

Using mdm 1.16.x in the mdm VA

User manual

User manual
Using mdm 1.16.x in the mdm VA

UM EN MDM VA, Revision 01 2024-07-22

This user manual is valid for:

Designation	Item No.
FL MGUARD DM UNLIMITED	2981974

110903_en_01

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

Table of contents

1 Introduction 5
1.1 Note for Windows users 5
1.2 Required files 6
1.3 System requirement 6
1.4 Additional requirements 6

2 Installing the mdm VA 7
2.1 Importing the Ubuntu Cloud image into VirtualBox 7
2.2 Adding the configuration file 8
2.3 Increasing the main memory 10
2.4 Adapting the MAC address 10
2.5 Starting mdm VA for the first time (initialization) 11

3 Configuring the mdm VA (WBM) 13
3.1 Log in via web browser 13
3.2 Activating administrative access 14
3.3 Using the terminal 14
3.4 Changing the password for the VA user 14
3.5 Adapting the network settings 15
3.6 Updating the software 16
3.7 Changing the display language 17

4 Installing mdm 19
4.1 Available mdm components 20
4.2 Performing the installation 21
4.2.1 Quick installation 21
4.2.2 Individual installation (apt) 21
4.2.3 Making specific settings 22
4.3 Adapting the components (optional) 25
4.3.1 Configuring the mdm server (preferences) 25
4.3.2 Activating or changing the web server authentication 25
4.3.3 Changing the web server certificate 26
4.3.4 Changing the CA server certificate 26
4.4 Applying for, using and activating a license 27
4.4.1 Requesting a new mdm license with new MAC address 27
4.4.2 Using an existing mdm license in mdm VA 27
4.4.3 Activating an mdm license in mdm VA 27
4.5 Using the mdm client 28

5 Migrating data 29
5.1 Migrating data from mdm 1.13.x (from Windows) 29
5.2 Migrating data from mdm as of 1.14.x (from mdm VA) 31
5.3 Migrating mdm databases 32

6 Update, backup, and support 33
6.1 Update mdm in the mdm-VA to the next minor version 33
6.2 Updating Ubuntu and mdm (Patch updates) 34
6.3 Backup and restore of the mdm databases 35
6.4 Backup and restore of the entire mdm installation 36
6.5 Creating a support snapshot 38

7 Appendix 39
7.1 Using Windows tools for remote access 39
7.1.1 PuTTY 40
7.1.2 WinSCP 41
7.2 Automating tasks in Windows 42
7.2.1 Backing up mdm databases (sample script) 43
7.2.2 Backing up the mdm installation (sample script) 43
7.3 Uploading the mGuard firmware update repository to the mdm web server 45
7.4 Installing mdm repository and mdm via console 47
7.5 Changing the keyboard layout of the mdm VA via console 48
7.6 Adapting the network settings via console 49
7.7 File locations in mdm VA and web server URLs 50

1 Introduction

With mdm 1.14.0 and higher, no version of the "*mdm installer for Windows*" is provided any more. This means that mdm 1.14.0 and subsequent versions can no longer be installed on a Windows system.

Updates are likewise not supported on a Windows system.

mdm 1.16.x

To be able to run mdm 1.16.x on a Windows system, you can, however, use the virtual machine "mdm VA" with an installed Ubuntu operating system (VA = *Virtual Appliance*).

The mdm VA is provided as an OVA file. It can be run with a suitable virtualization software program. This document describes how to use the *VirtualBox* virtualization software using an example.

The mdm VA is preconfigured by means of a configuration file provided by Phoenix Contact and enables the easy installation of mdm 1.16.x. Configuration and the mdm installation are performed via a web browser (WBM).

NOTE: With mdm 1.15.0 and higher, devices of the FL MGUARD 1000 series with the mGuard NT firmware version installed are no longer supported.

The required steps for installing mdm version 1.16.0 are described in this document:

1. Download *VirtualBox* and install it in Windows
2. Download the mdm VA and import it into *VirtualBox*
3. Download the configuration file and add it to the mdm VA
4. Installing mdm 1.16.x in the mdm VA
5. Migrating mdm databases from mdm (mdm 1.13.x to 1.15.x) to mdm 1.16.x

1.1 Note for Windows users

To install mdm in the mdm VA from your Windows system and configure it in the usual manner, you do not need to log in to the VA directly. Instead, you can connect to the VA via the network from your Window system.

Web interface

With mdm 1.15.0 and higher, a graphical user interface (web-based management – WBM) is provided for the mdm VA, via which the necessary settings for configuring the mdm VA as well as installing and updating mdm can be made via a web browser (see Section 3).

Options for connecting to the mdm VA

In addition to access via the WBM (HTTPS), you can also connect to the mdm VA via the SSH and SCP protocols.

1. **SSH** (secure shell): For accessing the command line of the mdm VA
2. **SCP** (secure copy): For copying files between Windows and the mdm VA

You can e.g., use the third-party programs *PuTTY* (SSH client) and *WinSCP* (SCP-Client), which are described in more detail in Section 7.1.

1.2 Required files

Installation

1. **VirtualBox** (or another virtualization solution)
   Download the latest version of the virtualization solution (e.g., *VirtualBox* from Oracle®) for your operating system from a trustworthy source (e.g., virtualbox.org).
2. **Ubuntu Cloud image**
   Download the file *ubuntu-22.04-server-cloudimg-amd64.ova* from the ubuntu.com website: Link --> cloud-images.ubuntu.com
   Verify the authenticity and integrity of the downloaded file on the basis of the specified checksums: https://cloud-images.ubuntu.com/releases/22.04/release/
3. **Configuration file**
   The configuration file "*user-data-1.16.0.iso*" is part of the installation package of the corresponding mdm version (FL MGUARD DM UNLIMITED_1.16.7z) and can be downloaded from the PHOENIX CONTACT web shop: phoenixcontact.net/product/2981974.

Migration

4. **Migration (from mdm 1.13.x / Windows)**
   The "*mdm-datacollector*" and "*mdm-winrestore*" programs, which are required for mdm migration from mdm 1.13.x (installed under Windows) to mdm 1.16.x (installed in the modern VA), are available once the mdm has been installed in the mdm VA: *mdm-datacollector* is offered for download at the mdm web server address once the *mdm-clientdownload* component has been installed in the mdm VA (see Section 4):
   - For this, connect to the mdm web server at the configured IP address: https://<IP address>/mdm
5. **Migration (from mdm 1.14.x or 1.15.x / Ubuntu)**
   The "*mdm-backup*" and "*mdm-restore*" programs, which are required for mdm migration from mdm 1.14.x/1.15.x to mdm 1.16.x, are available after the mdm installation in the respective mdm VA.

1.3 System requirement

System requirements for the mdm VA

- Main memory (RAM): at least 4096 MB
- Hard disk space: at least 10 GB

Note that the main memory and hard disk space assigned to the mdm VA will then no longer be available to the host system (e.g., Windows).

1.4 Additional requirements

The following prerequisites must be met for initial startup of the mdm VA:

1. The mdm VA must be able to access the Internet.
2. The mdm VA must initially receive its IP settings from a DHCP server.
   A corresponding DHCP server must be available in the network.

2 Installing the mdm VA

If the *VirtualBox* program is already installed on your Windows system, you must update it to the latest version.

Version 1.16.x of the mGuard device manager can be installed and run with very little effort on the virtual machine (mdm VA) that has been partially preconfigured by Phoenix Contact.

The basis of the virtual machine is the *Ubuntu Cloud image* provided by Ubuntu (Ubuntu version 22.04 LTS).

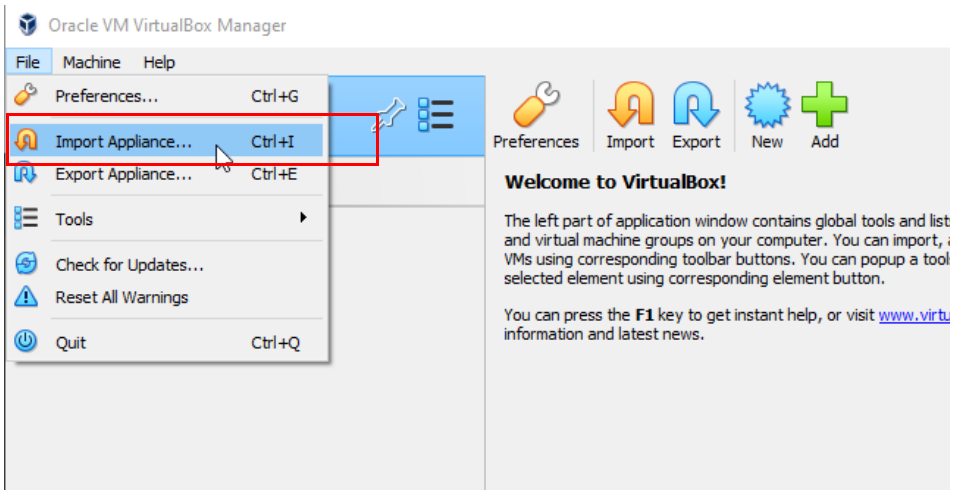
2.1 Importing the Ubuntu Cloud image into VirtualBox

To import the *Ubuntu Cloud image* into VirtualBox, proceed as follows:

Make the required files available on the Windows system (see Section 1.2):

- Virtual machine: *"ubuntu-22.04-server-cloudimg-amd64.ova"*
- Configuration file: "*user-data-1.16.0.iso*"

- Install the *VirtualBox* program on the Windows system on which mdm 1.16.x is to run. (Use the latest version.)
- Start *VirtualBox* on the Windows system.
- Open the "**File >> Import Appliance ...**" menu item.



- Select the file with the file name "*ubuntu-22.04-server-cloudimg-amd64.ova*", click on "**Next**", and then on "**Finish**".

↪ The virtual machine is imported into *VirtualBox* with the following name: *ubuntu-jammy-22.04-cloudimg-<DATE>*.

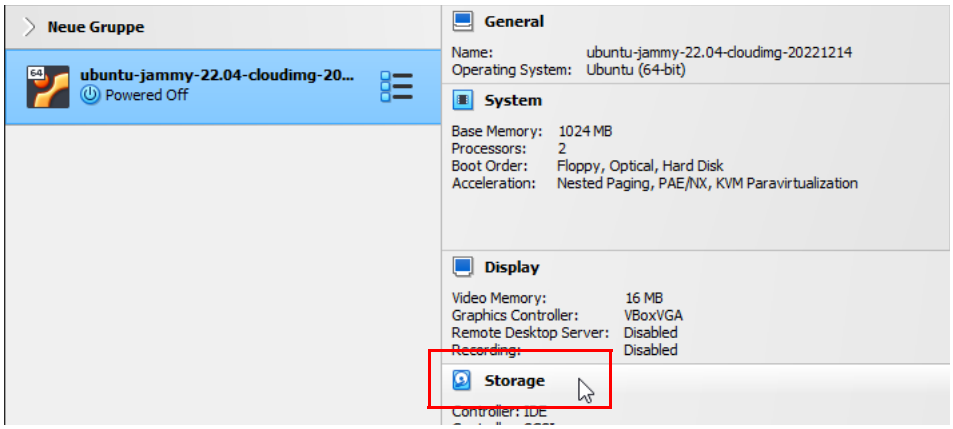
Before you start the virtual machine, you must add the configuration file from Phoenix Contact to the mdm VA in the next step (see Section 2.2).

