Mobile Patient Watch

Informasjonssystem for pasientdata

Programvare 1.2.n

Administrasjonshåndbok

ADVARSEL
All informasjon om produktene forutsetter god kjennskap til og overholdelse av denne dokumentasjonen og produktets bruksanvisning.

Dräger. Teknikk for livet.

Denne side er tom med vilje.

Innhold

1 Informasjon om dette dokumentet

1.1 Typografisk utforming

Tekst Tekster i fet skrift eller skråstilt angir skjermtekster. Fet eller skråstilt tekst er tekst som vises på skjermen.

1. Tall med et punktum bak angir de individuelle trinnene i en prosessekvens. Nummereringen for hver nye prosessekvens starter på 1 igjen.

a. Små bokstaver med et punktum bak angir underordnede prosesstrinn. Hvert nye overordnede prosesstrinn starter med bokstaven a igjen.

● Dette kulepunktet angir individuelle prosesstrinn uten en spesifikk sekvens.

► I sikkerhetsanvisninger og advarsler angir denne trekanten måter å unngå faren.

(1) Tall i parentes viser til elementer i illustrasjoner.

1 Tall i illustrasjonene viser til elementer som beskrives i teksten.

– Bindestrek angir et intervall.

> Større enn-tegnet viser navigasjonsbanen i en dialog.

Dette symbolet angir informasjon som vil forenkle bruken av produktet.

⇒ Denne pilen angir resultatet av et prosesstrinn.

✓ Dette hakemerket angir resultatet av en sekvens av prosesstrinn.

1.2 Ytterligere dokumenter

Informasjon om bruken av dette produktet beskrives i bruksanvisningen som fulgte med produktet.

2 Sikkerhetsrelatert informasjon

2.1 Krav til brukergruppe

Begrepet "brukergruppe" beskriver ansvarlig personell som er utpekt av driftsorganisasjonen til å utføre spesifikke oppgaver på produktet.

2.1.1 Driftsorganisasjonens plikter

Driftsorganisasjonen må sørge for følgende:

– Alle målgrupper har de nødvendige kvalifikasjonene (f.eks. har gjennomgått spesialopplæring eller tilegnet seg spesialkunnskap gjennom erfaring).
– Hver målgruppe er opplært til å utføre oppgaven.
– Hver målgruppe har lest og forstått de relevante kapitlene i dette dokumentet.

2.1.2 Brukergrupper

Servicepersonell

Servicepersonell
Servicepersonell utfører følgende oppgaver:

– Konfigurerer bruker og brukerrettigheter ved hjelp av Active Directory
– Vedlikehold av operativsystemer
– Håndtering av sertifikater
– Kundespesifikke tilpasninger (f.eks. tidsavbrudd for økt)

Spesialisert servicepersonell
Hvis det kreves produktspesifikk kunnskap, må spesialisert servicepersonell utføre tiltakene. Spesialisert servicepersonell er opplært av Dräger for serviceaktiviteter på dette produktet.
Spesialisert servicepersonell utfører følgende oppgaver:

– Installasjon av produktet
– Brukerkonfigurasjon i tilfeller hvor det ikke brukes Active Directory
– Konfigurasjon av tallbaserte parametere
– Aktivering av lisenser

2.2 Informasjon om sikkerhetsinstruksjoner

Sikkerhetsinstruksjoner advarer om farer og gir instruksjoner for sikker bruk av produktet. Type fare og konsekvensene av manglende etterlevelse er beskrevet i hver sikkerhetsinstruks. Unnlatelse av å følge dem kan føre til personskade eller materielle skader.

2.3 Sikkerhetsinstruksjoner

2.3.1 Igangkjøring

Konfigurasjon og igangsetting

Igangsettingen skjer etter første gangs installasjon eller etter en oppdatering. Funksjonsfeil kan oppstå hvis installasjonen og konfigurasjonen av programvaren er ufullstendig eller feil. Funksjonsfeil kan føre til personskade.

► Les informasjonen om igangsetting av MPW og følg instruksjonene.

► Før igangsettingen må den funksjonelle integriteten til programvaren, inkludert alle tilkoblede enheter og IT-systemer, kontrolleres og godkjennes.

Utfør følgende prosesstrinn:

– Dokumenter testresultatene.

– Hvis testen er bestått og den funksjonelle integriteten er verifisert, godkjenn programvaren.

Sertifikat

Hvis sertifikatet ikke er riktig installert eller har utløpt, vil nettleseren din avvise tilkoblingen mellom klienten og nettserveren eller vise den som upålitelig.

► Servicepersonell må installere sertifikatet på riktig måte.

2.3.2 Bruk

Pasientovervåking

Hvis MPW brukes som en aktiv pasientmonitor, er det mulig at kritiske pasienttilstander ikke blir oppdaget, noe som kan føre til personskade. Programvaren skal ikke brukes som en aktiv pasientmonitor.

► Les av data fra den primære datakilden.

Behandlingsavgjørelser

Forsinket visning av data og trender eller visning av data som ikke er gyldig lenger kan føre til diagnostiske eller terapeutiske feiltolkninger som kan føre til personskade. Kontinuerlig registrerte parametre som er mer enn 15 sekunder gamle vises i grått. Dette gjelder ikke periodisk registrerte parametere, som NIBP.

► Bruk ikke dataene som vises som det eneste grunnlaget til å ta diagnostiske eller terapeutiske avgjørelser.

