Mobile Patient Watch

Système d’information des données patients

Logiciel 1.2.n

Manuel d’administration

AVERTISSEMENT
Toute utilisation du produit nécessite une connaissance spécifique et le respect de cette documentation et de la notice d'utilisation du produit.

Dräger. La technologie pour la vie.

Cette page est intentionnellement laissée vierge.

Sommaire

1 Informations sur ce document

1.1 Conventions typographiques

Texte Les textes en gras ou en italique indiquent des textes sont affichés à l'écran.

1. Les chiffres suivis d'un point indiquent les étapes individuelles de la séquence d'un processus. La numérotation pour chaque nouvelle séquence recommence par le chiffre 1.

a. Les lettres minuscules suivies d'un point indiquent des étapes de processus secondaires. L'attribution des lettres recommence par a pour chaque nouvelle étape d'un processus de niveau supérieur.

● Ce point indique les étapes individuelles d'un processus sans séquence spécifique.

► Dans les consignes de sécurité et les avertissements, ce triangle indique des moyens d'éviter le danger.

(1) Les nombres indiqués entre parenthèses renvoient à des éléments dans les illustrations.

1 Les nombres des illustrations indiquent des éléments auxquels il est fait référence dans le texte.

– Les tirets indiquent des listes.

> Le symbole supérieur à indique le chemin de navigation dans une boîte de dialogue.

Ce symbole indique des informations qui facilitent l'utilisation du produit.

⇒ Cette flèche indique le résultat de l'étape d'un processus.

✓ Cette coche indique le résultat d'une séquence d'étapes au sein d'un processus.

1.2 Autres documents

Les informations sur l'utilisation du produit sont indiquées dans la notice d'utilisation fournie avec le produit.

2 Informations relatives à la sécurité

2.1 Exigences liées au groupe d'utilisateurs

Le terme « Groupe d'utilisateurs » décrit le personnel responsable ayant été assigné par l'exploitant pour réaliser une tâche spécifique sur le produit.

2.1.1 Obligations de l'organisation opérationnelle

L'organisation opérationnelle doit s'assurer des points suivants :

– chaque groupe d’utilisateurs dispose des qualifications requises (p.ex. a suivi une formation spécialisée ou acquis des connaissances spécialisées dans l'exercice de son travail).
– Chaque groupe d’utilisateurs a été formé pour accomplir la tâche.
– Chaque groupe d'utilisateurs a lu et compris les chapitres correspondants de ce document.

2.1.2 Groupes d'utilisateurs

Personnel d'entretien

Personnel d'entretien
Le personnel d'entretien effectue les tâches suivantes :

– Configuration des utilisateurs et des droits des utilisateurs à l'aide d'Active Directory
– Maintenance des systèmes d'exploitation
– Gestion des certificats
– Modifications spécifiques au client (p. ex. délai d'expiration de session)

Personnel d'entretien spécialisé
Si une tâche exige des connaissances spécifiques au produit, elle doit être réalisée par le personnel d’entretien spécialisé. Le personnel d'entretien spécialisé a été formé par Dräger pour les opérations d’entretien concernant ce produit.
Le personnel d'entretien spécialisé effectue les tâches suivantes :

– Élimination du dispositif
– Configuration utilisateur dans les cas où Active Directory n'est pas utilisé
– Configuration des paramètres numériques
– Activation des licences

2.2 Informations relatives aux consignes de sécurité

Les consignes de sécurité signalent les risques et délivrent les instructions pour utiliser le produit en toute sécurité. Le type de risque et les conséquences du non-respect des instructions sont décrits dans chaque consigne de sécurité. Le non-respect de ces instructions peut causer des dommages physiques ou matériels.

2.3 Consignes de sécurité

2.3.1 Mise en service

Configuration et mise en service

La mise en service est effectuée après une première installation ou après une mise à jour. Des dysfonctionnements peuvent apparaître si l'installation et la configuration du logiciel sont incomplètes ou incorrectes. Les dysfonctionnements peuvent entraîner des blessures.

► Observer les informations concernant la mise en service de la MPW et suivre les instructions.

► Avant la mise en service, il convient de vérifier et de valider l'intégrité fonctionnelle du logiciel, y compris celle des périphériques raccordés et de tous les systèmes informatiques connectés.

Suivre les étapes suivantes :

– Consigner les résultats du test.

– Si le test est réussi et si l'intégrité fonctionnelle est vérifiée, valider le logiciel.

Certificat

Si le certificat n'est pas correctement installé ou s'il a expiré, votre navigateur refusera la connexion entre le client et le serveur web ou l'affichera comme non fiable.

► Le personnel d'entretien doit installer le certificat de manière appropriée.

2.3.2 Utilisation

Surveillance du patient

Si la MPW est utilisée comme moniteur patient, les états critiques du patient peuvent ne pas être identifiés, ce qui peut conduire à des blessures. Le logiciel ne doit pas être utilisé comme moniteur patient actif.

► Observer les valeurs de la source de données principale.

Décisions thérapeutiques

L'affichage retardé des données et des tendances ou l'affichage de données obsolètes peut entraîner des erreurs de diagnostic ou d'interprétation et causer des blessures. Les paramètres enregistrés en continu datant de plus de 15 secondes apparaissent en gris. Ce n'est pas le cas des paramètres enregistrés par intermittence, comme la PNI.

► Ne pas utiliser les données affichées comme fondement unique du diagnostic et des décisions thérapeutiques.

► Observer la source de données principale pour le diagnostic et prendre des décisions thérapeutiques.