2.2 Adding the configuration file

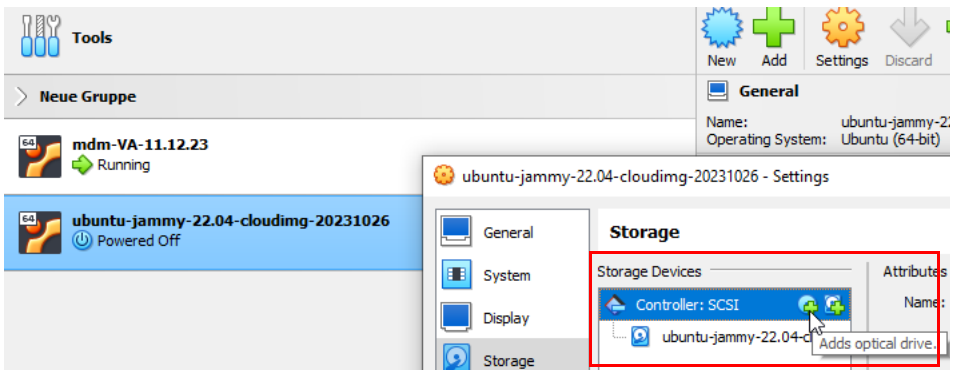
Before starting the virtual machine for the first time, you must add the configuration file provided by Phoenix Contact to the mdm VA.

Proceed as follows:

- In *VirtualBox*, highlight the imported visual machine, *ubuntu-jammy-22-cloudimg* [...].
- Open the *Mass Storage* configuration.

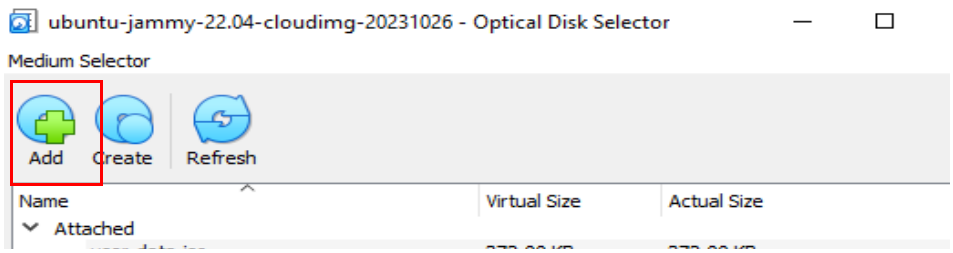


- Remove the *Controller: Floppy* and *Controller: IDE* menu items.
- Click on the *Controller: SCSI menu item*



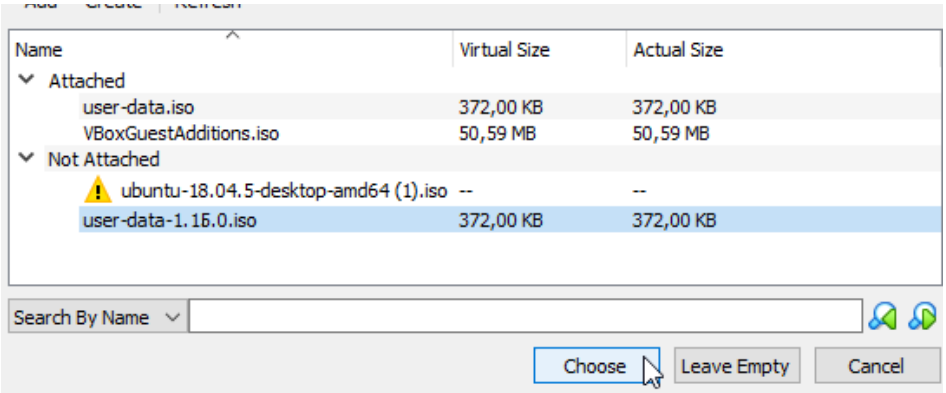
- There, click on the *Add optical drive* icon.

↪ The *Optical Disc Selector* window opens.

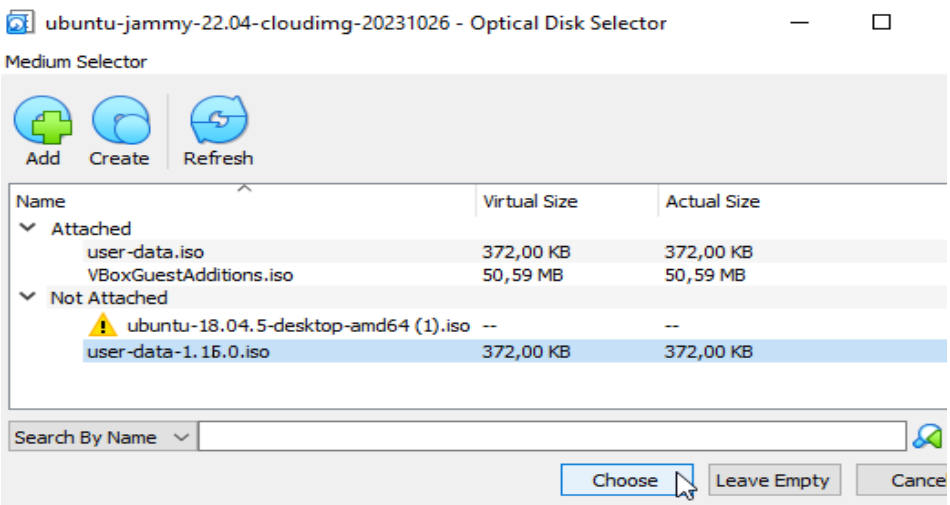


- There, click on the *Add* icon.

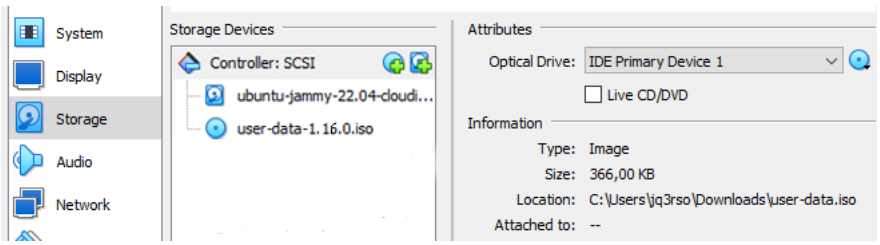
- Switch to the directory containing the file “*user-data-1.16.0.iso*”.
- Select the file and then click on *Open*.



↪ The file “*user-data-1.16.0.iso*” is added to the list of optical media.



- Select the file, then click on *Choose*.
- Click on *OK* to apply the settings.



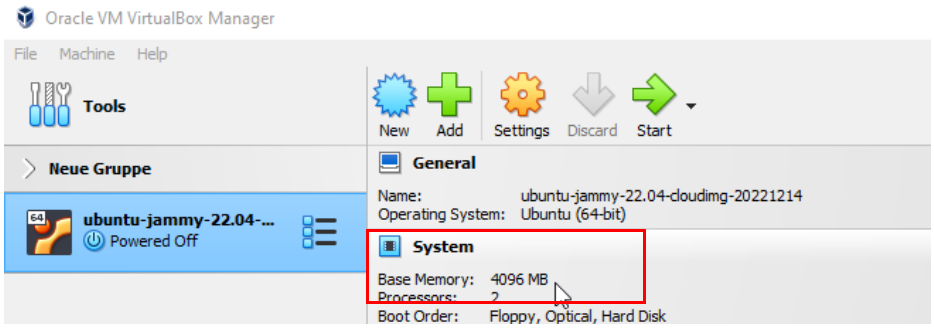
↪ The configuration file is added to the mdm VA.

↪ The virtual machine is configured and starts the Ubuntu 22.04 operating system.
  - User name: *vadmin*
  - Password: *private*

2.3 Increasing the main memory

To meet the memory requirements of the mdm server, you must customize the system settings of the mdm VA:

- Highlight the imported virtual machine, *ubuntu-jammy-22-cloudimg* [...]
- Open the *System* configuration.



- Click on the *Main memory* menu item.
- Increase the main memory (RAM disk) to at least 4096 MB.
- Click on *OK*.

Note that the main memory assigned to the mdm VA will then no longer be available to the host system (e.g., Windows).

2.4 Adapting the MAC address

The mdm license involving a charge for running FL MGUARD DM UNLIMITED is always linked to a MAC address specified during the license assignment, which must be used to run the mdm instance (mdm server) (see Section 4.4).

If you want to migrate mdm from an existing mdm installation to the mdm VA and continue using an already acquired mdm license, proceed as follows:

NOTE: Assigne the MAC address in the network to only one device
A MAC address may only be assigned to one device or network interface in a network. Make sure that the MAC address used is not used by multiple instances after a migration from another mdm installation.

- Open the purchased mdm license with a text editor.
- Determine the MAC address that was assigned to the mdm license.
- In *VirtualBox*, highlight the imported visual machine, *ubuntu-jammy-22-cloudimg* [...].
- Shut down the virtual machine if it has already been started.
- Open the *Network* configuration.
- Click on *Advanced.*
- Change the MAC address of the virtual machine (mdm VA).
  (Note that the MAC address must be specified without colons.)
- Click on *OK*.

Note: A granted mdm license may only be used to run a single mdm instance (mdm server).

2.5 Starting mdm VA for the first time (initialization)

Requirements:

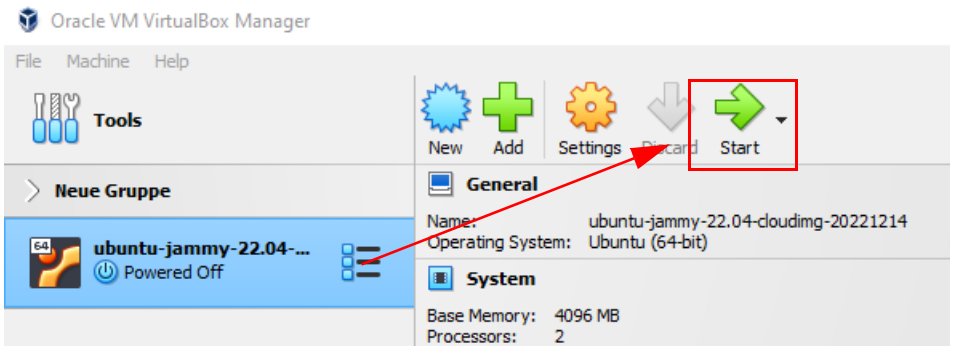
The mdm VA must be able to access the Internet.

The mdm VA must initially receive its IP settings from a DHCP server.
A corresponding DHCP server must be available in the network.

The initialization is only successful if the mdm VA has automatically terminated itself once during initialization.

