Mobile Patient Watch

Informacioni sistem podataka o pacijentima

Softver 1.2.n

Priručnik za administratore

UPOZORENJE
Preduslov za sve radove na ovom proizvodu je poznavanje i poštovanje ove dokumentacije i uputstva za korišćenje proizvoda.

Dräger. Technology for Life®

Ova strana je namerno ostavljena prazna.

Sadržaj

1 Informacije o ovom dokumentu

1.1 Tipografske konvencije

Tekst Podebljani tekstovi ili kurzivno pismo označavaju tekstove na ekranu. Podebljani, kurzivni tekst označava tekstove koji su prikazani na ekranu.

1. Brojevi sa tačkom označavaju pojedinačne korake u okviru niza procesa. Numerisanje za svaki novi niz procesa počinje ponovo od broja 1.

a. Mala slova sa tačkom označavaju sekundarne korake procesa. Obeležavanje slovima za svaki novi korak procesa višeg nivoa počinje ponovo od slova a.

● Ova istaknuta tačka označava pojedinačne korake procesa u okviru određenog redosleda.

► U bezbednosnim uputstvima i obaveštenjima sa upozorenjima, ovaj trougao ukazuje na načine za izbegavanje opasnosti.

(1) Brojevi u zagradi upućuju na elemente na ilustracijama.

1 Brojevi na ilustracijama označavaju elemente na koje se upućuje u tekstu.

– Crtice predstavljaju spiskove.

> Simbol „veće od“ ukazuje na putanju navigacije kroz dijalog.

Ovaj simbol označava informacije koje će olakšati korišćenje proizvoda.

⇒ Ova strelica ukazuje na rezultat koraka obrade.

✓ Ovaj znak za potvrdu označava rezultat niza koraka obrade.

1.2 Ostala dokumentacija

Informacije o primeni proizvoda su opisane u uputstvu za korišćenje koje je isporučeno uz proizvod.

2 Bezbednosne informacije

2.1 Zahtevi korisničke grupe

Termin „korisnička grupa“ opisuje odgovorno osoblje koje je dodelila ustanova u kojoj se koristi proizvod za obavljanje određenog zadatka na proizvodu.

2.1.1 Obaveze ustanove u kojoj se koristi proizvod

Ustanova u kojoj se koristi proizvod mora da osigura sledeće:

– Svaka korisnička grupa ima potrebne kvalifikacije (npr. članovi su prošli stručnu obuku ili su stekli stručno znanje putem iskustva).
– Svaka grupa korisnika je obučena za obavljanje zadatka.
– Svaka grupa korisnika je pročitala i shvatila relevantna poglavlja u ovom dokumentu.

2.1.2 Korisničke grupe

Servisno osoblje

Servisno osoblje
Servisno osoblje obavlja sledeće delatnosti:

– Konfiguracija korisnika i korisničkih prava pomoću aktivnog direktorijuma
– Održavanje operativnih sistema
– Upravljanje sertifikatima
– Korisnička podešavanja (npr. vremensko ograničenje sesije)

Specijalizovano servisno osoblje
Kada su potrebna stručna znanja specifična za proizvod, servisne aktivnosti mora da obavi specijalizovano servisno osoblje. Kompanija Dräger je obučila specijalizovano servisno osoblje za obavljanje tih servisnih aktivnosti na ovom proizvodu.
Specijalizovano servisno osoblje obavlja sledeće delatnosti:

– Instalacija proizvoda
– Konfiguracija korisnika, kada se ne koristi aktivni direktorijum
– Konfiguracija numeričkih parametara
– Aktivacija licenci

2.2 Informacije o bezbednosnim uputstvima

Bezbednosna uputstva upozoravaju na rizike i daju uputstva za bezbedno korišćenje proizvoda. Tip rizika i posledice neusklađenosti su opisani u svakom bezbednosnom uputstvu. Njihovo nepoštovanje može dovesti do telesne povrede ili oštećenja imovine.

2.3 Bezbednosna uputstva

2.3.1 Puštanje u rad

Konfiguracija i puštanje u rad

Puštanje u rad se obavlja posle prve instalacije ili posle ažuriranja. Mogu se javiti nepravilne funkcije ako je instalacija i konfiguracija softvera nepotpuna ili pogrešna. Nepravilne funkcije mogu da izazovu nastanak povreda.

► Poštujte informacije u vezi sa puštanjem u rad softvera MPW i sledite uputstva.

► Pre prvog puštanja u rad je potrebno proveriti i odobriti funkcionalnost softvera kao i svih priključenih uređaja i svih povezanih IT sistema.

Izvršiti sledeće radne korake:

– Dokumentovati rezultate provera.

– Kada je provera uspešno okončana i funkcija verifikovana, odobriti rad softvera.

Sertifikat

Ukoliko sertifikat nije propisno instaliran ili je istekao, pregledač odbija vezu između klijenta i veb- servera ili se ona prikazuje kao nepouzdana.

► Servisno osoblje mora propisno da instalira sertifikat.

2.3.2 Korišćenje

Monitoring pacijenta

Kada se MPW koristi kao aktivni monitor pacijenta, kritična stanja pacijenta mogu da ostanu neprepoznata i da dovedu do nastanka povreda. Softver nije dozvoljeno koristiti kao aktivan monitor pacijenta.

► Poštujte podatke iz primarnog izvora podataka.

Odluke u vezi terapije

Usled zakasnelog ili neaktuelnog prikaza podataka može doći do donošenja pogrešnih dijagnostičkih ili terapeutskih odluka koje mogu da dovedu do nastanka povreda. Kontinuirano prikupljeni parametri, stariji od 15 sekundi, su prikazani sivom bojom. Ovo ne važi za intermintentno prikupljene parametre, npr. NIBP.

► Prikazane podatke ne koristiti kao jedinu osnovu za donošenje dijagnostičkih i terapeutskih odluka.

