



FL MGUARD DM UNLIMITED Upgrade to Version mdm 1.13.x

Application Note AH EN MDM UPGRADE



Application Note FL MGUARD DM UNLIMITED Upgrade to Version mdm 1.13.x

AH EN MDM UPGRADE, Revision 08

2021-05-12

This Application Note is valid for the product FL MGUARD DM UNLIMITED.



Make sure you always use the latest documentation. It can be downloaded at: <u>phoenixcontact.net/products</u>. Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at: <u>phoenixcontact.com</u>.

1 Upgrade FL MGUARD DM UNLIMITED to version 1.13.x



Document-ID: 107821_en_08

Document-Description: AH EN MDM UPGRADE © PHOENIX CONTACT 2021-05-12



Make sure you always use the latest documentation. It can be downloaded using the following link <u>phoenixcontact.net/products</u>.

Contents of this document

This document explains how to upgrade mGuard device manager (mdm) to version 1.13.x.

1.1	Introduction	1
1.2	General notes	2
1.3	Known issues	
1.4	Operating system: Microsoft Windows	5
1.5	Operating system: Ubuntu Linux	
1.6	Batch files and shell scripts	
1.7	mdm 1.13.x Installer for Windows	
1.8	Ubuntu's package management tools	

1.1 Introduction

Since mdm versions 1.5.2 (Windows) and 1.7.0 (Windows and Ubuntu) *mGuard device manager* as well as mdm and third-party components can be installed and upgraded automatically via the included *mdm Installer for Windows* or Ubuntu's package management tools.

If your system does not fulfill the system requirements demanded in Table 1-1 and Table 1-2, *mdm server* and *mdm CA server databases* must either be dumped and imported to a newly installed mdm 1.13.x or the installed mdm version must be upgraded stepwise to mdm 1.13.x.

The following chapters describe

- how to upgrade your mdm installation and third-party components and
- how to migrate your existing mdm databases on Windows and Linux systems using batch files and shell scripts (see Chapter 1.6).

For a detailed view on the installation, configuration and usage of mGuard device manager (mdm) 1.13.x, please refer to the *mdm User Manual*, available <u>online</u> or as a PDF version in the PHOENIX CONTACT Webshop (<u>phoenixcontact.net/product/2981974</u>).

1.2	General notes
NOTE:	Backup important files and databases
Keep b grade p	ackup copies of the following files and databases to avoid data loss during the up process of mdm:
– cui	rrent mdm server and mdm CA server databases
– pre	eferences.xml and ca-preferences.xml
Th the	ese files usually contain individual parameters that are to be taken over again afte upgrade.
– та	Im license file
Yo	u need the license file to use the mdm to its full extent.
NOTE:	Incompatibility of PostgreSQL databases
To upg change databa	rade from an older version to mdm 1.13.x, it is necessary to make irreversible as to the backing PostgreSQL database. Once these changes have been made, th se can no longer be accessed with an older version.
NOTE:	Java Runtime Environment (JRE) will be uninstalled
As of ve <i>Runtim</i>	ersion mdm 1.11.0, mdm uses the Java platform <i>OpenJDK</i> and no longer the <i>Java e Environment</i> (JRE).
The <i>m</i> c OpenJi	Im 1.11.x Installer for Windows automatically installs the required version of DK and uninstalls existing versions of the Java Runtime Environment.
Migratii databa and coi	ng mdm installations with the provided batch files/shell scripts restores only the se(s) dumped and imported. Any other installation data (e.g. pull server certificate nfig files) must be manually copied to the new installation as explained below.
The pro (check and <i>ca</i> -	ovided batch files/shell scripts will only work in case of standard mdm installation default database names, ports, and user names in the provided <i>preferences.xml</i> <i>preferences.xml</i> files).
mdm s proces	erver (and CA server) will be stopped and restarted during the dump generation s.

4 0 \sim . -

1.3 Known issues

	1.3.1	CA database migration using equal CA certificate attri- butes
Issue	If the mdm installed r – from a	n CA database migration (via provided database export/import scripts) to a newly ndm version 1.13.x on Windows a different operating system or an installed mdm version < 1.12.0
	is done us mdm CA s	sing the same CA certificate attributes on the new mdm 1.13.x installation, the server will fail to start.
Solution	During the identical to	e installation of mdm 1.13.x do not provide all certificate attributes of the CA o the ones of the older installation (e.g. add a suffix to the <i>Common Name</i>).
	1.3.2	Different HTTP Server Directory Structure and Password Protection in Ubuntu and Windows
Issue	The HTTF Ubuntu's	P server directory structures created by the <i>mdm Installer for Window</i> s and package managing tools are different:
	 In Wir are us 	ndows, the server access is password protected, and three different directories sed: "atv", "crl", and "fw", where "fw" is defined as the root directory.
	 In Ub is use 	untu, the server access is not password protected, and the server root directory ed to store pull configuration files, firmware upgrade packages and CRL files.
Solution	To enable A) Edit tl	e password protection in Ubuntu, proceed as follows: he file "/var/www/mdm/.htaccess" and uncomment and edit the existing lines: AuthType Basic AuthName "username" AuthUserFile /etc/mdm/mdm-webbase/.htpasswd Require valid-user
	a B) Use (ccess to. as sudo) the Apache tool "htpasswd" to create the desired user password
	config config c	guration in the file "/etc/mdm/mdmwebbase/.htpasswd": sudo htpasswd -c /etc/mdm/mdm-webbase/.htpasswd username Vhere "username" must be replaced with the username you want to grant the ac- ess to. You will be asked to introduce the desired password.
	To use the A) Edit ti	e same directory structure in Ubuntu and Windows, proceed as follows: he file "/etc/apache2/sites-available/mdm-webbase-ssl.conf": Define the aliases " atv ", and " crl ". E.g.: Alias "/atv/" "/var/www/mdm/" Alias "/atv" "/var/www/mdm/" Alias "/crl/" "/etc/mdm/security/crl/" Alias "/crl" "/etc/mdm/security/crl/" <directory crl="" etc="" mdm="" security=""></directory> Options +Indexes -FollowSymLinks +Multiviews AllowOverride All

Require all granted </Directory>

i

This will not change the real directory structure in the system, but will make it possible for already configured mGuards which expect the directories **atv**, and **crl** to download pull configurations, and CRL files successfully.

