



Digistat® Care

Manuel de l'utilisateur

Version 7.0

2020-12-31

Digistat® Care version 1.1

Digistat® Care est produit par Ascom UMS s.r.l (<http://www.ascom.com>).



Digistat® Care est un produit porteur de marquage ⁰⁴⁷⁶ conformément à la directive 93/42/CEE et (“dispositifs médicaux”) et modifiée par la directive 2007/47/EC.

Ascom UMS est certifié au titre de la norme CEI EN ISO 13485:2012 pour «*Product and specification development, manufacturing management, marketing, sales, production, installation and servicing of information, communication and workflow software solutions for healthcare including integration with medical devices and patient related information systems*».

License Logiciel

Digistat® Care ne doit être utilisé qu'après obtention d'une licence valide d'Ascom UMS ou du distributeur.

Licences et marques enregistrées

Digistat® est une marque enregistrée D'Ascom UMS s.r.l. Toutes les autres marques enregistrées sont la propriété de leur détenteurs respectifs.

Aucune partie de la présente publication ne peut être reproduite, transmise, transcrite ou enregistrée sur quelque support que ce soit ni ne peut être traduite dans une langue quelconque, sous quelque forme et par quelque moyen que ce soit, sans l'autorisation écrite d'Ascom UMS.

Contenu

1. Utilisation du guide.....	5
1.1 Objectifs	5
1.2 Conventions typographiques utilisés et terminologie	6
1.3 Conventions	6
1.4 Symboles	7
1.5 Aperçu de la Digistat Suite	8
1.6 Digistat Suite « About Box »	8
2. Digistat Care	9
2.1 Usage prévu	10
2.2 Utilisation “off-label” du Digistat Care.....	11
2.3 Population de patients	11
2.4 Avertissements de sécurité	11
2.5 Risques résiduels	13
2.6 Responsabilités de l'organisation des soins de santé	14
2.7 Responsabilité du fabricant	14
2.8 Traçage du produit	15
2.9 Système de surveillance après-vente	15
2.10 Vie du Produit.....	15
3. Spécifications du logiciel et du hardware.....	16
3.1 Central & Bedside	17
3.1.1 Hardware	17
3.1.2 Logiciel d'exploitation	17
3.1.3 Logiciel de système	17
3.2 Serveur	18
3.2.1 Hardware	18
3.2.2 Logiciel d'exploitation.....	18
3.2.3 Logiciel de système.....	18
3.3 Digistat Mobile.....	18
3.4 Digistat “Web”	19
3.5 Avertissements.....	19
3.6 Fonctionnalité de streaming audio/vidéo	20
3.7 Parefeu et antivirus	21
3.7.1 Autres précautions recommandées pour la cyberprotection	22
3.8 Caractéristiques du réseau local.....	23
4. Avant le démarrage.....	24
4.1 Avertissements sur l'installation et la maintenance	24

4.2 Politique de confidentialité	25
4.2.1 Caractéristiques et utilisation des informations d'identification de l'utilisateur.....	28
4.2.2 Administrateurs système.....	29
4.2.3 Journal système.....	29
4.2.4 Investigation du log	29
4.3 Dispositifs compatibles	30
4.3.1 Dispositifs DAS.....	30
4.3.2 Dispositifs DIS	31
4.3.3 Avertissements	32
4.4 Distribution des alarmes sans danger pour un seul défaut (« single fault safe »)....	34
4.4.1 Tour d'alarme LED.....	35
4.5 Fiabilité du système	36
4.5.1 Ordinateur de bureau	36
4.5.2 Mobile.....	37
4.5.3 Causes de non fiabilité	38
4.6 Indisponibilité du système	39
5. Coordonnées du fabricant.....	40

1. Utilisation du guide

Ce manuel d'utilisation doit être utilisé en combinaison avec les manuels spécifiques aux modules, listés ci-dessous. Reportez-vous aux manuels applicables, en fonction des modules utilisés dans l'organisation des soins de santé:



USR FRA Controlbar
USR FRA Smart Central
USR FRA Fluid Balance
USR FRA Infusion
USR FRA Patient Explorer
USR FRA Scoring Calculator
USR FRA Smart Monitor
USR FRA Smart Monitor Web
USR FRA MDI Web
USR FRA Vitals Web
USR FRA Smart Central Mobile
USR FRA Vitals Mobile
USR FRA Mobile Launcher

1.1 Objectifs

Ce manuel fournit toutes les informations nécessaires pour une utilisation sûre et correcte de Digistat Care et permet l'identification du fabricant. En outre, c'est un guide de référence pour l'utilisateur qui souhaite savoir comment effectuer des opérations spécifiques et pour utiliser correctement le logiciel afin de prévenir toute maladresse potentiellement dangereuse.

1.2 Conventions typographiques utilisés et terminologie

L'utilisation de Digistat Care nécessite une connaissance de base des termes et des concepts informatiques les plus courants. De même, pour comprendre le contenu de ce manuel.

Par ailleurs, l'utilisation de Digistat Care ne doit être accordée qu'à un personnel professionnel qualifié, certifié et formé.

Par rapport au manuel papier la version „on line“ du document contient des liens hypertextes. Ceci signifie qu'à chaque référence d'une image ("Fig 10", par exemple) ou à un paragraphe ("paragraphe 2.2.1", par exemple), vous pouvez cliquer la référence et accéder directement à telle image ou tel paragraphe en particulier.

Les données cliniques affichées dans les images contenues dans les manuels d'Ascom UMS sont des exemples créés dans un environnement de test, dont le seul but est d'expliquer la structure et les procédures du Digistat Care. Elles ne sont pas et ne doivent pas être considérées comme des données réelles extraites de procédures cliniques réelles.



Les pièces relatives à la configuration du Digistat Care sont présentées en anglais dans les manuels Ascom UMS. Ces configurations dépendent des procédures et des noms adoptés par l'organisation de soins de santé utilisant le Produit. Elles seront donc dans la langue demandée par l'organisation de soins de santé.

1.3 Conventions

Les conventions suivantes sont utilisées dans ce document :

- Les noms des boutons, des commandes de menu, des options, des icônes, des champs et de tout élément de l'interface utilisateur avec lequel l'utilisateur peut interagir (toucher, cliquer ou sélectionner) sont formatés en **gras**.
- Les noms/en-têtes d'écrans, de fenêtres et d'onglets sont inscrits entre "guillemets".
- Le code de programmation est formaté dans Courier.
- La puce ➤ indique une action que l'utilisateur doit effectuer pour réaliser une opération spécifique.
- Les références aux documents externes sont en *italique*.

1.4 Symboles

Les symboles suivants sont utilisés dans ce manuel.

Information utiles



Ce symbole apparaît sur le côté de l'information supplémentaire concernant les caractéristiques et emploi de Digistat Care. Ceci peut être un exemple d'explication, des procédures alternatives ou toute autre info 'extra' considérée utile pour une meilleure compréhension du produit.

Avertissement!



Ce symbole est utilisé pour souligner l'information prévenant d'un usage impropre du logiciel ou pour attirer l'attention sur les procédures critiques qui pourraient comporter des risques.

Par conséquent il est nécessaire d'y prêter attention à chaque fois que ce symbole apparaît.

Les symboles suivants sont utilisés dans la zone d'information de la Digistat Suite (« About box »):



Nom et adresse du fabricant



Attention, consulter les documents d'accompagnement



Ce symbole indique la nécessité pour l'utilisateur de consulter le mode d'emploi pour des informations importantes telles que des mises en garde et des précautions qui ne peuvent, pour diverses raisons, être présentées sur le dispositif médical lui-même.

1.5 Aperçu de la Digistat Suite

Digistat Suite est un PDMS modulaire conçu pour créer des solutions répondant aux besoins liés à la gestion des données des patients. Les différentes solutions sont créées afin de permettre aux modules nécessaires qui font partie des deux produits de la suite de fonctionner, à savoir :

- Digistat Docs (dispositif non médical);
- Digistat Care (dispositif médical de classe IIb).

Digistat Docs est un logiciel qui enregistre, transfère, stocke, organise et affiche les informations du patient et celles qui lui sont associées afin d'aider les soignants à établir un dossier électronique du patient.

Digistat Docs n'est pas un appareil médical.

Digistat Care est un logiciel qui gère les informations et les données relatives au patient, y compris les données et les événements provenant d'appareils et de systèmes médicaux, fournissant des informations pour soutenir le traitement, les diagnostics, la prévention, la surveillance, la prévision, le pronostic et la réduction de la maladie.

Digistat Care (dispositif médical de classe IIb).

Les deux produits étant modulaires, l'organisation de soins de santé spécifique peut choisir d'activer tous les modules disponibles ou seulement un sous-ensemble, en fonction de ses besoins et objectifs.

Les modules peuvent être ajoutés à des moments différents. La suite logicielle résultante peut évoluer dans le temps en fonction des modifications éventuelles des besoins de l'organisation. Dans ces cas, une formation supplémentaire spécifique est dispensée et la configuration validée à nouveau avec l'organisation responsable.

1.6 Digistat Suite « About Box »

Le bouton **About** du menu principal affiche une fenêtre contenant des informations sur la version du Digistat Suite, le produit installé et les licences associées.

L'étiquetage réel est celui d'About Box affiché sur les postes de travail clients et les appareils mobiles sur lesquels la Digistat Suite est installé.



