Mobile Patient Watch

Patientdatainformationssystem

Software 1.2.n

Administrationshåndbog

ADVARSEL
Alle handlinger på produktet kræver nøje kendskab til og overholdelse af denne dokumentation og brugsanvisningen til produktet.

Dräger. Teknik for Livet.

Denne side skal være tom.

Indholdsfortegnelse

1 Information om dette dokument

1.1 Typografiske konventioner

Tekst Tekst med fed eller kursiv skrift angiver skærmtekst. Fed, kursiveret tekst angiver tekst, der vises på skærmen.

1. Tal efterfulgt af et punktum angiver de enkelte trin i en processekvens. Nummereringen af hver ny processekvens starter forfra med nummer 1.

a. Små bogstaver med punktum angiver sekundære procestrin. Bogstaveringen af hvert nyt procestrin på højere niveau starter forfra med bogstavet a.

● Dette punkttegn angiver de enkelte trin i en proces uden en bestemt rækkefølge.

► I sikkerhedsinstruktioner og advarselsbemærkninger angiver denne trekant måder at undgå farer.

(1) Numre i parenteser henviser til elementer i illustrationer.

1 Numre i illustrationer angiver elementer, der henvises til i teksten.

– Tankestreger angiver lister.

> Symbolet større end angiver navigationsstien i en dialog.

Dette symbol angiver oplysninger, der vil lette brugen af produktet.

⇒ Denne pil angiver resultatet af et procestrin.

✓ Dette afkrydsningstegn angiver resultatet af en række procestrin.

1.2 Yderligere dokumenter

Oplysninger om brug af produktet beskrives i brugsanvisningen, der leveres med produktet.

2 Sikkerhedsrelaterede oplysninger

2.1 Krav til brugergrupper

Begrebet "brugergruppe" betegner det ansvarlige personale, som er blevet tildelt udførelsen af et specifikt arbejde på produktet af driftsorganisationen.

2.1.1 Pligter for den organisation, der driver produktet

Driftsorganisationen skal sikre følgende:

– Hver brugergruppe skal have de nødvendige kvalifikationer (har f.eks. modtaget specialtræning eller opnået specialistviden gennem erfaring).
– Hver brugergruppe er blevet trænet i at udføre opgaven.
– Hver brugergruppe har læst og forstået de relevante kapitler i dette dokument.

2.1.2 Brugergrupper

Teknisk servicepersonale

Teknisk servicepersonale
Teknisk servicepersonale udfører følgende opgaver:

– Konfigurering af brugere og brugerrettigheder vha. Active Directory
– Vedligeholdelse af operativsystemerne
– Administration af certifikater
– Kundespecifikke justeringer (f.eks. sessionstimeout)

Specialiseret servicepersonale
Hvis produktspecifik viden er påkrævet, skal specialiseret teknisk servicepersonale implementere de pågældende foranstaltninger. Det specialiserede tekniske servicepersonale er uddannet af Dräger til teknisk servicering af dette produkt.
Specialiseret teknisk servicepersonale udfører følgende opgaver:

– Installation af produktet
– Brugerkonfiguration i tilfælde, hvor Active Directory ikke benyttes
– Konfiguration af numeriske parametre
– Aktivering af licenser

2.2 Information om sikkerhedsinstruktioner

Sikkerhedsinstruktioner advarer om risici og indeholder instruktioner om sikker brug af produktet. Risikotypen og konsekvensen af manglende overholdelse er beskrevet i hver enkelt sikkerhedsinstruktion. Manglende overholdelse kan medføre personskade eller materiel skade.

2.3 Sikkerhedsinstruktioner

2.3.1 Idriftsættelse

Konfiguration og idriftsættelse

Idriftsættelsen foregår efter den første installation eller efter en opdatering. Der kan opstå funktionsfejl, hvis installationen og konfigurationen af softwaren er ufuldstændig eller ukorrekt. Funktionsfejl kan resultere i personskade.

► Læs oplysningerne om idriftsættelse af MPW, og følg instruktionerne.

► Inden idriftsættelse skal softwarens funktionelle integritet kontrolleres og godkendes, herunder alle tilsluttede enheder og IT-systemer.

Udfør følgende procestrin:

– Dokumenter testresultaterne.

– Hvis testen gennemføres og den funktionelle integritet bekræftes, skal du godkende softwaren.

Certifikat

Hvis certifikatet ikke er installeret korrekt, eller hvis det er udløbet, afviser din browser forbindelsen mellem klienten og webserveren, eller den meddeler, at der ikke er tillid til den.

► Det tekniske servicepersonale skal installere certifikatet korrekt.

2.3.2 Brug

Patientmonitorering

Hvis MPW anvendes som aktiv patientmonitor, genkendes alvorlige patienttilstande muligvis ikke, hvilket kan resultere i personskade. Softwaren må ikke anvendes som en aktiv patientmonitor.

► Observer dataene fra den primære datakilde.

Behandlingsbeslutninger

Den forsinkede visning af data og trend, eller visning af data, der ikke er aktuelle, kan resultere i diagnostiske eller behandlingsmæssige fejlfortolkninger, hvilket kan medføre personskade. Kontinuerligt registrerede parametre, der er over 15 sekunder gamle, vises med gråt. Dette gælder ikke periodevist registrerede parametre såsom NIBP.

► Brug ikke udelukkende viste data som basis for diagnosticering og behandlingsmæssige beslutninger.