If you additionally want to have the same directory structure in the system, you have to create the corresponding directories and define the access permissions of each in *mdm-webbase-ssl.conf*.

1.4 Operating system: Microsoft Windows

mdm 1.13.x can only be installed on supported Microsoft Windows systems if the required preconditions are fulfilled (see Table 1-1 on page 6).



NOTE: Windows Defender must be disabled!

Prior to the **installation or upgrade** of mdm, Microsoft *Windows Defender* **must be disabled** on the Windows system.

With Microsoft *Windows Defender* enabled, the existing mdm installation may otherwise be irreparably damaged.

After the installation/upgrade of mdm has been completed successfully, Microsoft *Windows Defender* can be activated again.



NOTE: Incorrectly installed *Microsoft Visual C++ 2017 Redistributable Package* (*x64*) may break current mdm installation

Prior to the **installation or upgrade** of mdm, *Microsoft Visual* C++ 2017 Redistributable Package (x64) (or newer versions) must have been **successfully** installed on the Windows system.

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

NOTE: It is possible that the specified link is no longer valid. In any case make sure that the correct version is used!

Precondition: All current Windows Update Packages must have been installed first.

Make sure that the package has been installed without warnings or error messages.

If the package has been installed unsuccessfully or incomplete, the mdm installation may fail and break existing mdm installations.



NOTE: All current Windows Update Packages must have been installed

Prior to the **installation or upgrade** of mdm or Windows components, all available update packages for the Windows operating system must have been **successfully** installed.

Caution: It might be necessary to re-check several times that all necessary packages have been installed. Sometimes some of the packages will not be installed during the first or even second Windows Update session.

If your system does not fulfill the system requirements demanded in Table 1-1 *mdm server* and *mdm CA server databases* must either be dumped and imported to a newly installed mdm 1.13.x or the installed mdm version must be upgraded stepwise to mdm 1.13.x.

S

System requirements							
Table 1-1 S	ystem requirements (Mic	rosoft Windows systems	6)				
	mdm Client	mdm Server	mdm CA				
Supported operating system	 Windows Server 2016 Windows Server 2012 R2 Windows 10 (mdm client only) Windows 7 (mdm client only) 						
Hardware	 A minimum of 512 MB RAM 500 MB free hard disk space Color monitor with at least 1280 x 1024 resolution 	 A minimum of 4 GB RAM 100 GB free hard disk space 	 A minimum of 512 MB RAM 5 GB free hard disk space 				
Software Components	 Third-party components (<i>PostgreSQL 10.16, Apache Webserver 2.4.46, OpenJDK 11.0.9, Python 3.8.3, and OpenSSL 1.1.1k</i>) will automatically be installed via the <i>mdm 1.13.x Installer for Windows</i>. <i>Apache Web Server</i> requires <i>Microsoft Visual C++ 2017 Redistributable Package (x64)</i> (or newer) to be installed. Download: https://aka.ms/vs/16/release/VC_redist.x64.exe NOTE: It is possible that the specified link is no longer valid. In any case make sure that the correct version is used! mdm clients, independently run on systems other than the "server system", require the Java platform <i>OpenJDK 11</i> to be installed. 						
Precondition	 If not installed via mdm Installer for Windows: OpenJDK 11 	 mdm not installed er installed). PostgreSQL not in previous mdm inst Apache Web Serve (or installed ar other than 443 (or installed by 	d (or mdm 1.12.0 or lat- istalled (or installed by allations). <i>er</i> not installed nd listening to a port 3), / previous mdm instal-				

_

lations).

installed..

Microsoft Visual C++ 2017

Redistributable Package (x64) (or newer)

Upgrade on supported Micro	soft Windows systems			
From mdm 1.12.0 or later	To upgrade mdm version 1.12.x or later on supported Microsoft Windows systems, use the <i>mdm 1.13.x Installer for Windows</i> (see "mdm 1.13.x Installer for Windows" on page 23)			
	It is not necessary to uninstall mdm version 1.12.x and components.			
	The <i>mdm Installer for Windows</i> will automatically create database dumps of the curren mdm installation 1.12.x.			
From mdm < 1.12.0	To upgrade installed mdm version 1.5.2 or later on supported Microsoft Windows systems, there are two options:			
	 mdm Installer for Windows: Upgrade the current mdm installation stepwise to the next minor version, using the corresponding <i>mdm Installer for Windows</i>, until mdm 1.13.x is installed (e.g. from mdm 1.5.2 >> 1.6.2 >> 1.7.0 >> 1.8.0 >> 1.9.x >> 1.10.x >> 1.11.x >> 1.12.x to mdm 1.13.x) or 			
	2. Database dumps: create, export and import database dumps of the <i>mdm sever</i> and <i>CA server databases</i> as described below:			
	 dump and backup the databases, 			
	 remove the complete man installation, install mdm 1.13.x via the mdm 1.13.x Installer for Windows. 			
	 import the dumped databases. 			
	NOTE: Irreversible data loss!			
	Data of your current mdm server and CA server database will be deleted. Keep a backup copy of your current databases in a secure place.			
	NOTE: Incompatibility of mdm databases!			
	To upgrade from an older version to mdm 1.13.x, it is necessary to make irreversible changes to the backing PostgreSQL database. Once these changes have been made, the database can no longer be accessed with an older version. Keep a backup copy of your current databases in a secure place.			
	To dump and backup the databases, proceed as follows:			
	A) Make database dumps of the mdm and mdm CA server database			
	1. Copy the required batch files to the Windows system where mdm is installed.			
	2. Execute (as administrator) the batch file <i>export_mdm_server.bat</i> .			
	 Provide the path where the database dump shall be saved (default: C:\Users\username\Documents\mdm-server sql) 			
	 Provide the path to your current mdm installation directory 			
	(default: C:\Program Files\mGuard device manager).			
	5. Provide the password of the database user <i>innomms</i> if required.			
	6. Press <i>any key</i> to close the command prompt when the database dump generation has finished.			
	 (If necessary)) Repeat 1–6 but execute the batch file export_mdm_ca.bat to dump the mdm CA server database (default: mdm_ca_server.sql, database user = mdmca). 			

