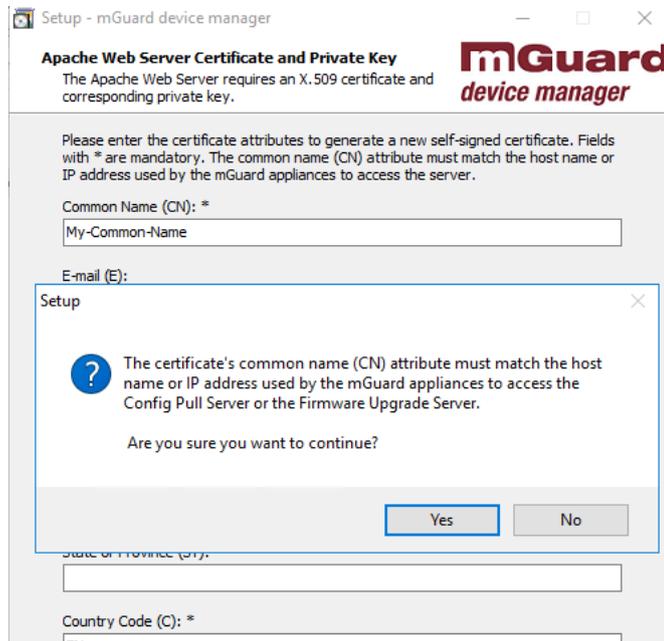


Bild 1-5 Für das Zertifikat zu verwendende Attribute

9. Der Zugriff auf die durch den Webserver geschützten Verzeichnisse kann optional mit Benutzernamen und Passwort geschützt werden. Wählen Sie, ob Sie diesen Schutz wünschen und geben Sie ggf. Benutzernamen und Passwort ein.

The screenshot shows a window titled "Setup - mGuard device manager" with the mGuard device manager logo. The main heading is "Apache Web Server" with the subtitle "Advanced configuration". The text reads: "You have the opportunity to protect web access to the directory with a username and password." There is a checked checkbox for "Use Apache web directory access protection". Below this are three input fields: "Username:" with the value "mdm", "Password:", and "Repeat password:". At the bottom, there are buttons for "< Back", "Next >", and "Cancel", along with a "Visit homepage" link.

Bild 1-6 Apache Webserver – Schutz bei Webzugriff

10. Folgendes gilt nur, wenn die mdm CA installiert ist: Das Installationsprogramm erstellt ein CA-Zertifikat mit passendem privaten Schlüssel. Geben Sie die für das Zertifikat zu verwendenden Attribute ein.

The screenshot shows a window titled "Setup - mGuard device manager" with the mGuard device manager logo. The main heading is "CA Certificates and Private Keys" with the subtitle "The CA Server requires an X.509 certificate and corresponding private key." The text reads: "Please enter the certificate attributes to generate a new CA certificate. Fields with * are mandatory." There are several input fields: "Common Name (CN): *" with the value "CA_SERVER_CN", "E-mail (E):", "Organizational Unit (OU): *", "Organization (O): *", "Locality (L):", "State or Province (ST):", "Country Code (C): *" with the value "EN", and "Certificate Validity End Date: *" with the value "5/7/2069".

Bild 1-7 Für das Zertifikat zu verwendende Attribute

11. Das Installationsprogramm kann optional Verknüpfungen zum Startmenü hinzufügen. Wählen Sie in diesem Fall ein Verzeichnis aus, zu dem die Verknüpfungen hinzugefügt werden sollen.

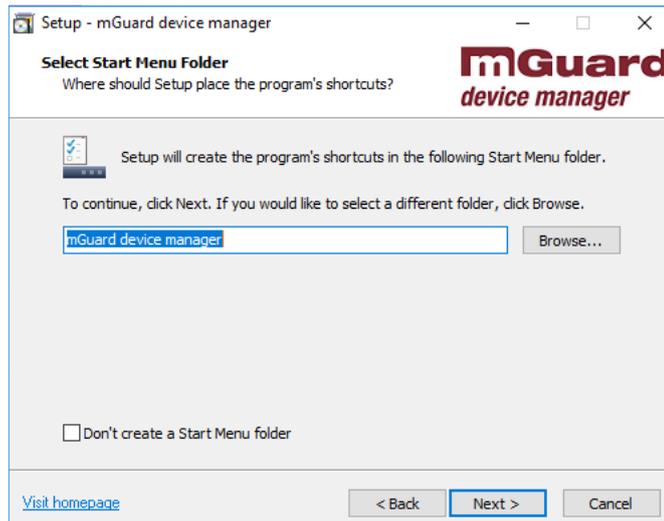


Bild 1-8 Startmenüordner – Verknüpfungen (Shortcuts)

