Mobile Patient Watch

Информационна система за данни на пациента

Софтуер 1.2.n

Наръчник за администриране

ПРЕДУПРЕЖДЕНИЕ
Всички работи по продукта предполагат точно познаване и спазване на тази документация и на ръководството за работа на продукта.

Техника за живота.

Тази страница умишлено е оставена празна.

Съдържание

1 Информация за този документ

1.1 Типографски конвенции

Текст Текстовете в удебелен шрифт или в курсив са екранни текстове. Удебеленият шрифт заедно с курсив означава текстове, които се показват на екрана.

1. Цифрите с точка след тях обозначават отделните стъпки в последователността на процеса. Номерирането за всяка последователност на процес започва отново с цифрата 1.

a. Малката буква с точка обозначава вторични стъпки на процеса. Обозначаването с буква за всяка стъпка на процес от по-високо ниво започва отново с буква a.

● Тази точка обозначава отделни стъпки от процес без конкретна последователност.

► В инструкциите за безопасност и в предупрежденията този триъгълник обозначава начин за избягване на опасност.

(1) Цифрите в кръгли скоби се отнасят до елементи в илюстрациите.

1 Числата в илюстрациите обозначават елементи, споменати в текста.

– Тиретата показват списъци.

> Символът "по-голямо от" посочва пътя за навигация в диалог.

Този символ обозначава информация, която подпомага употреба на продукта.

⇒ Тази стрелка показва резултат от определен етап в процес.

✓ Тази отметка обозначава резултат от последователни етапи в процес.

1.2 Други документи

Информацията за използването на продукта е описана в ръководството за работа, което се доставя заедно с продукта.

2 Информация във връзка с безопасността

2.1 Изисквания към групата потребители

Терминът “група потребители” описва отговорния персонал, определен от експлоатиращата организация да изпълни определена задача с продукта.

2.1.1 Задължения на експлоатиращата организация

Експлоатиращата организация трябва да осигури следното:

– Всяка група потребители да притежава необходимата квалификация (напр. да е преминала специализирано обучение или да е придобила специализирани познания от опит).
– Всяка група потребители да е обучена за изпълнение на задачата.
– Всяка група потребители да е прочела и разбрала съответните глави на този документ.

2.1.2 Групи потребители

Сервизен персонал

Сервизен персонал
Сервизният персонал извършва следните дейности:

– Конфигуриране на потребителите и на правата им с помощта на Active Directory
– Поддръжка на операционните системи
– Управление на сертификатите
– Специфични за клиента настройки (напр. изтичане на сесията)

Специализиран сервизен персонал
Ако са необходими специфични за продукта познания, работите трябва да се извършват от специализиран сервизен персонал. Специализираният сервизен персонал е обучен от Dräger да извършва тези сервизни дейности по продукта.
Специализираният сервизен персонал извършва следните дейности:

– Инсталиране на продукта
– Конфигуриране на потребителите, ако не се използва Active Directory
– Конфигуриране на числови параметри
– Активиране на лицензи

2.2 Информация относно инструкциите за безопасност

Инструкциите за безопасност предупреждават за опасности и дават инструкции за безопасна употреба на продукта. Във всяка инструкция за безопасност са описани видът на риска и последствията от неспазването ѝ. Неспазването на инструкциите може да доведе до нараняване на хора или до повреда на имущество.

2.3 Инструкции за безопасност

2.3.1 Въвеждане в експлоатация

Конфигуриране и въвеждане в експлоатация

Въвеждане в експлоатация се извършва след първоначално инсталиране или след актуализация. Ако инсталирането или конфигурирането на софтуера е непълно или грешно, могат да възникнат грешни функции. Грешните функции могат да доведат до увреждане на хора.

► Съобразявайте се с информацията за пускане на MPW в експлоатация и следвайте инструкциите.

► Преди пускане в експлоатация трябва да се провери и одобри функционалността на софтуера, включително всички свързани уреди и IT системи.

Изпълнете следните действия:

– Документирайте резултатите от проверката.

– Ако проверката е успешна и функционалността е потвърдена, софтуерът е одобрен за ползване.

Сертификат

Ако сертификатът не е инсталиран правилно или е изтекъл, връзката между клиента и уеб-сървъра ще бъде отказана от браузъра или ще бъде показана като не надеждна.

► Сервизният персонал трябва да инсталира сертификата правилно.

2.3.2 Употреба

Наблюдение на пациента

Ако MPW се използва като активен пациентски монитор, е възможно да не бъдат разпознати критични състояния на пациента и това да доведе до увреждането му. Софтуерът не трябва да се използва като активен пациентски монитор.

► Съобразявайте се с данните от първичния източник на данни.

Терапевтични решения

От забавено или не актуално показване на данни могат да възникнат грешни диагностични или терапевтични оценки, които да доведат до увреждане на хора. Непрекъснато регистрираните параметри, които са по-стари от 15 секунди, се показват в сиво. Това не се отнася за периодично регистрирани параметри, напр. неинвазивно кръвно налягане.

► Не използвайте показаните данни като единствена база за диагностични и терапевтични решения.

► За диагностични и терапевтични решения се съобразявайте с първичния източник на данни.

Място на приложение (мобилно приложение)

Според директивите на здравното заведение, в определени зони на здравното заведение не трябва да се използват мобилни уреди, напр. по технически или хигиенни причини.

