Mobile Patient Watch

Patientendaten-Informationssystem

Software 1.2.n

Administrationshandbuch

WARNUNG
Alle Tätigkeiten am Produkt setzen die genaue Kenntnis und Beachtung dieser Dokumentation und der Gebrauchsanweisung des Produkts voraus.

Dräger. Technik für das Leben®

Diese Seite wurde absichtlich leer gelassen.

Inhaltsverzeichnis

1 Informationen zu diesem Dokument

1.1 Typografische Konventionen

Text Texte, die fett und kursiv sind, kennzeichnen Bildschirmtexte.

1. Ziffern mit einem Punkt kennzeichnen die einzelnen Handlungsschritte einer Handlungsabfolge. Die Nummerierung beginnt bei jeder neuen Handlungsabfolge wieder mit der Ziffer 1.

a. Kleinbuchstaben mit einem Punkt kennzeichnen untergeordnete Handlungsschritte. Die Nummerierung beginnt bei jedem neuen übergeordneten Handlungsschritt wieder mit dem Buchstaben a.

● Dieser Punkt kennzeichnet einzelne Handlungsschritte ohne spezifische Reihenfolge.

► Dieses Dreieck kennzeichnet in Sicherheitshinweisen und in Warnhinweisen die Möglichkeiten zur Vermeidung der Gefährdung.

(1) Ziffern in Klammern beziehen sich auf Elemente in Abbildungen.

1 Ziffern in Abbildungen kennzeichnen Elemente, auf die im Text Bezug genommen wird.

– Spiegelstriche kennzeichnen Aufzählungen.

> Das Größer-als-Zeichen gibt den Navigationspfad in einem Dialog an.

Dieses Symbol kennzeichnet Informationen, die die Verwendung des Produkts erleichtern.

⇒ Dieser Pfeil kennzeichnet das Ergebnis eines Handlungsschritts.

✓ Dieses Häkchen kennzeichnet das Ergebnis einer Handlungsabfolge.

1.2 Weitere Dokumente

Informationen zur Anwendung des Produkts werden in der Gebrauchsanweisung beschrieben, die mit dem Produkt mitgeliefert wird.

2 Sicherheitsbezogene Informationen

2.1 Anforderungen an Benutzergruppen

Der Begriff "Benutzergruppe" beschreibt das verantwortliche Personal, das für die jeweilige Tätigkeit am Produkt vom Betreiber benannt wird.

2.1.1 Pflichten des Betreibers

Der Betreiber muss Folgendes sicherstellen:

- Jede Benutzergruppe verfügt über die erforderliche Qualifikation (z. B. eine fachliche Ausbildung oder durch Erfahrung erworbenes fachliches Wissen).
- Jede Benutzergruppe ist in die Tätigkeit eingewiesen.
- Jede Benutzergruppe hat die erforderlichen Kapitel in diesem Dokument gelesen und verstanden.

2.1.2 Benutzergruppen

Instandhaltungspersonal

Instandhaltungspersonal
Das Instandhaltungspersonal führt die folgenden Tätigkeiten aus:

- Konfigurieren der Benutzer und Benutzerrechte mithilfe von Active Directory
- Wartung der Betriebssysteme
- Management der Zertifikate
- Kundenspezifische Anpassungen (z. B. Sitzungstimeout)

Spezialisiertes Instandhaltungspersonal
Wenn produktspezifische Kenntnisse erforderlich sind, müssen die Maßnahmen von spezialisiertem Instandhaltungspersonal durchgeführt werden. Das spezialisierte Instandhaltungspersonal wurde von Dräger für diese Maßnahmen an diesem Produkt geschult.
Das spezialisierte Instandhaltungspersonal führt die folgenden Tätigkeiten aus:

- Installation des Produkts
- Konfiguration von Benutzern, wenn kein Active Directory verwendet wird
- Konfiguration von numerischen Parametern
- Aktivieren von Lizenzen

2.2 Informationen zu Sicherheitshinweisen

Sicherheitshinweise warnen vor Gefahren und geben Anweisungen für die sichere Verwendung des Produkts. Die Art der Gefährdung und die Folgen bei Nichtbeachtung sind in jedem Sicherheitshinweis aufgeführt. Bei Nichtbeachtung können Personenschäden oder Sachschäden entstehen.

2.3 Sicherheitshinweise

2.3.1 Inbetriebnahme

Konfiguration und Inbetriebnahme

Die Inbetriebnahme erfolgt nach einer Erstinstallation oder nach einem Update. Wenn die Installation und Konfiguration der Software unvollständig oder fehlerhaft ist, können Fehlfunktionen auftreten. Die Fehlfunktionen können zu Personenschäden führen.

► Informationen zur Inbetriebnahme von MPW beachten und den Anweisungen folgen.

► Vor der Inbetriebnahme muss die Funktionsfähigkeit der Software inklusive aller angeschlossenen Geräte und aller verbundenen IT-Systeme geprüft und freigegeben werden.

Die folgenden Handlungsschritte durchführen:

– Die Prüfergebnisse dokumentieren.

– Wenn die Prüfung bestanden wurde und die Funktionsfähigkeit verifiziert ist, die Software freigeben.

Zertifikat

Wenn das Zertifikat nicht sachgerecht installiert wird oder abgelaufen ist, wird die Verbindung zwischen Client und Webserver durch den Browser verweigert oder als nicht vertrauenswürdig angezeigt.

► Das Instandhaltungspersonal muss das Zertifikat sachgerecht installieren.

2.3.2 Verwendung

Patientenmonitoring

Wenn MPW wie ein aktiver Patientenmonitor verwendet wird, können kritische Patientenzustände möglicherweise nicht erkannt werden und zu Personenschäden führen. Die Software darf nicht wie ein aktiver Patientenmonitor verwendet werden.

► Die Daten der primären Datenquelle beachten.

Behandlungsentscheidungen

Durch eine verzögerte oder nicht aktuelle Anzeige der Daten können diagnostische oder therapeutische Fehleinschätzungen entstehen, die zu Personenschäden führen können. Kontinuierlich erfasste Parameter, die älter als 15 Sekunden sind, werden grau angezeigt. Dies gilt nicht für intermittierend erfasste Parameter, z. B. NIBP.

► Die angezeigten Daten nicht als alleinige Basis für diagnostische und therapeutische Entscheidungen verwenden.

► Für diagnostische oder therapeutische Entscheidungen die primäre Datenquelle beachten.