Environnement d’utilisation (utilisation mobile)

Conformément aux directives de l’établissement de santé, les appareils mobiles ne peuvent pas être utilisés dans certains services de l’établissement, notamment pour des raisons techniques ou d’hygiène.

► Utiliser la MPW uniquement dans les services de l’établissement de santé adaptés à l’utilisation d’appareils mobiles.

► Suivre les directives de l’établissement de santé.

2.3.3 Réseaux informatiques

Défaut du logiciel ou du réseau

En cas de panne de l’alimentation électrique ou des composants réseau, les données du dossier peuvent ne pas s’afficher correctement ou de manière incomplète et causer des blessures.

► L’exploitant doit s’assurer que le client est connecté au réseau.

Synchronisation avec un serveur horaire

Un écart temporaire entre la source de données primaire et le client peut entraîner l’affichage de données incorrectes.

► Veiller à ce que la source de données primaire et le client soient connectés au même serveur horaire.

2.3.4 Alarmes

Le logiciel n’émet pas d’alarmes sonores ou visuelles ni de notifications.

► Observer les alarmes et les notifications de la source de données primaire.

2.3.5 Entretien

Si l'entretien n'est pas effectué de manière régulière, des dysfonctionnements peuvent se produire, qui sont susceptibles d'entraîner des blessures du personnel et des dommages matériels.

► Effectuer les opérations d'entretien conformément au chapitre "Entretien".

2.3.6 Intégrité du logiciel

Si la fonctionnalité Windows File System Auditing a été configurée lors de l'installation comme recommandé par Dräger, l'accès en écriture aux fichiers du logiciel, par exemple les fichiers exécutables ou les DLL, est consigné dans le journal de sécurité.

Une entrée avec l'un des ID d'événement suivants dans le journal de sécurité peut indiquer un accès non autorisé et donc un incident de sécurité :

- 4663 : un accès au fichier a été détecté.
- 4660 : le fichier a été supprimé.
- 4719 : les paramètres d'Auditing ont été modifiés. Cela indique que la fonction Auditing a été désactivée.
- 1102 : le journal de sécurité a été supprimé.

► Pour garantir l'intégrité du logiciel, surveiller en temps réel les entrées du journal de sécurité avec les ID d'événement répertoriés, p. ex. en utilisant SIEM (Security Information and Event Management, informations de sécurité et gestion d'événements).

► Analyser les entrées à l'aide des ID d'événements répertoriés pour détecter tout accès non autorisé.

3 Vue d'ensemble

3.1 Prérequis

Pour garantir un fonctionnement sûr, les heures entre la source de données principale et le serveur MPW doivent correspondre.

Pour cela, la synchronisation temporelle via le serveur NTP doit être activée sur tous les périphériques impliqués (comme les moniteurs, les serveurs et les clients).

Dräger recommande d'intégrer la passerelle Infinity Gateway et le MPW-Backend dans le concept de sécurité informatique de l'hôpital.

Tous les mots de passe doivent être changés après l'installation, par exemple pour éviter que des programmes tentent de deviner les mots de passe ("Password guessing"). Le mot de passe doit comporter au moins 10 caractères. Dräger recommande d'utiliser des mots de passe très différents les uns des autres. Les mots de passe ne doivent pas être accessibles aux personnes non autorisées.

3.2 Abréviations

Abréviation	Explication
ACL	Access Control List Contrôle d'accès au système d'exploitation
AD	Active Directory Service d'annuaire de Microsoft Windows Server
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
NTP	Network Time Protocol, protocole horaire en réseau
PKI	Public key infrastructure (infrastructure à clé publique)
R/O	Lecture seule (gestion des droits)
R/W	Accès en lecture et écriture (gestion des droits)
TCP	Transmission Control Protocol Groupe de protocoles de communication
TLS	Transport Layer Security (protocole de chiffrement)
WSS	Web Services Security, protocole de communication

4 Données d’application

4.1 Utilisateurs Windows et groupes d'utilisateurs Windows

Les utilisateurs et groupes d’utilisateurs doivent être configurés pour exécuter l'application MPW. Les utilisateurs avec les ID 3,4,5 et 6 sont installés avec MPW Installer.

ID	Utilisateurs Windows Groupes d’utilisateurs Windows	Description
1	Personnel d'entretien spécialisé	Le personnel d'entretien spécialisé est responsable de l'installation et de la maintenance du logiciel et de l'installation des correctifs.
2	Utilisateurs non autorisés du serveur Windows	Tous les utilisateurs et processus qui ne sont pas nécessaires pour exécuter l'application MPW.
3	*mpw-gateway-wrapper*	Nom du processus Windows de l'utilisateur du service Windows utilisé pour exécuter le MPW Gateway Wrapper.
4	*mpw-gateway-fetcher*	Nom du processus Windows de l'utilisateur du service Windows utilisé pour exécuter le MPW Gateway Fetcher. Le MPW Gateway Fetcher reçoit les données traitées dans le Gateway Wrapper de la passerelle Infinity Gateway. Selon la version, le nom *mpw-gateway-fetcher-7.2* ou *mpw-gateway-fetcher-8.0* et supérieur peut être utilisé.
5	*mpw-backend*	Nom du processus Windows de l'utilisateur du service Windows utilisé pour exécuter l'application MPW.
6	*postgres*	Nom du processus Windows de l'utilisateur du service Windows utilisé pour exécuter la base de données Postgres. S'il s'agit d'une installation dans un établissement du Department of Defense, la base de données Postgres ne sera pas installée. Au lieu de cela, l'administration des utilisateurs est mappée via Active Directory.