► Bruk den primære datakilden til å ta diagnostiske eller terapeutiske avgjørelser.

Bruksmiljø (mobil bruk)

I samsvar med retningslinjene for helseinstitusjonen kan mobile enheter kanskje ikke brukes i visse områder i helseinstitusjonen, f.eks. pga. tekniske årsaker eller pga. hygiene.

► Bruk MPW kun i de områdene av helseinstitusjonen som er ment for bruk av mobile enheter.

► Følg retningslinjene for helseinstitusjonen.

2.3.3 IT-nettverk

Feil på programvaren eller nettverket

Hvis strømforsyningen eller individuelle nettverkskomponenter svikter, kan kasusrelaterte data vises feil eller ufullstendig og føre til personskade.

► Driftsorganisasjonen må sikre at klienten er tilkoblet nettverket.

Synkronisering med en tidsserver

Et midlertidig avvik mellom den primære datakilden og klienten kan forårsake feil datavisning.

► Påse at den primære datakilden og klienten er tilkoblet den samme tidsserveren.

2.3.4 Alarmer

Programvaren utsteder verken akustiske eller visuelle alarmmeldinger eller varsler.

► Observer alarmene og varslene på den primære datakilden.

2.3.5 Service

Hvis ikke service utføres jevnlig, kan det forekomme feilfunksjoner, noe som kan resultere i personskade og materiell skade.

► Utfør service i tråd med kapittelet "Service".

2.3.6 Programvareintegritet

Hvis funksjonen for Windows File System Auditing ble konfigurert som anbefalt av Dräger ved installasjonen, loggføres tilgang til filer i programvaren med skriverettigheter, som f.eks. kjørbare filer eller DLL-er, i sikkerhetsloggen.

En oppføring i sikkerhetsloggen med en av følgende hendelses-ID-er kan henvise til uautorisert tilgang og dermed et sikkerhetsbrudd:

– 4663: Filtilgang ble oppdaget.
– 4660: Fil ble slettet.
– 4719: Auditing-innstillinger ble endret. Dette angir at Auditing-funksjonen ble slått av.
– 1102: Sikkerhetsloggen ble slettet.

► For å garantere programvarens integritet skal sikkerhetsloggen overvåkes for oppføringer med de ovenfor angitte hendelses-ID-ene i sanntid, f.eks. ved hjelp av SIEM (Security Information and Event Management).

► Oppføringer med angitte hendelses-ID-er skal analyseres for uautorisert tilgang.

3 Systemoversikt

3.1 Forutsetninger

For sikker drift må klokkeslettet avstemmes mellom den primære datakilden og MPW-serveren.

Dette oppnås ved at alle anvendte apparater (f.eks. monitorer, servere og klienter) aktiverer tidssynkronisering med en NTP-server.

Dräger anbefaler at Infinity Gateway og MPW-backendserver integreres i sykehusets IT-sikkerhetskonsept.

Alle passord skal endres etter installasjonen, for å unngå ting som "Password Guessing"angrep. Passordlengden skal aldri være under 10 tegn. Dräger anbefaler at det brukes passord som er svært ulike hverandre. Passord skal ikke gjøres tilgjengelige for uvedkommende.

3.2 Forkortelser

Forkortelse	Forklaring
ACL	Access Control List Tilgangsstyring for operativsystemet
AD	Active Directory Katalogtjeneste fra Microsoft Windows Server
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifikasjon
NTP	Network Time Protocol
PKI	Public Key Infrastruktur
R/O	Kun lesetilgang (rettighetsforvaltning)
R/W	Lese- og skrivetilgang (rettighetsforvaltning)
TCP	Transmission Control Protocol Gruppering av kommunikasjonslogger
TLS	Transport Layer Security (krypteringsprotokoll)
WSS	Web Services Security, kommunikasjonslogg

4 Programdata

4.1 Windows-brukere og Windows-brukergrupper

Følgende Windows-brukere og Windows-brukergrupper må konfigureres før drift av MPW. Brukere med ID 3,4,5 og 6 installeres sammen med MPW-Installer.

ID	Windows-bruker Windows-brukergrupper	Beskrivelse
1	Spesialisert servicepersonell	Det spesialiserte servicepersonellet installerer og vedlikeholder programvaren og installerte patcher.
2	Uautoriserte Windows Server-brukere	Alle brukere og prosesser som ikke kreves for drift av MPW.
3	*mpw-gateway-wrapper*	Windows-prosessnavn på Windows-tjenestebrukeren som MPW-Gateway-Wrapper kjører under.
4	*mpw-gateway-fetcher*	Windows-prosessnavn på Windows-tjenestebrukeren som MPW-Gateway-Fetcher kjører under. MPW-Gateway-Fetcher innhenter data fra Infinity Gateway som så behandles i Gateway-Wrapper. Avhengig av versjonen kan navnet *mpw-gateway-fetcher-7.2* eller *mpw-gateway-fetcher-8.0* og høyere brukes.
5	*mpw-backend*	Windows-prosessnavn på Windows-tjenestebrukeren som MPW kjører under.
6	*postgres*	Windows-prosessnavn på Windows-tjenestebrukeren som Postgres-databasen kjører under. Hvis det dreier seg om installasjon i en innretning hos Department of Defense (forsvarsdepartementet i USA), installeres ikke Postgres-databasen. I stedet skjer brukerforvaltningen via Active Directory.