1.4.1 Upgrade on supported Microsoft Windows systems

Upgrade on supported Microsoft Windows systems			
	B) 1. 2.	Keep a backup copy of the database dumps Open the directory where the database dumps have been saved. Copy the database dump(s) created at step (A) to a secure place (e.g. a secure backup folder at another company server).	
	C)	(If necessary)) Backup the pull server configuration	
	1.	 To backup the web server configuration file, copy the following file to a secure place: <i>cpath to mdm installation>\apache\conf\extra\httpd-mdm.conf</i> Search for the following entries (your entries may differ from the default settings of the mdm installer given below) and write down the aliases of the pull config. 	
		 of the mdm Installer given below) and write down the aliases of the pull config server: # 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/" - If you have configured a service to send the pull feedback to mdm, search for and write down the following entries (CustomLog) as well: # Pull Config-Feedback an den mdm-Server (derzeit auskommentiert). # CustomLog "I /bin/nc -u -i1 127.0.0.1 7514" common <your configuration="" feedback=""></your> To backup the certificate and private key, copy the following files to a secure place:	
		<path installation="" mdm="" to="">\apache\conf\server.key</path>	
	D) 1.	Remove the complete mdm installation from the Windows system Remove the mdm installation by using its own unistaller or Microsoft Window's standard uninstall procedures (e.g. <i>Control Panel/Programs/Programs and</i> <i>Features</i>).	
	E)	Install mdm 1.13.x and desired components via the mdm 1.13.x Installer for Windows.	
	1.	Use the <i>mdm 1.13.x Installer for Windows</i> as described in Section 1.7.	
		Do not provide all certificate attributes of the CA identical to the ones of the older installation (e.g. add a suffix to the <i>Common Name</i>).	

Upgrade on supported Microsoft Windows systems			
	F)	Import the dumped databases (mdm server and mdm CA server)	
-	1.	Make the dumped databases available on the system where mdm 1.13.x has been installed.	
2	2.	Execute (as administrator) the batch file <i>import_mdm_server.bat</i> .	
(3.	Provide the path to the database dump (default: C:\Users\username\Documents\mdm-server.sql).	
4	4.	Provide the installation path of mdm 1.13.x (default: C:\Program Files\mGuard device manager).	
Į	5.	Provide the password of the database user innomms if required.	
(6.	Press any key to close the command prompt when the database import has finished.	
-	7.	(If necessary)) Repeat 1–6 but execute the batch file <i>Import_mdm_ca.bat</i> to import the dumped <i>mdm CA server database</i> (default: <i>mdm_ca_server.sql</i> , database user = <i>mdmca</i>).	
8	8.	mdm will restart automatically and connect to the imported databases.	
(G)	(If necessary)) Update the firmware upgrade/pull server configuration	
-	1.	Open Apache HTTP Server Monitor (included in the mdm installation) and stop the service ApacheMDM .	
2	2.	Compare the web server configuration file, with the backup file copied and stored in step (C):	
		<path installation="" mdm="" to="">\apache\conf\extra\httpd-mdm.conf Compare the aliases of the pull config server. If your former settings differ from the default settings of the mdm Installer (given below), replace the default settings accordingly to your settings (e.g. 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/" Alias /atv "C:/Program Files/mGuard device manager/apache-data/atv/" Update the pull configuration feedback to the mdm server, if it must be configured: # Pull Config-Feedback an den mdm-Server (derzeit auskommentiert). # CustomLog "I /bin/nc -u -i1 127.0.0.1 7514" common</path>	
	3.	Copy the certificate and private key, backed up and stored in step (C) to <path installation="" mdm="" to="">\apache\conf\server.crt <path installation="" mdm="" to="">\apache\conf\server.key</path></path>	
2	4.	Open Apache HTTP Server Monitor and start the service ApacheMDM.	

1.4.2 Upgrade from unsupported Microsoft Windows systems

Upgrade from unsupported Microsoft Windows systems

	-				
All mdm versions	mdm versions installed on unsupported Windows systems cannot be upgraded to mdm 1.13.x.				
	To reuse the databases of these mdm versions on supported Windows systems, you have to:				
	 dump and backup the databases, 				
	- install mdm 1.13.x via the <i>mdm 1.13.x Installer for Windows</i> on a supported system (see Section 1.7),				
	 import the dumped databases. 				
	To dump and import the <i>mdm server database</i> and <i>mdm CA server database</i> , proceed as described above ("From mdm < 1.12.0" on page 7).				