► Anvend den primære datakilde til diagnostiske eller behandlingsmæssige beslutninger.

Anvendelsesområde (mobil brug)

I overensstemmelse med sundhedsinstitutionens retningslinjer må mobile enheder ikke benyttes i bestemte områder af sundhedsinstitutionen, f.eks. af tekniske eller hygiejniske årsager.

► Brug kun MPW på de områder i sundhedsinstitutionen, der er beregnet til brug af mobile enheder.

► Følg sundhedsinstitutionens retningslinjer.

2.3.3 IT-netværk

Fejl i software eller på netværket

Hvis strømforsyningen eller individuelle netværkskomponenter svigter, vises sagsrelaterede data muligvis ukorrekt eller ufuldstændigt og kan resultere i personskade.

► Driftsorganisationen skal sikre, at klienten er sluttet til netværket.

Synkronisering med en tidsserver

En tidsmæssig afvigelse mellem den primære datakilde og klienten kan resultere i ukorrekt visning af data.

► Kontroller, at den primære datakilde og klienten er sluttet til samme tidsserver.

2.3.4 Alarmer

Softwaren udsender hverken akustiske eller visuelle alarmmeddelelser.

► Observer alarmerne og meddelelserne fra den primære datakilde.

2.3.5 Teknisk service

Hvis produktet ikke serviceres regelmæssigt, kan der forekomme funktionsfejl, hvilket kan resultere i personskader og materielle skader.

► Servicering skal foregå i overensstemmelse med kapitel "Teknisk service".

2.3.6 Softwareintegritet

Hvis funktionen af Windows File System Auditing er konfigureret som anbefalet af Dräger under installationen, logføres skriveadgang til softwarens filer, f.eks. eksekverbare filer eller DLL-filer, i sikkerhedsprotokollen.

En post med én af følgende hændelses-ID'er i sikkerhedsprotokollen kan tyde på uautoriseret adgang og dermed en sikkerhedsmæssig hændelse:

– 4663: Der blev registreret en filadgang.
– 4660: Filen blev slettet.
– 4719: Auditing-indstillinger blev ændret. Dette tyder på, at Auditing-funktionen er blevet deaktiveret.
– 1102: Sikkerhedsprotokollen blev slettet.

► For at sikre softwarens integritet skal sikkerhedsprotokollen overvåges for poster med de anførte hændelses-ID'er i realtid, f.eks. med SIEM (Security Information and Event Management).

► Posterne med de anførte hændelses-ID'er skal analyseres for uautoriseret adgang.

3 Systemoversigt

3.1 Forudsætninger

For at sikre sikker drift skal tiderne mellem den primære datakilde og MPW-serveren stemme overens.

Dertil bør tidssynkroniseringen med en NTP-server aktiveres på alle involverede apparater (f.eks. monitorer, servere og klienter).

Dräger anbefaler at integrere Infinity Gateway og MPW-backend-serveren i hospitalets IT-sikkerhedskoncept.

Efter installationen skal alle adgangskoder ændres for f.eks. at undgå "Password Guessing"-angreb. Adgangskoden bør ikke indeholde færre end 10 tegn. Dräger anbefaler at benytte adgangskoder, der er meget forskellige fra hinanden. Adgangskoder må ikke være tilgængelige for uautoriserede personer.

3.2 Forkortelser

Forkortelse	Forklaring
ACL	Acces Control List Operativsystemets adgangskontrol
AD	Active Directory Katalogtjeneste fra Microsoft Windows Server
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifikation
NTP	Network Time Protocol
PKI	Public-Key-infrastruktur
R/O	Kun læserettigheder (rettighedsstyring)
R/W	Læse- og skriveadgang (rettighedsstyring)
TCP	Transmission Control Protocol Gruppe af kommunikationsprotokoller
TLS	Transport Layer Security (krypteringsprotokol)
WSS	Web Services Security, kommunikationsprotokol

4 Programdata

4.1 Windows-brugere og Windows-brugergrupper

Følgende Windows-brugere og Windows-brugergrupper skal konfigureres til drift af MPW. Brugerne med ID-nr. 3, 4, 5 og 6 installeres med MPW-installationsprogrammet.

ID	Windows-brugere Windows-brugergrupper	Beskrivelse
1	Specialiseret servicepersonale	Det specialiserede tekniske servicepersonale installerer og vedligeholder softwaren og installerer programrettelser.
2	Uautoriserede Windows Server-brugere	Alle brugere og processer, der ikke er nødvendige til drift af MPW.
3	*mpw-gateway-wrapper*	Windows-procesnavn for den Windows-tjeneste-bruger, med hvilken MPW-Gateway-Wrapper udføres.
4	*mpw-gateway-fetcher*	Windows-procesnavn for den Windows-tjeneste-bruger, med hvilken MPW-Gateway-Fetcher udføres. MPW-Gateway-Fetcher modtager data fra Infinity Gateway, som behandles i Gateway-Wrapper. Afhængig af versionen kan navnet *mpw-gateway-fetcher-7.2* eller *mpw-gateway-fetcher-8.0* og højere benyttes.
5	*mpw-backend*	Windows-procesnavn for den Windows-tjeneste-bruger, med hvilken MPW udføres.
6	*postgres*	Windows-procesnavn for den Windows-tjeneste-bruger, med hvilken Postgres-databasen udføres. Hvis det drejer sig om en installation i et Department of Defense-anlæg, installeres Postgres-databasen ikke. I stedet vises brugeradministration via Active Directory.