4.2 Rettighetsforvaltning for Infinity Gateway-serveren

Dette avsnittet inneholder informasjon om Windows-brukere sine tilgangsrettigheter til programdata. Programdata må angis uttrykkelig via Windows sin sikkerhetsmekanisme (ACL).

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

Mappen inneholder programdata som kreves for kjøring av Gateway-Wrapper.

Tilgangsrettigheter:

– R/W for spesialisert servicepersonell
– R/O for *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Ingen tilgang for uautoriserte Windows Server-brukere

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

Filen inneholder konfigurasjoner og innstillinger som kreves for sikker drift av MPW.

Tilgangsrettigheter:

– R/W for spesialisert servicepersonell
– R/O for *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Ingen tilgang for uautoriserte Windows Server-brukere

4.3 Rettighetsforvaltning for MPW-serveren

Dette avsnittet inneholder informasjon om Windows-brukere sine tilgangsrettigheter til programdata.

C:\ProgramData\mpw-pgdata

Mappen er lagringsplass for databasefiler som inneholder påloggingsinformasjon for MPW-brukere. Hvis det foreligger en AD-forbindelse til MPW, eksisterer ikke denne mappen.

Tilgangsrettigheter:

– R/W for spesialisert servicepersonell og *postgres*
– Ingen tilgang for uautoriserte Windows Server-brukere

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

I denne filen kan visningen av apparatparametre konfigureres.

Tilgangsrettigheter:

– R/W for spesialisert servicepersonell
– R/O for *mpw-backend*
– Ingen tilgang for uautoriserte Windows Server-brukere og *postgres*

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

I denne filen finnes det eksempler på konfigurasjon for visningen av apparatparametre. Filen installeres ikke i innretninger hos Department of Defence (forsvarsdepartementet i USA).

Tilgangsrettigheter:

– R/W for spesialisert servicepersonell
– R/O for *mpw-backend*
– Ingen tilgang for uautoriserte Windows Server-brukere og *postgres*

C:\Program Files\Draeger\MPW-Backend

Mappen inneholder programdata som kreves for å drive MPW.

Tilgangsrettigheter:

– R/W for spesialisert servicepersonell
– R/O for *mpw-backend*
– Ingen tilgang for uautoriserte Windows Server-brukere og *postgres*

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

Filen inneholder konfigurasjoner og innstillinger som kreves for sikker drift av MPW.

Tilgangsrettigheter:

– R/W for spesialisert servicepersonell
– R/O for *mpw-backend*
– Ingen tilgang for uautoriserte Windows Server-brukere og *postgres*

4.4 Filen application.properties

4.4.1 Gateway-Wrapper-webserver

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

Eksempeloppføring	Beskrivelse
logging.level.org.springframework=INFO	Konfigurasjon av Logging-Levels for Spring
logging.level.com.draeger=TRACE	Konfigurasjon av Logging-Levels for MPW
server.port=8443	Porten til webserveren
igw.user=<bruker>	Infinity Gateway-bruker
igw.password=<passord>	Infinity Gateway-passord

4.4.2 MPW-webserver

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

Eksempeloppføring	Beskrivelse
logging.level.org.springframework=INFO	Innstilling av programspesifikke hendelser
logging.level.com.draeger=TRACE	Innstilling av programspesifikke overvåkingshendelser
logging.level.com.draeger.upw.mpw.backend.log.session=OFF	Innstilling for loggføring av alle hendelser i brukerøkter
server.port=8444	Porten til webserveren for nettleserklienter
mpw.session.mobile.timeout=30	Relativt økttidsavbrudd for mobile klienter
mpw.session.desktop.timeout=120	Relativt økttidsavbrudd for stasjonære klienter
mpw.session.absolute.timeout=720	Absolutt økttidsavbrudd for alle klienter
server.ssl.keyStoreType=PKCS12	Sertifikat av Keystore-type
server.ssl.key-store-password=<passord>	PKI-sertifikatpassord
gateway.url=https://<gateway.server.name>:8444	Tilkoblingsinformasjon for Gateway-Wrapper
spring.datasource.password=<password>	Passord til databasen i brukerforvaltningen (brukes ikke med AD-forbindelse)
spring.datasource.username=<postgres.username>	Brukernavn til databasen i brukerforvaltningen (brukes ikke med AD-forbindelse)
server.name=<MPW domain>	Domenenavn for MPW Domenenavnet må stemme overens med domenenavnet på sertifikatet
ad.domain	For mer informasjon, se: "Active Directory", side 17.
ad.url	
ad.searchFilter	
ad.groupMapping [<<AD-gruppe>>]=<<Care-Unit>>	
ad.groupMapping[Leger]=ICU	
ad.groupMapping[Leger]=OP1,OP2	
ad.groupMapping[Leger\ OP]=OP	

5 Brannmurregler

5.1 Gateway-Wrapper-webserver

Som standard startes programmet på port 8443. Denne porten brukes som standardinnstilling under installasjonen. Standardinnstillingen kan endres via filen *application.properties*. Søk da etter *server.port*. Porten må være godkjent som "Inbound Rule" (TCP).

5.2 MPW-webserver

Som standard startes programmet på port 8444. Denne porten brukes som standardinnstilling under installasjonen. Standardinnstillingen kan endres via filen *application.properties*. Søk da etter *server.port*. Porten må være godkjent som "Inbound Rule" (TCP).

5.3 Forbindelser

For at frontend skal kunne forbindes med backend må nettverket tillatte HTTPS- og WSS-tilkoblinger. Som port for WSS (Websocket-ekvivalent til HTTPS) brukes *server.port* på backend. For mer informasjon, se: "Filen application.properties", side 12.