Einsatzbereich (mobile Anwendung)

Mobilgeräte dürfen entsprechend den Richtlinien der Gesundheitseinrichtung in bestimmten Bereichen der Gesundheitseinrichtung nicht verwendet werden, z. B. aus technischen oder hygienischen Gründen.

- ► MPW nur in den Bereichen der Gesundheitseinrichtung verwenden, die für die Verwendung von Mobilgeräten vorgesehen sind.
- ► Die Richtlinien der Gesundheitseinrichtung beachten.

2.3.3 IT-Netzwerk

Ausfall der Software oder des Netzwerks

Durch den Ausfall der Spannungsversorgung oder einzelner Netzwerkkomponenten können fallrelevante Daten fehlerhaft oder unvollständig angezeigt werden und zu Personenschäden führen.

- ► Der Betreiber muss die Verbindung des Endgeräts zum Netzwerk sicherstellen.

Synchronisation mit einem Zeitserver

Eine zeitliche Abweichung zwischen der primären Datenquelle und dem Endgerät kann zu einer fehlerhaften Anzeige der Daten führen.

- ► Sicherstellen, dass die primäre Datenquelle und das Endgerät mit demselben Zeitserver verbunden sind.

2.3.4 Alarme

In der Software werden weder akustische noch visuelle Alarmmeldungen oder Benachrichtigungen angezeigt.

- ► Die Alarme und Benachrichtigungen der primären Datenquelle beachten.

2.3.5 Instandhaltung

Wenn die Instandhaltungsmaßnahmen nicht regelmäßig durchgeführt werden, können Fehlfunktionen auftreten, die zu Personenschäden und Sachschäden führen können.

- ► Die Instandhaltung gemäß dem Kapitel „Instandhaltung“ durchführen.

2.3.6 Softwareintegrität

Wenn die Funktionalität für Windows File System Auditing wie von Dräger empfohlen bei der Installation konfiguriert wurde, wird schreibender Zugriff auf Dateien der Softwareanwendung, z. B. ausführbare Dateien oder DLLs, im Sicherheitsprotokoll protokolliert.

Ein Eintrag mit einer der folgenden Ereignis-IDs im Sicherheitsprotokoll kann auf einen unautorisierten Zugriff und somit auf einen Sicherheitsvorfall hindeuten:

- 4663: Dateizugriff wurde festgestellt.
- 4660: Datei wurde gelöscht.
- 4719: Auditing-Einstellungen wurden geändert. Dies ist ein Hinweis darauf, dass die Auditing-Funktionalität abgeschaltet wurde.
- 1102: Sicherheitsprotokoll wurde gelöscht.

► Um die Softwareintegrität zu gewährleisten, das Sicherheitsprotokoll auf Einträge mit den aufgelisteten Ereignis-IDs in Echtzeit überwachen, z. B. mithilfe von SIEM (Security Information and Event Management).

► Die Einträge mit den aufgelisteten Ereignis-IDs auf unautorisierten Zugriff analysieren.

3 Übersicht

3.1 Voraussetzungen

Für den sicheren Betrieb müssen die Zeiten zwischen der primären Datenquelle und dem MPW-Server übereinstimmen.

Dafür sollten in allen beteiligten Geräten (z. B. Monitore, Server und Endgeräte) die Zeitsynchronisierung mit einem NTP-Server aktiviert werden.

Dräger empfiehlt, das Infinity Gateway und den MPW-Backendserver in das IT-Sicherheitskonzept im Krankenhaus zu integrieren.

Alle Passwörter müssen nach der Installation geändert werden, um z. B. „Password Guessing“-Attacken zu vermeiden. Die Passwortlänge sollte nicht kleiner als 10 Zeichen sein. Dräger empfiehlt Passwörter zu verwenden, die sich stark voneinander unterscheiden. Passwörter dürfen nicht für unbefugte Personen zugänglich sein.

3.2 Abkürzungen

Abkürzung	Erklärung
ACL	Acces Control List Zugriffssteuerung des Betriebssystems
AD	Active Directory Verzeichnisdienst von Microsoft Windows Server
HTTPS	Hypertext Transfer Protocol Secure, sicheres Hypertext-Übertragungsprotokoll
ID	Identifikation
NTP	Network Time Protocol
PKI	Public-Key-Infrastruktur
R/O	Nur Lesezugriff (Rechteverwaltung)
R/W	Lese- und Schreibzugriff (Rechteverwaltung)
TCP	Transmission Control Protocol Gruppe von Kommunikationsprotokollen
TLS	Transport Layer Security (Verschlüsselungsprotokoll)
WSS	Web Services Security, Kommunikationsprotokoll

4 Applikationsdaten

4.1 Windows-Benutzer und Windows-Benutzergruppen

Die folgenden Windows-Benutzer und Windows-Benutzergruppen müssen für den Betrieb von MPW konfiguriert werden. Die Benutzer mit der ID 3,4,5 und 6 werden mit dem MPW-Installer installiert.

ID	Windows-Benutzer Windows-Benutzergruppen	Beschreibung
1	Spezialisiertes Instandhaltungspersonal	Das spezialisierte Instandhaltungspersonal installiert und warten die Software und installiert Patches.
2	Nicht autorisierte Windows Server-Benutzer	Alle Benutzer und Prozesse, die für den Betrieb von MPW nicht benötigt werden.
3	*mpw-gateway-wrapper*	Windows-Prozessname des Windows-Dienst-Benutzers, mit dem der MPW-Gateway-Wrapper ausgeführt wird.
4	*mpw-gateway-fetcher*	Windows-Prozessname des Windows-Dienst-Benutzers, mit dem der MPW-Gateway-Fetcher ausgeführt wird. Der MPW-Gateway-Fetcher empfängt Daten von Infinity Gateway, die im Gateway-Wrapper verarbeitet werden. Je nach Version kann der Name *mpw-gateway-fetcher-7.2* oder *mpw-gateway-fetcher-8.0* und höher verwendet werden.
5	*mpw-backend*	Windows-Prozessname des Windows-Dienst-Benutzers, mit dem MPW ausgeführt wird.
6	*postgres*	Windows-Prozessname des Windows-Dienst-Benutzers, mit dem die Postgres-Datenbank ausgeführt wird. Wenn es sich um eine Installation in einer Einrichtung des Department of Defense handelt, wird die Postgres-Datenbank nicht installiert. Stattdessen wird die Benutzerverwaltung über Active Directory abgebildet.