4.2 Rettighedsstyring for Infinity-Gateway-serveren

Dette afsnit indeholder oplysninger om adgangsrettigheder for Windows-brugere til programdata. Programdataene skal eksplicit angives via Windows-sikkerhedsmekanismen (ACL).

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

Mappen indeholder programdata, der er nødvendige for drift af Gateway-Wrapper.

Adgangsrettigheder:

– R/W for specialiseret teknisk servicepersonale
– R/O for *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Ingen adgang for uautoriserede Windows-server-brugere

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

Filen indeholder konfigurationer og indstillinger, der er nødvendige for sikker drift af MPW.

Adgangsrettigheder:
– R/W for specialiseret teknisk servicepersonale
– R/O for *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Ingen adgang for uautoriserede Windows-server-brugere

4.3 Rettighedsstyring for MPW-serveren

Dette afsnit indeholder oplysninger om adgangsrettigheder for Windows-brugere til programdata.

C:\ProgramData\mpw-pgdata

Mappen er en filplacering til databasefiler, der indeholder logonoplysninger for MPW-brugere. Hvis der findes en AD-forbindelse til en MPW, eksisterer mappen ikke.

Adgangsrettigheder:
– R/W for specialiseret teknisk servicepersonale og *postgres*
– Ingen adgang for uautoriserede Windows-server-brugere

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

I denne fil kan visningen af apparatparametre konfigureres.

Adgangsrettigheder:
– R/W for specialiseret teknisk servicepersonale
– R/O for *mpw-backend*
– Ingen adgang for uautoriserede Windows-server-brugere og *postgres*

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

I denne fil findes eksempler på konfiguration af visning af apparatparametre. Filen installeres ikke i Department of Defense-anlæg.

Adgangsrettigheder:
– R/W for specialiseret teknisk servicepersonale
– R/O for *mpw-backend*
– Ingen adgang for uautoriserede Windows-server-brugere og *postgres*

C:\Program Files\Draeger\MPW-Backend

Mappen indeholder programfiler, der er nødvendige for drift af MPW.

Adgangsrettigheder:
– R/W for specialiseret teknisk servicepersonale
– R/O for *mpw-backend*
– Ingen adgang for uautoriserede Windows-server-brugere og *postgres*

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

Filen indeholder konfigurationer og indstillinger, der er nødvendige for sikker drift af MPW.

Adgangsrettigheder:

– R/W for specialiseret teknisk servicepersonale
– R/O for *mpw-backend*
– Ingen adgang for uautoriserede Windows-server-brugere og *postgres*

4.4 Filen application.properties

4.4.1 Gateway-Wrapper-webserver

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

Eksempler på poster	Beskrivelse
logging.level.org.springframework=INFO	Konfiguration af logføringsniveauer for Spring
logging.level.com.draeger=TRACE	Konfiguration af logføringsniveauer for MPW
server.port=8443	Webserverport
igw.user=<bruger>	Infinity-Gateway-bruger
igw.password=<adgangskode>	Infinity-Gateway-adgangskode

4.4.2 MPW-webserver

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

Eksempler på poster	Beskrivelse
logging.level.org.springframework=INFO	Indstilling af programspecifikke hændelser
logging.level.com.draeger=TRACE	Indstilling af programspecifikke overvågnings-hændelser
logging.level.com.draeger.upw.mpw.back-end.log.session=OFF	Indstilling af logføring for alle bruger-sessions-hændelser
server.port=8444	Webserverport for browserklienter
mpw.session.mobile.timeout=30	Relativ sessionstimeout for mobile klienter
mpw.session.desktop.timeout=120	Relativ sessionstimeout for desktop-klienter
mpw.session.absolute.timeout=720	Absolut sessionstimeout for alle klienter
server.ssl.keyStoreType=PKCS12	Certifikat af Keystore-type
server.ssl.key-store-password=<password>	PKI-certifikat-adgangskode
gateway.url=https://<gateway.server.name>:8444	Forbindelsesoplysninger for Gateway-Wrapper
spring.datasource.password=<adgangskode>	Databasens adgangskode i brugeradministratio-nen (benyttes ikke ved en AD-forbindelse)
spring.datasource.username=<postgres.user-name>	Databasens bruger i brugeradministrationen (benyttes ikke ved en AD-forbindelse)
server.name=<MPW domain>	Domænenavn for MPW Domænenavnet skal stemme overens med domænenavnet i certifikatet

Eksempler på poster	Beskrivelse
ad.domain	For yderligere oplysninger, se: "Active Directory", side 18.
ad.url	
ad.searchFilter	
ad.groupMapping [<<AD-gruppe>>]=<<CareU-nit>>	
ad.groupMapping[læger]=ICU	
ad.groupMapping[læger]=OP1,OP2	
ad.groupMapping[læger\ OP]=OP	

5 Firewallregler

5.1 Gateway-Wrapper-webserver

Som standard starter programmet på port 8443. Denne port benyttes som standardindstilling under installationen. Standardindstillingen kan være ændret vha. filen *application.properties* . Dertil skal *server.port* findes. Porten skal være frigivet som "Inbound Rule" (TCP).

5.2 MPW-webserver

Som standard starter programmet på port 8444. Denne port benyttes som standardindstilling under installationen. Standardindstillingen kan være ændret vha. filen *application.properties* . Dertil skal *server.port* findes. Porten skal være frigivet som "Inbound Rule" (TCP).