5.4 Brannmurregler og virusbeskyttelse

Brannmuren på Infinity Gateway og backend må tillates "inbound" på den konfigurerte HTTPS-/WSS-porten.

Følgende virusskannere er teste for bruk med backend-serveren:

– McAfee 5 med middels deteksjonsnivå

Alle mapper på backend-serveren er harmløse i en virusskanning.

6 Loggføring

6.1 Loggføringsnivåer

Alle programmer som utleveres med MPW loggføres til Windows-hendelsesloggen. Programmet kontrollerer at loggføringssystemet fungerer ved oppstart. Hvis det oppstår en feil, starter ikke programmet. Loggføringsfeil under drift finner du i hendelsesoversikten (Event Viewer) i Windows-systemloggen med kilden "Hendelseslogg". MPW oppretter alle hendelser med loggføringsnivåene "Information", "Warning" eller "Error." Følgende loggføringsnivåer er tilgjengelige:

Loggføringsnivåer	***application.properties***	**Beskrivelse**
TRACE	logging.level.org.springframework=TRACE logging.level.com.draeger=TRACE	Betegner mer detaljerte informasjonhendelser enn loggføringsnivået DEBUG.
DEBUG	logging.level.org.springframework=DEBUG logging.level.com.draeger=DEBUG	Betegner mer detaljerte informasjonhendelser som er nyttige for å utbedre feil i et program.
INFO	logging.level.org.springframework=INFO logging.level.com.draeger=INFO	Betegner informasjonmeldinger som viser fremdriften til programmet på et udifferensiert nivå.
WARN	logging.level.org.springframework=WARN logging.level.com.draeger=WARN	Betegner potensielle feilsituasjoner.
ERROR	logging.level.org.springframework=ERROR logging.level.com.draeger=ERROR	Betegner oppståtte feil som programmet muligens fortsatt kan kjøres med.

For å endre loggføringsnivået må filen *application.properties* for MPW og Gateway-Wrapper tilpasses som i tabellen (se "Filen application.properties", side 12). Standardinnstillingen etter installasjonen er "INFO".

6.2 Øktloggføring

Øktloggen (*mpw-backend-sessions.log*) inneholder potensielle personopplysninger som IP-adresse og brukernavn. For å deaktivere øktloggføringen må følgende linjer finnes i filen *application.properties*:

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

For mer informasjon, se: "MPW-webserver", side 12.

6.3 Tidsavbrudd for økt

Økttidsavbruddet har standardverdien 30 minutter for mobilbruk og 120 minutter for stasjonærbruk etter installasjonen. Varigheten for økttidsavbruddet må konfigureres i henhold til personvernreglene for helseinstitusjoner. Verdien kan konfigureres i filen *application.properties*.

application.properties	Beskrivelse
mpw.session.mobile.timeout=30	Relativt økttidsavbrudd Økten avsluttes når den innstilte tidsperioden er omme, så lenge det ikke skjer noen brukerhandlinger.
mpw.session.desktop.timeout=120	
mpw.session.absolute.timeout=720	Absolutt økttidsavbrudd Økten avsluttes alltid etter at den innstilte tidsperioden er omme.

Tidsenheten er minutter, og må ligge mellom 1 og 720 minutter.

For mer informasjon, se: "MPW-webserver", side 12.

6.4 Søke opp hendelser

6.4.1 Hendelsesvisning

For en bedre søkeevne i MPW-loggene opprettes det en egen logg på den aktuelle serveren med navnet "Draeger" ved installasjonen av MPW-backend og MPW-Gateway-Wrapper.

Hendelsesvisningen for Windows (Event Viewer) har funksjoner som lar deg forvalte loggførte hendelser (f.eks. arkivering, rotering, lagring, sletting eller videresending av hendelser). Denne informasjonen finnes i Windows sin vitenskapsdatabase.

I hendelsesvisningen i Windows kategoriseres hendelser typisk basert på følgende egenskaper: *Nivå*, *Kilde*, *Hendelses-ID* og *Oppgavekategori*. Opptil *Oppgavekategori* kan disse egenskapene brukes til å filtrere MPW-logger.

– *Oppgavekategori* brukes ikke.
– *Kilde* gjelder navnene på MPW-programmer og kan dermed inneholde en av følgende verdier: *MPW-Backend*, *Bulkport*, *PasswordResetter*, *UserAdmin*, *PostgreSQL* og *MPW-Gateway-Wrapper*.
– *Hendelses-ID* brukes til innholdsmessig kategorisering av loggoppføringer. I det følgende listes det opp hvordan MPW-loggoppføringer kategoriseres i *Hendelses-ID-ene*.