Upgrade from Linux systems					
All mdm versions	 To reuse the databases of mdm versions, installed on Linux systems, on supported Windows systems, you have to: dump and backup the databases, install mdm 1.13.x via the <i>mdm 1.13.x Installer for Windows</i> on a supported system (see Section 1.7). 				
	-	rt the dumped databases.			
		<u> </u>	NOTE: Incompatibility of mdm databases!		
		!)	To upgrade from an older version to mdm 1.13.x, it is necessary to make irreversible changes to the backing PostgreSQL database. Once these changes have been made, the database can no longer be accessed with an older version. Keep a backup copy of your current databases in a secure place.		
	Pro	Proceed as follows:			
	A)	Make	e database dumps of the mdm and mdm CA server database		
	1.	Сору	the required shell script files to the Linux system where mdm is installed.		
	2.	Exec	ute (as sudo) the shell script export_mdm_server.sh .		
	3.	Provi	de the path where the database dump shall be saved		
		(defa	ult: /tmp/mdm-server.sql).		
	4.	Provi	de the password of the database user innomms if required.		
	5.	(If nee the <i>m</i> <i>mdm</i>	cessary)) Repeat 1–4 but execute the shell script export_mdm_ca.sn to dump adm CA server database (default: mdm_ca_server.sql, database user = ca).		
	B)	Кеер	a backup copy of the database dumps		
	1.	Open	the directory where the database dumps have been saved.		
	2.	Copy backı	the database dump(s) created at step (A) to a secure place (e.g. a secure up folder at another company server).		
	C)	(lf ne	cessary)) Backup the pull server configuration		
	1.	To ba file to store	ackup the web server configuration file, copy the following server configuration a secure place. E.g. if you are using Apache 2.x, your configuration file may be d in: <i>/etc/apache2/sites-available/your-server.conf</i> .		
		– II d	f your server configuration defines any aliases for the pull configuration lirectory, write them down. They may look like: <i>Alias /atv/ "/var/www/mdm-pull/</i> " <i>Alias /atv "/var/www/mdm-pull/</i> "		
	2.	To ba	ackup the certificate and private key, proceed as follows:		
		– C a if	Check the configuration file from step (1.) (e.g. /etc/apache2/sites- available/your-server.conf) and look for the certificates used by your server. E.g. i you are using Apache 2.x, the entries may look like: SSLCertificateFile /etc/mdm/mdm-pull-server/cert.pem SSLCertificateKeyFile /etc/mdm/mdm-pull-server/key		
		- 0	Copy those files to a secure place, using the following file names: <path certificate="" to="">/server.crt <path certificate="" to="">/server.key</path></path>		

1.4.3 Upgrade from Linux systems



1.5 Operating system: Ubuntu Linux

Versions mdm 1.11.x or later can only be installed on Ubuntu (Server) 18.04 LTS. To upgrade an older versions of mdm to mdm 1.13.x, you must first upgrade Ubuntu 16.04 LTS to Ubuntu 18.04 LTS via Ubuntu's package management tools. See also:

"Quick Guide: Upgrade Ubuntu 16.04 to 18.04" on page 19

"Quick Guide (Ubuntu): Upgrade mdm 1.12.x to 1.13.x" on page 20

"Quick Guide (Ubuntu): Upgrade mdm 1.11.x to 1.12.x" on page 20

"Quick Guide (Ubuntu): Upgrade mdm 1.10.x to 1.11.x" on page 20

If your system does not fulfill the system requirements demanded in Table 1-2, *mdm server* and *mdm CA server databases* must either be dumped and imported to a newly installed mdm 1.13.x or the installed mdm version must be upgraded stepwise to mdm 1.13.x.



i

Privacy notice: Access to the *mdm software repository* server is logged to ensure the security and stability of the service. Only anonymized data is retained for statistical analysis.

System requirements

Table 1-2	System requirements (Ubuntu Linux)
-----------	------------------------------------

	mdm Client	mdm Server	mdm CA			
Operating system	 Ubuntu Desktop 18.04 LTS 	- Ubuntu (Server) 18.04 LTS				
Hardware	 A minimum of 512 MB RAM 500 MB free hard disk space Color monitor with at least 1280 x 1024 resolution 	 A minimum of 4 GB RAM 100 GB free hard disk space 	 A minimum of 512 MB RAM 5 GB free hard disk space 			
Software components	 Third-party compo OpenJDK 11, Pyth be installed via the 	Third-party components (<i>PostgreSQL 10, Apache Webserver 2.4, OpenJDK 11, Python 3.8, and OpenSSL 1.1.x</i>) will automatically be installed via the package management of Ubuntu.				
Precondition	 If not installed via Ubuntu's pack- age managing tools: OpenJDK 11 	Ivia-mdm not installed (or mdm 1.12.0 or later installed).g-All components of previous mdm installations < 1.7.0 must have been removed.				

Upgrade on supported and unsupported Linux systems				
From mdm 1.12.0 or later (installed on Ubuntu 18.04 LTS)	 To upgrade mdm versions 1.12.0 or later, installed on Ubuntu Server 18.04 LTS, you have to: upgrade mdm via Ubuntu's package management tools: Upgrade the installed mdm version via the package management tools of Ubuntu 18.04 LTS to version mdm 1.13.x. See "Quick Guide (Ubuntu): Upgrade mdm 1.12.x to 1.13.x" on page 20 NOTE: In the case of FL MGUARD 1000 devices (mGuard NT 1.3), values of the configuration are mostly reset to factory settings of mGuard NT 1.4. 			
From mdm 1.11.0 or later (installed on Ubuntu 18.04 LTS)	 To upgrade mdm versions 1.11.0 or later, installed on Ubuntu Server 18.04 LTS, you have to: upgrade mdm stepwise via Ubuntu's package management tools: Upgrade the installed mdm version in two steps via the package management tools of Ubuntu 18.04 LTS first to version mdm 1.12.x and then to mdm 1.13.x. See "Quick Guide (Ubuntu): Upgrade mdm 1.11.x to 1.12.x" on page 20. See "Quick Guide (Ubuntu): Upgrade mdm 1.12.x to 1.13.x" on page 20. For further information see mdm User Manual. 			
From mdm 1.10.0 or later (installed on Ubuntu 16.04 LTS)	 To upgrade mdm versions 1.10.0 or later, installed on Ubuntu Server 16.04 LTS, you have to: upgrade Ubuntu Server 16.04 LTS to Ubuntu Server 18.04 LTS: see "Quick Guide: Upgrade Ubuntu 16.04 to 18.04" on page 19. upgrade mdm stepwise via Ubuntu's package management tools: Upgrade the installed mdm version in several steps via the package management tools of Ubuntu 18.04 LTS first to version mdm 1.11.x and then in two more steps via version mdm 1.12.x to to mdm 1.13.x. see "Quick Guide (Ubuntu): Upgrade mdm 1.10.x to 1.11.x" on page 20 "Quick Guide (Ubuntu): Upgrade mdm 1.11.x to 1.12.x" on page 20 see "Quick Guide (Ubuntu): Upgrade mdm 1.12.x to 1.13.x" on page 20 			
From mdm 1.7.0 or later (installed on Ubuntu 16.04 LTS)	 To upgrade mdm version 1.7.0 or later, installed on Ubuntu Server 16.04 LTS, you have to proceed stepwise: 1. Upgrade the installed mdm version in several steps via the package management tools of Ubuntu 16.04 LTS to the next possible version (mdm 1.7.x >> 1.8.x >> 1.9.x >> 1.10.x). 2. Upgrade mdm 1.10.x to mdm 1.11.x as described above (<i>From mdm 1.10.0 or later</i>). For further information see mdm User Manual. 			