To configure Ubuntu 22.04 on the virtual machine, proceed as follows:

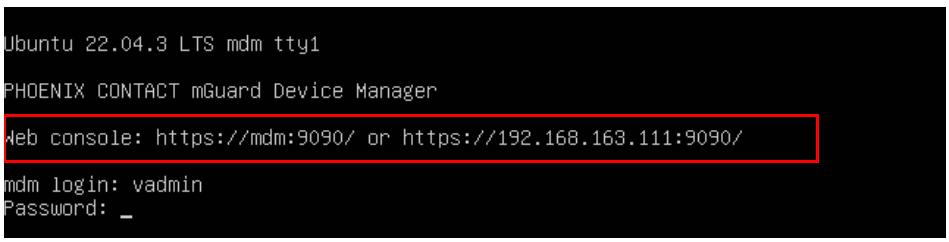
- Start the *VirtualBox* program.
- Highlight the imported virtual machine, *ubuntu-jammy-22-cloudimg* [...]
- Click on the "**Start**" icon to start the virtual machine.



↪ The mdm VA virtual machine is started and initialized.
↪ The initialization process can take several minutes.
↪ After initialization, the mdm VA is automatically shut down and terminated.

- **Important**: Be sure to wait until the mdm VA shuts itself down automatically.
- **Important**: Before restarting the mdm VA, remove the file *1.16.0-user-data.iso* from the optical drive.
- Restart the mdm VA.

↪ The mdm-VA obtains its network settings from a DHCP server (if available). The IP address under which you can reach the VA is displayed.



↪ You can now log in to the mdm VA using a web browser (HTTPS).
   a) to configure it (see Section 3),
   b) to customize its network configuration (see Section 3.5),
   c) to install and configure mdm 1.16.x (see Section 4).

If you have initialized the mdm VA without an existing Internet connection and without an existing DHCP server, there is no network connection to the mdm VA and you can only log in directly.
In this case, you should discard the mdm VA you have just installed. Then establish an Internet connection and DHCP address assignment and reinstall the mdm VA as described in this document.

Alternatively, in this case you can also assign a static IP configuration to the mdm VA (see Section 7.6). Then install the desired components of mdm 1.16.x as described in the manual 111024_en_xx at phoenixcontact.net/product/2981974 (Section 2.1.4).

3 Configuring the mdm VA (WBM)

3.1 Log in via web browser

After installation, a graphical user interface of the mdm VA (WBM) can be accessed via HTTPS via a web browser. You can log into the mdm VA in the web browser and make further settings. A Linux terminal is provided in the web browser, which can be used to make further settings.

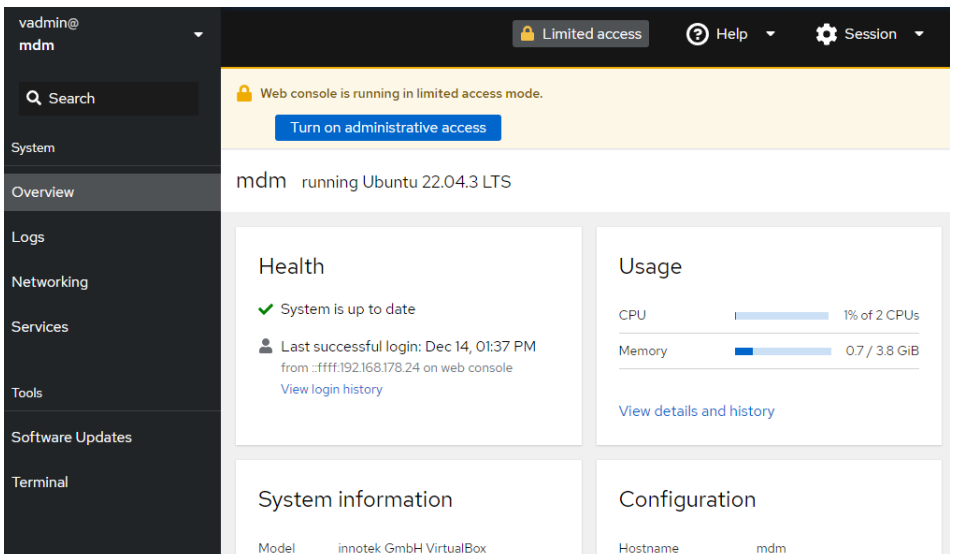
To log into the mdm VA using a web browser (HTTPS), proceed as follows:

- Start a web browser and enter the IP address or host name of the mdm VA (https://<IP address>:9090 or https://mdm:9090).

↪ The login window appears.



- Log in as “*vadmin*” user with the password “*private*”.



↪ You have logged into the mdm VA and can make further settings in the web browser.

3.2 Activating administrative access

After logging into the mdm VA, the user only has limited user rights (“Limited access”).

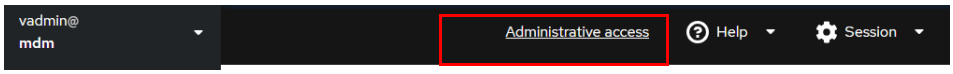
To make changes or to install and configure mdm, you must assign administrator rights to the user.

Proceed as follows:



- Click on the “Limited access” button.

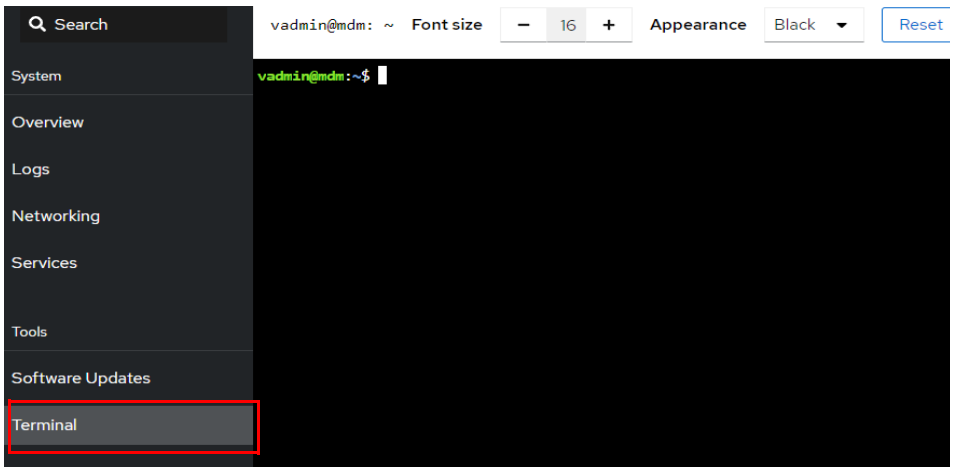
↪ “Administrative access” is activated.



↪ The *vadmin* user is given full administrator rights.

3.3 Using the terminal

The web interface of the mdm VA provides a command line (terminal window) in which you can execute the commands for configuring the mdm VA or for installing and managing mdm.



3.4 Changing the password for the VA user

NOTE: Should you forget the newly selected password, you will no longer be able to access the VA and thus the mdm installation. In this case, you would need to reinstall the VA.

- Open the command line (terminal).
- To change the default password of the “*vadmin*” user, run the following command: **passwd**
- Follow the instructions on the screen.

3.5 Adapting the network settings

In the “Network” menu item, you can configure the network settings for the network interface used for the mdm VA.

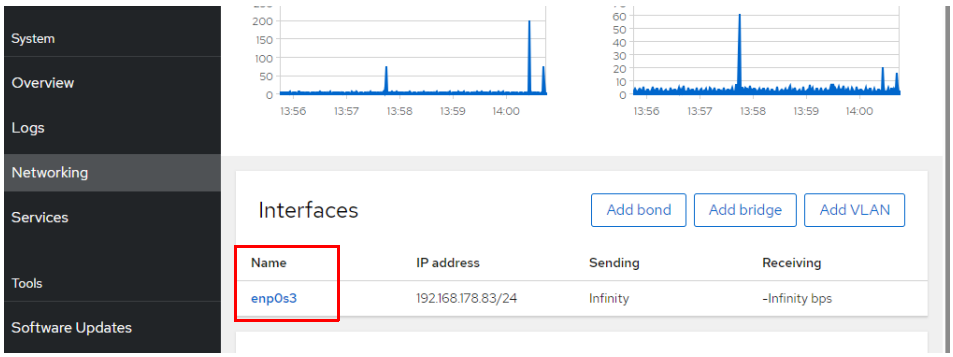
Using static network settings instead of DHCP

In the default setting, the mdm VA gets its network settings from a DHCP server.

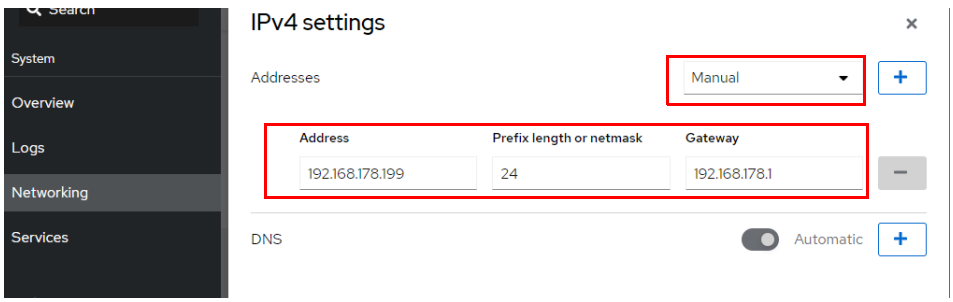
If you instead want to integrate the mdm VA to your network via a static IP configuration, proceed as follows:

Note that the current connection to the mdm VA will be terminated after the IP address is reconfigured. You need to log in again to the newly assigned static IP address.

- Network menu: Click on the name of the network interface (*enp0s3*).



- If the setting is “IPv4 Automatic (DHCP)”: Click on “Edit”.
- From the drop-down menu: Select the “Manual” entry.



- Enter a static IP address, a netmask, and a default gateway.
- Optional: Configure additional network parameters, if necessary.
- Click on the “Apply” button.

↪ A warning message appears.

- Click on the “Bridge Port Settings” button to apply the new network configuration.

↪ The network connection is interrupted and static network configuration is activated.

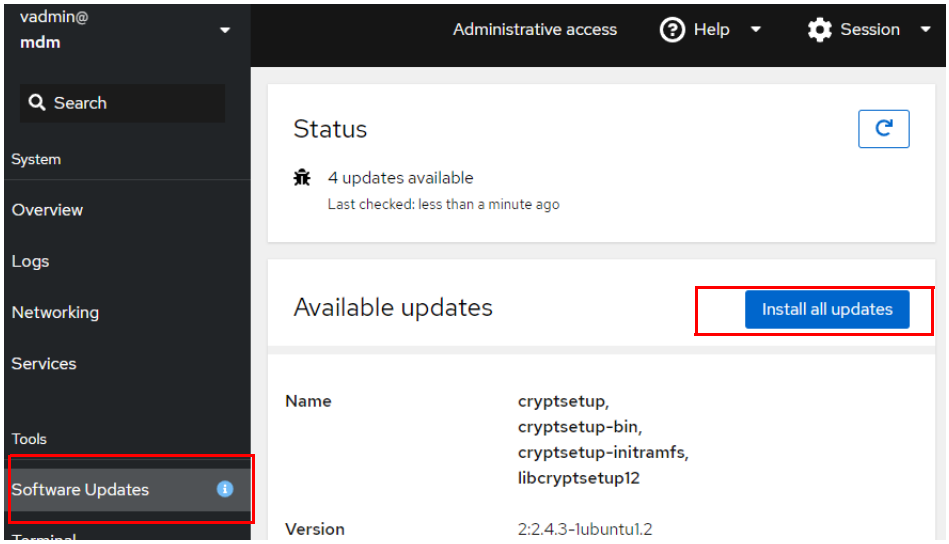
↪ You can now use the **new static IP address** to connect to the mdm VA.

