

KONICA MINOLTA

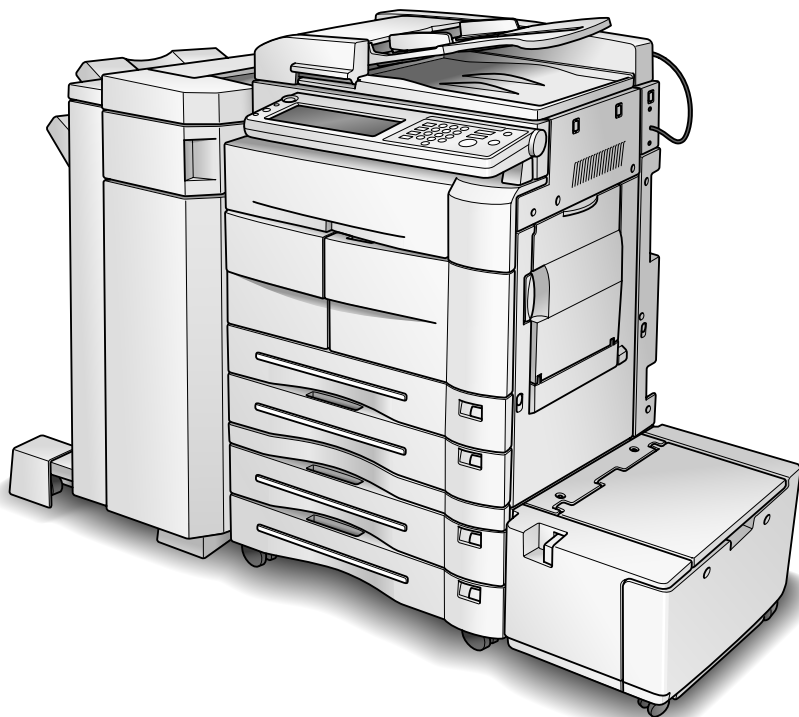
MANUEL
UTILISATEUR

7222

Sécurité

7228

7235



Les pages intérieures de ce livre sont imprimées sur du papier recyclé.

7222/7228/7235

Sécurité

7222/7228/7235 – Version du logiciel de contrôle : 10.0000 et ultérieures

MANUEL UTILISATEUR

À propos de la fonction d'affichage de version de mémoire ROM :

La version du logiciel de contrôle du périphérique 7222/7228/7235 peut être confirmée à l'aide de la fonction d'affichage de version de mémoire ROM d'administrateur de service (CE) mode 25.

Lorsque vous affichez la version de mémoire ROM, la version du logiciel de contrôle et la version de la mémoire d'amorçage s'affichent également.

Version du logiciel de contrôle : 2 chiffres + 4 décimales (ex. : 10.0001)

Version de mémoire ROM d'amorçage : 3 caractères alphanumériques (ex. : B01)

Dans l'exemple ci-dessus, la ligne affichera "10.0001 B01."

Si les quatre chiffres qui suivent les décimales de la version du logiciel de contrôle sont "0", ils n'apparaîtront pas.

Version du logiciel de contrôle : 10.0000

Version de mémoire ROM d'amorçage : B01

Dans ce cas, la ligne s'affichera de la façon suivante : "10 B01".

N'oubliez pas de prendre cette remarque en compte lorsque vous vérifiez la version du logiciel de contrôle.

Table des Matières

Fonctions de sécurité	1
Mode Accès sécurisé	2
Description du mode Accès sécurisé	2
Données protégées par le mode Accès sécurisé	3
Affichage lorsque le mode Accès sécurisé est activé	4
Protection et suppression des données après utilisation	6
Empêcher l'accès et la modification des données de la zone Archives	7
Accéder à une boîte d'utilisateur en mode Accès sécurisé	8
Supprimer des données dans la boîte d'utilisateur en mode Accès sécurisé.....	11
Enregistrer des données numérisées / modifier le mot de passe de boîte en mode Accès sécurisé	13
Sortie de données dans la boîte d'impression confidentielle.....	16
Sortie de données dans la boîte de télécopie confidentielle	18
Fonctions de sécurité de responsable	20
Activation/Désactivation du mode Accès sécurisé	20
Enregistrer/modifier l'ID d'utilisateur et le mot de passe dans la boîte d'utilisateur	23
Impression du journal d'audit.....	26
Analyse du journal d'audit.....	29

Fonctions de sécurité

Le périphérique 7222/7228/7235 est équipé de deux modes de sécurité.