1.5.1 Upgrade on supported and unsupported Linux systems

Upgrade on supported and unsupported Linux systems				
From mdm < 1.7.0		mdm versions < 1.7.0, installed on supported and unsupported Linux systems, cannot be upgraded to mdm 1.13.x.		
		reuse the databases of these mdm versions on supported Linux systems, you have to: dump and backup the databases, install Ubuntu Server 18.04 LTS, install mdm 1.13.x via Ubuntu's package management tools on Ubuntu Server 18.04 LTS (see Section).		
	-	import the dumped databases.		
		D NOTE: Incompatibility of mdm databases! To upgrade from an older version to mdm 1.13.x, it is necessary to make irreversible changes to the backing PostgreSQL database. Once these changes have been made, the database can no longer be accessed with an older version. Keep a backup copy of your current databases in a secure place.		
	Pro	ceed as follows:		
	A)	Make database dumps of the mdm and mdm CA server database		
	1.	Copy the required shell script files to the Linux system where mdm is installed.		
	2.	Execute (as sudo) the shell script export_mam_server.sn .		
	з.	(default: /tmp/mdm-server.sal).		
	4.	Provide the password of the database user <i>innomms</i> if required.		
		(If necessary)) Repeat 1–4 but execute the shell script <i>export_mdm_ca.sh</i> to dump the <i>mdm CA server database</i> (default: <i>mdm_ca_server.sql</i> , database user = <i>mdmca</i>).		
		Keep a backup copy of the database dumps		
	1.	Open the directory where the database dumps have been saved.		
		Copy the database dump(s) created at step (A) to a secure place (e.g. a secure backup folder at another company server).		
	C)	(If necessary)) Backup the pull server configuration		
		To backup the web server configuration file, copy the following server configuration file to a secure place. E.g. if you are using Apache 2.x, your configuration file may in: /etc/apache2/sites-available/your-server.conf.		
		 If your server configuration defines any aliases for the pull configuration directory, write them down. They may look like: Alias /atv/ "/var/www/mdm-pull/" Alias /atv "/var/www/mdm-pull/" 		
	2.	To backup the certificate and private key, proceed as follows:		
		 Check the configuration file from step (1.) (e.g. /etc/apache2/sites- available/your-server.conf) and look for the certificates used by your server. E.g. if you are using Apache 2.x, the entries may look like: SSLCertificateFile /etc/mdm/mdm-pull-server/cert.pem SSLCertificateKeyFile /etc/mdm/mdm-pull-server/key Copy those files to a secure place, using the following file names: 		
		<pre><pre>cpath to certificate>/cert.pem <pre>cpath to certificate>/key</pre></pre></pre>		



Upgrade from Microsoft Wind	dows syst	tems	
All mdm versions	 To reuse the databases of mdm versions, installed on Windows systems, on Ubuntu Server 18.04 ITS, you have to: dump and backup the databases, install Ubuntu Server 18.04 LTS, install mdm 1.13.x via Ubuntu's package management tools on Ubuntu Server 18.04 LTS (see Section 1.8), import the dumped databases. NOTE: Incompatibility of mdm databases! To upgrade from an older version to mdm 1.13.x, it is necessary to make irreversible changes to the backing PostgreSQL database. Once these changes have been made, the database can no longer be accessed with an older version. Keep a backup copy of your current databases in a secure place.		
	Proceed	as follows:	
	A) Mak	e database dumps of the mdm and mdm CA server database	
	1. Cop	y the required batch files to the Windows system where mdm is installed.	
	2. Exec	cute (as administrator) the batch file <i>export_mdm_server.bat</i> .	
	3. Prov (defa	ide the path where the database dump shall be saved ault: <i>C:\Users\username\Documents\mdm-server.sql</i>).	
	4. Prov (defa	ide the path to your current mdm installation directory ault: <i>C:\Program Files\mGuard device manager</i>).	
	5. Prov	ide the password of the database user innomms if required.	
	6. Pres	s <i>any key</i> to close the command prompt when the database dump generation finished.	
	7. (If ne the r mdn	ecessary)) Repeat 1–6 but execute the batch file export_mdm_ca.bat to dump <i>ndm CA server database</i> (default: <i>mdm_ca_server.sql</i> , database user = <i>nca</i>).	
	B) Kee	p a backup copy of the database dumps	
	1. Ope	n the directory where the database dumps have been saved.	
	2. Cop back	y the database dump(s) created at step (A) to a secure place (e.g. a secure sup folder at another company server).	

