DOMINO

Domino D-Series
Manuel d'utilisation
Pharma

D120i

D320i

D620i

PAGE VIERGE

TABLE DES MATIÈRES

PAGE VIERGE

INTRODUCTION

Ce manuel d'utilisation Pharma décrit le fonctionnement du système de marquage Laser D-Series utilisé via le TouchPanel distant ou via un PC équipé du logiciel Quickstep et de Microsoft Windows 7® ou Microsoft Windows 8®.

Il décrit les fonctionnalités spécifiques à la version Pharma du système de marquage Laser D-Series. Celui-ci comporte un système de gestion des codes utilisateur et des mots de passe, ainsi qu'une fonctionnalité de signatures électroniques et d'enregistrements électroniques.

Remarque : Une clé Domino Pharma doit être insérée dans le contrôleur et le Mode de sécurité doit être défini sur « Avancé » afin d'activer l'ID utilisateur et le mot de passe, ainsi que les fonctionnalités de signature et d'enregistrements électroniques.

Reportez-vous au manuel d'utilisation D-Series pour plus d'informations sur les fonctionnalités non spécifiques au modèle Pharma.

RÉGLAGE

(1) Connectez-vous à l'aide du nom d'utilisateur et du mot de passe d'administrateur.

(2) Sélectionnez *Paramètres* > *Sécurité* > *Configuration*.

(3) Sinon, cliquez sur la liste déroulante *Mode de sécurité* et sélectionnez *Avancé*.

Activer connexion auto : Sélectionnez cette option uniquement si vous souhaitez activer la connexion automatique pour un utilisateur sélectionné.

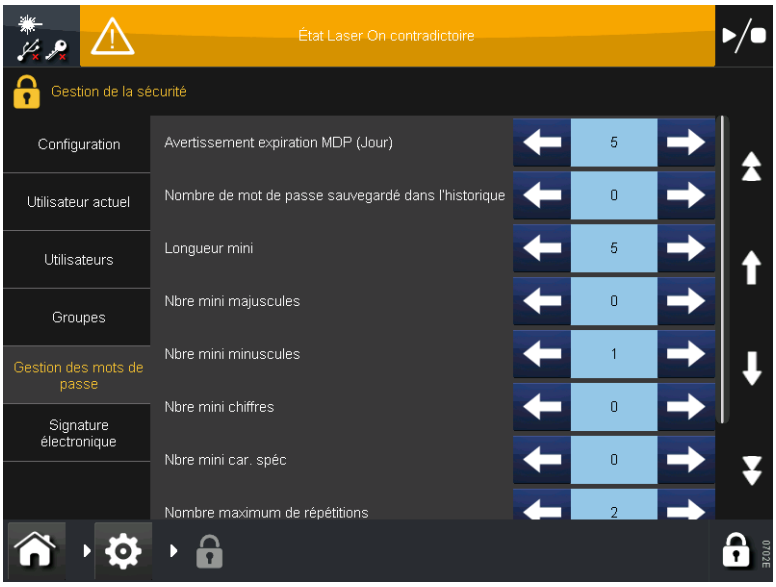
Utilisateur à connexion automatique : Sélectionnez l'utilisateur dans la liste déroulante.

Avertissement d'expiration du compte utilisateur (Jours) : Saisissez le nombre de jours précédant l'expiration du compte d'un utilisateur selon lequel un rappel doit s'afficher à l'écran.

Nombre maximum de tentatives de connexions autorisées : Saisissez le nombre maximum d'échecs de connexion autorisé avant le verrouillage d'un compte.

GESTION DES MOTS DE PASSE

Sélectionnez *Paramètres* > *Sécurité* > *Gestion des mots de passe*.



Il est possible de configurer les éléments suivants :

- Avertissement expiration MDP (Jours).
- Nombre de mots de passe de passe sauvegardé dans l'historique : nombre de nouveaux mots de passe utilisés avant la répétition d'un mot de passe.
- Longueur mini.
- Nbre mini majuscules.
- Nbre mini minuscules.
- Nombre mini chiffres.
- Nbre mini car. spéc.
- Nombre maximum de répétitions : nombre maximum de caractères dupliqués qu'un mot de passe peut contenir.
- Caractères ID max : nombre maximum de caractères correspondant à l'ID utilisateur qu'un mot de passe peut contenir.
- Caractères spéciaux : saisissez les caractères spéciaux requis (vous pouvez sélectionner le caractère de votre choix sur le clavier).

