FL MGUARD 2000/4000
Device replacement and migration mGuard 8 --> mGuard 10

Application note

Application note

FL MGUARD 2000/4000 - Device replacement and migration mGuard 8 --> mGuard 10

AH EN MGUARD MIGRATE 10, Revision 03 2025-03-31

This user manual is valid for

Designation	Item No.
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

Firmware version: mGuard 10.5.x

Applicable documentation (available at phoenixcontact.net/product/<item number>):

Release Notes

mGuard 10.5.x Firmware – Release Notes

User Manual „Installation and startup“

UM EN HW FL MGUARD 2000/4000 – 110192_en_xx

User Manual „Web-based management“

UM EN FW MGUARD10 – 110191_en_xx

User Manual „Installation, Configuration and Usage of the mGuard device manager (mdm)“:

UM EN MDM 1.17 – 111024_en_xx

111259_en_03

1 Device replacement and migration

1.1 Migration from mGuard 8.x to mGuard 10.x

The devices of the new FL MGUARD 2000/4000 series are compatible with the devices of the previous series (previous models with mGuard 8.x firmware) (see Table 1-1).

It is therefore possible to import and activate a configuration profile created on the predecessor model (mGuard 8.x) on the new device (mGuard 10.x).

The configuration can be migrated or imported in three ways:

– Import via web interface (Section 1.3.1)
– Import via SD card (Section 1.3.2)
– Import via “mGuard device manager (mdm)” (see mdm user manual)

For the majority of applications, the migration is performed directly and without additional configuration effort.

Table 1-1 Migration of the configuration of compatible devices: mGuard 8.x --> 10.5

New devices – mGuard 10	Item number	Previous models – mGuard 8	Item number
FL MGUARD 4302 FL MGUARD 4302/KX	1357840 1696708	FL MGUARD RS4000 TX/TX (VPN) FL MGUARD RS4000 TX/TX-P	2700634 / (2200515) 2702259
FL MGUARD 4305 FL MGUARD 4305/KX	1357875 1696779	FL MGUARD RS4004 TX/DTX (VPN)	2701876 / (2701877)
FL MGUARD 2102	1357828	FL MGUARD RS2000 TX/TX VPN FL MGUARD RS2000 TX/TX-B	2700642 2702139
FL MGUARD 2105	1357850	FL MGUARD RS2005 TX VPN	2701875
FL MGUARD 4102 PCI	1441187	FL MGUARD PCI4000 VPN	2701275
FL MGUARD 4102 PCIE	1357842	FL MGUARD PCIE4000 VPN	2701278
The models specified on the right do not represent predecessor models in the true sense. However, your configuration can still be migrated to the new devices with corresponding adjustments.		FL MGUARD GT/GT (VPN)	2700197 / (2700198)
		FL MGUARD SMART2 (VPN)	2700640 / (2700639)
		FL MGUARD DELTA TX/TX (VPN)	2700967 / (2700968)
		FL MGUARD RS4000 TX/TX VPN-M	2702465

In rare cases and for certain configurations, it may be necessary to adapt the existing configuration (mGuard 8) before migrating (see Section 1.4).

Please note that configurations of FL MGUARD (RS)4000 series devices can only be migrated after adjustments to FL MGUARD 2000 series devices.

1.2 General procedure

- Start the old device (mGuard 8).
- Save the current configuration of the old device to an external data carrier.
- Check whether unsupported functions are activated.
- If necessary, set unsupported functions to the default settings.
- Save and export the adapted configuration of the old device.
- Start the new device (mGuard 10).
- Import the previously exported configuration onto the new device.
- Check exactly whether the configuration has been imported successfully.
- If not already done so: Activate the imported configuration on the new device.
- Disconnect the old device from the power supply.
- Disconnect the old device from the network.
- If necessary, disconnect the service contacts (I/Os) of the old device.
- Connect the new device to the network.
- If necessary, connect the service contacts (I/Os) of the new device.
- Start the new device.

↳ Firewall rules are activated.

↳ Network connections and VPN connections are established.

- Check whether the connections in your network behave as expected.
- If necessary, remove the SD card from the device.

Result

↳ The old device configuration was imported and activated on the new device.

↳ All migrated functions are executed on the new device as usual.

↳ The old device can be removed and taken out of operation (Decommissioning mode).

Video

The process of device migration is also shown in a short video on the Phoenix Contact website.