3.6 Updating the software

You can use the “Software update” menu item to check whether the software packages of the mdm VA (Ubuntu base system) and installed mdm components are up-to-date. Updates provided can be installed from the configured package sources.

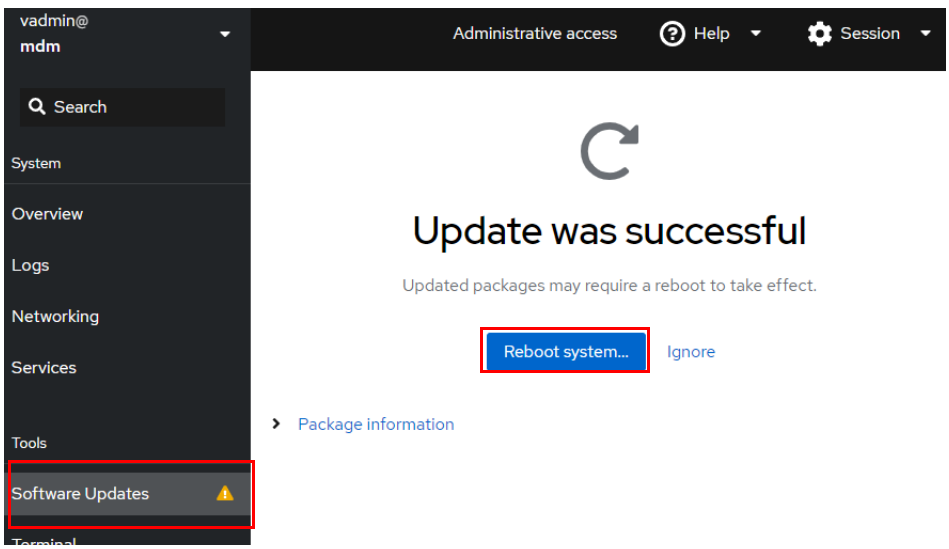
Proceed as follows:

↪ “Software Updates” menu: All outdated packets are displayed.



- Click on “Install all updates” button.

↪ All available updates for packages from the configured package sources are installed.



- Restart the mdm VA to complete the process.

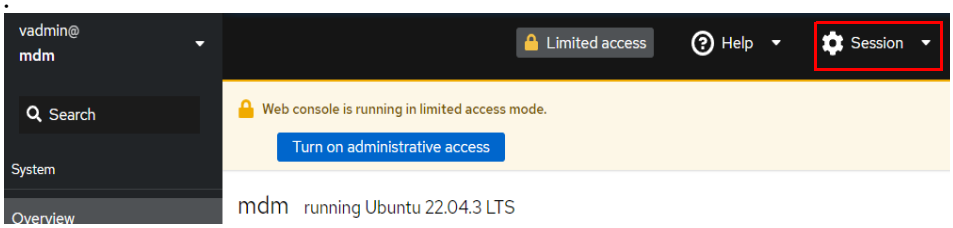
↪ The system has been updated.

3.7 Changing the display language

To change the display language of the mdm VA, proceed as follows:

- Open the “Session” drop-down menu.

.



- Select the “Display Language” menu item.
- Select the desired language and click on the “Select” button.
- Reload the web browser window and log in again, if necessary.

↪ The display language has been changed.

4 Installing mdm

For licensing reasons, it is not possible to provide the mGuard device manager (mdm) already preinstalled with the mdm VA. The installation of mdm 1.16.x must therefore be performed manually.

Phoenix Contact recommends connecting to the mdm VA using a web browser.

mdm software repository

mdm 1.16.x is installed in the mdm VA using the Ubuntu package manager from the Phoenix Contact *mdm software repository*.

For a complete mdm installation, several components and mdm packages are provided for installation (see Table 4-1).

Some components, like the mdm CA (CA = *Certificate Authority*), can be installed optionally.

Using the Apache web server as a configuration pull server (for downloading device configurations by managed mGuard devices) or for downloading firmware updates is also optional.

Other components, such as the database server or web server, are automatically installed and updated from the Ubuntu default repositories.

Refer to Section 4.2 for a description on how to install the packages.

4.1 Available mdm components

Table 4-1 Installable packages from the *mdm software repository*

Package	Description
mdm-common	Contains basic mdm components such as the *Software License Terms* (SLT).
mdm-all-server	Meta package for installing all mdm server components as well as other components *(mdm-server, mdm-ca, mdm-configpull, mdm-clientdownload, mdm-webbase, mdm-backup, mdm-support-snapshot).*
mdm-server	Contains the server components of the mdm server. Starts as *systemd* service. The device configurations of the mGuard devices are managed via the mdm server.
mdm-ca	Contains the components of the mdm Certificate Authority (CA) and the mdm CA server. The CA server can be used to create the certificates used by mGuard devices (e.g., machine certificates).
mdm-configpull	Configures the web server in such a way that it can be used by mGuard devices as a download server for ATV configurations (*config pull server* – see the mdm user manual).
mdm-webbase	Configures the web server in such a way that it can be used by mGuard devices as a firmware update server (see the mdm user manual).
mdm-clientdownload	Configures the web server in such a way that the mdm client (*mdm-client.zip*) and the Windows program for mdm migration (*mdm-datacollector*) can be downloaded using a web browser. The programs are available at: https://<web server IP address>/mdm
mdm-winrestore	Package for providing the *mdm-winrestore* program for the mdm migration from an mdm 1.13.x Windows installation (import into the mdm VA).
mdm-backup	Package for providing the programs for a) performing a backup/restore of the mdm databases in one or several mdm VAs (e.g., from mdm 1.15.0 to mdm 1.16.0): – *mdm-db-backup*/*mdm-db-restore* b) performing a backup/restore of the entire mdm installation in one or several mdm VAs (e.g., from mdm 1.15.0 to mdm 1.16.0): – *mdm-backup*/*mdm-restore*
mdm-support-snapshot	Package for providing the *mdm-support-snapshot* program for creating a support snapshot.
mdm-cockpit	Package for providing the web-based management of mdm VA.

4.2 Performing the installation

Data protection notice: Phoenix Contact logs access to the mdm repository server to ensure the security and stability of the service. For statistical evaluations, only anonymized data is saved. If you have any questions, please contact the Phoenix Contact data protection officer.

The mdm VA has already installed all the necessary software repositories for installing the desired mdm components.

4.2.1 Quick installation

All mdm components can be installed quickly using a Phoenix Contact shell script via the command line (terminal):

Proceed as follows:

- Connect to the mdm VA via the web browser (Section 3).
- Open the command line (terminal) to execute the necessary commands.
- Install all mdm components with the command:

  ```
  sudo pxccs-install-mdm
  ```
- First, accept the *Software License Terms* (SLT):
  - Read the SLTs. (Press the Enter key to change pages.)
  - When you have read the SLTs, accept them at the bottom of the document with "*yes*".
- Follow the instructions on the screen and enter the required parameters as well as any optional parameters (see Section 4.2.3).

↪ All mdm components have been installed.

4.2.2 Individual installation (apt)

Proceed as follows:

- Connect to the mdm VA via the web browser (Section 3).
- Open the command line (terminal) to execute the necessary commands.
- Reload the package information:

  ```
  sudo apt update
  ```
- Install the package and first accept the *Software License Terms* (SLTs):

  ```
  sudo DEBIAN_FRONTEND=readline apt install mdm-common
  ```
  - Read the SLTs. (Press the Enter key to change pages.)
  - When you have read the SLTs, accept them at the bottom of the document with "*yes*".
- Install the mdm server and other mdm components according to your individual requirements (see Table 4-1), e.g., with the command:

  ```
  sudo apt install mdm-all-server mdm-winrestore
  ```
- Follow the instructions on the screen and enter the required parameters as well as any optional parameters (see Section 4.2.3).

4.2.3 Making specific settings

Configuring the mdm certificate authority (CA)

The following attributes are only configured if the mdm CA is installed. The installation program creates a CA certificate and a matching private key.

Enter the attributes to be used (some optional) for the certificate:

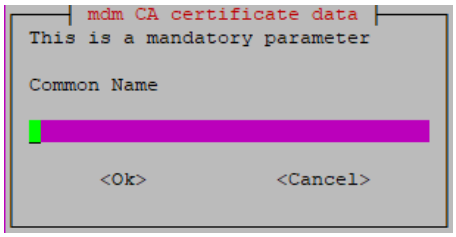


Figure 4-1 The *Common Name* of the certificate is a mandatory entry

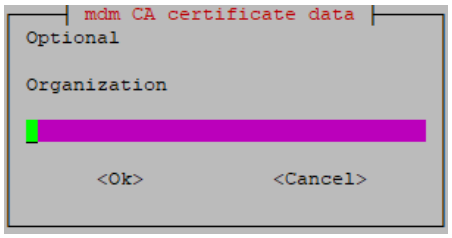


Figure 4-2 The input of an issuing organization is optional

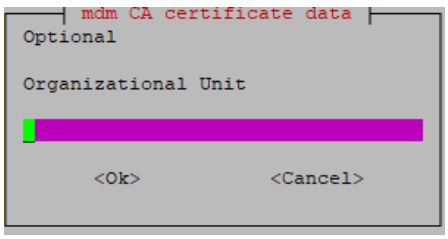


Figure 4-3 The input of an organizational unit is optional

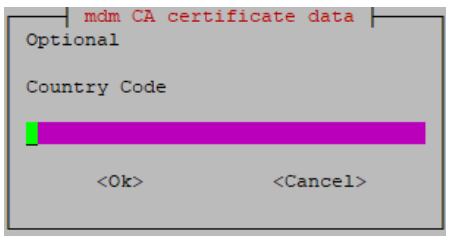


Figure 4-4 The input of a country code (e.g., DE or EN) is optional

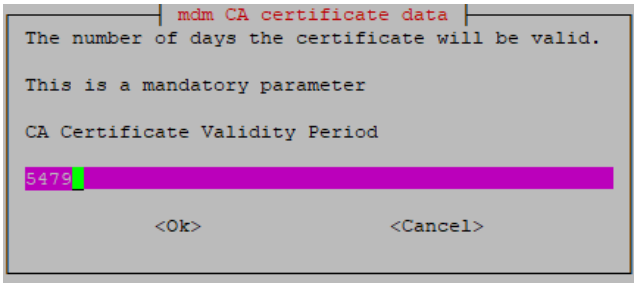


Figure 4-5 The period of validity of the certificate is a mandatory entry

Creating a web server certificate

During the installation of the *mdm-webbase* package, a self-signed X.509 certificate with a private key is automatically created for the mdm web server and saved to the following location: */etc/mdm/mdm-webbase/cert.pem*.

This certificate must be uploaded as a peer certificate to the mGuard devices that get their configuration via *Config Pull* from the mdm web server.

Enter the attributes to be used for the certificate.