► Използвайте MPW само в такива зони на здравното заведение, които са предвидени за използване на мобилни уреди.

► Спазвайте директивите на здравното заведение.

2.3.3 IT мрежа

Отказ на софтуера или на мрежата

При спиране на тока или отказ на отделни мрежови компоненти, някои данни, имащи отношение към конкретен случай, могат да се покажат непълни и да доведат до увреждане на хора.

► Операторът трябва да гарантира връзката на крайния уред с мрежата.

Синхронизация със сървър за време

Разлика във времето между първичния източник на данни и крайния уред може да доведе до грешно показване на данни.

► Уверете се, че първичният източник на данни и крайният уред са свързани с един и същ сървър за време.

2.3.4 Аларми

Софтуерът не показва нито акустични, нито визуални алармени съобщения или уведомления.

► Съобразявайте се с алармите и уведомленията от първичния източник на данни.

2.3.5 Сервиз

Ако сервизът не се извършва редовно, могат да възникнат неизправности, които да доведат до увреждане на хора и до материални щети.

► Извършвайте сервиза в съответствие с глава "Сервиз".

2.3.6 Цялост на софтуера

Ако функционалността за Windows File System Auditing е конфигурирана при инсталирането, както е препоръчано от Dräger, достъпът за писане във файлове от софтуерното приложение, напр. изпълними файлове или DLL файлове, се протоколира в протокол за безопасност.

Запис в протокола за безопасност с един от следните идентификатори на събития може да показва неоторизиран достъп и по този начин пробив в сигурността:

– 4663: Установен е достъп до файл.
– 4660: Изтрит е файл.
– 4719: Настройките за одит са променени. Това е индикация, че функцията за одит е изключена.
– 1102: Изтрит е протокол за безопасност.

► За да се гарантира целостта на софтуера, наблюдавайте в реално време протокола за безопасност за записи с изброените идентификатори на събития, напр. с помощта на SIEM (Security Information and Event Management – Информация за безопасността и управление на събития).

► Анализирайте за неоторизиран достъп записите с изброените идентификатори на събития.

3 Преглед на системата

3.1 Предпоставки

За безопасна работа, астрономическото време на първичния източник на данни и сървъра на MPW трябва да съвпадат.

За целта във всички участващи уреди (напр. монитори, сървъри и крайни уреди) трябва да е активирана синхронизация на времето със сървър на NTP.

Dräger препоръчва Infinity Gateway и Backend сървърът на MPW да се интегрират в болничната система за IT безопасност.

След инсталиране всички пароли трябва да се променят, напр. за да се избегнат атаки от типа "Налучкване на парола". Паролите не трябва да са по-кратки от 10 знака. Dräger препоръчва да се използват пароли, които силно се различават една от друга. Паролите не трябва да са достъпни за неоторизирани лица.

3.2 Съкращения

Съкращение	Обяснение
ACL	Acces Control List (списък за контрол на достъпа) Управление на достъпа до операционната система
AD	Active Directory Услуга за директория на сървъра Microsoft Windows
HTTPS	Hypertext Transfer Protocol Secure (защитен протокол за трансфер на хипер-текст), безопасен протокол за трансфер на хипер-текст
ID	Идентификация
NTP	Network Time Protocol (протокол за мрежово време)
PKI	Инфраструктура с публичен ключ
R/O	Достъп само за четене (управление на права)
R/W	Достъп за четене и писане (управление на права)
TCP	Transmission Control Protocol (протокол за управление на предаването) Група от комуникационни протоколи
TLS	Transport Layer Security (протокол за шифроване)
WSS	Web Services Security (безопасност на уеб услуги), комуникационен протокол

4 Данни за приложението

4.1 Потребители на Windows и групи потребители на Windows

За работа с MPW трябва да се конфигурират следните потребители на Windows и групи потребители на Windows. Потребителите с ID 3,4,5 и 6 се инсталират с инсталатора на MPW.

ID	Потребители на Windows Групи потребители на Windows	Описание
1	Специализиран сервизен персонал	Специализираният сервизен персонал инсталира и поддържа софтуера и инсталира пачове.
2	Неоторизирани потребители на Windows сървъра	Всички потребители и процеси, които не са необходими за работата на MPW.
3	*mpw-gateway-wrapper*	Име на процес в Windows на потребител на услугите на Windows, който процес се изпълнява с Gateway Wrapper на MPW.
4	*mpw-gateway -etcher*	Име на процес в Windows на потребител на услугите на Windows, който процес се изпълнява с Gateway-Fetcher на MPW. Gateway Fetcher на MPW получава данни от Infinity Gateway, които се обработват в Gateway Wrapper. Според версията може да се използва името *mpw-gateway-fetcher-7.2* или *mpw-gateway-fetcher-8.0* или по-високо.
5	*mpw-backend*	Име на процес в Windows на потребител на услугите на Windows, който процес се изпълнява с MPW.
6	*postgres*	Име на процес в Windows на потребител на услугите на Windows, който процес се изпълнява с базата данни Postgres. Ако софтуерът се инсталира в съоръжение на Министерството на отбраната (Department of Defense), базата данни Postgres няма да бъде инсталирана. Вместо това управлението на потребителите се изобразява чрез Active Directory.

4.2 Управление на права за сървъра Infinity Gateway

Този раздел съдържа информация за правата за достъп на потребителите на Windows до данни за приложението. Данните на приложението трябва да бъдат зададени изрично чрез механизма за безопасност на Windows (ACL).