Conformément au règlement UE n° 207/2012 du 9 mars 2012, les instructions d'utilisation sont fournies sous forme électronique. La zone « À propos » du produit contient l'adresse d'une ressource Web où la dernière version des instructions d'utilisation peut être téléchargée.

2. Digistat Care

Digistat Care est un système de gestion des données patient et un système d'alarme mettant en œuvre un ensemble varié de fonctionnalités.

Digistat Care permet d'afficher des tableaux de bord pour la surveillance des patients quasiment en temps réel, d'ajouter de nouveaux paramètres collectés à l'intérieur du système, afin de permettre de calculer de nouveaux paramètres dérivés (ex. scores ou CDSS).

Digistat Care s'intègre sur certains appareils médicaux (pompes à perfusion, moniteur patient, ventilateur, dialyseur, etc.) afin d'afficher, sur les PC des postes de travail et sur certains smartphones, une notification secondaire des événements et des alertes aux utilisateurs cliniques.

Digistat Care est capable d'afficher des données provenant à la fois d'appareils non destinés à être utilisés dans un système d'alarme distribué fiable et d'appareils destinés à être utilisés dans un système d'information distribué (non fiable).

Digistat Care est conçu pour fournir une vue d'ensemble de l'état des appareils, mettant en évidence les alarmes ou les avertissements se produisant sur l'appareil connecté sélectionné, afin que l'utilisateur soit informé en un coup d'œil de la situation dans son service.

En outre, Digistat Care introduit les supports portables. Digistat Care fournit également aux cliniciens des informations supplémentaires, telles que des systèmes de notation (même en combinaison avec des appareils portables) et une aide à la décision clinique (c.-à-d. le calcul automatique de l'équilibre hydrique, l'interaction médicamenteuse ou la notification d'allergie du patient).

2.1 Usage prévu

Digistat Care est un logiciel qui transfère, stocke, élabore, regroupe, organise et affiche les informations du patient et les données associées au patient, y compris les données et événements de dispositifs et systèmes médicaux, ainsi que les informations saisies manuellement, afin de piloter la gestion clinique en fournissant des informations pour :

- Soutenir le traitement, les diagnostics, la prévention, la surveillance, la prévision, le pronostic et l'atténuation des maladies.
- Trier ou identifier les premiers signes de maladie ou d'affection.

Digistat Care comprend :

- La collecte de données et d'événements cliniques à partir d'appareils et de systèmes médicaux en temps quasi-réel ;
- La collecte des données saisies par l'utilisateur ;
- L'application de filtres/traitements configurables pour optimiser/réduire la fréquence et le nombre des événements notifiés aux professionnels de la santé afin de présenter les informations cliniquement exploitables ;
- L'affichage des données traitées et les informations de statut des dispositifs médicaux quasiment en temps réel et rétrospectivement, aux professionnels de la santé sur le ou les écrans désignés ;
- Les composants d'un système d'information distribué destiné à permettre aux professionnels de la santé de notifier les alarmes physiologiques et techniques, ainsi que des données cliniques et non cliniques supplémentaires à l'appui de la surveillance des patients ;
- L'acquisition de données et d'événements cliniques, à partir de dispositifs et de systèmes sélectionnés, et transmission fiable d'alarmes physiologiques et techniques aux professionnels de la santé vers des dispositifs d'affichage désignés et vers des systèmes spécifiques ;
- L'élaboration de données pour fournir des informations supplémentaires au clinicien, telles que les systèmes de notation et d'aide à la décision clinique ;
- Le transfert des informations acquises vers des systèmes externes, cliniques et non cliniques, en temps quasi réel via une interface d'abonnement ou de manière rétrospective via une requête de données.

Digistat Docs est un logiciel autonome installé sur un matériel spécifique. Il repose sur l'utilisation et le fonctionnement corrects des dispositifs médicaux, des systèmes, des dispositifs d'affichage et du réseau informatique médical connectés.

Digistat Docs travaille avec Digistat Care, l'autre produit de la Digistat Suite;

Digistat Care est installé dans les établissements de soins, les unités de réanimation et de soins intensifs, les services d'hospitalisation normaux et les autres départements.

La population de patients et les conditions du patient sont établies par les systèmes connectés et par la configuration particulière de Digistat Docs demandée par l'organisation de soins de santé.

Les utilisateurs sont des professionnels de la santé formés.

2.2 Utilisation “*off-label*” du Digistat Care

Toute utilisation du Digistat Care (Produit, ci-après), non-conforme aux indications figurant dans l'Utilisation prévue (généralement appelée utilisation “*off-label*”) se fait à l'entière discrétion et sous l'entière responsabilité de l'utilisateur et de l'organisation responsable.

Le producteur ne garantit aucunement la sécurité du Produit et son adéquation par rapport à son utilisation lorsqu'il est utilisé de manière non-conforme aux indications figurant dans l'Utilisation prévue.

2.3 Population de patients

Le produit est destiné à être utilisé avec des dispositifs et systèmes médicaux et il détermine la population de patients. Le produit présente les limites techniques suivantes :

- Poids du patient entre 0,1 kg et 250 kg
- Taille du patient entre 15 cm et 250 cm

2.4 Avertissements de sécurité

L'Utilisateur devra faire des diagnostics et interventions préventives uniquement sur la vérification directe de la source d'informations. L'Utilisateur a la responsabilité exclusive de vérifier l'exactitude des informations fournies par le Produit, ainsi que de l'usage approprié de ces dernières.

Seuls les imprimés signés numériquement ou sur papier par des médecins professionnels agréés doivent être considérées comme constituant une documentation médicale valable. En signant les susdits imprimés, l'Utilisateur certifie qu'il a vérifié l'exactitude et l'exhaustivité des données figurant sur le document.

Lors de la saisie des données relatives au patient, l'utilisateur a la responsabilité de vérifier l'identité du patient, le département ou l'unité de soins de l'établissement de santé et que les informations relatives au lit affichées dans le produit sont exactes. Cette vérification revêt une importance fondamentale en cas d'actions critiques comme, par exemple, l'administration de médicaments.

L'établissement de santé est responsable de l'identification et de la mise en œuvre des procédures appropriées pour garantir que les erreurs potentielles qui se produisent sur le Produit et/ou dans l'utilisation du Produit soient détectées et corrigées rapidement et qu'elles ne constituent pas un risque pour le patient ou l'opérateur. Ces procédures dépendent de la configuration du produit et de la méthode d'utilisation préférée par l'établissement de santé.

Selon la configuration, le Produit peut donner accès à des informations sur les médicaments. L'établissement de soins de santé est chargé de vérifier initialement et périodiquement que ces informations sont à jour et actualisées.

Afin d'utiliser le Produit dans un environnement clinique, tous les composants du système, dont le Produit, doivent satisfaire à toutes les exigences réglementaires applicables.

Si le Produit fait partie d'un "système médical électrique" par une connexion électrique et fonctionnelle avec des dispositifs médicaux, l'établissement de soin est responsable des tests requis de vérification et d'acceptation de la sécurité électrique, même si Ascom UMS effectue totalement ou partiellement les connexions nécessaires.

Si certains des dispositifs utilisés pour le Produit se trouvent à l'intérieur de l'espace patient ou sont reliés à des équipements qui se trouvent à l'intérieur de l'espace patient, l'organisation de soins de santé a la responsabilité de s'assurer que l'ensemble de la combinaison est conforme à la norme internationale CEI 60601-1 et à toute exigence supplémentaire établie par les réglementations locales.

Le produit est un logiciel autonome pouvant s'exécuter sur des ordinateurs standard et/ou des périphériques mobiles standard connectés au réseau local de l'établissement soins de santé. L'établissement des soins de santé est responsable de protéger de manière adéquate les ordinateurs, les appareils et le réseau local contre les cyberattaques et autres dysfonctionnements.

Le Produit doit être installé uniquement sur des ordinateurs et des dispositifs qui répondent à la configuration matérielle minimum et uniquement sur les systèmes d'exploitation et browsers supportés.

L'utilisation du produit doit être autorisée, au moyen d'une configuration spécifique des comptes utilisateurs et d'une surveillance active, seuls pour les Utilisateurs 1) formés selon les indications du Produit par du personnel autorisé par le producteur ou par ses distributeurs, et 2) qualifiés professionnellement pour interpréter correctement les informations fournies par le Produit, et mettre en œuvre les procédures de sécurité nécessaires.

2.5 Risques résiduels

Un processus de gestion des risques a été mis en place dans le cycle de vie du Produit en adoptant les normes techniques pertinentes. Des mesures de contrôle des risques ont été identifiées et mises en œuvre afin de réduire les risques au minimum et de les rendre acceptables par rapport aux avantages apportés par le produit. Le risque résiduel global est également acceptable si on le compare aux mêmes avantages.

Les risques résiduels énumérés ci-dessous ont été pris en compte et réduits au minimum possible. Étant donné la nature inhérente du concept de «risque», il est impossible de les supprimer complètement ; ces risques résiduels sont divulgués aux utilisateurs.