5.3 Forbindelser

For at Frontend kan forbindes med Backend, skal HTTPS- og WSS-forbindelser i netværket være tilladt. Som port for WSS (Websocket-ækvivalent til HTTPS) benyttes *server.port* for Backend. For yderligere oplysninger, se: "Filen application.properties", side 12.

5.4 Firewallregler og virusbeskyttelse

Firewallen på Infinity Gateway og Backend skal begge "inbound" tillade den konfigurerede HTTPS/WSS-port.

Følgende virusscanner er testet til brug på Backend-serveren:

– McAfee 5 med medium påvisningsniveau

En antivirusscanning kan udføres sikkert på alle Backend-serverens mapper.

6 Logføring

6.1 Logføringsniveauer

Samtlige programmer, der leveres med MPW, skriver protokollerne i Windows-hændelsesloggen. Programmerne kontrollerer ved opstart, om protokolsystemet fungerer. Hvis der opstår en fejl, starter programmet ikke. Protokolfejl under drift kan findes i logbogen (Event Viewer) i Windows-systemloggen med kilden "Hændelseslog". Efter installationen opretter MPW alle hændelser med logføringsniveauet "information", "advarsel" eller "fejl." Der er følgende mulige logføringsniveauer:

Logføringsniveau	*application.properties*	Beskrivelse
TRACE	logging.level.org.springframework=TRACE logging.level.com.draeger=TRACE	Betegner mere detaljerede informationshændelser end logføringsniveauet DEBUG.
DEBUG	logging.level.org.springframework=DEBUG logging.level.com.draeger=DEBUG	Betegner detaljerede informationshændelser, som er mest relevante ved fjernelse af fejl i et program.
INFO	logging.level.org.springframework=INFO logging.level.com.draeger=INFO	Betegner oplysningsmeddelelser, der viser programstatus på et udifferentieret niveau.
WARN	logging.level.org.springframework=WARN logging.level.com.draeger=WARN	Betegner situationer, der kan være fejlbehæftede.
ERROR	logging.level.org.springframework=ERROR logging.level.com.draeger=ERROR	Betegner fejlhændelser, med hvilke programmet muligvis kan fortsættes.

For at kunne ændre logføringsniveauet skal filen *application.properties* fra MPW og Gateway-Wrapper tilpasses som i tabellen (se "Filen application.properties", side 12). Standardindstillingen efter installationen er "INFO".

6.2 Logføring af sessioner

Sessionsloggen (*mpw-backend-sessions.log*) indeholder data, der kan indeholde personoplysninger, som f.eks. IP-adresse og brugernavn. For at deaktivere sessionsloggen skal følgende linje stå i filen *application.properties*:

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

For yderligere oplysninger, se: "MPW-webserver", side 12.

6.3 Sessionstimeout

Efter installationen har sessionstimeout standardværdierne 30 minutter for mobil brug og 120 minutter for desktop-brug. Tiden for sessionstimeout skal konfigureres iht. sundhedsinstitutionens regler om databeskyttelse. Værdierne kan konfigureres i filen *application.properties*.

application.properties	Beskrivelse
mpw.session.mobile.timeout=30	Relativ sessionstimeout Sessionen afsluttes efter den indstillede tid, hvis der ikke har været brugerhandlinger i denne tid.
mpw.session.desktop.timeout=120	
mpw.session.absolute.timeout=720	Absolut sessionstimeout Sessionen afsluttes altid, når den indstillede tid er gået.

Enheden er minutter, og værdien skal ligge mellem 1 og 720 minutter.

For yderligere oplysninger, se: "MPW-webserver", side 12.

6.4 Søgning efter hændelser

6.4.1 Logbog

Under installationen af MPW-Backend og MPW-Gateway-Wrapper oprettes en egen logfil med navnet "Draeger" på den pågældende server for bedre at kunne finde MPW-protokollerne.

Windows-logbogen (Event Viewer) har funktioner til administration af logførte hændelser (f.eks. arkivering, rotation, lagring, sletning eller videresendelse af hændelser). Disse oplysninger kan findes i Microsoft-videnbasen.

I Windows-logbogen kategoriseres hændelser sædvanligvis efter følgende egenskaber: *niveau*, *kilde*, *hændelses-ID* og *opgavekategori*. Med undtagelse af *opgavekategori* kan alle disse egenskaber benyttes til at filtrere MPW-logfiler.

– *Opgavekategori* benyttes ikke.
– *Kilde* svarer til MPW-programmets navn og kan derfor indeholde en af følgende værdier: *MPW-Backend*, *Bulkport*, *PasswordResetter*, *UserAdmin*, *PostgreSQL* og *MPW-Gateway-Wrapper*.
– *Hændelses-ID* benyttes til indholdsmæssig kategorisering af logfilposter. Nedenfor er anført, hvordan MPW-logfilposter kategoriseres vha. *hændelses-ID'er*.