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

Директорията съдържа данни на приложението, които са необходими за работата на Gateway Wrapper.

Права за достъп:

– R/W за специализиран сервизен персонал
– R/O за *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Без достъп за неоторизирани потребители на Windows сървъра

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

Файлът съдържа конфигурации и настройки, които са необходими за безопасна работа на MPW.

Права за достъп:

– R/W за специализиран сервизен персонал
– R/O за *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Без достъп за неоторизирани потребители на Windows сървъра

4.3 Управление на права за сървъра на MPW

Този раздел съдържа информация за правата за достъп на потребителите на Windows до данни за приложението.

C:\ProgramData\mpw-pgdata

Директорията е място за запаметяване на файлове от базата данни, които съдържат данни за вписване на потребители на MPW. Ако в MPW съществува свързване с AD, директорията не съществува.

Права за достъп:

– R/W за специализиран сервизен персонал и за *postgres*
– Без достъп за неоторизирани потребители на Windows сървъра

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

В този файл може да се конфигурира показването на параметрите на уредите.

Права за достъп:

– R/W за специализиран сервизен персонал
– R/O за *mpw-backend*
– Без достъп за неоторизирани потребители на Windows сървъра и за *postgres*

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

В този файл се съдържат примери за конфигуриране на показването на параметрите на уредите. Файлът не се инсталира в съоръжение на Министерството на отбраната (Department of Defense).

Права за достъп:

– R/W за специализиран сервизен персонал
– R/O за *mpw-backend*
– Без достъп за неоторизирани потребители на Windows сървъра и за *postgres*

C:\Program Files\Draeger\MPW-Backend

Директорията съдържа файлове на приложението, които са необходими за работата на MPW.

Права за достъп:

– R/W за специализиран сервизен персонал
– R/O за *mpw-backend*
– Без достъп за неоторизирани потребители на Windows сървъра и за *postgres*

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

Файлът съдържа конфигурации и настройки, които са необходими за безопасна работа на MPW.

Права за достъп:

– R/W за специализиран сервизен персонал
– R/O за *mpw-backend*
– Без достъп за неоторизирани потребители на Windows сървъра и за *postgres*

4.4 Файл application.properties

4.4.1 Уеб сървър на Gateway Wrapper

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

Примерни записи	Описание
logging.level.org.springframework=INFO	Конфигуриране на нивата на вписване за Spring
logging.level.com.draeger=TRACE	Конфигуриране на нивата на вписване за MPW
server.port=8443	Порт на уеб сървъра
igw.user=<Потребител>	Потребител на Infinity Gateway
igw.password=<Парола>	Парола за Infinity Gateway

4.4.2 Уеб сървър на MPW

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

Примерни записи	Описание
logging.level.org.springframework=INFO	Настройка на специфични за приложението събития
logging.level.com.draeger=TRACE	Настройка на специфични за приложението събития при наблюдение на пациент
logging.level.com.draeger.upw.mpw.backend.log.session=OFF	Настройка за вписване на всички събития по време на сесията на потребителя
server.port=8444	Порт на уеб сървъра за клиенти на браузъра
mpw.session.mobile.timeout=30	Относително изтичане на сесията за мобилни клиенти
mpw.session.desktop.timeout=120	Относително изтичане на сесията за десктоп клиенти
mpw.session.absolute.timeout=720	Абсолютно изтичане на сесията за всички клиенти
server.ssl.keyStoreType=PKCS12	Сертификат за тип хранилище на ключове

Примерни записи	Описание
server.ssl.key-store-password=<password>	Парола за PKI-сертификат
gateway.url=https://<gateway.server.name>:8444	Информация за свързване към Gateway Wrapper
spring.datasource.password=<password>	Парола на базата данни в управление на потребителите (не се използва при свързване с AD)
spring.datasource.username=<postgres.username>	Потребители на базата данни в управление на потребителите (не се използва при свързване с AD)
server.name=<MPW domain>	Име на домейна за MPW Името на домейна трябва да е еднакво с името на домейна в сертификата
ad.domain	За повече информация виж: "Active Directory", страница 20.
ad.url	
ad.searchFilter	
ad.groupMapping [<<Група от AD>>]=<<Болнично отделение>>	
ad.groupMapping[Лекари]=ICU	
ad.groupMapping[Лекари]=OP1,OP2	
ad.groupMapping[Лекари\ OP]=OP	

5 Регулиране на защитната стена

5.1 Уеб сървър на Gateway Wrapper

Стандартно приложението стартира от порт 8443. При инсталиране този порт се използва като стандартна настройка. Стандартната настройка може да се промени чрез файла *application.properties*. За целта търсете *server.port*. Портът трябва да е одобрен като "Inbound Rule" (TCP).

5.2 Уеб сървър на MPW

Стандартно приложението стартира от порт 8444. При инсталиране този порт се използва като стандартна настройка. Стандартната настройка може да се промени чрез файла *application.properties*. За целта търсете *server.port*. Портът трябва да е одобрен като "Inbound Rule" (TCP).

5.3 Връзки

За да може Frontend да се свърже с Backend, в мрежата трябва да са разрешени връзки HTTPS и WSS. Като порт за WSS (еквивалент на Websocket за HTTPS) се използва *server.port* на Backend. За повече информация виж: "Файл application.properties", страница 13.