4.2 Gestion des droits pour le serveur Infinity Gateway

Cette section contient des informations sur les droits d'accès aux données de l'application pour les utilisateurs Windows. Les données de l'application doivent être définies explicitement à l'aide du mécanisme de sécurité Windows (ACL).

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

Ce dossier contient les données d'application nécessaires à l'exécution du Gateway Wrapper.

Droits d’accès :

– R/W pour le personnel d'entretien spécialisé
– R/O pour *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Pas d'accès pour les utilisateurs non autorisés du serveur Windows

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

Ce fichier contient les configurations et les paramètres nécessaires au fonctionnement sécurisé de la MPW.

Droits d’accès :

– R/W pour le personnel d'entretien spécialisé
– R/O pour *mpw-gateway-wrapper*, *mpw-gateway-fetcher*
– Pas d'accès pour les utilisateurs non autorisés du serveur Windows

4.3 Gestion des droits pour le serveur MPW

Cette section contient des informations sur les droits d'accès aux données de l'application pour les utilisateurs Windows.

C:\ProgramData\mpw-pgdata

Ce dossier est un emplacement de stockage pour les fichiers de base de données qui contiennent les informations de connexion des utilisateurs de la MPW. S'il y a une connexion à AD avec la MPW, ce dossier n'existe pas.

Droits d’accès :

– R/W pour le personnel d'entretien spécialisé et *postgres*
– Pas d'accès pour les utilisateurs non autorisés du serveur Windows

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

L'affichage des paramètres de l'appareil peut être configuré dans ce fichier.

Droits d’accès :

– R/W pour le personnel d'entretien spécialisé
– R/O pour *mpw-backend*
– Pas d'accès pour les utilisateurs non autorisés du serveur Windows et *postgres*

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

Ce fichier contient des exemples de configuration pour l'affichage des paramètres de l'appareil. Ce fichier n'est pas installé dans un établissement du Department of Defense.

Droits d’accès :

– R/W pour le personnel d'entretien spécialisé
– R/O pour *mpw-backend*
– Pas d'accès pour les utilisateurs non autorisés du serveur Windows et *postgres*

C:\Program Files\Draeger\MPW-Backend

Ce dossier contient les données d'application nécessaires à l'exécution de l'application MPW.

Droits d’accès :

– R/W pour le personnel d'entretien spécialisé
– R/O pour *mpw-backend*
– Pas d'accès pour les utilisateurs non autorisés du serveur Windows et *postgres*

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

Ce fichier contient les configurations et les paramètres nécessaires au fonctionnement sécurisé de la MPW.

Droits d’accès :

– R/W pour le personnel d'entretien spécialisé
– R/O pour *mpw-backend*
– Pas d'accès pour les utilisateurs non autorisés du serveur Windows et *postgres*

4.4 Fichier application.properties

4.4.1 Serveur web Gateway-Wrapper

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

Exemples d'entrées	Description
logging.level.org.springframework=INFO	Configuration du niveau de journalisation pour Spring
logging.level.com.draeger=TRACE	Configuration du niveau de journalisation pour la MPW
server.port=8443	Port du serveur web
igw.user=<user>	Utilisateur Infinity Gateway
igw.password=<password>	Mot de passe Infinity Gateway

4.4.2 Serveur web MPW

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

Exemples d'entrées	Description
logging.level.org.springframework=INFO	Réglage d'événements spécifiques à l'application
logging.level.com.draeger=TRACE	Réglage d'événements d'analyse spécifiques à l'application
logging.level.com.draeger.upw.mpw.backend.log.session=OFF	Réglage pour la journalisation de tous les événements de la session utilisateur
server.port=8444	Port du serveur web pour les clients de navigateur
mpw.session.mobile.timeout=30	Délai d'expiration de session relatif pour les clients mobiles
mpw.session.desktop.timeout=120	Délai d'expiration de session relatif pour les clients de bureau
mpw.session.absolute.timeout=720	Délai d'expiration de session absolu pour tous les clients
server.ssl.keyStoreType=PKCS12	Certificat de type keystore
server.ssl.key-store-password=<password>	Mot de passe de certificat PKI
gateway.url=https://<gateway.server.name>:8444	Informations de connexion pour le Gateway Wrapper
spring.datasource.password=<password>	Mot de passe de la base de données dans l’administration des utilisateurs (non utilisée s’il y a une connexion à AD)

Exemples d'entrées	Description
spring.datasource.username=<postgres.user-name>	Utilisateur de la base de données dans l'adminis-tration des utilisateurs (non utilisé s'il y a une connexion à AD)
server.name=<MPW domain>	Nom de domaine pour la MPW Le nom de domaine doit correspondre au nom de domaine figurant sur le certificat
ad.domain	Pour plus d’informations voir : "Active Directory", page 19.
ad.url	
ad.searchFilter	
ad.groupMapping [<<Groupe AD>>]=<<Service>>	
ad.groupMapping[Médecins]=ICU	
ad.groupMapping[Médecins]=OP1,OP2	
ad.groupMapping[Médecins\ BO]=OP	

5 Règles relatives au pare-feu

5.1 Serveur web Gateway Wrapper

Par défaut, l'application démarre sur le port 8443. Ce port est utilisé par défaut lors de l'installation. Le réglage par défaut peut avoir été modifié via le fichier *application.properties*. Pour cela, rechercher le *server.port*. Le port doit être activé sur "Inbound Rule" (TCP).

5.2 Serveur web MPW

Par défaut, l'application démarre sur le port 8444. Ce port est utilisé par défaut lors de l'installation. Le réglage par défaut peut avoir été modifié via le fichier *application.properties*. Pour cela, rechercher le *server.port*. Le port doit être activé sur "Inbound Rule" (TCP).