4.2 Rechteverwaltung für den Infinity-Gateway-Server

Dieser Abschnitt enthält Informationen über Zugriffsrechte für Windows-Benutzer auf Applikationsdaten. Die Applikationsdaten müssen über den Windows-Sicherheitsmechanismus (ACL) explizit gesetzt werden.

C:\Program Files (x86)\Draeger\MPW-Gateway-Wrapper

Der Ordner enthält Applikationsdaten, die für den Betrieb des Gateway-Wrappers notwendig sind.

Zugriffsrechte:

– R/W für spezialisiertes Instandhaltungspersonal
– R/O für *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Kein Zugriff für nicht autorisierte Windows-Server-Benutzer

***C:\Program Files (x86)\Draeger\MPW-Gateway-Wrapper*\application.properties**

Die Datei enthält Konfigurationen und Einstellungen, die für den sicheren Betrieb von MPW notwendig sind.

Zugriffsrechte:

– R/W für spezialisiertes Instandhaltungspersonal
– R/O für *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Kein Zugriff für nicht autorisierte Windows-Server-Benutzer

4.3 Rechteverwaltung für den MPW-Server

Dieser Abschnitt enthält Informationen über Zugriffsrechte für Windows-Benutzer auf Applikationsdaten.

C:\ProgramData\mpw-pgdata

Der Ordner ist ein Speicherort für Datenbankdateien, die Anmeldeinformationen für MPW-Benutzer enthalten. Wenn eine AD-Anbindung an MPW vorhanden ist, existiert der Ordner nicht.

Zugriffsrechte:

– R/W für spezialisiertes Instandhaltungspersonal und *postgres*
– Kein Zugriff für nicht autorisierte Windows-Server-Benutzer

***C:\Program Files\Draeger\MPW-Backend*\device-parameter-config.csv**

In dieser Datei kann die Anzeige von Geräteparametern konfiguriert werden.

Zugriffsrechte:

– R/W für spezialisiertes Instandhaltungspersonal
– R/O für *mpw-backend*
– Kein Zugriff für nicht autorisierte Windows-Server-Benutzer und *postgres*

***C:\Program Files\Draeger\MPW-Backend*\device-parameter-config-sample.csv**

In dieser Datei sind Beispiele zur Konfiguration für die Anzeige von Geräteparametern enthalten. Die Datei wird in einer Einrichtung des Department of Defense nicht installiert.

Zugriffsrechte:

– R/W für spezialisiertes Instandhaltungspersonal
– R/O für *mpw-backend*
– Kein Zugriff für nicht autorisierte Windows-Server-Benutzer und *postgres*

C:\Program Files\Draeger\MPW-Backend

Der Ordner enthält Applikationsdateien, die für den Betrieb von MPW notwendig sind.

Zugriffsrechte:

– R/W für spezialisiertes Instandhaltungspersonal
– R/O für *mpw-backend*
– Kein Zugriff für nicht autorisierte Windows-Server-Benutzer und *postgres*

***C:\Program Files\Draeger\MPW-Backend*\application.properties**

Die Datei enthält Konfigurationen und Einstellungen, die für den sicheren Betrieb von MPW notwendig sind.

Zugriffsrechte:

– R/W für spezialisiertes Instandhaltungspersonal
– R/O für *mpw-backend*
– Kein Zugriff für nicht autorisierte Windows-Server-Benutzer und *postgres*

4.4 Datei application.properties

4.4.1 Gateway-Wrapper-Webserver

C:\Program Files (x86)\Draeger\MPW-Gateway-Wrapper\application.properties

Beispieleinträge	Beschreibung
logging.level.org.springframework=INFO	Konfiguration des Logging-Levels für Spring
logging.level.com.draeger=TRACE	Konfiguration des Logging-Levels für MPW
server.port=8443	Port des Webservers
igw.user=<Benutzer>	Infinity-Gateway-Benutzer
igw.password=<Passwort>	Infinity-Gateway-Passwort

4.4.2 MPW-Webserver

C:\Program Files (x86)\Draeger\MPW-Backend\application.properties

Beispieleinträge	Beschreibung
logging.level.org.springframework=INFO	Einstellung von applikationsspezifischen Ereignissen
logging.level.com.draeger=TRACE	Einstellung von applikationsspezifischen Überwachungsereignissen
logging.level.com.draeger.upw.mpw.backend.log.session=OFF	Einstellung für das Loggen von allen Benutzer-Sitzungsereignissen
server.port=8444	Port des Webservers für Browserclients
mpw.session.mobile.timeout=30	Relative Sitzungstimeout für mobile Clients
mpw.session.desktop.timeout=120	Relative Sitzungstimeout für Desktop-Clients
mpw.session.absolute.timeout=720	Absolute Sitzungstimeout für alle Clients
server.ssl.keyStoreType=PKCS12	Zertifikat Keystore-Typ
server.ssl.key-store-password=<password>	PKI-Zertifikat Passwort
gateway.url=https://<gateway.server.name>:8444	Verbindungsinformationen zum Gateway-Wrapper
spring.datasource.password=<password>	Passwort der Datenbank in der Benutzerverwaltung (wird nicht bei einer AD-Anbindung verwendet)
spring.datasource.username=<postgres.username>	Benutzer der Datenbank in der Benutzerverwaltung (wird nicht bei einer AD-Anbindung verwendet)
server.name=<MPW domain>	Domainname für MPW Der Domainname muss mit dem Domainnamen im Zertifikat übereinstimmen

Beispieleinträge	Beschreibung
ad.domain	Für weitere Informationen siehe: „Active Directory“, Seite 19.
ad.url	
ad.searchFilter	
ad.groupMapping [<<AD-Gruppe>>]=<<CareUnit>>	
ad.groupMapping[Aerzte]=ICU	
ad.groupMapping[Aerzte]=OP1,OP2	
ad.groupMapping[Aerzte\ OP]=OP	

5 Firewallregeln

5.1 Gateway-Wrapper-Webserver

Standardmäßig startet die Anwendung auf Port 8443. Dieser Port wird als Standardeinstellung während der Installation verwendet. Die Standardeinstellung kann über die Datei *application.properties* geändert worden sein. Hierfür nach *server.port* suchen. Der Port muss als „Inbound Rule“ (TCP) freigegeben sein.