- Incapacité d'utiliser le Produit ou certaines de ses fonctionnalités comme prévu, ce qui pourrait provoquer des retards et/ou des erreurs dans les actions thérapeutiques/diagnostiques.
 - Un des risques serait par exemple l'incapacité de l'utilisateur à détecter une alarme (l'utilisateur étant, par exemple, temporairement distrait par une autre tâche). Une notification sonore retentit alors afin d'attirer l'attention de l'utilisateur et ainsi de réduire le risque.
- Ralentissement des performances du produit, pouvant entraîner des retards ou des erreurs dans les actions thérapeutiques et diagnostiques.
- Actions non autorisées effectuées par les utilisateurs, qui pourraient causer des erreurs dans les actions thérapeutiques/diagnostiques et dans l'attribution des responsabilités de ces actions.
- Configuration incorrecte ou incomplète du produit pouvant entraîner des retards ou des erreurs dans les actions thérapeutiques et diagnostiques.
- Attribution d'informations à un mauvais patient (échange de patient), pouvant entraîner des retards et/ou des erreurs dans les actions thérapeutiques/diagnostiques.
- Traitement incorrect des données du patient, y compris les erreurs de visualisation, d'ajout, de modification et de suppression de données susceptibles d'entraîner des retards et/ou des erreurs dans les actions thérapeutiques/diagnostiques.
- Utilisation non conforme du produit (par exemple, produit utilisé comme système de notification d'alarme primaire lorsque les dispositifs médicaux connectés ne le supportent pas, décisions thérapeutiques ou diagnostiques et interventions basées uniquement sur les informations fournies par le produit.
- Divulgaration non autorisée des données personnelles des utilisateurs et/ou des patients.

RISQUES RELATIFS À LA PLATE-FORME MATÉRIELLE POUR LE DISPOSITIF MÉDICAL

- Choc électrique pour le patient et/ou l'utilisateur, qui peut provoquer des lésions et/ou le décès du patient/l'utilisateur.
- Surchauffe des composants du matériel, qui peut provoquer des lésions au patient/l'utilisateur.
- Contraction d'une infection pour le patient/l'utilisateur.

2.6 Responsabilités de l'organisation des soins de santé

Ascom UMS décline toute responsabilité en cas de conséquences dommageables pour la sécurité et le bon fonctionnement du dispositif suite à des interventions techniques de réparation ou de maintenance effectuées par du personnel n'appartenant pas au Service Technique ou par des techniciens non autorisés par Ascom UMS ou ses distributeurs autorisés.

L'attention de l'utilisateur et le représentant légal de l'établissement de soins où le dispositif est utilisé est attiré sur leurs responsabilités, dans le cadre de la réglementation locale en vigueur en matière de sécurité et de santé au travail et toute procédure de sécurité supplémentaire à l'échelle locale.

Les services de Ascom UMS et de ses distributeurs autorisés sont en mesure de fournir aux clients le soutien nécessaire pour assurer durablement la sécurité et le bon fonctionnement des produits fournis, en garantissant compétences, instruments et pièces détachées, permettant ainsi de garantir durablement la pleine conformité des dispositifs aux caractéristiques structurelles d'origine.

Le produit est conçu en tenant compte des exigences et des meilleures pratiques présentes dans la norme IEC 80001 et ses rapports techniques complémentaires. En particulier, la norme IEC/TR 80001-2-5 est très pertinente pour le produit. Comme précisé dans la série IEC 80001, une partie des activités nécessaires et des mesures de contrôle des risques sont sous le contrôle et la responsabilité de l'organisation de soins de santé. Veuillez-vous référer à la norme et à ses garanties pour identifier les activités nécessaires et les mesures de contrôle des risques; se référer notamment à la version valide actuelle des documents suivants:



- IEC 80001-1
- IEC/TR 80001-2-1
- IEC/TR 80001-2-2
- IEC/TR 80001-2-3
- IEC/TR 80001-2-4
- IEC/TR 80001-2-5

2.7 Responsabilité du fabricant

Ascom UMS est responsable pour la sécurité, la fiabilité et la performance du produit uniquement si:

- L'installation et la configuration ont été effectuées par du personnel formé et autorisé par Ascom UMS;
- L'utilisation et la maintenance sont conformes aux instructions fournies dans la documentation du Produit (y compris ce Manuel de l'utilisateur);
- Les configurations, les modifications et la maintenance sont uniquement effectuées par du personnel formé et autorisé par Ascom UMS;
- L'environnement d'utilisation du Produit est conforme aux consignes de sécurité et aux réglementations applicables;
- L'environnement où le Produit est utilisé (y compris les ordinateurs, l'équipement, les connexions électriques, etc.) est conforme aux réglementations locales applicables.

2.8 Traçage du produit

Afin de garantir la traçabilité des dispositifs et les actions correctives sur site, conformément aux normes EN 13485 et MDD 93/42/CEE, le propriétaire est invité à informer Ascom UMS/le distributeur de tout transfert de propriété par écrit en précisant le produit dont il s'agit ainsi que les données d'identification de l'ancien et du nouveau propriétaire.

Les données de l'appareil se trouvent sur l'étiquette du produit (« rubrique à propos » affichée dans le produit - voir paragraphe 1.6).

En cas de doute/de questions sur l'identification du produit, veuillez contacter l'assistance technique de Ascom UMS/du distributeur (pour les contacts, voir paragraphe 5).

2.9 Système de surveillance après-vente

Le dispositif marqué CE fait l'objet d'une surveillance post-commercialisation - fournie par Ascom UMS et son distributeur pour chaque copie commercialisée - concernant les risques réels et potentiels, tant pour le patient que pour l'utilisateur, tout au long du cycle de vie du produit.

En cas de détérioration des caractéristiques de l'appareil, de performances médiocres ou d'instructions utilisateur inadéquates ayant été ou pouvant constituer un risque pour la santé du patient ou de l'utilisateur ou pour la sécurité environnementale, l'utilisateur doit immédiatement avvertir Ascom UMS ou son distributeur.

Dès réception des commentaires d'un utilisateur ou s'il en a été informé en interne, ASCOM UMS ou le distributeur démarrera immédiatement la révision et de vérification et effectuera les actions correctives nécessaires.

2.10 Vie du Produit

La durée de vie du produit ne dépend pas de l'usure ou d'autres facteurs pouvant compromettre la sécurité. Elle est influencée par l'obsolescence de l'environnement logiciel (par exemple, OS, .NET Framework) et est donc prévue pour une durée de 5 ans à compter de la date de publication de la version du produit (disponible dans la rubrique À propos).

3. Spécifications du logiciel et du hardware



Le Produit ne doit être installé que par du personnel qualifié. Le terme inclut le personnel d'Ascom UMS et/ou de son Distributeur et toute autre personne spécialement formée et explicitement autorisée par Ascom UMS et/ou son Distributeur. Sans une autorisation explicite et directe d'Ascom UMS et/ou de son Distributeur, le personnel de l'établissement de santé n'est pas autorisé à effectuer des procédures d'installation et/ou à modifier la configuration de Digistat.



Le Produit doit uniquement être utilisé par du personnel qualifié. Le Produit ne peut pas être utilisé sans une formation adéquate, qui est dispensée par le personnel d'Ascom UMS et/ou son Distributeur.

Ce chapitre dresse la liste des caractéristiques logicielles et matérielles requises pour que le Produit Digistat puisse fonctionner correctement. Les informations fournies dans cette section couvrent les obligations d'information du producteur spécifiées dans la norme IEC 80001-1 (*Application of risk management for IT-networks incorporating medical devices*).

Il incombe à l'organisation de soins de santé de maintenir l'environnement d'exécution du produit, notamment le matériel et les logiciels, tels que décrits dans ce chapitre. La maintenance comprend les mises à niveau, les mises à jour et les correctifs de sécurité des systèmes d'exploitation, des navigateurs Web, de Microsoft NET Framework, d'Adobe Reader, etc., ainsi que l'adoption des autres meilleures pratiques pour la maintenance des composants logiciels et matériels.

Selon la norme IEC 60601-1, si un dispositif électrique est situé à proximité du lit, il est nécessaire d'utiliser des dispositifs de type médical. Dans ces situations, des PANEL PC de qualité médicale sont généralement utilisés. Sur demande, Ascom UMS peut proposer d'autres appareils possibles de ce type.



Un lecteur PDF pris en charge doit être installé sur le poste de travail afin d'afficher l'aide en ligne. Voir 3.1.3 pour les exigences logicielles des postes de travail centraux et de chevet.

3.1 Central & Bedside

3.1.1 Hardware

Spécifications minimum du hardware:

- Processeur Intel® I3 ou supérieur
- Mémoire RAM 4GB
- Disque dur avec au moins 60 GB d'espace libre
- Moniteur : écran 22", résolution minimale 1920 x 1080, avec haut-parleur intégré. Écran tactile recommandé.
- Souris ou autre dispositif compatible
- Interface Ethernet 100 Mb/s (ou plus)

Si un poste de travail central/de chevet est configuré pour afficher des flux vidéo (fonctionnalité prise en charge uniquement dans Smart Central ou OranJ avec l'intégration de caméra activée), la configuration minimale requise est la suivante :

- Processeur Intel® I3 ou supérieur
- Mémoire : 4 Go de RAM + 50 Mo pour chaque flux de caméras affiché simultanément (par exemple, avec 20 caméras affichées 4 Go + 1 Go)
- Disque dur avec au moins 60 GB d'espace libre
- Moniteur : écran 22", résolution minimale 1920 x 1080, avec haut-parleur intégré. Écran tactile recommandé.
- Souris ou autre dispositif compatible
- Interface Ethernet 100 Mb/s (ou plus)

Quelques exemples : avec un processeur Intel i7 6600 2.60 Ghz, un flux de 10 caméras ayant un débit de 3138 kbps, le taux d'utilisation du processeur est d'environ 45 %. Avec un processeur I3 7100t 3,4 Ghz, un flux de 16 caméras ayant un débit de 958 kbps, le taux d'utilisation du processeur est d'environ 30 %.