5.3 Connexions

Pour permettre la connexion au serveur frontal et au serveur principal, les connexions HTTPS et les connexions WSS doivent être autorisées dans le réseau. Le *server.port* du serveur principal sert de port pour le WSS (WebSocket, équivalent à HTTPS). Pour plus d’informations voir : "Fichier application.properties", page 13.

5.4 Règles relatives au pare-feu et à la protection antivirus

Le pare-feu sur la passerelle Infinity Gateway et le serveur principal doivent tous les deux être compatibles avec le port HTTPS/WSS sur "inbound".

Les antivirus suivants ont été testés pour une utilisation sur le serveur principal :

– McAfee 5 avec niveau de confidentialité moyen

Tous les dossiers du serveur principal sont sûrs pour une recherche de virus.

6 Journalisation

6.1 Niveaux de journal

Toutes les applications qui sont fournies avec la MPW écrivent des journaux dans le journal d'événements Windows. Au démarrage, les applications vérifient que le système d'enregistrement fonctionne. Si une erreur apparaît, l'application ne démarre pas. Les erreurs du journal en fonctionnement figurent dans l'observateur d'événements (Event Viewer) dans le journal système de Windows avec la source "Journal d'événements". Après l'installation, la MPW génère tous les événements avec le niveau de journal "Information", "Warning" ou "Error." Les niveaux de journal suivants sont disponibles :

Niveau de journal	*application.properties*	Description
TRACE	logging.level.org.springframework=TRACE logging.level.com.draeger=TRACE	Désigne des événements d'informations plus détaillés que le niveau de journal DEBUG.
DEBUG	logging.level.org.springframework=DEBUG logging.level.com.draeger=DEBUG	Désigne les événements d'informations détaillés les plus utiles pour corriger les erreurs dans une application.
INFO	logging.level.org.springframework=INFO logging.level.com.draeger=INFO	Désigne les messages d'information qui indiquent l'avancement de l'application à un niveau indifférencié.
WARN	logging.level.org.springframework=WARN logging.level.com.draeger=WARN	Désigne les situations potentiellement incorrectes.
ERROR	logging.level.org.springframework=ERROR logging.level.com.draeger=ERROR	Désigne les événements d'erreur qui peuvent permettre à l'application de continuer à fonctionner.

Pour changer les niveaux de journal, le fichier *application.properties* de la MPW et du Gateway Wrapper doivent être adaptés comme indiqué dans le tableau (Voir "Fichier application.properties", page 13). Le réglage par défaut après l'installation est "INFO".

6.2 Journalisation des sessions

Le journal des sessions (*mpw-backend-sessions.log*) contient potentiellement des informations personnelles telles que l'adresse IP et le nom d'utilisateur. Pour désactiver la journalisation des sessions, la ligne suivante doit être présente dans le fichier *application.properties* :

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

Pour plus d'informations voir : "Serveur web MPW", page 13.

6.3 Délai d'expiration de session

Après l'installation, les délais d'expiration de session par défaut sont de 30 minutes pour une utilisation mobile et de 120 minutes pour une utilisation de bureau. La durée des délais d'expiration de session doit être configurée conformément à la politique de confidentialité de l'établissement de santé. Les valeurs peuvent être configurées dans le fichier *application.properties*.

application.properties	Description
mpw.session.mobile.timeout=30	Délai d'expiration de session relatif La session se termine une fois la période de temps définie écoulée si l'utilisateur n'a effectué aucune action pendant cette période.
mpw.session.desktop.timeout=120	
mpw.session.absolute.timeout=720	Délai d'expiration de session absolu La session est toujours terminée une fois cette période de temps définie écoulée.

L'unité est la minute et la valeur doit être comprise entre 1 et 720 minutes.

Pour plus d’informations voir : "Serveur web MPW", page 13.

6.4 Recherche d'événements

6.4.1 Observateur d'événements

Pour faciliter la recherche les journaux de la MPW, un journal séparé nommé "Draeger" est créé sur les serveurs respectifs pendant l'installation du serveur principal MPW et MPW Gateway Wrapper.

L'observateur d'événements (Windows Event Viewer) possède des fonctions de gestion des événements enregistrés (p. ex. archivage, rotation, stockage, suppression ou transfert d'événements). Des informations complémentaires se trouvent dans la base de connaissances Microsoft.

Dans l'observateur d'événements (Windows Event Viewer), les événements sont généralement catégorisés selon les propriétés suivantes : *niveau*, *source*, *ID événement* et *Catégorie de tâche*. À l'exception de la *Catégorie de tâche*, ces propriétés peuvent être utilisées pour filtrer les journaux de la MPW.

– *Catégorie de tâche* n’est pas utilisé.
– La *Source* correspond au nom de l'application MPW et peut donc contenir l'une des valeurs suivantes : *MPW-Backend*, *Bulkport*, *PasswordResetter*, *UserAdmin*, *PostgreSQL* et *MPW-Gateway-Wrapper*.
– *ID événement* sert à catégoriser les contenus des entrées du journal. Ci-dessous se trouve une liste indiquant la façon dont les entrées du journal de la MPW sont catégorisées en fonction des *ID événement*.