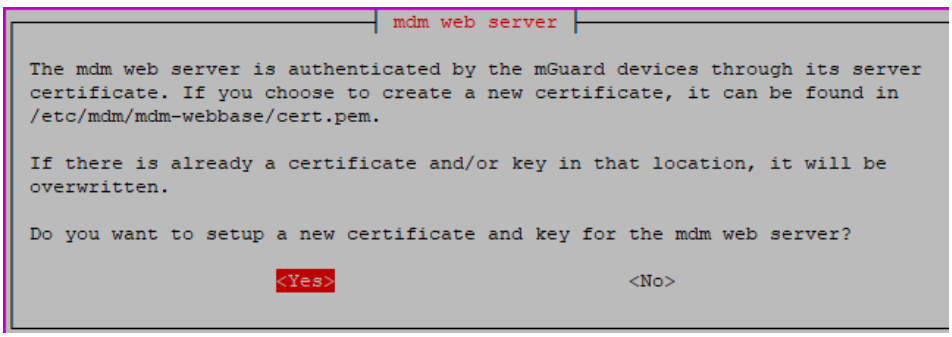


Figure 4-6 Creating a web server certificate

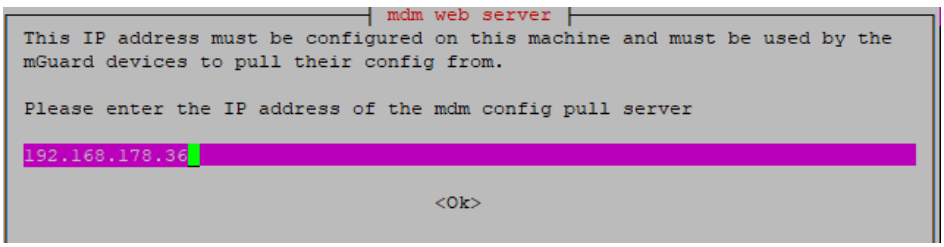


Figure 4-7 The IP address or the host name at which the mdm web server can be reached is linked to the certificate.
Note: If the web server is to be accessed via the DNS name (host name) instead of via the IP address, then it is essential that you specify the DNS name (= *Common Name* in the certificate) here.

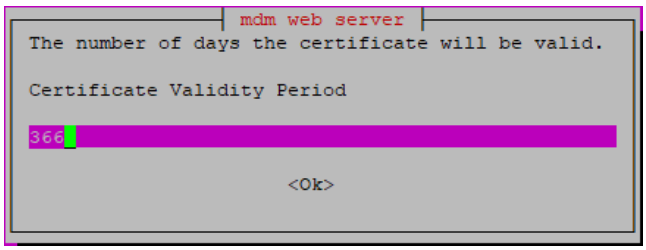


Figure 4-8 Defining the period of validity of the certificate

Creating the web server credentials (user name and password)

Access to the mdm web server can be optionally protected with a user name and a password. If no credentials are assigned, certain web server services cannot be accessed (*Pull Config Server*/*Firmware Repository*).

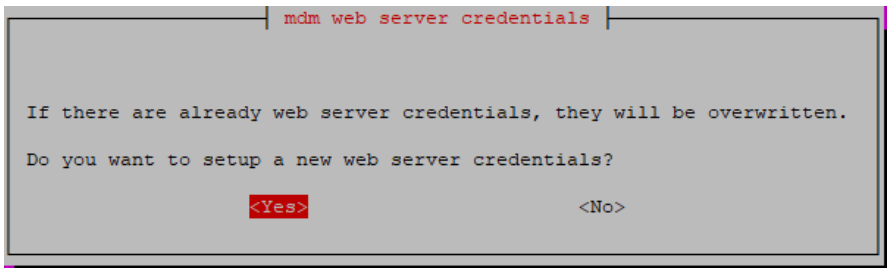


Figure 4-9 Creating mdm web server credentials

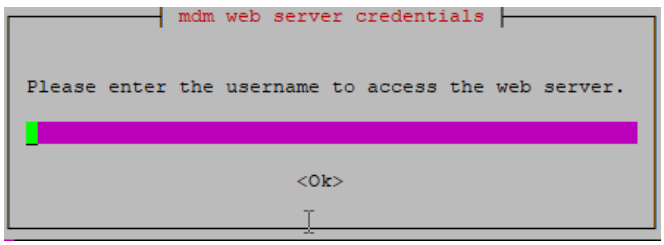


Figure 4-10 Creating the user name for the mdm web server login

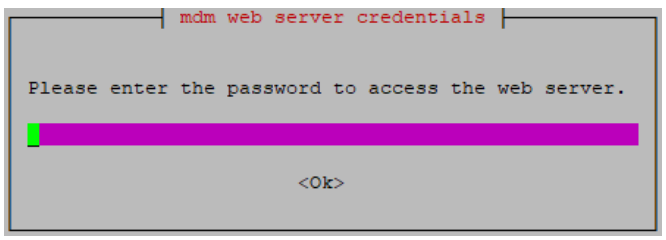


Figure 4-11 Assigning the password for mdm web server login

4.3 Adapting the components (optional)

With the initial installation, the installed mdm components were comprehensively configured.

You can, however, make customizations subsequently. This concerns the following components:

– Configuring the mdm server/CA server
– Activating or changing the web server authentication (*mdm-configpull, mdm-webbase*)
– Changing the web server certificate
– Changing the CA server certificate

4.3.1 Configuring the mdm server (preferences)

To configure the mdm server, use the file *preferences.xml*:

– */etc/mdm/mdm-server/preferences.xml*

To edit the *preferences.xml* file from a Windows configuration computer in the mdm VA, first you must connect to the VA:

- Use the *WinSCP* program to connect to the mdm VA (Section 7.1.2).
- Open the file with a text editor.
- Edit the file.
- Save the file to its original storage location.

↪ You have changed but not yet activated the server configuration.

To activate the changes, the corresponding server must be restarted:

- Connect to the mdm VA using a web browser (see Section 3).
- At the command line (terminal), execute the corresponding command:

```
sudo systemctl restart mdm server
```

↪ The server configuration has been activated.

4.3.2 Activating or changing the web server authentication

If the web server authentication was not activated during the mdm installation or if you want to change the credentials (user name/password) for web server authentication, proceed as follows:

- Connect to the mdm VA using a web browser (see Section 3).
- At the command line (terminal), execute the corresponding command:

```
sudo dpkg?reconfigure mdm-webbase
```

- Answer the question "*Do you want to setup a new certificate and key for the mdm web server?*" with **No**.
- Answer the question "*Do you want to setup new web server credentials?*" with **Yes**.
- Specify a new user name for web server login.
- Specify the password for the new user.

4.3.3 Changing the web server certificate

To change the certificate of the mdm web server, proceed as follows:

- Connect to the mdm VA using a web browser (see Section 3).
- At the command line (terminal), execute the corresponding command:
  `sudo dpkg?reconfigure mdm-webbase`
- Answer the question "*Do you want to setup a new certificate and key for the mdm web server?*" with **Yes**.
- Enter the appropriate parameters for recreating the web server certificate in accordance with your requirements (see Section 4.2.3).

4.3.4 Changing the CA server certificate

To change the certificate of the mdm CA server, proceed as follows:

- Connect to the mdm VA using a web browser (see Section 3).
- At the command line (terminal), execute the corresponding command:
  `sudo dpkg?reconfigure mdm-ca`
- Answer the question "*Do you want to setup a new certificate and key for the mdm ca server?*" with **Yes**.
- Enter the appropriate parameters to recreate the CA server certificate in accordance with your requirements (see Section 4.2.3).

4.4 Applying for, using and activating a license

It is possible to continue using an already purchased mdm license in the mdm VA. For this, the mdm VA must be run with the MAC address specified in the mdm license (see Section 2.4).

NOTE: Assigning the MAC address in the network to only one device
A MAC address may only be assigned to one device or network interface in a network. Make sure that the MAC address used is not used by multiple instances after a migration from another mdm installation.

You can use the *mGuard device manager* without a license in evaluation mode or with a license with charge (*Unlimited*).

1. **Evaluation mode**: If you do not specify a license file during installation, the mdm server will start with a maximum of ten configurable devices and two simultaneously connected clients.
2. **Unlimited**: With the Unlimited license, there are no functional restrictions.

4.4.1 Requesting a new mdm license with new MAC address

You have already purchased an mdm license, but would like to run mdm in the mdm VA with a new or different MAC address. In this case, please contact Phoenix Contact Support. You will then be provided with a new license for use with the MAC address of the mdm VA.

4.4.2 Using an existing mdm license in mdm VA

If you have already purchased a license and want to continue using it, you must adjust the MAC address of the mdm VA in VirtualBox so that it matches the MAC address of the mdm license (see Section 2.4).

NOTE: Protecting security-related data against unauthorized access
Make sure that all security-related data, in particular backup files, is protected against unauthorized access at all times.

4.4.3 Activating an mdm license in mdm VA

Proceed as follows:

- Copy the mdm license to the directory */home/vadmin* in the mdm VA with the name *mdmlic.lic* (see Section 7.1.2).
- Connect to the mdm VA via the web browser (see Section 3).
- Copy the license file to the directory */etc/mdm/mdm-server/* with the file name *mdmlic.lic*:

  ```
  sudo cp /home/vadmin/mdmlic.lic /etc/mdm/mdm-server/mdmlic.lic
  ```
- Restart the mdm server to activate the license:

  ```
  sudo systemctl restart mdm server
  ```

↪ The license is activated for the mdm VA.

4.5 Using the mdm client

The mdm client cannot be run in the configured mdm VA.
Use the mdm client for mdm 1.16.x instead in a separate Windows or Ubuntu operating system.

System requirements for the mdm client

- Operating system: Ubuntu/Windows
- Java platform (JRE): *OpenJDK 11* or later
- Main memory (RAM): at least 512 MB
- Hard disk space: at least 500 MB
- Color monitor resolution: at least 1280 × 1024

Using the mdm client

To use the mdm client, proceed as follows:

- Make the contents of the file *mdm-client.zip* available on the desired system:
  - For this, connect from there to the mdm web server at the configured IP address: https://<IP address>/mdm
    - The file is offered for download.
    - Download the file.
    - Unpack the zip file.
- Start the mdm client by double-clicking on the file *mdm-client-1.16.x.jar* or using the command line: `java -jar mdm-client-1.16.x.jar`.

5 Migrating data

NOTE: Protecting security-related data against unauthorized access
Make sure that all security-related data, in particular backup files, is protected against unauthorized access at all times.

An existing mdm license is only restored and activated if the MAC address of the mdm VA matches the MAC address specified in the mdm license. Usually, this is the case if the MAC address of the mdm VA from which the backup was created is used (see Section 4.4).

5.1 Migrating data from mdm 1.13.x (from Windows)

To continue using the data from mdm 1.13.x (Windows installation) in the mdm VA under mdm 1.16.x, you must migrate it.

Phoenix Contact provides two programs for this purpose, which you can use to automate the migration process (exporting and importing the data):

1. **Export**: *mdm-datacollector*
2. **Import**: *mdm-winrestore*

Migrated components

The following components are migrated from mdm 1.13.x to 1.16.x (if they are already included in the 1.13.x installation):

- The mdm databases (device and certificate database)
- Server certificates (Apache web server, mdm server, and CA server)
- The server configurations (*preferences.xml* and *ca-preferences.xml*)
- The device configurations (ATV profiles)
- The mGuard firmware update repositories

Exporting mdm files (under Windows/mdm 1.13.x)

You must have administrator rights on your Windows system to run the *mdm-datacollector-1.16.x.jar* program.