► Za donošenje dijagnostičkih i terapeutskih odluka poštovati primarni izvor podataka.

Polje primene (mobilna primena)

Mobilne uređaje nije dozvoljeno koristiti u određenim područjima u skladu sa smernicama zdravstvene ustanove, npr. iz tehničkih ili higijenskih razloga.

► MPW koristiti samo u područjima zdravstvene ustanove koja su predviđena za korišćenje mobilnih uređaja.

► Poštovati smernice zdravstvene ustanove.

2.3.3 IT mreža

Otkaz softvera ili mreže

Usled otkaza strujnog napajanja ili pojedinih mrežnih komponenata, podaci relevantni za dati slučaj mogu da budu pogrešno ili nepotpuno prikazani i da dovedu do nastanka povreda.

► Ustanova mora da obezbedi vezu krajnjeg uređaja sa mrežom.

Sinhronizacija sa vremenskim serverom

Vremensko odstupanje između primarnog izvora podataka i krajnjeg uređaja može da dovede do pogrešnog prikaza podataka.

► Uverite se da su primarni izvor podataka i krajnji uređaj povezani na isti vremenski server.

2.3.4 Alarmi

Softver ne prikazuje ni zvučne ni vizuelne poruke alarma ili obaveštenja.

► Poštujte alarme i obaveštenja iz primarnog izvora podataka.

2.3.5 Servis

Ako se servis ne obavlja redovno, može doći do kvarova, koji mogu da dovedu do fizičke povrede i oštećenja imovine.

► Obavljajte servis u skladu sa poglavljem "Servis".

2.3.6 Integritet softvera

Kada je funkcija za nadgledanje Windows sistema datoteka (Windows File System Auditing) prilikom instalacije konfigurisana po preporukama kompanije Dräger, u sigurnosnom protokolu se dokumentuje pristup upisivanja datoteka aplikativnog softvera, npr. izvršne datoteke ili DLL datoteke.

Unos sa nekim od sledećih ID događaja u sigurnosnom protokolu može da ukazuje na neovlašćeni pristup a time i na sigurnosni incident:

– 4663: Ustanovljen je pristup datoteci.
– 4660: Datoteka je obrisana.
– 4719: Izmenjena su podešavanja nadgledanja. Ovo ukazuje na to da je funkcija nadgledanja isključena.
– 1102: Sigurnosni protokol je obrisan.

► Da bi se obezbedio integritet softvera, potrebno je vršiti nadzor sigurnosnog protokola u pogledu unosa sa izlistanim ID-om događaja u realnom vremenu, npr. pomoću alata SIEM (Security Information and Event Management).

► Unosi se analiziraju u pogledu neovlašćenog pristupa sa izlistanim ID-om događaja.

3 Pregled

3.1 Preduslovi

Za bezbedan rad potrebno je da se poklapaju vremena primarnog izvora podataka i MPW servera.

U tom cilju je na svim uključenim uređajima (npr. monitorima, serverima i krajnjim uređajima) potrebno aktivirati sinhronizaciju vremena sa NTP serverom.

Dräger preporučuje da se Infinity Gateway i MPW pozadinski server integrišu u IT bezbednosni koncept bolnice.

Sve lozinke moraju da budu promenjene nakon instalacije, da bi se izbegli npr. napadi "pogađanja lozinke". Dužina lozinke ne bi trebala da bude manja od 10 znakova. Dräger preporučuje korišćenje takvih lozinki koje se međusobno veoma razlikuju. Lozinke ne smeju da budu dostupne neovlašćenim licima.

3.2 Skraćenice

Skraćenica	Objašnjenje
ACL	Acces control list — Lista kontrole pristupa Kontrola pristupa operativnog sistema
AD	Aktivni direktorijum Direktorijum Microsoft Windows servera
HTTPS	Hypertext Transfer Protocol Secure (Sigurni protokol za prenos hiperteksta)
ID	Identifikacija
NTP	Network Time Protocol - Mrežni vremenski protokol
PKI	Infrastruktura javnih ključeva
R/O	Samo pravo pristupa čitanja podataka (upravljanje pravima)
R/W	Pravo upisa i čitanja podataka (upravljanje pravima)
TCP	Transmission control protocol — Transmisioni kontrolni protokol Grupa komunikacionih protokola
TLS	Transport Layer Security (protokol enkripcije)
WSS	Web Services Security — Bezbednost veb servisa, komunikacioni protokol

4 Aplikativni podaci

4.1 Windows korisnici i Windows korisničke grupe

Za rad softvera MPW potrebno je konfigurisati sledeće Windows korisnike i Windows korisničke grupe. Korisnici sa ID-om 3, 4, 5 i 6 se instaliraju pomoću MPW instalacionog programa.

ID	Windows korisnici Windows korisničke grupe	Opis
1	Specijalizovano servisno osoblje	Specijalizovano servisno osoblje instalira i održava softver i instalira zakrpe.
2	Neovlašćeni korisnici Windows servera	Svi korisnici i procesi koji nisu neophodni za rad softvera MPW.
3	*mpw-gateway-wrapper*	Windows naziv procesa i korisnika Windows servisa sa kojim se izvršava MPW Gateway Wrapper.
4	*mpw-gateway-fetcher*	Windows naziv procesa i korisnika Windows servisa sa kojim se izvršava MPW Gateway Fetcher. MPW Gateway Fetcher prima podatke od programskog paketa Infinity Gateway koji se obrađuju u procesu Gateway Wrapper. Zavisno od verzije se može koristiti naziv *mpw-gateway-fetcher-7.2* ili *mpw-gateway-fetcher-8.0* ili više.
5	*mpw-backend*	Windows naziv procesa i korisnika Windows servisa sa kojim se izvršava MPW.
6	*postgres*	Windows naziv procesa i korisnika Windows servisa sa kojim se izvršava Postgres baza podataka. Kada se radi o instalaciji u ustanovama ministarstva odbrane (Department of Defense), ne instalira se Postgres baza podataka. Umesto toga se upravljanje korisnicima prikazuje preko aktivnog direktorijuma.