5.2 MPW-Webserver

Standardmäßig startet die Anwendung auf Port 8444. Dieser Port wird als Standardeinstellung während der Installation verwendet. Die Standardeinstellung kann über die Datei *application.properties* geändert worden sein. Hierfür nach *server.port* suchen. Der Port muss als „Inbound Rule“ (TCP) freigegeben sein.

5.3 Verbindungen

Damit sich das Frontend mit dem Backend verbinden kann, müssen im Netzwerk HTTPS- und WSS-Verbindungen erlaubt sein. Als Port für WSS (Websocket-Äquivalent zu HTTPS) wird der *server.port* des Backends verwendet. Für weitere Informationen siehe: „Datei application.properties“, Seite 13.

5.4 Firewallregeln und Virenschutz

Die Firewall auf dem Infinity Gateway und dem Backend muss „inbound“ jeweils den konfigurierten HTTPS/WSS-Port zulassen.

Folgende Virenscanner sind für die Verwendung auf dem Backend-Server getestet:

– McAfee 5 mit mittlerer Erkennungsstufe

Alle Ordner des Backend-Servers sind unbedenklich für einen Virenscan.

6 Protokollierung

6.1 Protokollebenen

Sämtliche Anwendungen, die mit MPW ausgeliefert werden, schreiben die Protokolle in das Windows-Ereignisprotokoll. Die Anwendungen prüfen beim Starten, ob das Protokollsystem funktioniert. Wenn ein Fehler auftritt, startet die Anwendung nicht. Protokollfehler im Betrieb können in der Ereignisanzeige (Event Viewer) im Windows Systemprotokoll mit der Quelle „Ereignisprotokoll“ gefunden werden. MPW erzeugt nach der Installation alle Ereignisse mit der Protokollebene „Information“, „Warning“ oder „Error.“ Folgende Protokollebenen stehen zur Verfügung:

Protokollebene	*application.properties*	Beschreibung
TRACE	logging.level.org.springframework=TRACE logging.level.com.draeger=TRACE	Bezeichnet detailliertere Informationsereignisse als die Protokollebene DEBUG.
DEBUG	logging.level.org.springframework=DEBUG logging.level.com.draeger=DEBUG	Bezeichnet detaillierte Informationsereignisse, die zum Beseitigen von Fehlern in einer Anwendung am nützlichsten sind.
INFO	logging.level.org.springframework=INFO logging.level.com.draeger=INFO	Bezeichnet Informationsmeldungen, die den Fortschritt der Anwendung auf einer undifferenzierten Ebene anzeigen.
WARN	logging.level.org.springframework=WARN logging.level.com.draeger=WARN	Bezeichnet potentiell fehlerhafte Situationen.
ERROR	logging.level.org.springframework=ERROR logging.level.com.draeger=ERROR	Bezeichnet Fehlerereignisse, mit denen die Anwendung möglicherweise weiterhin ausgeführt werden kann.

ℹ Für die Änderung der Protokollebenen muss die Datei *application.properties* von MPW und Gateway-Wrapper wie in der Tabelle angepasst werden (siehe „Datei application.properties“, Seite 13). Die Standardeinstellung nach der Installation ist „INFO“.

6.2 Sitzungsprotokollierung

Das Sitzungsprotokoll (*mpw-backend-sessions.log*) enthält potenziell personenbezogene Daten wie IP-Adresse und Benutzername. Um das Sitzungsprotokoll zu deaktivieren, muss folgende Zeile in der Datei *application.properties* vorhanden sein:

application.properties
logging.level.com.draeger.upw.mpw.backend.log.session=OFF

Für weitere Informationen siehe: „MPW-Webserver“, Seite 13.

6.3 Sitzungstimeout

Die Sitzungstimeouts haben nach der Installation die Standardwerte 30 Minuten für die mobile Anwendung und 120 Minuten für die Desktopanwendung. Die Zeitdauer der Sitzungstimeouts muss gemäß den Datenschutzrichtlinien der Gesundheitseinrichtung konfiguriert werden. Die Werte können in der Datei *application.properties* konfiguriert werden.

application.properties	Beschreibung
mpw.session.mobile.timeout=30	Relative Sitzungstimeout Die Sitzung wird nach der eingestellten Zeitdauer beendet, wenn keine Benutzeraktion in dieser Zeit erfolgt ist.
mpw.session.desktop.timeout=120	
mpw.session.absolute.timeout=720	Absolute Sitzungstimeout Die Sitzung wird immer nach Erreichen der eingestellten Zeitdauer beendet.

Die Einheit sind Minuten und müssen zwischen 1 und 720 Minuten liegen.

Für weitere Informationen siehe: „MPW-Webserver“, Seite 13.

6.4 Auffinden von Ereignissen

6.4.1 Ereignisanzeige

Zur besseren Auffindbarkeit der MPW-Protokolle wird bei der Installation von MPW-Backend und MPW-Gateway-Wrapper auf den jeweiligen Servern ein eigenes Log mit dem Namen „Draeger“ angelegt.

Die Ereignisanzeige von Windows (Event Viewer) verfügt über Funktionen, protokollierte Ereignisse zu verwalten (z. B. Archivierung, Rotation, Speicherung, Löschung oder Weiterleitung von Ereignissen). Diese Informationen können der Microsoft-Wissensdatenbank entnommen werden.

In der Ereignisanzeige von Windows werden Ereignisse typischerweise durch folgende Eigenschaften kategorisiert: *Ebene*, *Quelle*, *Ereignis-ID* und *Aufgabenkategorie*. Bis auf *Aufgabenkategorie* können diese Eigenschaften zum Filtern der MPW-Protokolle genutzt werden.

– *Aufgabenkategorie* wird nicht verwendet.
– *Quelle* entspricht dem Namen der MPW-Anwendung und kann demnach einen der folgenden Werte enthalten: *MPW-Backend*, *Bulkport*, *PasswordResetter*, *UserAdmin*, *PostgreSQL* und *MPW-Gateway-Wrapper*.
– *Ereignis-ID* dient zur inhaltlichen Kategorisierung von Protokolleinträgen. Im Folgenden wird aufgelistet, wie MPW-Protokolleinträge anhand der *Ereignis-IDs* kategorisiert werden.

