KONICA MINOLTA

bizhub PRESS C1100/C1085

Sécurité

bizhub PRESS C1100/C1085

COLOUR PRODUCTION PRINTING SYSTEM

Giving Shape to Ideas

Table des matières

1 Introduction

1 Introduction

1.1 Bienvenue

Nous vous remercions d'avoir porté votre choix sur cette machine.

Ce Guide de l'utilisateur décrit des fonctions de sécurité. Ce Guide de l'utilisateur est disponible quand vous voulez savoir comment utiliser le mode Sécurité renforcée ou comment utiliser cette machine en cas d'utilisation de la fonction Sécurité renforcée.

1.1.1 Composition et utilisation de ce Guide

Quand vous voulez en savoir plus sur les fonctions détaillées ou les procédures de fonctionnement, consultez le **Guide de l'utilisateur HTML** présent sur le **DVD du Guide de l'utilisateur**.

Titre du manuel sur le DVD du Guide de l'utilisateur	Sommaire
Guide rapide IC-602	Ce guide décrit les opérations de base de la machine, les procédures d'installation du pilote d'imprimante et des applications pour l'utilisation du **contrôleur d'image IC-602**, les procédures de remplacement des consommables ainsi que d'autres informations générales relatives à l'utilisation de la machine.
Guide rapide pour le serveur couleur Fiery	Ce guide décrit les opérations de base de la machine, les procédures d'installation du pilote d'imprimante et des applications pour l'utilisation du **contrôleur d'image IC-308** ou du **contrôleur d'image IC-310**, les procédures de remplacement des consommables et d'autres informations générales relatives à l'utilisation de la machine.
Informations de sécurité	Ce guide dispense des précautions et instructions à suivre pour garantir une utilisation sûre de la machine. Veuillez lire ce guide avant d'utiliser la machine.
Guide de l'utilisateur - Sécurité (ce guide)	Ce guide décrit les fonctions de sécurité. Ce guide est disponible quand vous voulez savoir comment utiliser le mode Sécurité renforcée ou comment utiliser cette machine en cas d'utilisation de la fonction Sécurité renforcée.
Guide de l'utilisateur HTML	Ce guide décrit les opérations de base, les fonctions qui facilitent les opérations, comment procéder à l'entretien, au dépannage élémentaire ainsi que diverses méthodes de réglage de cette machine.

Notez que les utilisateurs doivent disposer de notions techniques de base sur le produit pour effectuer des interventions d'entretien ou des opérations de dépannage. Les opérations d'entretien et de dépannage devraient être effectuées comme indiqué dans ce guide et le **Guide de l'utilisateur HTML** présent sur le **DVD du Guide de l'utilisateur**.

Si vous rencontrez le moindre problème, veuillez contacter votre technicien S.A.V.

REMARQUE

Sous Mac OS X 10.7 ou ultérieur, il se peut que le paramètre du montage soit désactivé si une icône ne s'affiche pas sur le bureau, même si le DVD des Guides de l'utilisateur est inséré ; vérifiez si le paramètre de montage est désactivé ou non sous "Preferences" du menu Finder.

1.2 Conventions utilisées dans ce guide

1.2.1 Symboles utilisés dans ce guide

Les symboles qui figurent dans ce guide pour présenter divers types d'informations.

Chaque symbole concernant l'utilisation correcte et sûre de cette machine est décrit ci-après.

Pour utiliser cette machine en toute sécurité

⚠AVERTISSEMENT

- La négligence de cet avertissement peut provoquer des blessures graves, voire mortelles.

⚠ATTENTION

- Le non-respect de cette précaution peut provoquer des blessures graves, ou des dommages matériels.

REMARQUE

Ce symbole indique un risque de dommage à la machine ou aux originaux. Suivez les instructions pour éviter les dommages matériels.

Instructions concernant les procédures opératoires

✔ Cette coche indique une option qui est nécessaire pour utiliser les conditions ou les fonctions préalables à une procédure.

1 Un chiffre à ce format "1" représente la première étape.

2 Un chiffre sous cette forme représente l'ordre d'une séquence d'étapes.

➔ Ce symbole indique une explication supplémentaire concernant une instruction de procédure.

Les procédures opératoires sont explicitées par des illustrations.

➔ Ce symbole indique le changement du panneau de contrôle pour accéder à un élément de menu désiré.

La page concernée est affichée.

Pour info
Ce symbole indique une référence.

Consultez la référence selon les besoins.

Symboles des touches

[ ]

Les noms de touches sur l'écran tactile ou sur l'écran de l'ordinateur, ou un nom de Guide de l'utilisateur figurent entre crochets.

Texte Gras

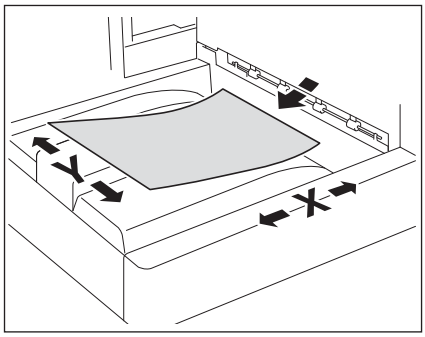
Les noms des touches sur **panneau de contrôle**, les noms des composants, les noms de produit et les noms d'option figurent en texte gras.

1.2.2 Indications relatives au papier et aux originaux

Format papier

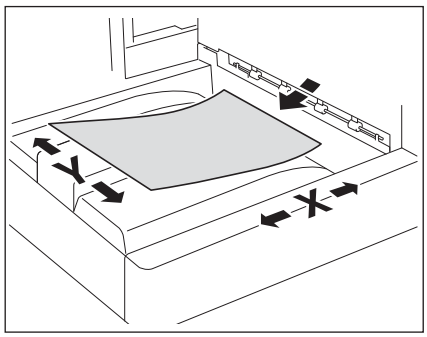
Ce qui suit explique les indications relatives aux originaux et au papier décrits dans ce manuel.

Dans toute indication relative à l'original ou au format de papier, l'axe Y représente la largeur et l'axe X, la longueur.

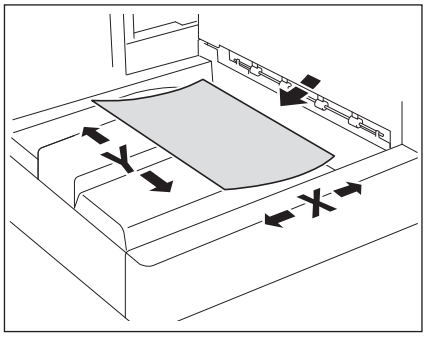


Indication papier

▭ indique le format de papier dont la longueur (X) est supérieure à la largeur (Y).



▯ indique le format de papier dont la longueur (X) est inférieure à la largeur (Y).



2 Fonctions de Sécurité

2 Fonctions de Sécurité

2.1 Logiciel de commande

2.1.1 Version du logiciel de commande

La version du logiciel de contrôle est la suivante.

Version programme de contrôle image (Image Control I1/I4) :

A5AW0Y0-00I1-G00-10

A5AW0Y0-00I4-G00-10

Version programme de contrôle Contrôleur (IC Controller P1) :

A5AW0Y0-00P1-G00-10

Si vous voulez confirmer l'environnement d'évaluation pour ISO15408 (comme les versions du logiciel et du pilote d'imprimante), contactez votre technicien S.A.V.

2.1.2 À propos de la fonction d'affichage de la version ROM

La version du logiciel de contrôle de **bizhub PRESS C1100/C1085** indiquée ci-dessus peut être vérifiée grâce à la fonction d'affichage de la version ROM en mode Ingénieur Support Client (CE).

Lors de l'utilisation de la fonction d'affichage de la version ROM, la version du programme de contrôle s'affiche comme suit.

Exemple : Contrôle image I1 : A5AW0Y0-00I1-G00-** (** est un nombre à deux chiffres)

Gardez cela à l'esprit lors de la vérification de la version du programme de contrôle.

2.2 Fonctions de Sécurité

2.2.1 Mode Sécurité

Le **bizhub PRESS C1100/C1085** possède deux modes de sécurité.

Mode Normal

Utilisez ce mode quand la machine est utilisée par une seule personne et qu'il y a une faible possibilité d'accès ou d'utilisation illicite. Ce mode est déjà réglé comme réglage d'usine. Pour utiliser cette machine en mode normal, consultez les guides de l'utilisateur fournis pour chaque opération.

Sécurité renforcée

Utilisez Sécurité renforcée quand la machine est reliée à un réseau local ou à des réseaux externes via une ligne téléphonique ou tout autre moyen. Un administrateur désigné pour la gestion de la machine doit suivre les instructions de ce guide pour que les utilisateurs puissent bénéficier d'un environnement d'exploitation sûr.

Pour utiliser la Sécurité renforcée, contactez votre technicien S.A.V. pour les réglages suivants.

Un technicien S.A.V. doit définir un mot de passe CE pour l'authentification CE et un code administrateur sur la machine. Le technicien S.A.V. entre le mot de passe CE pour les interventions CE. L'administrateur qui obtient le code administrateur auprès du technicien S.A.V. se sert du code pour procéder à des réglages liés à la Sécurité renforcée.

L'administrateur ne doit jamais divulguer le code administrateur à d'autres personnes.

L'administrateur ayant reçu le code administrateur gère la machine configurée avec la Sécurité renforcée en procédant à des réglages dans l'ordre suivant :

1. ACTIVER/DÉSACTIVER la Sécurité renforcée
2. Code verrouillage DD
3. Ajouter/Modifier/Supprimer des utilisateurs enregistrés

L'administrateur est également responsable de fournir aux utilisateurs les instructions suivantes :

- Ne jamais divulguer son mot de passe à d'autres.
- S'assurer de se déconnecter avant de quitter la machine après s'être connecté via l'authentification de l'utilisateur.

S'assurer d'utiliser la Sécurité renforcée pour empêcher tous accès non autorisé au disque dur.

Quand la Sécurité renforcée est activé, la machine affiche une icône de sécurité 

en bas à droite de l'écran tactile.

L'icône de sécurité disparaît quand la Sécurité renforcée est désactivée. Si l'administrateur désactive par inadvertance la Sécurité renforcée, contacter le technicien S.A.V. Demander à un ingénieur support client (CE) de vérifier l'environnement et les réglages de sécurité avant de réactiver la Sécurité renforcée.

2.2.2 Environnement

Environnement dans lequel la Sécurité renforcée est recommandée

Un environnement dans lequel la machine est surveillée via une ligne téléphonique ou un réseau

Créer un environnement sûr

Pour la sécurité, nous recommandons que les superviseurs et un administrateur utilisent la Sécurité renforcée et établissent un environnement comme suit.

Un ordinateur client dédié à la commande de la machine devrait être utilisé dans un état sûr en appliquant les dernières mises à jour disponibles au public pour le système d'exploitation et les applications (logiciels antivirus, pilotes d'imprimante, navigateurs, etc.).

Les fichiers d'impression sécurisée et les fichiers d'impression sur authentification ne sont pas cryptés pendant la transmission d'un PC client à la machine. Mettre en œuvre des mesures contre les écoutes téléphoniques, telles que l'installation d'un appareil de communication cryptographique ou un équipement anti-bogage afin de protéger les fichiers d'impression sécurisée et les fichiers d'impression sur authentification.

- Qualifications requises pour devenir administrateur :
  un superviseur sélectionne une personne fiable possédant les connaissances, les aptitudes techniques et l'expérience nécessaires en qualité d'administrateur à qui déléguer l'administration de la machine.
- Garantie d'un ingénieur support client (CE) :
  un superviseur ou un administrateur peut utiliser la Sécurité renforcée après s'être assuré qu'un contrat de maintenance a été signé avec un ingénieur support client (CE). Stipuler clairement dans le contrat de maintenance que l'ingénieur support client (CE) ne commettra aucune action frauduleuse.
- LAN sécurisé :
  s'assurer de bien raccorder la machine à un réseau local protégé par un pare-feu afin d'interdire l'accès depuis les réseaux externes. S'assurer également qu'aucun appareil illicite n'est connecté au réseau local.
- Un administrateur devrait désigner l'emplacement d'installation censé n'être disponible que pour les utilisateurs du produit. Installer la machine dans un local fermé à clé durant la nuit et pendant la journée à un emplacement permettant à l'administrateur de surveiller la machine de sorte que des pièces telles qu'un disque dur ne puissent pas être volées ou que tout autre appareil spécial tel qu'un analyseur interne ne puisse pas être raccordé à la machine. L'équipement retiré de la machine tel qu'un disque dur doit être traité de la même manière que la machine elle-même.
- La présence d'un administrateur est requise lors des interventions d'un ingénieur support client (CE) telles que les travaux d'installation ou de maintenance.
- Un administrateur devrait vérifier à intervalles réguliers que le réglage de la date/l'heure est correct sur la machine.

2.2.3 Description de la Sécurité renforcée

Les fonctions de sécurité sont renforcées comme suit.

Protection et suppression de données restantes après utilisation

Il existe deux types de données d'image archivées dans la mémoire ou sur le disque dur : les données AHA comprimées et les données non comprimées au format TIFF et PDF et les données PS. La zone image de la mémoire ou du disque dur hébergeant les données AHA comprimées est libérée une fois que les données ont été effacées. En mode normal, les données ne sont pas entièrement supprimées, ce qui peut permettre une lecture non autorisée des données. Avec la Sécurité renforcée, la zone image de la mémoire ou du disque dur est écrasée par des données non liées à l'image avant que le secteur ne soit libéré sans tenir compte du fait que les données images archivées soient comprimées.

Mots de passe renforcés

Il existe 5 mots de passe différents fournis pour les fonctions de sécurité.

- Mot de passe CE
- Code administrateur
- Mot de passe utilisateur
- Mot de passe du compte
- Code verrouillage DD

Le mot de passe CE et le code administrateur devraient comporter 8 caractères alphanumériques (les caractères alphabétiques étant sensibles à la casse).

Le mot de passe du compte devrait comporter 1 à 8 caractères alphanumériques (sensibles à la casse).

Normalement, le mot de passe utilisateur comporte de 1 à 64 caractères alphanumériques (sensibles à la casse) ; toutefois un mot de passe utilisateur de moins de 8 caractères ne peut pas être utilisé en Sécurité renforcée. Si vous entrez 64 caractères ou plus, le caractère saisi en dernier sera identifié comme 64e caractère.

Le code verrouillage DD devrait comporter de 8 à 32 caractères alphanumériques (sensibles à la casse). Si vous entrez 32 caractères ou plus, le caractère saisi en dernier sera identifié comme 32e caractère.

À l'instar du mot de passe CE, du code administrateur et du mot de passe du compte, la machine reconnaît le dernier caractère saisi en tant que huitième caractère en cas de saisie de 8 caractères ou plus.

En Sécurité renforcée, la machine rejette également toute saisie pendant 5 secondes, si un mot de passe incorrect est saisi pour l'un des 5 mots de passe mentionnés ci-dessus.

En cas d'oubli de tout mot de passe relevant de la sécurité, agir comme suit en fonction du type de mot de passe.

- Pour un mot de passe utilisateur ou un mot de passe du compte, contacter l'administrateur.
- En cas d'oubli du mot de passe administrateur ou du code verrouillage DD, contacter le technicien S.A.V.

Nous recommandons de modifier chaque mot de passe à intervalles réguliers afin d'empêcher tout accès illicite ou toute altération des données.

