Product change information

PCN No.:	CDN180070	Date:	06.11.2018
Products:	Communication technology – Industrial Ethernet – cyber security		

Order No.	Designation	As of product revision	Hardware/firmware, old	Hardware/firmware, new
2700642	FL MGUARD RS2000 TX/TX VPN	9	05/8.6.1	10/8.7.0
2702139	FL MGUARD RS2000 TX/TX-B	5	03/8.6.1	10/8.7.0
2701875	FL MGUARD RS2005 TX VPN	5	01/8.6.1	10/8.7.0
2700634	FL MGUARD RS4000 TX/TX	8	05/8.6.1	10/8.7.0
2200515	FL MGUARD RS4000 TX/TX VPN	8	05/8.6.1	10/8.7.0
2701876	FL MGUARD RS4004 TX/DTX	5	01/8.6.1	10/8.7.0
2701877	FL MGUARD RS4004 TX/DTX VPN	5	01/8.6.1	10/8.7.0
2700640	FL MGUARD SMART2	6	01/8.6.1	10/8.7.0
2700639	FL MGUARD SMART2 VPN	6	01/8.6.1	10/8.7.0
2702547	FL MGUARD CENTERPORT	2	00/8.6.1	10/8.7.0
2702259	FL MGUARD RS4000 TX/TX-P	4	02/8.6.1	10/8.7.0
2701275	FL MGUARD PCI4000 VPN	5	04/8.6.1	10/8.7.0
2701274	FL MGUARD PCI4000	5	04/8.6.1	10/8.7.0
2701278	FL MGUARD PCIE4000 VPN	5	04/8.6.1	10/8.7.0
2700197	FL MGUARD GT/GT	7	06/8.6.1	10/8.7.0
2700198	FL MGUARD GT/GT VPN	7	06/8.6.1	10/8.7.0
2702465	FL MGUARD RS4000 TX/TX VPN-M	3	02/8.6.1	10/8.7.0
2700968	FL MGUARD DELTA TX/TX VPN	3	02/8.6.1	10/8.7.0
2702863	FL MGUARD MGUARD CORE TX VPN	3	02/8.6.1	10/8.7.0
2700967	FL MGUARD DELTA TX/TX	8	07/8.6.1	10/8.7.0
2702831	FL MGUARD CORE TX VPN	3	01/8.6.1	10/8.7.0

Description of change		
□ Product appearance (fit)	□ Product geometry (form)	□ Product function (function)
Firmware and hardware changes		
Due to a supplier unexpectedly discontinuing a component, the flash memory installed in these products is to be replaced. The firmware will be adapted as a part of this replacement. Please refer to the attached change/release notes for detailed information on the changes. Devices with hardware version 10 or later can now only be operated with firmware version 8.7.0 or later. With respect to the technical data and functions documented in the data sheet, there are no changes from the previous revision. In order to ensure consistent availability of the above listed products, the changeover must, as an exception, be completed within a very short period of time.		

Expected initial delivery of the changed product(s)	As of now

mGuard Firmware

Version 8.7.0 - Release Notes

PHOENIX CONTACT Cyber Security AG
Richard-Willstätter-Strasse 6
12489 Berlin, Germany
Tel.: +49 30 921028-0
e-mail: contact-pxccs@phoenixcontact.com
http://www.phoenixcontact-cybersecurity.com

All information contained in this documentation is subject to change without previous notice. PHOENIX CONTACT Cyber Security AG offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes.
In addition, PHOENIX CONTACT Cyber Security AG is neither liable for errors in this documentation nor for damage, accidental or otherwise, caused in connection with delivery, output or use of these documents.

PHOENIX CONTACT Cyber Security AG Document Number: I18018_en_02

Vertical bars to the left mark significant changes in firmware 8.7.0 in comparison to the release notes for firmware version 8.6.1.

1 Product Description

1.1 Supported Hardware

The firmware can be operated on all currently available FL MGUARD and TC MGUARD hardware platforms, as well as on all legacy “Innominate Security Technologies AG” devices.

For detailed information about these platforms visit the PHOENIX CONTACT web shop at www.phoenixcontact.com and search for the product you are interested in.

1.2 Software Features

The firmware provides the functionality of a network firewall with support for VPN connections (license controlled) and other services.
The complete set of features is listed and described in detail within the user manual, which is available at the download section of the PHOENIX CONTACT web shop. Visit www.phoenixcontact.com and search for the product you are using.

1.3 Changes Since Previous Release

This minor firmware release provides these new features:

- Support for a higher capacity MEMPlug
- Support for a new flash memory type
- Improved flash memory handling in production
- QoS settings for VPN connections are no longer supported.

And fixes the following minor CVEs

- *OpenSSL*: CVE-2017-3737, CVE-2018-0739, CVE-2018-0737
- *Linux*: CVE-2017-18079, CVE-2017-16939, CVE-2017-17448, CVE-2017-17558, CVE-2017-17712, CVE-2018-5344, CVE-2018-6927, CVE-2018-1068, CVE-2018-18255, CVE-2018-10087, CVE-2018-10124, CVE-2018-1000199
-
- *cURL*: CVE-2018-1000005, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000300
- SSH: CVE-2016-10708
- ntp: CVE-2018-7182, CVE-2018-7184

1.4 Firmware installation and update

- The update for the first generation devices: “mGuard industrial RS”, “mGuard smart”, “mGuard pci”, “mGuard blade”, “EAGLE / mGuard”, “FL MGUARD RS” is not supported anymore since version 8.4.0. Please use the flash procedure to update the firmware of these devices.
- The Configuration Pull mechanism must be disabled during the time of the update.
- The “CRL checking” feature (verifying the validity of X.509 certificates with the help of a Certificate Revocation List) must be disabled.

1.5 Important update information

The devices listed in the following table and equipped with the given firmware version can be updated to firmware version 8.7.0. Please see chapter 5 on page 24 for a mapping of Innominate devices to Phoenix Contact devices.

All devices operating an older firmware can be updated by the flash procedure.

1.5.1 Obtaining the firmware and update files

The firmware and update files as well as a detailed update documentation are available at the download section of the PHOENIX CONTACT web shop. Visit www.phoenixcontact.com and search for the product you are using.

	FL MGUARD SMART2	FL MGUARD CORE TX	FL MGUARD PCI(E)4000	FL MGUARD DELTA TX/TX	FL MGUARD RSx000 TX/TX	FL MGUARD GT/GT	TC MGUARD RSx000 3G VPN	TC MGUARD RSx000 4G VPN	FL MGUARD RS2000 TX/TX-B	FL MGUARD RS4004 TX/DTX	FL MGUARD RS4000 TX/TX-P	FL MGUARD RS2005 TX VPN	FL MGUARD CENTERPORT
8.6.1	√	√	√	√	√	√	√	√	√	√	√	√	√

2 Version History

This chapter lists the changes between former versions of the mGuard firmware.