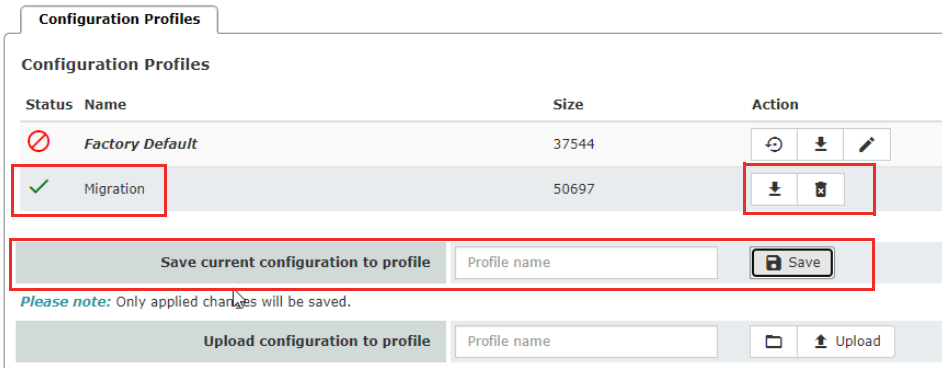
Link to the video: phoe.co/security-router-mGuard

1.3 Saving and importing the device configuration

1.3.1 Import via web-based management (WBM)

In rare cases and for certain configurations, it may be necessary to adapt the existing configuration (mGuard 8) before migrating (see Section 1.4).

To export a configuration via the WBM from an mGuard 8 device and import it to an mGuard 10.5 device, proceed as follows.



Exporting the configuration profile

First, create and export a configuration profile on the old device (mGuard 8.x):

- Open the menu “Management >> Configuration Profiles >> Configuration Profiles”.
- At “Save current configuration to profile”:
  - Give the profile a profile name.
  - Click on „Save“.

↪ The configuration profile appears in the list of saved profiles.

- Click on the name of the configuration profile you want to migrate.

↪ The profile is downloaded to the configuration computer: *<name>.atv*

Importing the configuration profile

Then import the exported configuration profile into the new device (mGuard 10.5):

- Open the menu “Management >> Configuration Profiles >> Configuration Profiles”.
- At “Upload configuration to profile”:
  - Give the profile a profile name.
  - Click on the icon to select the previously created configuration profile.
  - Click on “Upload”.

↪ The configuration profile is imported into the device and appears in the list of saved profiles.

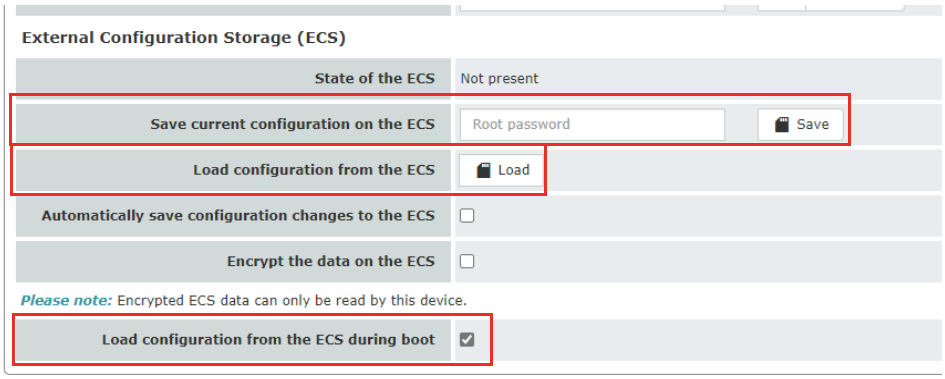
- Activate the profile by clicking on the “Restore profile” icon.

↪ The configuration profile is activated.

1.3.2 Import via SD card (ECS)

In rare cases and for certain configurations, it may be necessary to adapt the existing configuration (mGuard 8) before migrating (see Section 1.4).

To export an SD card configuration from an mGuard 8 device and import it to an mGuard 10.5 device, proceed as follows.



Exporting a configuration

Save the configuration of the old device (mGuard 8.x) on an SD card:

- Open the menu “Administration >> Configuration Profiles >> External Configuration Storage (ECS)”:
- At “Save current configuration on the ECS”:
  - Enter the password of the user *Root* on.
  - Click on the “Save” button .

↪ The currently stored configuration is written to the SD card inserted.

The configuration on the external storage medium also contains the encrypted passwords (hashed) for the *root*, *admin*, *netadmin*, *audit*, and *user* users, as well as for SNMPv3 users. These are also applied during charging.

Importing a configuration

The configuration can be imported in two ways:

1. **Automatically on startup**

- Insert the SD card with the saved configuration **before startup** into the new device.
- Start the device.

↪ The configuration is automatically loaded and activated.

2. **Manual**

- Insert the SD cards with the saved configuration **after the start** into the new device.
- Log in to the web interface (WBM) of the device.
- Open the menu “Administration >> Configuration Profiles >> External Configuration Storage (ECS)”.
- Start the “Load configuration from the ECS” function.

↪ The configuration is loaded and activated.

1.3.3 Signed configuration profiles

From firmware version mGuard 10.5.0, it is possible to sign configuration profiles. On devices configured accordingly, it is then only possible to import and use signed configuration profiles. Unsigned configurations will be rejected.