Mode normal

Utilisez ce mode si l'appareil est utilisé par une seule personne et que les risques d'accès et d'utilisation non autorisés sont peu probables. C'est le mode par défaut réglé en usine. Pour utiliser le mode normal, veuillez vous reporter au guide d'utilisateur livré avec chaque type d'appareil.

Mode Accès sécurisé

Utilisez ce mode si l'appareil est connecté à un réseau local (LAN) ou à des réseaux externes via une ligne téléphonique ou d'autres modes d'accès. Un responsable gère l'appareil de la façon décrite dans ce guide, afin que les utilisateurs puissent travailler en toute sécurité.

Votre responsable est la seule personne à pouvoir activer ou désactiver le mode Accès sécurisé et effectuer d'autres modifications ; c'est votre représentant de service après-vente qui désignera le responsable.

Pour activer le mode Accès sécurisé, le représentant de service après-vente doit choisir un mot de passe de responsable pour l'appareil.

Nous vous recommandons d'utiliser le mode Accès sécurisé si souhaitez empêcher tout accès non autorisé à vos données ou toute modification et/ou effacement de celles-ci.

Environnements dans lesquels le mode Accès sécurisé est recommandé.

- Le périphérique est connecté à un réseau local (LAN), une ligne téléphonique externe ou Internet.
- L'appareil est contrôlé par une ligne téléphonique ou un réseau.

Pour travailler en toute sécurité

Pour des raisons de sécurité, il est recommandé que les superviseurs et le responsable utilisent le mode Accès sécurisé et établissent le type d'environnement suivant.

- Où installer l'appareil ?
Installez l'appareil dans un endroit où seul le personnel désigné pourra l'utiliser. Connectez l'appareil à un réseau afin que le responsable puisse facilement y accéder.
- Gestion physique des données
Installez le disque dur avec des supports de fixation pouvant uniquement être retirés par l'administrateur de service (CE). Si vous souhaitez utiliser un kit d'accès sécurisé, veuillez contacter le représentant du service après-vente.
- Transmission de documents sur un réseau interne
Si vous souhaitez transmettre un document sur un réseau en utilisant la fonction de numérisation vers FTP ou e-mail et qu'il est possible que cette transmission soit interceptée, n'envoyez alors aucun document confidentiel.
- Formation des utilisateurs
Le responsable doit fournir une formation adéquate aux utilisateurs afin de garantir l'utilisation de l'appareil en toute sécurité. Les utilisateurs doivent conserver en lieu sûr les ID d'utilisateur et les mots de passe définis par le responsable, ainsi que leurs propres mots de passe.
- Qui choisir comme responsable ?
Un superviseur doit sélectionner une personne fiable disposant des connaissances, des capacités techniques et de l'expérience requises, à qui il pourra confier la gestion de l'appareil.
- Garantie de l'administrateur de service (CE)
Un superviseur ou un responsable peut utiliser le mode Accès sécurisé après avoir vérifié qu'un contrat de service après-vente a bien été signé avec l'administrateur de service (CE). Indiquez clairement dans le contrat de service que l'administrateur de service s'engage à n'effectuer aucun acte frauduleux.

Mode Accès sécurisé

Description du mode Accès sécurisé

Les éléments suivants bénéficieront d'un accès sécurisé.

- **Protection et suppression des données en mémoire et sur le disque dur**

Deux types de données d'image seront conservées en mémoire et sur le disque dur : des données compressées de type LZ et des données non compressées (format TIFF et PDF). Lorsque vous supprimez des données, les zones de la mémoire et du disque dur qui contiennent ces données sont libérées. Cependant, en mode normal, les données ne sont pas complètement supprimées et elles peuvent donc être consultées de façon illicite. En mode Accès sécurisé, avant de libérer les zones d'image, les données sont entièrement supprimées.

Pour les données non compressées, la zone d'image est libérée après avoir été complètement effacée en mémoire et sur le disque dur, là où les données étaient enregistrées (0 FILL).

Pour les données compressées LZ, la zone est libérée lorsqu'une partie des données est détruite ou écrasée un certain nombre de fois à partir de la zone de données, rendant ainsi la décompression des données impossible.

- **Mot de passe sécurisé**

Ce mot de passe comprend 8 caractères alphanumériques (sensibles à la casse). Le système n'accepte pas de mot de passe consistant en un seul caractère répété plusieurs fois de suite.