2.1 Changes made between 8.6.0 and 8.6.1

This release improves the functionality with the following changes:

- Errors during configuration pull of encrypted profiles and after boot have been removed.
- Specially crafted, but valid ICMP packets are not reported as malformed anymore.
- Certificate renewal by the CMP protocol now also works via a HTTP(S) proxy.
- The following minor CVEs were fixed
    - *OpenSSL*: CVE-2017-3735
    - *Linux*: CVE-2017-14106, CVE-2017-14991, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-15649, CVE-2017-16531, CVE-2017-16533, CVE-2017-16534, CVE-2017-16535, CVE-2017-12190
    - *busybox*: CVE-2017-16544
    - *cURL*: CVE-2017-1000099, CVE-2017-1000101

2.2 Changes made between 8.5.3 and 8.6.0

This minor firmware release provides these new features:

- The Certificate Management Protocol is supported for IPsec VPN certificates.
- A DHCP server is available on the DMZ port.
- A “system use notification” displayed on login screens may be configured.
- The Blade Controller hardware is supported again.
- Clicking Firewall log entries jumps to the Firewall rule.
- The following 3rd party software has been updated
    - Busybox, NTP, stunnel, trousers, quagga
- The SNMPv3 user name can be configured to something different than the default of “admin”.
- The autodetect stealth mode automatically discovers the DNS server used by the client and uses it, too.

It improves the functionality with the following changes:

- Resolved Web-Interface displaying issues:
    - Correct display of certificates without attributes.
    - MAC-Filter columns are hidden in Router-Mode.
    - The Management-IP is shown in multi stealth mode as external IP.
    - The Remote-Port-IDs in the LLDP table are shown correctly.
- HTTPS and SSH access to the virtual IP through Open VPN connections is possible.
- The SNMP MAU-Mib index is now identical to the *ifIndex* of the interface.
- The hardware addresses returned in the SNMP interface table are set to a reasonable value for interfaces without hardware layer.
- Pull-config credentials now may contain \`@\` and \`:\` characters.
- The SFP modules used in FL MGUARD GT/GT devices are enabled after

boot.

- The gaiconfig command does not fail during pullconfig of special profiles.

And it fixes the following minor CVEs:

- linux: CVE-2016-9178, CVE-2017-1000364, CVE-2017-1000365, CVE-2017-11473, CVE-2017-13693, CVE-2017-13694, CVE-2017-13695, CVE-2017-13715, CVE-2017-7533, CVE-2017-10661
- openvpn: CVE-2017-7520
- zlib: CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843

Based on results of a higly appreciated review executed by Oppida http://www.oppida.fr, we further improved the security of the firmware and the firmware update process.

2.3 Changes made between 8.5.2 and 8.5.3

This release does not change the behavior of the devices in any way, but only fixes a manufacturing issue.

2.4 Changes made between 8.5.1 and 8.5.2

This release fixes the security issue CVE-2013-6466 by disabling IKEv2 packet handling.

2.5 Changes made between 8.5.0 and 8.5.1

- The Mem Plug handling of the FL MGUARD GT/GT has been improved.
- The GPS Position is now correctly shown after boot.
- The dynamic timeout of User Firewall rules inside Ipsec connections, triggered via the external interface is now calculated correctly.
- Changing a password right before rebooting the device now works reliably.
- The mGuard correctly handles VLAN tagged ARP requests for NATed IP addresses for remote VPN networks.
- The configuration-pull mechanism has been hardened to work reliably over low-speed/high latency connections.
- The LLDP peer detection and display has been improved.
- This release fixes many minor usability quirks and issues in the WebUI.
- The following minor security issues have been fixed:
  - linux: CVE-2015-1350 CVE-2017-7184 CVE-2017-7308 CVE-2017-8890 CVE-2017-2671
  - curl: CVE-2017-7407
  - openvpn: CVE-2017-7479
  - ntp: CVE-2017-6458

2.6 Changes made between 8.4.2 and 8.5.0

- The COM Server functionality has been extended to also support 7-bit serial lines.
- State changes of the CMD inputs can trigger an SNMP trap.
- OpenVPN supports the TLS-Auth mechanism and local 1:1 NAT.
- The pathfinder client functionality has been extended to support the proxy authentication mechanisms: BasicAuth, NTLM and Digest.
- FL MGUARD RS2000 devices support configurable firewall rules.
- FL MGUARD RS4000 TX/TX-P devices support 250 VPN connections,

Firewall and VPN redundancy and CIFS Integrity Monitoring without installing additional licenses.

- The AV Scan-Connector functionality has been removed.
- If no IPsec VPN connection is configured, UDP port 500 is not accessible.
- CRL upload via WebUI works correctly for IPsec.
- The DNS lookup behavior for DNS based firewall has been improved.
- The parallel use of PSK and X.509 authorized IPsec connections has been improved.
- OSPF uses the correct metric for GRE tunnel and does not stop propagating IPsec remote networks after reconfiguration.
- GPS based time synchronisation works correctly in different time zones.
- FTP via port-forwarding also works for other than the default port 21.
- The PPPoE MSS handling has been improved with this release.
- The update to firmware version 8.5.0 is possible in mobile network CDMA mode with configured SIM cards.
- The Verizon registration mechanism and the sending of text messages in CDMA mode have been fixed.
- The following minor security issues have been fixed:
  - uClibC: CVE-2016-2224 CVE-2016-2225
  - Linux: CVE-2016-8645 CVE-2016-8655 CVE-2016-6213 CVE-2016-6786 CVE-2016-6787 CVE-2016-9793 CVE-2016-9806 CVE-2014-9914 CVE-2017-5970 CVE-2016-10200 CVE-2015-8962 CVE-2015-8964 CVE-2016-7910 CVE-2016-7915 CVE-2016-7916 CVE-2015-8709 CVE-2016-4997
  - NTP: CVE-2015-7848 CVE-2016-7426 CVE-2016-7427 CVE-2016-7428 CVE-2016-7431 CVE-2016-7433
  - OpenSSH: CVE-2016-10011 CVE-2016-6210

2.7 Changes made between 8.4.1 and 8.4.2

- This release correctly handles Firewall Rule Records that reference other Firewall Rule Records.
- The upload of Machine Certificates via the Web UI has been fixed with this release.
- The options and actions for managing the ECS are now visible in the Web UI of FL MGUARD PCI2 and FL MGUARD PCIe2 cards.
- The serial line options are now configurable on rs2000 devices on the Web UI.
- The FL MGUARD GT/GT now supports two 100MBit Fiber modules correctly.
- This firmware correctly replies to ARP requests for 1:1 NATed IP addresses in redundancy mode.