GROUPES

Un groupe comprend un nombre sélectionné d'autorisations utilisateur. Le modèle D-Series est fourni avec quatre groupes par défaut : Admin, Logout, Supervisor, Operator, chacun comportant un ensemble propre d'autorisations sélectionnées. Toutefois, l'ensemble d'autorisations de chaque groupe est modifiable, le cas échéant.

Les nouveaux utilisateurs et les utilisateurs existants héritent d'autorisations lorsqu'ils sont associés à un ou plusieurs groupes.

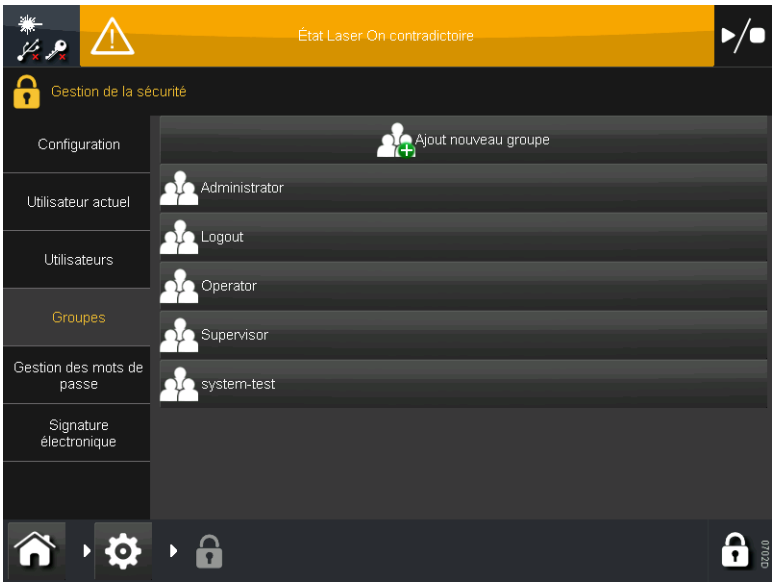
Il est également possible d'ajouter de nouveaux groupes, avec des autorisations requises.

AJOUT DE NOUVEAUX GROUPES

Cette fonction permet de créer des groupes associés à des autorisations définies. Les utilisateurs associés à un ou plusieurs de ces groupes héritent des autorisations du/des groupe(s) en question.

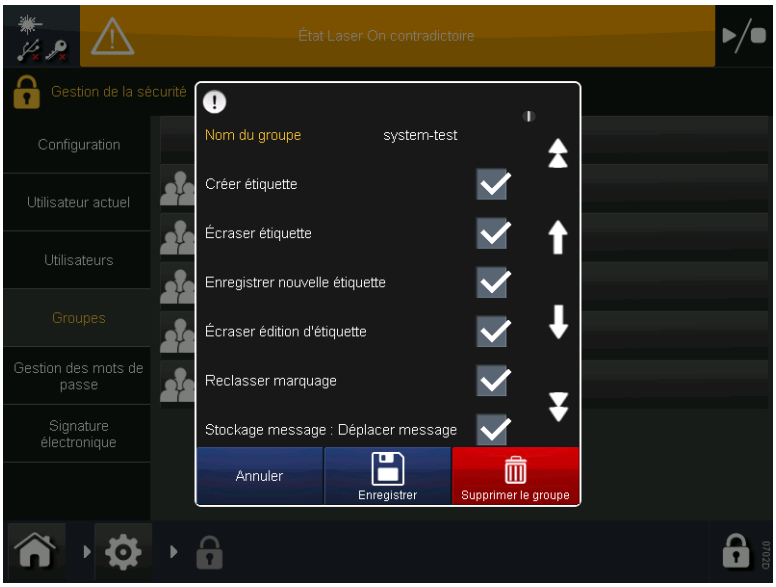
(1) Sélectionnez *Paramètres* > *Sécurité* > *Groupes*.

(2) Sélectionnez *Ajout nouveau groupe*.



(3) Saisissez un nouveau nom de groupe et sélectionnez *Enregistrer*.

(4) Cochez les cases des autorisations requises pour le groupe.



(5) Sélectionnez *Enregistrer* afin d'afficher le nouveau groupe dans la liste Groupes.

SUPPRESSION DE GROUPES

(1) Sélectionnez *Paramètres* > *Sécurité* > *Groupes*.

(2) Sélectionnez le groupe souhaité dans la liste Groupes, puis sélectionnez *Supprimer le groupe*.

(3) Sélectionnez *OK* afin de confirmer l'opération.