4.2 Upravljanje pravima za Infinity Gateway server

Ovaj odeljak sadrži informacije o pravima pristupa za Windows korisnike ka aplikativnim podacima. Aplikativni podaci se eksplicitno određuju preko Windows sigurnosnog mehanizma (ACL).

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

Ova direktorijum sadrži aplikativne podatke koji su neophodni za rad komponente Gateway-Wrapper.

Prava pristupa:

– R/W za specijalizovano servisno osoblje
– R/O za *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Bez pristupa za neovlašćene korisnike Windows servera

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

Ova datoteka sadrži konfiguracije i podešavanja koja su neophodna za bezbedan rad softvera MPW.

Prava pristupa:

– R/W za specijalizovano servisno osoblje
– R/O za *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Bez pristupa za neovlašćene korisnike Windows servera

4.3 Upravljanje pravima za MPW server

Ovaj odeljak sadrži informacije o pravima pristupa za Windows korisnike ka aplikativnim podacima.

C:\ProgramData\mpw-pgdata

Direktorijum je mesto za skladištenje podataka banke podataka koji sadrže informacije o prijavama za MPW korisnike. Kada postoji AD konekcija na softveru MPW, onda nema direktorijuma.

Prava pristupa:

– R/W za specijalizovano servisno osoblje i *postgres*
– Bez pristupa za neovlašćene korisnike Windows servera

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

U ovoj datoteci se može konfigurisati prikaz paramtera uređaja.

Prava pristupa:

– R/W za specijalizovano servisno osoblje
– R/O za *mpw-backend*
– Bez pristupa za neovlašćene korisnike Windows servera i *postgres*

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

U ovoj datoteci su sadržani primeri konfiguracije za prikaz parametara uređaja. Datoteka se ne instalira u ustanovama ministarstva odbrane (Department of Defense).

Prava pristupa:

– R/W za specijalizovano servisno osoblje
– R/O za *mpw-backend*
– Bez pristupa za neovlašćene korisnike Windows servera i *postgres*

C:\Program Files\Draeger\MPW-Backend

Ovaj direktorijum sadrži aplikativne podatke koji su neophodni za rad softvera MPW.

Prava pristupa:

– R/W za specijalizovano servisno osoblje
– R/O za *mpw-backend*
– Bez pristupa za neovlašćene korisnike Windows servera i *postgres*

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

Ova datoteka sadrži konfiguracije i podešavanja koja su neophodna za bezbedan rad softvera MPW.

Prava pristupa:
- R/W za specijalizovano servisno osoblje
- R/O za *mpw-backend*
- Bez pristupa za neovlašćene korisnike Windows servera i *postgres*

4.4 Datoteka application.properties

4.4.1 Gateway Wrapper veb server

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

Primeri unosa	Opis
logging.level.org.springframework=INFO	Konfiguracija nivoa evidentiranja za Spring
logging.level.com.draeger=TRACE	Konfiguracija nivoa evidentiranja za MPW
server.port=8443	Port veb servera
igw.user=<Korisnik>	Infinity Gateway korisnik
igw.password=<Lozinka>	Infinity Gateway lozinka

4.4.2 MPW veb server

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

Primeri unosa	Opis
logging.level.org.springframework=INFO	Podešavanje događaja specifičnih za aplikaciju
logging.level.com.draeger=TRACE	Podešavanje nadziranih događaja specifičnih za aplikaciju
logging.level.com.draeger.upw.mpw.backend.log.session=OFF	Podešavanje za evidentiranje svih korisničkih događaja sesije
server.port=8444	Port veb servera za klijentske pregledače
mpw.session.mobile.timeout=30	Relativno vremensko ograničenje sesije za mobilne klijente
mpw.session.desktop.timeout=120	Relativno vremensko ograničenje sesije za računarske klijente
mpw.session.absolute.timeout=720	Apsolutno vremensko ograničenje sesije za sve klijente
server.ssl.keyStoreType=PKCS12	Sertifikat za Keystore tip
server.ssl.key-store-password=<Lozinka>	Lozinka za PKI sertifikat
gateway.url=https://<gateway.server.name>:8444	Informacije veze ka komponenti Gateway Wrapper
spring.datasource.password=<Lozinka>	Lozinka baze podataka u upravljanju korisnicima (ne koristi se kod AD konekcije)
spring.datasource.username=<postgres.username>	Korisnik baze podataka u upravljanju korisnicima (ne koristi se kod AD konekcije)
server.name=<MPW domain>	Naziv domena za MPW Naziv domena mora da se poklapa sa nazivom domena u sertifikatu

Primeri unosa	Opis
ad.domain	Za dodatne informacije pogledajte: "Aktivni direktorijum", str. 18.
ad.url	
ad.searchFilter	
d.groupMapping [<<AD grupa>>]=<<CareUnit>>	
ad.groupMapping[Lekari]=ICU	
ad.groupMapping[Lekari]=OP1,OP2	
ad.groupMapping[Lekari\ OP]=OP	

5 Pravila zaštitnog zida

5.1 Gateway Wrapper veb server

Standardno se aplikacija pokreće na portu 8443. Ovaj port se koristi kao standardno podešavanje u toku instalacije. Standardno podešavanje se može izmeniti preko datoteke *application.properties*. U tom cilju potražite *server.port*. Port mora da bude odobren kao "Dolazno pravilo (Inbound Rule)" (TCP).

5.2 MPW veb server

Standardno se aplikacija pokreće na portu 8444. Ovaj port se koristi kao standardno podešavanje u toku instalacije. Standardno podešavanje se može izmeniti preko datoteke *application.properties*. U tom cilju potražite *server.port*. Port mora da bude odobren kao "Dolazno pravilo (Inbound Rule)" (TCP).