Accès aux données

S'assurer qu'un utilisateur est requis pour saisir un mot de passe renforcé ayant été défini par l'administrateur afin d'archiver les données dans la boîte utilisateur stockée sur le DD ou pour imprimer les données archivées.

Lors de la sauvegarde de données numérisées dans une boîte utilisateur, il est possible d'améliorer la sécurité en définissant un mot de passe renforcé. Seuls les administrateurs peuvent supprimer les dossiers et les boîtes utilisateur hébergeant les données numérisées. Une fois que l'attribut d'une boîte utilisateur a été modifié, l'authentification de l'utilisateur avec un mot de passe renforcé est requise. L'authentification de l'utilisateur est également requise pour utiliser les données numérisées sauvegardées.

Réglages Carte réseau machine

Quand la Sécurité renforcée est activée, la carte réseau machine ne peut pas être utilisée.

Blocage des accès externes

Aucun accès n'est autorisé via les lignes téléphoniques autre que CS Remote Care.

Créer, enregistrer et analyser un journal des événements

Un historique des opérations de la fonction de sécurité est créé et enregistré sous la forme d'un journal des événements. La date et l'heure, des informations d'identification de la personne ayant procédé à l'opération, les détails de l'opération et les résultats de l'opération sont enregistrés, ce qui permet d'analyser les accès non autorisés. Ce journal sera écrasé si le secteur d'événement est supprimé.

Authentification de l'administrateur

Un technicien S.A.V. est censé configurer les données d'authentification pour un administrateur. En fonction de ces données d'authentification, l'administrateur bénéficie d'un accès autorisé après avoir saisi le code administrateur. Une seule chaîne d'authentification peut être enregistrée par machine.

Mode Réglage administrateur

La machine passe en mode réglage administrateur quand l'authentification du mot de passe est effectuée avec succès par l'administrateur. En mode réglage administrateur, le changement de réglage de diverses fonctions de la machine est disponible.

S'assurer de bien quitter le mode réglage administrateur si la machine est laissée sans surveillance avec ce mode activé.

Carte IC

Avec la Sécurité renforcée activée, la machine rejette l'authentification de l'utilisateur avec une carte IC.

Fonctions de port USB

Les fonctions suivantes sont encore disponibles via un port USB même quand la Sécurité renforcée est activée :

- USB Memory ISW
- Archivage de données de listes ou de rapports via USB
- Enregistrement de catégories dans Contrôle densité couleur
- Enregistrer des données dans Réglage uniformité densité
- Imprimer des mires via USB (pour CE)
- Clavier, souris

Imprimante

L'exécution d'une opération d'impression depuis un PC nécessite un contrôleur d'imprimante et un pilote d'imprimante. En utilisant le contrôleur d'imprimante prenant en charge la Sécurité renforcée, il est possible d'enregistrer les données d'impression dans la mémoire interne ou sur le disque dur en saisissant un nom d'utilisateur depuis le pilote d'imprimante. Les données archivées peuvent être imprimées une fois que le nom d'utilisateur a été authentifié avec succès avec son mot de passe correspondant saisi depuis le pilote d'imprimante lors de la sauvegarde des données. Veuillez noter que les données archivées peuvent être potentiellement imprimées par d'autres en cas d'utilisation du nom d'utilisateur de quelqu'un d'autre pour enregistrer les données d'impression.

Pour des détails sur le contrôleur d'imprimante et le pilote d'imprimante prenant en charge la Sécurité renforcée, veuillez contacter le technicien S.A.V.

Pour la procédure d'utilisation du contrôleur ou du pilote d'imprimante, consulter le guide de l'utilisateur correspondant.

2.2.4 Données protégées par la Sécurité renforcée

Utiliser la Sécurité renforcée pour empêcher d'être écrites vers un disque dur connecté de manière illicite.

De même, il vaut mieux sécuriser les données suivantes gérées par l'administrateur :

- les données de l'utilisateur
- les données permettant de gérer la machine

Données exemptes de protection par la Sécurité renforcée

Quand la machine est connectée à des PC au sein d'un réseau local, les mots de passe saisis depuis les PC ne sont pas soumis à la Sécurité renforcée. Éviter de saisir tout mot de passe depuis de tels PC afin d'éviter toute fuite.

ACTIVER/DÉSACTIVER la Sécurité renforcée

L'administrateur est responsable de l'activation/la désactivation de la Sécurité renforcée.

L'administrateur ne devrait jamais oublier d'activer la Sécurité renforcée. Faire plus particulièrement attention lors de la désactivation de la Sécurité renforcée en gardant à l'esprit que l'accès aux données est potentiellement possible.

2.2.5 Protection et suppression de données restantes après utilisation

Les données des modes Copie, Numérisation et Imprimante sont temporairement archivées en mémoire ou sur le disque dur et supprimées après utilisation en l'absence d'une action telle que leur enregistrement dans une boîte utilisateur.

Les données sont comprimées de manière spéciale et ne peuvent généralement pas être décomprimées en externe. Lors de la suppression des données comprimées, en outre, une partie des données est soit détruite ou écrasée ce qui désactive la décompression des données proprement dite.

- Les données temporairement archivées en mémoire seront écrasées par des données invalides si la tâche est interrompue ou arrêtée.
- Les données enregistrées sur plusieurs secteurs de la mémoire seront simultanément écrasées par des données invalides.

Les données enregistrées dans une boîte seront écrasées par des données invalides lors de l'émission d'une instruction de suppression.

- Si les données sont transmises en externe, elles seront écrasées par des données invalides quand la transmission sera terminée.
- Si l'administrateur émet une instruction de suppression pour chaque boîte, elle seront écrasées par des données invalides.

2.3 Fonctions de Sécurité Administrateur

L'administrateur ACTIVE/DÉSACTIVE la Sécurité renforcée à partir de l'écran du menu Utilitaire. Pour cette opération il faut configurer un mot de passe CE et un code administrateur sur la machine. Demandez à votre technicien S.A.V. de configurer un code administrateur. Une fois spécifié, le mot de passe peut être modifié par l'administrateur. Pour des informations détaillées sur la configuration et l'utilisation du code administrateur, consultez le Guide de l'utilisateur HTML.

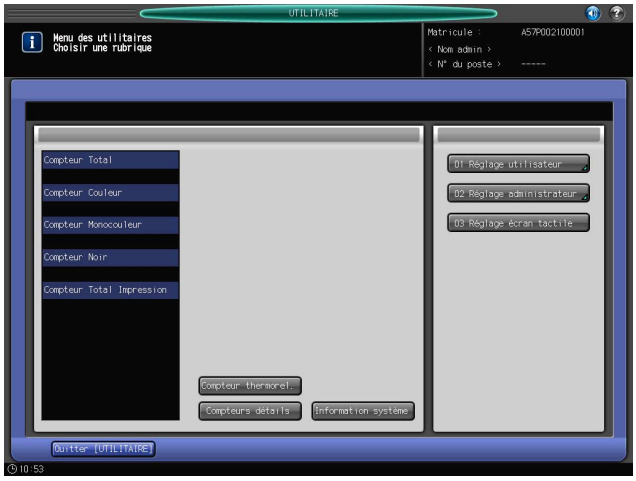
Pour protéger les données archivées sur la machine contre toute fuite ou altération, veillez à désigner un administrateur et activez la Sécurité renforcée. Activez la Sécurité renforcée et configurez un code verrouillage DD avant d'ajouter, de modifier ou de supprimer des utilisateurs enregistrés.

2.3.1 ACTIVER/DÉSACTIVER la Sécurité renforcée

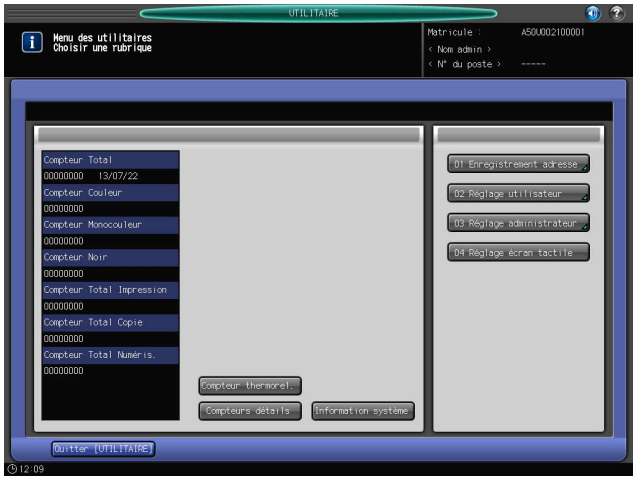
Cette section décrit comment ACTIVER/DÉSACTIVER la Sécurité renforcée.

1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

2 Appuyez sur [02 Réglage administrateur].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [03 Réglage administrateur].



L'écran Code administrateur s'affiche.

3 Entrez le code administrateur.

➔ Entrez le code administrateur composé de 8 caractères alphanumériques et symboles sur le clavier de l'écran tactile et appuyez sur [OK].

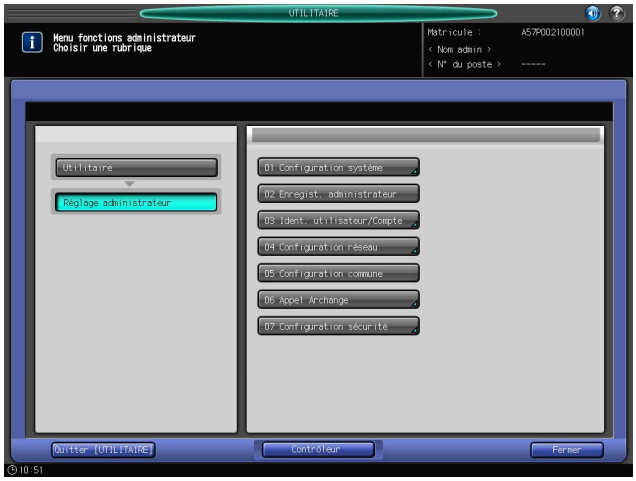
➔ Les caractères alphabétiques sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques/symboles et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

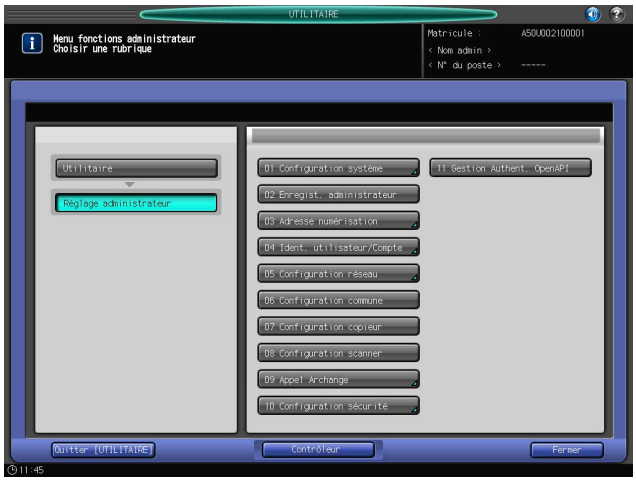
➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal d'événements.

L'écran du menu Réglage administrateur s'affiche.

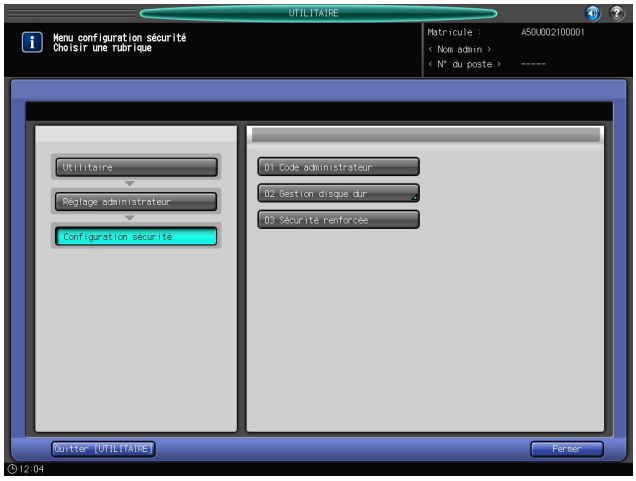
4 Appuyez sur [07 Configuration sécurité].



Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [10 Configuration sécurité].

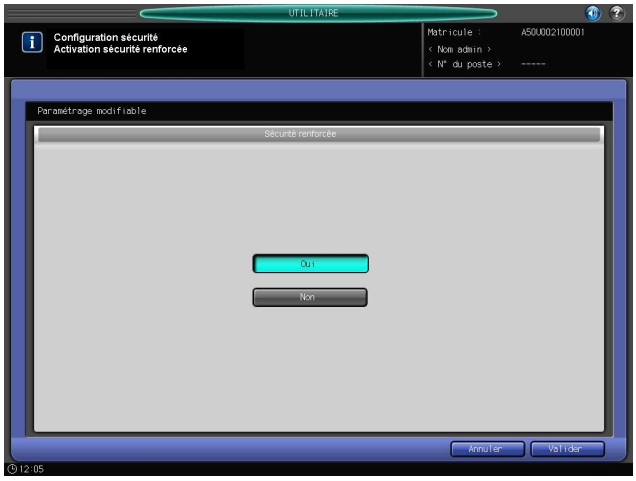


5 Appuyez sur [03 Sécurité renforcée].



6 ACTIVEZ/DÉSACTIVEZ la Sécurité renforcée.

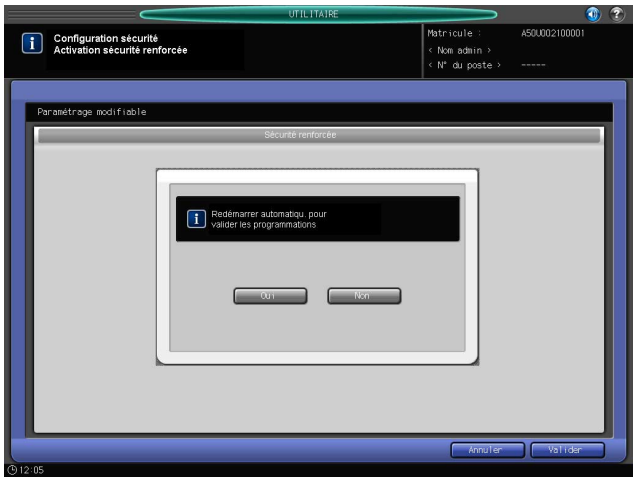
➔ Sélectionnez [Oui] pour activer la Sécurité renforcée ou sélectionnez [Non] pour la désactiver.

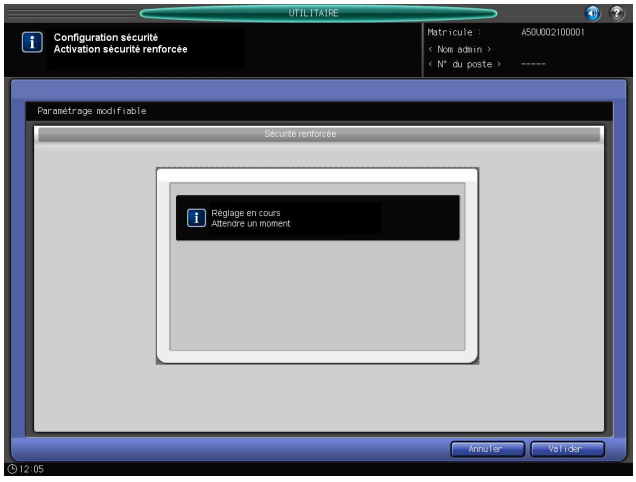


7 Appuyez sur [Valider].

➔ Une boîte de dialogue s'affiche pour vous demander de redémarrer.