MODIFICATION DES AUTORISATIONS

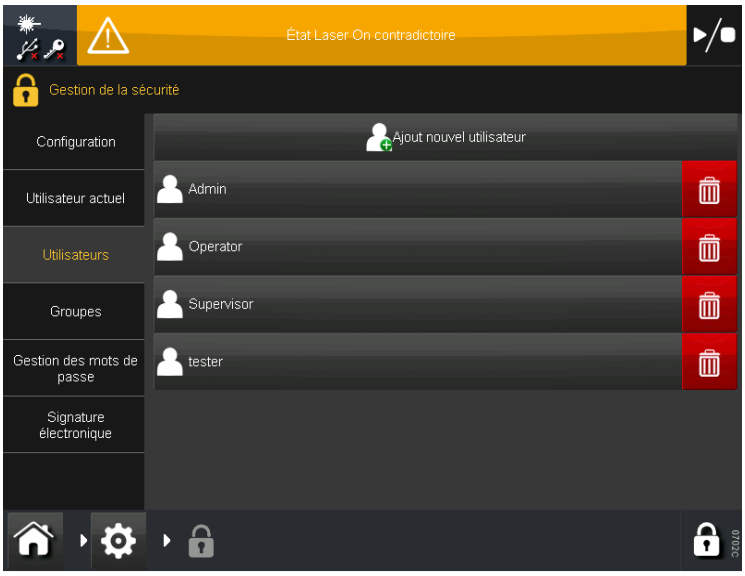
(1) Sélectionnez *Paramètres* > *Sécurité* > *Groupes*.

(2) Sélectionnez le groupe requis et modifiez les autorisations, selon les besoins.

(3) Sélectionnez *Enregistrer* pour confirmer les modifications.

AJOUT DE NOUVEAUX UTILISATEURS

(1) Sélectionnez *Paramètres* > *Sécurité* > *Utilisateurs*.



(2) Sélectionnez *Ajout nouvel utilisateur*.

Nom d'utilisateur : saisissez le nom d'utilisateur requis (c.-à-d. user-id.).

Mot de passe : saisissez le mot de passe choisi.

Ressaisir le mot de passe : confirmez le mot de passe.

Groupes : Dans la liste déroulante, saisissez le ou les groupes dont les autorisations sont requises pour le nouvel utilisateur.

État : Dans la liste déroulante, sélectionnez *Actif, Inactif* ou *Verrouillé*.

Vérifiez que la case *Vous devez changer votre mot de passe* est cochée, afin d'obliger le nouvel utilisateur à modifier son mot de passe lorsqu'il se connectera pour la première fois.

Si nécessaire, entrez le *Nom*, le *Prénom* et le *Département* du nouvel utilisateur.

Temporisation d'inactivité en minutes : Le cas échéant, définissez le délai d'inactivité de l'utilisateur qui provoquera une déconnexion automatique.

Expiration du compte activée : Cochez la case pour activer l'option.

Date d'expiration du compte : Le cas échéant, sélectionnez la date à laquelle le compte de l'utilisateur arrivera automatiquement à expiration.

Jours avant l'expiration du mot de passe : entrez le nombre de jours à l'issue duquel le mot de passe de l'utilisateur arrivera à expiration, nécessitant la création d'un nouveau mot de passe.

SUPPRESSION D'UTILISATEURS

Remarque : L'action de suppression ne peut pas être annulée.

(1) Sélectionnez *Paramètres* > *Sécurité* > *Utilisateurs*.

(2) Sélectionnez le symbole de suppression de l'utilisateur souhaité  .

(3) Sélectionnez *OK* pour supprimer l'utilisateur.

MODIFICATION DES MOTS DE PASSE UTILISATEUR

(1) Sélectionnez *Paramètres* > *Sécurité* > *Utilisateurs* et sélectionnez l'utilisateur requis.

(2) Sélectionnez, puis saisissez le nouveau mot de passe et ressaisissez-le pour le confirmer.

(3) Sélectionnez *Modifier* et *Enregistrer* pour modifier le mot de passe.

MODIFICATION DE L'ÉTAT D'UN UTILISATEUR

Vous avez la possibilité de remplacer l'état actuel de l'utilisateur (par exemple, « Verrouillé ») par un nouvel état (par exemple, « Actif »).

(1) Sélectionnez *Paramètres* > *Sécurité* > *Utilisateurs* et sélectionnez l'utilisateur requis.

(2) Sélectionnez le nouvel état souhaité dans la liste déroulante État : *Actif, Inactif* ou *Verrouillé*.