2.8 Changes made between 8.4.0 and 8.4.1

This patch release fixes two update issues. The functionality of the firmware itself does not change since the last release.

- Updating from version 7 to version 8.4.0 resulted in a scrambled WebUI. The update however succeeded.
- Updating to version 8.4.0 did reset the password of the “admin” user to the default value. Customers who updated devices to version 8.4.0 are strongly advised to change the password of the user “admin”.

2.9 Changes made between 8.3.1 and 8.4.0

- The Mobile engine sub-system has been extended for more flexibility and now supports the new mGuard LTE devices:
  - TC MGUARD RS4000 4G VPN
  - TC MGUARD RS2000 4G VPN
- The configuration management and web interface have been re-designed.
  - Errors are now displayed immediately on value change.
  - All WebUI actions (buttons) may now be executed also via SNMP and command line.
- With this release DNS host names can be used for firewall source or destination IPs via the IP Group feature.
- The SNMP MIB has been cleaned up. Especially the objects mGuardUpdateInitiate, mGuardUpdateFilename and mGuardAction have been replaced by other MIB objects.
- The recovery procedure no longer modifies the current configuration, but instead saves it as configuration profile and then restores the factory default.
- Modbus TCP filtering is supported by this release.
- The current values (IP, Mask, Gateway) of the external interface can be queried via command line.
- CMD button/switch activities are now logged.
- A Firmware update can be triggered via command line and SNMP
- This firmware supports to configure a token to reboot the device via a Text Message (SMS)
- The NTP server access can now be configured for other interfaces than the internal one with access rules like those for HTTPS or SSH access.
- The CDMA functionality now automatically performs a registration.
- The following security vulnerabilities have been addressed in this release:
  - OpenSSL: CVE-2016-2107 CVE-2016-2109 CVE-2016-0705 CVE-2016-0797 CVE-2016-0799 CVE-2015-3197 CVE-2016-2182 CVE-2016-6302
  - linux: CVE-2016-4482 CVE-2016-4486 CVE-2016-4805 CVE-2015-1350 CVE-2015-2686 CVE-2015-4177 CVE-2015-8830 CVE-2016-3138 CVE-2015-8816 CVE-2015-8844 CVE-2015-8845 CVE-2016-2069 CVE-2016-2550 CVE-2016-2847 CVE-2016-3134 CVE-2016-3156 CVE-2016-3672 CVE-2013-4312 CVE-2016-0723 CVE-2016-0821 CVE-2016-4997 CVE-2016-4998 CVE-2014-7145 CVE-2014-9870 CVE-2014-9888 CVE-2014-9900 CVE-2015-8944 CVE-2016-5696 CVE-2016-7117 CVE-2015-3288 CVE-2016-6828 CVE-2016-5195
  - curl: CVE-2016-0755 CVE-2016-5419 CVE-2016-5420 CVE-2016-5421
  - openswan: CVE-2016-5361
  - ntp: CVE-2016-4953 CVE-2016-4954 CVE-2016-4955
  - openSSH: CVE-2016-6515
  - c-ares: CVE-2016-5180

2.10 Changes made between 8.3.0 and 8.3.1

- A malformed IP address in the SNMP VPN State Change Trap has been corrected.
- The Hub & Spoke with VPN 1:1 NAT functionality has been fixed.
- The IPSec license limit counter now accepts rekeying.
- Several issues with starting and stopping IPSec connections have been fixed.
- This release fixes Centerport related OSPF and Pathfinder issues.
- WebUI issues regarding the IPSec and netadmin configuration have been

fixed.

- This release always uses A-GPS if GPS is enabled to avoid connection issues with some 3G Providers.
- NTP time synchronization now works reliable in case of interface changes.
- The following security vulnerabilities have been addressed in this release:
  - NTP: CVE-2015-7871
  - Linux: CVE-2015-7799, CVE-2015-5707, CVE-2013-7446, CVE-2015-8543, CVE-2015-8569
  - OpenSSL: CVE-2015-3194, CVE-2015-3195, CVE-2015-3196

2.11 Changes made between 8.1.8 and 8.3.0

- Implemented support for GRE.
- Implemented support for dynamic routing using OSPF.
- Firewall rules can now be described using named groups of IPs/ports.
- Configuration profiles can be loaded in the Web UI for editing them first, instead of applying them at once.
- Support for OpenVPN connections as client.
- IPsec VPN connections now support iOS clients.
- VPN license counts are now dynamically shown in the Web UI.
- Support for the server side of the mSVC PathFinder feature.
- Timeout for VPN connections established on demand.
- The CIFS IM feature now supports hostnames for configuring the shares.
- A new access scan feature was added to CIFS IM.
- Logs generated during CIFS IM scans now contain the whole scanner history instead of just the result of the last scan.
- Various issues concerning Verizon telephony/CDMA 2000 have been fixed.
- The following security vulnerabilities have been addressed in this release:
  - CVE-2015-5364 / CVE-2015-5366
  - CVE-2015-5621
  - CVE-2014-8104
- The tunnel group functionality is available as of firmware version 8.3 with all VPN licenses. For this reason, the 250 tunnel group license thus has become obsolete. As a consequence, the counting method will change: Instead of counting the number of tunnels, the devices, in between the tunnels will be established, will be counted. Therefore, the 250 tunnel group license will be discontinued.

2.12 Changes made between 8.1.7 and 8.1.8

- Added support for some RS4000/RS2000 hardware revisions.

2.13 Changes made between 8.1.6 and 8.1.7

- This release fixes VPN security issue CVE-2015-3966 which allows temporary denial of service attacks to a VPN responder during IPsec SA (Phase II) establishment, but only after the authentication with a X.509 certificate or pre-shared secret key was accomplished. Please also see our Security Advisory at the PHOENIX CONTACT web shop.
- A problem with the IP number format used in the SNMP VPNStateChange trap has been fixed.
- The combination of 1:1 NAT and IP Masquerading with router-dhcp mode has been fixed in this release.
- The parameters of a manually uploaded CRL are now correctly displayed in

the web GUI.
- The GPS time synchronization on 3G devices has been fixed to synchronize the internal realtime clock of the mGuard.
- The reliability of devices with a full filesystem and during a sudden power interruption has been further improved in this release.