If you still want to import unsigned, already exported configuration profiles on such a device, you can also sign them manually with a machine certificate of the mGuard device before importing them. The procedure is described below.

Required files

Make the following files available.

Table 1-2 Required files (the names are examples)

my_profile.atv = configuration profile	Configuration profile (e.g. *my_profile.atv)* that is to be signed.
sign.crt = machine certificate	Machine certificate with which the configuration profile is to be signed. (The associated private key is *sign.pem*). The machine certificate, but not the associated private key, can be downloaded from an mGuard device (or, like *sign.pem*, provided using a saved file). The certificate must be PEM-encoded. It is a text file. It begins with "-----BEGIN CERTIFICATE-----".
sign.pem = private key	Private key of the machine certificate. (The corresponding machine certificate is *sign.crt*). The private key must be PEM-encoded. The text file begins with "-----BEGIN RSA PRIVATE KEY-----".

Requirements

The configuration profile (e.g. *my_profile.atv*)

- must not contain an existing signature. Lines beginning with "#sig" must be removed (see below).
- must use the Unix convention for line endings (simple "Newline"). If the file uses the Windows convention ("Carriage Return" followed by "Newline"), it must be recoded accordingly.
- must end with an end-of-line character ("Newline").

Creating a signature

You can use the *sign.crt* and *sign.pem* files to create the signature with which the *my_profile.atv* configuration profile is to be signed:

- Use the following Linux command to create a signature:

  ```
  openssl cms -sign -signer sign.crt -inkey sign.pem -in
  my_profile.atv -binary -out signature.pem -outform PEM
  ```

↪ The command creates the signature file *signature.pem*.

- Open the *signature.pem* file in a text editor.
- Remove the header ("-----BEGIN CMS-----") and footer ("-----END CMS-----").
- Prefix each line with the text string "#sig" followed by a space character.

  To do this, use the following Linux command (including all space characters):

  ```
  sed '/^-/d; s/^/#sig /' signature.pem > signature.txt
  ```

↪ The modified file is saved in the new *signature.txt* file.

Signing the configuration profile

You can sign the configuration profile *my_profile.atv* with the created signature (*signature.txt*).

- Use the following Linux command:

  cat signature.txt >> my_profile.atv

↪ The signature is appended to the configuration profile *my_profile.atv* and the profile is signed.

↪ You can now import the signed configuration profile on devices that only accept signed configuration profiles. The corresponding certificates for verification must be installed on these devices (machine certificate s*ign.crt* or corresponding CA certificates that form a chain of trust with *sign.crt)*.