6.4.2 Hændelses-ID'er til søgning på hændelser

Standardindstillingen for logføringsniveau er "Information" og indeholder logføringsniveauerne "Advarsel" og "Fejl"

Hændelses-ID	Programmer	Beskrivelse
10	MPW-Backend, Bulkport, PasswordResetter, UserAdmin, MPW-Gateway-Wrapper	Programspecifikke logfiler

Hændelses-ID	Programmer	Beskrivelse
11[1)]	MPW-Backend	Sessionshændelser om logon (f.eks. fuldførte og mislykkede logon-forsøg)
0[2)]	PostgreSQL	Intern database for Backends brugeradministration
12	Kommunikationsoplysninger	IP-adresser for tilsluttede systemer. Fuldførte og mislykkede forsøg på at opnå adgang til eller ændre sikkerhedsobjekter.
13	Sessionsoplysninger	Sessionstimeout, sletning, fornyelse af brugersessions-ID'er
15	Brugergodkendelse	Fuldførte, mislykkede logon-forsøg
16	Fuldførte eller mislykkede forsøg på at opnå adgang til fejlfindingsoplysninger	Healthpage

1) Logføring af sessionerne skal aktiveres eksplicit, da logfilerne indeholder brugernavn og sessions-ID. Før aktiveringen skal der indhentes informationer om lovforskrifter til beskyttelse af brugernes privatliv, og disse lovforskrifter skal overholdes.
2) PostgreSQL-logfilposter kommer direkte fra PostgreSQL-databasen. Dräger har ingen indflydelse på indholdet af disse logfilposter (det er også grunden til, at hændelses-ID'et er 0). Dräger ændrer heller ingen standardindstillinger mht. logføringsniveau eller lign. for PostgreSQL.

6.4.3 Logfilposter ikke medtaget i Dräger-logfilen

Følgende hændelser skrives ikke i Dräger-logfilen:

– Opstart og afslutning af tjenester
  Logfilposter om opstart og afslutning af de installerede MPW-tjenester skrives automatisk af Windows i systemloggen. Disse logfilposter kan findes under kilden "Service Control Manager" ved at søge efter f.eks. "mpw-backend" eller "mpw-gateway-wrapper".
– Filændringer
  Windows kan logføre filadgang til f.eks. konfigurationsfiler via Audit File System Policy. De tilhørende poster gemmes i sikkerhedsprotokollen.

7 Konfiguration

7.1 Active Directory

Key	Værdi
ad.domain	AD-domain (f.eks. *company.com*)
ad.url	AD-URL (f.eks. *ldaps://ad.company.com*)
ad.rootDn	RootDn for AD (om nødvendigt)
ad.searchFilter	AD-søgefilter til at finde autoriserede brugere i AD Standardindstilling: *(&(objectClass=user)(userPrincipalName={0}))* Ved "[...]*Name={0}*" udskiftes {0} ved søgningen med "username@domain". Ved "[...]*Name={1}*" udskiftes *{1}* ved søgningen med brugernavnet ("username").

For at fastlægge hvilken arbejdspladsgruppe de enkelte AD-grupper kan se, skal der oprettes en tilknytning i filen *application.properties* mellem navnet på AD-gruppen og navnet på arbejdspladsgruppen.

For hver AD-gruppe, som der skal oprettes en tilknytning for, skal der tilføjes en linje i konfigurationsfilen med følgende format:

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

ℹ Betegnelsen for <<CareUnit>> skal stemme overens med den pågældende betegnelse i Infinity Gateway-netværket.

<<AD-gruppe>> og *<<CareUnit>>* skal udskiftes med det pågældende navn. For f.eks. at give AD-gruppen "Læger" adgang til arbejdspladsgruppen (CareUnit) "ICU", skal der tilføjes følgende linje:

ad.groupMapping[Læger]=ICU

Hvis en AD-gruppe skal have adgang til flere arbejdspladsgrupper, skal de angives efter hinanden adskilt med et komma.

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

Mellemrum i AD-gruppenavnet skal angives med "\" + "mellemrum".

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

7.2 Fjernelse af AD-brugere

Brugere, der er fjernet fra Active Directory og stadigvæk har en gyldig brugersession, kan udelukkes fra drift ved at genstarte Windows-servicen MPW-Backend. Genstart af MPW-Backend bevirker, at alle brugersessioner lukkes. Hvis der ikke foretages en genstart af MPW-Backend, lukkes sessionen senest, når det absolutte sessionstimeout er nået.

8 Sikkerhedskopi og genoprettelse efter nedbrud

Der skal oprettes en sikkerhedskopi for at kunne geninstallere systemet i tilfælde af problemer. Derefter skal MPW geninstalleres, og alle konfigurationsfiler skal importeres fra sikkerhedskopien.

Dertil kræves følgende konfigurationsfiler:

Gateway

– *application.properties*

MPW-Backend

– *application.properties*
– *device-parameter-config-sample.csv*
– Det anvendte certifikat. Den pågældende fil kan ændres i filen *application.properties* (standardværdi: *cert.p12*).

Hvis hele hardwaren udskiftes, skal licensen geninstalleres. Kontakt specialiseret teknisk servicepersonale før udskiftning af hardwaren.

Hvis MPW er blevet installeret med den interne brugerdatabase, skal den først sikres som kopi og derefter geninstalleres. Kontakt specialiseret teknisk servicepersonale.

9 Public-Key-infrastruktur

For at kunne bruge den egne PKI kan servercertifikatet importeres under installationen. Efter installationen kan certifikatet ændres i filen *application.properties*. Dertil skal følgende poster tilpasses:

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

For at kunne kvalificere certifikatet som pålideligt skal domænenavnet "server.name" i filen *application.properties* stemme overens med domænenavnet i certifikatet.