5.4 Регулиране на защитната стена и защита от вируси

Защитната стена на Infinity Gateway и на Backend трябва да допуска "inbound" за съответния порт, конфигуриран за HTTPS/WSS.

За употреба в сървъра на Backend са тествани следните вирусни скенери:

– McAfee 5 със средно ниво на разпознаване

Всички директории на сървъра на Backend са подходящи за вирусно сканиране.

6 Протоколиране

6.1 Нива на протоколиране

Всички приложения, които се доставят с MPW, записват протоколи в протокола за събития на Windows. При стартирането си приложенията проверяват дали системата на протоколите функционира. Ако се появи грешка, приложението не стартира. Грешките на протоколите по време на работа могат да се намерят в прегледа на събитията (Event Viewer) в системния протокол на Windows с източник "Протокол на събитията". След инсталирането си MPW създава всички събития с ниво на протокола "Information" (Информация), "Warning" (Предупреждение) или "Error" (Грешка). На разположение са следните нива на протокола:

Ниво на протокола	***application.properties***	**Описание**
TRACE	logging.level.org.springframework=TRACE logging.level.com.draeger=TRACE	Обозначава по-подробни информационни събития, отколкото ниво на протокола DEBUG.
DEBUG	logging.level.org.springframework=DEBUG logging.level.com.draeger=DEBUG	Обозначава подробни информационни събития, които са най-полезни за отстраняване на грешки в дадено приложение.
INFO	logging.level.org.springframework=INFO logging.level.com.draeger=INFO	Обозначава информационни съобщения, които показват напредъка на приложението на недиференцирано ниво.
WARN	logging.level.org.springframework=WARN logging.level.com.draeger=WARN	Обозначава потенциално грешни ситуации.
ERROR	logging.level.org.springframework=ERROR logging.level.com.draeger=ERROR	Обозначава грешки, с които приложението евентуално може да продължи да работи.

ℹ За промяна на нивата на протоколите е необходимо файлът *application.properties* от MPW и Gateway Wrapper да бъде коригиран, както е показано в таблицата (виж "Файл application.properties", страница 13). След инсталиране стандартната настройка е "INFO".

6.2 Протоколиране на сесии

Протоколът на сесии (*mpw-backend-sessions.log*) потенциално съдържа лични данни, като IP-адрес и потребителско име. За да се деактивира протоколът на сесиите, във файла *application.properties* трябва да съществува следния ред:

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

За повече информация виж: "Уеб сървър на MPW", страница 13.

6.3 Изтичане на сесията

След инсталиране на софтуера, изтичането на сесиите е стандартно зададено след 30 минути за мобилно приложение и 120 минути за десктоп приложение. Времето да изтичане на сесията трябва да се конфигурира според директивите на здравното заведение за защита на данни. Стойностите могат да се конфигурират във файла *application.properties*.

application.properties	Описание
mpw.session.mobile.timeout=30	Относително изтичане на сесията Сесията се затваря след изтичане на зададеното време, ако през това време не е регистрирана активност на потребителя.
mpw.session.desktop.timeout=120	
mpw.session.absolute.timeout=720	Абсолютно изтичане на сесията Сесията се затваря винаги след изтичане на зададеното време.

Мерната единица е минути, а стойността трябва да е между 1 и 720 минути.

За повече информация виж: "Уеб сървър на MPW", страница 13.

6.4 Намиране на събития

6.4.1 Преглед на събитията

За по-лесно намиране на протоколите на MPW, при инсталиране на Backend на MPW-Gateway-Wrapper на MPW, на съответните сървъри се задава дневник с името "Draeger".

Прегледът на събитията във Windows (Event Viewer) разполага с функции за управление на протоколирани събития (напр. архивиране, ротация, запаметяване, изтриване или препращане на събития). Тази информация може да се намери в базата от знания на Microsoft.

В прегледа на събитията във Windows събитията обикновено се категоризират чрез следните качества: *ниво*, *източник*, *ID на събитието* и *категория на задачата*. Тези качества, освен *категория на задачата*, могат да се използват за филтриране на протоколи на MPW.

– *Категория на задачата* не се използва.
– *Източник* отговаря на името на MPW приложението и според това може да съдържа една от следните стойности: *MPW-Backend*, *Bulkport*, *PasswordResetter*, *UserAdmin*, *PostgreSQL* и *MPW-Gateway-Wrapper*.
– *ID на събитието* служи за категоризация на съдържанието на протоколните записи. По-долу е изброено как се категоризират протоколните записи в MPW въз основа на *ID на събитията*.