2.14 Changes made between 8.1.5 and 8.1.6

- VPN transport connections in autodetect stealth mode are now properly established if the remote gateway is given as DNS-name.
- Configurations with many connections to remote gateways given as DNS-names will now establish all connections.
- The DPD negotiation between an mGuard device and Cisco devices has been fixed for this release.
- This release fixes the VPN reestablishment after reboot on the initiating side. With previous releases it could happen that a VPN connection was displayed as established, but no traffic traversed the tunnel.
- In stealth mode all IP packets accepted by the firewall will now pass the device.
- The remote administration of mGuard devices via VPN now works with all MTU settings.
- The GPS time synchronization on 3G devices got improved and hardened to ignore inconsistent time information.
- Transfering huge OPC data (> 100Kb) with the OPC inspector enabled now works if the OPC sanity-check is disabled.
- The USB ACA21 external configuration storage is now properly recognized on Eagle-mGuard devices.
- This release fixes the remote access via VPN if several connections with multiple tunnels are configured.

2.15 Changes made between 8.1.4 and 8.1.5

- This release fixes NTP security issue CVE-2014-9295 which allows remote code execution with reduced privileges. Please also see our Security Advisory at the PHOENIX CONTACT web shop.
- It fixes communication failure due to dynamically opened ports under certain conditions not being allowed by the OPC Inspector
- It improves data transfer speed through VPN on centerport class devices

2.16 Changes made between 8.1.3 and 8.1.4

This patch release supports three new hardware variants, fixes two security issues and some minor functionality issues:

- The new hardware devices mGuard rs2000 5TX/TX, rs4000 4TX/TX and rs4000 TX/TX PA are supported with this release.
- This release fixes the OpenVPN security issue CVE-2014-8104 which allows to attack the mGuard IPSec TCP encapsulation. Please also see our Security Advisory at the PHOENIX CONTACT web shop.
- It also fixes a privilege escalation issue for the admin user (CVE-2014-9193). Please also see our Security Advisory at the PHOENIX CONTACT web shop.
- It incorporates the fix for the PPPD integer overflow issue tracked as CVE-2014-3158, even though the issue cannot be used to attack the mGuard.
- The recovery procedure on 3G based devices now correctly sets the local IP to 192.168.1.1.

- Remote VPN masquerading by the internal mGuard IP is now fully supported.
- This release improves the memory management for many VPN connections on legacy devices.
- It improves the storage of the SNMPv3 credentials.
- The reliability of devices with a full filesystem and during a sudden power interruption got improved in this release.

2.17 Changes made between 8.1.2 and 8.1.3

This patch release fixes a compatibility issue with the Innominate mGuard device manager (mdm) version 1.4:

- A device configuration created with mdm for devices with firmware version 8.1.0, 8.1.1 or 8.1.2 cannot be applied if the device version in mdm is set to 7.4 or below.

2.18 Changes made between 8.1.1 and 8.1.2

This patch release contains bug fixes observed in version 8.1.0 and 8.1.1:

- It re-enables local 1:1 NAT in a Hub&Spoke VPN scenario.
- It increases the partition size of centerport devices.
- It fixes and re-enables the redundancy feature (memory issue and accessability after interface reconfiguration)
- It fixes issues with importing and saving configuration profiles.
- The following Release-Notes issues got fixed:
  - Issue “Expected conntrack entries are not deleted” (Ref. 12227)
  - Issue “The DMZ port of the centerport2 device is not usable” (Ref. 12318)
  - Issue “Serial console over USB not working on smart^2” (Ref. 11995)

2.19 Changes made between 8.1.0 and 8.1.1

This release fixes the OpenSSL security issue CVE-2014-0224. The affected mGuard firmware versions are 8.0.0, 8.0.1, 8.0.2 and 8.1.0.

It is strongly recommended to update all devices operating with the firmware version 8.0.0, 8.0.1, 8.0.2 or 8.1.0.

After the update the device should be rebooted. Please also see our Security Advisory at the PHOENIX CONTACT web shop.

2.20 Changes made between 8.0.2 and 8.1.0

- The new mGuard OPC Inspector enables firewall filtering and NAT on OPC Classic traffic.
- This release supports several different Dynamic DNS providers and configurable dyndns.com-compatible providers.
- It supports mapping multiple internal network segments into a single VPN channel using 1:1 NAT.
- The list of currently logged in Firewall users is now updated dynamically in the Web UI. Changes to Firewall Rules affecting logged in users are now applied immediately without the need for users to log in again.
- Firewall Rule Records and VPN Connections can now be triggered by up to three external switches, the command line interface, the Web interface or a CGI URL.
- Supervising VPN Connections and Firewall Rule Records using a hardware output can now be configured independently of a controlling switch or button.
- The User-Firewall and switchable Firewall Rule Records are now usable inside VPN connections.

- This release supports querying different states via the CGI interface like CIFS Integrity Monitoring results, Firewall Rule Record states, VPN states, ECS and Modem states.
- The CGI interface now also allows to perform actions like starting and stopping CIFS scans or Firewall Rule Records, as well as logging out Firewall users.

2.21 Changes made between 8.0.1 and 8.0.2

- This release fixes the OpenSSL security issue CVE-2014-0160 known as Heartbleed vulnerability. The affected mGuard firmware versions are 8.0.0 and 8.0.1. All other mGuard software releases are not affected. Please also see our Security Advisory at the PHOENIX CONTACT web shop.

2.22 Changes made between 7.6.2 and 8.0.1

- A short abstract of the software features supported on the new mGuard rs2000 4TX/3G and mGuard rs4000 4TX/3G/TX VPN devices:
  - Mobile Network connection (2G/3G technology) for Europe
  - Sending and receiving SMS
  - Positioning System (GPS).
  - Configuration of the managed switch
  - Multicast support
  - Additional Network port (DMZ) (rs4000 4TX/3G/TX VPN only)
- This release supports sending E-Mails triggered by configurable events.
- It extends the options to temporarily enable VPN connections as there are SMS, command-line and Web UI.
- It provides an RFC2217 compliant TCP to Serial line service.
- System events are now updated automatically in the Web UI without the need to refresh the page.
- It improves the CIFS-IM and CIFS-AV feature in combination with Windows 95/98 hosts.
- It fixes the QoS feature.

2.23 Changes made between 7.6.1 and 7.6.2

- This release fixes TCP encapsulated VPN connections in configurations where the redundancy feature is enabled.
- ARP replies for VPN remote networks on the external interface in multi stealth mode are suppressed with this release.
- All IPSec SAs are now deleted in case of shutting down a connection because of a dead peer detection (DPD).
- This release improves reestablishment of VPN connections over unstable lines like an overloaded WLAN.
- It also fixes an issue that broke the CIFS feature during an update on mGuard smart, pci, blade, delta and EAGLE mGuard.
- A rare, unexpected reboot under heavy load is fixed in this release.
- Management access via the internal IP through a VPN tunnel works correctly now when the VPN network is a subnet of the local network.
- TCP Encapsulation and any other HTTP traffic initiated by the mGuard using a Sophos Proxy with NTLM authentication is now supported.
- This release fixes failures of Hub&Spoke triggered by configuration changes of the involved VPN connections.
- Syslog messages to a remote Syslog server are now sent through the

appropriate VPN connection, even with local 1:1 NAT enabled inside the VPN tunnel.