10 Certifikat

10.1 Installation af TrustedRoot-posten for MPW-TLS-certifikatet på klienter

Hvis hospitalets rodcertifikat ikke allerede er distribueret til klienterne, skal rodcertifikatet installeres på klienterne.

I øjeblikket er kun Microsoft Edge, Google Chrome og Apple Safari (iOS) tilladt.

Rodcertifikatet er ikke det samme som det, der benyttes af Backend. Rodcertifikatet har underskrevet Backend-certifikatet.

Certifikatet er blevet installeret korrekt, når man kan logge sig på apparatet. Det er ikke tilstrækkeligt at kunne åbne logon-skærmen. Man skal kunne logge sig på.

10.1.1 Microsoft Windows

Det skal sikres, at den anvendte browser har tillid til det certifikat, der benyttes på serveren.

Ved manuel installation:

1. Dobbeltklik på certifikatfilen.
   ⇒ Windows Certifikatstyring åbnes.
2. Tilføj certifikatet som rod (den automatiske genkendelse genkender det ikke korrekt).

10.1.2 Apple iOS

Det skal sikres, at den anvendte browser har tillid til det certifikat, der benyttes på serveren.

Ved manuel installation: Rodcertifikatet skal først sendes pr. e-mail til en postkasse, som der er adgang til fra en iPhone. Certifikatet kan kun installeres, hvis e-mailen åbnes i appen ***Mail***, og det vedhæftede certifikat vælges. Apparat-PIN er nødvendig.

Når der klikkes på certifikatet, installeres det først som ikke-pålideligt. Udfør følgende trin for at aktivere det som pålideligt:

Indstillinger > ***Generelt*** > ***Om*** > ***Indst. til certifikatgodkendelse*** > ***Slå Fuld godkendelse af rodcertifikater til***.

Under ***Generelt*** > ***Profil*** kan certifikatet fjernes igen.

11 Fjernelse af installation

For at fjerne alle følsomme data anbefaler Dräger at geninstallere computeren efter fjernelsen af softwaren.

12 Teknisk service

12.1 Definition af begreber inden for teknisk service

Koncept	Definition
Teknisk service	Alle tiltag (kontrol, vedligeholdelse, reparation), der er beregnet til at bevare eller genoprette produktets funktion
Kontrol	Tiltag til bestemmelse af et produkts aktuelle tilstand
Vedligeholdelse	Regelmæssige, specificerede tiltag til opretholdelse af produktets funktion
Reparation	Tiltag til genoprettelse af produktets funktion efter en apparatfejl

Det anbefales, at der indgås en servicekontrakt med Dräger.

12.2 Vedligeholdelse

Komponent	Interval	Tiltag	Brugergruppe
TLS-certifikat	Efter kundens ønske	Fornyelse af TLS-certifikat	Teknisk servicepersonale
Harddisk	Hvert 2. år	Kontrol af harddiskkapacitet	Teknisk servicepersonale
		Arkivering og sletning af logføringsfiler om nødvendigt	

Sikkerhedsopdateringer

Servicepakker og programrettelser fra f.eks. Microsoft Windows afhjælper sikkerhedsproblemer, retter fejl eller forbedrer funktioner. Dräger frigiver installationen af nye sikkerhedsopdateringer til MPW. Følgende punkter skal overholdes mht. sikkerhedsopdateringer:

- Deaktiver den automatiske opdateringsfunktion på MPW-serveren for servicepakker og programrettelser.
- Når der offentliggøres en ny sikkerhedsopdatering, skal der afventes frigivelse fra Dräger for MPW-systemet. Hvis Dräger ikke meddeler nogen indsigelser inden for 4 uger efter offentliggørelse af en sikkerhedsopdatering, gælder den som frigivet for MPW.
- Hvis der findes et testsystem, anbefaler Dräger at teste den nye sikkerhedsopdatering på testsystemet.

13 Tekniske data

13.1 Systemkrav

13.1.1 Softwaremiljø og infrastruktur

Versioner af Infinity Gateway Inklusive tilvalget WinAccess API	7.2, 8.0, 9.0
WLAN i anvendelsesområde	
Båndbredde	Mindst 1 Gbit/s i det netværk, som forbinder datakilderne og serveren med hinanden.
Porte	8443 (standardindstilling), konfigurerbar

13.1.2 Server

Server til software (Mobile Patient Watch)

Operativsystem	Windows Server 2016 (fysisk eller virtuel server)
Processor	8 CPU-kerner med en boostfrekvens på 3200 MHz
Arbejdshukommelse (RAM)	32 GB
Harddisk SSD	2 TB

Server til Infinity Gateway

På hardwaren for Infinity Gateway skal der være installeret en yderligere software til modtagelse af data. Derved forhøjes systemkravene. Der må ikke være andet end denne software på den samme server, som bruger Infinity Gateway som datakilde.

Dette resulterer i følgende systemkrav:

Operativsystem	Windows Server 2016 (fysisk eller virtuel server)
Processor	8 CPU-kerner med 3000 MHz
Arbejdshukommelse (RAM)	32 GB
Harddisk SSD	60 GB

13.1.3 Klienter

Anbefalede klienter

Softwaren kan anvendes og vises fuldstændigt på anbefalede apparater. Den specificerede sweep-hastighed er garanteret.

