Release notes

Infinity® M300 and M300+ Series

WARNING

To properly use this medical device, read and comply with the Instructions for use, all supplements, and these release notes.

Infinity® M300 and M300+ Series Software VG3.0

Contents

This page has been left blank intentionally.

Introduction

This document describes the VG3.0 software version for the Infinity® M300 and M300+. The VG3.0 software adds software enhancements, performance enhancements, and addresses limitations identified in preceding software versions.

Enhancements

The VG3.0 release provides the following software enhancements:

- Cybersecurity enhancements
  - Encryption and authentication
  - Service user password enhancement
  - Malformed Application Control Service (ACS) protection
  - Security protocol updates
  - Security modes of operation
  - Network support matrix
  - Network security troubleshooting and error conditions
  - PSK security credential expiration
- Other enhancements
  - Support for the Greek language
  - KRACK (Key Re-installation Attack) fix with a wireless module update

Cybersecurity enhancements

Encryption and authentication

The VG3.0 release provides secure authentication, integrity, and encryption capability on the Infinity network for the exchange of data between the Infinity CentralStation (ICS) and the Infinity M300 and M300+ devices.

Service user password enhancement

Users are now required to create a unique password to access the Service menu and tools.

Packet storm resiliency

The packet storm protection with added user notifications prevents a network packet storm from interrupting patient monitoring.

Malformed Application Control Service (ACS) protection

Added protection to drop malformed network packets.

Security protocol updates

Enhanced security by removing FTP and HTTP web access and adding SFTP.

Security modes of operation

Secure mode is an enhanced Infinity network protocol that includes authentication, integrity, and encryption. Secure communication can be intercepted but not read or altered by an unauthorized device. The ICS always uses Legacy communication (standard Infinity protocol) to communicate with all other non-M300/M300+ devices on the Infinity network.

For Secure mode, PSKs are loaded on the ICS and M300/M300+ to establish an authorized network connection. Both devices must share the same key to communicate. A mismatch, missing or expired key on one or both devices will prevent communication and patient monitoring.

NOTE

PSKs should always be loaded on the ICS first and then the M300/M300+.

All Infinity devices should contain the same pre-shared key.

DrägerService, specialized service personnel, or the hospital's trained biomedical staff loads the PSKs to the Infinity devices using the Dräger INST software tool.

Legacy mode is the standard Infinity network protocol that exchanges data between the M300/M300+ and ICS, and other Infinity devices.

WARNING

Risk of cybersecurity attacks in Legacy mode

Disabling Secure mode and operating in Legacy mode lessens cybersecurity protection of the Infinity network communication. Legacy communication can be intercepted, read, or altered by an unauthorized device connected to the Infinity network, such as a malicious laptop.

Always operate devices in Secure mode when possible.

Secure/Legacy mode symbols

One of the following symbols displays on the ICS depending on which security mode is selected:

Symbol	Description
	Secure mode.
	Legacy mode.

Network support matrix

The following matrix identifies the interaction of Dräger devices on the Infinity network when the operation mode is secure and legacy:

Product	**Security Mode**	**ICS VG4**	**ICS VG4**	**ICS VG3 and below**	**M300 (+) VG3**	**M300 (+) VG3**	**M300 (+) VG2.4**	**IACS/ M540 VG7.1.1 and below**	**Delta[2] VF10 and below**	
Security Mode		Secure	Legacy	Legacy	Secure	Legacy	Legacy	Legacy	Legacy	Secure
Action		Admit	Admit	Remote View	Remote View	Remote View	Remote View	Remote View	Remote View	Transfer M300/ Bedside
ICS VG4	Secure	-	-	-	Y	Partial[1]	Partial[1]	Y	Y	-
ICS VG4	Legacy	-	-	-	Partial[1]	Y	Y	Y	Y	-
ICS VG3 and below	Legacy	-	-	-	Partial[1]	Y	Y	Y	Y	-
M300 (+) VG3	Secure	Y	N	N	-	-	-	-	-	Y
M300 (+) VG3	Legacy	N	Y	Y	-	-	-	-	-	N
M300 (+) VG2.4	Legacy	N	Y	Y	-	-	-	-	-	N
M540 VG7.1.1 and below	Legacy	Y	Y	Y	-	-	-	-	-	-
IACS VG7.1.1 and below	Legacy	Y	Y	Y	Partial[1]	Y	Y	Y	Y	-
Delta[2] VF10 and below	Legacy	Y	Y	Y	Partial[1]	Y	Y	Y	Y	N

1) In remote view with Legacy mode, the waveforms and patient parameters can be viewed. Remote control (alarm settings, arrhythmia settings, alarm silence, pause, and record) are not supported.
2) DSCP (Quality of Service) must be set to 0 for Delta devices.