3.1.2 Logiciel d'exploitation

- Microsoft Corporation Windows 8.1 x86/x64 Professional
- Microsoft Corporation Windows 10

3.1.3 Logiciel de système

- Microsoft Framework .NET 4.5
- Adobe Acrobat Reader 10



Le manuel utilisateur du produit est un fichier PDF créé conformément à la version standard PDF 1.5 et donc lisible par Adobe Acrobat 6.0 ou supérieur. De plus, le manuel utilisateur du produit a été testé avec Adobe Acrobat Reader 10. L'organisation hospitalière peut utiliser une version différente d'Acrobat Reader: la vérification du produit installé inclura la vérification de la lisibilité correcte du manuel utilisateur.

3.2 Serveur

3.2.1 Hardware

Configuration matérielle minimale requise (petite installation, 20 lits, 4 appareils chacun) :

- Processeur Intel® I5 à 4 cœurs.
- Mémoire: 4 GB RAM (8 GB recommandés)
- Disque dur avec au moins 120 GB d'espace libre
- Interface Ethernet 100 Mb/s (ou plus). Conseillé 1 Gb/s.

Configuration matérielle recommandée (installation de taille moyenne, 100 lits, 4 appareils chacun, Connect et Mobile) :

- Processeur Intel® I7 à 8 cœurs.
- Mémoire: 4 GB RAM (8 GB recommandés)
- Disque dur avec au moins 120 GB d'espace libre
- Interface Ethernet 100 Mb/s (ou plus). Conseillé 1 Gb/s.

3.2.2 Logiciel d'exploitation

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016
- Microsoft Corporation Windows Server 2019

3.2.3 Logiciel de système

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Framework.NET 4.5

3.3 Digistat Mobile

Digistat mobile est compatible avec les appareils Android de la version 4.4.2 à la version 10.0. Il a été vérifié sur les appareils Ascom Myco SH1 et SH2 wifi et les téléphones cellulaires intelligents, avec la version Android 5.1 (Myco 2) et la version Android 9.0 (Myco3). De plus, il a été très vérifié sur l'appareil Zebra Phone TC51 avec Android version 7.1.

L'application est conçue pour être compatible avec d'autres appareils Android avec une taille d'écran minimale de 3,5"; la compatibilité avec un appareil spécifique doit être vérifiée avant l'utilisation clinique.

Contactez Ascom UMS pour une liste complète des dispositifs prenant en charge Digistat Mobile.

3.4 Digistat “Web”

Les navigateurs suivants sont pris en charge pour une utilisation avec les applications Digistat “Web” (ci-après “Digistat Web”):

- Chrome 83
- Firefox 77
- Edge 83
- Internet Explorer 11



L'échelle d'affichage du navigateur doit toujours être définie sur 100%.

3.5 Avertissements



Si le produit est utilisé pour la notification principale d'alarmes, au moins deux postes de travail clients doivent être installés dans le même département ou, à défaut, au moins un poste de travail Digistat Care et une tour d'alarme LED. Consultez la section 4.4.1 pour de plus amples informations.



Pour les modules mobiles et de bureau, le séparateur décimal et, plus généralement, les paramètres régionaux (formats de date, par exemple) utilisés par le produit dépendent des paramètres du système d'exploitation de la station de travail ou du périphérique mobile sur lequel le produit est installé.

Pour les modules Web, le séparateur décimal et, plus généralement, les paramètres régionaux (par exemple, les formats de date) utilisés par le produit dépendent de la configuration du produit.



Pour utiliser correctement le Produit, il est nécessaire que le Display Scaling de Microsoft Windows soit configuré sur 100%. D'autres réglages peuvent empêcher l'exécution du produit ou créer des dysfonctionnements au niveau de la représentation graphique. Pour définir la valeur Display Scaling, consulter la documentation de Microsoft Windows.



Les ordinateurs et autres dispositifs employés doivent être adéquats pour l'environnement dans lequel ils sont utilisés et doivent par conséquent respecter les normes et les règlements applicables.



Il est obligatoire de se conformer aux indications du producteur pour le stockage, le transport, l'installation, la maintenance et l'élimination du matériel de tierces parties. Ces opérations devront être effectuées uniquement par du personnel compétent et adéquatement formé.

Le Produit a été vérifié et validé pendant la phase d'installation ou de mise à niveau et son test d'acceptation a été effectué sur le matériel (PC, serveur, appareils mobiles) et avec les logiciels (par exemple, le système d'exploitation), ainsi qu'avec d'autres composants logiciels (par exemple, le navigateur, l'antivirus, etc.) déjà présents. Tout autre matériel ou logiciel installé peut compromettre les contrôles de sécurité, d'efficacité et de conception du Produit.



Il est obligatoire de consulter un distributeur agréé/un technicien Ascom UMS avant d'utiliser tout autre logiciel avec le Produit, autres que ceux validés lors de la phase d'installation ou de mise à niveau.

Si un autre logiciel (utilitaires ou programmes d'application) doit être installé sur le matériel sur lequel le Produit s'exécute, l'organisme de soins de santé doit en informer le distributeur agréé/un technicien Ascom UMS pour une validation supplémentaire. Il est suggéré d'appliquer une politique d'autorisation qui empêche les utilisateurs d'effectuer des procédures telles que l'installation de nouveaux logiciels.



L'organisation responsable est tenue d'appliquer un mécanisme de synchronisation de la date et de l'heure des postes de travail sur lesquels tourne le Produit avec une source temporelle de référence.



Les exigences matérielles et logicielles des périphériques tiers (y compris le module adaptateur intelligent (Smart Adapter Module) de Project Engineering, les serveurs de port de Lantronix, etc.) sont décrites dans leurs modes d'emploi respectifs, fournis par les fournisseurs. Les contacts des fournisseurs d'appareils tiers peuvent être fournis par Ascom ou par des distributeurs agréés.

3.6 Fonctionnalité de streaming audio/vidéo

Dans certaines configurations, le produit met en œuvre des fonctionnalités de streaming audio/vidéo.

Dans les cas où certaines parties du produit agissent en tant que visualiser de flux vidéo, le produit n'est pas la source du flux vidéo et n'enregistre aucune information de cette manière. Il incombe à l'organisation des soins de santé de gérer le système de manière à se conformer à la réglementation en matière de protection des données, y compris l'installation et la configuration des caméras source.

Dans les cas où certaines parties du produit gèrent l'audio et les images liées aux utilisateurs et/ou aux patients, y compris l'acquisition, l'élaboration et l'enregistrement, il incombe à l'organisation des soins de santé de mettre en œuvre les procédures nécessaires pour se conformer à la réglementation locale en matière de protection des données. Y compris, sans toutefois s'y limiter, la définition des limites d'utilisation et la formation des utilisateurs.

La fonctionnalité du streaming vidéo sur les postes de travail de bureau a été testée avec les codecs vidéo H264 et H265. Tout autre codec vidéo présent ou installé par défaut par des applications tierces (par exemple, VLC Media Player) doit être testé avant utilisation.

Attention : chaque source vidéo prend en charge un nombre maximal de clients connectés simultanément. Il incombe à l'organisation des soins de santé de déterminer ce nombre maximal et d'informer les utilisateurs.

La fonctionnalité de streaming vidéo sur les appareils mobiles ne prend en charge que les flux vidéo RTSP avec les types d'authentification suivants :

- Pas authentification ;
- Authentification de base ;
- Authentification Digest.

La fonctionnalité de streaming vidéo sur les appareils mobiles ne prend en charge que les codecs vidéo H263, H264 et H265.

3.7 Parefeu et antivirus

Pour protéger le Produit contre d'éventuelles attaques informatiques, il est nécessaire:

- que le pare-feu de Windows® soit actif à la fois sur les postes de travail que sur le serveur ;
- qu'un logiciel antivirus/antimalware soit activé et régulièrement mis à jour tant sur le poste de travail que sur le serveur.

Il incombe à l'organisation responsable de s'assurer que ces deux protections soient mises en place. Ascom UMS a testé le produit avec F-SECURE Antivirus. Au vu toutefois des choix et des politiques préalables de l'établissement de santé, le choix de l'antivirus spécifique est laissé à l'organisation responsable. Ascom UMS ne peut garantir que le Produit soit compatible avec chaque antivirus ou sa configuration.



Des incompatibilités avec des parties du Produit ont été signalées avec l'utilisation de l'anti-virus Kaspersky, dont la solution a nécessité la définition de règles spécifiques à cet anti-virus.



Il est fortement conseillé de garder uniquement ouvert les ports TCP et UDP qui sont effectivement nécessaires. Ces Ports peuvent changer en fonction de la configuration du système. Il est donc recommandé de s'adresser à l'assistance technique pour tous les détails nécessaires.

3.7.1 Autres précautions recommandées pour la cyberprotection

Afin de mieux protéger le Produit d'éventuelles cyber-attaques, il est fortement recommandé de:

- planifier et mettre en œuvre le «durcissement» de l'infrastructure informatique, y compris la plateforme informatique qui constitue l'environnement d'exécution du Produit,
- mettre en œuvre un Système de détection et de prévention des intrusions (IDPS),
- effectuer un Test de pénétration et, si une faiblesse est détectée, effectuer toutes les actions requises pour réduire le risque de cyberintrusion,
- ne plus utiliser et remplacer les appareils quand ils ne peuvent plus être mis à jour,
- planifier et effectuer une vérification périodique de l'intégrité des fichiers et des configurations,
- mettre en œuvre une solution DMZ (zone démilitarisée) pour les serveurs Web qui ont besoin d'être exposés sur Internet.