6.4.2 Ereignis-IDs zum Auffinden von Ereignissen

Die Standardeinstellung der Protokollebene ist „Information“ und enthält die Protokollebenen „Warning“ und „Error“

Ereignis-ID	Anwendungen	Beschreibung
10	MPW-Backend, Bulkport, PasswordResetter, UserAdmin, MPW-Gateway-Wrapper	Applikationsspezifische Protokolle
11[1)]	MPW-Backend	Anmeldesitzungsereignisse (z. B. erfolgreiche und nicht-erfolgreiche Anmeldeversuche)
0[2)]	PostgreSQL	Interne Benutzerverwaltungsdatenbank des Backends
12	Kommunikationsinformationen	IP-Adressen von verbundenen Systemen. Erfolgreiche und erfolglose Versuche, auf Sicherheitsobjekte zuzugreifen oder diese zu ändern.
13	Sitzungsinformationen	Sitzungsteimout, Löschung, Erneuerung von Benutzersession-IDs
15	Benutzerauthentifizierung	Erfolgreiche, erfolglose Anmeldeversuche
16	Erfolgreiche oder erfolglose Versuche auf Debuginformationen zuzugreifen	Healthpage

1) Das Protokollieren der Sitzungen muss explizit aktiviert werden, da die Protokolle den Benutzernamen und die Sitzungs-ID enthalten. Vor der Aktivierung Informationen über die gesetzlichen Bestimmungen zum Schutz der Privatsphäre der Benutzer einholen und diese Bestimmungen beachten.

2) PostgreSQL-Protokolleinträge kommen direkt von der PostgreSQL-Datenbank. Dräger hat keinen Einfluss auf den Inhalt dieser Protokolleinträge (das ist auch der Grund, warum die Ereignis-ID 0 ist). Dräger ändert auch keine Standardeinstellungen hinsichtlich Protokollebene o. ä. für PostgreSQL.

6.4.3 Protokolleinträge außerhalb des Dräger-Protokolls

Folgende Ereignisse werden nicht ins Draeger-Protokoll geschrieben:

– Starten und Beenden der Dienste
  Protokolleinträge zum Starten und Beenden der installierten MPW-Dienste werden automatisch durch Windows in das Systemprotokoll geschrieben. Diese Protokolleinträge können dort unter der Quelle „Service Control Manager“ durch Suchen nach z. B. „mpw-backend“ oder „mpw-gateway-wrapper“ gefunden werden.

– Dateiänderungen
  Windows kann über die Audit File System Policy Dateizugriffe loggen, z. B. auf Konfigurationsdateien. Entsprechende Einträge werden im Sicherheitsprotokoll hinterlegt.

7 Konfiguration

7.1 Active Directory

Key	Wert
ad.domain	AD-Domain (z. B. *company.com*)
ad.url	AD-URL (z. B. *ldaps://ad.company.com*)
ad.rootDn	RootDn des ADs (wenn erforderlich)
ad.searchFilter	AD-Suchfilter, um autorisierte Benutzer im AD zu finden Standardeinstellung: *(&(objectClass=user)(userPrincipalName={0}))* Bei „[...]*Name={0}*“ wird {0} bei der Suche durch „username@domain“ ersetzt. Bei „[...]*Name={1}*“ wird *{1}* bei der Suche durch den Benutzernamen („username“) ersetzt.

Um festzulegen, welche AD-Gruppe welche Arbeitsplatzgruppe sehen kann, muss in der Datei *application.properties* ein Mapping zwischen dem Namen der AD-Gruppe und dem Namen der Arbeitsplatzgruppe erstellt werden.

Für jede AD-Gruppe, für die ein Mapping durchgeführt wird, muss eine Zeile in der Konfigurationsdatei im folgenden Format eingefügt werden:

ad.groupMapping[<<AD-Gruppe>>]=<<CareUnit>>

ℹ Die Bezeichnung für <<CareUnit>> muss der jeweiligen Bezeichnung im Netzwerk des Infinity Gateway entsprechen.

<<AD-Gruppe>> und *<<CareUnit>>* müssen durch den jeweiligen Namen ersetzt werden. Um z. B. der AD-Gruppe „Ärzte“ Zugriff auf die Arbeitsplatzgruppe (CareUnit) „ICU“ zu geben, muss folgende Zeile hinzugefügt werden:

ad.groupMapping[Aerzte]=ICU

Wenn eine AD-Gruppe Zugriff auf mehrere Arbeitsplatzgruppen haben soll, müssen diese hintereinander durch ein Komma getrennt angegeben werden.

Beispiel: *ad.groupMapping[Aerzte]=OP1,OP2*

Leerzeichen im AD-Gruppennamen müssen mit „\“ + „Leerzeichen“ angegeben werden.

Beispiel: *ad.groupMapping[Aerzte\ OP]=OP*

7.2 Entfernen von AD-Benutzern

Benutzer, die aus dem Active Directory entfernt wurden und noch eine gültige Benutzersitzung haben, können durch Neustarten des Windows-Service MPW-Backend vom Betrieb ausgeschlossen werden. Das Neustarten des MPW-Backend führt dazu, dass alle Benutzersitzungen beendet werden. Wenn kein Neustarten des MPW-Backend erfolgt, wird die Sitzung spätestens zum absoluten Sitzungstimeout beendet.

8 Backup und Disaster Recovery

Um bei Problemen das System neu aufzusetzen, muss ein Backup erstellt werden. Anschließend muss MPW neu installiert und müssen alle Konfigurationsdateien aus dem Backup eingespielt werden.

Die folgenden Konfigurationsdateien sind dafür notwendig:

Gateway

– *application.properties*

MPW-Backend

– *application.properties*
– *device-parameter-config-sample.csv*
– Das verwendete Zertifikat. Die entsprechende Datei kann in der Datei *application.properties* geändert werden (Standardwert: *cert.p12*).

Wenn die komplette Hardware ausgetauscht wird, muss die Lizenz neu eingespielt werden. Vor dem Austausch der Hardware das spezialisierte Instandhaltungspersonal kontaktieren.

Wenn MPW mit der internen Benutzerdatenbank installiert wurde, muss die Benutzerdatenbank vorher gesichert und anschließend wieder neu eingespielt werden. Dazu das spezialisierte Instandhaltungspersonal kontaktieren.

9 Public-Key-Infrastruktur

Um die hauseigene PKI zu nutzen, kann während der Installation das Server-Zertifikat eingespielt werden. Nach der Installation kann das Zertifikat in der Datei *application.properties* nachträglich geändert werden. Die folgenden Einträge müssen dafür angepasst werden:

– server.ssl.key-store-password
– server.ssl.key-store-store

Damit das Zertifikat als vertrauenswürdig eingestuft wird, muss der Domainname „server.name“ in der Datei *application.properties* mit dem Domainnamen im Zertifikat übereinstimmen.