6.4.2 ID événement pour la recherche d'événements

Le réglage par défaut pour le niveau de journal est "Information" et contient les niveaux de journal "Warning" et "Error"

ID événement	Applications	Description
10	MPW Backend, Bulkport, PasswordResetter, UserAdmin, MPW Gateway Wrapper	Journaux spécifiques à l'application
11[1)]	Serveur principal MPW	Événements de session de connexion (par exemple, tentatives de connexion ayant réussi ou échoué)
0[2)]	PostgreSQL	Base de données interne d'administration des utilisateurs du serveur principal
12	Informations sur la communication	Adresses IP des systèmes connectés. Tentatives d'accès ou de modification d'objets de sécurité ayant réussi ou échoué.
13	Informations sur la session	Délai d'expiration de session, suppression, renouvellement des ID session utilisateur
15	Authentification utilisateur	Tentatives de connexion ayant réussi ou échoué
16	Tentatives d'accès aux informations de débogage ayant réussi ou échoué	Page d'intégrité (Health page)

1) La journalisation des sessions doit être explicitement activée car les journaux contiennent le nom d'utilisateur et l'ID de session. Avant l'activation, se renseigner sur les dispositions légales en matière de protection de la vie privée des utilisateurs et s'assurer du respect de ces dispositions.
2) Les entrées du journal PostgreSQL proviennent directement de la base de données PostgreSQL. Dräger n'a aucune influence sur le contenu de ces entrées du journal (c'est pourquoi l'ID événement est 0). De plus, Dräger ne modifie pas les paramètres par défaut en ce qui concerne le niveau de journal ou équivalent pour PostgreSQL.

6.4.3 Entrées non incluses dans le journal Dräger

Les événements suivants ne sont pas écrits dans le journal Draeger :

– Démarrage et arrêt des services
  Windows écrit automatiquement les entrées du journal pour démarrer et arrêter les services de la MPW installés dans le journal système. Ces entrées de journal figurent ici sous la source "Service Control Manager" et sont accessibles en recherchant par exemple "mpw-backend" ou "mpw-gateway-wrapper".
– Modifications de fichiers
  Windows peut enregistrer les accès aux fichiers, par exemple aux fichiers de configuration, via la politique système de fichier d’audit (Audit File System Policy). Les entrées correspondantes sont enregistrées dans le journal sécurité.

7 Configuration

7.1 Active Directory

Touche	Valeur
ad.domain	Domaine AD (p. ex. *company.com*)
ad.url	URL AD (p. ex. *ldaps://ad.company.com*)
ad.rootDn	RootDn de l'AD (si nécessaire)
ad.searchFilter	Filtre de recherche pour AD pour trouver des utilisateurs autorisés dans l'AD Paramètre par défaut : *(&(objectClass=user)(userPrincipalName={0}))* Pour "[...]*Name={0}*", {0} est remplacé par "username@domain" durant la recherche. Pour "[...]*Name={1}*", *{1}* est remplacé par le nom d'utilisateur ("username") durant la recherche.

Pour déterminer quel groupe AD peut voir quel groupe d'espaces de travail, il faut faire un mapping dans le fichier *application.properties* entre le nom du groupe AD et le nom du groupe d'espaces de travail.

Pour chaque groupe d'AD mappé, une ligne doit être insérée dans le fichier de configuration avec le format suivant :

ad.groupMapping[<<Groupe AD>>]=<<Service>>

ℹ La désignation de <<Service>> doit correspondre à la désignation correspondante sur le réseau de l'Infinity Gateway.

<<Groupe AD>> et *<<Service>>* doivent être remplacés par le nom voulu. Par exemple, pour permettre au groupe d'AD "Médecins" d'accéder au groupe d'espaces de travail de l'"UCI" (service), la ligne suivante doit être ajoutée :

ad.groupMapping[Médecins]=ICU

Si un groupe d'AD particulier doit avoir accès à plusieurs groupes d'espaces de travail, ces groupes doivent être spécifiés l'un après l'autre, séparés par une virgule.

Exemple : *ad.groupMapping[Médecins]=OP1,OP2*

Les espaces dans le nom du groupe d'AD doivent être spécifiés avec "\" + "espace".

Exemple : *ad.groupMapping[Médecins\ BO]=OP*

7.2 Retrait des utilisateurs d'AD

Les utilisateurs qui ont été supprimés de l'Active Directory et qui disposent encore d'une session utilisateur valide peuvent être exclus de l'utilisation en redémarrant le service Windows MPW-Backend. Le redémarrage du MPW-Backend met fin à toutes les sessions utilisateur. Si le MPW-Backend n'est pas redémarré, la session sera interrompue au plus tard à l'expiration du délai absolu de la session.

8 Sauvegarde et récupération d'urgence

Pour pouvoir réinstaller le système en cas de problèmes, il faut créer une sauvegarde. La MPW doit ensuite être réinstallée et tous les fichiers de configuration doivent être importés depuis la sauvegarde.

Pour cela, les fichiers de configuration suivants sont nécessaires :

Passerelle

– *application.properties*

Serveur principal MPW

– *application.properties*
– *device-parameter-config-sample.csv*
– Le certificat utilisé. Le fichier correspondant peut être modifié dans le fichier *application.properties* (valeur par défaut : *cert.p12*).

Si le matériel complet est remplacé, la licence doit être réinstallée. Avant de remplacer le matériel, contacter le personnel d'entretien spécialisé.

Si la MPW a été installée avec la base de données utilisateur interne, la base de données utilisateur doit d'abord être sauvegardée puis réinstallée. Pour cela, contacter le personnel d'entretien spécialisé.

9 Public key infrastructure (infrastructure à clé publique)

Pour utiliser le PKI interne, le certificat de serveur peut être importé pendant l'installation. Après l’installation, le certificat du serveur peut être modifié dans le fichier *application.properties*. Les entrées suivantes doivent être adaptées à cet effet :

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

Pour que le certificat soit considéré comme digne de confiance, le nom de domaine "server.name" dans le fichier *application.properties* doit correspondre au nom de domaine dans le certificat.