Network security troubleshooting and error conditions

The following alarms may display on the M300/M300+ and/or ICS when secure communication is failed. If the device displays the error persistently, the clinician should contact the hospital's biomedical department, DrägerService, or specialized service personnel, or replace the device.

No.	Condition	Action/Condition that caused error	Error message	Admit screen pop-up
1	ICS in Secure mode and M300/M300+ in Legacy mode	Admit a new patient at M300/M300+.	ICS: ***Secure communication failure %s*** [1)] M300/M300+: ***Offline***	***Secure communication failed for %1. Please verify the M300 is in secure mode and the security PSK keys are valid.*** [1)]
	ICS in Legacy mode and M300/M300+ in Secure mode	Admit a new patient at M300/M300+.	ICS: ***%s: remote control failed*** [2)] M300/M300+: ***Secure Comm Failure*** and ***Offline***	None
2	ICS in Secure mode and M300/M300+ in Legacy mode	There is a mismatch of security settings when remote viewing the M300/M300+.	ICS: ***Secure communication failure %s*** [1)] M300/M300+: None	None
	ICS in Legacy mode and M300/M300+ in Secure mode	There is a mismatch of security settings when remote viewing the M300/M300+.	ICS: ***%s: remote control failed*** [2)] M300/M300+: ***Secure Comm Failure***	None
3	Mismatch of PSKs between ICS and M300/M300+	Two devices do not contain the same PSK.	ICS: ***Secure communication failure %s*** [1)] M300/M300+: ***Network config error***	None

No.	Condition	Action/Condition that caused error	Error message	Admit screen pop-up
4	ICS in Secure mode and PSK expired	Admit a new patient at M300/M300+.	ICS: None M300/M300+: ***Offline***	***Infinity network security PSK keys expire in less than seven days. Telemetry devices cannot be admitted.***
5	ICS in Secure mode and PSK is expiring	PSK will expire in 90 days.	ICS: Low-priority alarm banner ***Service due (renew %1): %2*** [3)]	None
6	ICS in Secure mode and PSK is expiring	PSK will expire in 7 days.	ICS: Medium-priority alarm banner ***Service due (renew %1): %2*** [3)]	***Infinity network security PSK keys expire in less than seven days. Telemetry devices cannot be admitted.***
7	ICS in Secure mode and PSK is expiring	PSK will expire in 1 day.	ICS: High-priority alarm banner ***Service due (renew %1): %2*** [3)]	***Infinity network security PSK keys expire in less than seven days. Telemetry devices cannot be admitted.***
8	M300/M300+ in Secure mode and PSK is expiring	PSK will expire in 90 days.	M300/M300+: Low-priority alarm ***Service due (renew PSK): %2*** [3)]	None
9	M300/M300+ in Secure mode and PSK is expiring	PSK will expire in 7 days.	M300/M300+: Medium-priority alarm ***Service due (renew PSK): %2*** [3)]	None
10	M300/M300+ in Secure mode and PSK is expiring	PSK will expire in 1 day.	M300/M300+: High-priority alarm ***Service due (renew PSK): %2*** [3)]	None
11	ICS in Secure mode and ICS does not have a PSK		ICS: ***Error: Failed to read: %1*** [4)]	None
12	ICS in Secure mode and ICS does not have a PSK	Open BedView, System setup, Trends/Data, or Telemetry defaults.	ICS: ***Error: Failed to read: %1*** [4)] and ***%s: remote control failed*** [2)]	None

1) <%s> is the IP address of the M300/M300+.
2) <%s> is the Bed label of the M300/M300+.
3) <%1> is the PSK filename, <%2> is the time remaining until expiration.
4) <%1> is the PSK filename.

PSK security credential expiration

The PSK security credential is valid for 2.5 years by default. The M300/M300+ will generate an expiration warning when the device is in Secure mode, and the security credential is about to expire.

