Innominate mGuard

Version 7.6.8 - Release Notes

**Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin, Germany
Tel.: +49 30 921028-0
e-mail: contact@innominate.com
http://www.innominate.com/**

April 2015

“Innominate” and “mGuard” are registered trademarks of the Innominate Security Technologies AG. All other brand names or product names are trade names, service marks, trademarks, or registered trade marks of their respective owners.

mGuard technology is protected by the German patents #10138865 and #10305413. Further national and international patent applications are pending.

All information contained in this documentation is subject to change without previous notice. Innominate offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes. In addition, Innominate 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.

Innominate Document Number: I15005_en_00

Vertical bars to the left mark significant changes in firmware 7.6.8 in comparison to the release notes for firmware version 7.6.7.

1 Product Description

1.1 Supported Hardware

The firmware can be operated on the following hardware platforms:

- mGuard core²
- mGuard pci² SD
- mGuard pcie² SD
- mGuard delta²
- mGuard rs2000
- mGuard rs4000
- mGuard centerport
- mGuard industrial RS
- mGuard smart²
- mGuard smart
- mGuard core
- mGuard pci
- mGuard blade
- EAGLE mGuard / mGuard industrial
- mGuard delta
- FL MGUARD GT/GT

For detailed information about these platforms please see the technical data sheets, which are offered for download at http://www.innominate.com/ .

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 features are listed and described in detail within the user manual, which can be downloaded from http://www.innominate.com/ .

1.3 Changes Since Previous Release

This section lists the changes since the previous release. Changes since earlier versions are listed in the chapter “Version History” below.

- This release fixes CVE-2015-0204 known as FREAK. Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20150407_001_en.pdf
- VPN transport connections in automatic 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.
- The reliability of devices with a full filesystem and during a sudden power interruption got improved in this release.
- In stealth mode all IP packets matching the firewall rules will now pass the device.
- Flashing with rollout-script of newer devices (produced with Firmware 8) now works without modifications of the rollout script.

- 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 after reboot, but no traffic traversed the tunnel..

1.4 Updating from previous releases

Updating to 7.6.8 is supported from the following releases.
All platforms but mGuard industrial RS, smart, PCI, Blade, delta and EAGLE mGuard:

- 7.0.0, 7.0.1, 7.0.2
- 7.1.0, 7.1.1
- 7.2.0, 7.2.1

All Platforms:

- 7.3.0, 7.3.1
- 7.4.0, 7.4.1
- 7.5.0
- 7.6.0, 7.6.1, 7.6.2, 7.6.3, 7.6.4, 7.6.5, 7.6.6, 7.6.7

Devices still operating with older software versions must either be updated to at least version **7.0.0** first or may be installed from scratch using the flash mechanism. Please refer to the user manual.
The update from version 7.3.0 is only supported for those platforms for which version 7.3.0 was released. Please refer to the corresponding release notes. Devices with less than 64 MB of RAM cannot be updated to version 7.6.8.
The “Local Update” feature may be used. Innominate strongly suggests to use this feature for devices which are configured with network mode “Router” and a router mode other than “static”.

- The "update-7.x-7.6.8" allows it to update from the listed 7.x versions to 7.6.8.

The “Automatic Update” feature may be used.

- With the listed 7.x.y version the 7.6.8 release is automatically chosen when using the "Install latest minor release" function.
- With the listed 7.6.y version the 7.6.8 release is automatically chosen when using the "Install latest patches" function.

The “Online Update” feature may be used.

- With the listed 7.x.y versions the 7.6.8 release is installed when the package set name "update-7.x-7.6.8" is used for "Install Package Set".

1.4.1 Important update information (updating from 7.x.y)

- Please make sure to backup saved configuration profiles from the mGuard and delete them from the device before starting the upgrade process. After the upgrade has been finished, the backed up configuration profiles can be uploaded to the device again.
- Any private extensions (like a tcpdump) you might have stored on the mGuard's file system must be removed before the update.
- Devices with less than 64 MB of RAM are not supported anymore.
- The Configuration Pull mechanism must be disabled during the time of the update.
- The automatic and online update are not supported on IXP4xx based devices if the update server is accessed through a VPN channel.