12. Klicken Sie auf die Schaltfläche **Install**.



Bild 1-9 Installation von mdm

Die mdm Komponenten werden im System installiert. Die durch den Apache Webserver bedienten Orte werden in einem Bericht aufgeführt. mdm kann jetzt verwendet werden.

1.8 Paketverwaltung von Ubuntu

Zur Installation der folgenden mdm Komponenten auf Ubuntu Linux kann die automatische Installation über die Paketverwaltung von Ubuntu und das *mdm software repository* genutzt werden.



Datenschutzhinweis: Der Zugriff auf den *mdm-Repository-Server* wird protokolliert, um die Sicherheit und Stabilität des Dienstes zu gewährleisten. Für statistische Auswertungen werden nur anonymisierte Daten gespeichert.

Tabelle 1-5 Installierbare Pakete aus dem *mdm software repository*

Paket	Beschreibung
<i>mdm-all-server</i>	Metapaket zur Installation aller mdm-Serverkomponenten.
<i>mdm-common</i>	Enthält grundlegende Komponenten, die für die Installation von mdm vorausgesetzt werden.
<i>mdm-server</i>	Enthält die Serverkomponenten von mdm. Startet als systemd -Service.
<i>mdm-client</i>	Enthält die Client-Komponenten von mdm. Startet als systemd -Service.
<i>mdm-ca</i>	Enthält die CA-Komponenten von mdm (CA-Server).
<i>mdm-configpull</i>	Richtet den Apache2-Server so ein, dass die mdm Konfiguration gezogen werden kann (siehe mdm-Benutzerhandbuch).
<i>mdm-clientdownload</i>	Richtet den Apache2-Server so ein, dass der mdm-Client heruntergeladen werden kann.
<i>mdm-webbase</i>	Konfiguriert Apache2 für mdm und ermöglicht die Verwendung als Firmware-Server (siehe mdm-Benutzerhandbuch).

Der Datenbankserver *PostgreSQL* und *OpenSSL* werden automatisch aus den Standard-Repositories von Ubuntu installiert.

Voraussetzungen

Es gelten die folgenden Systemanforderungen und Voraussetzungen (siehe Tabelle 1-2 auf Seite 14).

Lizenzdatei installieren

Speichern Sie die Lizenzdatei unter */etc/mdm/mdm-server/mdmlic.lic*. Der Pfad der Lizenzdatei kann anschließend in der Datei *preferences.xml* konfiguriert werden (siehe [mdm-Benutzerhandbuch](#)). Wenn Sie keinen Pfad für die Lizenzdatei in der Datei *preferences.xml* angeben, geht mdm davon aus, dass sich die Lizenzdatei im gleichen Verzeichnis befindet wie der mdm-Server.

Installieren Sie die Lizenz vor der Installation des mdm-Serverpakets in */etc/mdm/mdm-server/mdmlic.lic* und erstellen Sie dabei den benötigten Pfad, oder führen Sie nach Installation einer neuen Lizenz manuell einen Neustart des Servers durch.

1.8.1 Vollständige mdm-Installation über die Paketverwaltung

Gehen Sie zur Installation von mdm und den Komponenten auf Ubuntu (Server) 18.04 LTS mit der Paketverwaltung von Ubuntu wie folgt vor:



Sie benötigen Administrator-Rechte, um mdm und Komponenten zu installieren.



Achten Sie darauf, dass das korrekte Repository zur Datei `/etc/apt/sources.list` hinzugefügt wurde. Überprüfen Sie die Integrität des bereitgestellten Schlüssels des Repositorys.



Wird mdm 1.13.x über die Kommandozeile installiert, muss die Variable `DEBIAN_FRONTEND` mit dem Wert `readline` bei der Installation des Pakets `mdm-common` verwendet werden. Nur dann können die *Software License Terms* (SLT) angezeigt und akzeptiert werden.