3.8 Caractéristiques du réseau local

Cette section répertorie les fonctions du réseau local sur lequel le Produit est installé afin de garantir la pleine fonctionnalité du système.

- Le Produit utilise un protocole de communication TCP/IP.
- Le réseau LAN doit être exempt de saturations.
- Le Produit requiert un LAN d'au moins 100 mégabits disponible sur le poste de travail du client. Un backbone d'1gigabit Ethernet serait utile.
- Aucun filtre ne doit être présent sur le trafic TCP/IP entre les postes de travail, les serveurs et les dispositifs secondaires.
- Si les dispositifs (serveur, poste de travail et dispositifs secondaires) sont reliés à différents sous-réseaux, il doit y avoir un routage entre ces sous-réseaux.
- Il est recommandé d'adopter des techniques de redondance afin d'assurer le service du réseau également en cas de dysfonctionnement.
- Il est conseillé de planifier, de concert avec Ascom UMS/Distributeurs, le calendrier de maintenance afin que Ascom UMS ou le distributeur agréé puisse assister efficacement l'établissement de santé au niveau de la gestion des éventuels dysfonctionnements dus aux activités de maintenance.



Si le réseau local est au moins partiellement basé sur des connexions Wi-Fi, étant donné l'intermittence possible de la connexion Wi-Fi, des déconnexions du réseau sont possibles, ce qui provoque l'activation du « Mode déconnecté ou récupération » ("Recovery or Disconnected Mode") qui, dans le cas où le produit est utilisé pour la notification principale des alarmes, peut provoquer l'indisponibilité du système. L'organisation responsable doit prendre des mesures pour garantir une couverture et une stabilité optimales du réseau Wi-Fi et informer le utilisateursconcerné sur la gestion d'éventuelles déconnexions temporaires.



De plus amples détails sur les caractéristiques requises du réseau local (y compris le réseau sans fil) où Digistat Suite est installée sont disponibles dans les manuels *Installation et Configuration de Digistat Suite*.

4. Avant le démarrage

4.1 Avertissements sur l'installation et la maintenance

Les avertissements suivants concernant l'installation correcte et la maintenance du Produit doivent être scrupuleusement respectés.



L'installation, l'entretien et les réparations doivent être effectués conformément aux procédures et directives Ascom UMS uniquement par des techniciens Ascom UMS/distributeur ou du personnel formé et autorisé par Ascom UMS/distributeur.



Nous recommandons à l'établissement de santé qui utilise le produit, de conclure un contrat de maintenance avec Ascom UMS ou un Distributeur agréé.



Le Produit doit être installé et configuré par du personnel compétent et autorisé. Il peut s'agir du personnel Ascom UMS (ou d'un distributeur autorisé) et de toute autre personne ayant suivi une formation spéciale et expressément autorisée par Ascom UMS ou un distributeur. De même, les interventions de maintenance et de réparation sur le Produit doivent être effectuées conformément aux directives Ascom UMS uniquement par le personnel Ascom UMS/Distributeur ou toute autre personne ayant suivi une formation spéciale et expressément autorisée par Ascom UMS ou un distributeur.

- Utiliser des dispositifs de fournisseurs tiers recommandés par Ascom UMS/Distributeurs.
- Seules les personnels formées et autorisées peuvent installer les dispositifs de fournisseurs tiers.
- L'Établissement de soins veillera à ce que la maintenance du produit et de tout dispositif de fournisseur tiers soit réalisée ainsi que nécessaire pour garantir la sécurité et l'efficacité et réduire le risque de dysfonctionnement ainsi que la survenue d'éventuels dangers pour le patient et l'utilisateur.
- La clé matérielle Digistat Care (clé/dongle USB) s'il est utilisé doit être stockée et utilisée dans des conditions ambiantes (température, humidité, champs électromagnétiques, etc.) adéquates, tel que spécifié par le fabricant, en tous les cas dans des conditions équivalentes à celles qui sont communément requises pour les dispositifs électroniques de bureau.
- L'organisation des soins de santé est responsable de la sélection des équipements adaptés à l'environnement dans lequel ils sont installés et utilisés. L'organisation des soins de santé, entre autres, devrait prendre en compte la sécurité électrique, les émissions CEM, les interférences de signaux radio, la désinfection et le nettoyage. Une attention particulière doit être portée aux appareils installés dans la zone patiente.
- L'organisation de soins de santé doit définir des procédures de travail alternatives au cas où le système ne serait plus fiable ou cesserait de fonctionner.

4.2 Politique de confidentialité

Des précautions appropriées seront prises pour protéger la vie privée des utilisateurs et des patients et pour garantir le traitement des données personnelles en respectant les droits, les libertés fondamentales et la dignité des personnes concernées, notamment en matière de protection de la confidentialité, de l'identité personnelle et des données personnelles.



L'expression “données personnelles” désigne toute information relative à une personne physique identifiée ou identifiable (“personne concernée”); une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, en particulier par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

Une attention particulière sera accordée aux données définies dans le “Règlement général de l'UE sur la protection des données 2016/679 (RGPD)” en tant que “Catégories spéciales de données à caractère personnel”.

Catégories spéciales de données personnelles:

(...) les données personnelles révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, et le traitement de données génétiques, les données biométriques dans le but d'identifier de manière unique une personne physique, les données de santé ou données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

L'établissement de soin doit s'assurer que l'utilisation du Produit est conforme aux exigences de la réglementation applicable en matière de confidentialité et de protection des données personnelles, en particulier à l'égard de la gestion des informations susmentionnées.

Le Produit gère et affiche les données personnelles.

Le Produit peut être configuré de telle façon qu'il est masqué automatiquement dans les écrans d'application lorsqu'aucun utilisateur n'est connecté dans le sous-ensemble de données personnelles qui peuvent être utilisées pour identifier une personne physique.

Les champs masqués sont les suivants :

- Prénom et nom de famille
- Date de naissance
- Sexe
- Code de patient
- Date d'admission à l'hôpital
- Date de sortie d'hôpital
- Poids du patient
- Taille du patient

L'ensemble des champs masqués peut être ajusté lors de la configuration du Produit.

Pour ce faire, dans l'application de configuration du Produit, réglez l'option du système appelée “Privacy Mode” [mode de confidentialité] sur “true” [vrai] (consulter le manuel de

configuration et d'installation du Produit pour lire la procédure détaillée). Sa valeur par défaut est "true" [vrai].

Si l'option "Privacy Mode" [mode de confidentialité] est réglé sur "true", les cas suivants sont possibles:

- si aucun utilisateur n'est connecté, aucune information sur le patient n'est affichée.
- si un utilisateur est connecté et qu'il n'a pas d'autorisation spécifique, aucune information sur le patient n'est affichée.
- si un utilisateur est connecté et qu'il a une autorisation spécifique, les informations sur le patient sont affichées.

L'option peut être appliquée à un seul poste de travail (c.-à-d. différentes stations de travail peuvent être configurées différemment).

Veuillez lire attentivement et respecter les précautions suivantes.

- Les PC utilisés ne doivent pas rester sans surveillance et accessibles pendant les sessions de travail avec le Produit. Il est par conséquent recommandé de se déconnecter du système à chaque fois que l'on quitte le poste de travail.
- Les données personnelles sauvegardées dans le système, comme les mots de passe ou données personnelles de patients ou utilisateurs, doivent être protégées par des logiciels appropriés (anti-virus et pare-feu) contre toute tentative d'accès non autorisé. Il relève de la responsabilité de l'établissement de santé d'implémenter ce logiciel et de le mettre continuellement à jour.
- L'utilisation fréquente de la fonction «Verrouiller» est fortement déconseillée. La fonction de déconnexion automatique a pour but de réduire la probabilité d'accès au système par des personnes non autorisées.
- Des données personnelles peuvent être présentes dans certains rapports produits par le Produit. L'établissement de soin doit gérer ces documents conformément aux normes en vigueur en matière de confidentialité et de protection des données personnelles.
- Les postes de travail (bureau et mobile) ne stockent pas les données du patient sur le disque. Les données des patient sont stockées uniquement dans la base de données et le stockage de la base de données dépend des procédures et des choix de la structure de santé (exemples: machine physique, SAN, environnement de virtualisation). Les données des patients doivent être traitées conformément à toutes les normes en vigueur en matière de confidentialité et de protection des données personnelles.
- L'établissement de soin est chargé de fournir une formation de base sur les questions relatives à la confidentialité, à savoir les principes de base, les règles, les règlements, les responsabilités et les sanctions dans un environnement de travail donné. Ascom UMS et/ou son Distributeur dispensera une formation spécialisée sur la meilleure manière d'utiliser le Produit en ce qui concerne les questions de confidentialité (c.-à-d. l'anonymisation de la base de données, le mode de confidentialité, les autorisations des utilisateurs, etc.).
- L'établissement de soin produira et tiendra à jour la documentation suivante:
 1. la liste à jour des administrateurs du système et du personnel de maintenance;
 2. les formulaires d'affectation signés et les attestations de participation aux cours de formation;

3. un registre des informations d'identification, des autorisations et des privilèges accordés aux utilisateurs;
 4. une liste à jour des utilisateurs du produit.
- L'établissement mettra en œuvre, testera et certifiera une procédure de désactivation automatique des utilisateurs qui ne sont plus actifs, après une certaine période.
 - L'établissement de soin codifiera, mettra en œuvre et documentera une procédure de vérification périodique des tâches incombant à l'administrateur du système et au personnel de maintenance technique.
 - L'établissement de soin effectuera des audits et des contrôles sur le comportement correct des opérateurs.