6.4.2 ID на събитията за намиране на събития

Стандартната настройка на нивото на протоколите е "Information" (Информация), като са възможни още нива на протоколи "Warning" (Предупреждение) и "Error" (Грешка)

ID на събитието	Приложения	Описание
10	MPW-Backend, Bulkport, PasswordResetter, UserAdmin, MPW-Gateway-Wrapper	Специфични за приложението протоколи
11[1)]	MPW-Backend	Събития, свързани с вписване за потребителска сесия (напр. успешни и неуспешни опити за вписване)
0[2)]	PostgreSQL	Вътрешна база данни за управление на потребители на Backend
12	Информация във връзка с комуникацията	IP-адреси на свързани системи. Успешни и неуспешни опити за достъп до обекти, свързани с безопасността или опити за изменение на такива обекти.
13	Информация във връзка със сесиите	Изтичане на сесия, изтриване, обновяване на ID на потребителска сесия
15	Идентифициране на потребители	Успешни, неуспешни опити за вписване
16	Успешни и неуспешни опити за достъп до информация за отстраняване на грешки	Страница на здравното заведение

1) Протоколирането на сесии трябва да е изрично активирано, тъй като протоколите съдържат потребителско име и ID на сесията. Преди активиране съберете информацията за законовите изисквания за защита на личното пространство на потребителите и се съобразете с тях.
2) Протоколните записи PostgreSQL идват директно от базата данни PostgreSQL. Dräger не влияе върху съдържанието на тези протоколни записи (това е причината ID на събитието да е 0). Dräger не променя също и стандартните настройки на нивото на протокола или подобни за PostgreSQL.

6.4.3 Протоколни записи извън протоколите на Dräger

В протоколите на Dräger не се записват следните събития:

– Начало и край на услугата
  Протоколните записи за начало и край на инсталираните услуги на MPW се записват автоматично чрез Windows в системния протокол. Тези протоколни записи могат да бъдат намерени там в източника "Service Control Manager" с търсене например на "mpw-backend" или "mpw-gateway-wrapper".
– Изменения на файлове
  Windows може да регистрира достъп например до конфигурационни файлове чрез Audit File System Policy. Съответните записи се въвеждат в протокола за безопасност.

7 Configuration

7.1 Active Directory

Ключ	Стойност
ad.domain	Домейн на AD (напр. *company.com*)
ad.url	URL на AD (напр. *ldaps://ad.company.com*)
ad.rootDn	RootDn на активната директория (ако е необходимо)
ad.searchFilter	Филтър за търсене на активната директория, за намиране на оторизирани потребители в нея Стандартна настройка: *(&(objectClass=user)(userPrincipalName={0}))* Ако "[...]*Name={0}*", при търсене {0} се замества с "username@domain". Ако "[...]*Name={1}*" при търсене *{1}* се замества с потребителското име ("username").

За да се определи коя група в активната директория коя група работни места може да вижда, във файла *application.properties* трябва да се създаде мапинг между името на групата от активната директория и името на групата работни места.

За всяка група от активната директория, за която е извършен мапинг, в конфигурационния файл трябва да се вмъкне ред в следния формат:

ad.groupMapping[<<Група от активната директория>>]=<<Болнично отделение>>

Означението за <<Болнично отделение>> трябва да е същото като означението в мрежата на Infinity Gateway.

<<Група от активната директория>> и *<<=<<Болнично отделение>>* трябва да се заменят със съответните имена. Например, за да се даде на групата "Лекари" от активната директория достъп до групата работни места (Болнично отделение) "ICU", трябва да се вмъкне следния ред:

ad.groupMapping[Лекари]=ICU

Ако някоя група от активната директория трябва да има достъп до няколко групи работни места, тези работни места трябва да се въведат едно след друга, разделени със запетая.

Пример: *ad.groupMapping[Лекари]=OP1,OP2*

Интервалите в името на групата в активната директория трябва да се въведат с "\" + "интервал".

Пример: *ad.groupMapping[Лекари\ OP]=OP*

7.2 Отстраняване на потребители от активната директория

Потребителите, които са отстранени от Active Directory, но все още имат валидна потребителска сесия, могат да бъдат изключени от работата чрез рестартиране на MPW-Backend от услугата на Windows. Рестартирането на MPW-Backend води до затваряне на всички потребителски сесии. Ако MPW-Backend не се рестартира, сесията завършва най-късно при абсолютното ѝ изтичане.

8 Резервно копие и възстановяване при срив

За да се възстанови системата при проблеми, трябва да се създаде резервно копие. След това MPW трябва да се инсталира отново и всички конфигурационни файлове трябва да се импортират от резервното копие.

За целта са необходими следните конфигурационни файлове:

Gateway

– *application.properties*

MPW-Backend

– *application.properties*
– *device-parameter-config-sample.csv*
– Използваният сертификат. Съответният файл може да се промени във файла *application.properties* (стандартна стойност: *cert.p12*).

Ако се сменя целият хардуер, лицензът трябва отново да се импортира. Преди смяна на хардуера, се свържете със специализирания сервизен персонал.

Ако MPW е инсталирана с вътрешната база данни за потребители, предварително трябва да се създаде резервно копие на тази база данни и след това базата данни да се импортира отново. За целта се свържете със специализирания сервизен персонал.

9 Инфраструктура с публичен ключ

За да се използва болничната PKI, сертификатът на сървъра може да бъде импортиран при инсталиране. След инсталиране сертификатът може да бъде допълнително променен във файла *application.properties*. За целта трябва да се коригират следните записи:

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

За да бъде сертификатът класифициран като надежден, името на домейна "server.name" във файла *application.properties* трябва да е еднакво с името на домейна в сертификата.

10 Сертификат

10.1 Инсталиране в крайните уреди на запис TrustedRoot за сертификат TLS за MPW

Ако основният сертификат на болницата вече не е активиран в крайните уреди, той трябва да бъде инсталиран в тези уреди.

ℹ В момента са допуснати до употреба само Microsoft Edge, Google Chrome и Apple Safari (iOS).