- **Accès à la boîte d'utilisateur à l'aide de l'ID d'utilisateur et du mot de passe**

Configurez le système de façon à ce que les utilisateurs doivent entrer un mot de passe sécurisé (voir ci-dessus) pour sauvegarder et imprimer des données enregistrées dans la boîte d'utilisateur avec un mot de passe enregistré dans la zone Archives. Vous pouvez aussi définir une ID d'utilisateur en utilisant 4 à 8 chiffres pour la boîte d'utilisateur, afin d'améliorer le niveau de sécurité.

Si un mot de passe sécurisé a été défini comme indiqué ci-dessus, vous bénéficierez d'un meilleur niveau de sécurité lorsque des données numérisées seront enregistrées dans la boîte d'utilisateur. Seul le responsable peut supprimer la boîte d'utilisateur dans laquelle les données numérisées sont enregistrées et la modification des attributs de la boîte d'utilisateur requiert une authentification par mot de passe sécurisé. Une authentification sera également requise pour pouvoir utiliser les données numérisées enregistrées dans la boîte.

- **Accès externe interdit**

Aucun accès n'est autorisé sur les lignes téléphoniques autres que Fax et KRDS.

- **Création, enregistrement et analyse d'un journal d'audit**

Un historique des opérations de la fonction Sécurité est créé et enregistré. La date, l'heure, des informations identifiant la personne qui a procédé à l'opération, le détail des opérations et le résultat de l'opération seront enregistrés, permettant une analyse des accès non autorisés. Ce journal ne peut être effacé qu'en formatant le disque dur.

- **Authentification du responsable**

Un représentant du service après-vente définira les données d'identification d'un responsable.

Pour accéder au système, le responsable devra ensuite entrer son mot de passe. Une seule chaîne d'authentification peut être enregistrée par appareil.

Données protégées par le mode Accès sécurisé

Les données protégées par le mode Accès sécurisé (pour les utilisateurs) sont les suivantes.

Données enregistrées dans la boîte d'utilisateur (à l'aide de l'ID d'utilisateur et du mot de passe)

Les données suivantes gérées par le responsable bénéficieront également d'une meilleure protection.

Données d'utilisateur

Données de commande de l'appareil

Données non protégées en mode Accès sécurisé


Lorsque l'appareil est connecté à des PC sur un réseau local, les mots de passe entrés sur ces PC ne sont pas concernés par le mode Accès sécurisé.

Affichage lorsque le mode Accès sécurisé est activé

Le responsable peut activer ou désactiver le mode Accès sécurisé.

DÉTAILS

Pour activer ou désactiver le mode Accès sécurisé, voir Fonctions de sécurité de responsable, page 20.

Lorsque le mode Accès sécurisé est activé, l'icône Accès sécurisé [] apparaît sur les écrans de base Copie/Scanner/Télécopieur/Imprimante et sur certains écrans de la zone Archives.

Écran de base Copie



Écran de base Scanner

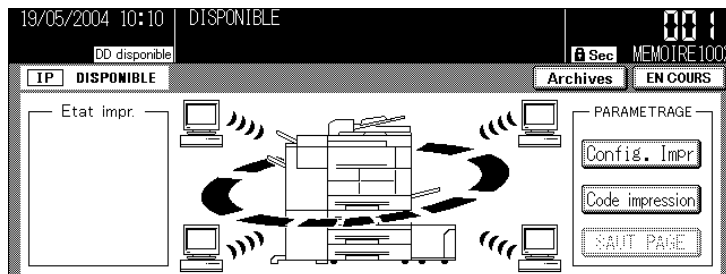


Écran de base Télécopie



Affichage lorsque le mode Accès sécurisé est activé (suite)

Écran de base Imprimante



Contrôlez l'icône Accès sécurisé sur chaque écran de base pour vérifier si le mode Accès sécurisé est activé ou désactivé.

Si le mode Accès sécurisé est désactivé, il est alors possible d'accéder aux données et de les modifier, les supprimer, etc., et cela ne sera pas enregistré dans le journal d'audit, ce qui peut s'avérer dangereux.

Si le mode Accès sécurisé est activé et qu'une personne a accédé aux données ou les a modifiées, il se peut que le responsable ne s'en rende compte qu'au moment où il analysera le journal d'audit. Il convient donc d'être prudent lorsque le responsable est absent pendant un certain temps.