Kopieren Sie vor der Installation Ihre mdm-Lizenzdatei `mdmlic.lic` in das Verzeichnis `/etc/mdm/mdm-server/` (Voreinstellung in `preferences.xml`).

1. Laden Sie den öffentlichen Schlüssel des Repositories (`pubkey.gpg`) herunter:

```
wget http://repositories.mguard.com/pubkey.gpg
```
2. Überprüfen Sie den Fingerabdruck des öffentlichen Schlüssels:

```
gpg -finger pubkey.gpg
```

Der Fingerabdruck **muss** mit dem folgenden Fingerabdruck übereinstimmen:
AD3E B1F9 473D 5CC7 2ED4 2D4C 0571 79A3 CC0F FA55.
3. Fügen Sie den öffentlichen Schlüssel des Repositories (`pubkey.gpg`) zum öffentlichen GPG-Schlüsselring (`trusted.gpg`) hinzu:

```
sudo apt-key add pubkey.gpg && apt-key list
```
4. Fügen Sie das *mdm software repository* zu Ihrer Paketverwaltung hinzu:

```
sudo apt-add-repository  
„deb http://repositories.mguard.com/mdm 1.13.x/“
```
5. Laden Sie die Paketinformationen neu:

```
sudo apt update
```
6. Suchen Sie nach dem Term `mdm`, um die verfügbaren mdm-Pakete anzuzeigen:

```
sudo apt search mdm
```
7. Installieren und bestätigen Sie zunächst die *Software License Terms* (SLT):

```
sudo DEBIAN_FRONTEND=readline apt install mdm-common
```
8. Installieren Sie mdm und Serverkomponenten:

```
sudo apt install mdm-all-server
```

Folgen Sie den Anweisungen auf dem Bildschirm und geben Sie die erforderlichen und optionalen Parameter ein (z. B. für CA-Komponenten und *Configuration-Pull-Server*).
9. Installieren Sie den mdm-Client über die Paketverwaltung:

```
sudo apt install mdm-client
```

1.8.2 Schnelle Installation des mdm-Servers und -Clients (vollständige Installation)

```
wget http://repositories.mguard.com/pubkey.gpg
sudo apt-key add pubkey.gpg
sudo apt-add-repository "deb http://repositories.mguard.com/mdm
1.13.x/"
sudo apt update
sudo DEBIAN_FRONTEND=readline apt install mdm-common
sudo apt install mdm-all-server mdm-client
```

1.8.3 Server-Log-Dateien analysieren

mdm-Server

Ausgabe der kompletten Log-Einträge des mdm-Servers:

```
journalctl -u mdm-server.service
```

Ausgabe der Log-Einträge des mdm-Servers seit dem letzten Neustart:

```
journalctl -b -u mdm-server.service
```

mdm-CA-Server

Ausgabe der kompletten Log-Einträge des mdm-CA-Servers:

```
journalctl -u mdm-ca.service
```

Ausgabe der Log-Einträge des mdm-CA-Servers seit dem letzten Neustart:

```
journalctl -b -u mdm-ca.service
```

Die Log-Dateien des mdm-CA-Servers werden von Ubuntu darüber hinaus in folgender Datei gespeichert: */var/log/mdm-ca.log* .

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.

Dieses Handbuch ist einschließlich aller darin enthaltenen Abbildungen urheberrechtlich geschützt. Jegliche Veränderung des Inhaltes oder eine auszugsweise Veröffentlichung sind nicht erlaubt.

Phoenix Contact behält sich das Recht vor, für die hier verwendeten Produktkennzeichnungen von Phoenix Contact-Produkten eigene Schutzrechte anzumelden. Die Anmeldung von Schutzrechten hierauf durch Dritte ist verboten.

Andere Produktkennzeichnungen können gesetzlich geschützt sein, auch wenn sie nicht als solche markiert sind.

So erreichen Sie uns

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen Geschäftsbedingungen finden Sie im Internet unter:

phoenixcontact.com.

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.

Diese steht unter der folgenden Adresse zum Download bereit:

phoenixcontact.net/products.

Ländervertretungen

Bei Problemen, die Sie mit Hilfe dieser Dokumentation nicht lösen können, wenden Sie sich bitte an Ihre jeweilige Ländervertretung.

Die Adresse erfahren Sie unter phoenixcontact.com.

Herausgeber

PHOENIX CONTACT GmbH & Co. KG

Flachmarktstraße 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