To use the *mdm-datacollector-1.16.0.jar* program, proceed as follows:

- Make the contents of the *mdm-datacollector.zip* file available on the Windows computer where the mdm version 1.13.x is installed (see Section 1.2):
  - For this, connect to the mdm web server at the configured IP address: https://<IP address>/mdm
    - The *mdm-datacollector.zip* file is offered for download.
    - Download the file and unzip it on the Windows system.
- Copy the *mdm-datacollector-1.14.0.jar* program to the mdm installation directory (default: *C:\Program Files\mGuard device manager*).
- Start the command prompt *cmd.exe.*
- Switch to the mdm installation directory.
- There, start the *mdm-datacollector-1.16.0.jar* program:

  ```
  jre\bin\java.exe -jar mdm-datacollector-1.16.0.jar
  ```

↪ The *mdm-data_<DATE>.zip* file is created and saved to the installation directory.

↪ The data can then be imported into mdm 1.16.x (see below).

Importing mdm files (in the mdm VA / mdm 1.16.x)

If mGuard devices already rolled out get their **configuration** from the *Configuration Pull Server* of the mdm 1.13.x Windows installation and contact the web server via its IP address, then the mdm VA must use the same IP address.

If mGuard devices already rolled out get their **firmware updates** from the *Firmware Update Server* of the mdm 1.13.x Windows installation and contact the web server via its IP address, then the mdm VA must use the same IP address.

If an existing mdm license is continued to be used, you must configure and use the same MAC address in the mdm VA that is specified in the license (see Section 4.4). The mdm VA must be disabled before configuring the MAC address.

To make the data exported from mdm 1.13.x available in mdm 1.16.x, proceed as follows:

- Install mdm 1.16.x in the VA (see Section 4).
- Make the *mdm-winrestore* program available in the mdm VA (see Section 4).
- Before importing, install an mdm license already purchased or newly requested for the mdm VA, if applicable (see Section 4.4).
- If necessary, change the MAC address of the mdm VA before importing.
- Copy the exported *mdm-data_<DATE>.zip* file to the directory */home/vadmin* of the mdm VA (see Section 7.1.2).
- Start the *mdm-winrestore* program to import the exported data to mdm 1.14.x:

  `sudo mdm-winrestore /home/vadmin/mdm-data_<DATE>.zip`
- If you have made changes to the default database user in mdm 1.13.x (name and/or password), you must also make these changes under mdm 1.16.x after the import. Contact Phoenix Contact Support if necessary.

↳ The migrated data from the mdm 1.13x installation is available in mdm 1.16.x.

↳ You can use mdm 1.16.x in the usual manner to configure existing and new devices.

5.2 Migrating data from mdm as of 1.14.x (from mdm VA)

To migrate the entire mdm installation from an existing mdm VA (as of mdm version 1.14.x) to the new mdm VA (provided for mdm 1.16.x), proceed as follows.

The following components are always migrated:

– The mdm databases (device and certificate database)
– The server configurations (*preferences.xml* and *ca-preferences.xml*)
– All certificates of the mdm installation
– Exported device configurations (ATV profiles) and firmware update repositories
– The mdm license (only valid when restoring the backup in the same mdm VA or in an mdm VA with the same MAC address.)

Backing up the mdm installation (Backup)

To back up the mdm installation for the migration, proceed as follows:

- Determine and note down the MAC address of the existing mdm VA.
  – (e.g., *VirtualBox*: Network >> Adapter 1 >> Extended >> MAC address)
- Connect to the existing mdm VA via the SSH client (see Section 7.1).
- Start the *mdm-backup* program: **`sudo mdm-backup`**

↪ The *mdm_backup-<DATE>.zip* file is created and saved to the current directory.

- Download the file from the mdm VA using the SCP client (see Section 7.1).
- Switch off the existing mdm VA: **`sudo poweroff`**

Restoring the mdm installation (Restore)

NOTE: Loss of data possible
Restoring the data will irretrievably delete any existing data in the mdm installation.

To restore the mdm installation backup created with the *mdm-backup* program, proceed as follows:

- Install the new mdm VA as described (see Section 2).
- If necessary, change the MAC address of the mdm VA so that it matches the MAC address of the mdm VA from which the data is migrated (see Section 2.4).
  – (e.g., *VirtualBox*: Network >> Adapter 1 >> Extended >> MAC address)
- Copy the backup file *mdm_backup-<DATE>.zip* with the mdm installation backup to the */home/vadmin* directory in the mdm VA (see Section 7.1.2).
- Connect to the mdm VA using a web browser (see Section 3).
- Change the network settings so that they correspond to the settings of the mdm VA from which the data is migrated (see Section 3.5).
- Open the command line (terminal).
- Run the *mdm-restore* program on the backup file:
  `sudo mdm-restore mdm_backup-<DATE>.zip`

↪ The mdm installation from the backup file is restored in the mdm VA together with all the components it contains. You can use mdm with all settings and device configurations in the usual manner.

5.3 Migrating mdm databases

If you do not want to migrate the entire mdm installation, but only the mdm databases (as of mdm 1.14.x) to 1.16.x, proceed as follows:

→ see Section 6.3

6 Update, backup, and support

NOTE: Protecting security-related data against unauthorized access
Make sure that all security-related data, in particular backup files, is protected against unauthorized access at all times.

Phoenix Contact recommends always using the latest firmware or software version for your devices and applications.

You can update *VirtualBox* at any time, regardless of the virtual machines already imported.

6.1 Update mdm in the mdm-VA to the next minor version

NOTE: Prevent data loss
Before updating to a new mdm version, always create a backup of the mdm databases or the mdm installation (see sections 6.3 and 6.4).

To update the mdm packages of the current mdm installation in the mdm-VA to a new minor version of mdm (e.g. mdm 1.15.x to mdm 1.16.0), you must first adapt the mdm repository.

Proceed as follows:

- Connect to the mdm VA using a web browser (see chapter 3).
- Change the mdm software repository to the desired mdm version 1.16.x:
  `sudo nano /etc/apt/sources.d/pxccs.list`
  Change the mdm version as follows:
  `deb http://repositories.mguard.com/mdm 1.16.x/`

After adding the repository, you can either continue on the command line (terminal) (see description below) or use the "Software updates" service in the WBM of the mdm VA (see chapter 3.6).

- Reload the package information:
  `sudo apt update`
- Execute the corresponding command on the command line (terminal):
  `sudo apt update && sudo apt upgrade`
- Follow the instructions on the screen and confirm the installation of new packages if necessary.

↪ Existing updates for all installed packages are downloaded from the configured repositories and installed.

6.2 Updating Ubuntu and mdm (Patch updates)

To update the Ubuntu version 22.04 packages and the mdm packages from the Phoenix Contact *mdm software repository*, you can use the “Software Updates” service in the WBM of the mdm VA (see Section 3.6).

Alternatively, you can use the Ubuntu package management:

- Connect to the mdm VA using a web browser (see Section 3).
- At the command line (terminal), execute the corresponding command:
  `sudo apt update && sudo apt upgrade`
- Follow the instructions on the screen and confirm the installation of new packages as appropriate.

↪ For all installed packages, available updates from the configured repositories are downloaded and installed.

6.3 Backup and restore of the mdm databases

Phoenix Contact recommends backing up the mdm databases at regular intervals. Use appropriate scripts where necessary to automate the data backup (see Section 7.2.1).

NOTE: Protecting security-related data against unauthorized access
Make sure that all security-related data, in particular backup files, is protected against unauthorized access at all times.

The available mdm databases (device and certificate database) can be saved to the mdm VA as a backup file. In the event of a data loss, the backup file can be restored to the same or a different mdm VA.

Phoenix Contact provides two programs for the mdm VA for this: *mdm-db-backup* and *mdm-db-restore*.

During the backup, the following components are saved to the backup file:
– The available mdm databases from the mdm VA (device and certificate database).

Database backup

To back up the databases (device and certificate database) of an mdm installation (e.g., mdm 1.15.x or 1.16.x), proceed as follows:
- Connect to the mdm VA using a web browser (see Section 3).
- Open the command line (terminal).
- Start the *mdm-db-backup* program:
  `sudo mdm-db-backup`

↪ The *mdm_db_backup-<DATE>.zip* file is created and saved to the current directory.
↪ You can use the backup file to restore the mdm database backups to the same or a different mdm VA.

Database restore

NOTE: Loss of data possible
Restoring the databases irretrievably deletes any existing databases in the mdm installation.

Previously created backups can only be restored to the same or a higher mdm version.

To restore the mdm databases (device and certificate database) backed up with the *mdm-db-backup* program, proceed as follows:
- Make the backup file *mdm_db_backup-<DATE>.zip* with the mdm database backups available in the mdm VA.
- Connect to the mdm VA using a web browser (see Section 3).
- Open the command line (terminal).
- Run the *mdm-db-restore* program on the backup file:
  `sudo mdm-db-restore mdm_db_backup-<DATE>.zip`

↪ The mdm databases from the backup file are restored in the mdm installation in the mdm VA. You can use mdm with all settings and device configurations in the usual manner.

6.4 Backup and restore of the entire mdm installation

Phoenix Contact recommends also backing up the mdm installation at regular intervals or at your own discretion. Use appropriate scripts where necessary to automate the data backup (see Section 7.2.1).

NOTE: Protecting security-related data against unauthorized access
Make sure that all security-related data, in particular backup files, is protected against unauthorized access at all times.

You can save the mdm installation to the mdm VA as a backup file. It is recommended to save the backup to a local system and to a directory that is subject to regular backups.

In the event of data loss, the mdm backup can be restored to the same or a different mdm VA.

Phoenix Contact provides two programs for the mdm VA for this:
mdm-backup und *mdm-restore*.m*dm-backup* and *mdm-restore*.

The following components are always saved during the backup:

– The mdm databases (device and certificate database)
– The server configurations (*preferences.xml* and *ca-preferences.xml*)
– All certificates of the mdm installation
– Exported device configurations (ATV profiles) and firmware update repositories
– The mdm license

mdm-backup

To back up the complete mdm installation (e.g., mdm 1.15.x or 1.16.x), proceed as follows:

- Connect to the mdm VA using a web browser (see Section 3).
- Open the command line (terminal).
- Start the *mdm-backup* program: **`sudo mdm-backup`**

↪ The *mdm_backup-<DATE>.zip* file is created and saved to the current directory.
↪ You can use the backup file to restore the mdm installation backup to the same or a different mdm VA.

mdm restore

NOTE: Loss of data possible
Restoring the data will irretrievably delete any existing data in the mdm installation.

The mdm license is only restored and activated if the MAC address of the mdm VA matches the MAC address specified in the mdm license. Usually, this is the case if the MAC address of the mdm VA from which the backup was created is used (see Section 4.4).

To restore the mdm installation backup created with the *mdm-backup* program, proceed as follows:

- Copy the backup file *mdm_backup-<DATE>.zip* with the mdm installation backup to the */home/vadmin* directory in the mdm VA (see Section 7.1.2).
- If necessary, change the MAC address of the mdm VA before restoring the file.
- Connect to the mdm VA using a web browser (see Section 3).
- Open the command line (terminal).
- Run the *mdm-restore* program on the backup file:

```
sudo mdm-restore mdm_backup-<DATE>.zip
```

↳ The mdm installation from the backup file is restored in the mdm VA together with all the components it contains. You can use mdm with all settings and device configurations in the usual manner.