Example: ATV file with signature

```
[...]
VPN_TCPENCAP_LISTEN_PORT = "443"
VPN_UNIQUE_IDS = "no"
VPN_XFRM4_GC_THRESH = "2"
WWW_LANGUAGE = "de"
WWW_LEVEL = "10"
WWW_TIMEOUT = "1800"
// End of configuration profile
#sig MIIFcwYJKoZIhvcNAQcCoIIFZDCCBWACAQExDTALBglghkgBZQMEAgEwCwYJKoZI
#sig hvcNAQcBoIIC8DCCAuwwggHUoAMCAQICCDVQ08u5bnJBMA0GCSqGSIb3DQEBCwUA
#sig MC0xCzAJBgNVBAYTAmRlMQ4wDAYDVQQLEwVLQiBDQTEOMAwGA1UEAxMFS0IgQ0Ew
#sig HhcNMjQwODI4MDkyNTAwWhcNMzQwODI4MDkyNTAwWjAtMQswCQYDVQQGEwJkZTEO
#sig MAwGA1UECxMFS0IgQ0ExDjAMBgNVBAMTBUtCIENBMIIBIjANBgkqhkiG9w0BAQEF
#sig AAOCAQ8AMIIBCgKCAQEApjPzB1f6PwugA7anO+I1IS7TmrpDu3j63RGcIxahb8Yf
#sig 6SkogxzVvuQ9xzc39G5ByERKjamW7AbgnmnPHEU08d0x1WSA9XMTkTD8cXh1ih4S
#sig /K8L2edSdAunEHUkY9anCY0eC+MoGOMVA1XJOFBa1wZump91dKdoRmUfF1N4Nf3N
#sig sKkqHvwgR58dl9G66ovVhpZtqxKx0eAhsB20vg15cEdnTC7GZrWUgBoXGe0bdvwf
#sig 3NePis9b8NkzGByISGfe5L8RqpSZtfdDHO1zJzH10oBZtbK4iXa8YEUQagjGO92D
#sig R7AHxCA44ViSp1yXPPutRmKTYvOJvjGU4oH03yGkbwIDAQABoxAwDjAMBgNVHRME
#sig BTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQCTtf/Y2gYjviznleUUCcqq3G82cL9c
#sig 1EutiiakDhHUT6+lVSSFYj4H9QMKHWRmD5B3nmeqqm6pwti93teol9VGQnD/5oQM
#sig c2mikMfah32lXwN0RiyAcki56ss0EAmhXcBBmgG4rbt7RRwy7KU8KsrauxeOtwP1
#sig aIAwg1luDnEEWOfYcOKCoYg7Z55pQHibfP9QYVApfJ/4w8nFKcyVloHZ2fSQNhpv
#sig azgZMU5cVugBU2cWd666amYQsb1FtEmKXDlJ2iDK4MniUR2uedUxNwbafYqBUGFQ
#sig WKMFTK+gLkiOMjDx2TYjFaqT9qPCWdpD0zx9zTURjTZlLk0UR3SyE3UcMYICSTCC
#sig AkUCAQEwOTAtMQswCQYDVQQGEwJkZTEOMAwGA1UECxMFS0IgQ0ExDjAMBgNVBAMT
#sig BUtCIENBAgg1UNPLuW5yQTALBglghkgBZQMEAgGggeQwGAYJKoZIhvcNAQkDMQsG
#sig CSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMjUwMTA5MTMzNTU2WjAvBgkqhkiG
#sig 9w0BCQQxIgQgZYjoHiYvLsdilwjey6PC2Y/uOj2v6+KcSZQ0lE1AtdcweQYJKoZI
#sig hvcNAQkPMWwwajALBglghkgBZQMEASowCwYJYIZIAWUDBAEWMAsGCWCGSAFlAwQB
#sig AjAKBggqhkiG9w0DBzAOBggqhkiG9w0DAgICAIAwDQYIKoZIhvcNAwICAUAwBwYF
#sig Kw4DAgcwDQYIKoZIhvcNAwICASgwDQYJKoZIhvcNAQEBBQAEggEAFildP5txQr5S
#sig /7gkM6ORS4Ij2fHUd/+qGY6Bl2l8o6O/sVduYBBIG2xGt4OtBUAIormCzScXdMT3
#sig rTBEl13G6ec72qU1KpT0c+4eY+gdTVQLqp8qpaelU4sbFk4/SgpzyxT+M2pcOxD3
#sig Jik/yAYfkHuV/P4VsYNM0C0keK4Yb0XYUU85pAhStvCK8p4Fzekd+P9pODCx4VB/
#sig aSozgxhzz37pa1bxSowCMFAhZRgUtgieMuLEyAjQ+C0EwRqZT/zHzFmD3r0l72lw
#sig ZAvPvZGFkGk/C7VSworTa4fQwZNmIn8axP7Sx8CC/kEfrJl5DFtRY5xnDB+WXsNh
#sig hVzQQxbnGQ==
```

1.4 Cases that require manual adjustment

Some functions available on the previous models (mGuard 8) are not supported by the new devices (mGuard 10) (see).

In the event of a migration via web-based management, a corresponding error message would be displayed when attempting to import such a configuration.

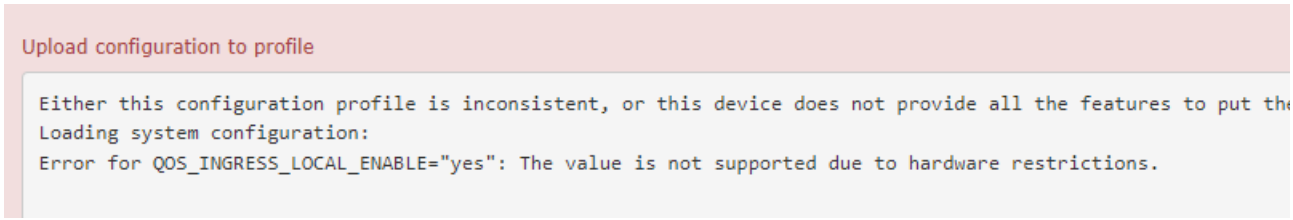


Figure 1-1 Example of an error message when importing incompatible configurations

Functions not supported in mGuard 10.5

Table 1-3 Functions not supported in mGuard 10.5

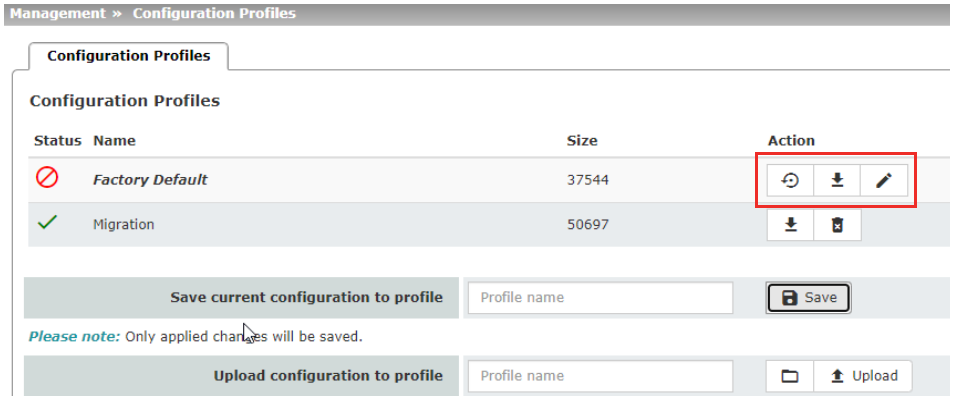
Network: Interfaces – PPPoE – PPTP – Secondary external interface
Network: Serial interface
Network: GRE tunnel (generic routing encapsulation)
VPN redundancy
Quality of Service (QoS)
CIFS Integrity Monitoring
SEC stick

What do you need to do?