Warning	Alarm	Action
90-day warning	A 90-day warning will be issued when the security credential is within 90 days of its expiration. The user will receive a single-shot advisory tone, and a persistent low-priority alarm banner in the header bar of the screen.	Contact your hospital's biomedical department, DrägerService, or specialized service personnel.
7-day warning	A 7-day warning will be issued when the security credential is within 7 days of its expiration. The user will receive a single-shot advisory tone, and a persistent medium-priority alarm banner in the header bar of the screen. The user will not be allowed to admit a patient on the M300/M300+. If the M300/M300+ travels out of wireless range while the patient is still admitted during the 7-day warning period, the device will re-connect when returned to the wireless range.	Contact your hospital's biomedical department, DrägerService, or specialized service personnel.
1-day warning	A 1-day warning will be issued when the security credential is within 1 day of its expiration. The user will receive a single-shot advisory tone, and a persistent high-priority alarm banner in the header bar of the screen. The user will not be allowed to admit a patient on the M300/M300+.	Contact your hospital's biomedical department, DrägerService, or specialized service personnel.

If you cannot admit an M300/M300+ patient to the ICS, refer to the clinical log for additional information and messages.

Other enhancements

Support for the Greek language

The Greek language is now available in the M300/M300+.

KRACK (Key Re-installation Attack) fix with a wireless module update

The wireless radio has been updated from version 1.2.6 to 1.8.2 which includes the KRACK vulnerability fix.

Corrected issues

The VG3.0 software release resolves the following issues. Unless otherwise noted, the corrected issues apply to both M300 and M300+.

- Sending malformed ACS messages to the M300 on either TCP port 1950 or 7100 could cause the M300 device to reset.
- Sending fast ACS messages to the M300 on TCP port 1950 could cause the M300 device to reset.
- M300 waveforms are sent to ICS while in ***Standby*** mode.
- The M300 Service menu allows viewing of EEPROM data with plain text passwords.
- It is possible to modify the web pages posted by the M300 via FTP.
- An erroneous ***Network error*** will be generated if the M300 is rebooted and a new patient is selected from the device. An ***Offline*** message is expected when a new patient is selected.
- M300 device reboots caused by I2C driver errors.

Hardware, software compatibility, and labeling

Software compatibility

The VG3.0 software has been validated with the following devices and software versions:

- M300 with integral battery
- M300+ with swappable battery
- Infinity CentralStation (ICS) VG4.0 (Secure mode)
- Infinity CentralStation (ICS) VG2.1.3 or greater (Legacy mode)
- Delta VF9.1 or greater (Legacy mode)
- Kappa VF9.1 or greater (Legacy mode)
- Infinity Acute Care System (IACS) VG4.n or greater (Legacy mode)
- M540 VG4.n or greater (Legacy mode)
- Infinity Gateway VF7.2 or greater (Legacy mode)
- R50N recorder software release VE0.2
- Dräger INST tool software release 1.1

Known limitations

The VG3.0 software release has the following unresolved issues. Unless otherwise noted, the limitations apply to both M300 and M300+.

- Pressing the ***Record*** button does not stop an alarm recording in process from printing as expected.
- Cyrillic numerical characters are not supported in the heart rate parameter box.
- Russian characters do not display on strip recordings.
- The umlaut E character displays as '?' in the patient demographics screen when the Russian language is configured.
- When a fault in processing a recording occurs, messages for recording start/finish are not displayed in the ICS message area as expected.
- When special characters are entered in a patient name field on the ICS for Polish, Czech and Hungarian languages, the characters may be displayed as a question mark.
- Instead of shutting down, the M300 will reset when the internal temperature has reached the acceptable limit.
- Occasionally, the M300 does not enter a fail state on the third reset within 10 minutes, as expected.
- A ***Recorder offline*** message does not display when the recorder is removed from the Infinity network.
- ECG print strip recordings may be clipped when the amplitude is greater than 1.3mv and negative peaks with a sinusoidal signal input are present.
- When a patient transfer is done from one M300 to another M300, the ***Type of implant*** demographics data is omitted.
- ST and PVC/min values are expected to be displayed as ***LRN*** in tabular and graphical trend when ***ECG relearn*** is manually selected, but no parameter values or ***LRN*** will be shown.
- When two M300s assigned to an ICS have the same IP address, one M300 will go offline and an alarm notification will annunciate at 100%.
- When an M300 device is configured for a Masimo SpO2 sensor, and a non-Masimo sensor is plugged in, the ***SpO2 unplugged*** status message, followed by the ***SpO2 Non-Masimo sensor*** message should appear on the M300 and ICS. The ICS only displays the ***SpO2 Non-Masimo sensor*** message.
- When the ECG color is changed, the paced color is not updated as expected.
- The SpO2 alarm will not update from a low to medium-priority alarm in the ICS BedView. The M300 and patient viewport will display the correct alarm priority.
- Erroneous pacer spikes can be generated when using the 2-meter extension cable. Dräger recommends the cable not be coiled when in use.
- Admitting and discharging a patient on the M300 from the ICS repeatedly at approximately 30-second intervals can leave the M300 and ICS in a de-synchronized state, and the M300 fails to discharge and shows in an offline state. In this state, the M300 shows on the ICS as discharged and when attempting to re-admit, the M300 shows as already in use.