ℹ Основният сертификат не същият, който се използва от Backend. Основният сертификат е подписал сертификата Backend.

Сертификатът е успешно инсталиран, ако е възможно вписване в уреда. Не е достатъчно да се отвори екранът за вписване, а трябва и самото вписване да е възможно.

10.1.1 Microsoft Windows

Трябва да е сигурно, че използваният браузър приема сертификата, използван на сървъра.

При ръчно инсталиране:

1. Кликнете два пъти върху файла със сертификата.
   ⇒ Отваря се мениджърът на сертификати на Windows.
2. Добавете сертификата като основен (функцията Auto Detection не го разпознава правилно).

10.1.2 Apple iOS

Трябва да е сигурно, че използваният браузър приема сертификата, използван на сървъра.

При ръчно инсталиране: Основният сертификат трябва първо да бъде изпратен с е-майл до електронна поща, в която може да се влезе през iPhone. Сертификатът може да се инсталира, само ако е-мейлът се отвори в приложението ***Mail*** и прикаченият сертификат бъде избран. Необходим е PIN на уреда.

Като се кликне върху сертификата, той се инсталира първоначално като не надежден. За да се активира неговата надеждност, е необходимо следното действие:

Einstellungen (Настройки) > ***Allgemein (Общо)*** > ***Info (Информация)*** > ***Zertifikatsvertrauenseinstellungen (Настройки на надеждността на сертификата)*** > ***volles Vertrauen für Root Zertifikat aktivieren (Активиране на пълна надеждност на основния сертификат)***.

Сертификатът може отново да се отстрани от ***Allgemein (Общо)*** > ***Profil (Профил)***.

11 Деинсталиране

За да се изтрият напълно всички чувствителни данни, Dräger препоръчва след деинсталиране на софтуера компютърът да се рестартира.

12 Сервиз

12.1 Дефиниция на сервизната терминология

Концепция	Дефиниция
Сервиз	Всички мерки (проверка, поддръжка, ремонт) за поддържане или възстановяване на функционалността на даден продукт
Проверка	Мерки за определяне и оценка на текущото състояние на даден продукт
Поддръжка	Редовни специфични мерки за поддържане на функционалността на даден продукт
Ремонт	Мерки за възстановяване на функционалността на даден продукт след авария

Препоръчва се сключване на договор за обслужване с Dräger.

12.2 Поддръжка

Компонент	Интервал	Мярка	Група потребители
Сертификат TLS	По данни на клиента	Възобновяване на сертификати TLS	Сервизен персонал
Твърд диск	На всеки 2 години	Проверка на капацитета на твърдия диск	Сервизен персонал
		Архивиране и изтриване на Log файлове, ако е необходимо	

Актуализации на безопасността

Пакетите за безопасност и пачовете, като например тези от Microsoft Windows, попълват уязвимости, отстраняват грешки и актуализират функции. Dräger одобрява за инсталиране новите актуализации на безопасността за MPW. При работа с актуализации на безопасността, спазвайте следните точки:

- В сървъра на MPW деактивирайте автоматичната актуализация на пачове и сервизни пакети.
- Когато е публикувана нова актуализация на безопасността, изчакайте одобрението на Dräger за системата MPW. Ако до 4 седмици след публикуване на нова актуализация на безопасността Dräger не съобщи за никакви възражения, актуализация на безопасността се счита за одобрена за MPW.
- Ако съществува тестова система, Dräger препоръчва новата актуализация на безопасността да се тества с нея.

13 Технически данни

13.1 Системни изисквания

13.1.1 Среда и инфраструктура на софтуера

Версии на Infinity Gateway Включително опцията WinAccess API	7.2, 8.0, 9.0
WLAN в мястото на използване	
Честотна лента	Най-малко 1 Gbit/s в мрежата, която свързва източниците на данни и сървърите.
Портове	8443 (стандартна настройка), може да се конфигурира

13.1.2 Сървър

Сървър за софтуер (Mobile Patient Watch)

Операционна система	Сървър Windows 2016 (физически или виртуален сървър)
Процесор	8 процесорни ядра с 3200 MHz Boost такт
Оперативна памет (RAM)	32 GB
Твърд диск SSD	2 TB

Сървър за Infinity Gateway

В хардуера на Infinity Gateway трябва да се инсталира допълнителен софтуер за получаване на данни, така че системните изисквания към хардуера се повишават. Освен този софтуер, в същия сървър не трябва да се инсталира никакъв друг софтуер, който Infinity Gateway да използва като източник на данни.

Това поражда следните изисквания към системата:

Операционна система	Сървър Windows 2016 (физически или виртуален сървър)
Процесор	8 процесорни ядра с 3000 MHz
Оперативна памет (RAM)	32 GB
Твърд диск SSD	60 GB

13.1.3 Крайни уреди

Препоръчани крайни уреди

Софтуерът може напълно да се показва и използва на препоръчаните крайни уреди. Скоростта на кривите съгласно спецификацията е гарантирана.

Мобилно приложение	
Операционна система	iOS 14
Браузър	Apple Safari (актуална версия)

Мобилно приложение	
Графична разделителна способност	– 2436 x 1125 px (458 ppi) – 2532 x 1170 px (460 ppi) – 2688 x 1242 px (458 ppi)

Десктоп приложение	
Операционна система	Windows 10 (актуална версия)
Браузър	Microsoft Edge (актуална версия) Google Chrome (актуална версия)
Графична разделителна способност	1920 x 1080 px (24 инча)

Съвместими крайни уреди

Софтуерът може напълно да се показва и използва на съвместимите крайни уреди. Скоростта на кривите може да се отклонява от спецификацията, но остава постоянна за уреда.