“License” restriction: The license is only restored and activated if the MAC address of the mdm VA matches the MAC address specified in the mdm license. This is done automatically when the MAC address of the mdm VA from which the backup was created is used.

6.5 Creating a support snapshot

NOTE: Protecting security-related data against unauthorized access
Make sure that all security-related data, in particular backup files, is protected against unauthorized access at all times.

If you need the assistance of Phoenix Contact Support to solve a problem with mdm or the mdm VA, you must provide information about your system as detailed as possible:

The mdm VA provides a program that automatically collects the relevant data on the current system state and summarizes it in a file.

The following data is **not** included in the support snapshot:

- Passwords and cryptographic keys
- The contents of the databases (device and certificate database)

Creating a support snapshot

To create a snapshot of the currently running system, proceed as follows:

- Make the *mdm-support-snapshot* program available in the mdm VA (see Section 4).
- Connect to the mdm VA using a web browser (see Section 3).
- Open the command line (terminal).
- Start the *mdm-support-snapshot* program:
  `sudo mdm-support-snapshot`

↪ The file *support-snapshot-<DATE>.zip* is created and saved to the current directory.

↪ Submit the support snapshot to Phoenix Contact Support via a secure transmission channel.

7 Appendix

7.1 Using Windows tools for remote access

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

NOTE: Protecting security-related data against unauthorized access
Make sure that all security-related data, in particular backup files, is protected against unauthorized access at all times.

For certain activities from a Windows computer, such as making files available in the mdm VA, downloading files, or running commands in the command line of the VA, you can use the programs *PuTTY* and *WinSCP* in Windows, for example, for the following tasks:

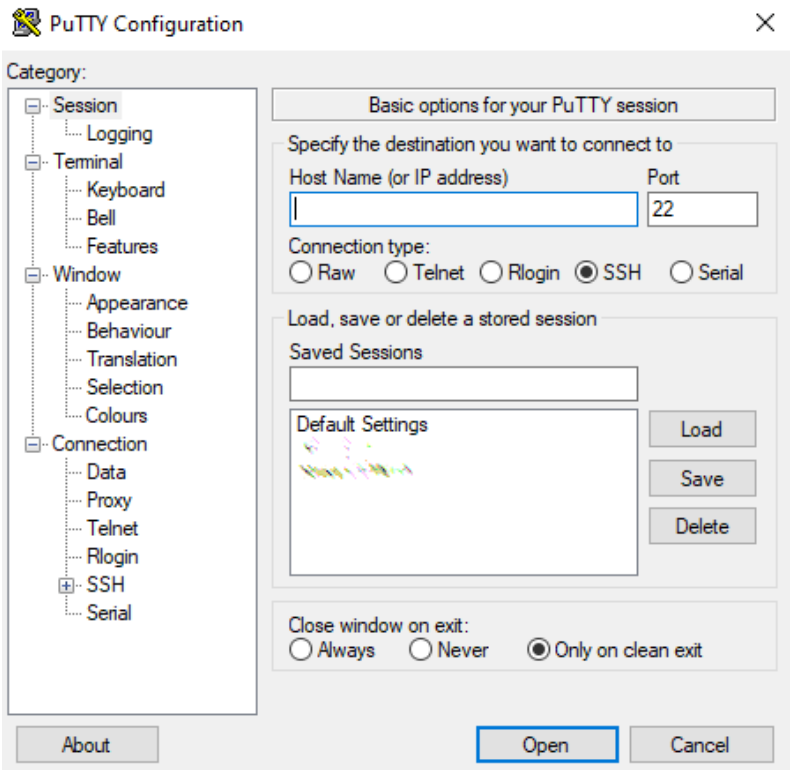
1. **PuTTY** (SSH client) --> see Section 7.1.1
   - Installing and configuring mdm and components
   - Moving files within the mdm VA
   - Changing the IP configuration of the mdm VA
   - Updating mdm and Ubuntu
2. **WinSCP** (SCP client) --> see Section 7.1.2
   - Downloading backup files for the data backup
   - Uploading the mdm license
   - Editing the configuration file of the mdm server (*preferences.xml*)
   - Downloading the web server certificate
   - Uploading and downloading ATV profiles
   - Uploading mGuard firmware update repositories

7.1.1 PuTTY

PuTTY (putty.org) is an open-source SSH client for Windows that can be used to establish a connection to the command line of the mdm VA.

To connect a Windows system via SSH to the VA, proceed as follows:

- Start the program *PuTTY* on a Windows computer that is connected to the VA via the network.



- Start a new session with the following connection data:
  - **Host Name (or IP address)**: IP address of the mdm VA (assigned to the VA via DHCP or in another way).
  - **Port**: Port number of the SSH server of the mdm VA (default port: 22)
  - **Connection type**: SSH
- Click on the **Open** button.

↪ You are connected to the VA.

↪ You have access to the command line of the mdm VA and can make corresponding settings.

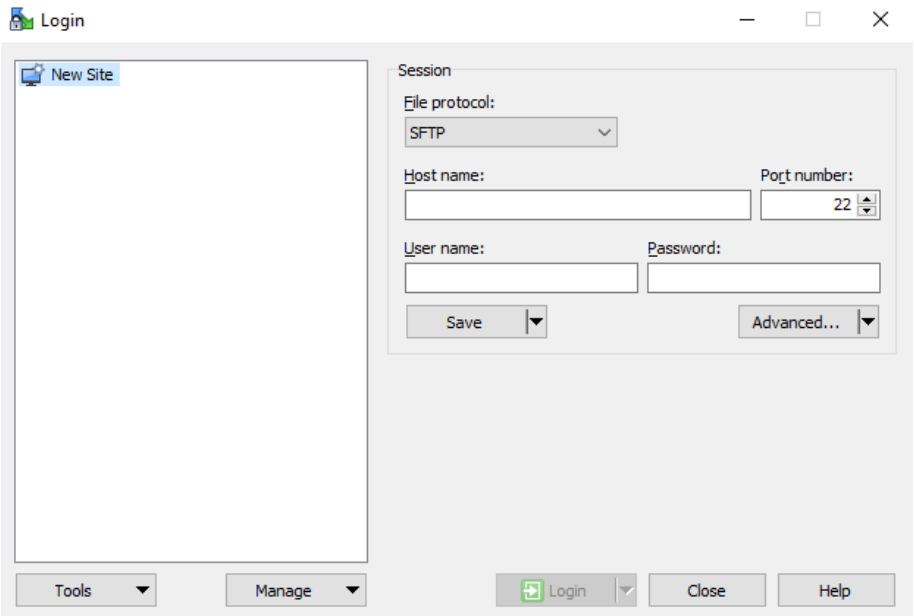
To copy texts to the command line using *copy & paste*, first you must copy the text as usual (e.g., Ctrl+c). Then **right-click** in the console window opened by *PuTTY* to paste the copied text.

7.1.2 WinSCP

WinSCP (winscp.net) is an open-source SFTP client for Windows that can be used for secure data transfer between two network devices.

To connect a Windows system via SFTP to the mdm VA, proceed as follows:

- Start the program *WinSCP* on a Windows computer that is connected via the network to the VA.



- Start a new session with the following connection data:
  - **File protocol**: SFTP
  - **Host name (address)**: IP address of the mdm VA (assigned to the VA via DHCP or in another way).
  - **User name**: User name of the mdm VA user (default: *vadmin*)
  - **Password**: Password of the mdm VA user (default: *private*)
- Click on the **Save** button to save the connection to the mdm VA under the selected file name.
- Click on the **Login** button.

↪ You are connected to the VA (directory: */home/vadmin*).

↪ You have read access to all directories.

↪ You have write access to the home directory */home/vadmin*.

↪ You additionally have write access to the file *preferences.xml* under: */etc/mdm/mdm-server/preferences.xml*

↪ Accordingly, you can exchange files between the Windows computer and the mdm VA via *drag & drop* as well as edit files directly in Windows.

7.2 Automating tasks in Windows

This chapter shows how the creation of backups (mdm databases/mdm installation) can be automated in Windows using batch files, using the program *PuTTY* as an example.

The installation of *PuTTY* not only provides an SSH client, but offers other tools for running selected commands in the mdm VA (using *plink.exe*) or uploading and downloading files (using *pscp.exe*), for example.

With these tools, the creation and downloading of the backups in Windows can be automated as follows.

NOTE: Protecting security-related data against unauthorized access
Make sure that all security-related data, in particular backup files, is protected against unauthorized access at all times.

Customizing variables

The sample scripts (batch files) specified below contain variables that must be customized to your environment:

– **PUTTY_PATH**: Path to the *PuTTY* installation on the Windows system
– **MDM_VA_IP**: IP address of the mdm VA
– **MDM_VA_USER**: User name for the mdm VA (default: *vadmin*)
– **MDM_VA_PW**: Password of the mdm VA user (*vadmin*). If you do not want to specify the password in plain text in the batch file, you can delete this line and set the password as an environment variable for the Windows user.
– **BACKUP_DESTINATION**: Destination directory to which the backup is to be written. It is advisable to select a directory that is subject to regular system backups.

Procedure:

- Copy the corresponding script from Section 7.2.1 or Section 7.2.2 and save it locally on the Windows system using the file name *mdm-db-backup.bat* or *mdm-backup.bat*, for example.
- Customize the variables in the script as described above.
- Test the script:
  – Open the command prompt (*cmd.exe*) and switch to the directory containing the script.
  – Run the script: *mdm-db-backup.bat* or *mdm-backup.bat*
  – The script has been successfully run if the backup directory specified above (BACKUP_DESTINATION) contains one of the following files:
    – *mdm_db_backup-<DATE_TIME>.zip*
    – *mdm_backup-<DATE_TIME>.zip*

↪ You can now incorporate the script into the Windows Task Scheduler and have it run at defined time intervals.