Before you start the migration, you must manually reset the functions specified in to default settings on the old device (mGuard 8). If an error message is shown in the WBM (see above), you can use it as a guide if necessary.

Proceed as described in Section 1.5 .

1.5 Resetting variables to the default settings



The variables that are no longer available on the new device () must be reset to the default settings on the old device before migrating.

If this is not the case, an error message is displayed for an incompatible configuration from which you can ideally derive the variables to be customized.

Alternatively, you can compare the current configuration with the factory default settings of the device. This is done using the “Compare” function in the web interface.

Once you have identified the corresponding variables, you must manually reset them to the default settings.

To do this, proceed as follows:

First, create a backup copy of your current configuration.

To do this, save the configuration profile on the device and download it or save it to an SD card (see Section 1.3).

1. Log into the device via web-based management (WBM).
2. Open the menu “Management >> Configuration Profiles”.
3. Click on the “Edit profile” icon to the right of the “Factory Default” configuration profile.

↪ The “Factory Default” configuration profile is loaded, but not activated yet.

NOTE: Do not activate the profile because it will change the network settings of the device and the network access will be lost.

↪ All entries that contain changes to the configuration currently used are highlighted in green on the relevant page and in the associated menu path.

4. Identify using and, if necessary, the variables that must be reset to the default settings using error messages in the WBM. Note the relevant variables.
5. **IMPORTANT**: Now restore your **currently used configuration** by clicking on the “Reset” icon .
6. In your configuration currently used, only return the identified variables manually to the default settings.
7. Then click on the “Apply” icon .
8. If necessary, repeat steps 3 – 7.

↪ Once you have reset all relevant variables to the default settings, you can start the migration (see Section 1.3).

1.6 Device differences

For more information, see the UM EN HW FL MGUARD 2000/4000 – 110192_en_xx device manual (available at phoenixcontact.net/product/<Item number>).

Network ports

Table 1-4 Designation of the network ports / switch ports

mGuard 8	mGuard 10	mGuard 8 (Internal)	mGuard 10 (Internal)
WAN	XF1	(n/a)	(n/a)
LAN1	XF2	swp2	swp0
FL MGUARD 2105/4305 (KX)			
LAN2	XF3	swp0	swp1
LAN3	XF4	swp1	swp2
FL MGUARD 2105			
LAN4	XF5	swp3	swp3
FL MGUARD 4305 (KX)			
DMZ	XF5	swp4	dmz0
Not for FL MGUARD 2105/FL MGUARD 4305 (KX)			
LAN5	(n/a)	swp4	(n/a)

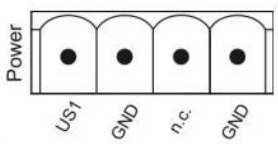
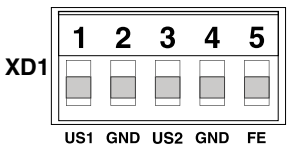
Switching inputs/switching outputs (I/Os)

Table 1-5 Switching inputs/switching outputs (I/Os) via Combicon connector

mGuard 8	mGuard 10
Switching inputs	
(Service 1) CMD1 (I1)	(XG1) CMD1 (I1)
(Service 2) CMD2 (I2)	(XG1) CMD2 (I2)
(Service) CMD3 (I3)	(XG1) CMD3 (I3)
Switching outputs (signal outputs)	
(Service) ACK1 (O1)	(XG2) ACK1 (O1)
(Service) ACK2 (O2)	(XG2) ACK2 (O2)
Switching output (alarm output)	
(Contact) FAULT (O4)	(XG2) O3

Supply voltage

Table 1-6 Power supply via Combicon connector

mGuard 8	mGuard 10 (Redundancy only for FL MGUARD 43xx)
	

1.6.1 Added functions that were already available on the old device platform

Variables that were already present on the old device platform but had been removed in the meantime were added again on the new device platform.