5.3 Konekcije

Da bi frontend mogao da se poveže sa backendom, u mreži moraju da budu odobrene HTTPS i WSS konekcije. Kao port za WSS (Websocket ekvivalent za HTTPS) koristi se *server.port* backenda. Za dodatne informacije pogledajte: "Datoteka application.properties", str. 12.

5.4 Pravila zaštitnog zida i antivirusna zaštita

Zaštitni zid na programskom paketu Infinity Gateway i na backendu mora da dozvoljava "dolazni saobraćaj (inbound)" konfigurisanog HTTPS/WSS porta.

Sledeći antivirus skeneri su testirani za upotrebu na pozadinskom serveru:

– McAfee 5 sa srednjim stepenom detekcije

Svi direktorijumi pozadinskog servera su bezbedni za skeniranje na viruse.

6 Protokoliranje

6.1 Nivoi protokola

Sve aplikacije koje se isporučuju uz softver MPW upisuju protokole u Windows protokol događaja. Aplikacije proveravaju pri pokretanju da li sistem protokola funkcioniše. Ukoliko dođe do greške, aplikacija se ne pokreće. Greške protokola u radu mogu se pronaći u prikazu događaja (Event Viewer) u Windows sistemskom protokolu sa izvorom "Protokol događaja". MPW posle instalacije generiše sve događaje sa nivoom protokola "Information", "Warning" ili "Error". Sledeći nivoi protokola se nalaze na raspolaganju:

Nivo protokola	*application.properties*	Opis
TRACE	logging.level.org.springframework=TRACE logging.level.com.draeger=TRACE	Označava sve detaljne informacione događaje kao nivo protokola DEBUG.
DEBUG	logging.level.org.springframework=DEBUG logging.level.com.draeger=DEBUG	Označava detaljne informacione događaje koji su najkorisniji za otklanjanje grešaka u nekoj aplikaciji.
INFO	logging.level.org.springframework=INFO logging.level.com.draeger=INFO	Označava informacione poruke koje prikazuju napredak aplikacije na nediferenciranom nivou.
WARN	logging.level.org.springframework=WARN logging.level.com.draeger=WARN	Označava potencijalne situacije greške.
ERROR	logging.level.org.springframework=ERROR logging.level.com.draeger=ERROR	Označava događaje greške sa kojima aplikacija možda može da nastavi da se izvršava.

Za promenu nivoa protokola potrebno je prilagoditi datoteku *application.properties* softvera MPW i komponente Gateway Wrapper kao što je prikazano u tabeli (videti "Datoteka application.properties", str. 12). Standardno podešavanje nakon instalacije je "INFO".

6.2 Protokoliranje sesije

Protokol sesije (*mpw-backend-sessions.log*) sadrži potencijalno lične datoteke kao što su IP adresa i korisničko ime. Za deaktiviranje protokola sesije potrebno je da postoji sledeća rečenica u datoteci *application.properties*:

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

Za dodatne informacije pogledajte: "MPW veb server", str. 12.

6.3 Vremensko ograničenje sesije

Vremenska ograničenja sesije nakon instalacije poseduju standardne vrednosti 30 minuta za mobilnu aplikaciju i 120 minuta za aplikaciju za računar. Trajanje vremenskog ograničenja sesije mora da bude konfigurisano u skladu sa smernicama za zaštitu podataka zdravstvene ustanove. Vrednosti se mogu konfigurisati u datoteci *application.properties*.

application.properties	Opis
mpw.session.mobile.timeout=30	Relativno vremensko ograničenje sesije Sesija se završava nakon podešenog vremenskog trajanja ako u tom vremenu nema aktivnosti korisnika.
mpw.session.desktop.timeout=120	
mpw.session.absolute.timeout=720	Apsolutno vremensko ograničenje sesije Sesija se uvek završava nakon dostizanja podešenog vremenskog trajanja.

Jedinica su minute i moraju da se nalaze između 1 i 720 minuta.

Za dodatne informacije pogledajte: "MPW veb server", str. 12.

6.4 Pronalaženje događaja

6.4.1 Prikaz događaja

Za bolje pronalaženje MPW protokola se prilikom instalacije MPW backenda i komponente MPW Gateway Wrapper kreira posebna evidencija sa nazivom "Draeger".

Prikaz događaja operativnog sistema Windows (Event Viewer) poseduje funkcije za upravljanje protokoliranim događajima (npr. arhiviranje, rotacija, čuvanje, brisanje ili prosleđivanje događaja). Ove informacije se mogu preuzeti iz Microsoft baze znanja.

U prikazu događaja operativnog sistema Windows se događaji tipično kategorizuju na osnovu sledećih karakteristika: *Nivo*, *Izvor*, *ID događaja* i *Kategorija zadatka*. Sve do *Kategorije zadatka* se ove karakteristike mogu koristiti za filtriranje MPW protokola.

– *Kategorija zadatka* se ne koristi.
– *Izvor* odgovara nazivu MPW aplikacije i može u skladu sa tim da sadrži sledeće vrednosti: *MPW-Backend*, *Bulkport*, *PasswordResetter*, *UserAdmin*, *PostgreSQL* i *MPW-Gateway-Wrapper*.
– *ID događaja* služi za kategorizaciju sadržaja unosa protokola. U nastavku se navodi lista načina na koji se vrši kategorizacija MPW unosa protokola na osnovu karakteristike *ID događaja*.