2.24 Changes made between 7.6.0 and 7.6.1

- Innominate mGuard blade devices did not function properly with the Innominate mGuard Firmware version 7.6.0. After an update the previous configuration was lost on blade devices. The blade controller did not show the blade menu in the web interface anymore. Affected devices are:
  - mGuard blade /533 // HW-104050
  - mGuard blade /266 // HW-104020
  - mGuard bladebase // HW-104500
  - mGuard bladepack /533 // HW-104850
  - mGuard bladepack /266 // HW-104820

  This is fixed in this release.

2.25 Changes made between 7.5.0 and 7.6.0

- The DPD (Dead-Peer-Detection) behavior and the connection-management of the VPN IPsec service have been improved.
- It now supports TPM (Trusted Platform Module) encrypted profiles and ECS storage on the platforms mGuard rs2000, mGuard rs4000, mGuard pci² SD, mGuard pcie² SD and mGuard centerport.
- The global Firewall selector now allows to permit ping (ICMP echo) next to allowing or rejecting all traffic.

2.26 Changes made between 7.4.1 and 7.5.0

- Redundancy in stealth mode “multiple clients” is supported with this release.
- A system-wide configuration option controls the conntrack table flush during firewall reconfiguration.
- The new setting Redundancy Failover Latency configures a grace period that must elapse, before a connectivity failure will take effect.
- It is now possible to configure a NAS identifier for RADIUS authentication.
- The FAULT LED and contact can now be configured to also supervise the configured temperature range and the redundancy connectivity check state.
- A NET-BIOS name can be configured to import network shares exported by Microsoft Windows 98 machines.
- Configuration profiles that can't be applied are now rejected during upload with an appropriate error message.
- Scanning of Microsoft Windows 98 shares was improved.
- Added function for renewing RSA keys via GUI and command line.
- RSA keys newly generated when flashing or using the new function have a modulus of 2048bit.
- The IP for incoming VPN connections can be configured now.

2.27 Changes made between 7.4.0 and 7.4.1

- It fixes an issue with “IKE Fragmentation” which could cause failure (hang/restart) of the IPsec VPN subsystem.
- It fixes memory leaks and connection stalls triggered by remote peers being located behind NAT gateways.
- It fixes an issue with administrative access to the mGuard via VPN failing if VPN is activated via CMD button or switch.
- It fixes the issue “Remote access through VPN” with administrative access to

the mGuard via VPN failing if the default route is via VPN.
- It fixes an issue with a VPN tunnel not being re-established after reboot if the CMD switch is still “enabled”.
- It fixes an issue with very large numbers of port forwarding rules (>1000).
- It fixes the issue “Many IPsec SAs established”: IPsec SAs are no longer unnecessarily generated with DynDNS monitoring enabled.
- It re-enables the “user” account to activate VPN tunnels using “nph-vpn.cgi” interface.
- It supports ICMP echo requests to the internal administrative IP of the mGuard through VPN tunnels with NAT settings enabled.
- It supports use of CA certificates with BMPSTRING subjects.
- It supports fast DHCP renewal after link loss on the external interface in Router/DHCP mode.
- It improves compatibility of NTLM proxy authentication with MS Forefront
- It improves detection of topology changes in autodetect Stealth Mode.

2.28 Changes made between 7.3.1 and 7.4.0

- Version 7.4.0 supports the new hardware platforms mGuard rs2000 and mGuard rs4000.
- It eases the password rollover for a redundancy pair.
- It allows to configure session limits for authenticated SSH sessions.
- The firewall in version 7.4.0 allows to filter or forward GRE protocol packets.
- It supports remote masquerading and improves the possible combinations of masquerading and 1:1 NAT through VPN connections.
- NAT-T handling with VPN redundancy is improved.
- The design of the GUI has been improved in this version.
- Enabling and disabling TCP encapsulated VPN connections by the CMD contact has been fixed.
- Version 7.4.0 fixes authentication failures of T-Online DSL connections with account numbers less than 24 digits which require the '#' sign.

2.29 Changes made between 7.2.1 and 7.3.1

(Version 7.3.0 was released for a limited set of platforms.)

- Devices with less than 64 MB of RAM are not supported anymore by firmware version 7.3.1.
- Version 7.3.1 revives the license controlled firewall redundancy feature for the network mode “Router”. For the mGuard centerport it even supports an improved fail-over switching time of one second at most (optionally longer).
- It adds the license controlled VPN redundancy feature.
- It adds support for the SHA2 algorithms SHA-256, SHA-384, and SHA-512 for VPN connections, see also issues “Interoperability of SHA2 and IPsec”.
- It adds support for preference lists of algorithms to use for VPN connections.
- It allows to configure a traffic limit for the lifetime of IPsec Security Associations (IPsec SAs).
- It adds the feature to use RADIUS servers for authentication of users of the web interface and the Command Line Interface. The RADIUS servers may optionally be reachable through VPN channels.
- It allows to perform the online downloads of future firmware versions through a VPN channel.
- It adds a configuration option which allows it to download CRLs through VPN channels.

- It improves the logging of administrative sessions and important administrative actions.
- It adds a configuration option which allows to disable the ARP replies at the external interface for 1:1 NAT scenarios.
- It adds optional Hub & Spoke support between a SEC-Stick connection and VPN connections.
- It fixes the issue “Remote access ports not configurable for access via VPN”.
- It fixes the issue “Features not supported with firmware version 7.2.1”.
- It avoids unexpected configuration changes of the blade controller.
- The changing of the password for the CIFS AV Scan Connector no longer requires a reboot.
- It improves use of several L2TP connections at the same time.
- It improves establishment of TCP encapsulated VPN connections after reboot.
- It improves the logging for TCP encapsulated VPN connections.
- It raises the limit for the number of port-forwardings per SEC-Stick connection.
- It fixes logging of SEC-Stick access.
- It adds support for enabling persistent logging for TCP encapsulated VPN connections.
- It closes the potential security issues CVE-2010-3301, CVE-2010-2240, CVE-2010-0405, CVE-2010-3301, CVE-2010-4258, CVE-2010-3848, CVE-2010-3849, and CVE-2010-3850. None of which affects the mGuard in a way which requires a user to take action immediately.