- The update interrupts the normal operation of the mGuard temporarily:
    - When watching the update progress at the web interface the user may get logged off with the message that a configuration change has been performed concurrently. This is harmless and caused by the update process which changes some variables for safety reasons but will restore them to their former values once the update is finished.
    - During the update the device becomes inaccessible and blocks network traffic. The update takes approximately 10 minutes. It may take longer for complex configurations.
    - The device reboots two times during the update.
    - VPN connections are terminated at the beginning of the update, and are re-established after the update.
    - Logs about the update progress are visible after the first login and in the log in the rare case of unexpected configuration content. Please read the information carefully.
- The following prerequisites must be met before a device can be updated. Please reconfigure your device accordingly. Otherwise the device will refuse the update.
    - The “CRL checking” feature (verifying the validity of X.509 certificates with the help of a Certificate Revocation List) must be disabled.
    - Only when updating from version 7.2.x and earlier the Firewall Redundancy feature must be disabled.

1.4.2 Important installation information (flashing with 7.6.8)

- Devices which have been shipped with firmware version 2.x.y or earlier need to be flashed or updated to firmware 4.1.x or 4.2.x first to get the boot loader updated.
- Devices produced before 2007 require **two** Major Upgrade Licenses before the 7.6.8 firmware image can be installed using the flash mechanism.
- If such a device had already been updated or flashed to any 5.x.y version successfully beforehand then just **one** Major Upgrade License is required for it.
- Devices produced before October 2007 require **one** Major Upgrade License before the 7.6.8 firmware image can be installed using the flash mechanism.
- Younger devices do not need a Major Upgrade License.
- If the device is flashed with 7.6.8 without appropriate license its error LED will signal the morse code “SOS” whenever it is started.
- The Major Upgrade License must be obtained for each device while it still operates firmware version 4.1.x, 4.2.x, or 5.x.y. Flash it with firmware 4.1.x, 4.2.x, or 5.x.y first if necessary. Please see their respective release notes and manual for details.
- To obtain a Major Upgrade License, a Major Upgrade Voucher needs to be purchased and redeemed first. The voucher must be cached with the help of the “Edit License Request Form” feature available within the “Management / Licensing” menu of the device. The device must therefore be connected to the Internet, for example by operating it in auto stealth mode and attaching it to a PC which is connected.
- The Major Upgrade License must be stored as a file.
- The license file must be copied to the tftp directory as a file named “licen**c**e.lic” in the same directory as the firmware image (e.g. the file “jffs2.img.p7s”).

- If two licenses are needed for a device, then only the one downloaded at last must to be copied to the tftp directory.
- Once a device has been flashed with firmware 6.x.y or 7.x.y successfully, further flashing of that device with firmware version 7.6.8 or older will not require any license file to be present within the tftp directory.
- The installation of the 7.6.8 firmware image (file “jffs2.img.p7s”) must be performed with exactly the file “install.p7s” it was shipped with. For the mGuard centerport the file names are “firmware.img.x86.p7s” and “install.x86.p7s” respectively. For the mGuard smart², rs2000 and rs4000 the file names are “ubifs.img.mpc83xx.p7s” and “install-ubi.mpc83xx.p7s” respectively.
- If a device needs to be downgraded from 7.6.8 to any older firmware version prior to 5.0.0, the file “install.p7s” from 7.6.8 must be used in combination with the older version's file “jffs2.img.p7s”.

1.4.3 Obtaining the update files

As of release 3.0.0 customers must register before downloading the update files for offline download or to access the online update server. Please refer to

http://www.innominate.com/register_software
http://www.innominate.de/register_software.

After registration user and password information is sent. Please note that the update server is operating using the “HTTPS” protocol.

2 Version History

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

2.1 Changes made between 7.6.6 and 7.6.7

- This release fixes NTP security issue CVE-2014-9295 which allows remote code execution with reduced privileges. Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20150120_001_en.pdf

2.2 Changes made between 7.6.5 and 7.6.6

- This release fixes the OpenVPN security issue CVE-2014-8104 which allows to attack the mGuard IPSec TCP encapsulation. Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20141217_002_en.pdf
- It also fixes a privilege escalation issue for the admin user (CVE-2014-9193). Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20141217_001_en.pdf
- 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.