(3) Sélectionnez *Enregistrer*.

ENREGISTREMENTS ET SIGNATURES ÉLECTRONIQUES

Le système permet l'utilisation de signatures électroniques et la création d'enregistrements électroniques.

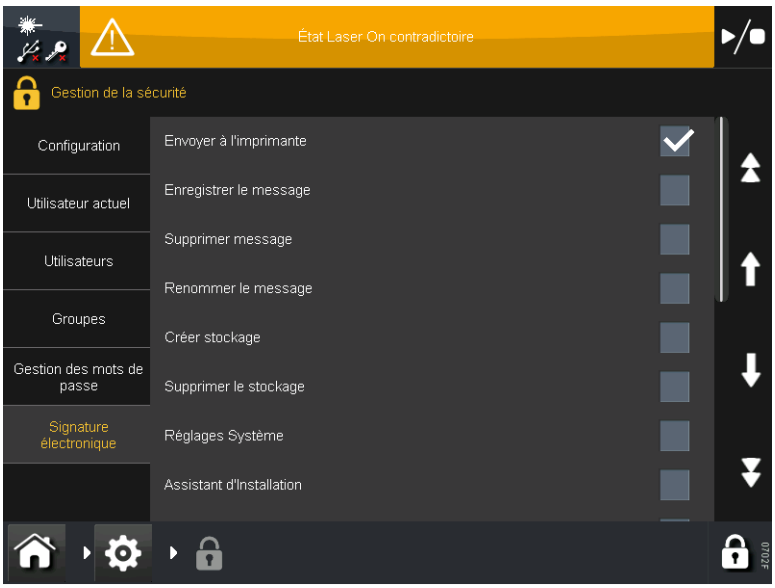
Lorsque les utilisateurs tentent d'exécuter une action, qui a été configurée comme nécessitant une signature électronique, ils sont invités à entrer leur mot de passe (c'est-à-dire à associer leur ID utilisateur et leur mot de passe à l'action en question) afin de créer un enregistrement électronique.

Un journal d'actions répertoriant les actions de l'utilisateur est créé. Ce journal peut être exporté sous la forme d'un fichier .db.

Exemple

L'exemple suivant illustre la fonctionnalité de signature et d'enregistrements électroniques.

(1) Connectez-vous en tant qu' « Administrator » et sélectionnez *Paramètres* > *Sécurité* > *Signature électronique*.



(2) Sélectionnez les autorisations pour lesquelles une signature électronique sera requise, puis sélectionnez *OK*. Dans cet exemple, l'autorisation « Envoyer à l'imprimante » est sélectionnée.

(3) Tous les utilisateurs seront désormais invités à entrer leur mot de passe avant de réaliser l'action sélectionnée dans la liste ci-dessus. Cette action, ainsi que la date et l'heure de sa réalisation, sera ensuite enregistrée et associée à leur nom dans le journal Audit Trail, et constituera un enregistrement électronique.

Remarque : Toute option de signature électronique sélectionnée s'appliquera à tous les utilisateurs, y compris l'administrateur.

(4) Accédez à l'Éditeur de messages, créez un message et insérez le texte « MESSAGE ONE ».

(5) Enregistrez le message en lui attribuant le nom souhaité.

(6) Sélectionnez *Envoyer à l'imprimante* et vous serez invité à saisir votre mot de passe ; une fois saisi, le message sera envoyé à l'imprimante. Cette action sera répertoriée dans le journal Audit Trial et constituera un enregistrement électronique.

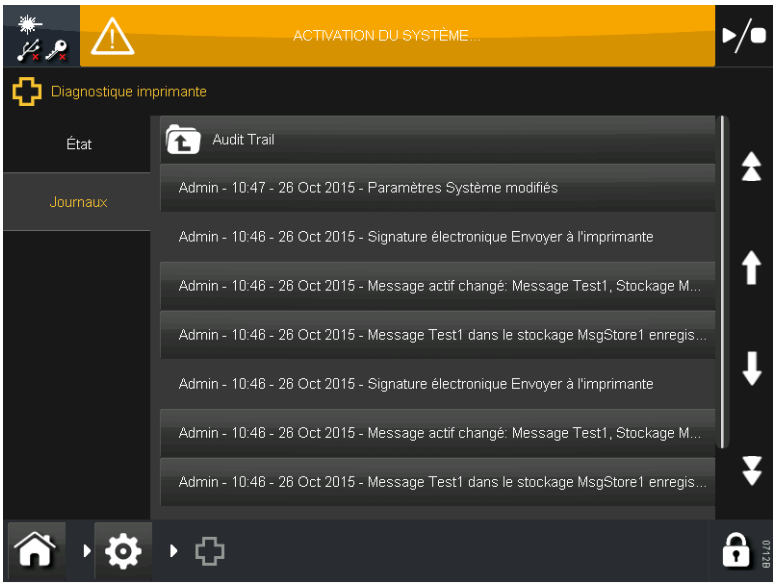
(7) Imprimez le message plusieurs fois.