6.4.2 Hendelses-ID-er for å finne hendelser

Standardinnstillingen for loggføringsnivå er "Information" og inneholder loggføringsnivåene "Warning" og "Error"

Hendelses-ID	Programmer	Beskrivelse
10	MPW-Backend, Bulkport, PasswordResetter, UserAdmin, MPW-Gateway-Wrapper	Programspesifikke logger
11[1)]	MPW-backend	Økthendelser for pålogging (f.eks. vellykkede og mislykkede påloggingsforsøk)
0[2)]	PostgreSQL	Intern brukerforvaltningsdatabase for backend
12	Kommunikasjonsinformasjon	IP-adresser og tilkoblede systemer. Vellykkede og mislykkede forsøk på tilgang til eller endring av sikkerhetsobjekter.
13	Øktinformasjon	Økttidsavbrudd, sletting eller fornyelse av brukerøkt-ID-er
15	Brukerautentisering	Vellykkede og mislykkede påloggingsforsøk
16	Vellykkede eller mislykkede forsøk på tilgang til feilsøkingsinformasjon	Helseside

1) Loggføringen for øktene må aktiveres eksplisitt, siden loggene inneholder brukernavn og økt-ID. Før aktiveringen må du innhente informasjon om lovbestemmelsene for brukernes personvern og følge disse.
2) PostgreSQL-loggoppføringer kommer direkte fra PostgreSQL-databasen. Dräger har ingen innflytelse på innholdet i disse loggoppføringene (dette er også grunnen til at hendelses-ID-en er 0). Dräger endrer heller ingen standardinnstillinger med hensyn til loggføringsnivå o.l. for PostgreSQL.

6.4.3 Loggoppføringer utenfor Dräger-loggen

Følgende hendelser føres ikke opp i Dräger-loggen:

– start og avslutning av tjenesten
  Loggoppføringer for start og avslutning av installerte MPW-tjenester loggføres automatisk til systemloggen via Windows. Disse loggoppføringene finner du i kilden "Service Control Manager" ved å søke etter f.eks. "mpw-backend" eller "mpw-gateway-wrapper".
– Filendringer
  Windows kan loggføre filtilgang via Audit File System Policy, f.eks. for konfigurasjonsfiler. Tilhørende oppføringer loggføres i sikkerhetsloggen.

7 Konfigurasjon

7.1 Active Directory

Key	Verdi
ad.domain	AD-domene (f.eks. *company.com*)
ad.url	AD-URL (f.eks. *ldaps://ad.company.com*)
ad.rootDn	RootDn for AD-er (når nødvendig)
ad.searchFilter	AD-søkefilter for å finne autoriserte brukere i AD Standardinnstilling: *(&(objectClass=user)(userPrincipalName={0}))* For "[...]*Name={0}*" erstattes {0} i søket med "user-name@domain". For "[...]*Name={1}*" erstattes *{1}* i søket med brukernavnet ("username").

For å fastsette hvilken AD-gruppe hvilke arbeidsplassgrupper kan se, må det i filen *application.properties* utføres en kartlegging mellom navnene til AD-gruppen og navnene til arbeidsplassgruppen.

For hver AD-gruppe som det utføres en kartlegging for, må det legges til en linje i konfigurasjonsfilen i følgende format:

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

ℹ Betegnelsen for <<CareUnit>> må tilsvare betegnelsen i nettverket til Infinity Gateway.

<<AD-gruppe>> og *<<CareUnit>>* må erstattes med de aktuelle navnene. For å f.eks. gi AD-gruppen "Leger" tilgang til arbeidsplassgruppen (CareUnit) "ICU", må følgende linje legges til:

ad.groupMapping[Leger]=ICU

Når en AD-gruppe skal ha tilgang til flere arbeidsplassgrupper, må disse angis etter hverandre adskilt av et komma.

Eksempel: *ad.groupMapping[Leger]=OP1,OP2*

Mellomrom i AD-gruppenavn må angis med "\" + "mellomrom".

Eksempel: *ad.groupMapping[Leger\ OP]=OP*

7.2 Fjerning av AD-brukere

Brukere som fjernes fra Active Directory og fortsatt har en gyldig brukerøkt, kan stenges ute ved å gjenstarte Windows-tjenesten MPW-backend. Slik gjenstart av MPW-backend fører til at alle brukerøkter avsluttes. Hvis det ikke utføres ny start av MPW-backend vil økten senest avsluttes ved absolutt økttidsavbrudd.

8 Sikkerhetskopi og katastrofegjenoppretting

For å kunne gjenopprette systemet ved problemer må det opprettes en sikkerhetskopi. Deretter må MPW installeres på nytt og alle konfigurasjonsfiler må legges inn fra sikkerhetskopien.

Følgende konfigurasjonsfiler kreves for å gjøre dette:

Gateway

– *application.properties*

MPW-backend

– *application.properties*
– *device-parameter-config-sample.csv*
– Det brukte sertifikatet. Den gjeldende filen kan endres i filen i *application.properties* (standardverdi: *cert.p12*).

Hvis all maskinvaren må skiftes ut, må også lisensen legges inn på nytt. Før utskifting av maskinvaren skal det spesialiserte servicepersonellet kontaktes.

Når MPW installeres med den interne brukerdatabasen, må brukerdatabasen først sikres og deretter legges inn på nytt. Kontakt da det spesialiserte servicepersonellet.

9 Public Key Infrastruktur

For å bruke egen PKI kan serversertifikatet legges inn under installasjonen. Etter installasjonen kan sertifikatet endres i filen *application.properties* i ettertid. Følgende oppføringer må da tilpasses:

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

For at sertifikatet skal klassifiseres som pålitelig, må domenenavnet "server.name" i filen *application.properties* stemme overens med domenenavnet på sertifikatet.

10 Sertifikat

10.1 Installasjon av TrustedRoot-oppføringen for MPW-TLS-sertifikatet på klienter

Hvis sykehusets rotsertifikat ikke allerede ligger på klienten, må rotsertifikatet installeres på klienten.

For øyeblikket er kun Microsoft Edge, Google Chrome og Apple Safari (iOS) tillatt.