Table 1-7 Newly added functions / variables / variable values

New function / variable / value	New function / Impact of migration	Firmware (Added with firmware version)
[Deep Packet Inspection / Modbus TCP] **Menu**: Network Security >> Deep packet Inspection >> Modbus TCP **Section**: Rule Records **Variable**: various **GAI variable**: MODBUS_RULESETS.x.FRIENDLY_NAME MODBUS_RULESETS.x.SET.y.MODBUS_FUNCTION_CODE MODBUS_RULESETS.x.SET.y.ADDRESS_RANGE MODBUS_RULESETS.x.SET.y.TARGET MODBUS_RULESETS.x.SET.y.COMMENT MODBUS_RULESETS.x.SET.y.LOG MODBUS_RULESETS.x.LOG_DEFAULT	The mGuard device can check packets of incoming and outgoing Modbus TCP connections (*Deep Packet Inspection*) and filter them if necessary. **Migration of older mGuard configurations** No effect. Already configured variable values will be adopted.	**10.5.0**
[Deep Packet Inspection / OPC Inspector] **Menu**: Network Security >> Deep packet Inspection >> OPC Inspector **Section**: OPC Inspector **Variable**: various **GAI variable**: IP_CONNTRACK_OPC IP_CONNTRACK_OPC_SANITY IP_CONNTRACK_OPC_TIMEOUT	Until now, the *OPC Classic* network protocol could only be used across firewalls if large port ranges were opened. Activating the *OPC Classic* function allows this network protocol to be used easily without having to configure the mGuard device's firewall in an insecure way. **Migration of older mGuard configurations** No effect. Already configured variable values will be adopted.	**10.5.0**

Table 1-7 Newly added functions / variables / variable values[...]

New function / variable / value	New function / Impact of migration	Firmware (Added with firmware version)

[Web access via HTTPS / Server certificate]
Menu: Management >> Web Settings >> Access
Section: HTTPS Web Access
Variable: HTTPS server certificate
GAI variable: HTTPS_SERVER_CERT_REF
 	
In previous firmware versions, the function was not officially available, but could be used as an unsupported expert function.
	Instead of the self-signed web server certificate pre-installed on the mGuard device, a separate machine certificate can be uploaded to the device and used. The device can use this certificate to authenticate itself to requesting clients.
	The use of CA certificates in conjunction with a certificate chain of trust is possible.
	
	Migration of older mGuard configurations
	If an HTTPS server certificate is already in use, its use must be deactivated **before migrating the configuration or updating the device.**
	`Command on the command line:`
	`gaiconfig --set HTTPS_SERVER_CERT_REF ""`
	You can now perform the migration/update again and use the certificate again (if it is valid).
	If no HTTPS server certificate is used, the following applies:
	No effect.
		10.5.0

1.6.2 Newly added functions

Variables have been added to the new device platform that are not available on the old device platform.

Table 1-8 Newly added functions / variables

New variable in WBM	New function / Impact of migration	Firmware (Added with firmware version)
[TCP-Dump] **Menu**: Support >> Advanced >> TCP Dump **Section**: TCP Dump **Variable** (Action): (1) Starting tcpdump (2) Stopping and downloading tcpdump	A packet analysis (*tcpdump*) can be used to analyze the content of network packets that are sent or received via a selected network interface. **Migration of older mGuard configurations** No effect.	**10.5.0**
[Logging] **Menu**: Logging >> Settings **Section**: Data protection **Variable**: Maximum retention period for log entries (0 = unlimited) **GAI variable**: LOGGING_MAX_DAYS	In order to comply with basic data protection requirements, it is possible to save log entries on the device only for a limited period of time. After a configurable storage period has expired, log entries will be deleted automatically from the device. **Migration of older mGuard configurations** No effect	**10.5.0**
[OpenVPN Client] **Menu**: OpenVPN Client >> Connections >> Tunnel Settings **Section**: Data Encryption **Variable**: Encryption algorithm **GAI variable**: OPENVPN_CONNECTION.x.VPN_ENCRYPTION	**The "Blowfish" encryption algorithm is no longer supported.** A total of six AES encryption algorithms can be selected instead of the previous three: AES-128-GCM / AES-192-GCM / AES-256-GCM / AES-128-CBC / AES-192-CBC / AES-256-CBC **Migration of older mGuard configurations** After migrating a configuration from an older firmware version with the "Blowfish" encryption algorithm configured, the value of the variable is set to "AES-256-GCM". The following applies to all other algorithms: The value from the migrated configuration is adopted unchanged. The configured encryption algorithm will not be changed.	**10.5.0**

Table 1-8 Newly added functions / variables [...]