2.3 Changes made between 7.6.4 and 7.6.5

- This release fixes the SSL protocol 3.0 security issue CVE-2014-3566 known as POODLE. Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20141022_001_en.pdf
- It additionally disables Session Tickets to take measures against the OpenSSL Session Ticket Memory Leak (CVE-2014-3567).

2.4 Changes made between 7.6.3 and 7.6.4

- This release fixes the Snapshot-Download security issue CVE-2014-2356. Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20140626_001_en.pdf
- It also incorporates the OpenSSL client vulnerability patch CVE-2014-0224 Please see the Innominate Security Advisory at: http://www.innominate.com/data/downloads/software/innominate_security_advisory_20140606_001_en.pdf

2.5 Changes made between 7.6.2 and 7.6.3

- This release fixes a bootloader issue which could lead to a non-booting device after an update or flashing to version 7.6.2.
- VPN connections with PSK and unspecified gateways (%any) are not rejected anymore.
- Packets accepted by the MAC filter are now additionally analyzed by the ARP DoS protection filter.
- Packets with the same source and destination address were not dropped in all occasions. This is fixed now.

- It fixes VPN connection problems that occurred when using TCP encapsulation together with redundancy on the centerport hardware with a dedicated synchronization interface.

2.6 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 multiple 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.

2.7 Changes made between 7.6.0 and 7.6.1

- Innominate mGuard blade devices did not function properly with the Innominate mGuard Software 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.

2.8 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.

2.9 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.

2.10 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.

2.11 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.

2.12 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.

2.13 Changes made between 7.2.0 and 7.2.1

- Version 7.2.1 adds support for a new hardware revision of the EAGLE mGuard product

3 Identified Issues and Workarounds

Issue “Mounting Microsoft Windows 98 shares” (Ref.9762)

	Description
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

Issue “Scanning of Windows shares may fail” (Ref.9651)

	Description
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.

Issue “CIFS AV Scan Connector with Microsoft Windows 98 shares” (Ref.9763)

	Description
Synopsis	When exporting shares for the AV Scan Connector functionality, there is a known limitation with Windows 98 shares. Currently, those shares are not shown as folders on the importing Windows host performing the AV scan.
Symptom	Directories from the exported share look like files on the importing Windows hosts.
Workaround / Action	None / Use a non-Windows system (Linux) as virus scanning host.

Issue “CIFS IM pattern matching is now case insensitive” (Ref.9432)

	Description

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.

Issue “Pull Update via VPN not supported on some devices” (Ref.9805)

	Description
Synopsis	The Pull Update through a VPN channel is not supported on the following devices: mGuard smart, mGuard PCI, mGuard industrial RS, mGuard blade, mGuard delta.
Symptom	The Pull Update will be rejected with an appropriate error message.
Workaround / Action	Use an other update mechanism.

Issue “Power OK shown late on mGuard Blade” (Ref. 1983)

	Description
Synopsis	The circuit checking the states of the redundant power supply units in the mGuard Blade does include filter capacitances. Due to these capacitances state changes are not signaled immediately. Power failure is signaled with a delay of 3-4 seconds, replacement of a power supply (now OK) is only signaled with a delay of 90 seconds.
Symptom	Display of the state of the power supply may still show failure even after the power supply has been re-enabled for 90s.
Workaround / action	None.

Issue “ICMP failure with transport VPN in Stealth Mode with SNMP”

	Description
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.

Issue “VPN firewall rule application for wrong tunnel”

	Description
Synopsis	If multiple tunnels are established to the same remote network originating from different local networks these tunnels conflict with one another.
Symptom	Firewall rules intended to be used within one tunnel are applied to connections of another one. Only one of those tunnels with the same remote network can be established at the same time. If a second one is established, the first one goes down.
Workaround / Action	Use only one tunnel for the same remote network, for example by extending the local network to include the former tunnels' local network.

Issue “Administrative Access From Moved Client in Single Stealth”

	Description
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.

Issue “Particular self signed certificates not accepted as HTTPS client certificates”

	Description
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`“

Issue “Changed Flood Protection Settings delayed for VPN connections”

	Description
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.

Issue “Reconfiguration of VLAN ID not noticed by DHCP server”

	Description
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.

Issue “Identical VPN connections just with different machine cert do no work”

	Description
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.

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

	Description
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.

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

	Description
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.