Mobil brug	
Operativsystem	iOS 14
Browser	Apple Safari (gældende version)
Grafikopløsning	– 2436 x 1125 px (458 ppi) – 2532 x 1170 px (460 ppi) – 2688 x 1242 px (458 ppi)

Desktop-brug	
Operativsystem	Windows 10 (gældende version)
Browser	Microsoft Edge (gældende version) Google Chrome (gældende version)
Grafikopløsning	1920 x 1080 px (24 in)

Kompatible klienter

Softwaren kan anvendes og vises fuldstændigt på kompatible apparater. Sweep-hastigheden kan afvige fra den specificerede værdi, men er dog altid lige høj på det samme apparat.

Mobil brug	
Klienter med operativsystemet iOS	
Version	iOS 14 og højere (aktuel version)
Browser	Apple Safari (gældende version)
Grafikopløsning	1136 x 640 px til 2688 x 1242 px
Pixeltæthed	326 ppi til 476 ppi
Billedformat	1,8:1 til 2,2:1
Klienter med operativsystemet Android	
Version	Android 9 og højere (aktuel version)
Browser	Chrome (aktuel version)
Processor	CPU-Octa-Core 1,6 GHz (+)
Grafikopløsning	1280 x 720 px til 3200 x 1440 px
Pixeltæthed	294 ppi til 563 ppi
Billedformat	1,8:1 til 2,2:1

Desktop-brug	
Operativsystem	Windows 10 (gældende version)
Browser	Microsoft Edge (gældende version) Google Chrome (gældende version)
Grafikopløsning	Vælges af driftsorganisationen.

ℹ Den tekniske dokumentation med yderligere information er tilgængelig efter anmodning.

13.2 Driftsparametre

Klassifikation

Europæisk klassifikation af medicinsk udstyr	Klasse IIb
UMDNS-kode, Universal Medical Device Nomenclature System (Universelt nomenklatursystem for medicinsk udstyr)	17223
GMDN-kode, Global Medical Device Nomenclature (Global nomenklatur for medicinsk udstyr)	44101

13.2.1 Visningsnøjagtighed

For værdiintervaller, visningsnøjagtighed af kurver, numeriske værdier og prøveudtagningshastigheden i trend skal oplysningerne i brugsanvisningen til Mobile Patient Watch og Infinity Gateway overholdes.

13.3 Kommunikation i netværket

Datakilde:	Infinity Gateway-computer med Gateway-Wrapper-komponent
Backend-server:	Kommunikerer med Infinity Gateway via en krypteret IP-forbindelse på port 8443 (standardindstilling, der kan tilpasses under installationen).
Klienter (PC eller mobile enheder):	Kommunikerer med Backend-serveren via en HTTPS-forbindelse og en WSS-forbindelse på port 8444 (standardindstilling, der kan tilpasses under installationen).

13.4 Tilslutning til IT-netværk

I et IT-netværk kan data udveksles via forbundne eller trådløse teknologier. Et IT-netværk kan være en hvilken som helst databrugerflade, der er beskrevet i standarder og konventioner.

Under drift kan produktet udveksle information med andre apparater ved hjælp af IT-netværk, og understøtter følgende funktioner:

– Visning af kurver og parameterdata
– Sengevisning via fjernbetjening
– Overførsel af apparatindstillinger og patientdata

Tilslutning af produktet til et netværk, der har andre apparater tilsluttet, eller efterfølgende ændringer på dette netværk kan medføre nye risici for patienter, brugere og tredjeparter. Før produktet tilsluttes et netværk, eller netværket ændres, skal disse risici identificeres, analyseres og evalueres, og der skal tages passende foranstaltninger.

Eksempler på efterfølgende ændringer på netværket:

– Ændring af netværkskonfigurationen
– Fjernelse af apparater og software fra netværket
– Tilføjelse af nye apparater og software til netværket
– Opgraderinger eller opdateringer af apparater og software, der er tilsluttet netværket

For at garantere sikker kommunikation mellem server og klient skal der være en TLS-infrastruktur. Før dette er muligt, skal der være installeret et certifikat på klienterne.

13.4.1 Information om tilslutning til et IT-netværk

13.4.1.1 Forudsætninger

Det er kun specialiseret teknisk servicepersonale, der må slutte dette produkt til netværket. Sundhedsinstitutionens IT-ansvarlige skal konsulteres først.

Følgende dokumenter skal overholdes:

– Medfølgende dokumenter til dette produkt
– Beskrivelser af netværket

Dräger anbefaler overholdelse af IEC 80001-1 (risikostyring inden for IT-netværk indbefattende medicinsk udstyr).

13.4.1.2 Tilslutning af primære datakilder

Primære datakilder tilsluttes kun via Infinity Gateway. For yderligere information om tilslutning af primære datakilder henvises til produktinformationen fra Infinity Gateway.

13.4.1.3 Tilslutning af klienter via netværk

– LAN-netværk konfigureres normalt i en stjernetopologi. Individuelle apparater kan kombineres i grupper ved hjælp af lag n-switches. Anden datatrafik afkobles ved hjælp af VLAN-netværk. Konfigurering af netværksindstillinger for produktet skal ske i overensstemmelse med denne brugsanvisning samt netværksspecifikationerne.
– Specifikationer for LAN-tilslutninger er beskrevet i følgende standarder:
  – Kablede netværk: IEEE 802.3
  – Trådløse netværk: IEEE 802.11 (b, g, n)
– Hvis produktet bruges med en lag 2-switch eller en lag 3-switch, skal portindstillingerne konfigureres på netværksswitchen. Før forsendelse af produktet kan Dräger konfigurere netværksindstillingerne på produktet, så de er kompatible med specifikationerne i driftsorganisationen.
– Produktet udveksler data med andet medicinsk udstyr over LAN-netværket. Netværket skal understøtte følgende transmissioner og protokoller:
  – TCP/IP
  – Unicast (statik eller dynamisk adressering med ARP- eller RARP-kommunikationsprotokoller)
  – Multicast
  – Broadcast

- IGMP (version 2)

  Produktet kan indgå i eller forlade en IP-multicastgruppe ved brug af IGMP-kommunikationsprotokollen.