➔ Appuyez sur [Oui].





8 La machine redémarre avec le nouveau réglage activé.

2.3.2 Code verrouillage DD

Quand la Sécurité renforcée est activée, vous pouvez spécifier un nouveau code de verrouillage (8 à 32 caractères alphanumériques, sensibles à la casse) en changeant le code de verrouillage par défaut initialement attribué au disque dur. Le fait de configurer un code de verrouillage va empêcher toute fuite des données de document en excluant tout disque dur connecté de manière illicite. Si quelqu'un essaie d'accéder au disque dur depuis l'extérieur, la lecture des données ne sera pas possible tant que le code de verrouillage correct n'est pas saisi.

REMARQUE

N'utilisez pas votre nom, votre date d'anniversaire, votre numéro d'employé, etc. pour un code que d'autres personnes peuvent facilement deviner.

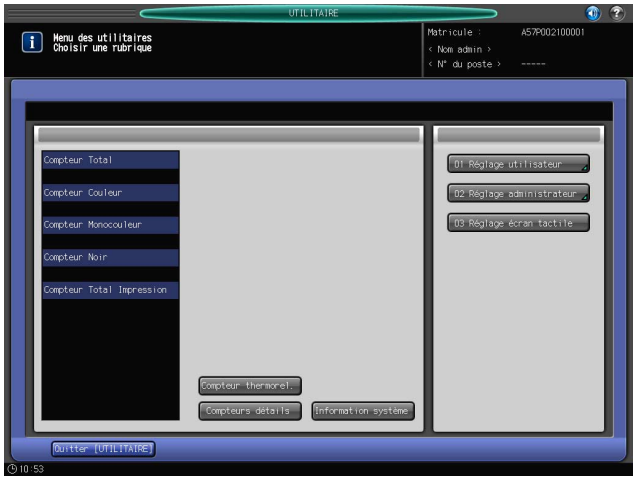
Veillez à n'informer personne de votre code et ne pas le divulguer à d'autres personnes.

1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

2 Appuyez sur [02 Réglage administrateur].

➔ Le code de verrouillage DD ne fonctionne que si la Sécurité renforcée est activée. Si la Sécurité renforcée est désactivée, le message [Veuillez définir réglage fonction de sécurité renforcée] s'affiche.

➔ Veillez à bien configurer un code de verrouillage DD en cas d'utilisation de la Sécurité renforcée.



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [03 Réglage administrateur].

L'écran Code administrateur s'affiche.

3 Entrez le code administrateur.

➔ Entrez le code administrateur composé de 8 caractères alphanumériques et symboles sur le clavier de l'écran tactile et appuyez sur [OK].

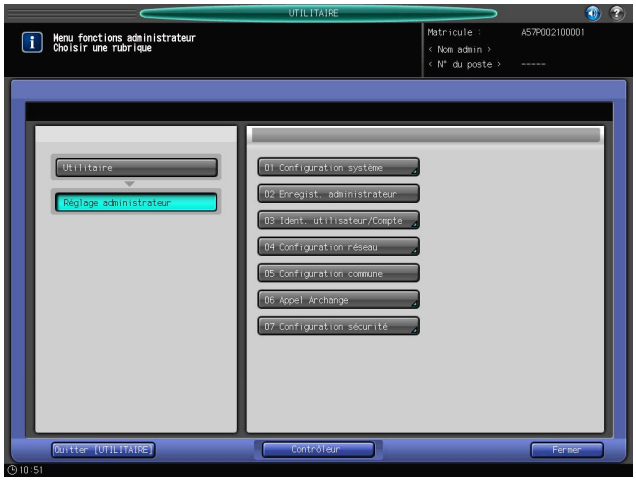
➔ Les caractères alphabétiques sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques/symboles et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

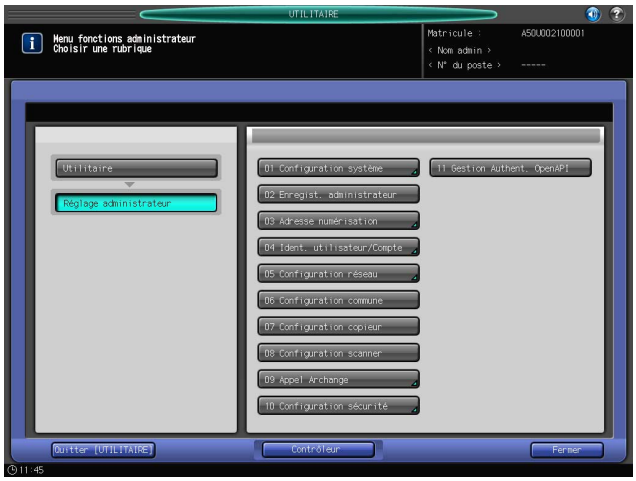
➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

L'écran du menu Réglage administrateur s'affiche.

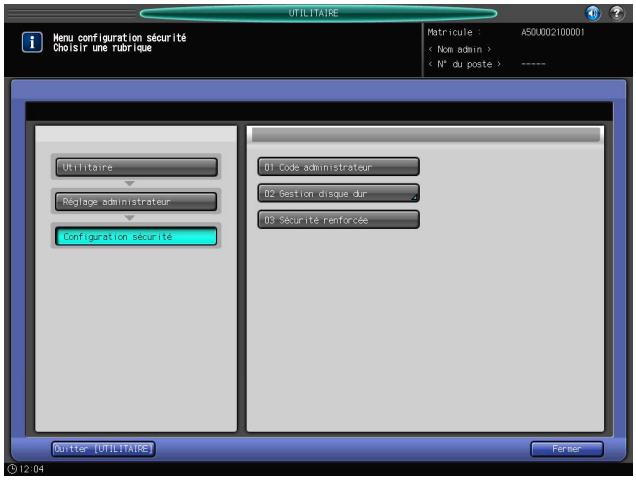
4 Appuyez sur [07 Configuration sécurité].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [10 Configuration sécurité].

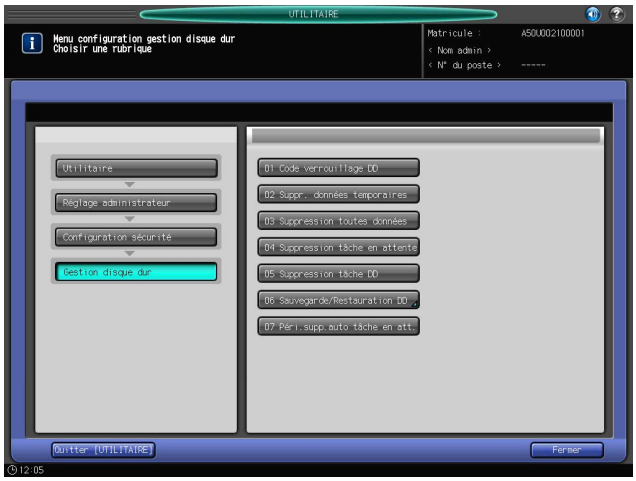


5 Appuyez sur [02 Gestion disque dur].



L'écran du menu Gestion disque dur s'affiche.

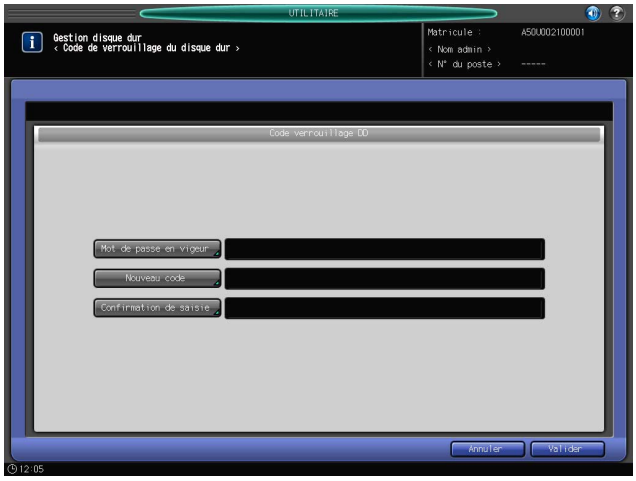
6 Appuyez sur [01 Code verrouillage DD].



L'écran Code verrouillage DD s'affiche.

7 Appuyez sur [Code actuel] pour entrer le code en vigueur, et appuyez sur [Valider].

Le mot de passe par défaut est le numéro de série de la machine composé de 13 caractères alphanumériques.



➔ Le numéro de série de la machine de 13 caractères alphanumériques s'affiche dans le coin supérieur gauche de l'écran du menu Utilitaire ou dans le coin supérieur droit du journal des événements imprimé. Pour des détails, voir page 2-25.

8 En cas de réussite de l'authentification, appuyez sur [Nouveau code] pour entrer un nouveau code.

REMARQUE

N'utilisez pas votre nom, votre date d'anniversaire, votre numéro d'employé, etc. pour un code que d'autres personnes peuvent facilement deviner.

➔ Le code de verrouillage DD peut comporter de 8 à 32 caractères alphanumériques.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

➔ Les informations relatives à la modification du code sont enregistrées dans le journal des événements.

➔ Le code actuel ne plus être réutilisé comme nouveau code.

➔ Appuyez sur [OK], une fois terminé.

9 Appuyez sur [Confirmation de saisie] pour saisir le même code que ci-dessus.

➔ Appuyez sur [OK], une fois terminé.

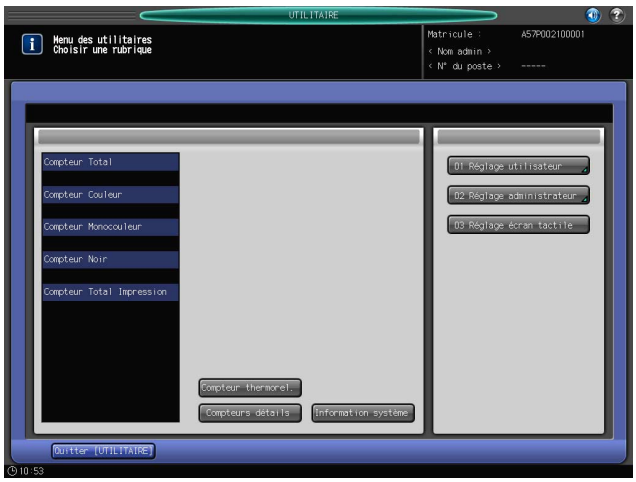
10 Appuyez sur [OK] sur l'écran Code verrouillage DD.

2.3.3 Suppression des données temporaires

Utilisez cette fonction pour sélectionner d'effacer ou non les données temporaires sur le disque dur ou dans la mémoire DRAM afin d'en empêcher toute réutilisation. Lors de l'effacement des données, sélectionnez aussi l'un des deux modes d'effacement indiqués à l'écran.

1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

2 Appuyez sur [02 Réglage administrateur].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [03 Réglage administrateur].

L'écran Code administrateur s'affiche.

3 Entrez le code administrateur.

➔ Entrez le code administrateur composé de 8 caractères alphanumériques et symboles sur le clavier de l'écran tactile et appuyez sur [OK].

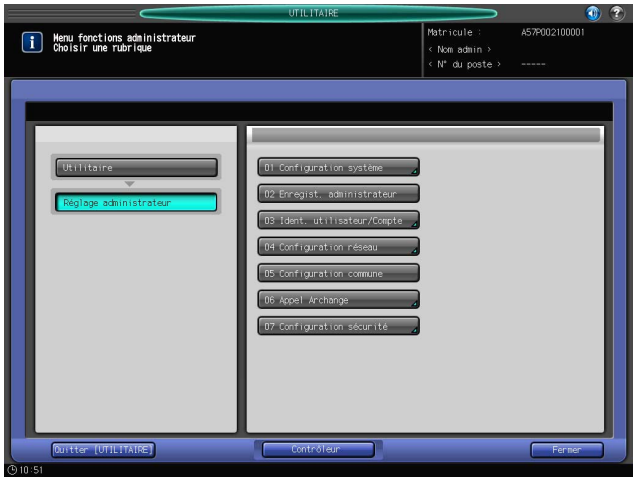
➔ Les caractères alphabétiques sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques/symboles et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

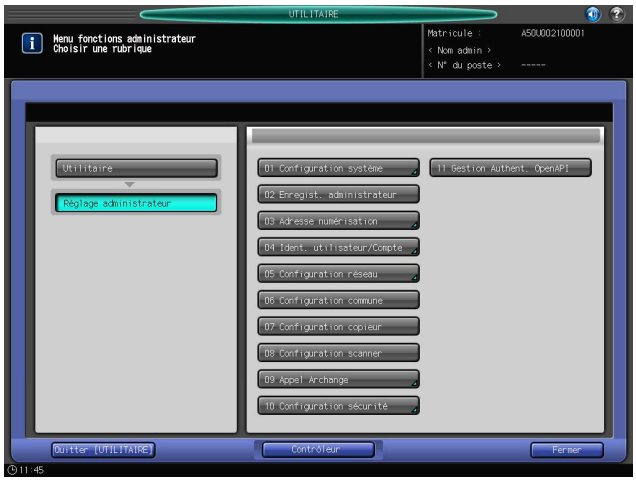
➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

L'écran du menu Réglage administrateur s'affiche.

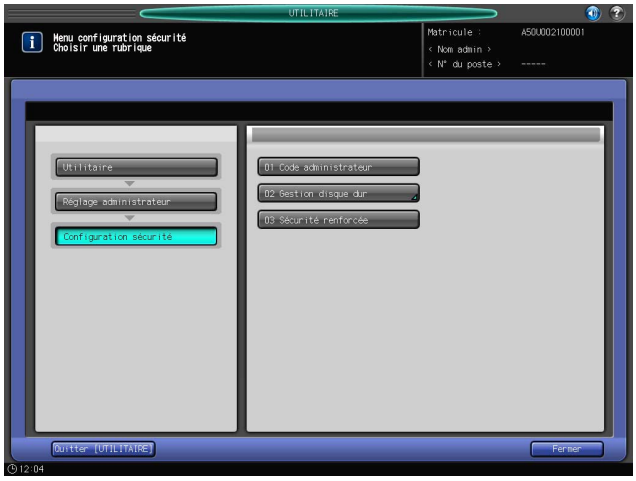
4 Appuyez sur [07 Configuration sécurité].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [10 Configuration sécurité].

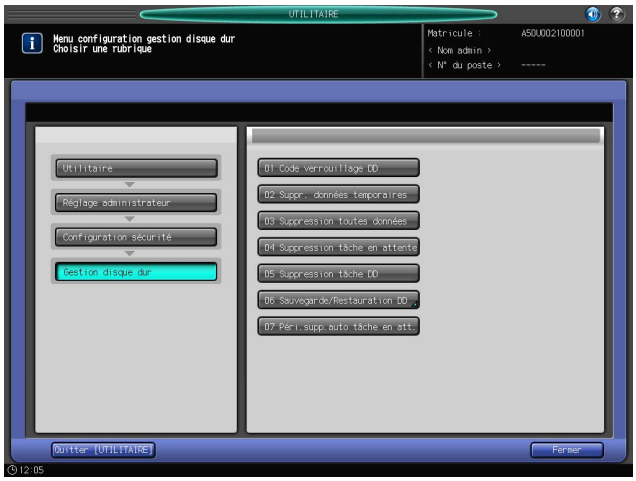


5 Appuyez sur [02 Gestion disque dur].



L'écran du menu Gestion disque dur s'affiche.