Issue “Configuration Pull interferes with Firmware Update ” (Ref. 6741)

	Description
Synopsis	If a firmware update was started interactively and is performed on an mGuard which is retrieving a new configuration profile from an HTTPS server at the same time, then the configuration pull procedure may be disturbed by the firmware update and / or the firmware update may fail.
Symptom	The application of the new configuration profile may fail. If the “rollback” feature of the configuration pull procedure is used the mGuard may be rolled back to a configuration which is not equivalent to the one which was active before the start of the procedure or the mGuard may even “forget” to roll back to the former configuration though it was not possible to reach the HTTPS server anymore after the new profile had been applied. The mGuard may fail to provide appropriate feedback to the IDM about the success or failure of the configuration pull procedure. The firmware update may fail. In particular this is likely to happen if the application of the profile initiates a reboot while the firmware update is still running.
Workaround / Action	Either initiate the firmware update with the help of the configuration pull procedure or deactivate the configuration pull procedure for the time of the firmware update.

Issue “netadmin cannot perform a test download for the Configuration Pull” (Ref.7540)

	Description
Synopsis	Through the GUI, the user “netadmin” cannot perform a test download of the configuration profile stored on a central HTTPS server.
Symptom	Even if the configuration is correct, “netadmin” will always see that the test download fails, for example with the message “The requested URL returned error: 401”.
Workaround / Action	None

Issue “mGuard PCI uses IP address assigned with DHCP after flashing” (Ref.8661)

	Description
Synopsis	If an mGuard PCI is flashed to firmware version 7.2.0 or later and the DHCP server TFTPD32.EXE (as recommended by Innominate) is used then at the end of the flash procedure the mGuard PCI reboots into the installed firmware and uses an IP address as management IP which is offered by TFTPD32.EXE via BOOTP. This is because of the feature described in section 5.2.1 of the user manual and because TFTPD32.EXE also answers BOOTP requests.
Symptom	The mGuard PCI uses a management IP address though it has not been configured yet.
Workaround / Action	Watch the logs of TFTPD32.EXE to learn the IP address it assigns to the mGuard and use this or 1.1.1.1 to access the mGuard.

Issue “Interoperability of SHA2 and IPsec” (Ref.8510)

	Description
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.

Issue “Fault LED on during flashing” (Ref.8823)

	Description
Synopsis	During the flash procedure of the devices industrial RS, rs2000 and rs4000 the Error LED is on and the FAULT ouput indicates an error.
Symptom	During the flash procedure, the device is non functional, which is indicated by the Fault LED since Firmware version 7.4.0. This behaviour is intended, but differs from previous firmware releases.
Workaround / Action	none

Issue “ECS storage on ACA21” (Ref.9978)

	Description
Synopsis	The external configuration storage ACA21 for EAGLE mGuard devices is not supported for encrypted profiles and manual modification of the stored data.
Symptom	The ECS data on SD cards or a USB storage (mGuard centerport) may be TPM-encrypted or (if not encrypted) manually modified by users. This does not apply to the EAGLE mGuard with ACA21, even though this is a USB storage, because of a missing TPM device.
Workaround / Action	none

Issue “Board temperature on mGuard centerport” (Ref.9803)

	Description
Synopsis	The board temperature is not shown on mGuard centerport devices in this release.
Symptom	In the web interface does not show the board temperature. Neither can it be queried via SNMP.
Workaround / Action	The next major release will support the board temperature again.

Issue “Factory Default on the blade controller” (Ref.10046)

	Description
Synopsis	The “factory default” settings on the mGuard blade controller are not applied correctly without reboot.
Symptom	After applying the factory default settings,

	the device is not accessible via the default IP address 192.168.1.1
Workaround / Action	Please reboot the mGuard blade controller after applying the factory default settings.

Issue “mGuard blade controller: wrong status of blade shown” (Ref.10047)

	Description
Synopsis	The blade controller display of a managed blade may show a wrong status (Blade Change Detected) even though the blade was not changed.
Symptom	If a configuration file on the blade controller gets deleted and afterwards uploaded from the client host to the controller, the Configuration status states [Blade Change Detected]
Workaround / Action	Do not delete the configuration of a managed blade prior to uploading it on the mGuard blade controller device.

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 Documentation Updates / Errata

- currently none