Les bases de données contenant des données sur les patients ou des informations sensibles ne peuvent pas quitter l'établissement de santé sans être cryptées ou masquées.



Les données du patient ne sont pas stockées dans des fichiers propriétaires. Le seul endroit où les données du patient sont stockées est la base de données.



Dans certaines circonstances, des données personnelles sont transmises sous forme non cryptée et au moyen d'une connexion non intrinsèquement sûre. Les communications HL7 sont un exemple de cette situation. Il relève de la responsabilité de l'établissement de santé de prendre les mesures de sécurité nécessaires pour respecter les lois et réglementations locales en matière de confidentialité.



Nous suggérons de configurer le serveur de base de données de manière à ce que la base de données du Produit soit cryptée sur le disque. Pour activer cette option, SQL Server Enterprise Edition est requis et, lors de son installation, il est nécessaire d'activer l'option TDE (*Transparent Data Encryption*).

4.2.1 Caractéristiques et utilisation des informations d'identification de l'utilisateur

Cette section explique les fonctions des identifiants utilisateur (nom utilisateur et mot de passe) du Produit, leur utilisation et la politique préconisée.

- Chaque utilisateur doit prendre toutes les précautions afin de garder le secret du nom utilisateur et le mot de passe.
- Nom utilisateur et mot de passe doivent rester privés. Ne pas permettre à d'autres personnes de connaître votre nom utilisateur et mot de passe.
- Tout employé peut avoir un ou plusieurs accès de données pour l'authentification (nom utilisateur et mot de passe). Les mêmes noms utilisateur et mots de passe ne doivent pas être utilisés par plusieurs employés.
- Les profils d'autorisation doivent être vérifiés et renouvelés au moins une fois par an.
- Les profils d'autorisation peuvent être regroupés suivant l'homogénéité des fonctions des différents utilisateurs.
- Chaque compte utilisateur doit être associé à une personne bien précise. L'utilisation d'utilisateurs génériques (par exemple "ADMIN" ou "INFIRMIÈRE") doit être évitée. En d'autres termes, il est nécessaire, pour des raisons de traçabilité, que chaque compte utilisateur soit utilisé uniquement par un seul utilisateur.
- Chaque utilisateur a un profil d'autorisation qui lui est associé, ce qui permet d'accéder seulement aux fonctionnalités utiles pour les tâches que chacun est chargé d'accomplir.
- Le mot de passe doit être composé d'au moins huit caractères.
- Le mot de passe ne doit pas contenir de références se rapportant facilement à l'employé (par exemple les ; prénom, nom, date de naissance, etc.).
- Le mot de passe est attribué par l'administrateur du système et doit être modifié par l'utilisateur lors de la première utilisation du système.
- Par la suite, le mot de passe doit être modifié au moins tous les trois mois.
- Si le nom d'utilisateur et le mot de passe restent inutilisés pendant plus de 6 mois, ils doivent être désactivés. Des identifiants utilisateur utilisés dans des buts de maintenance technique du Produit pour les procédures de configuration de cette caractéristique.
- Les données d'accès sont désactivées également en cas de perte de la part de l'utilisateur de la qualification correspondant à ces données (c'est le cas par exemple lorsqu'un utilisateur est muté vers un autre établissement). L'administrateur du système peut activer/désactiver manuellement un utilisateur. La procédure est décrite dans le manuel de configuration du Produit

Les informations suivantes sont adressées aux techniciens administrateurs du système:

Le mot de passe doit respecter une suite régulière définie par la configuration de Produit (par défaut ^.....*, soit 8 caractères).

Le mot de passe est attribué par l'administrateur du système au moment où un nouveau compte utilisateur est créé. L'administrateur du système peut contraindre l'utilisateur à modifier le mot de passe au premier accès au système. Le mot de passe expire après une durée pré-définie, l'utilisateur est tenu de changer le mot de passe à l'expiration de cette période. Il est possible de faire en sorte que le mot de passe d'un utilisateur n'expire pas.

Voir le manuel de configuration du Produit pour des informations détaillées sur la définition des comptes utilisateur et sur la configuration des mots de passe.

4.2.2 Administrateurs système

Lors du déroulement de l'installation, de mise à jour et d'assistance technique du Produit, le personnel Ascom UMS ou des distributeurs autorisés pourra avoir accès et traiter des données personnelles et sensibles mémorisées dans la base de données de Produit.

Ascom UMS/le distributeur, en matière de gestion et de traitement des données personnelles et sensibles, adopte des procédures et instructions de travail qui sont conformes aux dispositions de la loi en matière de protection des données en vigueur ("General Data Protection Regulation - EU 2016/679").

Pour l'accès à la base de données, le personnel Ascom UMS/et ou l'installateur est en mode "Administrateur système" pour le Produit (voir Mesure concernant le responsable de la protection des données sur les "Administrateurs système" du 25/11/2008). Le personnel désigné par Ascom UMS/le distributeur pour exercer ces activités, est habilité/formé aux dispositions relatives à la protection des données et en particulier au traitement des données sensibles.

Afin de satisfaire les requêtes des "Administrateurs du système", l'organisation responsable doit:

- définisse les accès de manière nominative ;
- active le registre des accès au niveau du système d'exploitation tant sur le serveur que sur les clients ;
- active le registre des accès à la base de données serveur Microsoft SQL Server (niveau audit) ;
- configure et gère ces deux registres de façon à garder une trace des accès pendant au moins un an.

4.2.3 Journal système

Le Produit enregistre les journaux système dans la base de données. Ces journaux sont conservés pour une durée qui peut être configurée. Les journaux sont conservés pendant des durées différentes en fonction de leur nature. Par défaut, les durées sont les suivantes:

- les journaux d'activités informatiques sont conservés pendant 10 jours ;
- les journaux d'activités correspondant à un avertissement/une alerte sont conservés pendant 20 jours ;
- les journaux d'activités correspondant à des erreurs sont conservés pendant 30 jours.

Ces durées peuvent être configurées. Voir le manuel de configuration pour la procédure de définition des durées de conservation des registres.

4.2.4 Investigation du log

Un sous-ensemble des journaux système mentionnés précédemment, défini conformément à la politique de chaque structure de soins de santé spécifique utilisant le produit comme «cliniquement pertinent» ou «cliniquement utile», peut être envoyé à un système externe (base de données SQL ou Syslog) pour être stocké selon les besoins et les règles de la structure de soins.

4.3 Dispositifs compatibles

4.3.1 Dispositifs DAS

Dispositifs permettant la mise en place d'un système d'alarme distribué fiable.

Les données acquises par ce type d'appareil sont affichées sur le Produit.

Les données acquises par ce type d'appareil peuvent également être générées en tant que HL7. HL7 output communication n'est pas fiable

- *Ventilateur Hamilton S1 et C6 et autres modèles prenant en charge le même protocole*

Pour utiliser le ventilateur Hamilton dans un système d'alarme distribué, il est nécessaire de configurer correctement les paramètres de communication du ventilateur conformément à la documentation technique de Hamilton.

De plus, le ventilateur Hamilton prend en charge l'option « silencieux ICU ». Cela signifie qu'il peut être utilisé avec le Produit pour fonctionner en mode silencieux.

Pour utiliser le ventilateur Hamilton dans un système d'alarme distribué comme ventilateur silencieux (par exemple dans une unité ICU silencieuse), il est possible de le faire fonctionner dans un état AUDIO OFF global.

Tout d'abord, le ventilateur doit être correctement configuré. Reportez-vous à la documentation technique du ventilateur Hamilton pour les instructions de configuration et les instructions détaillées sur le fonctionnement de l'appareil en mode silencieux (état AUDIO OFF).



Reportez-vous à la documentation du ventilateur Hamilton pour obtenir des instructions plus détaillées.

Il peut s'écouler jusqu'à deux secondes entre la génération de l'alarme et l'envoi de l'alarme sur le ventilateur Hamilton.

Le ventilateur attend ensuite un accusé de réception du Produit. Si cet accusé de réception n'est pas reçu dans les deux secondes, un délai d'attente survient.

Par conséquent, le délai maximum après lequel une notification d'alarme est envoyée est de 4 secondes.



S'il y a un délai d'attente :

- Une alarme de connexion est déclenchée. L'alarme peut être annulée par l'utilisateur. Elle est annulée si une nouvelle connexion avec une livraison confirmée est établie.
 - Tout silence actif est annulé.
 - L'envoi du message du ventilateur et la livraison confirmée sont arrêtés jusqu'à ce qu'une nouvelle connexion soit établie.
-



Le délai maximum mesuré dans un environnement de test entre l'affichage de notification sur le ventilateur et l'affichage de notification sur le Produit est de 600 ms (desktop)

Le délai maximum mesuré dans un environnement de test entre l'affichage de notification sur le ventilateur et l'affichage de notification sur le Mobile est de 1000 ms.



Le délai maximum mesuré dans un environnement de test entre la connexion du ventilateur Hamilton et l'affichage des données sur le Produit est de 22900 ms.

Le délai maximum mesuré dans un environnement de test entre la connexion du ventilateur Hamilton et l'affichage des données sur le Produit est de 20233 ms.