Rotsertifikatet er ikke det samme som benyttes av backend. Rotsertifikatet har underskrevet backend-sertifikatet.

Sertifikatet har blitt installert når du kan melde deg på apparatet. Det er ikke nok at du kan åpne påloggingsskjermen, du må kunne logge deg på.

10.1.1 Microsoft Windows

Det må sikres at den brukte nettleseren stoler på serversertifikatet.

Ved manuell installasjon:

1. Dobbeltklikk på sertifikatfilen.
   ⇒ Windows-sertifikatbehandling åpnes.
2. Tilføy sertifikatet som Root (autopåvisning gjenkjenner det ikke riktig).

10.1.2 Apple iOS

Det må sikres at den brukte nettleseren stoler på serversertifikatet.

Ved manuell installasjon: Rotsertifikatet må sendes via e-post til en innboks som er tilgjengelig på din iPhone. Sertifikatet kan bare installeres når e-posten åpnes i appen ***Mail*** og det vedlagte sertifikatet velges. Du må angi telefonens PIN-kode.

Ved å klikke på sertifikatet installeres det som upålitelig. For å sette det som pålitelighet kreves følgende trinn:

Innstillinger > ***Generelt*** > ***Om*** > ***Innstillinger for sertifikatgodkjenning*** > ***Aktiver full godkjenning av rotsertifikater***.

Under ***Generelt*** > ***Profil*** kan sertifikatet fjernes igjen.

11 Avinstallasjon

For å slette alle sensitive opplysninger helt, anbefaler Dräger at datamaskinen settes opp på nytt etter avinstallasjon av programvaren.

12 Service

12.1 Definisjon av serviceterminologi

Konsept	Definisjon
Service	Alle tiltak (inspeksjon, vedlikehold, reparasjon) som er ment å vedlikeholde eller gjenopprette produktets funksjonelle integritet
Inspeksjon	Tiltak som er ment å fastslå og vurdere produktets gjeldende tilstand
Vedlikehold	Jevnlige, spesifiserte tiltak som er ment å opprettholde produktets integritet
Reparasjon	Tiltak som er ment å gjenopprette produktets funksjonelle integritet etter en feil

Det anbefales å inngå en servicekontrakt med Dräger.

12.2 Vedlikehold

Komponent	Intervall	Tiltak	Brukergruppe
TLS-sertifikat	Etter kundeangivelse	Fornyelse av TLS-sertifikatet	Servicepersonell
Harddisk	Hvert annet år	Kontroll av lagringsplass på harddisk	Servicepersonell
		Arkivering og sletting av loggfiler ved behov	

Sikkerhetsoppdateringer

Servicepakker og patcher som f.eks. fra Microsoft Windows lukker sikkerhetshull, utbedrer feil eller oppdaterer funksjoner. Dräger gir ut sikkerhetsoppdateringer for MPW helt gratis. For omgangen med sikkerhetsoppdateringer skal følgende punkter overholdes:

- Deaktiver den automatisk oppdateringsfunksjonen for patcher og servicepakker på MPW-serveren.
- Når en ny sikkerhetsoppdatering utgis, avventer du Drägers godkjennelse for MPW-systemet. Hvis Dräger ikke meddeler deg om eventuelle problemer inne 4 uker etter utgivelsen av en sikkerhetsoppdatering, er oppdateringen å anse som godkjent for MPW.
- Dersom det foreligger et testsystem, anbefaler Dräger at nye sikkerhetsoppdateringer testes på testsystemet.

13 Tekniske data

13.1 Systemkrav

13.1.1 Programvaremiljø og infrastruktur

Versjoner av Infinity Gateway Inkludert WinAccess API-alternativ	7.2, 8.0, 9.0
WLAN i bruksområdet	
Båndbredde	Minst 1 Gbit/s i nettverket som forbinder datakilden og serveren.
Porter	8443 (standardinnstilling), konfigurerbar

13.1.2 Server

Server for programvare (Mobile Patient Watch)

Operativsystem	Windows Server 2016 (fysisk eller virtuell server)
Prosessor	8 CPU-kjerne med 3200 MHz boost-takt
RAM-minne	32 GB
Harddisk SSD	2 TB

Server for Infinity Gateway

På maskinvaren til Infinity Gateway må det installeres nok en programvare for mottak av data, hvilket gjør at systemkravene for maskinvaren øker. Foruten denne programvaren, skal ingen annen programvare installeres på den serveren som Infinity Gateway bruker som datakilde.

Dette skaper følgende systemkrav:

Operativsystem	Windows Server 2016 (fysisk eller virtuell server)
Prosessor	8 CPU-kjerne med 3000 MHz
RAM-minne	32 GB
Harddisk SSD	60 GB

13.1.3 Klienter

Anbefalte klienter

Programvaren kan vises og brukes på anbefalte klienter. Sveipehastigheten angitt i spesifikasjonene garanteres.

Mobil bruk	
Operativsystem	iOS 14
Nettleser	Apple Safari (gjeldende versjon)
Grafikkoppløsning	– 2436 x 1125 px (458 ppi) – 2532 x 1170 px (460 ppi) – 2688 x 1242 px (458 ppi)

Stasjonær bruk	
Operativsystem	Windows 10 (gjeldende versjon)
Nettleser	Microsoft Edge (gjeldende versjon) Google Chrome (gjeldende versjon)
Grafikkoppløsning	1920x1080 px (24 in)

Kompatible klienter

Programvaren kan vises og brukes på kompatible klienter. Sveipehastigheten kan avvike noe fra spesifikasjonene, men forblir høy på samme klient.