1.5.2 Upgrade from Microsoft Windows systems

Upgrade from Microsoft Windows C) 1.	s systems (If necessary)) Backup the pull server configuration To backup the web server configuration file, copy the following file to a secure place:
C) 1.	(If necessary)) Backup the pull server configuration To backup the web server configuration file, copy the following file to a secure place:
1.	To backup the web server configuration file, copy the following file to a secure place:
	<path installation="" mdm="" to="">\apache\conf\extra\httpd-mdm.conf</path>
	- Search for the following entries (your entries may differ from the default settings
	of the mdm Installer given below) and write down the aliases of the pull config
	server: # Verzeichnis für ATV-Profile (wie in preferences yml eingestellt)
	# Alias /atv/ /var/apache-data/atv/
	# <directory apache-data="" atv="" var=""></directory>
	Alias /atv/ "C:/Program Files/mGuard device manager/apache-data/atv/"
	Alias /atv "C:/Program Files/mGuard device manager/apache-data/atv/"
2.	To backup the certificate and private key, copy the following files to a secure place:
	<path installation="" mdm="" to="">\apache\conf\server.crt</path>
	<path installation="" mdm="" to="">\apache\conf\server.key</path>
D)	Install mdm 1.13.x and desired components via Ubuntu's package
	management tools
1.	Use Ubuntu's package management tools as described in Section .
ſ	• Do not provide all certificate attributes of the CA identical to the ones of the
L	lolder installation (e.g. add a suffix to the <i>Common Name</i>).
E)	Import the dumped detabases (mdm server and mdm CA server)
E) 1	Make the dumped databases available on the system where mdm 1.13 x has been
1.	installed.
2.	Execute (as sudo) the shell script <i>import_mdm_server.sh</i> .
3.	Provide the path to the database dump (default: /tmp/mdm-server.sql).
4.	(If necessary)) Repeat 1-3 but execute the shell script import_mdm_ca.sh to
	import the dumped mdm CA server database (default: <i>mdm_ca_server.sql</i> , database user – <i>mdmea</i>)
5	database user = munica).
5.	
F)	(If necessary)) Update the firmware upgrade/pull server configuration
1.	Stop (as sudo) the Apache web Server: service apache2 stop
Ζ.	(check files backup up and stored in step (C)), edit the Apache configuration file of
	your new mdm installation:
	/etc/mdm/mdm-webbase/30-configpull.conf
	- Add the aliases of your previous configuration (do not change the real export
	directory: /var/www/mdm/). E.g.:
	Allas /atv/ "/var/www/mdm/"
0	Allas /alv /val/www/mam/
3.	opy the certificate and private key, backed up and stored in step (C) to
	/etc/mdm/mdm-webbase/ cert.pem
4	Start (as sudo) the Apache Web Server: service apache? start
т.	

1.5.3 Quick Guide: Upgrade Ubuntu 16.04 to 18.04

Version mdm 1.11.0 or later can only be installed on Ubuntu (Server) 18.04 LTS.



NOTE: Data loss during the upgrade process

Backup your files before you upgrade the system.

Backup *mdm* and *mdm CA server databases* of the current mdm installation

- 1. Copy the required shell script files to the Linux system where mdm is installed.
- 2. Execute the shell script *export_mdm_server.sh* (as sudo/adminstrator).
- 3. Provide the path where the database dump shall be saved (default: */tmp/mdm-server.sql*).
- 4. Provide the password of the database user *innomms* if required.
- (If necessary) Repeat 1–4 but execute the shell script *export_mdm_ca.sh* to dump the *mdm CA server database* (default: *mdm_ca_server.sql*, database user = *mdmca*).
- 6. Copy the created database dumps to a secure location (such as a secure backup directory on another server in the organization).

Upgrade Ubuntu 16.04 LTS to Ubuntu 18.04 LTS

- 1. Reload the package information:
 - sudo apt update
- 2. Update the packages installed under Ubuntu 16.04 LTS: sudo apt upgrade
- 3. Start the upgrade to Ubuntu 18.04 LTS:
 - sudo do-release-upgrade
- 4. Follow the on-screen instructions or press Enter to continue the upgrade if necessary.

i

1.5.4 Quick Guide (Ubuntu): Upgrade mdm 1.12.x to 1.13.x

If mdm 1.13.x is installed via the command line, the variable *DEBIAN_FRONTEND* must be used with the value *readline*. This is obligatory to display and accept the *Software License Terms* (SLT).

1. Use a text editor to change the *mdm software repository* from 1.12.x/ to 1.13.x/ in Ubuntu's /*etc/apt/sources.list*:

sudo nano /etc/apt/sources.list

- 2. Alternatively you can use the following command to add the *mdm software repository of version 1.13.x* to your package management tools:
 - sudo apt-add-repository

```
"deb http://repositories.mguard.com/mdm 1.13.x/"
```

3. Reload the package information:

sudo apt update

- 4. Start the upgrade to mdm 1.13.x:
 - sudo DEBIAN_FRONTEND=readline apt upgrade
- 5. Agree to the Software License Terms (SLT).

1.5.5 Quick Guide (Ubuntu): Upgrade mdm 1.11.x to 1.12.x

Proceed in principle as described in Section 1.5.4, whereby the version specifications of the minor versions must be reduced by 1 in each case.

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

1.5.6 Quick Guide (Ubuntu): Upgrade mdm 1.10.x to 1.11.x



Do not update your mdm installation until the upgrade from Ubuntu 16.04 LTS to Ubuntu 18.04 LTS has successfully been completed (see "Quick Guide: Upgrade Ubuntu 16.04 to 18.04" on page 19).



If mdm 1.11.x is installed via the command line, the variable *DEBIAN_FRONTEND* must be used with the value *readline*. This is obligatory to display and accept the *Software License Terms* (SLT).

1. Use a text editor to change the *mdm software repository* from 1.10.x/ to 1.11.x/ in Ubuntu's /*etc/apt/sources.list*:

sudo nano /etc/apt/sources.list

2. Alternatively you can use the following command to add the *mdm software repository of version 1.11.x* to your package management tools:

sudo apt-add-repository

"deb http://repositories.mguard.com/mdm 1.11.x/"

3. Reload the package information:

sudo apt update

4. Start the upgrade to mdm 1.11.x:

sudo DEBIAN FRONTEND=readline apt upgrade

5. Agree to the Software License Terms (SLT).

1.5.7 Update PostgreSQL databases (cluster)

After an upgrade from Ubuntu 16.04 LTS to Ubuntu 18.04 LTS the *PostgreSQL 9.5* version remains installed on the system. *PostgreSQL 10* will be installed, when the installed mdm version is upgraded to mdm 1.11.x.

The *mdm server* and *CA server* databases, created with earlier mdm versions, were created with *PostgreSQL 9.5*. However, this is not a problem as *PostgreSQL 10* is backward compatible and supports databases created with older versions.

An adaptation of the existing *mdm server* and *CA server* databases is therefore not necessary for the operation of mdm 1.11.x.