Мобилно приложение	
Крайни уреди с операционна система iOS	
Версия	iOS 14 и по-висока (актуална версия)
Браузър	Apple Safari (актуална версия)
Графична разделителна способност	от 1136 x 640 px до 2688 x 1242 px
Плътност на пикселите	от 326 ppi до 476 ppi
Съотношение на страните	от 1,8:1 до 2,2:1
Крайни уреди с операционна система Android	
Версия	Android 9 и по-висока (актуална версия)
Браузър	Chrome (актуална версия)
Процесор	Осмоядрен процесор 1,6 GHz (+)
Графична разделителна способност	от 1280 x 720 px до 3200 x 1440 px
Плътност на пикселите	от 294 ppi до 563 ppi
Съотношение на страните	от 1,8:1 до 2,2:1

Десктоп приложение	
Операционна система	Windows 10 (актуална версия)
Браузър	Microsoft Edge (актуална версия) Google Chrome (актуална версия)
Графична разделителна способност	Изборът се прави от оператора.

ℹ Техническата документация с подробна информация може да се получи при поискване.

13.2 Работни характеристики

Класификация

Класификация на медицинския продукт, Европа	Клас IIb
Код UMDNS Universal Medical Device Nomenclature System – номенклатурна система за медицински уреди	17223
Код GMDN Global Medical Device Nomenclature – глобална номенклатура за медицински уреди	44101

13.2.1 Точност на показанията

За диапазона на стойностите, точността на показване на кривите, числовите стойности и честотата на вземане на проби за трендове, се съобразете с информацията от ръководствата за работа на Mobile Patient Watch и на Infinity Gateway.

13.3 Комуникация в мрежа

Източник на данни:	Компютър Infinity Gateway с компонент Gateway Wrapper
Сървър Backend:	Комуникира с Infinity Gateway чрез кодирана IP връзка при порт 8443 (стандартно, може да се коригира при инсталиране).
Крайни уреди (персонален компютър или мобилни уреди):	Комуникира със сървъра Backend чрез HTTPS и WSS връзка при порт 8444 (стандартно, може да се коригира при инсталиране).

13.4 Връзки с IT мрежи

В IT мрежа данните могат да се обменят чрез жични или безжични технологии. IT мрежата включва всички интерфейси за данни, които са описани в нормативи и конвенции.

При работа този продукт може да обменя информация с други уреди с помощта на IT мрежи и поддържа следните функции:

– Показване на криви и данни за параметри
– Изглед на легло чрез отдалечен достъп
– Трансфер на настройки на уреда и данни за пациента

Свързването на този продукт към мрежа, към която са свързани други уреди, както и допълнителни промени в тази мрежа, могат да доведат до нови опасности за пациентите, потребители или трети лица. Преди продуктът да се свърже към мрежата или преди мрежата да бъде променена, тези опасности трябва да бъдат установени, анализирани и оценени и да се предприемат подходящите мерки.

Примери за последващи промени на мрежата:

– Промяна на конфигурацията на мрежата
– Отстраняване на уреди и софтуер от мрежата
– Добавяне на други уреди и софтуер към мрежата
– Извършване на надстройки или актуализации на уредите и на софтуера, които са свързани към мрежата

За да се гарантира сигурна комуникация между сървъра и клиента, трябва да съществува TLS инфраструктура. За целта в крайните уреди трябва да се инсталира сертификат.

13.4.1 Информация за свързване към IT мрежа

13.4.1.1 Предпоставки

Този продукт трябва да се свързва към мрежа само от специализиран сервизен персонал. Преди това трябва да се направи консултация с IT отговорника на здравното заведение.

Трябва да бъдат изпълнени инструкциите от следните документи:

– Документи, придружаващи този продукт
– Описания на мрежата

Dräger препоръчва съобразяване с IEC 80001-1 (управление на риска за IT мрежи с медицински продукти).

13.4.1.2 Свързване на първични източници на данни

Свързването на първични източници на данни става само чрез Infinity Gateway. За повече информация относно свързване на първични източници на данни, съблюдавайте продуктовата информация на Infinity Gateway.

13.4.1.3 Свързване на крайни уреди чрез мрежи

– LAN мрежите обикновено са конфигурирани в звездна топология. Отделните уреди могат да бъдат комбинирани в групи чрез превключвател на n-ниво. Друг трафик на данни се отделя чрез отделни VLAN мрежи. Конфигурирайте мрежовите настройки на продукта в съответствие с това ръководство за работа и със изискванията към мрежата.
– Спецификациите на LAN връзките са описани в следните стандарти:
  – Кабелни мрежи: IEEE 802.3
  – Безжични мрежи: IEEE 802.11 (b, g, n)
– Ако продуктът се използва с превключвател на 2 ниво или превключвател на 3 ниво, настройките на порта трябва да се конфигурират при превключвателя на мрежата. Преди доставка на продукта, Dräger може да конфигурира мрежовите настройки според изискванията на оператора.
– Този продукт обменя данни с други медицински продукти чрез LAN мрежа. Мрежата трябва да поддържа следните начини на пренос и протоколи:
  – TCP/IP
  – Уникаст (статично или динамично адресиране с комуникационни протоколи ARP или RARP)

- Мултикаст
- Броудкаст
- IGMP (Версия 2)

С използване на комуникационен протокол IGMP този продукт може да влезе в IP-мултикаст група или да я напусне.