Mobil bruk	
Klient med iOS-operativsystem	
Versjon	iOS 14 og høyere (gjeldende versjon)
Nettleser	Apple Safari (gjeldende versjon)
Grafikkoppløsning	1136 x 640 px til 2688 x 1242 px
Pikseltetthet	326 ppi til 476 ppi
Sideforhold	1,8:1 til 2,2:1
Klient med Android-operativsystem	
Versjon	Android 9 og høyere (gjeldende versjon)
Nettleser	Chrome (gjeldende versjon)
Prosessor	CPU-Octa-Core 1,6 GHz (+)
Grafikkoppløsning	1280 x 720 px til 3200 x 1440 px
Pikseltetthet	294 ppi til 563 ppi
Sideforhold	1,8:1 til 2,2:1

Stasjonær bruk	
Operativsystem	Windows 10 (gjeldende versjon)
Nettleser	Microsoft Edge (gjeldende versjon) Google Chrome (gjeldende versjon)
Grafikkoppløsning	Valget gjøres av operatøren.

ℹ Den tekniske dokumentasjonen med ytterligere informasjon er tilgjengelig på forespørsel.

13.2 Driftskarakteristikker

Klassifisering

Klassifisert som medisinsk utstyr i Europa	Klasse IIb
UMDNS-kode (Universal Medical Device Nomenclature System)	17223
GMDN-kode (Global Medical Device Nomenclature)	44101

13.2.1 Visningsnøyaktighet

For verdiområder, visningsnøyaktigheten for kurver, tallverdier og prøvetakingshyppigheten for trender må du overholde informasjonen i bruksanvisningen for Mobile Patient Watch og Infinity Gateway.

13.3 Kommunikasjon i nettverket

Datakilde:	Infinity Gateway-datamaskin med Gateway-Wrapper-komponenter
Backend-server:	Kommuniserer med Infinity Gateway via en kryptert IP-tilkobling på port 8443 (standard – kan tilpasses under installasjonen).
Klient (PC eller mobilenhet):	Kommuniserer med backend-server via en HTTPS-tilkobling og WSS-tilkobling på port 8444 (standard – kan tilpasses under installasjonen).

13.4 Tilkoblinger til IT-nettverk

I et IT-nettverk kan data utveksles ved hjelp av kabelbaserte eller trådløse teknologier. Et IT-nettverk kan være ethvert datagrensesnitt som er beskrevet i standarder og konvensjoner.

Under drift kan dette produktet utveksle informasjon med annet utstyr ved hjelp av IT-nettverk og støtter følgende funksjoner:

– Visninger av kurver og parameterdata
– Sengevisning via ekstern tilgang
– Overføring av enhetsinnstillinger og pasientdata

Å koble dette produktet til et nettverk som innlemmer flere enheter eller å utføre etterfølgende endringer på dette nettverket, kan føre til nye farer for pasienter, brukere og tredjepersoner. Før produktet kobles til nettverket eller nettverket endres, må disse farene identifiseres, analyseres og evalueres, og egnede tiltak må treffes.

Eksempler på etterfølgende endringer på nettverket:

– endring av nettverkskonfigurasjonen
– fjerning av enheter og programvare fra nettverket
– legge nye enheter og programvare til nettverket
– utføring av oppgraderinger eller oppdateringer av enheter og programvare som er koblet til nettverket

For å sikre en sikker kommunikasjon mellom server og klient, må det foreligge TLS-infrastruktur. For at dette skal være mulig, må et sertifikat installeres på klientene.

13.4.1 Informasjon om tilkobling til et IT-nettverk

13.4.1.1 Forutsetninger

Dette produktet må bare kobles til nettverket av spesialisert servicepersonell. Helseinstitusjonens IT-representant må konsulteres på forhånd.

Følgende dokumenter må følges:

– medfølgende dokumenter til dette produktet
– beskrivelse av nettverket

Dräger anbefaler samsvar med NEK IEC 80001-1 (risikohåndtering for IT-nettverk som omfatter medisinsk utstyr).

13.4.1.2 Tilkobling av primære datakilder

Primære datakilder kobles kun til via Infinity Gateway. For mer informasjon om tilkobling av primære datakilder, se produktinformasjonen fra Infinity Gateway.

13.4.1.3 Tilkobling av klienter via nettverk

– LAN-nettverk er normalt konfigurert i en stjerneformet nettverksstruktur. Enkelte enheter kan kombineres i grupper ved hjelp av lag-n-brytere. Annen datatrafikk er avkoblet ved hjelp av separate VLAN-nettverk. Konfigurer produktets nettverksinnstillinger i overensstemmelse med bruksanvisningen og nettverksspesifikasjonene.
– Spesifikasjoner for LAN-tilkoblinger beskrives i de følgende standardene:
  – Kablet nettverk: IEEE 802.3
  – Trådløst nettverk: IEEE 802.11 (b, g, n)
– Hvis produktet brukes med en lag-2-bryter eller en lag-3-bryter, må portinnstillingene til nettverksbryteren konfigureres. Før produktet leveres, kan Dräger konfigurere produktets nettverksinnstillinger slik at de samsvarer med driftsorganisasjonens spesifikasjoner.
– Dette produktet utveksler data med annet medisinsk utstyr via LAN-nettverket. Nettverket må støtte følgende overføringer og protokoller:
  – TCP/IP
  – Unicast (statisk eller dynamisk adressering med ARP- eller RARP-kommunikasjonsprotokoller)
  – Multicast
  – Broadcast
  – IGMP (versjon 2)

  Dette produktet kan være med i eller forlate en IP-multicast-gruppe ved hjelp av IGMP-kommunikasjonsprotokollen.