6.4.2 ID događaja za pronalaženje događaja

Standardno podešavanje nivoa protokola je "Information" i sadrži nivoe protokola "Warning" i "Error"

ID greške	Aplikacije	Opis
10	MPW-Backend, Bulkport, PasswordResetter, UserAdmin, MPW-Gateway-Wrapper	Protokoli specifični za aplikaciju
11[1)]	MPW backend	Događaji prijave sesije (npr. uspešni i neuspešni pokušaji prijave)
0[2)]	PostgreSQL	Interna baza podataka upravljanja korisnicima za backend
12	Komunikacione informacije	IP adrese povezanih sistema. Uspešni i neuspešni pokušaji pristupa ili izmene sigurnosnih objekata.
13	Informacije sesije	Vremensko ograničenje sesije, brisanje, osvežavanje ID-a korisnika sesije
15	Autentifikacija korisnika	Uspešni, neuspešni pokušaji prijave
16	Uspešni ili neuspešni pokušaji pristupa Debug informacijama	Healthpage

1) Protokoliranje sesija mora da bude eksplicitno aktivirano, budući da protokoli sadrže korisnička imena i ID sesije. Pre aktiviranja pribaviti informacije o zakonskim propisima o zaštiti privatnosti korisnika i poštovati ove propise.
2) PostgreSQL unosi protokola dolaze direktno od PostgreSQL baze podataka. Dräger nema uticaja na sadržaj ovih unosa protokola (to je i razlog zašto je ID događaja 0). Dräger ne menja standardna podešavanja u pogledu nivoa protokola i sl. za PostgreSQL.

6.4.3 Unosi protokola izvan Dräger evidencije

Sledeći događaji se ne upisuju u Draeger evidenciju:

– Pokretanje i zaustavljanje servisa
  Windows automatski upisuje u sistemski protokol unose protokola za pokretanje i zaustavljanje instaliranih MPW servisa. Ovi unosi protokola se mogu pronaći u izvoru "Upravljač kontrole usluga (Service Control Manager)" traženjem npr. "mpw-backend" ili "mpw-gateway-wrapper".
– Izmene datoteka
  Windows može putem smernice za nadgledanje sistema datoteka (Audit File System Policy) da vrši evidentiranje pristupa datoteci npr. konfiguracionim datotekama. Odgovarajući unosi se skladište u sigurnosnom protokolu.

7 Konfiguracija

7.1 Aktivni direktorijum

Ključ	Vrednost
ad.domain	AD domen (npr. *company.com*)
ad.url	AD URL (npr. *ldaps://ad.company.com*)
ad.rootDn	RootDn za AD (kada potrebno)
ad.searchFilter	AD filter za pretraživanje kako bi se pronašli ovlašćeni korisnici u AD-u Standardno podešavanje: *(&(objectClass=user)(userPrincipalName={0}))* Kod "[...]*Name={0}*" se {0} zamenjuje prilikom pretrage sa "username@domain". Kod "[...]*Name={1}*" se *{1}* zamenjuje prilikom pretrage sa korisničkim imenom ("username").

Za utvrđivanje koja AD grupa može da vidi koju grupu radnih mseta, potrebno je u datoteci *application.properties* kreirati mapiranje između naziva AD grupe i naziva grupe radnih mesta.

Za svaku AD grupu za koju je izvršeno mapiranje, potrebno je dodati rečenicu u konfiguracionu datoteku u sledećem formatu:

ad.groupMapping[<<AD grupa>>]=<<CareUnit>>

ℹ Naziv za <<CareUnit>> mora da odgovara odgovarajućem nazivu u mreži programskog paketa Infinity Gateway.

<<AD grupa>> i *<<CareUnit>>* moraju da budu zamenjeni sa odgovarajućim nazivom. Da bi se npr. AD grupi "Lekari" obezbedio pristup grupi radnih mesta (CareUnit) "ICU", potrebno je dodati sledeću rečenicu:

ad.groupMapping[Lekari]=ICU

Ukoliko neka AD grupa treba da ima pristup ka više grupa radnih mesta, potrebno ih je navesti jednu za drugom i razdvojiti zarezom.

Primer: *ad.groupMapping[Lekari]=OP1,OP2*

Prazna mesta u nazivima AD grupa se moraju navesti sa "\" + "prazno mesto".

Primer: *ad.groupMapping[Lekari\ OP]=OP*

7.2 Uklanjanje AD korisnika

Korisnici koji su uklonjeni iz aktivnog direktorijuma a još uvek poseduju važeću korisničku sesiju, mogu se isključiti iz rada ponovnim pokretanjem Windows servisa MPW backend. Ponovno pokretanje MPW backenda dovodi do toga da sve korisničke sesije budu završene. Kada se izvrši ponovno pokretanje MPW backenda, sesija se završava najkasnije u apsolutnom vremenskom ograničenju sesije.

8 Rezervna kopija i oporavak od katastrofe

Za ponovno uspostavljanje sistema kod problema potrebno je kreirati rezervnu kopiju. Zatim je potrebno ponovo instalirati MPW i potrebno je učitati sve konfiguracione datoteke iz rezervne kopije.

Za to su potrebne sledeće konfiguracione datoteke:

Gateway

– *application.properties*

MPW backend

– *application.properties*
– *device-parameter-config-sample.csv*
– Korišćeni sertifikat. Odgovarajuća datoteka se može izmeniti u datoteci *application.properties* (standardna vrednost: *cert.p12*).

Kada se zameni kompletan hardver, potrebno je učitati licencu. Pre zamene hardvera kontaktirati specijalizovano servisno osoblje.

Kada je MPW instaliran sa internom korisničkom bazom podataka, korisnička baza podataka mora prethodno da bude sačuvana i zatim ponovo učitana. U tom cilju kontaktirati specijalizovano servisno osoblje.

9 Infrastruktura javnih ključeva

Da bi se koristio sopstveni PKI, u toku instalacije se može učitati sertifikat servera. Nakon instalacije se sertifikat u datoteci *application.properties* može naknadno izmeniti. U tom cilju je potrebno prilagoditi sledeće unose:

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

Da bi se sertifikat kategorizovao kao kredibilan, potrebno je da se naziv domena "server.name" u datoteci *application.properties* poklapa sa nazivom domena u sertifikatu.

10 Sertifikat

10.1 Instaliranje TrustedRoot unosa za MPW-TLS sertifikat na krajnjim uređajima

Ukoliko Root sertifikat bolnice nije već podeljen na krajnjim uređajima, potrebno je instalirati Root sertifikat na krajnje uređaje.