7.2.1 Backing up mdm databases (sample script)

With this batch file, you back up the **mdm databases** as described in Section 6.3:

```
@ECHO OFF

SET PUTTY_PATH=C:\Tools\Putty

SET MDM_VA_IP=10.1.0.77
SET MDM_VA_USER=vadmin
SET MDM_VA_PW=private
SET BACKUP_DESTINATION=C:\BACKUPS

:: Connect to the mdm VA and create the mdm database backup
"%PUTTY_PATH%\plink.exe" -ssh -l %MDM_VA_USER% -pw %MDM_VA_PW% ^
                         -batch %MDM_VA_IP% "sudo mdm-db-backup"

:: Download the mdm database backup to the local system
"%PUTTY_PATH%\pscp.exe" -l %MDM_VA_USER% -pw %MDM_VA_PW% ^
                      %MDM_VA_IP%:mdm_db_backup*.zip "%BACKUP_DES-
TINATION%"


:: Remove the mdm database backup file in the mdm VA
"%PUTTY_PATH%\plink.exe" -ssh -l %MDM_VA_USER% -pw %MDM_VA_PW% ^
                    -batch %MDM_VA_IP% "sudo rm mdm_db_backup*.zip"
```

Figure 7-1 Batch file (sample script): *mdm-db-backup.bat*

7.2.2 Backing up the mdm installation (sample script)

With this batch file, you back up the **complete mdm installation** as described in Section 6.4:

```
@ECHO OFF

SET PUTTY_PATH=C:\Tools\Putty

SET MDM_VA_IP=10.1.0.77
SET MDM_VA_USER=vadmin
SET MDM_VA_PW=private
SET BACKUP_DESTINATION=C:\BACKUPS

:: Connect to the mdm VA and create the mdm backup
"%PUTTY_PATH%\plink.exe" -ssh -l %MDM_VA_USER% -pw %MDM_VA_PW% ^
                         -batch %MDM_VA_IP% "sudo mdm-backup"

:: Download the mdm backup to the local system
"%PUTTY_PATH%\pscp.exe" -l %MDM_VA_USER% -pw %MDM_VA_PW% ^
                       %MDM_VA_IP%:mdm_backup*.zip "%BACKUP_DES-
TINATION%"

:: Remove the mdm backup file in the mdm VA
"%PUTTY_PATH%\plink.exe" -ssh -l %MDM_VA_USER% -pw %MDM_VA_PW% ^
                      -batch %MDM_VA_IP% "sudo rm mdm_backup*.zip"
```

Figure 7-2 Batch file (sample script): *mdm-backup.bat*

7.3 Uploading the mGuard firmware update repository to the mdm web server

mGuard devices can always download firmware updates from the default Phoenix Contact update server (update.innominate.com).

Alternatively, you can run a separate update server for mGuard firmware and install and configure it as part of the mdm installation.

Use the Windows programs *WinSCP* and *PuTTY*, for example, for this (see Section 7.1).

Proceed as follows:

- Connect via SSH to the mdm VA (see Section 7.1.1).
- Install the package *mdm-webbase* (see Section 4 and 4.2.3):

```
sudo apt install mdm-webbase
```

↪ You have configured the update server for the mGuard firmware.

In Windows

- Download the desired firmware repository (or repositories) from the corresponding product page in the Phoenix Contact online store to your Windows computer: phoenixcontact.net/product/<order number> >> Downloads >> Firmware Update

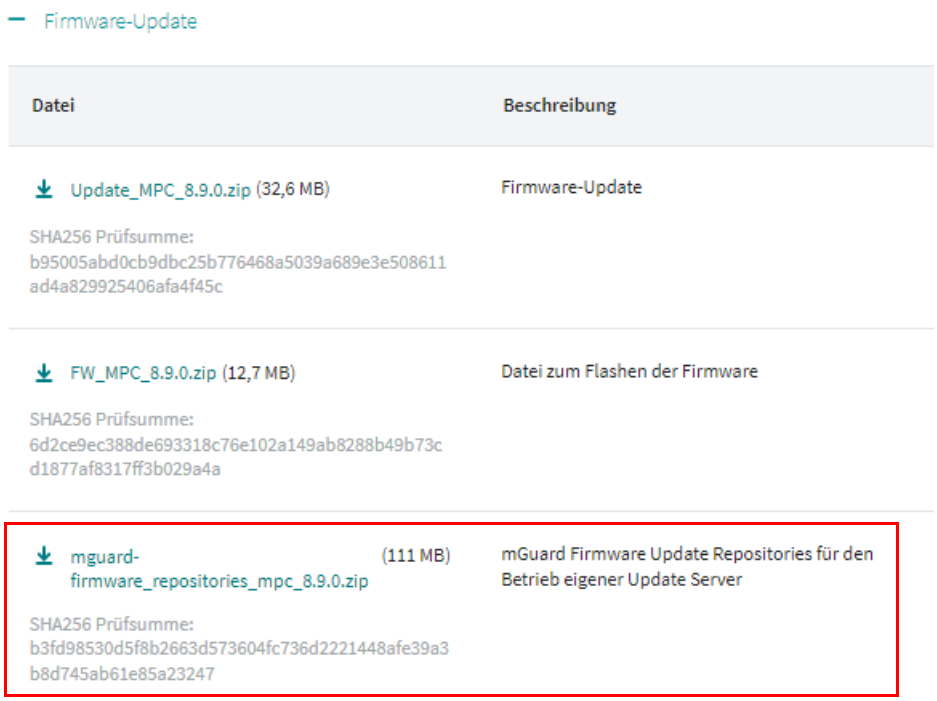


Figure 7-3 Example: Downloading a firmware repository from the online store

- Unpack the zip file in Windows so you can access the directories *mpc83xx* and *Packages*.
- Copy the directories *mpc83xx* and *Packages* and any necessary modem firmware using *WinSCP* to the home directory */home/vadmin* of the mdm VA.

In the mdm VA

- Move the uploaded directories using *PuTTY* to the firmware update directory of the mdm VA:

  ```
  sudo mv mpc83xx Packages /var/www/mdm/
  sudo mv <modem firmware> /var/www/mdm/
  ```
  (if present)

NOTE: Observe the order when moving files!
Note that the firmware update repositories with multiple versions must always be installed one after the other in ascending order based on the version number.

↪ The firmware is available on the update server and can be downloaded and installed by mGuard devices.

7.4 Installing mdm repository and mdm via console

Data protection notice: Phoenix Contact logs accesses to the mdm repository server to ensure the security and stability of the service. For statistical evaluations, only anonymized data is saved. If you have any questions, please contact the Phoenix Contact data protection officer.

To run the following commands using *copy & paste* in the command line, it is recommended to connect via an SSH client to the mdm VA (e.g., *PuTTY)* (see Section 7.1.1). Copy the respective command line and then right-click in the console window opened by *PuTTY* to paste.

Proceed as follows:

1. Connect via SSH to the mdm VA (Section 7.1.1).
2. Download the public key of the repository (*pubkey.gpg*):
   ```
   sudo wget http://repositories.mguard.com/pubkey.gpg
   ```
3. Check the fingerprint of the public key:
   ```
   gpg -finger pubkey.gpg
   ```
   The fingerprint **must** match the following fingerprint:
   AD3E B1F9 473D 5CC7 2ED4 2D4C 0571 79A3 CC0F FA55.
4. Add the public key of the repository (*pubkey.gpg*) to the GPG key public ring (*trusted.gpg*):
   ```
   sudo apt-key add pubkey.gpg && apt-key list
   ```
5. Add the *mdm software repository* to your package manager:
   Make sure to run the command exactly as described!
   ```
   sudo apt-add-repository
   "deb http://repositories.mguard.com/mdm 1.16.x/"
   ```
6. Reload the package information:
   ```
   sudo apt update
   ```
7. Install the package and accept the *Software License Terms* (SLTs):
   ```
   sudo DEBIAN_FRONTEND=readline apt install mdm-common
   ```

– Read the SLTs. (Press the Enter key to change pages.)
– When you have read the SLTs, accept them at the bottom of the document with “*yes*”.

8. Install the mdm server and other mdm components (see Table 4-1), e.g., with the command:
   ```
   sudo apt install mdm-all-server mdm-winrestore
   ```

Follow the instructions on the screen and enter the required as well as any optional parameters (see Section 4.2.3).

7.5 Changing the keyboard layout of the mdm VA via console

Should you prefer to work directly on the console of the mdm VA instead of using a Windows SSH client, you may need to customize the keyboard layout (*105-key, us_us*) to your local conditions (e.g., 105-key, de_de).

- Connect via SSH to the mdm VA.
- To customize the keyboard layout, run the following command:
  `sudo dpkg-reconfigure keyboard-configuration`
  – Follow the instructions on the screen.
- To activate the customizations, run the following command:
  `sudo setupcon`

↪ You have changed and activated the keyboard layout.

7.6 Adapting the network settings via console

If it is not possible to assign an IP configuration to the mdm VA via DHCP after the first start and the initialization has been performed, you must deactivate DHCP in the mdm VA and configure a static network setting instead.

Note that the current connection to the mdm VA will be terminated after the IP address is reconfigured. You will then need to log in again to the newly assigned static IP address.

Proceed as follows:

- Log in directly to the mdm VA.
- Perform the changes as root admin: **`sudo -i`**
- Disable DHCP:

  `echo "network: {config: disable}" > /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg`

↳ The mdm VA will no longer obtain its network configuration via DHPC.

- Create the configuration file for the static network configuration:

  `cp -rp /etc/netplan/50-cloud-init.yaml /etc/netplan/50-static.yaml`

- Configure the static network configuration (e.g., with the *nano* editor):

  `nano /etc/netplan/50-static.yaml`

- Use the following configuration example and customize the settings in accordance with your requirements (IP address with net mask, default gateway, name server address, MAC address):

```
network:
    ethernets:
        enp0s3:
            dhcp4: false
            addresses: [192.168.3.99/24]
            routes:
              - to: default
                via: 192.168.3.10
            nameservers:
              addresses: [192.168.3.10]
            match:
                macaddress: 08:00:27:1a:92:2c
            set-name: enp0s3
    version: 2
```

- Save your configuration by pressing the *Ctrl+o* key combination and confirm the entry with the Enter key.
- Exit the editor by pressing the *Ctrl+x* key combination.
- Restart the mdm VA: **`shutdown -r now`**

↳ The static network configuration is enabled after a restart.

↳ You can connect to the mdm VA via the statically configured IP address.

7.7 File locations in mdm VA and web server URLs

The table below shows the locations and web server URLs of selected files and programs available in the mdm VA.

Table 7-1 File locations and web server URLs

Item	Storage location (mdm VA)	URL (web server)
Web server certificate (*cert.pem*) that can be used to authenticate mGuard devices in order to download ATV configurations or firmware updates from the mdm web server. The certificate must be installed on the mGuard devices as a "Remote certificate".	/etc/mdm/mdm-webbase	
ATV configurations that can be downloaded from mGuard devices and activated as a configuration profile.	/var/www/mdm/atv	https://<web-server-IP>/atv
Firmware repositories: Update files that can be downloaded by mGuard devices to perform a firmware update.	/var/www/mdm	https://<web-server-IP>/
Certificate Revocation List (CRL)	/etc/mdm/security/crl	https://<web-server-IP>/crl
mdm client (*mdm-client.jar*): Program that runs the mdm client.	/etc/mdm/mdm-clientdownload/clientdownload	https://<web server IP>/mdm
mdm-datacollector (*mdm-datacollector.jar*): Program which is used to collect the data of the mdm installation (mdm 1.13.x) on the Windows machine to perform the data migration.	/etc/mdm/mdm-clientdownload/clientdownload	https://<web server IP>/mdm
Configuration file for the mdm server (*preferences.xml*)	/etc/mdm/mdm-server	
Configuration file for the mdm CA server (*ca-preferences.xml*)	/etc/mdm/mdm-ca	
Software License Terms (SLT) in form of a PDF file (*slt_mdm.pdf*)	/etc/mdm/mdm-common	

Please observe the following notes

General terms and conditions of use for technical documentation

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

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

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

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

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

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

How to contact us

Internet

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

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

Subsidiaries

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

Published by

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

Phoenix Contact Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

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

Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
Email: info@phoenixcontact.com
phoenixcontact.com



© Phoenix Contact 2024-07-22

110903_en_02
Item No. –02