10 Certificat

10.1 Installation de l'entrée TrustedRoot pour le certificat TLS de la MPW sur les clients

Si le certificat racine de l'hôpital n'a pas déjà été déployé sur les clients, le certificat racine doit être installé sur les clients.

ℹ Actuellement, seuls Microsoft Edge, Google Chrome et Apple Safari (iOS) sont autorisés.

ℹ Le certificat racine n'est pas le même que celui utilisé par le serveur principal. Le certificat racine a signé le certificat du serveur principal.

S'il est possible de se connecter à l'appareil, cela signifie que le certificat a été installé avec succès. Il ne suffit pas de pouvoir ouvrir l'écran de connexion, il faut également pouvoir se connecter.

10.1.1 Microsoft Windows

Il faut s'assurer que le navigateur utilisé fait confiance au certificat utilisé sur le serveur.

Pour l’installation manuelle :

1. Double-cliquer sur le fichier du certificat.
   ⇒ Le gestionnaire de certificats de Windows s’ouvre.
2. Ajouter le certificat en tant que racine (Auto Detection ne le reconnaît pas correctement).

10.1.2 Apple iOS

Il faut s'assurer que le navigateur utilisé fait confiance au certificat utilisé sur le serveur.

Pour l’installation manuelle : Le certificat racine doit d'abord être envoyé par e-mail à une boîte aux lettres accessible depuis l'iPhone. Le certificat ne peut être installé que si l'e-mail est ouvert dans l'application ***Mail*** et que le certificat joint est sélectionné. Le code PIN de l'appareil est nécessaire.

En cliquant sur le certificat, il est d'abord installé comme non fiable. Pour activer la fiabilité, effectuer l'étape suivante :

Réglages > ***Général*** > ***À propos*** > ***Paramètres du certificat*** > ***Activer une confiance totale pour le certificat racine***.

Le certificat peut à nouveau être supprimé dans ***Général*** > ***Profil***.

11 Désinstallation

Afin de supprimer complètement toutes les données sensibles, Dräger recommande de réinstaller l'ordinateur après avoir désinstallé le logiciel.

12 Entretien

12.1 Définition du terme « entretien »

Concept	Définition
Entretien	Toutes les mesures (inspection, maintenance, réparation) visant à préserver ou à restaurer l'intégrité fonctionnelle d'un produit
Inspection	Mesures destinées à déterminer et évaluer l'état actuel d'un produit
Maintenance	Mesures spécifiées et régulières destinées à préserver l'intégrité fonctionnelle d'un produit
Réparation	Mesures destinées à restaurer l'intégrité fonctionnelle d'un produit après une panne

Un contrat d'entretien avec Dräger est recommandé.

12.2 Maintenance

Composant	Intervalle	Mesure	Groupe d’utilisateurs
Certificat TLS	Comme spécifié par le client	Renouveler les certificats TLS	Personnel d'entretien
Disque dur	Tous les 2 ans	Contrôler l’espace sur le disque dur	Personnel d'entretien
		Archiver et supprimer les fichiers journaux si nécessaire	

Mises à jour de sécurité

Les Service Packs et les correctifs tels que ceux de Microsoft Windows, comblent les failles de sécurité, éliminent les erreurs ou améliorent les fonctions. Dräger publie de nouvelles mises à jour de sécurité à installer dans la MPW. Respecter les points suivants quant à la gestion des mises à jour de sécurité :

- Désactiver la fonction de mise à jour automatique des correctifs et des Service Packs sur le serveur MPW.
- Lorsqu'une nouvelle mise à jour de sécurité est publiée, attendre qu'elle soit publiée par Dräger pour le système MPW. Si Dräger ne soulève aucune objection dans un délai de 4 semaines suivant la publication d'une mise à jour de sécurité, celle-ci sera considérée comme publiée pour MPW.
- Si un système de test est disponible, Dräger recommande de tester la nouvelle mise à jour de sécurité dans le système de test.

13 Caractéristiques techniques

13.1 Configuration requise

13.1.1 Environnement logiciel et infrastructure

Versions de l'Infinity Gateway Avec l'option API WinAccess	7.2, 8.0, 9.0
WLAN dans la zone d'application	
Bande passante	Au moins 1 Gbit/s sur le réseau reliant les sources de données et les serveurs.
Ports	8443 (réglage par défaut), configurable

13.1.2 Serveur

Serveur pour logiciel (Mobile Patient Watch)

Système d'exploitation	Windows Server 2016 (serveur physique ou virtuel)
Processeur	8 cœurs de processeur avec fréquence de Boost à 3200 MHz
Mémoire de travail (RAM)	32 Go
Disque dur SSD	2 TB

Serveur pour Infinity Gateway

Un logiciel supplémentaire doit être installé sur le matériel de l'Infinity Gateway pour recevoir les données, ce qui augmente la configuration requise pour le matériel. Aucun autre logiciel que celui-ci ne peut être installé sur le même serveur qui utilise Infinity Gateway comme source de données.

Il en résulte la configuration requise suivante :

Système d'exploitation	Windows Server 2016 (serveur physique ou virtuel)
Processeur	8 cœurs de processeur à 3000 MHz
Mémoire de travail (RAM)	32 Go
Disque dur SSD	60 Go

13.1.3 Clients

Clients recommandés

Le logiciel peut être entièrement affiché et utilisé sur les appareils recommandés. Une vitesse de balayage conforme aux spécifications est garantie.