4.3.2 Dispositifs DIS

Dispositifs **permettant** pas la mise en place d'un système d'alarme distribué fiable.

Cette communication n'est pas fiable

Pour la liste complète des pilotes disponibles contactez ASCOM UMS / Distributor.



Pour des raisons qui sont hors du contrôle du logiciel, par exemple, la manière dont les périphériques physiques réels sont installés / câblés, des délais sont possibles entre la génération d'alarme et l'affichage réel de l'alarme.



La mise à jour des données affichées à l'écran provoquée par la connexion, la mise hors tension, la déconnexion et le changement d'état du dispositif dépend du temps nécessaire au dispositif pour communiquer les changements. Ce temps dépend de plusieurs facteurs. Parmi eux, il y a le type de dispositif et le type de connexion. Pour certains dispositifs, il y a des conditions où le retard de communication des changements peut être important. Compte tenu du fait qu'ils peuvent changer en fonction de la configuration et des conditions de fonctionnement des dispositifs, il n'est pas possible d'indiquer les retards pour tous les dispositifs possibles.



Les pilotes utilisés pour lire les données des dispositifs médicaux raccordés ont un cycle de lecture de moins de 3 secondes (à savoir que toutes les données des dispositifs sont lues toutes les 3 secondes maximum). Il y a cependant des dispositifs qui communiquent les informations moins fréquemment (par intervalles de 5-10 secondes). Consultez la documentation du pilote pour plus de détails sur le cycle de lecture.

Dans un environnement de test installé et configuré comme indiqué dans le «Manuel d'installation et de configuration du serveur», dès qu'un pilote détecte une alarme, il faut au maximum 1 seconde pour la transférer vers le Produit.

4.3.3 Avertissements



Le produit reçoit des données de plusieurs sources : dispositifs médicaux, systèmes d'information hospitaliers et saisies manuelles de l'utilisateur.

De plus, le produit calcule les informations dérivées (par exemple, le score).

La portée, la précision et l'exactitude de ces données dépendent des sources externes, des données saisies par l'utilisateur, et de l'architecture matérielle et logicielle sous-jacente.



Selon les caractéristiques des dispositifs médicaux connectés, le produit peut être utilisé pour la notification principale (DAS/CDAS) ou secondaire (DIS) d'alarmes. La présence d'un seul dispositif DIS rend le système complet secondaire. Dans ce cas, l'application affiche un avertissement indiquant que certains des périphériques connectés ne prennent pas en charge la notification principale des alarmes.]



Le Produit n'est pas conçu pour vérifier que les dispositifs fonctionnent correctement.



Déconnecter un dispositif durant son fonctionnement cause l'interruption de la saisie des données du Produit. Les données d'un dispositif perdu lors d'une déconnexion ne sont pas récupérées par le *Produit* après la reconnexion.



Ne désactivez jamais la notification d'alarme sur les dispositifs médicaux, sauf si la documentation du fabricant du dispositif médical et la procédure de l'établissement de soin ne l'autorisent explicitement.



L'organisation de soins de santé est responsable de garantir (par exemple, à l'aide de listes de contrôle appropriées) que la réception correcte de l'alarme est gérée dans le produit (que les sons de notification soient désactivés ou activés pour un patient spécifique sur l'appareil mobile).



Si une pompe à perfusion est connectée au produit, n'en modifiez pas le numéro de série.



Ne jamais désactiver le son (audio) des postes de travail sur les quels est en fonction le Produit.



Selon la décision de l'organisation des soins de santé, le produit pourrait être configuré pour filtrer ou remapper les alarmes générées par les dispositifs médicaux connectés.

Les utilisateurs doivent savoir que, en fonction de la configuration, les alarmes peuvent être présentées avec une priorité ou un message différent, ou peuvent ne pas être annoncées.

L'organisation des soins de santé est chargée de fournir aux utilisateurs des informations et une formation concernant la configuration du filtrage des alarmes. Les utilisateurs doivent être informés de toute modification suivante de la configuration du filtrage des alarmes.

L'opérateur doit se trouver à une distance maximale de 1 m (3,28 pi) pour pouvoir lire les alarmes sur le Produit. Sur une distance maximale de 4 m (13,12 pi), il est possible que l'opérateur constate qu'il y a une alarme. Ceci est vrai si :



- l'opérateur a une acuité visuelle de 0 sur l'échelle logMAR ou une vision de 6-6 (20/20) (corrigée s'il y a lieu),
 - le point d'observation est à l'endroit où l'opérateur se trouve ou à un point quelconque dans la base d'un cône sous-tendu par un angle de 30° par rapport à l'axe horizontal ou normal par rapport au centre du plan d'affichage de l'écran de contrôle ou de l'indication visuelle, l'éclairage ambiant se situe dans les limites de lx 100 à 1 500 lx.
-



Contrôlez que les dispositifs médicaux sont raccordés correctement en vérifiant que leurs données sont affichées sur le Produit.



Utilisez la procédure de vérification du son pour vérifier si le son de la station de travail/de l'appareil mobile fonctionne correctement (voir les documents *USR FRA Smart Central* et *USR FRA Smart Central Mobile* pour connaître la procédure à suivre sur les stations de travail de bureau et les périphériques mobiles). Si les modules Smart Central/Smart Central Mobile ne sont pas installés, la procédure n'est pas pertinente.



Le Produit acquiert les informations générées par les principaux appareils médicaux (c'est-à-dire les ventilateurs pulmonaires, les pompes à perfusion, etc.) et les affiche. Par conséquent, le Produit affiche toujours ce que les principaux dispositifs médicaux communiquent. L'attribution des priorités d'alarme est décidée en fonction du dispositif médical principal. Sur le Produit, il est possible de décider de l'ordre des dispositifs médicaux, pour chaque lit, en fonction de la préférence du client : par type d'appareil, modèle/fabricant. Ce ordre est configurée dans le Produit lors du déploiement du produit en fonction de la demande/préférence de l'utilisateur. La couleur de chaque carte de lit est toujours la couleur de l'alarme de priorité la plus élevée parmi toutes les alarmes se produisant sur ce lit.



Si le pilote générique Alaris® est utilisé, il est nécessaire d'attendre au moins dix secondes après avoir déconnecté une pompe à perfusion et avant d'en reconnecter une autre

4.4 Distribution des alarmes sans danger pour un seul défaut (« single fault safe »)

Selon les caractéristiques des dispositifs médicaux connectés, le Produit peut être sécurisé en condition de premier défaut (« single fault safe ») au niveau de la distribution des alarmes, s'il est installé et configuré en conséquence. Cela signifie que chaque partie du système impliqué dans la distribution des alarmes est surveillée en permanence, y compris le « contrôleur » lui-même (c.-à-d. L'agent de surveillance) et, si une défaillance survient dans une partie du système, une notification est envoyée aux utilisateurs. En cas de panne, le système cesse de fonctionner jusqu'à ce que la cause du défaut soit détectée et supprimée. Pour les postes de travail mobiles (appareils Myco), dans les mêmes conditions décrites ci-dessus, une notification est fournie à tous les appareils connectés. Cette notification a le même niveau de gravité qu'une alarme clinique et ne peut pas être supprimée tant que la cause n'est pas supprimée.

Pour garantir la « single fault safety », au moins deux postes de travail Digistat Care doivent être installés dans le même département, ou bien au moins un poste de travail Digistat Care et une tour d'alarme LED.

Chaque poste de travail ou tour d'alarme LED peut ainsi contrôler le bon fonctionnement des autres composants. . Les postes de travail de bureau et la tour d'alarme LED surveillent également le « contrôleur ». Voir le manuel technique du Produit pour une description détaillée de l'architecture du système.



L'organisation de soins de santé doit mettre en œuvre des procédures internes afin de toujours assurer la présence d'au moins un membre du personnel clinique à proximité des postes de travail de bureau Digistat Care et, le cas échéant, de la tour d'alarme LED, pour être informé rapidement de toute alarme.

L'organisme de soins de santé doit mettre en place des procédures adéquates pour rendre le Produit à nouveau fonctionnel dans les plus brefs délais.



L'organisation de soins de santé doit définir des procédures de travail alternatives au cas où le système ne serait plus fiable ou cesserait de fonctionner.

4.4.1 Tour d'alarme LED

Digistat Care est conçu pour communiquer avec une tour d'alarme LED standard à l'aide d'un protocole standard. Lorsque Digistat Care est installé et configuré pour une distribution fiable des alarmes, la tour d'alarme LED émet des notifications informatives visuelles et sonores qui informent les utilisateurs de manière redondante si le système fonctionne correctement ou non.

La tour d'alarme LED peut être utilisée comme alternative au deuxième poste de travail Digistat Care, qui est par ailleurs indispensable pour une distribution fiable des alarmes.

La présence de la tour d'alarme LED dépend d'une option du système. Si la tour d'alarme LED est présente, le système peut être validé avec un seul poste de travail Digistat Care. Voir le manuel de configuration du produit pour plus d'informations.

À propos de la tour d'alarme LED :

- le voyant vert est allumé et aucun son n'est émis si le système fonctionne correctement ;
- le voyant rouge s'allume et une alarme sonore retentit lorsqu'une alarme technique se déclenche (défaillance du système - voir les sections 4.9 et 4.9.1).
- le voyant rouge s'allume et une alarme retentit lorsque la communication entre la tour d'alarme LED et le superviseur intelligent (le « contrôleur » mentionné ci-dessus) est interrompue ; simultanément, le superviseur intelligent émet une alarme technique lorsque la communication avec la tour d'alarme LED est interrompue.