10 Zertifikat

10.1 Installieren des TrustedRoot-Eintrags für das MPW-TLS-Zertifikat auf den Endgeräten

Wenn das Root-Zertifikat des Krankenhauses nicht schon auf den Endgeräten ausgerollt wurde, muss das Root-Zertifikat auf den Endgeräten installiert werden.

ℹ Zurzeit sind nur Microsoft Edge, Google Chrome und Apple Safari (iOS) zugelassen.

ℹ Das Root-Zertifikat ist nicht dasselbe, das vom Backend verwendet wird. Das Root-Zertifikat hat das Backend-Zertifikat unterschrieben.

Das Zertifikat wurde erfolgreich installiert, wenn man sich auf dem Gerät anmelden kann. Es genügt nicht, den Anmeldebildschirm öffnen zu können, sondern eine Anmeldung muss möglich sein.

10.1.1 Microsoft Windows

Es muss sichergestellt werden, dass der verwendete Browser dem auf dem Server verwendeten Zertifikat vertraut.

Bei manueller Installation:

1. Auf die Zertifikatsdatei doppelklicken.
   ⇒ Der Windows Zertifikatsmanager öffnet sich.
2. Das Zertifikat als Root hinzufügen (Auto Detection erkennt es nicht korrekt).

10.1.2 Apple iOS

Es muss sichergestellt werden, dass der verwendete Browser dem auf dem Server verwendeten Zertifikat vertraut.

Bei manueller Installation: Das Root-Zertifikat muss zunächst per E-Mail an ein Postfach versendet werden, das vom iPhone aus zugreifbar ist. Das Zertifikat kann nur installiert werden, wenn die E-Mail in der App ***Mail*** geöffnet wird und das angehängte Zertifikat ausgewählt wird. Die Geräte-PIN wird benötigt.

Mit einem Klick auf das Zertifikat wird es zunächst als nicht vertrauenswürdig installiert. Um die Vertrauenswürdigkeit zu aktivieren, ist folgender Schritt notwendig:

Einstellungen > ***Allgemein*** > ***Info*** > ***Zertifikatsvertrauenseinstellungen*** > ***volles Vertrauen für Root Zertifikat aktivieren***.

Unter ***Allgemein*** > ***Profil*** kann das Zertifikat wieder entfernt werden.

11 Deinstallation

Um alle sensiblen Daten vollständig zu löschen, empfiehlt Dräger nach der Deinstallation der Software den Computer neu aufzusetzen.

12 Instandhaltung

12.1 Definition der Begriffe zur Instandhaltung

Begriff	Definition
Instandhaltung	Alle Maßnahmen (Inspektion, Wartung, Reparatur), die der Erhaltung oder Wiederherstellung der Funktionsfähigkeit eines Produkts dienen
Inspektion	Maßnahmen zur Beurteilung des Istzustands eines Produkts
Wartung	Regelmäßige, spezifizierte Maßnahmen zur Aufrechterhaltung der Funktionsfähigkeit eines Produkts
Reparatur	Maßnahmen zur Wiederherstellung der Funktionsfähigkeit eines Produkts nach einer Fehlfunktion

Es wird empfohlen, einen Servicevertrag mit Dräger abzuschließen.

12.2 Wartung

Komponente	Intervall	Maßnahme	Benutzergruppe
TLS-Zertifikat	Nach Kundenangabe	Erneuern der TLS-Zertifikate	Instandhaltungspersonal
Festplatte	Alle 2 Jahre	Prüfen der Festplattenkapazität	Instandhaltungspersonal
		Archivieren und Löschen der Logdateien, wenn notwendig	

Sicherheitsupdates

Servicepacks und Patches wie z. B. von Microsoft Windows schließen Sicherheitslücken, beheben Fehler oder rüsten Funktionen nach. Dräger gibt bei MPW neue Sicherheitsupdates zur Installation frei. Für den Umgang mit Sicherheitsupdates folgende Punkte einhalten:

- Auf dem MPW-Server die automatische Updatefunktion für Patches und Servicepacks deaktivieren.
- Wenn ein neues Sicherheitsupdate veröffentlicht wird, die Freigabe von Dräger für das MPW-System abwarten. Wenn Dräger innerhalb von 4 Wochen nach Veröffentlichung eines Sicherheitsupdates keine Einwände mitteilt, gilt das Sicherheitsupdate für MPW als freigegeben.
- Wenn ein Testsystem vorhanden ist, empfiehlt Dräger das neue Sicherheitsupdate im Testsystem zu testen.

13 Technische Daten

13.1 Systemvoraussetzungen

13.1.1 Softwareumgebung und Infrastruktur

Versionen von Infinity Gateway Inklusive der Option WinAccess API	7.2, 8.0, 9.0
WLAN im Anwendungsbereich	
Bandbreite	Mindestens 1 Gbit/s in dem Netzwerk, das die Datenquellen und die Server miteinander verbindet.
Ports	8443 (Standardeinstellung), konfigurierbar

13.1.2 Server

Server für Software (Mobile Patient Watch)

Betriebssystem	Windows Server 2016 (physikalischer oder virtueller Server)
Prozessor	8 CPU-Kerne mit 3200 MHz Boost-Takt
Arbeitsspeicher (RAM)	32 GB
Festplatte SSD	2 TB

Server für Infinity Gateway

Auf der Hardware von Infinity Gateway muss eine zusätzliche Software zur Entgegennahme der Daten installiert werden, sodass sich die Systemvoraussetzungen für die Hardware erhöhen. Neben dieser Software darf keine weitere Software auf demselben Server installiert werden, die Infinity Gateway als Datenquelle verwendet.

Daraus resultieren die folgenden Systemvoraussetzungen:

Betriebssystem	Windows Server 2016 (physikalischer oder virtueller Server)
Prozessor	8 CPU-Kerne mit 3000 MHz
Arbeitsspeicher (RAM)	32 GB
Festplatte SSD	60 GB

13.1.3 Endgeräte

Empfohlene Endgeräte

Die Software kann auf empfohlenen Geräten vollständig angezeigt und verwendet werden. Die Kurvengeschwindigkeit gemäß der Spezifikation ist garantiert.