Utilisation mobile	
Système d'exploitation	iOS 14
Navigateur	Apple Safari (version actuelle)

Utilisation mobile	
Résolution graphique	– 2436 x 1125 px (458 ppi) – 2532 x 1170 px (460 ppi) – 2688 x 1242 px (458 ppi)

Utilisation de bureau	
Système d’exploitation	Windows 10 (version actuelle)
Navigateur	Microsoft Edge (version actuelle) Google Chrome (version actuelle)
Résolution graphique	1920 x 1080 pixels (24 in)

Clients compatibles

Le logiciel peut être entièrement affiché et utilisé sur les appareils compatibles. La vitesse de balayage peut s'écarter de la spécification, mais reste toujours la même sur le même appareil.

Utilisation mobile	
Clients avec le système d'exploitation iOS	
Version	iOS 14 et supérieure (version actuelle)
Navigateur	Apple Safari (version actuelle)
Résolution graphique	1136 x 640 px à 2688 x 1242 px
Densité de pixels	326 ppi à 476 ppi
Proportions	1,8:1 à 2,2:1
Clients avec le système d'exploitation Android	
Version	Android 9 et supérieure (version actuelle)
Navigateur	Chrome (version actuelle)
Processeur	Octa-Core 1,6 GHz (+)
Résolution graphique	1280 x 720 px à 3200 x 1440 px
Densité de pixels	294 ppi à 563 ppi
Proportions	1,8:1 à 2,2:1

Utilisation de bureau	
Système d’exploitation	Windows 10 (version actuelle)
Navigateur	Microsoft Edge (version actuelle) Google Chrome (version actuelle)
Résolution graphique	Est choisie par l'exploitant.

La documentation technique comprenant des informations complémentaires peut être obtenue sur demande.

13.2 Caractéristiques de fonctionnement

Classification

Classification européennes des dispositifs médicaux	Classe IIb
Code UMDNS, Système de nomenclature universelle des dispositifs médicaux	17223
Code GMDN, Nomenclature mondiale des dispositifs médicaux	44101

13.2.1 Précision d'affichage

Pour les plages de valeurs, la précision d'affichage des courbes, les valeurs numériques et les taux d'échantillonnage des tendances, se référer aux informations des notices d'utilisation de la Mobile Patient Watch et de l’Infinity Gateway.

13.3 Communication réseau

Source de données :	Ordinateur Infinity Gateway avec un composant Gateway Wrapper
Serveur principal :	Communique avec la passerelle Infinity Gateway via une connexion IP cryptée sur le port 8443 (réglage par défaut qui peut avoir été effectué lors de l'installation).
Clients (PC ou appareils mobiles) :	Communiquer avec le serveur principal via une connexion HTTPS et une connexion WSS sur le port 8444 (par défaut qui peut avoir été ajusté pendant l'installation).

13.4 Connexions aux réseaux informatiques

Dans un réseau informatique, les données peuvent être échangées par des technologies filaires et sans fil. Un réseau informatique peut être une interface de données telle que décrite dans les normes et les conventions.

En cours de fonctionnement, ce produit peut échanger des données avec d’autres appareils par le biais de réseaux informatiques et prend en charge les fonctions suivantes :

– Affichage des courbes et des données de paramètres
– Visualisation du lit grâce à l'accès à distance
– Transfert des réglages du dispositif et des données patient

Le raccordement de ce produit à un réseau intégrant d’autres dispositifs ou les modifications ultérieures de ce réseau peuvent causer de nouveaux risques pour les patients, les utilisateurs et les tiers. Avant de raccorder le produit au réseau ou de modifier le réseau, il convient d’identifier, d’analyser et d’évaluer ces risques et de prendre les mesures adéquates.

Exemples de modifications ultérieures du réseau :

– Modification de la configuration du réseau
– Retrait d’appareils et du logiciel du réseau
– Ajout de nouveaux appareils et de logiciel dans le réseau
– Mises à jour ou à niveau des appareils et logiciels connectés au réseau

Pour assurer une communication sûre entre le serveur et le client, une infrastructure TLS doit être en place. Pour cela, un certificat doit être installé sur les clients.

13.4.1 Informations concernant la connexion à un réseau informatique

13.4.1.1 Prérequis :

Seul le personnel d'entretien spécialisé est autorisé à connecter ce dispositif au réseau. Consulter impérativement le responsable informatique de l’établissement de santé au préalable.

Respecter les documents suivants :

– Documents joints à ce produit
– Descriptions du réseau

Dräger recommande de se conformer à la norme CEI 80001-1 (Application du management du risque aux réseaux des technologies de l'information contenant les dispositifs médicaux).

13.4.1.2 Connexion de sources de données principales

Les sources de données principales sont connectées uniquement par Infinity Gateway. Pour en savoir plus sur la connexion des sources de données principales, consulter les informations produit de l'Infinity Gateway.

13.4.1.3 Raccordement de clients sur des réseaux

– La topologie des réseaux locaux est généralement en étoile. Les dispositifs peuvent être regroupés à l’aide de commutateurs de niveau n. Des réseaux locaux virtuels distincts permettent de découpler d’autres flux de données. Configurer les réglages réseau du produit conformément à cette notice d'utilisation et aux spécifications du réseau.
– Les spécifications des connexions du réseau local sont décrites dans les normes suivantes :
  – Réseaux filaires : IEEE 802.3
  – Réseaux sans fil : IEEE 802.11 (b, g, n)
– Si le produit est utilisé avec un commutateur de niveau 2 ou 3, les réglages du port doivent être configurés sur le commutateur réseau. Avant d’expédier le produit, Dräger peut configurer les réglages réseau du produit pour qu’ils soient compatibles avec les spécifications de l’exploitant.
– Ce produit échange des données avec d'autres dispositifs médicaux sur le réseau LAN. Le réseau doit supporter les transmissions et protocoles suivants :
  – TCP/IP
  – Unicast (adressage statique ou or dynamique avec les protocoles de communication ARP ou RARP)

- Multicast
- Broadcast
- IGMP (version 2)

Ce produit peut rejoindre ou quitter un groupe de multidiffusion IP en utilisant le protocole de communication IGMP.