ℹ Trenutno su odobreni samo Microsoft Edge, Google Chrome i Apple Safari (iOS).

ℹ Root sertifikat nije isti kao onaj koji koristi backend. Root sertifikat je potpisao backend sertifikat.

Sertifikat je uspešno instaliran kada možete da se prijavite na uređaj. Nije dovoljno da postoji mogućnost otvaranja ekrana prijave već mora da bude moguće i izvršiti prijavu.

10.1.1 Microsoft Windows

Potrebno je obezbediti da korišćeni pregledač daje kredibilitet sertifikatu koji se koristi na serveru.

Kod ručne instalacije:

1. Klinknite dva puta na datoteku sertifikata.
   ⇒ Otvara se Windows menadžer sertifikata.
2. Dodajte sertifikat kao Root (automatsko prepoznavanje ga ne prepoznaje pravilno).

10.1.2 Apple iOS

Potrebno je obezbediti da korišćeni pregledač daje kredibilitet sertifikatu koji se koristi na serveru.

Kod ručne instalacije: Root sertifikat je prethodno potrebno poslati e-porukom poštanskom sandučetu kojem se može pristupiti sa iPhone uređaja. Sertifikat je moguće instalirati samo kada se e-poruka otvori u aplikaciji ***Mail*** i kada se izabere priloženi sertifikat. Potreban je PIN uređaja.

Klikom na sertifikat se on prvo instalira kao nekredibilan. Da bi se aktivirala kredibilnost, potreban je sledeći korak:

Podešavanja (Settings) > ***Opšta (General)*** > ***O uređaju (About)*** > ***Podešavanja sertifikata(Certificate Trust Settings)*** > ***Aktivirati pun kredibilitet za Root sertifikat (Enable full trust for root certificates)***.

Pod ***Oopšta*** > ***Profil*** se sertifikat može ponovo ukloniti.

11 Deinstalacija

Da bi u potpunosti obrisali sve osetljive podatke, Dräger preporučuje da se nakon deinstalacije softvera računar ponovo instalira.

12 Servis

12.1 Definicija servisne terminologije

Koncept	Definicija
Servis	Sve mere (pregled, održavanje, popravka) koje za svrhu imaju održavanje ili obnavljanje funkcionalnog integriteta proizvoda
Pregled	Mere koje se primenjuju u cilju utvrđivanja i procene stvarnog stanja proizvoda
Održavanje	Redovne mere namenjene za održavanje funkcionalnog integriteta proizvoda
Popravka	Mere koje se primenjuju u cilju obnavljanja funkcionalnog integriteta proizvoda nakon njegovog kvara

Preporučuje se servisni ugovor sa kompanijom Dräger.

12.2 Održavanje

Komponenta	Interval	Mera	Korisnička grupa
TLS sertifikat	Prema zahtevu klijenta	Obnova TLS sertifikata	Servisno osoblje
Hard disk	Svake 2 godine	Provera kapaciteta hard diska	Servisno osoblje
		Arhiviranje i brisanje evidencijskih datoteka, ako neophodno	

Sigurnosna ažuriranja

Servisni paketi i zakrpe kao npr. oni za Microsoft Windows zatvaraju bezbednosne propuste, otklanjaju greške ili unapređuju funkcije. Dräger omogućava kod softvera MPW instalaciju novih sigurnosnih ažuriranja. Za postupanje sa sigurnosnim ažuriranjima pratiti sledeće stavke:

- Na MPW serveru deaktivirati funkciju automatskog ažuriranja za zakrpe i servisne pakete.
- Kada se objavi novo sigurnosno ažuriranje, sačekajte odobrenje kompanije Dräger za MPW sistem. Ukoliko Dräger u roku od 4 nedelje od objavljivanja sigurnosnog ažuriranja ne saopšti nikakve zamerke, sigurnosno ažuriranje se smatra odobrenim za MPW.
- Ukoliko postoji test sistem, Dräger preporučuje da se novo sigurnosno ažuriranje testira pomoću test sistema.

13 Tehnički podaci

13.1 Sistemski zahtevi

13.1.1 Softversko okruženje i infrastruktura

Verzije programskog paketa Infinity Gateway Uključujući opciju WinAccess API	7.2, 8.0, 9.0
WLAN u području primene	
Propusni opseg	Najmanje 1 Gbit/s u mreži koja povezuje izvor podataka i server.
Portovi	8443 (standardno podešavanje), može se konfigurisati

13.1.2 Server

Server za softver (Mobile Patient Watch)

Operativni sistem	Windows Server 2016 (fizički ili virtuelni server)
Procesor	8 CPU jezgara sa 3200 MHz radnim taktom
Radna memorija (RAM)	32 GB
Hard disk SSD	2 TB

Server za Infinity Gateway

Na hardveru za Infinity Gateway mora biti instaliran dodatni softver za preuzimanje podataka, tako da su veći sistemski zahtevi u pogledu hardvera. Osim ovog softvera na istom serveru ne sme da bude instaliran drugi softver koji Infinity Gateway koristi kao izvor podataka.

Iz toga proističu sledeći sistemski zahtevi:

Operativni sistem	Windows Server 2016 (fizički ili virtuelni server)
Procesor	8 CPU jezgara sa 3000 MHz
Radna memorija (RAM)	32 GB
Hard disk SSD	60 GB

13.1.3 Krajnji uređaji

Preporučeni krajnji uređaji

Softver se može u potpunosti prikazivati i koristiti na preporučenim uređajima. Brzina krive je zagarantovana u skladu sa specifikacijama.