La vérification du Digistat Care a été effectuée avec la tour de signalisation de surveillance réseau de Patlite, mais d'autres modèles pourraient être compatibles avec Digistat Care. Pour plus d'informations, contactez l'assistance technique Ascom UMS ou d'un distributeur.

La Tour de signalisation de surveillance réseau de Patlite est une tour de signalisation à trois niveaux avec une alarme sonore. Elle a la capacité de signaler immédiatement lorsqu'un événement réseau se produit via une connexion réseau.



Fig 1

4.5 Fiabilité du système

Si le système devient peu fiable, Une notification spécifique « Erreur système » est alors fournie sur les postes de travail de bureau (Fig 2), sur les appareils mobiles (Fig 3) et sur la tour d'alarme LED optionnel.

Lorsqu'une « erreur système » se produit, dans tous les lits concernés, aucune donnée patient ne s'affiche jusqu'à ce que le système redevienne fiable.

Les causes possibles de manque de fiabilité sont énumérées au paragraphe 4.5.3.

4.5.1 Ordinateur de bureau

Sur les postes de travail de bureau, les notifications restent sur la barre latérale (Fig 2 **B**) jusqu'à ce que les causes de non-fiabilité soient supprimées et que le système redevienne fiable. Dans tous les lits concernés par le manque de fiabilité, aucune donnée patient n'est affichée jusqu'à ce que le système soit à nouveau fiable.

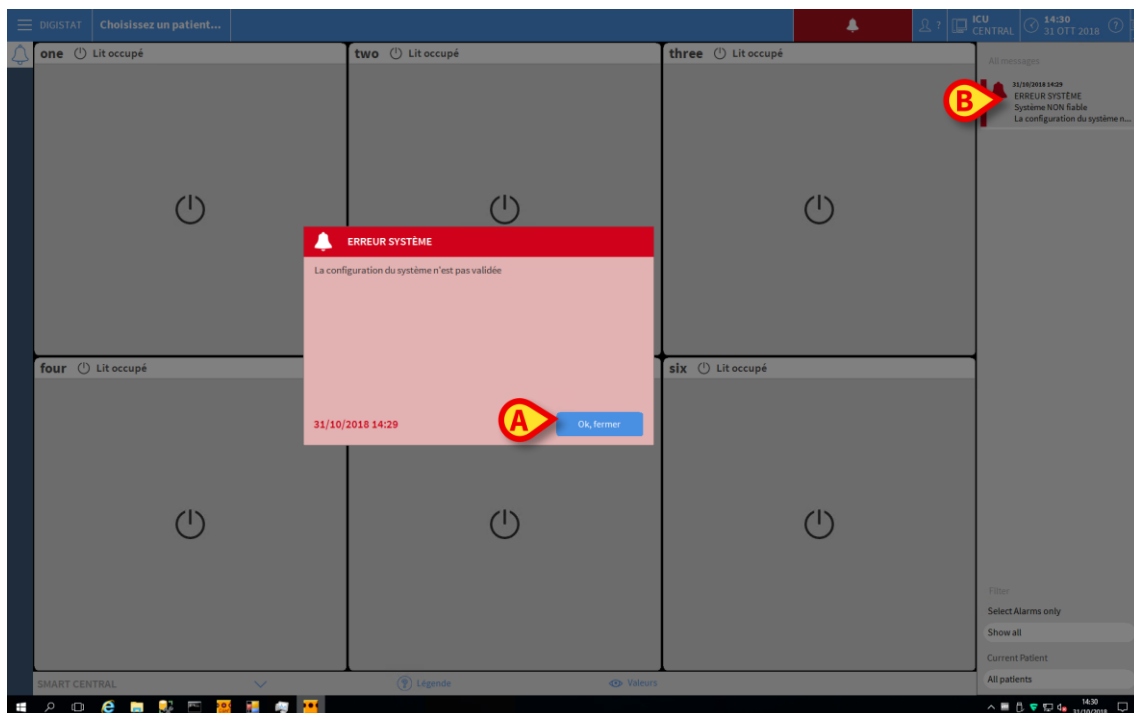


Fig 2 - Système non fiable (bureau)

- Cliquez sur **Ok, Fermer** sur la notification pour en accuser réception (Fig 2 **A**).

4.5.2 Mobile

Sur les appareils mobiles, la notification suivante est fournie (Fig 3 **A**). Une alarme sonore/vibratoire est également fournie.

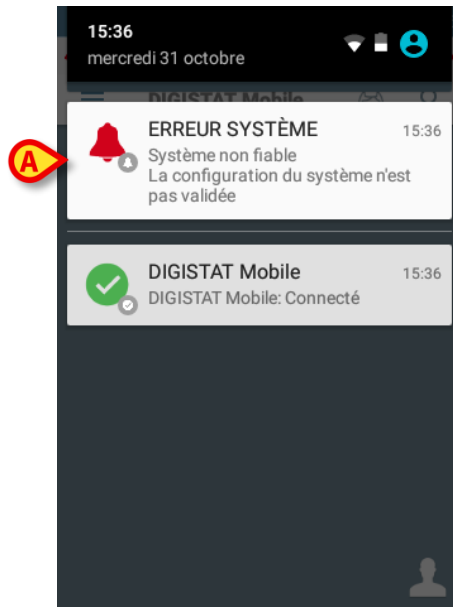


Fig 3 - Système non fiable (mobile)

- Glissez la notification vers le bas pour l'accepter sur le mobile (Fig 3 **A**). Après cette action, le son/la vibration s'arrête.

Un avertissement reste au dessus de chaque écran du mobile (Fig 4 **A**) jusqu'à ce que les causes de non-fiabilité soient supprimées et que le système redevienne fiable. Dans tous les lits concernés par le manque de fiabilité, aucune donnée patient n'est affichée jusqu'à ce que le système soit à nouveau fiable.



Fig 4

4.5.3 Causes de non fiabilité

En cas de manque de fiabilité du système, une alarme technique est fournie. L'alarme est une notification « Erreur système », qui fournit également une brève description des causes de non-fiabilité.

Les causes de non-fiabilité possibles sont les suivantes :

- « La configuration du système n'est pas validée »
- « Smart Central ne fonctionne pas correctement. Erreurs non gérées. Contactez les administrateurs système. »
- « Erreur de connexion Tour d'éclairage ({0}) »
- « Délai de réponse sur le système CDAS externe »
- « Système CDAS externe déconnecté »
- « Erreur d'accès à la base de données »
- « Anomalie dans le composant {0} ({1}) »
- « Le composant {0} ({1}) ne répond pas »
- « Le pilote {0} sur {1} ne répond pas »
- « Texte libre envoyé depuis le pilote »



Les caractères « {0} et ({1}) » représentent le nom du composant réel.

Dans ces cas, aucune donnée patient ne s'affiche jusqu'à ce que le système redevienne fiable.



Il est de la responsabilité de l'organisation de soins de santé utilisant le Produit de définir une procédure d'urgence à mettre en œuvre en cas d'indisponibilité du système.

4.6 Indisponibilité du système

Si le poste de travail (y compris les appareils mobiles) sur lequel le Produit est installé rencontre des problèmes lors de la connexion au serveur, un message d'information spécifique s'affiche.



Si le réseau ne correspond pas aux fonctions requises, les performances du Produit se détériorent progressivement. Le système peut enfin passer en mode "Recovery".

Le Produit tente de récupérer ses fonctionnalités automatiquement. Si la récupération automatique échoue, il est nécessaire de contacter l'assistance technique.. Voir 5 pour la liste des contacts.



La structure qui utilise le Produit est tenue de définir une procédure d'urgence à mettre en place en cas d'indisponibilité du système. Cette procédure a pour but:

1. de ne pas interrompre les activités des services
 2. de rétablir le plus rapidement possible la disponibilité du système (la politique de sauvegarde fait partie de cette gestion).
-

Ascom UMS ou le distributeur de référence sont disponibles pour fournir un soutien complet dans la définition de cette procédure. Voir la section 5 pour la liste de contacts.

Les caractéristiques et fonctionnalités décrites dans les sections 4.4, 4.4.1, 4.5 et 4.5.3 sont également applicables lorsque le produit n'est pas installé, ni configuré pour une distribution primaire des alarmes. C'est-à-dire lorsque la communication avec les dispositifs médicaux n'est pas fiable en raison des caractéristiques ou de l'utilisation prévue du protocole de communication des dispositifs médicaux.

Dans ces cas, les caractéristiques et fonctionnalités mentionnées ci-dessus fonctionnent comme un mécanisme de sécurité redondant supplémentaire supervisant les composants du produit. Ils ne supervisent pas la connexion avec les dispositifs médicaux.



Dans ces conditions, l'ensemble du système ne peut pas être considéré « single fault safe » et ne peut pas être utilisé pour une communication fiable des alarmes.

5. Coordonnées du fabricant

Pour toute question, s'adresser en premier au Distributeur qui a installé le produit.
Ci-dessous les coordonnées du fabricant:

Ascom UMS s.r.l unipersonale

Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italie

Tél. (+39) 055 0512161

Fax (+39) 055 8290392

Assistance technique

support.it@ascom.com

800999715 (numéro gratuit, Italie uniquement)

Informations ventes et produits

it.sales@ascom.com

Informations générales

it.info@ascom.com