3 Identified Issues and Workarounds

GPS on 3G mGuard Devices

Synopsis	GPS positioning data remains invalid with a very outdated local clock.
Symptom	The GPS module is not able to acquire a fix and the current location can not be determined.
Workaround / Action	Set the mGuard's clock to at least the approximate time or enable NTP.
Reference	17647

Redundancy

Synopsis	Master and backup server fail to synchronize encrypted over the dedicated interface (Centerport only).
Symptom	The failover time for high availability redundancy systems may be higher in this release and existing connections may be re-established after a failover if the state synchronization is configured to use the dedicated interface and to encrypt the traffic.
Workaround / Action	Disable encryption if synchronization is configured to use the dedicated interface.
Reference	17380

OpenVPN non-matching algorithms

Synopsis	An OpenVPN tunnel is shown as established even if the crypto settings don’t match the server.
Symptom	An OpenVPN tunnel is shown as established, but no traffic passes the tunnel.
Workaround / Action	Configure the same crypto and hash algorithms on both peers.
Reference	15356

PSK + Aggressive Mode is insecure

Synopsis	The IKE Aggressive Mode protocol has known flaws in combination with PSK. This is a protocol weakness and not an mGuard weakness.
Symptom	VPN Connections may be decrypted and modified by unauthorized entities.
Workaround / Action	Avoid using PSK+Aggressive Mode. The use of certificates with Main Mode is strongly recommended.
Reference	12168

PSK + Aggressive mode with DH groups

Synopsis	Aggressive Mode VPN connection initiators behind the same NAT gateway must use the same, fixed DH group. If there are several Aggressive Mode connections to which the mGuard is the responder, it will be necessary to set the DH group on the responder to "all algorithms". If a fixed DH group is used on the responder, it must be the same group for all Aggressive Mode connections.
Symptom	Aggressive Mode connections with different DH groups not matching the restrictions above are not established.
Workaround / Action	The use of certificates with Main Mode is strongly recommended.
Reference	12051

Redundancy internal link detection devices with switch

Synopsis	The setting “Ethernet link detection only” for the redundancy connectivity checks of the internal interface on devices with internal switch always reports an established link even without connectivity.
Symptom	A link failure on one of the switch ports LAN1 - LAN4 is not detected.
Workaround / Action	Use ICMP echo request targets for connectivity checks of the internal interface on devices with internal switch.
Reference	10959

VLAN in stealth mode with redundancy enabled

Synopsis	When operating a device in stealth mode with redundancy and VLAN enabled may unexpectedly block some traffic.
Symptom	Some VLAN traffic will be blocked unexpectedly.
Workaround / Action	None.
Reference	10425

Flow control does not send PAUSE frames

Synopsis	In case of enabled and negotiated Flow-Control, the device will not send PAUSE frames in case of congestion.
Symptom	The device will drop more packets as expected even with Flow-Control enabled on this port.
Workaround / Action	None.
Reference	10986

Radius authentication over VPN with redundancy

Synopsis	Radius authentication over VPN from the passive device in a redundancy setup over the VPN connection of the active device does not work.
Symptom	Login with radius authentication on a passive device in a redundancy setup does not work if the radius server is only reachable via a VPN tunnel of the active device.
Workaround / Action	None.
Reference	10913

Mounting Microsoft Windows 98 shares

Synopsis	A once correctly configured NetBIOS name (RFC1001) for Microsoft Windows 98 shares will stay active until a reboot.
Symptom	When mounting several shares from the same Microsoft Windows 98 host all shares can be mounted successfully as long as the correct NetBIOS name was supplied at least once for at least one share.
Workaround / Action	Reboot the mGuard after reconfiguration
Reference	9762

Scanning of Windows shares may fail

Synopsis	The scan report may not be created when the report-share is a subdirectory of the share to be scanned.
Symptom	The scan report “integrity-check-log.txt” is not updated or created. The check finishes with the following status message: *Last check aborted with error code 1. The process failed due to an unforeseen condition, please consult the logs.* This effect depends on the version of the Microsoft Windows operating system.
Workaround / Action	Use a different share for the report/ database, which is not a subdirectory of the share to be scanned on the Windows host.
Reference	9651

CIFS IM pattern matching is now case insensitive

Synopsis	The filename pattern matching functionality of the CIFS Integrity Monitoring is now case-insensitive.
Symptom	Filenames containing uppercase letters in their extension are now recognized and will be shown as unexpected files after an update from version 7.4.1 or below.
Workaround / Action	Regenerate the CIFS IM database.
Reference	9432

ICMP failure with transport VPN in Stealth Mode with SNMP

Synopsis	ICMP echo requests are not answered through a transport mode VPN connection if the device is in stealth mode and SNMP is activated
Symptom	From a remote peer a client protected by an mGuard shall be pinged through a transport mode VPN. The tunnel is up and other traffic succeeds but ICMP echo requests are not answered. This problem only occurs if SNMP is enabled on the mGuard.
Workaround / Action	None.

Administrative Access From Moved Client in Single Stealth

Synopsis	In single stealth auto detect and static modes the client cannot access the mGuard if the client was moved to the extern (unprotected) side.
Symptom	In single stealth mode the mGuard records the client computer's IP and MAC address at the internal (protected) interface and uses it to direct traffic to the client. If the client computer is moved to the extern (unprotected) side and tries to communicate with the mGuard (even using the management IP address) communication is not possible, as the mGuard still tries to direct the traffic to the internal (protected) side.
Workaround / Action	Do connect another client computer to the internal (protected) interface so that mGuard can learn new addresses for IP and MAC or reboot the mGuard.

Particular self signed certificates not accepted as HTTPS client certificates

Synopsis	Self signed certificates can be configured as acceptable certificates “per definition” if they are used by browsers to authenticate administrative access to the mGuard's GUI. Nonetheless such certificates are rejected if the command “`openssl verify -CAfile cert.crt -purpose sslclient cert.crt`” would verify them as invalid.
Symptom	Access is rejected by the mGuard, although the configured self-signed certificate is used by the browser.
Workaround / Action	Create a different certificate having an appropriate or no key usage extension. For hints about which key usage extensions are missing, please check the output of the command “`openssl verify -issuer_checks -CAfile cert.crt -purpose sslclient cert.crt`“

Changed Flood Protection Settings delayed for VPN connections

Synopsis	When settings are changed within the menu “Network Security / DOS Protection”, these do not become effective for VPN connections immediately, while they do for the incoming and outgoing firewall. The changed settings become effective as soon as VPN connections are restarted.
Symptom	Changed flood protection settings have no effect for established VPN connections.
Workaround / Action	Restart the VPN connections or reboot the device.