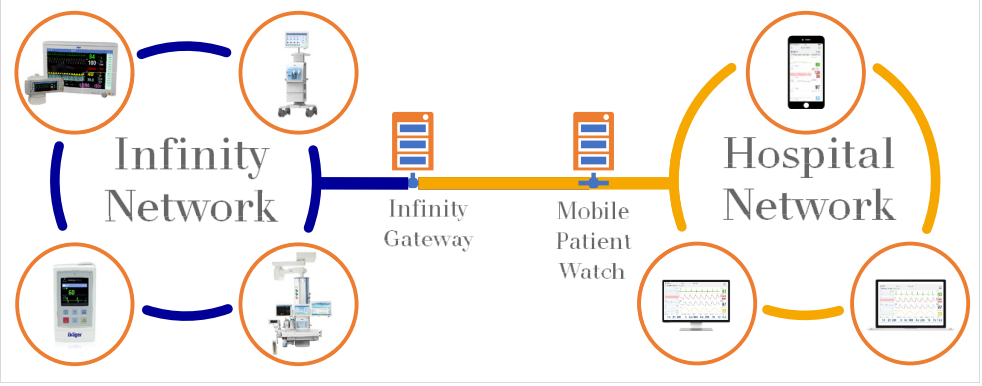
13.4.1.4 Konsekvenser ved brug af et uegnet netværk

Hvis netværk ikke overholder kravene, kan der opstå farlige situationer. Der kan opstå følgende situationer med dette produkt:

- Under en afbrydelse af netværksforbindelsen:
  - Data vises ikke eller vises med forsinkelse.
- Uden en firewall:
  - Data er ikke beskyttet.
  - Produktindstillinger ændres.
- Der sendes ufuldstændige data, de sendes til det forkerte produkt eller slet ikke.
- Patientdata opsnappes, forfalskes eller beskadiges.
- Data har forkerte tidsstempler.

13.4.1.5 Påkrævede egenskaber

De primære datakilder og Infinity Gateway befinder sig i det samme netværk. De påkrævede egenskaber gælder for dette netværk. Overhold produktoplysningerne for Infinity Gateway. På MPW-serveren modtages data vha. MPW-Gateway-Wrapper, som er installeret på den samme server som Infinity Gateway. MPW kan benyttes i et hospitalsnetværk, som forbinder alle klienter med MPW-serveren. Dertil kræves følgende adgangsrettigheder.



Yderligere oplysninger om firewallregler findes i installationsvejledningen under "Firewallregler".

Det netværk, hvori MPW installeres og benyttes, skal kontrolleres af driftsorganisationen.

Der skal træffes forholdsregler for at undgå uautoriseret adgang og spredning af skadelig software i netværket. Der kan f.eks. træffes følgende forholdsregler:

- Begrænsning af den fysiske adgang til aktive netværksudgange
- Kun de porte, der er nødvendige til driften, konfigureres. Alle andre porte skal lukkes.
- Kun apparater, der har den samme eller et højere tillidsniveau, må befinde sig i netværket.

– Sikker isolering af netværket (fysisk eller virtuelt)
– Anvendelse af en firewall
– Administration af programrettelser
– Implementering iht. ISO/IEC 27033

13.4.1.6 Udnyttelse af netværk

Mellem Gateway-Wrapper og MPW-Backend sendte data pr. patient

Antal browser-sessioner	Upstream [kb/s]	Downstream [kb/s]	Datatype
1	689,63	32,11	Størstedelen af de overførte data består af de relevante data, som skal vises på MPW, såsom parametre, trenddata og kurver. Testopsætningen målte overførselshastigheden for en patient med 17 standardparametre, 4 monitoreringsdata med tilhørende kurver og trends med stigende sessionsantal. Disse data viser, at datatrafik mellem Gateway-Wrapper og MPW- Backend forbliver relativt stabil. Der kan forventes en øget datatrafik, hvis antallet af samtidigt viste patienter ændres.
2	666,8	31,00	
3	698,54	31,92	
4	652,04	30,37	

Data, der sendes mellem MPW-Backend og klienten

Antal browser-sessioner	Upstream [kb/s]	Downstream [kb/s]	Datatype
1	78,39	19,00	Testopstillingen er uforandret. Dataene viser, at datatrafik mellem MPW-Backend og klient stiger proportionalt. Med stigende antal browsersessioner kan der forventes øget datatrafik.
2	152,64	37,31	
3	246,36	57,22	
4	317,46	72,64	

13.4.1.7 Antal understøttede apparater

Ved at installere softwaren kan data fra maksimalt 45 arbejdspladser (patientmonitorer) vises samtidigt på op til 100 klienter.

Indeks

Denne side skal være tom.

Denne side skal være tom.

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

CE 0123

www.draeger.com

9511695 – 6405.022 da

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