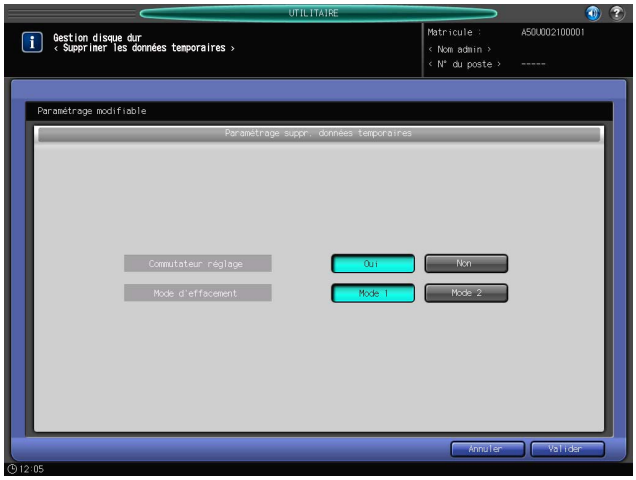
6 Appuyez sur [02 Suppr. données temporaires].



L'écran Paramétrage suppression données temporaires s'affiche.

7 Sélectionnez s'il faut ou non écraser les données temporaires.

➔ Pour écraser les données temporaires, appuyez sur [OUI]. Sinon, appuyez sur [NON].



8 Si vous choisissez d'écraser les données, sélectionnez le mode d'effacement souhaité.

➔ Appuyez sur [Mode 1] ou sur [Mode 2]. Pour des informations détaillées sur la configuration et l'utilisation des modes d'effacement, consultez le Guide de l'utilisateur HTML.

➔ Si vous choisissez de ne pas écraser les données, la sélection du mode ne change rien.

9 Appuyez sur [OK] sur l'écran Paramétrage suppr. données temporaires.

10 Mettez l'**interrupteur secondaire** sur ARRÊT, puis l'**interrupteur principal** sur ARRÊT.

➔ N'actionnez pas l'interrupteur principal quand le message [Refroidissement en cours/Extinction automatique après refroidissement] est affiché.

11 Patientez plus de 10 secondes.

12 Mettez l'**interrupteur principal** et l'**interrupteur secondaire** sur ON (Marche).

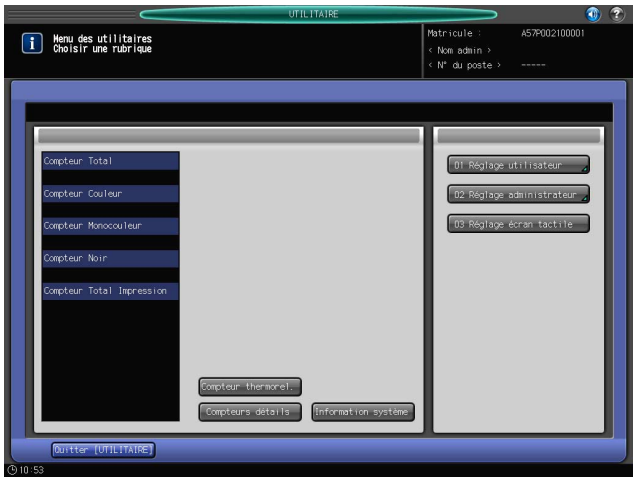
2.3.4 Suppression de toutes les données

Vous pouvez choisir de supprimer toutes les données de document archivées sur le disque dur. Si vous choisissez de supprimer toutes les données, sélectionnez l'un des 8 modes proposés.

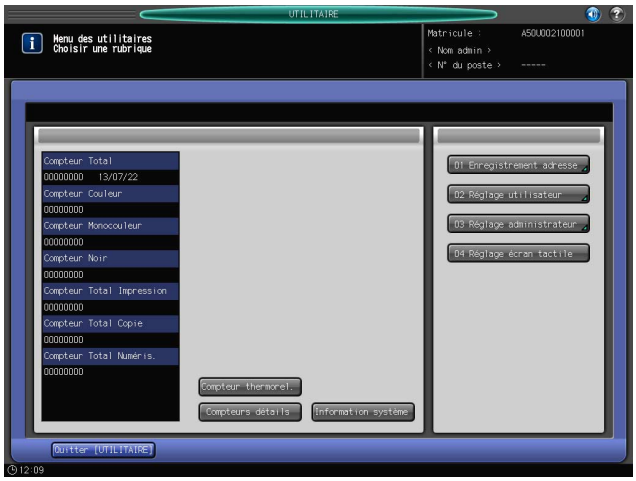
1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

➔ Pour utiliser cette fonction de suppression de toutes les données, contactez votre technicien S.A.V.

2 Appuyez sur [02 Réglage administrateur].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [03 Réglage administrateur].



L'écran Code administrateur s'affiche.

3 Entrez le code administrateur.

➔ Entrez le code administrateur composé de 8 caractères alphanumériques et symboles sur le clavier de l'écran tactile et appuyez sur [OK].

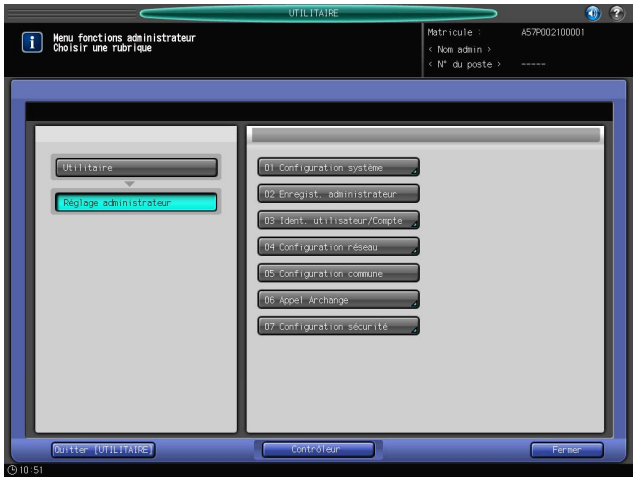
➔ Les caractères alphabétiques sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques/symboles et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

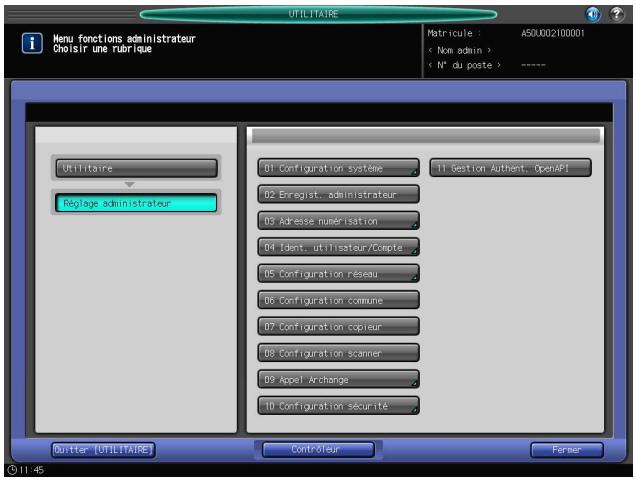
➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

L'écran du menu Réglage administrateur s'affiche.

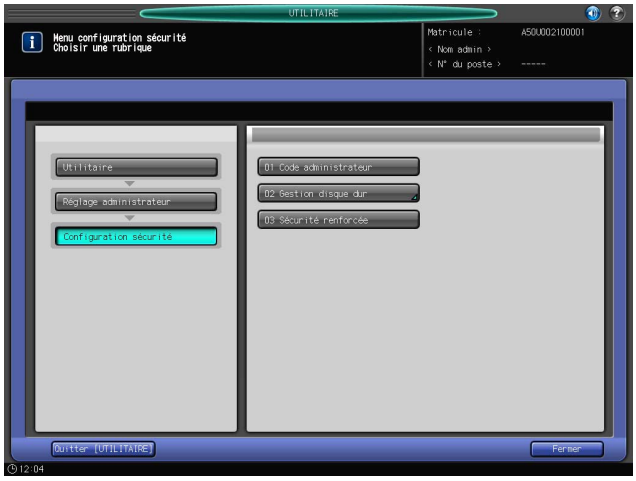
4 Appuyez sur [07 Configuration sécurité].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [10 Configuration sécurité].

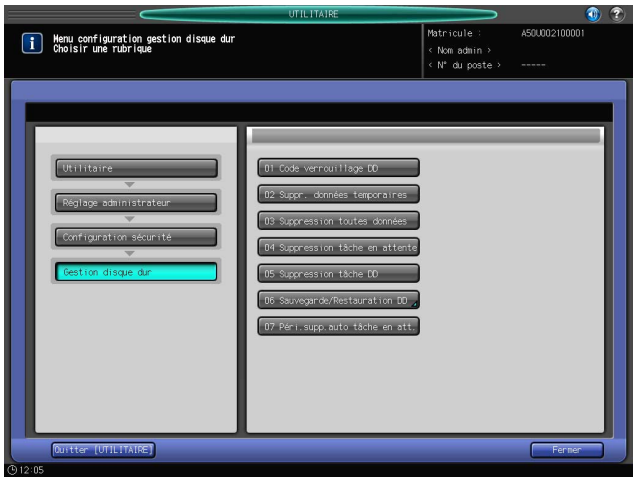


5 Appuyez sur [02 Gestion disque dur].



L'écran du menu Gestion disque dur s'affiche.

6 Appuyez sur [03 Suppression toutes données].



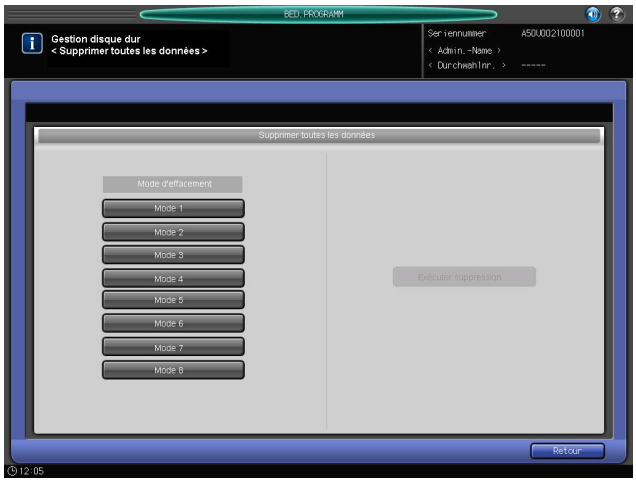
L'écran Paramétrage suppression données temporaires s'affiche.

7 Sélectionnez le mode d'effacement souhaité et appuyez sur [Exécuter suppression].

➔ Pour des informations détaillées sur la configuration et l'utilisation des modes d'effacement, consultez le Guide de l'utilisateur HTML.

REMARQUE

Si vous supprimez des données avec la touche [Exécuter suppression], aucune donnée du disque dur ne pourra être réutilisée. Toutes les données nécessaires devraient être transférées vers un autre périphérique avant de poursuivre.



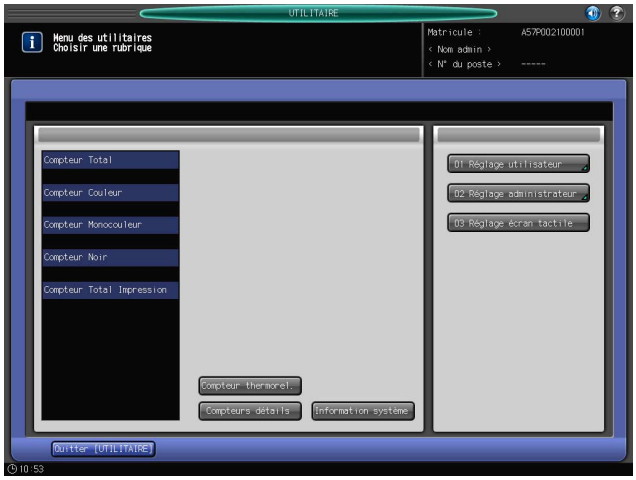
8 Appuyez sur [Retour] sur l'écran Suppression toutes données.

2.3.5 Sortie du journal des événements

Un journal des événements est automatiquement créé en cas d'accès aux données sauvegardées sur la machine. Toutes les données du journal des événements peuvent être sorties comme suit.

1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

2 Appuyez sur [02 Réglage administrateur].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [03 Réglage administrateur].

Un écran de saisie du code s'affiche.

3 Entrez le code administrateur.

➔ Entrez le code administrateur composé de 8 caractères alphanumériques et symboles sur le clavier de l'écran tactile et appuyez sur [OK].

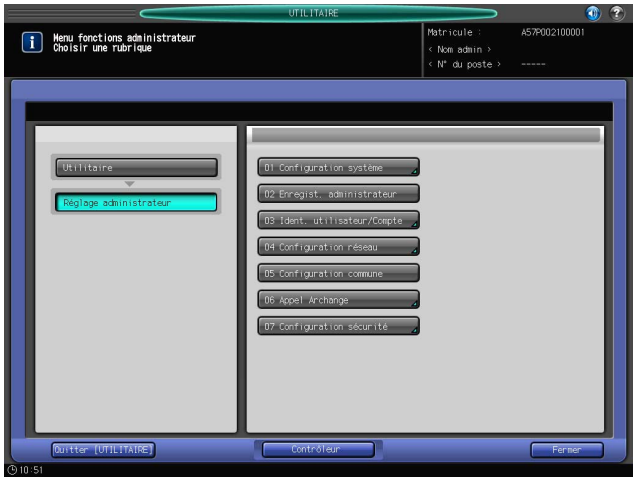
➔ Les caractères alphabétiques sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

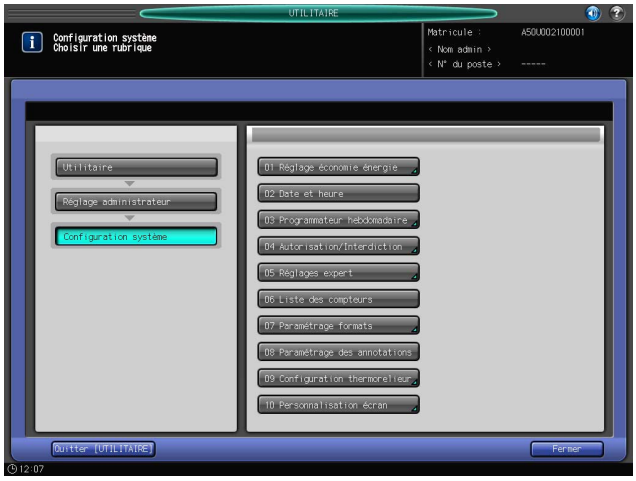
➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

L'écran du menu Réglage administrateur s'affiche.