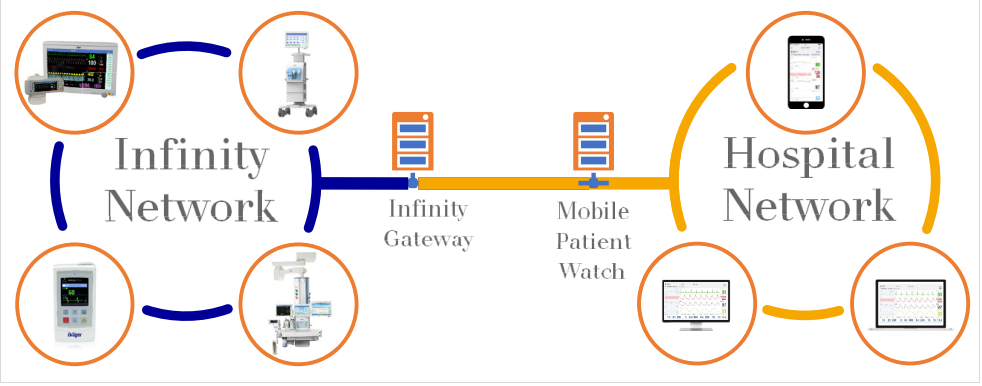
13.4.1.4 Conséquences de l’utilisation d'un réseau inadapté

Le non-respect des exigences de réseau peut être dangereux. Les situations suivantes peuvent survenir avec ce produit :

- En raison d’une interruption de la connexion réseau :
  - Les données ne sont pas affichées ou leur affichage est retardé.
- Sans pare-feu :
  - Les données ne sont pas protégées.
  - Les réglages du produit sont modifiés.
- Les données envoyées sont incomplètes, envoyées au mauvais produit ou pas du tout envoyées.
- Les données patient sont interceptées, falsifiées ou endommagées.
- Les données ont des estampilles temporelles incorrectes.

13.4.1.5 Propriétés requises

Les sources de données principales et l’Infinity Gateway se trouvent sur le même réseau. Les propriétés requises s'appliquent à ce réseau. Observer les informations produit de l’Infinity Gateway à ce sujet. Le serveur MPW reçoit les données à l'aide du MPW-Gateway-Wrapper installé sur le même serveur que l’Infinity Gateway. La MPW peut être utilisée dans un réseau hospitalier qui connecte tous les clients au serveur MPW. Cela nécessite des droits d’accès.



Pour plus d'informations sur les règles relatives au pare-feu, se reporter aux "règles relatives au pare-feu" dans le guide d'installation.

Le réseau sur lequel la MPW est installée et fonctionne doit être contrôlé par l'exploitant.

Prendre des précautions pour empêcher tout accès non autorisé et la propagation de programmes malveillants sur le réseau. Les précautions suivantes, par exemple, peuvent être prises :

- Restreindre l'accès physique aux prises réseau actives
- Seuls les ports nécessaires au fonctionnement peuvent être configurés. Tous les autres ports doivent être fermés.
- Seuls les appareils ayant le même niveau de confiance ou un niveau de confiance supérieur sont autorisés sur le réseau.
- Isolement réseau sécurisé (physique ou virtuel)
- Utilisation d'un pare-feu
- Gestion des correctifs pour les appareils
- Mise en œuvre conforme ISO/CEI 27033

13.4.1.6 Utilisation du réseau

Données par patient envoyées entre le Gateway-Wrapper et le MPW-Backend

Nombre de sessions du navigateur	En amont [kb/s]	En aval [b/s]	Type de données
1	689,63	32,11	Les données transmises se composent principalement des données pertinentes à afficher pour la MPW, comme les paramètres, les données de tendance et les courbes. Le paramétrage test a mesuré le débit de données pour un patient avec 17 paramètres par défaut, 4 jeux de données de surveillance avec les tendances et courbes associées avec un nombre croissant de sessions. Les données montrent que le trafic de données entre le Gateway-Wrapper et le MPW-Backend reste relativement stable. On peut supposer une augmentation du trafic de données si le nombre de patients consultés en même temps change.
2	666,8	31,00	
3	698,54	31,92	
4	652,04	30,37	

Données envoyées entre le MPW-Backend et le client

Nombre de sessions du navigateur	En amont [kb/s]	En aval [b/s]	Type de données
1	78,39	19,00	Le paramétrage test est inchangé. Les données montrent que le trafic de données entre le MPW-Backend et le client (terminal) augmente proportionnellement. On peut supposer une augmentation du trafic de données lorsque le nombre de sessions du navigateur augmente.
2	152,64	37,31	
3	246,36	57,22	
4	317,46	72,64	

13.4.1.7 Nombre d'appareils pris en charge

Une fois le logiciel installé, les données de 45 espaces de travail (moniteurs de patients) max. peuvent être affichées simultanément sur 100 clients maximum.

Index

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

CE 0123

www.draeger.com

9510547 – 6405.022 fr

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