1.6 Batch files and shell scripts

Dump and import of the databases can be executed using batch files (Windows) and shell scripts (Linux) provided by Phoenix Contact available in the PHOENIX CONTACT Webshop (phoenixcontact.net/product/2981974).



Migrating mdm installations with the provided batch files/shell scripts restores only the database(s) dumped and imported. Any other installation data (e.g. pull server certificate and config files) must be manually copied to the new installation as explained below.



The provided batch files/shell scripts will only work in case of standard mdm installations (check default database names, ports, and user names in the provided preferences.xml and ca-preferences.xml files).

If mdm 1.13.x has been successfully installed via the mdm 1.13.x Installer for Windows or Ubuntu's package management tools, the batch files/shell scripts have been installed automatically in the following system folders:

Microsoft Windows

mdm server and mdm CA server: cpath to 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 files and shell scripts

Tał	ble	1-3	١
ıaı	Jie	1-3	

ıble 1-3	Windows batch files

Name	Description
export_mdm_server.bat	Windows batch file to dump the mdm server database
export_mdm_ca.bat	Windows batch file to dump the mdm CA server database
import_mdm_server.bat	Windows batch file to import the dumped <i>mdm server</i> database
import_mdm_ca.bat	Windows batch file to import the dumped <i>mdm CA server</i> database

Table 1-4 Linux shell script files

Name	Description
export_mdm_server.sh	Linux shell script file to dump the mdm server database
export_mdm_ca.sh	Linux shell script file to dump the mdm CA server database
import_mdm_server.sh	Linux shell script file to import the dumped <i>mdm server</i> database
import_mdm_ca.sh	Linux shell script file to import the dumped <i>mdm CA server</i> database



Run the installation program as the **Local Administrator** of the Windows system. The installation by another user with (**only**) administrator rights may lead to an error.

If you plan to run the mdm server, the PostgreSQL database server, and the mdm CA server (if applicable) on a single Microsoft Windows system, the automatic installer program can be used.

The installer program can additionally set up the server as a configuration pull server (see "Upload configurations to mGuard devices" in the <u>mdm User Manual</u>) or as a firmware upgrade server (see "Manage firmware upgrades with mdm" in the <u>mdm User Manual</u>).

Preconditions

The following system requirements and preconditions must be fulfilled (see Table 1-1 on page 6).

Copy the license file to a folder of your choice. You will be prompted for the file during the

installation process. The path of the license file can be configured in the *preferences.xml* file afterwards (see "mdm server (preferences.xml file)" in the <u>mdm User Manual</u>). Install the li-

If you do not specify a license file during installation, the mdm server will start in evalua-

tion mode (Evaluation License) with an allowed number of 10 devices and 2 concurrently connected clients. To purchase a license, visit the PHOENIX CONTACT Webshop at

Installation of the license file



i

mdm installation procedure

To install mdm on supported Microsoft Windows systems, proceed as follows:

- 1. Make sure that the system requirements in Table 1-1 are met.
- 2. Install the package Microsoft Visual C++ 2017 Redistributable Package (x64) or newer.

😸 Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.... 🗕 🗌 🗙



cense file prior to the start of the server.

phoenixcontact.net/product/2981974.

MICROSOFT-SOFTWARE-LIZENZBESTIMMUNGEN

MICROSOFT VISUAL C++ 2019 RUNTIME

Diese Lizenzbestimmungen sind ein Vertrag zwischen Ihnen und der Microsoft Corporation (bzw. abhängig von Ihrem Wohnsitz einem mit Microsoft verbundenen Unternehmen). Sie gelten für die oben angeführte Ich stimme den Bedingungen des Lizenzvertrags zu

Installieren Schließen

٨

Figure 1-1 Install Microsoft Visual C ++ 2015-2019 Redistributable Package (x64)

- 3. Run the installer program with as the Local Administrator of the Windows system.
- 4. Click the **Next** button on the welcome screen and accept the mdm and third-party software licenses on the following screens.

mGuard Device Manager - mdm

 Select a location where to install mdm. The default location usually needs not be modified.

Select Destination Location Where should mGuard device manager be in	nstalled?	Guard ice manager	
Setup will install mGuard device manager into the following folder. To continue, click Next. If you would like to select a different folder, click Browse.			
C:\Program Files\mGuard device manager		Browse	
At least 849.7 MB of free disk space is requ	ired.		
Visit homepage	< Back Nex	t > Cancel	

Figure 1-2 Select destination location

6. Choose which mdm components to install.

NOTE: The notification that an upload to an FL MGUARD 1000 device was successful or failed can only be reported back to mdm and displayed there if the "mdm Windows Pull Feedback" option is selected.



Figure 1-3 Install mdm components

The mdm Server, OpenJDK, PostgreSQL Database Server, mdm Service Launcher (used to run the mdm server as a service), and Apache Web Server are always installed, while the mdm Certification Authority (CA) is optional.

The Apache Web Server can also optionally be set up as Configuration Pull Server and Firmware Upgrade Server.

•

The mdm client is made available to other hosts through the web server. The hosts must support Java 11 (system-wide or via local Java binary). To run the client, download the *ZIP* file from the web server, unpack it, and start the mdm-client-1.13.x.jar file.

7. Provide a license file for the mdm server or skip license file installation to run mdm in evaluation mode.

Installation of the license Please choose a valid license file.	mguard device manager
Please select now the license file that you re License file:	eceived from your system partner.
	Browse
Install without license (evaluation mode)	
<u>Visit homepage</u>	< Back Next > Cancel



8. The installer program creates a self-signed X.509 certificate and a matching private key to be used by the https web server. Enter attributes to be used for the certificate.