4 Appuyez sur [01 Configuration système].

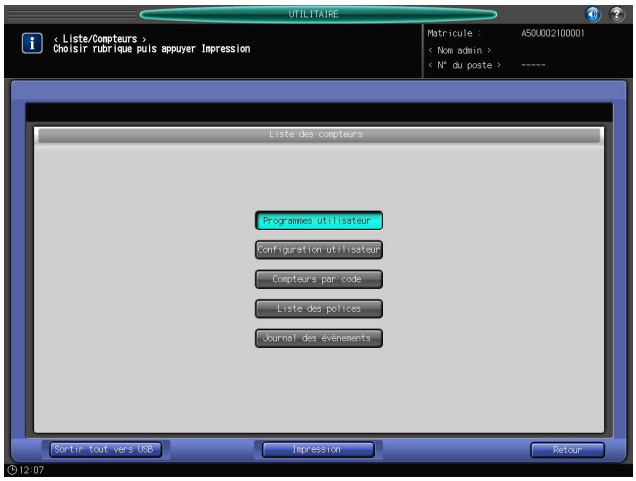


5 Appuyez sur [06 Liste des compteurs].



L'écran Liste des compteurs s'affiche.

6 Sélectionnez [Journal des événements], puis appuyez sur [Mode d'impression].



7 Imprimez le journal.

➔ Appuyez sur **Départ** sur le **panneau de contrôle**.

➔ Pour arrêter l'impression, appuyez sur **Arrêt** sur le **panneau de contrôle**. Une boîte de dialogue de confirmation s'affiche. Appuyez sur [Annuler tâche] pour annuler la tâche de sortie.

➔ Une fois que la tâche de sortie est terminée, appuyez sur [Fermer].

2.3.6 Journal des événements

L'administrateur doit analyser le journal des événements régulièrement (une fois par mois) ou en cas d'accès illicite aux données sauvegardées dans la machine ou en cas d'altération de celles-ci.

La machine est censée archiver plus de 750 journaux par mois. Si plus de 750 journaux sont censés être archivés tous les mois, procédez à l'analyse plus fréquemment avant les journaux non analysés n'atteignent ce nombre.

Audit log report

P.1
10/01/2013 13:44
A50U011901002
TC:2712

No	date/time	id	action	result	No	date/time	id	action	result
0001	2012/10/13 11:23	-1	16	OK	0002	2012/10/13 11:23	-1	15	OK
0003	2012/10/13 11:21	-1	15	OK	0004	2012/10/13 11:20	-1	15	OK
0005	2012/10/13 11:16	-2	03	OK	0006	2012/10/13 11:16	-2	02	OK
0007	2012/10/13 11:15	-2	02	NG	0008	2012/10/13 11:15	-3	11	NG
0009	2012/10/13 11:14	-3	11	NG	0010	2012/10/13 11:14	-3	11	NG
0011	2012/10/13 10:56	2	11	OK	0012	2012/10/13 10:54	-2	02	OK
0013	2012/10/13 10:54	2	07	OK	0014	2012/10/13 10:53	-2	02	OK
0015	2012/10/13 10:53	-3	11	NG	0016	2012/10/13 10:52	-3	11	NG
0017	2012/10/13 10:51	1	11	OK	0018	2012/10/13 10:51	-3	11	NG
0019	2012/10/13 10:50	1	11	OK	0020	2012/10/13 10:50	-3	11	NG
0021	2012/10/13 10:49	-3	11	NG	0022	2012/10/13 10:49	1	11	OK
0023	2012/10/13 10:43	1	07	OK	0024	2012/10/13 10:43	-2	02	OK
0025	2012/10/13 10:42	-2	02	OK	0026	2012/10/13 10:40	-2	03	OK
0027	2012/10/10 13:33	-1	16	OK	0028	2012/10/05 21:02	-1	15	OK

Informations du journal des événements

Le journal des événements contient les informations suivantes :

1. date/heure : enregistre la date et l'heure de l'opération ayant déclenché la création d'une entrée de journal.

2. id : identifie la personne ayant effectué l'opération ou un sujet pour la protection de sécurité.

- -1 : opération par l'ingénieur support client (CE)
- -2 : opération par l'administrateur
- -3 : opération par l'utilisateur non enregistré
- Autre entier : indique des sujets pour la protection de sécurité et les ID d'action suivants réduisant le sujet pour la protection. ID utilisateur : nombres de 1 à 1000. ID utilisateur sécurisé : nombres de 1 à 99999.

3. action : indique un numéro spécifiant l'opération. Pour des détails, consultez le tableau suivant.

4. résultat : enregistre le résultat de l'opération. Pour l'authentification du mot de passe, le succès/l'échec est indiqué par OK/NG. Pour les opérations sans authentification du mot de passe, toutes les entrées du journal sont indiquées comme étant OK.

Tableau des éléments enregistrés dans le journal des événements

N°	Opération	ID du journal	Action enregistrée	Résultat
1	CE Authentification	ID CE	01	OK/NG
2	Authentification de l'administrateur	ID administrateur	02	OK/NG
3	Définir/Changer la Sécurité renforcée	ID administrateur	03	OK
4	Imprimer journal des événements/Sortir tout vers USB	ID CE/ID administrateur	04	OK
5	Changer/enregistrer mot de passe CE	ID CE	05	OK
6	Changer/enregistrer le code de l'administrateur	ID CE/ID administrateur	06	OK
7	Créer utilisateur par l'administrateur	ID utilisateur	07	OK
8	Changer/enregistrer mot de passe de l'utilisateur par l'administrateur	ID utilisateur	08	OK
9	Supprimer utilisateur par l'administrateur	ID utilisateur	09	OK
10	Changer l'attribut utilisateur par l'administrateur	ID utilisateur	10	OK
11	Authentification du mot de passe pour l'utilisateur	ID utilisateur[*1]/ID utilisateur non enregistré[*2]	11	OK/NG
12	Changer les attributs de l'utilisateur par l'utilisateur (mot de passe utilisateur, etc.)	ID utilisateur	12	OK
13	(non utilisé)			
14	(non utilisé)			
15	Accès à une tâche archivée (Impression en attente/Tâche Enreg. DD, rappel d'une tâche Enreg. DD pour mettre tâche en attente, enregistrement de la tâche en attente sur le DD)	ID utilisateur	15	OK
16	Supprimer tâche enregistrée	ID utilisateur	16	OK
17	(non utilisé)			
18	(non utilisé)			
19	Modifier code protection DD	ID administrateur	19	OK
20	Réglage date/heure	ID utilisateur	20	OK

[*1] : ID du journal des événements est enregistré comme ID utilisateur quant l'authentification de l'utilisateur a réussi ou en présence d'une non concordance du mot de passe avec un nom d'utilisateur enregistré.

[*2] : l'ID du journal des événements est enregistré en tant qu'ID utilisateur non enregistré en cas d'échec de l'authentification avec un nom d'utilisateur non enregistré.

L'analyse du journal des événements a pour objet de comprendre les points suivants et à prendre des contremesures :

- Si quelqu'un a accédé ou non aux données ou si elles ont été altérées
- Cibles d'une attaque
- Détails de l'attaque
- Résultat de l'attaque

Pour les méthodes d'analyse spécifiques, consultez la description suivante.

Spécification d'actions non autorisées : authentification du mot de passe

Si des journaux affichent NG comme résultat de l'authentification du mot de passe (action : 01, 02, 11), il se peut que les éléments protégés par des mots de passe aient été attaqués.

- Les entrées de journal d'échec de l'authentification du mot de passe (NG) indiquent qui a effectué l'opération et montrent si des actions non autorisées ont été effectuées lors de l'échec de l'authentification du mot de passe.
- Même en cas de succès de l'authentification du mot de passe (OK), il vous faut peut-être vérifier si c'est un utilisateur légitime qui a créé l'action. Une vérification minutieuse est recommandée plus particulièrement quand l'authentification réussit après une série d'échecs ou pour les tentatives effectuées en dehors des heures de travail normales.

Spécification d'actions non autorisées : autres que l'authentification du mot de passe

Puisque tous les résultats d'opération autres que l'authentification du mot de passe sont indiquées comme étant (OK), utilisez l'ID et essayez de déterminer si des actions non autorisées ont été effectuées.

- Puisqu'un simple ID ne vous permet pas d'identifier ce qui a fait l'objet de l'attaque, vous devez consulter le tableau de correspondance des actions à la page précédente pour déterminer si des actions non autorisées ont été effectuées sur une boîte privée ou une boîte sécurisée.
- Vérifiez l'heure de l'opération et cherchez à savoir si l'utilisateur responsable de l'opération a procédé à des actions non autorisées.

Par exemple :

si un document enregistré dans une boîte est imprimé avec une authentification frauduleuse, l'entrée du journal des événements suivante sera créée.

1. Authentification du mot de passe pour la boîte :

action = 11

id = boîte pour laquelle l'authentification a été effectuée

résultat = OK/NG

2. Accès au document dans la boîte :

action = 13

id = boîte pour laquelle l'authentification a été effectuée

Vérifiez la date et l'heure de l'opération et cherchez à savoir si l'utilisateur étant intervenu sur des documents dans la boîte privée/sécurisée spécifique était un propriétaire légitime de la boîte.

Solution en cas d'opérations non autorisées

Si vous découvrez une fuite de mot de passe après avoir analysé le journal des événements, changez immédiatement le mot de passe.

- Il se peut que l'utilisateur légitime ne puisse pas accéder à la boîte parce que le mot de passe a été modifié de manière frauduleuse. L'administrateur doit contacter l'utilisateur pour confirmer la situation et si c'est le cas, elle/il doit traiter le problème soit en changeant le mot de passe ou en supprimant les données archivées.
- Si un document archivé reste introuvable ou si son contenu est altéré, il se peut que des actions non autorisées aient été effectuées. Si tel est le cas, des contre-mesures similaires doivent être appliquées.

Problèmes possibles lors du transfert de toutes les données du journal des événements vers un lecteur flash USB

Si la machine ne peut pas reconnaître le lecteur flash USB, le message [Connexion de la clé USB n'a pas été reconnue] s'affichera pour indiquer une indisponibilité de la sortie par lots.

Si vous recevez des erreurs telles qu'un échec d'écriture ou de manque de capacité du lecteur flash USB pendant la tâche de sortie, le message [Erreur de téléchargement] va s'afficher et la sortie par lors sera suspendue.

2.4 Authentification utilisateur en mode Sécurité renforcée

Quand la Sécurité renforcée est activée, les fonctions liées à l'authentification des utilisateurs sont renforcées comme suit.

- L'option de réglage "Authent. utilisateur" à l'écran et accessible depuis [02 Réglage administrateur] - [03 Ident. utilisateur/Compte] - [01 Méthode authentification] est automatiquement réglée sur [ON (MFP)].
- Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, l'option de réglage "Authent. utilisateur" à l'écran et accessible depuis [03 Réglage administrateur] - [04 Ident. utilisateur/Compte] - [01 Méthode authentification] est automatiquement réglée sur [ON (MFP)].
- Une authentification utilisateur est toujours requise dans les conditions suivantes pour exploiter les données utilisateur à protéger :

- Onglet [LISTE TRAVAUX] et [Retenir Tâche] sont actionnés.
- Onglet [RAPPEL DD] est actionné.
- Onglet [COPIE] est actionné.
- Onglet [NUMÉRISATION] est actionné.

- Le mot de passe pour l'authentification utilisateur (mot de passe utilisateur) doit comporter de 8 à 64 caractères alphanumériques (les caractères alphabétiques étant sensibles à la casse). Sinon, le mot de passe devient indisponible. Pour continuer à utiliser le nom d'utilisateur avec un mot de passe comportant moins de 8 caractères, l'administrateur devrait changer le mot de passe pour qu'il comporte au moins 8 caractères.
- En cas de saisie d'un nom d'utilisateur/mot de passe (ou nom de compte/mot de passe) incorrect pour l'authentification, aucune tentative pour réessayer n'est possible pendant 5 secondes.
- Avec la Sécurité renforcée activée, la machine rejette l'authentification de l'utilisateur avec une carte IC.

Quand un utilisateur accède à un fichier avec un mot de passe spécifié, les opérations d'authentification du mot de passe sont enregistrées sous forme de journaux d'événements.

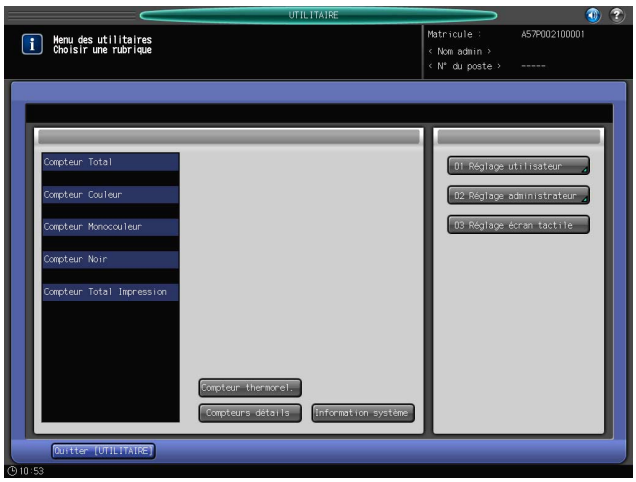
Au départ, l'authentification utilisateur n'est pas disponible. Lors de l'activation de l'authentification utilisateur, vous devriez changer le nombre de comptes à distribuer en fonction de vos besoins. Pour des informations détaillées sur l'activation et l'utilisation de l'authentification utilisateur, consultez le guide de l'utilisateur HTML.

2.4.1 Ajouter un enregistrement utilisateur

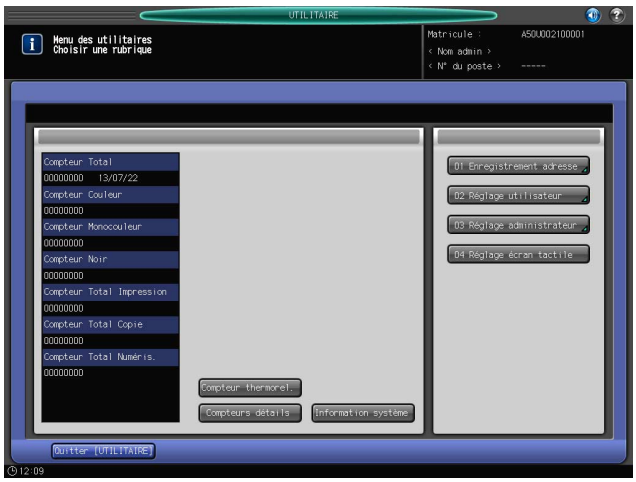
Suivez la procédure pour configurer un nouveau nom d'utilisateur et mot de passe requis pour l'authentification utilisateur en mode Sécurité renforcée.

1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

2 Appuyez sur [02 Réglage administrateur].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [03 Réglage administrateur].



L'écran Code administrateur s'affiche.

3 Entrez le code administrateur.

Entrez le code administrateur composé de 8 caractères alphanumériques et symboles sur le clavier de l'écran tactile et appuyez sur [OK].

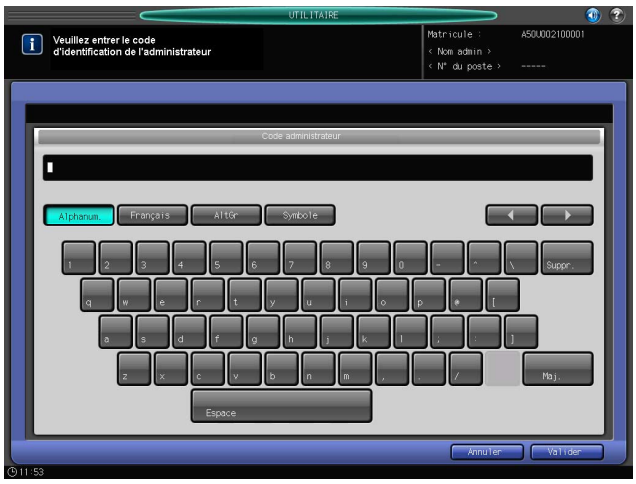
➔ Les mots de passe sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques/symboles et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

➔ Le mot de passe utilisé le plus récemment ne peut pas être configuré.