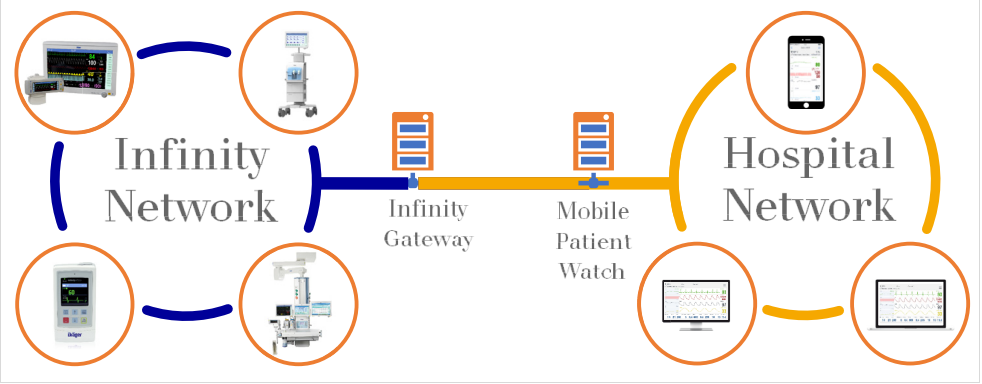
13.4.1.4 Последствия от използването на неподходяща мрежа

Ако мрежата не удовлетворява изискванията, това може да доведе до опасни ситуации. При този продукт могат да възникнат следните ситуации:

- При прекъсване на връзка с мрежата:
  - Данните не се показват или се показват със закъснение.
- Без защитна стена:
  - Данните не са защитени.
  - Настройките на продукта се променят.
- Данните се изпращат непълни, изпращат се към погрешен продукт или изобщо не се изпращат.
- Данните за пациента се задържат, изопачават или променят.
- Данните имат неправилни отметки за време.

13.4.1.5 Необходими качества

Първичните източници на данни и Infinity Gateway да се намират в една и съща мрежа. За тази мрежа са валидни необходимите качества. За целта се съобразете с продуктовата информация за Infinity Gatway. Сървърът на MPW получава данните с помощта на MPW-Gateway-Wrapper, който е инсталиран в същия сървър, както Infinity Gateway. MPW може да работи в болнична мрежа, която свързва всички крайни уреди със сървъра на MPW. За целта са необходими права за достъп.



За повече информация относно регулиране на защитната стена, виж инструкцията за инсталиране "Регулиране на защитната стена".

Мрежата, в която се инсталира и изпълнява MPW, трябва да е под контрола на оператора.

За да се избегне не оторизиран достъп и разпространяване на зловреден софтуер в мрежата, трябва да се вземат предпазни мерки. Примерно, могат да се вземат следните предпазни мерки:

– Ограничаване на физически достъп до активните разпределителни кутии на мрежата
– Могат да се конфигурират само тези портове, които са необходими за работа. Всички други портове трябва да са затворени.
– С мрежата могат да са свързани само уреди, които имат същата или по-висока степен на надеждност.
– Сигурно изолиране на мрежата (физическо или виртуално)
– Използване на защитна стена
– Управление на пачовете за уредите
– Прилагане по ISO/IEC 27033

13.4.1.6 Натоварване на мрежата

Данни за всеки пациент, изпращани между Gateway Wrapper и Backend на MPW

Брой сесии на браузъра	Нагоре по веригата [kb/s]	Надолу по веригата [kb/s]	Вид данни
1	689,63	32,11	Трансферираните данни се състоят в по-голямата си част от релевантни данни, които трябва да се покажат в MPW, като например параметри, данни за трендове и криви. Структурата на теста измерва пропускателната способност на данни за един пациент със 17 стандартни параметъра, 4 вида данни за наблюдение на пациента със съответните криви и трендове с увеличаващ се брой сесии. Данните показват, че обменът на данни между Gateway Wrapper и Backend на MPW остава почти стабилен. При промяна на броя на пациентите, които се наблюдават едновременно, може да се очаква повишен обмен на данни.
2	666,8	31,00	
3	698,54	31,92	
4	652,04	30,37	

Данни, изпращани между Backend на MPW и Gateway Wrapper

Брой сесии на браузъра	Нагоре по веригата [kb/s]	Надолу по веригата [kb/s]	Вид данни
1	78,39	19,00	Структурата на теста е непроменена. Данните показват, че обменът на данни между Backend на MPW и клиента (крайния уред) се покачва пропорционално. С увеличаване на броя сесии на браузъра може да се очаква повишен обмен на данни.
2	152,64	37,31	
3	246,36	57,22	
4	317,46	72,64	

13.4.1.7 Брой поддържани уреди

С едно инсталиране на софтуера могат едновременно да се показват данни от максимално 45 работни места (пациентски монитори) на до 100 крайни уреда.

Индекс

A–Z

Г

И

П

С

Тази страница умишлено е оставена празна.

Тази страница умишлено е оставена празна.

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

CE 0123

www.draeger.com

9511692 – 6405.022 bg

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