Reconfiguration of VLAN ID not noticed by DHCP server

Synopsis	If an mGuard is operated in *stealth mode* with a *DHCP* server on the *internal interface,* a reconfiguration of the VLAN ID is not noticed by the DHCP server. The DHCP server continues to use the old VLAN ID.
Symptom	After reconfiguration of the VLAN ID the internal DHCP server does no longer respond to requests from clients.
Workaround / Action	Please disable and re-enable the DHCP server or restart the mGuard after such a configuration change.

Identical VPN connections just with different machine cert do no work

Synopsis	If several VPN connections (at least two) are configured to use the same settings except for the local machine certificate and if they use a CA-certificate to authenticate remote sites the mGuard might assign incoming connections the wrong way.
Symptom	All incoming VPN connections are always assigned to the first VPN connection which matches the credentials provided by the peer. Thus the mGuard always uses the first machine certificate to authenticate itself to the remote side – even if the remote side is configured to accept the other machine certificate only. The connection attempt fails.
Workaround / Action	Please distinguish your remote sites by issuing certificates from a different (sub-)certification authority for them. A different (sub-)CA-certificate is required per VPN connection. Sites to connect to the same connection must use certificates issued by the same CA-Certificate.

Transport mode VPN with %any as gateway not supported in stealth mode

Synopsis	For any stealth mode operation the mGuard does not support the a VPN connection in transport mode with %any as gateway and CA authentication of several peers at once. Such scenarios do work only if just one peer connects.
Symptom	If more than one peer establishes a connection to the same transport mode VPN connection of the mGuard operating in stealth mode then packets might not get through the channel.
Workaround / action	Please use tunnel mode VPN connections.

IPsec VPN with %any as gateway and PSK

Synopsis	IPsec PSK authentication with %any requires identical PSK for all connections
Symptom	Failures to establich all IPsec VPN connections If more than one PSK authenticated IPsec connection with %any is configured with different PSKs.
Workaround / action	We strongly recommend to use X.509 certificate authentication for security reasons. If PSK must be used, all PSK+%any connections must use the same PSK.
Reference	17488

Remote access ports not configurable for stealth(multi) with VLAN

Synopsis	If an mGuard is operated in network mode “stealth” with “multiple clients” and has a VLAN ID configured for its management IP then HTTPS/SSH/SNMP remote access to that IP does only work if default ports are configured (443/22/161).
Symptom	If other than the default remote access ports are configured, no connection can be established to the management IP on those ports. The mGuard does not respond.
Workaround / Action	Do not change the default ports.

Interoperability of SHA2 and IPsec

Synopsis	When configured to use a SHA2 (SHA-256, SHA-384, and SHA-512) algorithm for use with IPsec the mGuard is not interoperable with some other vendors' implementations of IPsec in combination with SHA2.
Symptom	If the other VPN appliance also supports SHA2 and is correctly configured the ISAKMP SA and the IPsec SA are established. But no traffic is passed through the VPN tunnel. The mGuard rejects to decrypt traffic from the peer and vice versa. The reason is that the mGuard and the peer do not agree about the number of bits to which to reduce the output of the SHA2 algorithms.
Workaround / Action	Please use an mGuard at both sides or do not use SHA2 for IPsec if interoperability with the particular vendors is required.
Reference	8510

UDP EXT2 probes in autodetect stealth mode do not work

Synopsis	UDP based probes like IKE-Ping or DNS-Ping do not recognize a functional external network in autodetect stealth mode. The ICMP-ping however does.
Symptom	Supervising temporary modem startup in autodetect stealth mode with only IKE- or DNS-ping will never shut down the modem, even if the external RJ45 connection is functional.
Workaround / Action	Use ICMP-ping for EXT2 probes in autodetect stealth mode.
Reference	14445

No PCI driver mode support available

Synopsis	PCI driver mode is no longer supported since version 8.0.0 of the mGuard firmware.
Symptom	None.
Workaround / Action	None.
Reference	14354

Connection is not started automatically when a license becomes available

Synopsis	When the VPN license pool is exhausted and a VPN connection terminates, thus making a license slot available, the connections that could not be started due to the license restrictions are not started automatically.
Symptom	A VPN connection which is not started due to license restrictions is not started automatically once a license slot becomes available.
Workaround / Action	Start the VPN connection manually.
Reference	15398

VPN restrictions in stealth mode

Synopsis	In stealth mode, a configuration in which the remote network in VPN is a subnet of of the network in which the mGuard is located is not supported.
Symptom	The VPN connection is established, but the packets would not reach the expected hosts.
Workaround / Action	None.
Reference	14777

Signal strength in CDMA mode

Synopsis	The display of the signal strength in the Web UI and the LEDs may be wrong in CDMA mode.
Symptom	When a mobile connection using CDMA is configured to use both 1xRTT (2G) and EvDO (3G), the displayed signal strength may be that of the 2G network even if 3G is used.
Workaround / Action	None.
Reference	17085

Signal Level on RS2000 AT&T (4G or 3G/4G) is switching between 1 and 100%

Synopsis	When a 4G connection is established the signal level indicator toggles between 1% and 100%. no accurate signal level is reported.
Symptom	In 4G mode the signal strength indicator jumps from 1% to 100% and back when a 4G connection is established.
Workaround / Action	None.
Reference	MG8-416

OTA doesn't work on AT&T after manually setting the APN

Synopsis	When the APN was manually configured on AT&T devices, OTA updates to the APN will no longer reliably work.
Symptom	The APN is not updated on AT&T devices if manually set to another value
Workaround / action	Manually set the correct value.
Reference	MG8-475

Memory consumption on legacy devices

Synopsis	A higher memory consumption because of new features and functionality in the 8.4 firmware may lead to an exhaustion of the memory on legacy devices based on the IXP4xx CPU.
Symptom	The device reboots unexpectedly and/or reports out of memory errors in the log.
Workaround / Action	Reduce the number of enabled services, especially SNMP and CIFS.
Reference	17285

4 Known Restrictions

- The Safari browser needs to have all sub-CA certificates installed in its trust store if they are used to authenticate for administrative access to the mGuard via X.509 certificate.
- The same browser instance cannot be used to administrate the mGuard with X.509 authentication and to login into the mGuard's user firewall at the same time.
- Configuration of the mGuard via its web interface, via its Command Line Interface (shell access), and via SNMP must not happen concurrently. Concurrent configuration operations via different access methods may cause unexpected results.
- The external DHCP server of the mGuard cannot be used in multi stealth mode if a VLAN ID is assigned to the management IP.

5 mGuard Product Mapping

This chapter itemizes all mGuard products for this software release.