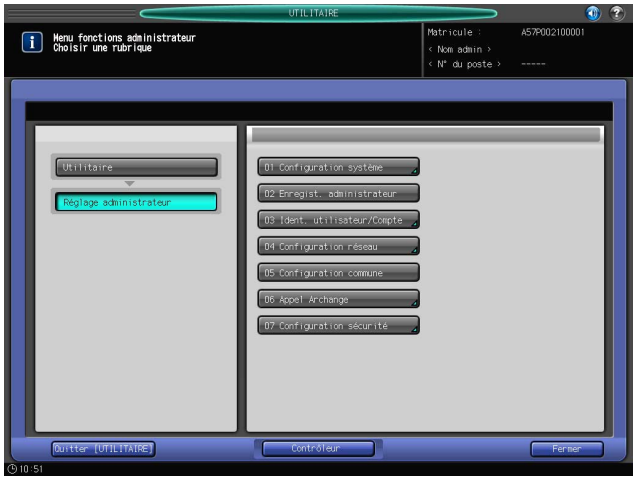
➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

➔ Le nombre de caractères saisi est affiché à l'écran par le même nombre d'astérisques "*".

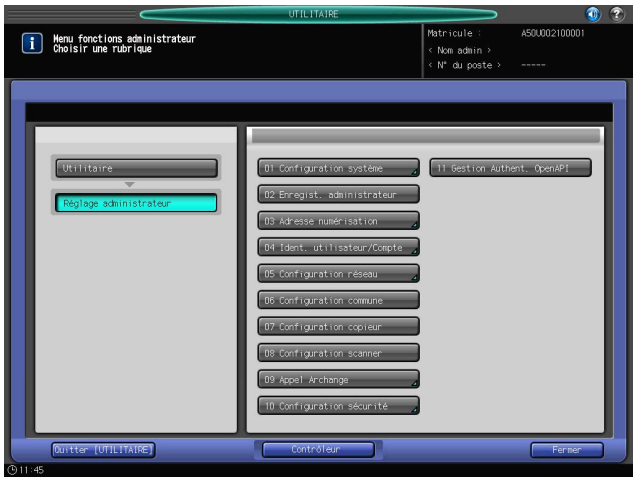


L'écran du menu Réglage administrateur s'affiche.

4 Appuyez sur [03 Ident. utilisateur/Compte].

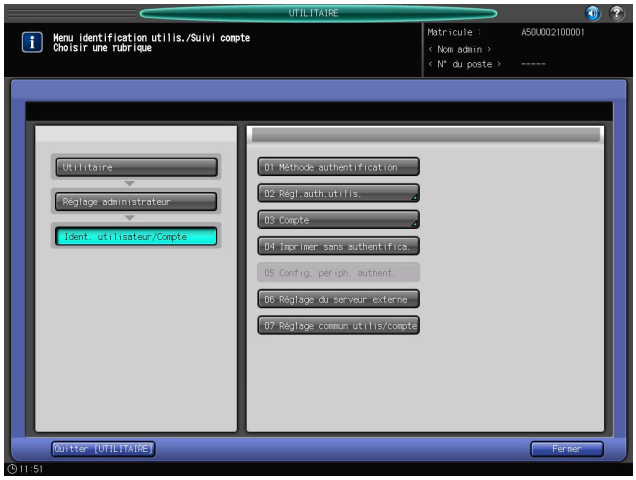


➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [04 Ident. utilisateur/Compte].



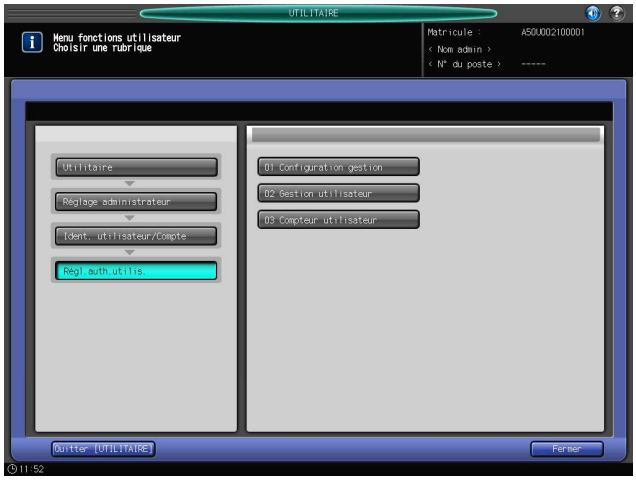
L'écran du menu Ident. utilisateur/Compte s'affiche.

5 Appuyez sur [02 Régl.auth.utilis.].



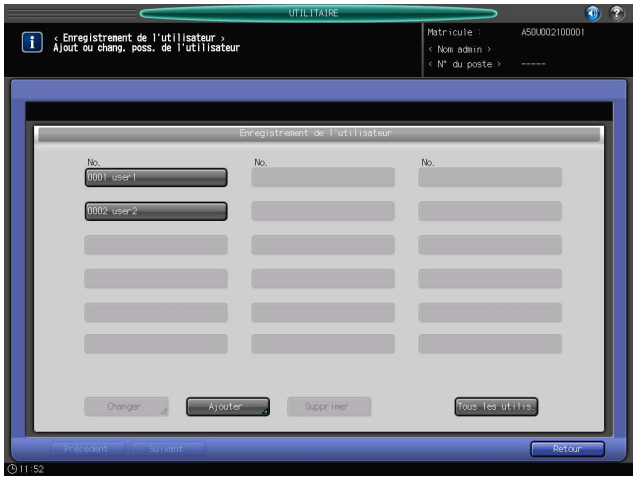
L'écran du menu Régl.auth.utilis s'affiche.

6 Appuyez sur [02 Gestion utilisateur].



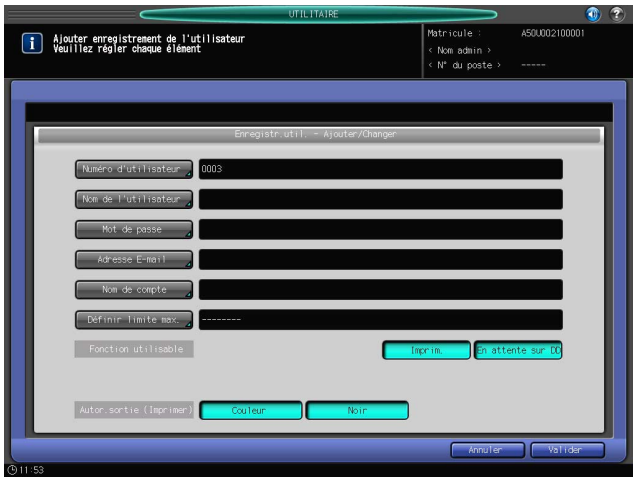
L'écran Enregistrement utilisateur s'affiche.

7 Appuyez sur [Ajouter].



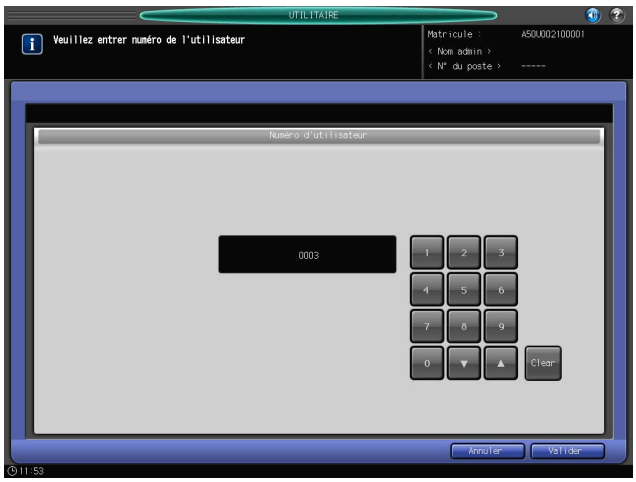
L'écran Enregistr.util. - Ajouter/Changer s'affiche.

8 Appuyez sur [N° utilisateur].



Utilisez le clavier de l'écran tactile, [▼], ou [▲] pour saisir le numéro d'utilisateur souhaité.

➔ Vous pouvez utiliser 1 à 1000 pour le numéro d'utilisateur.



Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

9 Appuyez sur [Nom Utilis].

L'écran Enregistrement utilisateur s'affiche. Entrez le nom d'utilisateur souhaité.

➔ Le nom d'utilisateur peut comporter jusqu'à 64 caractères alphanumériques, symboles compris. Le nom d'utilisateur ne peut pas être saisi en double.

Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

10 Appuyez sur [Mot de passe].

L'écran Mot de passe s'affiche. Entrez un mot de passe pour le nom d'utilisateur saisi à l'étape 9.

➔ Entrez 8 à 64 caractères alphanumériques pour le mot de passe utilisateur (les caractères alphabétiques étant sensibles à la casse).

REMARQUE

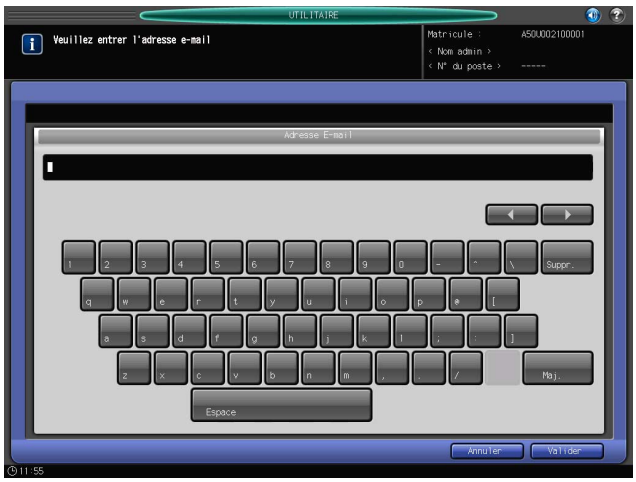
Veillez à bien saisir 8 caractères alphanumériques ou plus pour le mot de passe. Un mot de passe de moins de 8 caractères ne peut pas être utilisé quand la Sécurité renforcée est activée.

Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

11 Appuyez sur [Adresse E-mail].

L'écran Adresse E-mail s'affiche.

➔ L'adresse e-mail peut comporter jusqu'à 320 caractères alphanumériques et symboles.



Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

12 Appuyez sur [Nom de compte].

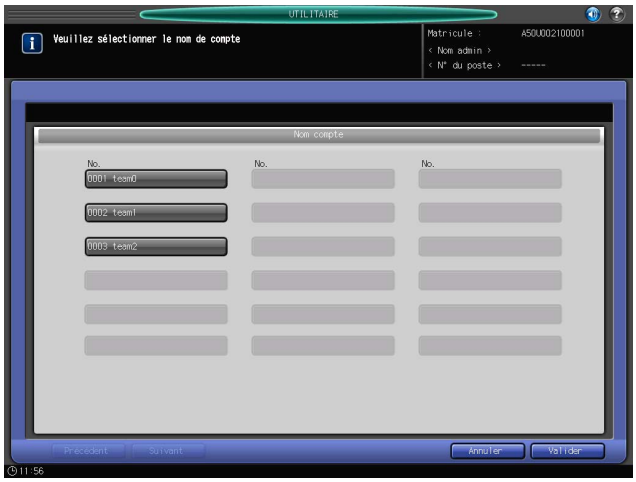
L'écran Nom de compte s'affiche. Sélectionnez le compte souhaité.

REMARQUE

Si [Synchroniser Utilisateur/Gestion compte] de Méthode d'authentification est réglé sur [Synchroniser], vous pouvez configurer [Nom de compte].

REMARQUE

Le compte doit être enregistré au préalable. Sélectionnez l'un des comptes enregistrés et affichés à l'écran.

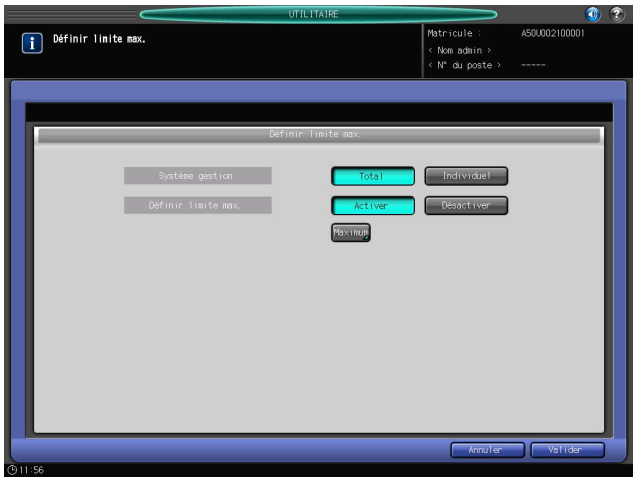


Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

13 Appuyez sur [Définir limite max.].

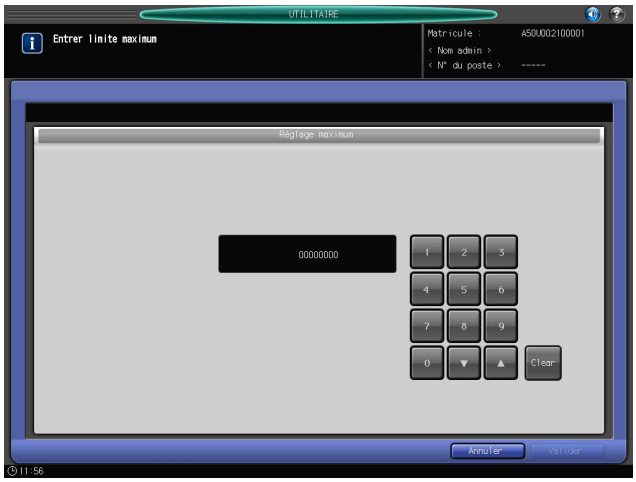
➔ Spécifiez le nombre maximal d'impressions autorisées pour l'utilisateur après une authentification réussie.

➔ Appuyez sur [Total] sur la droite de "Système gestion", [Activer] à droite de "Définir limite max." et [Maximum].



➔ Utilisez le clavier de l'écran tactile, [▼], ou [▲] pour saisir le nombre d'impressions autorisées. La plage disponible pour la limite max. est comprise entre 0 et 99 999 999.

➔ Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.



➔ La limite autorisée pour les impressions en couleur et en noir peut être spécifiée séparément.

➔ Appuyez sur [Individuel] sur la droite de "Système gestion", [Activer] à droite de "Définir limite max." et [Maximum].

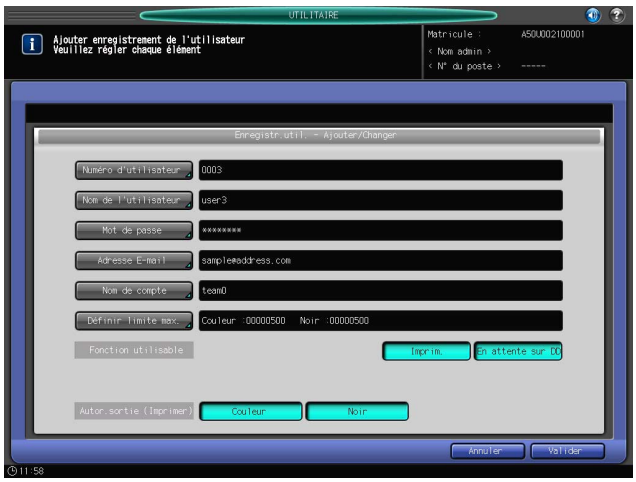
➔ Utilisez le clavier de l'écran tactile, [▼], ou [▲] pour saisir le nombre d'impressions autorisées. La plage disponible pour la limite max. est comprise entre 0 et 99 999 999.

Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

14 Appuyez sur [Imprim.] ou sur [En attente sur DD] à droite de "Fonction utilisable" pour sélectionner des fonctions de la machine disponibles pour l'utilisateur.

➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [Copier], [Numéris.], [Imprim.] ou sur [En attente sur DD] à droite de "Fonction utilisable".

15 Appuyez sur [Couleur] ou sur [Noir] à droite de "Autorisé sortie (Impression)" pour sélectionner le type d'impression accessible à l'utilisateur.



16 Appuyez sur [Valider].

➔ Quand les réglages sont terminés, appuyez sur [Retour] sur l'écran Enregistrement utilisateur.

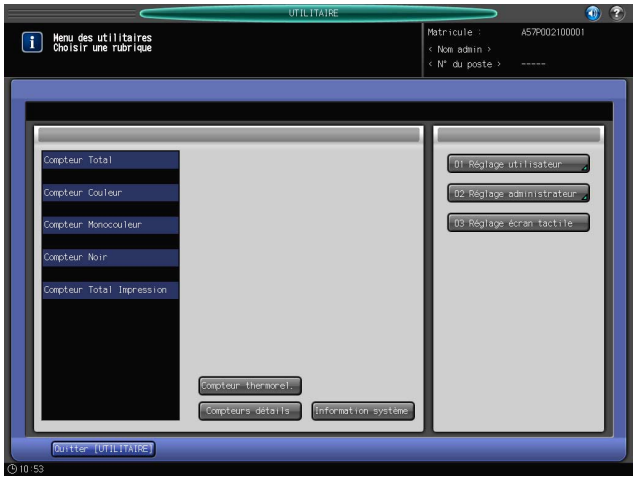
L'écran du menu Régl.auth.utilis. est restauré.

2.4.2 Changer un enregistrement utilisateur

Suivez la procédure pour changer le nom d'utilisateur et le mot de passe requis pour l'authentification utilisateur en mode Sécurité renforcée.

1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

2 Appuyez sur [02 Réglage administrateur].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [03 Réglage administrateur].

L'écran Code administrateur s'affiche.

3 Entrez le code administrateur.

Entrez le code administrateur composé de 8 caractères alphanumériques et symboles sur le clavier de l'écran tactile et appuyez sur [OK].

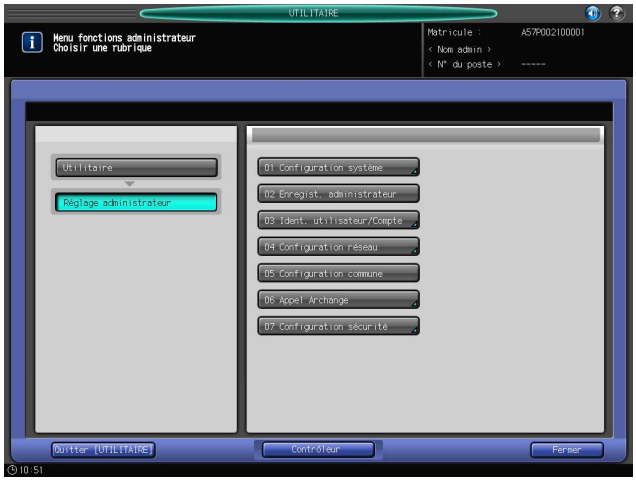
➔ Les caractères alphabétiques sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

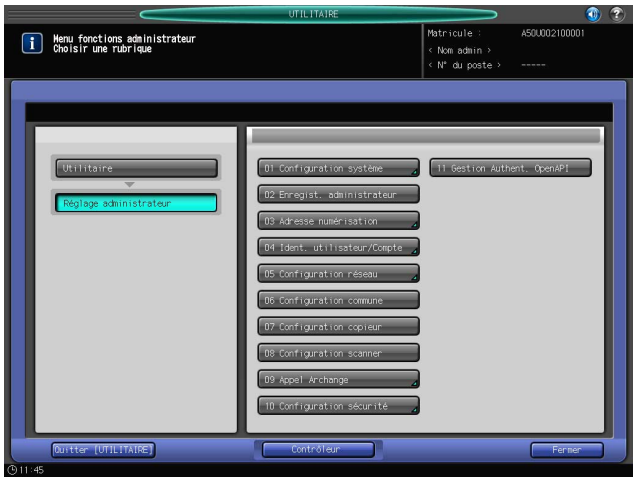
➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

L'écran du menu Réglage administrateur s'affiche.

4 Appuyez sur [03 Ident. utilisateur/Compte].

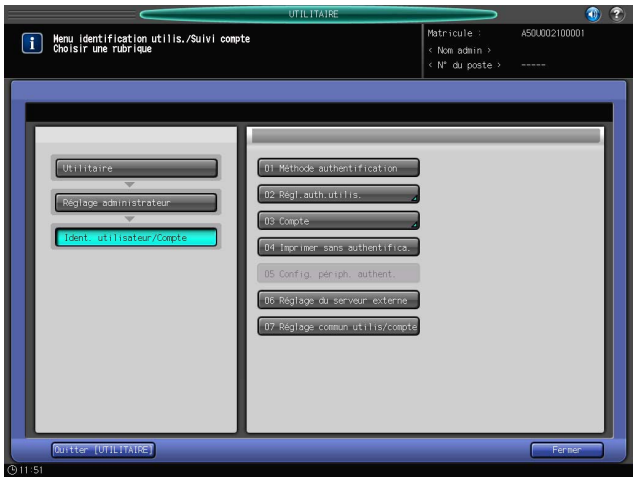


➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [04 Ident. utilisateur/Compte].



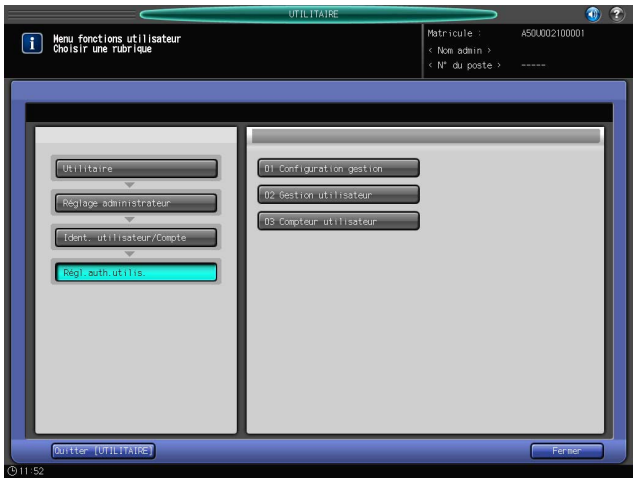
L'écran du menu Ident. utilisateur/Compte s'affiche.

5 Appuyez sur [02 Régl.auth.utilis.].



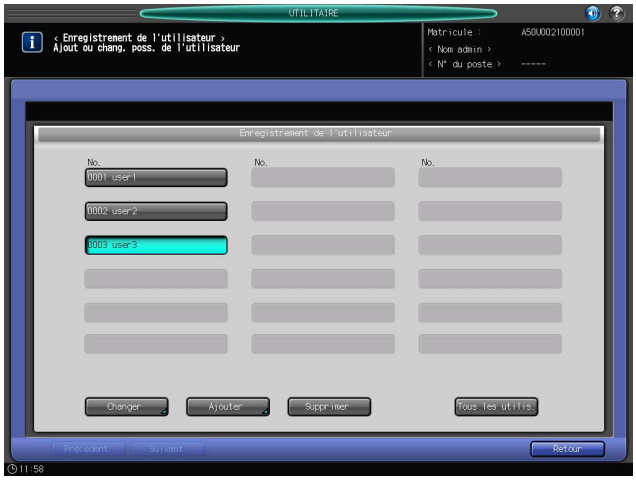
L'écran du menu Régl.auth.utilis s'affiche.

6 Appuyez sur [02 Gestion utilisateur].



L'écran Enregistrement utilisateur s'affiche.

7 Sélectionnez la touche avec le numéro d'utilisateur et le nom d'utilisateur à changer.



8 Appuyez sur [Changer] pour afficher l'écran Enregistr.util. - Ajouter/Changer.

➔ Le numéro de l'utilisateur ne peut pas être modifié.

9 Pour changer le nom de l'utilisateur, appuyez sur [Nom utilisateur].

10 Entrez un nouveau nom d'utilisateur.

➔ Le nom d'utilisateur peut comporter jusqu'à 64 caractères alphanumériques, symboles compris. Le nom d'utilisateur ne peut pas être saisi en double.

Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

11 Pour changer le mot de passe, appuyez sur [Mot de passe].

➔ L'écran Mot de passe s'affiche. Entrez un nouveau mot de passe pour le nom d'utilisateur saisi à l'étape 9.

➔ Entrez 8 à 64 caractères alphanumériques pour le mot de passe utilisateur (les caractères alphabétiques étant sensibles à la casse).

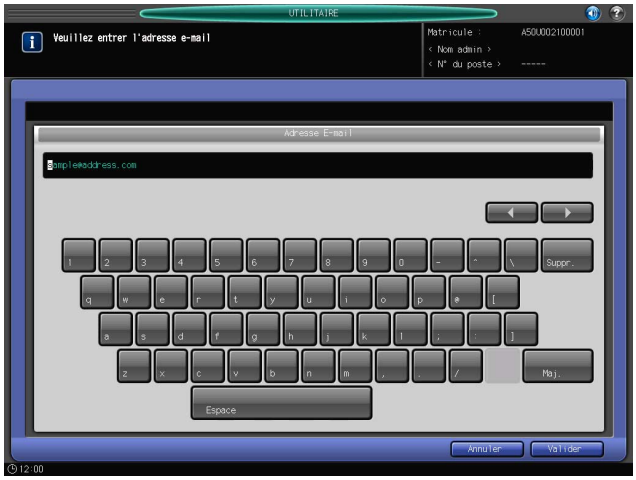
➔ Le code actuel ne plus être réutilisé comme nouveau code.

Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

12 Pour changer l'adresse e-mail, appuyez sur [Adresse E-mail].

➔ L'écran Adresse E-mail s'affiche.

➔ L'adresse e-mail peut comporter jusqu'à 320 caractères alphanumériques et symboles.



Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

13 Pour changer le compte, appuyez sur [Nom de compte].

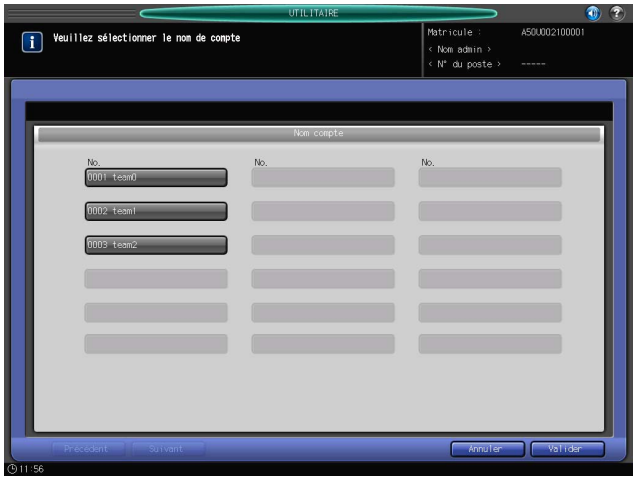
➔ L'écran Nom de compte s'affiche. Sélectionnez le compte souhaité.

REMARQUE

Si [Synchroniser Utilisateur/Gestion compte] de Méthode d'authentification est réglé sur [Synchroniser], vous pouvez configurer [Nom de compte].

REMARQUE

Le compte doit être enregistré au préalable. Sélectionnez l'un des comptes enregistrés et affichés à l'écran.



Appuyez sur [OK] pour retourner à l'écran Enregistr.util. - Ajouter/Changer.

14 Pour changer la limite autorisée, appuyez sur [Définir limite max.]. Changez le nombre maximal d'impressions autorisées pour l'utilisateur après une authentification réussie.

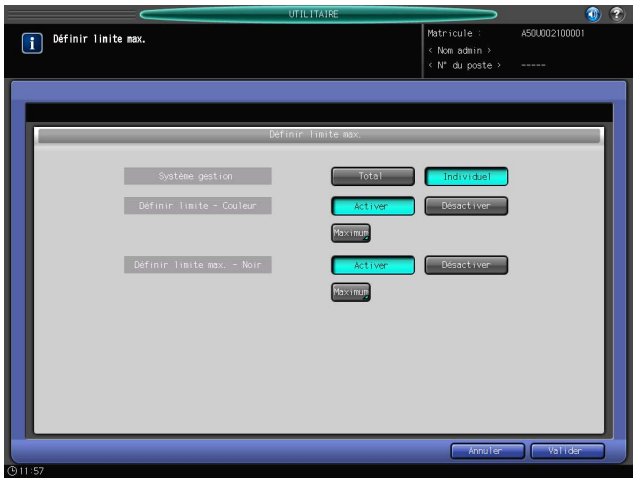
➔ Appuyez sur [Total] sur la droite de "Système gestion", [Activer] à droite de "Définir limite max." et [Maximum].

➔ Utilisez le clavier de l'écran tactile, [▼], ou [▲] pour saisir le nombre d'impressions autorisées. La plage disponible pour la limite max. est comprise entre 0 et 99 999 999.

➔ Appuyez deux fois sur [OK] pour retourner à l'écran Enregistrement utilisateur.

➔ La limite autorisée pour les impressions en couleur et en noir peut être changée séparément.

➔ Appuyez sur [Individuel] à droite de "Système gestion", [Activer] à droite de "Définir limite - Couleur" ou "Définir limite max. - Noir" et [Maximum].



➔ Utilisez le clavier de l'écran tactile, [▼], ou [▲] pour saisir le nombre d'impressions autorisées. La plage disponible pour la limite max. est comprise entre 0 et 99 999 999.

Appuyez deux fois sur [OK] pour retourner à l'écran Enregistrement utilisateur.

15 Appuyez sur [Imprim.] ou sur [En attente sur DD] à droite de "Fonction utilisable" pour sélectionner des fonctions de la machine disponibles pour l'utilisateur.

➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [Copier], [Numéris.], [Imprim.] ou sur [En attente sur DD] à droite de "Fonction utilisable".

16 Appuyez sur [Couleur] ou sur [Noir] à droite de "Autorisé sortie (Impression)" pour sélectionner le type d'impression accessible pour l'utilisateur.

17 Appuyez sur [Valider].

➔ Quand les réglages sont terminés, appuyez sur [Retour] sur l'écran Enregistrement utilisateur.