The Apa corresp	ache Web Server requires an X.509 certificate and onding private key.	device manage
Please e with * a IP addre	enter the certificate attributes to generate a new se re mandatory. The common name (CN) attribute mu ess used by the mGuard appliances to access the se	If-signed certificate. Fields st match the host name or ·ver.
Commo	n Name (CN): *	
My-Cor	nmon-Name	
E 1 0	-).	
	-/·	
?	The certificate's common name (CN) attribute name or IP address used by the mGuard appli	e must match the host ances to access the
?	The certificate's common name (CN) attribute name or IP address used by the mGuard applic Config Pull Server or the Firmware Upgrade Se Are you sure you want to continue?	e must match the host ances to access the erver.
?	The certificate's common name (CN) attribute name or IP address used by the mGuard applic Config Pull Server or the Firmware Upgrade Se Are you sure you want to continue? Ye	e must match the host ances to access the erver.
?	The certificate's common name (CN) attribute name or IP address used by the mGuard applic Config Pull Server or the Firmware Upgrade Se Are you sure you want to continue? Ye	e must match the host ances to access the erver.
2	The certificate's common name (CN) attribute name or IP address used by the mGuard appli Config Pull Server or the Firmware Upgrade Se Are you sure you want to continue? Ye	e must match the host ances to access the ever.
	The certificate's common name (CN) attribute name or IP address used by the mGuard appli Config Pull Server or the Firmware Upgrade Se Are you sure you want to continue?	e must match the host ances to access the erver.
Country	The certificate's common name (CN) attribute name or IP address used by the mGuard applic Config Pull Server or the Firmware Upgrade Se Are you sure you want to continue? Ye Your Code (C): *	e must match the host ances to access the erver.

Figure 1-5 Attributes to be used for the certificate

9. Access to the directories served by the web server can optionally be protected with a user name and password. Choose whether you want this protection, and if so, enter a user name and password.

🔄 Setup - mGuard device manager	– 🗆 ×
Apache Web Server Advanced configuration	mguard device manager
You have the opportunity to protect web acc and password. Use Apache web directory access protect Username:	cess to the directory with a username tion
mdm Password: Repeat password:]
<u>Visit homepage</u>	< Back Next > Cancel

Figure 1-6 Apache Web Server – Web access protection

10. The following applies only if the mdm CA is installed: The installer program creates a CA certificate and matching private key. Enter attributes to be used for the certificate.

×
d

Figure 1-7 Attributes to be used for the certificate

Upgrade FL MGUARD DM UNLIMITED to version 1.13.x

11. The installer can optionally add shortcuts to the Start menu. If this is desired, choose a folder to which to add the shortcuts.

	Setup - mGuard device manager	-			×
	Select Start Menu Folder Where should Setup place the program's shortcuts?	device	G ma	ua Inagel	rd
	Setup will create the program's shortcuts in the follow	wing Start I	Menu	folder.	
	To continue, click Next. If you would like to select a different	folder, click	Brow	ise.	
	mGuard device manager		Bro	wse	
	□ Don't create a Start Menu folder				
	—				
<u>Vi</u>	sit homepage < Back	Next >		Cance	el

Figure 1-8 Start Menu Folder – Shortcuts

12. Click on the **Install** button.

🛐 Setup - mGuard device manager	_		\times
Ready to Install Setup is now ready to begin installing mGuard device manager on your computer.	device r	iua manage	rd #
Click Install to continue with the installation, or click Back if yo change any settings.	ou want to rev	iew or	
Start Menu folder: mGuard device manager Software version informations: PostgreSQL 10.7-1 OpenJDK Platform Version 11.0.2 Apache 2.4.38 OpenSSL 1.1.1b Microsoft Visual C++ 2010 Redistributable Package Microsoft Visual C++ 2013 Redistributable Package		~	
Visit homepage < Back	Install	Can	cel

Figure 1-9 Install mdm

The mdm components will be installed on the system. The locations served through the Apache web server will be reported. mdm is now ready to be used.

1.8 Ubuntu's package management tools

For the installation of the following mdm components on Ubuntu Linux, the automatic installation via Ubuntu's package management tools and the *mdm software repository* can be used.

1

Privacy notice: Access to the *mdm software repository* server is logged to ensure the security and stability of the service. Only anonymized data is retained for statistical analysis.

Package	Description				
mdm-all-server	Meta package to install all mdm server components.				
mdm-common	Contains basic components required to in- stall mdm.				
mdm-server	Contains the server component of mdm.				
	Starts as systemd service.				
mdm-client	Contains the client components of mdm.				
	Starts as systemd service.				
mdm-ca	Contains the CA components of mdm (CA server).				
mdm-configpull	Sets up the apache2 server to provide the mdm configuration pull feature (see mdm. User Manual).				
mdm-clientdownload	Sets up the apache2 server to allow the mdm client download.				
mdm-webbase	Configures apache2 for mdm and allows it to be used as firmware server (see mdm. User Manual).				

 Table 1-5
 Installable packages from the mdm software repository

PostgreSQL database server and *OpenSSL* may be automatically installed from Ubuntu's standard repositories.

PreconditionsThe following system requirements and preconditions must be fulfilled (see Table 1-2 on
page 13).Installation of the license
fileSave the license file as /etc/mdm/mdm-server/mdmlic.lic. The path of the license file can be
configured in the preferences.xml file afterwards (see mdm User Manual). If you do not
specify a path for the license file in the preferences.xml file, mdm assumes the license file
to be in the same directory as the mdm server.
Install the license file prior to the installation of the mdm server package into /etc/mdm/mdm-
server/mdmlic.lic, creating the path as needed, or restart the server manually after you have
installed a new license.

1.8.1 Full mdm installation

To install **mdm and components** on Ubuntu (Server) 18.04 LTS using Ubuntu's package management tools, proceed as follows:



1.8.2 Quick mdm server and client installation (full 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 Analyzing server log files

mdm server

Output of the complete log entries of the mdm server:

journalctl -u mdm-server.service

Output of the log entries of the mdm server since the last reboot:

journalctl -b -u mdm-server.service

mdm CA Server

Output of the log entries of the mdm CA server:

journalctl -u mdm-ca.service

Output of the log entries of the mdm CA server since the last restart:

journalctl -b -u mdm-ca.service

The mdm CA server log files are also saved by Ubuntu to the file: /var/log/mdm-ca.log .

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 <u>phoenixcontact.com</u> .
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