5.1 Platform MGUARD2

This platform includes the following devices:

PHOENIX CONTACT Devices		*Innominate Devices*	
2700642	FL MGUARD RS2000 TX/TX VPN	HW-108010	mGuard rs2000 TX/TX VPN
2701875	FL MGUARD RS2005 TX VPN	HW-108020	mGuard rs2000 5TX/TX VPN
2903441	TC MGUARD RS2000 3G VPN	HW-108030	mGuard rs2000 4TX/3G VPN
2700634	FL MGUARD RS4000 TX/TX	HW-107010	mGuard rs4000 TX/TX
2200515	FL MGUARD RS4000 TX/TX VPN	BD-701000	mGuard rs4000 TX/TX VPN
2701876	FL MGUARD RS4004 TX/DTX	HW-107020	mGuard rs4000 4TX/TX
2701877	FL MGUARD RS4004 TX/DTX VPN	BD-702000	mGuard rs4000 4TX/TX VPN
2903440	TC MGUARD RS4000 3G VPN	BD-703000	mGuard rs4000 4TX/3G/TX VPN
2702139	FL MGUARD RS2000 TX/TX-B		
2702259	FL MGUARD RS4000 TX/TX-P		
2702470	FL MGUARD RS4000 TX/TX-M		
2701274	FL MGUARD PCI4000	HW-102061	mGuard pci2 SD
2701275	FL MGUARD PCI4000 VPN	BD-111040	mGuard pci2 SD VPN
2701277	FL MGUARD PCIE4000	HW-102071	mGuard pcie2 SD
2701278	FL MGUARD PCIE4000 VPN	BD-111060	mGuard pcie2 SD VPN
		BD-111070	mGuard pcie2 SD HT VPN
2700967	FL MGUARD DELTA TX/TX	HW-103060	mGuard delta2 TX/TX
2700968	FL MGUARD DELTA TX/TX VPN	BD-211010	mGuard delta2 TX/TX VPN
2700640	FL MGUARD SMART2	HW-101130	mGuard smart2
2700639	FL MGUARD SMART2 VPN	BD-101030	mGuard smart2 VPN
2702884	FL MGUARD CORE TX	HW-101210	mGuard core2
2702831	FL MGUARD CORE TX VPN		
2903588	TC MGUARD RS2000 4G VPN		
2903586	TC MGUARD RS4000 4G VPN		

5.2 Platform FL MGUARD GT/GT

This platform includes the following devices:

PHOENIX CONTACT Devices		*Innominate Devices*	
2700197	FL MGUARD GT/GT		
2700198	FL MGUARD GT/GT VPN		

5.3 Platform Intel IXP4xx

This platform includes the following devices:

PHOENIX CONTACT Devices		***Innominate Devices***	
	FL MGUARD RS	HW-105000	mGuard industrial RS
	FL MGUARD RS VPN	BD-501000	mGuard industrial RS VPN
	FL MGUARD RS VPN ANALOG	BD-501010	mGuard industrial RS VPN analog
	FL MGUARD RS VPN ISDN	BD-501020	mGuard industrial RS VPN isdn
	FL MGUARD RS-B		
	FL MGUARD PCI/266	HW-102020	mGuard PCI/266
	FL MGUARD PCI/533	HW102050	mGuard PCI/533
	FL MGUARD PCI/266 VPN	BD-111010	mGuard PCI/266 VPN
	FL MGUARD PCI/533 VPN	BD-111020	mGuard PCI/533 VPN
		HW-103050	mGuard delta
		BD-201000	mGuard delta VPN
		HW-101020	mGuard smart/266
		HW-101050	mGuard smart/533
		BD-101010	mGuard smart/266 VPN
		BD-101020	mGuard smart/533 VPN
		HW-104020	mGuard blade/266
		HW-104050	mGuard blade/533

5.4 Platform Centerport and Centerport2

This platform includes the following devices:

PHOENIX CONTACT Devices		***Innominate Devices***	
2702547	FL MGUARD CENTERPORT	HW-106010	mGuard centerport2
		BD-621000	mGuard centerport2 250
2702820	FL MGUARD CENTERPORT VPN-1000	BD622000	mGuard centerport2 1.000
		HW-106000	mGuard centerport
		BD-601000	mGuard centerport VPN-250
		BD-602000	mGuard centerport VPN-1000
		HW-106100	mGuard centerport 1U
		BD-611000	mGuard centerport 1U VPN-250
		BD-622000	mGuard centerport 1U VPN-1000

6 Documentation Updates / Errata

- currently none

Phoenix Contact Art.Nr.;Phoenix Contact Art.Bez.;Bemerkung

2700642	HW/FW alt: 05/8.6.1	HW/FW neu: 10/8.7.0
2700642	HW/FW alt: 03/8.6.1	HW/FW neu: 10/8.7.0
2702139	HW/FW alt: 01/8.6.1	HW/FW neu: 10/8.7.0
2701875	HW/FW alt: 05/8.6.1	HW/FW neu: 10/8.7.0
2700634	HW/FW alt: 05/8.6.1	HW/FW neu: 10/8.7.0
2200515	HW/FW alt: 01/8.6.1	HW/FW neu: 10/8.7.0
2701876	HW/FW alt: 01/8.6.1	HW/FW neu: 10/8.7.0
2701877	HW/FW alt: 01/8.6.1	HW/FW neu: 10/8.7.0
2700640	HW/FW alt: 01/8.6.1	HW/FW neu: 10/8.7.0
2700639	HW/FW alt: 00/8.6.1	HW/FW neu: 10/8.7.0
2702547	HW/FW alt: 02/8.6.1	HW/FW neu: 10/8.7.0
2702259	HW/FW alt: 04/8.6.1	HW/FW neu: 10/8.7.0
2701275	HW/FW alt: 04/8.6.1	HW/FW neu: 10/8.7.0
2701274	HW/FW alt: 04/8.6.1	HW/FW neu: 10/8.7.0
2701278	HW/FW alt: 06/8.6.1	HW/FW neu: 10/8.7.0
2700197	HW/FW alt: 06/8.6.1	HW/FW neu: 10/8.7.0
2700198	HW/FW alt: 02/8.6.1	HW/FW neu: 10/8.7.0
2702465	HW/FW alt: 02/8.6.1	HW/FW neu: 10/8.7.0
2700968	HW/FW alt: 02/8.6.1	HW/FW neu: 10/8.7.0
2702863	HW/FW alt: 07/8.6.1	HW/FW neu: 10/8.7.0
2700967	HW/FW alt: 01/8.6.1	HW/FW neu: 10/8.7.0
2702831	;FL MGUARD CORE TX VPN;	