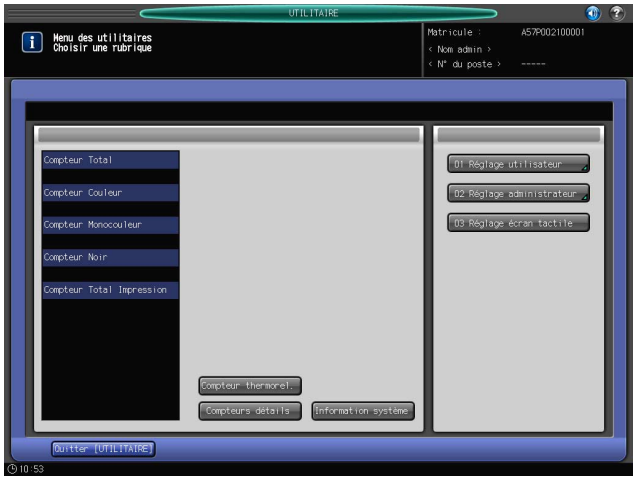
L'écran du menu Régl.auth.utilis. est restauré.

2.4.3 Suppression des données utilisateur

Suivez la procédure pour supprimer un nom d'utilisateur et mot de passe requis pour l'authentification utilisateur en mode Sécurité renforcée ainsi que pour supprimer un dossier privé.

1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

2 Appuyez sur [02 Réglage administrateur].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [03 Réglage administrateur].

L'écran Code administrateur s'affiche.

3 Entrez le code administrateur.

➔ Entrez le code administrateur composé de 8 caractères alphanumériques et symboles sur le clavier de l'écran tactile et appuyez sur [OK].

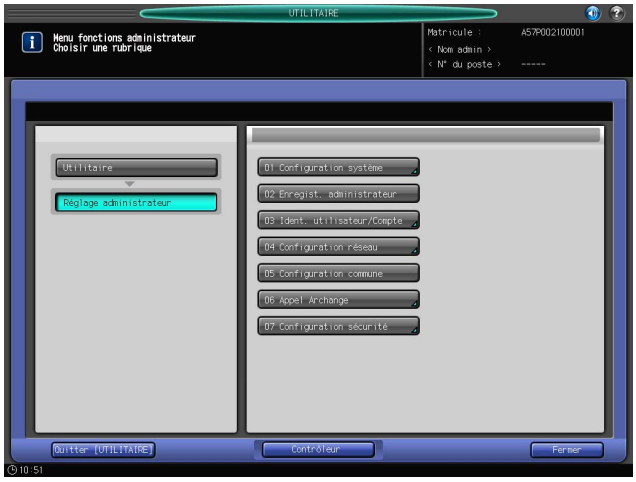
➔ Les caractères alphabétiques sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques/symboles et que [OK] est actionné, le message d'avertissement [Code incorrect/Attendre un moment] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

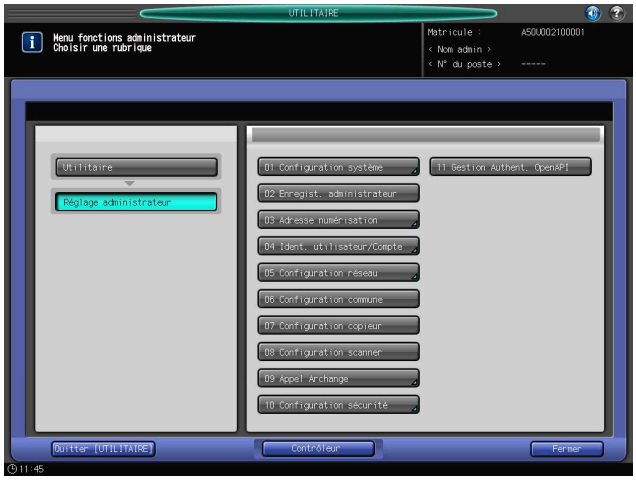
➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

L'écran du menu Réglage administrateur s'affiche.

4 Appuyez sur [03 Ident. utilisateur/Compte].

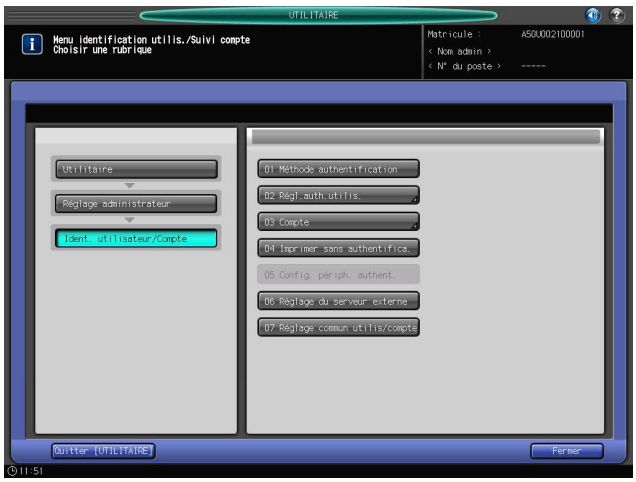


➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [04 Ident. utilisateur/Compte].



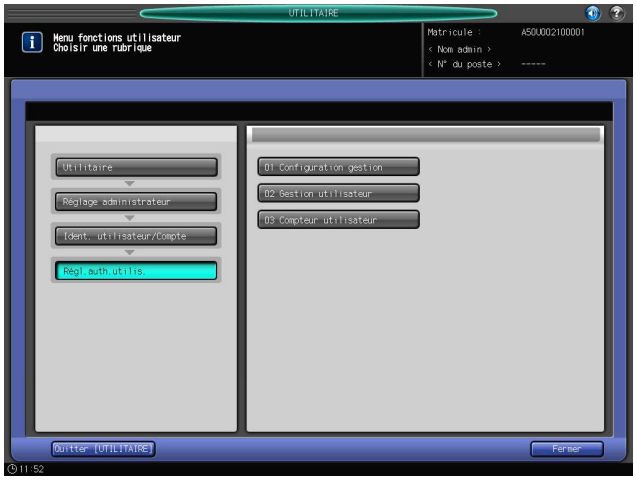
L'écran du menu Ident. utilisateur/Compte s'affiche.

5 Appuyez sur [02 Régl.auth.utilis.].



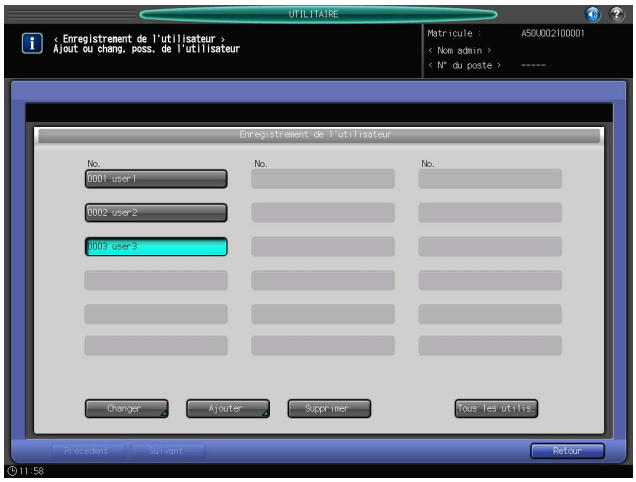
L'écran du menu Régl.auth.utilis s'affiche.

6 Appuyez sur [02 Gestion utilisateur].



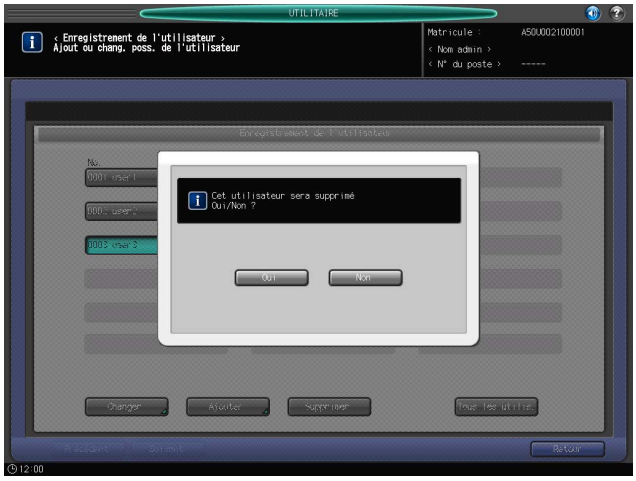
L'écran Enregistrement utilisateur s'affiche.

7 Appuyez sur le nom d'utilisateur à supprimer.



8 Appuyez sur [Supprimer].

➔ Une boîte de dialogue de confirmation s'affiche.



Appuyez sur [Oui]. Les données utilisateur sélectionnées et le dossier privé sont supprimés.

2.4.4 Changement du mot de passe par l'utilisateur

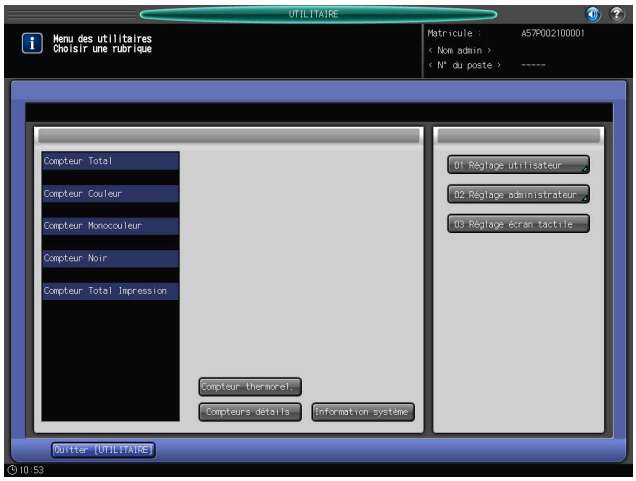
Les utilisateurs généraux peuvent changer le mot de passe requis pour l'authentification de l'utilisateur. Pour plus de sécurité, nous recommandons que les utilisateurs changent eux-mêmes le mot de passe attribué par l'administrateur.

REMARQUE

Pour changer un mot de passe utilisateur sans authentification utilisateur effectuée, il faut entrer le nom d'utilisateur spécifié avec ce mot de passe.

1 Appuyez sur **Utilitaire/Compteur** sur le **panneau de contrôle** pour afficher l'écran du menu Utilitaires.

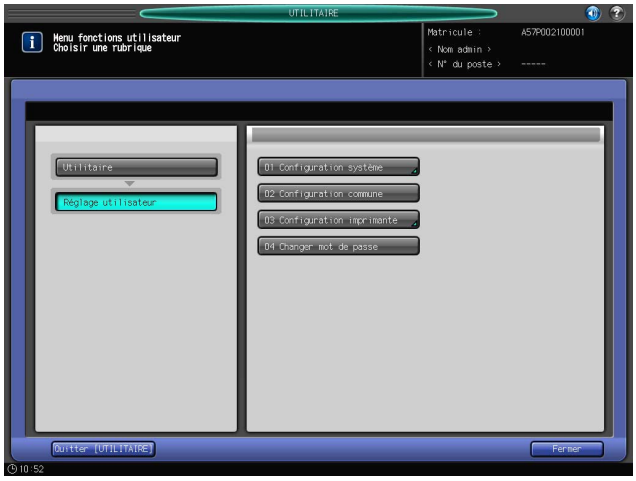
2 Appuyez sur [01 Réglage utilisateur].



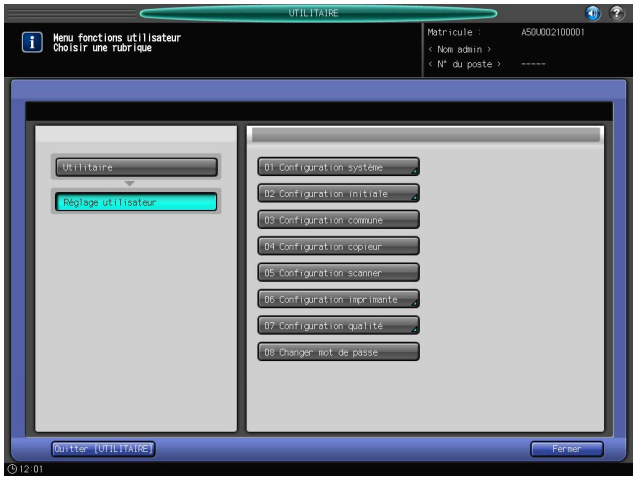
➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [02 Réglage utilisateur].

L'écran du menu Réglage utilisateur s'affiche.

3 Appuyez sur [04 Changer mot de passe].



➔ Pour la machine équipée de l'**Unité d'alimentation papier PF-708**, appuyez sur [08 Changer mot de passe].

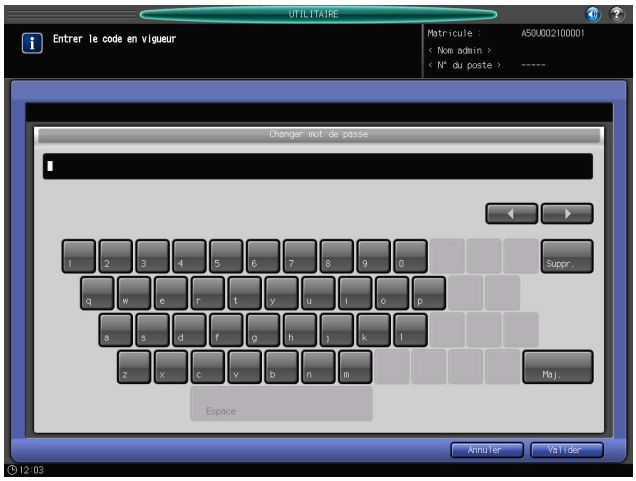


L'écran Changer mot de passe s'affiche.

4 Appuyez sur [Nom d'utilisateur], puis entrez le nom d'utilisateur spécifié avec le mot de passe à changer.

Appuyez sur [Valider].

5 Appuyez sur [Code actuel] et entrez le mot de passe actuel correspondant au nom d'utilisateur entré à l'étape 4.



Appuyez sur [Valider].

Le mot de passe saisi s'affiche à l'écran avec des astérisques (********).

➔ Les mots de passe sont sensibles à la casse.

➔ En cas de saisie d'un mot de passe incorrect ou inférieur à 8 caractères alphanumériques et que [OK] est actionné, le message d'avertissement [Code incorrect] s'affiche et aucune touche ne peut être actionnée pendant 5 secondes. Entrez le mot de passe correct au bout de cinq secondes.

➔ Les informations relatives à l'échec de l'authentification sont enregistrées dans le journal des événements.

6 Spécifiez un nouveau mot de passe sur l'écran Changer mot de passe.

➔ Appuyez sur [Nouveau code] et entrez un nouveau mot de passe pour le nom d'utilisateur entré à l'étape 4.

➔ Entrez 8 à 64 caractères alphanumériques pour le mot de passe utilisateur (les caractères alphabétiques étant sensibles à la casse).

Appuyez sur [OK].

REMARQUE

N'utilisez pas votre nom, votre date d'anniversaire, votre numéro d'employé, etc. pour un code que d'autres personnes peuvent facilement deviner.

➔ Les informations relatives à l'échec de l'authentification seront enregistrées dans le journal des événements.

➔ Le code actuel ne plus être réutilisé comme nouveau code.

7 Retapez le nouveau mot de passe pour confirmation.

➔ Appuyez sur [Confirmation de saisie] pour saisir le même code que ci-dessus.
Appuyez sur [Valider].

8 Appuyez sur [OK].

L'écran du menu Régl.auth.utilis s'affiche.

9 Appuyez sur [Quitter [UTILITAIRE]].

L'écran retourne à l'écran précédemment affiché avant l'écran du menu Utilitaire.

3 Index

3 Index

3.1 Index par élément

3.2 Index par touche