- The pulse alarms will annunciate earlier than specified in the Instructions for use, but do not delay clinical treatment.
- When pediatric monitoring is selected, and the heart rate is set to 325 BPM or greater, the M300 will sometimes display values lower than 300 while the expected result is +++ or ***VF.***
- When the patient profile is changed (e.g. ***Adult*** to ***Pediatric***), the patient data will be recorded under a new instance. The ICS will maintain two separate sessions for before and after the patient profile change. All full disclosure, events and alarm histories are viewable under either of these instances.
- While configured with WPA2-Enterprise, if the M300 tries to reconfigure or re-authenticate, a gap of approximately 20 seconds is observed on the real-time waveform and full disclosure. Events that occur during this time are backfilled on the ICS after successful re-authentication of M300.
- If the patient is discharged from the M300 while in an offline state, the ICS will show the device in use when trying to admit a new patient. The state is corrected by discharging the patient from the device again.
- In the event of an M300 reset, the clinician will immediately be alerted with a visual and audible ***Offline*** alarm at the ICS.
- Configuring wireless infrastructures with WPA or WPA+WPA2 will cause the M300 to use the deprecated TKIP cipher which may compromise security. Dräger recommends configuring the network infrastructure to use WPA2 only.
- When Secure mode is enabled, and a PSK is set to expire (90, 7, or 1-day expiration) there may be up to a 5-minute latency in the PSK expiration message.
- When any of the settings under ***Telemetry defaults > Alarms > Device settings*** are selected, the selection does not take effect immediately for the M300 patient who has been admitted to the ICS. The patient must be re-admitted for the selection to be applied.
- In the system logs, the SpO2 parameter is displayed as "SO2 SO2," and the PLS parameter is displayed as "SO2 PR". Logs for alarm/audio pause and pacer fusion settings may contain incorrect information.
- The color of the ST parameter box in BedView for medium-priority alarms may be cyan instead of yellow.
- When a network load is heavy in Legacy mode, the M300 may continually reset to a fail state after the device goes out of range of the Access Point (AP) and back in range.
- When the M300 goes offline and tries to go back online, it may fail to go back online and stay offline until the user reboots the device.
- Non-English patient name and ID on strip recordings may display as garbled.
- M300 device observes reset when the main processor does not receive any communication from the digital signal processor (DSP). This issue was observed during product testing on VG2.4 and VG3.0. The root cause of this miscommunication remains unknown. Users can perform a power cycle on M300 to resolve this issue and use M300 again.
- M300 device continually resets to fail state when connected to 8 or more ICS devices due to memory issues. Users can perform a power cycle on M300 to resolve this issue. Further, they can choose to connect their M300 to 7 or fewer ICS devices as a workaround.