Mobile Anwendung	
Betriebssystem	iOS 14
Browser	Apple Safari (aktuelle Version)
Grafikauflösung	– 2436x1125 px (458 ppi) – 2532x1170 px (460 ppi) – 2688x1242 px (458 ppi)

Desktopanwendung	
Betriebssystem	Windows 10 (aktuelle Version)
Browser	Microsoft Edge (aktuelle Version) Google Chrome (aktuelle Version)
Grafikauflösung	1920x1080 px (24 Zoll)

Kompatible Endgeräte

Die Software kann auf kompatiblen Geräten vollständig angezeigt und verwendet werden. Die Kurvengeschwindigkeit kann von der Spezifikation abweichen, bleibt jedoch auf dem gleichen Gerät immer gleich hoch.

Mobile Anwendung	
Endgeräte mit Betriebssystem iOS	
Version	iOS 14 und höher (aktuelle Version)
Browser	Apple Safari (aktuelle Version)
Grafikauflösung	1136x640 px bis 2688x1242 px
Pixeldichte	326 ppi bis 476 ppi
Seitenverhältnis	1,8:1 bis 2,2:1
Endgeräte mit Betriebssystem Android	
Version	Android 9 und höher (aktuelle Version)
Browser	Chrome (aktuelle Version)
Prozessor	CPU-Octa-Core 1,6 GHz (+)
Grafikauflösung	1280x720 px bis 3200x1440 px
Pixeldichte	294 ppi bis 563 ppi
Seitenverhältnis	1,8:1 bis 2,2:1

Desktopanwendung	
Betriebssystem	Windows 10 (aktuelle Version)
Browser	Microsoft Edge (aktuelle Version) Google Chrome (aktuelle Version)
Grafikauflösung	Die Auswahl erfolgt durch den Betreiber.

ℹ Die Technische Dokumentation mit weiterführenden Informationen ist auf Anfrage erhältlich.

13.2 Betriebskennwerte

Klassifizierung

Klassifizierung Medizinprodukt Europa	Klasse IIb
UMDNS-Code Universal Medical Device Nomenclature System	17223
GMDN-Code Global Medical Device Nomenclature	44101

13.2.1 Anzeigegenauigkeit

Für Wertebereiche, die Anzeigegenauigkeit von Kurven, numerischen Werten und die Abtastrate der Trends, die Informationen in den Gebrauchsanweisungen von Mobile Patient Watch und Infinity Gateway beachten.

13.3 Kommunikation im Netzwerk

Datenquelle:	Infinity Gateway-Rechner mit Gateway-Wrapper-Komponente
Backend-Server:	Kommuniziert mit dem Infinity Gateway über eine verschlüsselte IP-Verbindung auf Port 8443 (Standard, der bei der Installation angepasst worden sein kann).
Endgeräte (PC oder Mobilgeräte):	Kommunizieren mit dem Backend-Server über eine HTTPS-Verbindung und WSS-Verbindung auf Port 8444 (Standard, der bei der Installation angepasst worden sein kann).

13.4 Verbindungen zu IT-Netzwerken

In einem IT-Netzwerk können Daten mit Hilfe von kabelgebundenen und drahtlosen Technologien ausgetauscht werden. Unter IT-Netzwerk fallen alle Datenschnittstellen, die in Normen und Konventionen beschrieben sind.

Dieses Produkt kann während des Betriebs mit Hilfe von IT-Netzwerken Informationen mit anderen Geräten austauschen und unterstützt folgende Funktionen:

– Anzeige von Kurven und Parameterdaten
– Bettansicht per Fernzugriff
– Übertragung von Geräteeinstellungen und Patientendaten

Das Anschließen dieses Produkts an ein Netzwerk, das weitere Geräte einbindet, oder nachträgliche Änderungen an diesem Netzwerk können zu neuen Risiken für Patienten, Anwender und Dritte führen. Bevor das Produkt an das Netzwerk angeschlossen wird oder das Netzwerk geändert wird, müssen diese Risiken identifiziert, analysiert und bewertet werden und entsprechende Maßnahmen ergriffen werden.

Beispiele für nachträgliche Änderungen am Netzwerk:

– Ändern der Netzwerkkonfiguration
– Entfernen von Geräten und Software aus dem Netzwerk
– Hinzufügen weiterer Geräte und Software zum Netzwerk
– Durchführen von Upgrades oder Updates bei Geräten und Software, die an das Netzwerk angeschlossen sind

Um eine sichere Kommunikation zwischen Server und Client sicherzustellen, muss eine TLS-Infrastruktur vorhanden sein. Dazu muss ein Zertifikat auf den Endgeräten installiert werden.

13.4.1 Informationen zum Anschließen an das IT-Netzwerk

13.4.1.1 Voraussetzungen

Dieses Produkt darf nur von dem spezialisierten Instandhaltungspersonal an das Netzwerk angeschlossen werden. Zuvor muss der IT-Verantwortliche der Gesundheitseinrichtung konsultiert werden.

Folgende Dokumente müssen beachtet werden:

– Begleitdokumente dieses Produkts
– Beschreibungen des Netzwerks

Dräger empfiehlt, die IEC 80001-1 (Risikomanagement für IT-Netzwerke mit Medizinprodukten) zu beachten.

13.4.1.2 Anbindung von primären Datenquellen

Die Anbindung von primären Datenquellen erfolgt ausschließlich über Infinity Gateway. Für weitere Informationen zum Anbinden von primären Datenquellen die Produktinformationen von Infinity Gateway beachten.

13.4.1.3 Anbindung von Endgeräten über Netzwerke

– LAN-Netzwerke werden meist in Sterntopologie konfiguriert. Mit Hilfe von Layer-n-Switches können einzelne Geräte zu Gruppen zusammengefasst werden. Die Entkopplung vom weiteren Datenverkehr erfolgt durch separate VLAN-Netzwerke. Die Netzwerkeinstellungen des Produkts entsprechend dieser Gebrauchsanweisung und der Netzwerkvorgaben konfigurieren.
– Spezifikationen für LAN-Verbindungen sind in den folgenden Normen beschrieben:
  – Kabelgebundene Netzwerke: IEEE 802.3
  – Drahtlose Netzwerke: IEEE 802.11 (b, g, n)
– Wenn das Produkt mit einem Layer-2-Switch oder Layer-3-Switch verwendet wird, müssen die Port-Einstellungen am Netzwerk-Switch konfiguriert werden. Bevor das Produkt ausgeliefert wird, kann Dräger die Netzwerkeinstellungen des Produkts nach Vorgaben des Betreibers konfigurieren.
– Dieses Produkt tauscht über das LAN-Netzwerk Daten mit anderen Medizinprodukten aus. Das Netzwerk muss die folgenden Übertragungen und Protokolle unterstützen:
  – TCP/IP
  – Unicast (statische oder dynamische Adressierung mit den Kommunikationsprotokollen ARP oder RARP)

- Multicast
- Broadcast
- IGMP (Version 2)

Dieses Produkt kann durch die Verwendung des Kommunikationsprotokolls IGMP einer IP-Multicast-Gruppe beitreten oder sie verlassen.