Mobilna aplikacija	
Operativni sistem	iOS 14
Pregledač	Apple Safari (aktuelna verzija)
Rezolucija	– 2436 x 1125 px (458 ppi) – 2532 x 1170 px (460 ppi) – 2688 x 1242 px (458 ppi)

Aplikacija za računar	
Operativni sistem	Windows 10 (aktuelna verzija)
Pregledač	Microsoft Edge (aktuelna verzija) Google Chrome (aktuelna verzija)
Rezolucija	1920 x 1080 px (24 inča)

Kompatibilni krajnji uređaji

Softver se može u potpunosti prikazivati i koristiti na kompatibilnim uređajima. Brzina krive može da se razlikuje od specifikacija ali na istom uređaju uvek ostaje konstantno visoka.

Mobilna aplikacija	
Krajnji uređaji sa operativnim sistemom iOS	
Verzija	iOS 14 i više (aktuelna verzija)
Pregledač	Apple Safari (aktuelna verzija)
Rezolucija	1136 x 640 px do 2688 x 1242 px
Gustina piksela	326 ppi do 476 ppi
Format strane	1,8:1 do 2,2:1
Krajnji uređaji sa operativnim sistemom Android	
Verzija	Android 9 i više (aktuelna verzija)
Pregledač	Chrome (aktuelna verzija)
Procesor	CPU-Octa-Core 1,6 GHz (+)
Rezolucija	1280 x 720 px do 3200 x 1440 px
Gustina piksela	294 ppi do 563 ppi
Format strane	1,8:1 do 2,2:1

Aplikacija za računar	
Operativni sistem	Windows 10 (aktuelna verzija)
Pregledač	Microsoft Edge (aktuelna verzija) Google Chrome (aktuelna verzija)
Rezolucija	Ustanova vrši izbor.

ℹ Na zahtev je dostupna tehnička dokumentacija sa dopunskim informacijama.

13.2 Radne karakteristike

Klasifikacija

Evropska klasifikacija medicinskih sredstava	Klasa IIb
UMDNS kod Universal Medical Device Nomenclature System Univerzalni sistem klasifikacije medicinskih sredstava	17223
GMDN kod Global Medical Device Nomenclature Međunarodna klasifikacija medicinskih sredstava	44101

13.2.1 Tačnost prikaza

Za opsege vrednosti poštovati tačnost prikaza kriva, numeričkih vrednosti i intervala uzorkovanja trendova koji se odnose na informacije u uputstvima za korišćenje za Mobile Patient Watch i Infinity Gateway.

13.3 Komunikacija unutar mreže

Izvor podataka:	Infinity Gateway računar sa komponentom Gateway Wrapper
Pozadinski server:	Komunicira sa programskim paketom Infinity Gateway preko enkriptovane IP konekcije na portu 8443 (standardno, može se prilagoditi prilikom instalacije).
Krajnji uređaji (personalni računari ili mobilni uređaji):	Komunicira sa pozadinskim serverom preko HTTPS konekcije i WSS konekcije na portu 8444 (standardno, može se prilagoditi prilikom instalacije).

13.4 Veze ka IT mrežama

U IT mreži, podaci mogu da se razmene putem žičanih ili bežičnih tehnologija. IT mreža može da bude bilo koji interfejs podataka koji je opisan u standardima i konvencijama.

Tokom rada, ovaj proizvod može da razmeni informacije sa drugim uređajima pomoću IT mreža i podržava sledeće funkcije:

– Prikaz talasnih oblika i podataka parametara
– Prikaz kreveta daljinskim pristupom
– Prenos podešavanja uređaja i podataka o pacijentu

Povezivanje ovog proizvoda na mrežu koja obuhvata druge uređaje ili obavljanje naknadnih izmena na toj mreži može dovesti do novih rizika za pacijenta, korisnike i treće strane. Pre nego što se proizvod poveže na mrežu ili se mreža promeni, ovi rizici moraju da se identifikuju, analiziraju, procene i da se preduzmu odgovarajuće mere.

Primeri naknadnih izmena na mreži:

– Promena mrežne konfiguracije
– Uklanjanje uređaja i softvera sa mreže
– Dodavanje novih uređaja i softvera na mrežu
– Obavljanje nadogradnji ili ažuriranja na uređajima i softveru koji su povezani na mrežu

Da bi se obezbedila bezbedna komunikacija između servera i klijenta, potrebno je da postoji TLS infrastruktura. U tom cilju na krajnjim uređajima mora da bude instaliran sertifikat.

13.4.1 Informacije o povezivanju na IT mrežu

13.4.1.1 Preduslovi

Ovaj proizvod sme da poveže na mrežu samo specijalizovano servisno osoblje. IT predstavnik zdravstvene ustanove mora unapred da se konsultuje.

Moraju se poštovati sledeći dokumenti:

– Propratna dokumentacija proizvoda
– Opisi mreže

Dräger preporučuje usklađenost sa standardom IEC 80001-1 (Primena upravljanja rizikom za IT mreže koje sadrže medicinske uređaje).

13.4.1.2 Povezivanje primarnih izvora podataka

Povezivanje se vrši isključivo preko programskog paketa Infinity Gateway. Za dodatne informacije u vezi povezivanja primarnih izvora podataka sledite informacije o proizvodu Infinity Gateway.

13.4.1.3 Povezivanje krajnjih uređaja putem mreže

– LAN mreže se obično konfigurišu u topologiji zvezde. Pojedinačni uređaji mogu da se kombinuju u grupe pomoću prekidača nivoa pristupa n. Ostali podaci o saobraćaju se izoluju pomoću odvojenih VLAN mreža. Konfigurisati mrežna podešavanja proizvoda u skladu sa ovim uputstvima za korišćenje i mrežnim specifikacijama.
– Specifikacije za LAV veze su opisane u sledećim standardima:
  – Žičane mreže: IEEE 802.3
  – Bežične mreže: IEEE 802.11 (b, g, n)
– Ukoliko se proizvod koristi sa prekidačem sloja 2 ili prekidačem sloja 3, podešavanja porta moraju da se konfigurišu na mrežnom prekidaču. Pre isporuke proizvoda, Dräger može da konfiguriše mrežna podešavanja proizvoda tako da ona budu kompatibilna sa specifikacijama ustanove.
– Ovaj proizvod razmenjuje podatke sa drugim medicinskim sredstvima preko LAN mreže. Mreža mora da podržava sledeće prenose i protokole:
  – TCP/IP
  – Unicast (statičko i dinamičko adresiranje sa komunikacionim protokolima ARP ili RARP)
  – Multicast
  – Emitovanje

- IGMP (verzija 2)

Ovaj proizvod može da pristupi ili napusti IP Multicast grupu korišćenjem komunikacionog protokola IGMP.