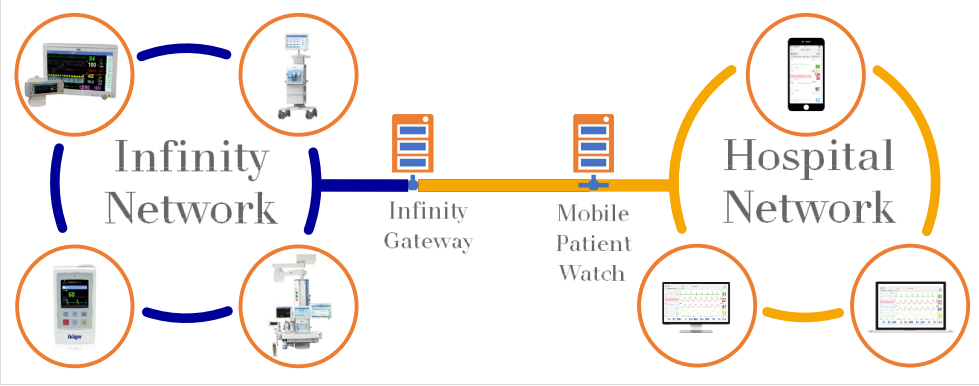
13.4.1.4 Konsekvenser av å bruke et uegnet nettverk

Hvis nettverket ikke oppfyller kravene, kan det føre til farlige situasjoner. De følgende situasjonene kan oppstå med dette produktet:

– Under et avbrudd i nettverksforbindelsen:
  – Data vises ikke eller vises med en forsinkelse.
– Uten brannmur:
  – Dataene beskyttes ikke.
  – Produktinnstillingene endres.
– Data sendes ufullstendig, sendes til feil produkt eller sendes ikke i det hele tatt.
– Pasientdata fanges opp, falsifiseres eller skades.
– Data har feil tidsstempler.

13.4.1.5 Nødvendige egenskaper

Den primære datakilden og Infinity Gateway er i samme nettverk. Dette nettverket må ha alle de nødvendige egenskapene. Mer informasjon om dette finnes i produktinformasjonen for Infinity Gateway. På MPW-serveren innhentes data ved hjelp av MPW-Gateway-Wrappers, som er installert på samme server som Infinity Gateway. MPW kan drives i et sykehusnettverk hvor alle klienter tilkobles MPW-serveren. Dette krever tilgangsrettigheter.



for mer informasjon om brannmurregler, se installasjonsanvisningene for "Brannmurregler".

Nettverket som MPW installeres og kjøres i må være underlagt operatørens kontroll.

For å unngå uautorisert tilgang og utbredelse av skadelig programvare i nettverket må det settes inn tiltak. Følgende tiltak kan eksempelvis settes inn:

- Begrensing av fysisk tilgang til aktive nettverkskontakter
- Kun porter som er nødvendige for driften konfigureres. Alle andre porter stenges.
- Kun klienter som har samme eller høyere tillitsnivå skal befinne seg i nettverket.
- Sikker isolasjon av nettverket (fysisk eller virtuell)
- Bruk av brannmur
- Patchforvaltning for klienter
- Implementering iht. NS-ISO/IEC 27033

13.4.1.6 Nettverksbruk

Data sendt mellom Gateway-Wrapper og MPW-backend per pasient

Antall nettlese-røkter	Opplasting [kb/s]	Nedlasting [kb/s]	Datatype
1	689,63	32,11	De overførte dataene består hovedsakelig av relevante, viste data for MPW som parametre, trenddata og kurver. Testoppsettet har en datagjennomstrømning for en pasient med 17 standardparametre, 4 monitordata med tilhørende kurver og trender med stigende målte øktantall. Data viser at datatrafikken mellom Gateway-Wrapper og MPW-backend forblir stabil. Ved en endring på antallet pasienter som sjekkes samtidig forutsettes det en økning i datatrafikken.
2	666,8	31,00	
3	698,54	31,92	
4	652,04	30,37	

Data sendt mellom MPW-backend og klient

Antall nettlese-røkter	Opplasting [kb/s]	Nedlasting [kb/s]	Datatype
1	78,39	19,00	Testoppsettet er uforandret. Dataene viser at datatrafikken mellom MPW-backend og klient (brukerenhet) stiger proporsjonalt. Med stigende antall nettleserøkter må man gå ut fra økning i datatrafikken.
2	152,64	37,31	
3	246,36	57,22	
4	317,46	72,64	

13.4.1.7 Antall støttede klienter

Ved å installere programvaren kan data fra maksimalt 45 arbeidsplasser (pasientmonitorer) vises samtidig på opptil 100 klienter.

Stikkordfortegnelse

B

I

S

V

Denne side er tom med vilje.

Denne side er tom med vilje.

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

CE 0123

www.draeger.com

9511700 – 6405.022 no
© Drägerwerk AG & Co. KGaA
Utgave/Edition: 2 – 2021-03 (Utgave/Edition: 1 – 2019-10)
Dräger forbeholder seg retten til å foreta endringer på det medisinske utstyret uten forvarsel.