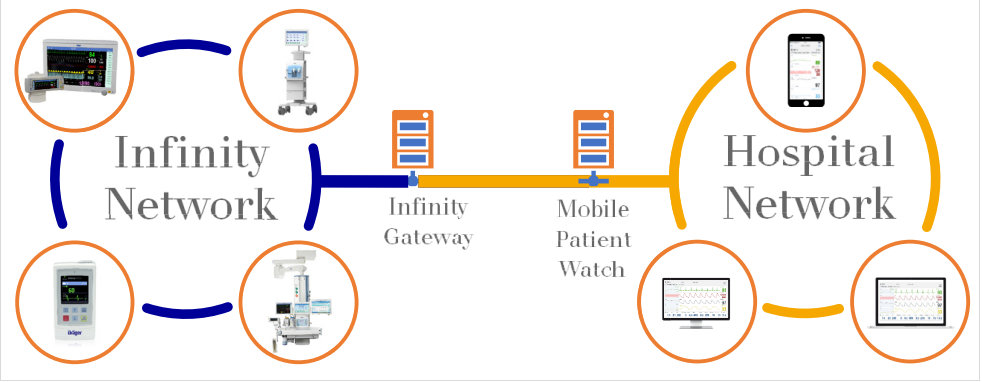
13.4.1.4 Folgen aufgrund eines ungeeigneten Netzwerks

Wenn das Netzwerk die erforderlichen Eigenschaften nicht aufweist, können daraus gefährliche Situationen entstehen. Bei diesem Produkt können folgende Situationen entstehen:

- Während einer Unterbrechung der Netzwerkverbindung:
  - Daten werden nicht oder verzögert angezeigt.
- Ohne Firewall:
  - Daten sind nicht geschützt.
  - Produkteinstellungen werden verändert.
- Daten werden nicht, unvollständig oder an das falsche Produkt gesendet.
- Patientendaten werden abgefangen, verfälscht oder beschädigt.
- Daten weisen falschen Zeitstempel auf.

13.4.1.5 Erforderliche Eigenschaften

Die primären Datenquellen und Infinity Gateway befinden sich im selben Netzwerk. Für dieses Netzwerk gelten die erforderlichen Eigenschaften. Dazu die Produktinformationen von Infinity Gatway beachten. Auf dem MPW-Server werden Daten mithilfe des MPW-Gateway-Wrappers empfangen, der auf dem selben Server installiert ist wie Infinity Gatway. MPW kann in einem Krankenhausnetzwerk betrieben werden, das alle Endgeräte mit dem MPW-Server verbindet. Dazu sind Zugriffsrechte notwendig.



Weitere Informationen zu Firewallregeln, siehe Installationsanleitung „Firewallregeln“.

Das Netzwerk, in dem MPW installiert und ausgeführt wird, muss sich unter der Kontrolle des Betreibers befinden.

Um einen nicht-autorisierten Zugriff und die Verbreitung von Schadsoftware im Netzwerk zu vermeiden, müssen Vorkehrungen getroffen werden. Folgende Vorkehrungen können beispielsweise getroffen werden:

– Einschränkung des physischen Zugriffs auf aktive Netzwerkdosen
– Nur für den Betrieb benötigte Ports dürfen konfiguriert werden. Alle anderen Ports müssen geschlossen werden.
– Es dürfen sich nur Geräte im Netzwerk befinden, die die gleiche oder eine höhere Vertrauensstufe haben.
– Sichere Isolierung des Netzwerks (physisch oder virtuell)
– Verwendung einer Firewall
– Patchverwaltung für Geräte
– Implementierung nach ISO/IEC 27033

13.4.1.6 Netzwerkauslastung

Zwischen Gateway-Wrapper und MPW-Backend gesendete Daten pro Patient

Anzahl Browser-Sessions	Upstream [kb/s]	Downstream [kb/s]	Datenart
1	689,63	32,11	Die übertragenen Daten bestehen größtenteils aus den relevanten, anzuzeigenden Daten für MPW wie Parameter, Trenddaten und Kurven. Der Testaufbau hat den Datendurchsatz für einen Patienten mit 17 Standardparametern, 4 Monitoringdaten mit zugehörigen Kurven und Trends mit steigender Sessionanzahl gemessen. Die Daten zeigen, dass der Datenverkehr zwischen Gateway-Wrapper und MPW- Backend annähernd stabil bleibt. Bei einer Veränderung der gleichzeitig angesehenen Patienten ist von einer Erhöhung des Datenverkehrs auszugehen.
2	666,8	31,00	
3	698,54	31,92	
4	652,04	30,37	

Zwischen MPW-Backend und Client gesendete Daten

Anzahl Browser-Sessions	Upstream [kb/s]	Downstream [kb/s]	Datenart
1	78,39	19,00	Der Testaufbau ist unverändert. Die Daten zeigen, dass der Datenverkehr zwischen MPW-Backend und Client (Endgerät) proportional steigt. Mit steigender Anzahl der Browser-Sessions ist von einer Erhöhung des Datenverkehrs auszugehen.
2	152,64	37,31	
3	246,36	57,22	
4	317,46	72,64	

13.4.1.7 Anzahl unterstützter Geräte

Durch eine Installation der Software können Daten von maximal 45 Arbeitsplätzen (Patientenmonitore) auf bis zu 100 Endgeräten gleichzeitig angezeigt werden.

Stichwortverzeichnis

B

I

S

W

Hersteller
Drägerwerk AG & Co. KGaA
Moislinger Allee 53 – 55
23542 Lübeck
Deutschland
+49 451 8 82-0

CE 0123

www.draeger.com

9510543 – 6405.022 de

Ausgabe: 2 – 2021-03 (Ausgabe: 1 – 2019-10)