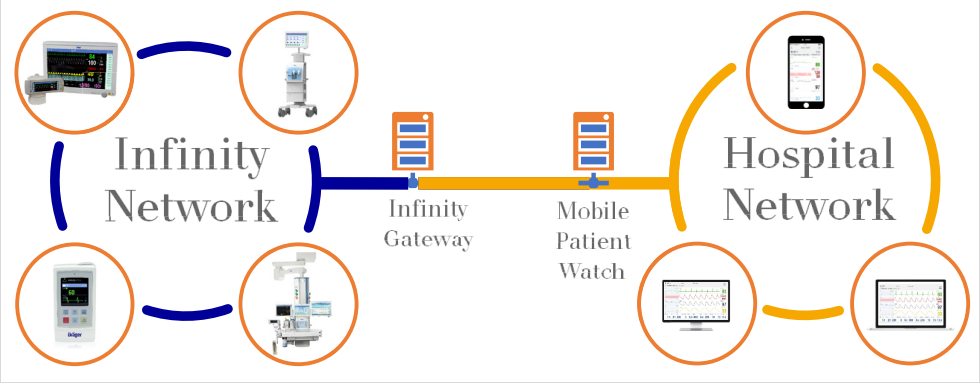
13.4.1.4 Posledice korišćenja neprikladne mreže

Ukoliko mreža ne zadovoljava zahteve, može doći do opasnih situacija. Na ovom proizvodu može doći do sledećih situacija:

- Tokom prekida mrežne veze:
  - Podaci se ne prikazuju ili se prikazuju sa zadrškom.
- Bez zaštitnog zida:
  - Podaci nisu zaštićeni.
  - Podešavanja proizvoda se menjaju.
- Podaci se šalju nepotpuni, šalju se na pogrešan proizvod ili se uopšte ne šalju.
- Podaci o pacijentu su presretnuti, falsifikovani ili oštećeni.
- Podaci imaju netačne vremenske oznake.

13.4.1.5 Potrebne karakteristike

Primarni izvori podataka i Infinity Gateway se nalaze na istoj mreži. Za ovu mrežu važe potrebne karakteristike. U tom cilju sledite informacije o proizvodu Infinity Gateway. Na MPW serveru se podaci primaju pomoću komponente MPW GatewayWrapper koja je instalirana na istom serveru kao Infinity Gateway. MPW se može koristiti na bolničkoj mreži koja povezuje sve krajnje uređaje sa MPW serverom. U tom cilju su potrebna prava pristupa.



Dodatne informacije u vezi pravila zaštitnog zida, vidi uputstvo za instalaciju "Pravila zaštitnog zida".

Mreža na kojoj je instaliran MPW i na kojoj se izvršava mora da bude pod kontrolom ustanove.

Potrebno je preduzeti odgovarajuće mere da bi se izbegao neovlašćen pristup i širenje štetnog softvera unutar mreže. Na primer moguće je preduzeti sledeće mere:

- Ograničenje fizičkog pristupa aktivnim pristupnim mrežnim utičnicama.
- Dozvoljeno je konfigurisati samo portove koji su neophodni za rad. Svi ostali portovi moraju da budu zatvoreni.

– Na mreži mogu da se nalaze samo oni uređaji koji imaju isti ili viši stepen kredibiliteta.
– Sigurna izolacija mreže (fizička ili virtuelna)
– Upotreba zaštitnog zida
– Upravljanje zakrpama za uređaje
– Implementacija u skladu sa standardom ISO/IEC 27033

13.4.1.6 Iskorišćenost mreže

Poslati podaci po pacijentu između komponente Gateway Wrapper i MPW backenda

Broj sesija pregledača	Odlazni podaci [kb/s]	Dolazni podaci [kb/s]	Vrsta podataka
1	689,63	32,11	Preneti podaci se uglavnom sastoje od relevantnih, prikazanih podataka za MPW kao što su parametri, podaci trenda i krive. Struktura testa ima protok podataka za jednog pacijenta sa 17 standardnih parametara, 4 monitoring podatka sa pripadajućim krivama i trendovima sa uzlaznim brojem sesija. Podaci prikazuju da razmena podataka između komponente Gateway Wrapper i MPW backenda ostaje približno stabilna. Kod promene istovremeno posmatranog pacijenta dolazi do povećanja razmene podataka.
2	666,8	31,00	
3	698,54	31,92	
4	652,04	30,37	

Podaci poslati između MPW backenda i klijenta

Broj sesija pregledača	Odlazni podaci [kb/s]	Dolazni podaci [kb/s]	Vrsta podataka
1	78,39	19,00	Struktura testa ostaje nepromenjena. Podaci pokazuju da razmena podataka između MPW backenda i klijenta (krajni uređaj) proporcionalno raste. Sa porastom broja sesija pregledača dolazi do povećanja razmene podataka.
2	152,64	37,31	
3	246,36	57,22	
4	317,46	72,64	

13.4.1.7 Broj podržanih uređaja

Jedna instalacija softvera može istovremeno da prikazuje podatke za maksimalno 45 radnih mesta (monitora pacijenata) na do 100 krajnjih uređaja.

Indeks

Ova strana je namerno ostavljena prazna.

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

CE 0123

www.draeger.com

9511706 – 6405.022 sr

Izdanje/Edition: 2 – 2021-03 (Izdanje/Edition: 1 – 2019-10)