- When an M300 device is configured for a Nellcor SpO2 sensor and a non-Nellcor sensor is plugged in, the device displays the ***SpO2 Non-Nellcor sensor*** status message only for 40 seconds instead of being persistent. Then the device updates the message to ***SpO2 unplugged*** even though a wrong sensor is plugged in. If users reconnect the non-Nellcor sensor, the device displays the ***SpO2 Non-Nellcor sensor*** message again for another 40 seconds. Users are recommended to check the proper connection of the sensor and which sensor is selected to the monitor when they see status messages such as ***SpO2 Non-Nellcor sensor*** or ***SpO2 unplugged***.
- When using 5 GHz/802.11an wireless band with Cisco 802.11ax access points, M300 (0.4+HW) may show latency issues with patient admission (e.g., takes several attempts at admit). To mitigate this issue users can configure their M300 devices to 2.4 GHz/802.11bgn.
- When an M300/M300+ device is connected to 8 or more network recorders, the requested recording or a generated alarm may not generate. The recorders were observed to be inconsistent with the requests. This issue is not observed when 7 or fewer recorders are connected. Users are advised not to exceed 7 recorders set for a device.
- M300/M300+ fails IEC 60601-2-27 3rd edition: 201.12.1.101.8 Impulse Response standard. The baseline following the pulse is recorded to be more than 0.1 mV and the slope is recorded more than 0.3 mV/s, exceeding the specifications per the standard test. This issue may have an impact on ST segments when viewed in the ***Full disclosure ECG*** window. At all times, ST measurements are not affected as they are calculated from a separate signal path. For real-time analysis, clinicians should refer to the measured ST values or perform ST analysis under the ***ST complexes*** tab under ***ECG views***, accessible under BedView for a selected patient.

During a network packet storm, the following defects could occur:

- The M300 and M300+ medium and high-priority alarms may not flash correctly on the device, however the alarm will be visible and annunciate.
- The alarm pause timer may not display the count down correctly on display. The correct alarm pause time is maintained.
- A breakthrough alarm could annunciate as a persistent alarm versus a series of beep intervals.
- A low-priority Couplet (CPT) alarm will annunciate but the banner message will not display.

Dräger coordinated disclosure statement

At Dräger we develop technology for life which is why patient safety and medical device security are our top priorities. We endeavor to make our products as secure as possible against vulnerabilities that could affect the functioning of the products and the security, integrity and privacy of the electronic information and data used. We are committed to continuously improving the cybersecurity posture of our products and, as part of this effort and in line with our Coordinated Disclosure Policy, we have proactively issued an advisory to make you aware of some potential cybersecurity risks with our Infinity M300/M300+ patient monitors (software versions VG2.4 and earlier).

Dräger has identified that in the unlikely event that an unauthorized person, who has the skills and the access to the hospital network could potentially cause the Infinity M300 device to reboot, lose alarm functionality, and/or lose communication with the Infinity network.

Details of these vulnerabilities are published at the following Dräger Product Security Advisory link:

https://static.draeger.com/security/download/2019-09-13-Cybersecurity-M300-VGxx-Security-advisory-update_v1-3.pdf

Important Note: Dräger has received no reports of patient harm or successful exploits associated with these vulnerabilities.

Training recommendations

The VG3.0 Instructions for use can be downloaded from ServiceConnect. Dräger, the manufacturer of Infinity M300/M300+, requires that clinicians as well as those responsible for setting up and servicing devices read all Instructions for use manuals and supplements prior to employing the system in the care of patients.

Dräger recommends the responsible organization personnel refer to the ***Cybersecurity information and recommendations*** in the Instructions for use for all network security guidance.

Contact DrägerService, or specialized service personnel for assistance with all installation requirements.

If needed, Dräger will provide product training specific to the enhancements and corrected issues referenced in these release notes, enabling your organization to fulfill the requirements of local regulations. Contact your Dräger representative for details.

Trademarks

This page has been left blank intentionally.

This page has been left blank intentionally.

This page has been left blank intentionally.

These release notes only apply to
Infinity® M300 and M300+ Series VG3.0
with the Serial No.:
If no Serial No. has been filled in by Dräger, these release notes are provided for general information only and are not intended for use with any specific machine or unit.
This document is provided for customer information only, and will not be updated or exchanged without customer request.

CE 0123

CE

The radio equipment in the Infinity M300 patient monitor complies with the Radio Equipment Directive (2014/53/EU). A copy of the Declaration of Conformity is available at the following Internet address:
www.draeger.com/doc-radio

Manufacturer:

Draeger Medical Systems, Inc.
3135 Quarry Road
Telford, PA 18969-1042
U.S.A.
(215) 721-5400
(800) 4DRAGER
(800 437-2437)
FAX (215) 723-5935
http://www.draeger.com

EC REP **Drägerwerk AG & Co. KGaA**
Moislinger Allee 53 – 55
23542 Lübeck
Germany
+49 451 8 82-0
FAX +49 451 8 82-20 80
http://www.draeger.com

3720599 – RI 00 en

Edition: 1 – 2022-03

3 7 2 0 5 9 9