New variable in WBM	New function / Impact of migration	Firmware (Added with firmware version)
[HTTPS access] **Menu**: Management >> Web Settings >> Access **Section**: HTTPS Web Access **Variable**: Lowest supported TLS version **GAI variable**: TLS_MIN_VERSION	Some functions of the mGuard device use TLS encryption, e.g.: – Web server (HTTPS access) – OpenVPN Client The used TLS version is negotiated between the remote peers. It is possible that a TLS version will be selected, that is no longer considered secure. To prevent this, it can be specified which TLS version will be accepted by the mGuard device as the lowest TLS version. Connections with lower TLS versions will be rejected by the mGuard device. Default: TLS 1.2 **Migration of older mGuard configurations** The variable will be configured with the value TLS 1.0/1.1. All TLS versions from TLS 1.0 are accepted by the mGuard device.	**10.5.0**
[LINK Mode] **Menu**: Network >> Interfaces >> General **Section**: Network Status / Network Mode **Variable**: LINK mode **GAI variable**: ROUTER_MODE_LINK	The mGuard device can use the device "CELLULINK" available from Phoenix Contact to establish a mobile data connection to other networks or the Internet (e.g. via the 4G network). If LINK mode is activated, a hyperlink to the web-based management of the device "CELLULINK" is displayed in the WBM area of the mGuard device. **Migration of older mGuard configurations** No effect.	**10.5.0**

Table 1-8 Newly added functions / variables [...]

New variable in WBM	New function / Impact of migration	Firmware (Added with firmware version)
[Web access via HTTPS / Server certificate] **Menu**: Management >> Web Settings >> Access **Section**: HTTPS Web Access **Variable**: HTTPS server certificate **GAI variable**: HTTPS_SERVER_CERT_REF In previous firmware versions, the function was not officially available, but could be used as an unsupported expert function.	Instead of the self-signed web server certificate pre-installed on the mGuard device, a separate machine certificate can be uploaded to the device and used. The device can use this certificate to authenticate itself to requesting clients. The use of CA certificates in conjunction with a certificate chain of trust is possible. **Migration of older mGuard configurations** If an HTTPS server certificate is already in use, its use must be deactivated **before migrating the configuration or updating the device.** Command on the command line: `gaiconfig --set HTTPS_SERVER_CERT_REF ""` You can now perform the migration/update again and use the certificate again (if it is valid). If no HTTPS server certificate is used, the following applies: No effect.	**10.5.0**
[OpenVPN Client] **Menu**: OpenVPN Client >> Connections >> Tunnel Settings **Section**: Data Encryption **Variable**: Hash algorithm (HMAC authentication) **GAI variable**: OPENVPN_CONNECTION.x.VPN_-AUTH_HMAC	The hash function used to calculate the checksum can be configured. **Migration of older mGuard configurations** After migrating a configuration from an older firmware version, the value of the newly added variable is set to "SHA-1".	**10.4.0**

Table 1-8 Newly added functions / variables [...]

New variable in WBM	New function / Impact of migration	Firmware (Added with firmware version)
[Update Server] **Menu**: Management >> Update >> Update **Section**: Update Servers **Variable**: Server certificate **GAI variable**: PSM_REPOSITORIES.x.REMOTE_CERT_REF	To ensure that a secure HTTPS connection is established to the configured update server, a server certificate for the update server can be installed on the mGuard device. This can be used by the mGuard device to check the authenticity of the update server. **Migration of older mGuard configurations** After migrating a configuration from an older firmware version, the value of the newly added variable is set to "Ignore".	**10.3.0**
[Alarm Output] **Menu**: Management >> Service I/O >> Alarm Output **Section**: Operation Supervision **Variable**: Passwords not configured **GAI variable**: PASSWORD_CHECK	A configurable alarm "Passwords not configured" for default passwords that have not been changed (*admin/root)* has been added to the device. The alarm triggers the alarm output via I/Os and the corresponding FAIL LED. **Migration of older mGuard configurations** After migrating a configuration from an older firmware version, the value of the newly added variable is set to "Supervise".	**10.3.0**

1.6.3 Changed default settings

In a few cases, the default settings of existing variables on the old and new device platform differ.

Table 1-9 Changed default settings

Function	Changed default settings / Impact of migration	Firmware (Added with firmware version)
[OpenVPN Client] **Menu**: OpenVPN Client >> Connections >> Tunnel Settings **Section**: Data Encryption **Variable**: Encryption algorithm **GAI variable**: OPENVPN_CONNECTION.x.VPN_ENCRYPTION	In the default settings, the encryption algorithm "AES-256-GCM" is used instead of "AES-256-CBC" as before. **Migration of older mGuard configurations** After migrating a configuration from an older firmware version with the "Blowfish" encryption algorithm configured, the value of the variable is set to "AES-256-GCM". The following applies to all other algorithms: The value from the migrated configuration is adopted unchanged. The configured encryption algorithm will not be changed.	**10.5.0**
[OpenVPN Client] **Menu**: OpenVPN Client >> Connections >> Tunnel Settings **Section**: Data Encryption **Variable**: Hash algorithm (HMAC authentication) **GAI variable**: OPENVPN_CONNECTION.x.VPN_AUTH_HMAC	In the default settings, the hash algorithm "SHA-256" is used instead of "SHA-1" as before. **Migration of older mGuard configurations** The value from the migrated configuration is adopted unchanged. The configured hash algorithm will not be changed.	**10.5.0**
[E-Mail] **Menu**: Management >> System Settings >> E-Mail **Section**: E-Mail **Variable**: Encryption mode for the e-mail server **GAI variable**: EMAIL_RELAY_TLS	In the default settings, the encryption algorithm "TLS Encryption" is used instead of "No encryption" as before. **Migration of older mGuard configurations** The value from the migrated configuration is adopted unchanged. The configured encryption mode will not be changed.	**10.5.0**