(8) Modifiez le message en changeant le texte en « MESSAGE TWO ».

(9) Enregistrez le message, puis envoyez-le à l'imprimante en entrant le mot de passe dans la boîte de dialogue de signature électronique, comme détaillé précédemment. Imprimez le message plusieurs fois.

(10) Sélectionnez *Paramètres* > *Diagnostics* > *Journaux* > *Audit Trail*. Cet écran affiche une liste d'actions avec la date et l'heure de réalisation de chaque action, l'ID utilisateur de la personne l'ayant réalisée et une description de l'action.

(11) Sélectionnez l'entrée « Objet texte 1 changé ».



(12) Le détail des modifications apportées au texte est alors affiché.

JOURNAL AUDIT TRAIL

Pour optimiser les performances du système, un archivage quotidien est effectué dans le journal d'actions ; les anciens enregistrements de la base de données active sont ainsi déplacés vers la base de données d'archivage.

Le journal Audit Trail affiche les 300 enregistrements les plus récents ainsi que toute entrée créée depuis le dernier archivage.

Vous pouvez l'exporter à tout moment. Toutefois, lorsque 183 jours (nombre de jours par défaut) se sont écoulés depuis sa création, il est impossible d'activer le marquage tant que le journal n'a pas été exporté.

Lorsque le journal existe depuis 153 jours (nombre de jours par défaut), un message d'avertissement s'affiche afin de signaler que ce journal doit être exporté.

Pour modifier le nombre de jours au bout duquel les messages d'avertissement et d'erreur sont affichés, sélectionnez *Accueil* > *Paramètres* > *Configuration des alertes* > *Alertes classées*.

Pour exporter le journal Audit Trail

(1) Insérez un périphérique de stockage USB dans l'un des ports USB du contrôleur, ou dans le port USB de votre périphérique d'accès à distance (tel que le panneau à écran tactile).

(2) Sélectionnez *Accueil* > *Paramètres* > *Gestion des fichiers* > *PrinterDisk* > *Journaux*.

(3) Sélectionnez l'icône en forme de crayon du journal Audit Trail et sélectionnez *Copier*.

(4) Sélectionnez *Gestion des fichiers,* puis *le* périphérique mémoire USB approprié.

(5) Sélectionnez *Coller* pour copier le journal dans le périphérique mémoire USB.

Le fichier journal d'audit (extension : .log) sera répertorié sur le périphérique mémoire USB.

DYN3LOGVIEWER DE DOMINO

Une fois l'exportation effectuée, l'utilitaire Dyn3LogViewer de Domino, disponible sur demande auprès de Domino, peut être utilisé pour visualiser le journal Audit Trail (enregistrements actifs ou archivés) sur un PC MS Windows classique avec .NET Framework 3.5 installé.

L'utilitaire Dyn3LogViewer peut aussi être utilisé pour exporter le journal d'actions vers un fichier texte.

Pour afficher le journal Audit Trail :

Ouvrez l'utilitaire Dyn3LogViewer et sélectionnez *File* > *Open*, puis sélectionnez le journal Audit Trail requis à l'emplacement où il est enregistré.

La langue des entrées du journal peut être modifiée en sélectionnant *Language* puis en choisissant la langue souhaitée dans la liste déroulante.

Pour exporter le journal Audit Trail en tant que fichier texte :

Ouvrez l'utilitaire Dyn3LogViewer et sélectionnez *File* > *Open* > *Export To Text File* ; sélectionnez ensuite l'emplacement auquel vous souhaitez enregistrer le fichier et appuyez sur le bouton *Save*.

SUPPRESSION DU JOURNAL AUDIT TRAIL

(1) Sélectionnez *Paramètres* > *Diagnostics* > *Journaux* > *Audit Trail*.

(2) Sélectionnez l'icône rouge  pour afficher la valeur « Supprimer les entrées plus anciennes que (jours) ». Le cas échéant, modifiez le paramètre « nombre de jours » et sélectionnez *OK*.