Table 1-9 Changed default settings

Function	Changed default settings / Impact of migration	Firmware (Added with firmware version)
[Network Address Translation] **Menu**: Network >> NAT >> Masquerading **Section**: Network Address Translation/IP Masquerading **Variable**: Outgoing on interface / From IP	In default settings, a table row/rule with the following variable values is added: – Outgoing on interface: External – From IP: 0.0.0.0/0 IP masquerading is thus activated for all packets that are routed from the internal network (LAN) to the external network (WAN) (LAN --> WAN). **Migration of older mGuard configurations** The values from the migrated configuration are adopted unchanged. A new table row/rule will not be added.	**10.3.0**
[Network Settings] **Menu**: Network >> Interfaces >> General **Section**: Network Mode **Variable**: Network mode	All devices of the new device generation are delivered in the network mode "Router". The external WAN interface receives its IP configuration via DHCP. In the default setting, however, the firewall prevents remote access to the device via the WAN interface. The device can be accessed from the LAN network via the internal LAN interface under the network address 192.168.1.1/24. Devices connected to the LAN interface can obtain their IP configuration via the DHCP server of the mGuard device. **Migration of older mGuard configurations** The values from the migrated configuration are adopted unchanged. The configured network mode will not be changed.	**10.3.0**

1.6.4 Changed variable values

In a few cases, variable values are no longer available on the new device platform and are replaced by other values.

Table 1-10 Changed variable values

Function	Changed variable values / Impact of migration	Firmware (Added with firmware version)
[OpenVPN Client] **Menu**: OpenVPN Client >> Connections >> Tunnel Settings **Section**: Data Encryption **Variable**: Encryption algorithm **GAI variable**: OPENVPN_CONNECTION.x.VPN_ENCRYPTION	**The "Blowfish" encryption algorithm is no longer supported.** A total of six AES encryption algorithms can be selected instead of the previous three: AES-128-GCM / AES-192-GCM / AES-256-GCM / AES-128-CBC / AES-192-CBC / AES-256-CBC **Migration of older mGuard configurations** After migrating a configuration from an older firmware version with the "Blowfish" encryption algorithm configured, the value of the variable is set to "AES-256-GCM". The following applies to all other algorithms: The value from the migrated configuration is adopted unchanged. The configured encryption algorithm will not be changed.	**10.5.0**

[Shell access]
Menu: Management >> System Settings >> Shell Access
Section: Maximum Number of Concurrent Sessions per Role
Variable: Admin / Netadmin / Audit
GAI variables:
SSH_ADMIN_LOGIN_ALLOWED_MAX
SSH_NETADMIN_LOGIN_ALLOWED_MAX
SSH_AUDIT_LOGIN_ALLOWED_MAX
	The "Maximum Number of Concurrent Sessions per Role" is limited to 10.
	Migration of older mGuard configurations
	– Applies to all configured values **<= 10**:
	  – The value from the migrated configuration is adopted unchanged. The configured maximum number of concurrent sessions per role will not be changed.
	– The following applies to configured values **> 10**:
	  – After the migration, the value of the variable "Maximum Number of Concurrent Sessions per Role" will be set to 10 in each case.
		10.5.0

Table 1-10 Changed variable values[...]

Function	Changed variable values / Impact of migration	Firmware (Added with firmware version)
[Multicast] **Menu**: Network >> Ethernet >> Multicast **Section**: General Multicast Configuration **Variable**: IGMP snooping	To ensure that data in "Static multicast groups" is forwarded correctly to the configured ports, "IGMP snooping" must be activated **Migration of older mGuard configurations** After a migration, the value of the variable will be changed as follows: – **Enabled**: If "Static Multicast Groups" are configured. – **Enabled**: If "IGMP snooping" is enabled in the old configuration. – **Deactivated**: If no "Static Multicast Groups" are configured and "IGMP snooping" is deactivated in the old configuration.	**10.3.0**

1.6.5 Modified designation of GAI variables

The designation of some GAI variables will be changed after the migration from mGuard 8.x to mGuard 10.3 or higher.

Table 1-11 Modified designations of GAI variables following migration

GAI variable (mGuard 8.x)	GAI variable (mGuard 10.3 or higher)
PORT_MIRROR_RECEIVER	MIRROR_RECEIVER
PHY_SETTING	SWITCHPORT
STATIC_MULTICAST_GROUP	MULTICAST_GROUP

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 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 documentation data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

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

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.com/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

111259_en_03
Item No. –03