Protection et suppression des données après utilisation

Les données de chaque mode (copie/scanner/télécopieur/imprimante) seront enregistrées temporairement en mémoire ou sur le disque dur et elles seront ensuite supprimées, sauf si elles sont enregistrées dans la zone Archives.

Les données sont compressées selon une méthode particulière, afin qu'elles ne puissent pas être décompressées au niveau externe.

Lorsque vous supprimez des données compressées, une partie d'entre elles sera détruite ou écrasée, afin d'en empêcher la décompression.

Les données d'image enregistrées en format TIFF ou PDF seront automatiquement et entièrement supprimées (0 FILL) dans l'ordre suivant.

Les données enregistrées temporairement en mémoire seront supprimées lorsque le travail sera interrompu ou terminé.

Les données enregistrées dans plusieurs zones de la mémoire seront supprimées simultanément. Les données de la zone Archives seront supprimées lorsqu'une commande de suppression sera émise.

Si des données sont envoyées à l'extérieur du réseau, elles seront supprimées une fois la transmission terminée.

Les données obtenues à partir de l'extérieur via un pilote TWAIN seront supprimées lorsqu'une commande de suppression sera émise à partir du pilote TWAIN.

Si le responsable émet une commande de suppression pour chaque boîte, celles-ci seront supprimées.

Empêcher l'accès et la modification des données de la zone Archives

Pour enregistrer et envoyer des données, utilisez une boîte d'utilisateur de la zone Archives.

En mode Accès sécurisé, le fait de définir une ID d'utilisateur et un mot de passe dans une boîte d'utilisateur permet d'améliorer les conditions de sécurité.

Pour éviter que n'importe qui puisse accéder aux données et les modifier, les supprimer, etc., nous vous recommandons d'utiliser une boîte d'utilisateur pour laquelle un mot de passe a été défini. Si une ID d'utilisateur et un mot de passe sont définis pour la boîte d'utilisateur, cela améliorera les conditions de sécurité.

Étant donné qu'il s'agit d'une opération réservée au responsable de l'appareil, c'est celui-ci qui doit définir une ID d'utilisateur et un mot de passe pour chaque boîte d'utilisateur, comme indiqué ci-dessous.

ID d'utilisateur : 4 à 8 chiffres

Mot de passe : 8 caractères alphanumériques (sensibles à la casse)

(Un mot de passe de moins de 8 caractères ou comportant plusieurs fois le même caractère alphanumérique ne sera pas accepté.)

Si vous avez entré un mot de passe incorrect, vous devrez attendre cinq secondes avant de pouvoir essayer à nouveau.



CONSEIL

Pour définir une ID d'utilisateur et un mot de passe pour une boîte d'utilisateur en mode Accès sécurisé, voir page 23.

Si une ID d'utilisateur et un mot de passe ont été définis pour une boîte d'utilisateur en mode normal et qu'ils ne respectent pas les conditions liées au mode Accès sécurisé, vous ne pourrez pas accéder à la boîte lorsque l'appareil est en mode Accès sécurisé.

Dans ce cas, contactez le responsable afin qu'il désactive le mode Accès sécurisé et définissez un nouveau mot de passe en respectant les conditions ci-dessus.

Après authentification, les utilisateurs peuvent changer leur mot de passe en toute liberté, à condition qu'ils respectent les conditions ci-dessus. Ils ne peuvent pas le régler de façon à ne pas utiliser de mot de passe. L'ID d'utilisateur ne peut pas être modifiée.

Même si vous êtes parvenu à accéder à une boîte d'utilisateur, l'authentification avec l'ID d'utilisateur et le mot de passe sera nécessaire dans les conditions suivantes.

- L'alimentation principale a été coupée.
- L'alimentation secondaire a été coupée.
- Quelqu'un a appuyé sur la touche [AUTO] du panneau de commande.
- L'opération de sortie de données dans une boîte est terminée.
- Quelqu'un a appuyé sur la touche FIN de l'écran Liste des documents.
- Quelqu'un a appuyé sur la touche [ÉCONOMIE D'ÉNERGIE] du panneau de commande.
- La fonction de réinitialisation automatique/arrêt automatique est active.



DÉTAILS

Lorsqu'un utilisateur accède à une boîte d'utilisateur pour laquelle un mot de passe a été défini dans la zone Archives, toutes les opérations d'authentification avec l'ID d'utilisateur et le mot de passe seront enregistrées dans le journal d'audit.

Empêcher l'accès et la modification des données de la zone Archives (suite)

Accéder à une boîte d'utilisateur en mode Accès sécurisé

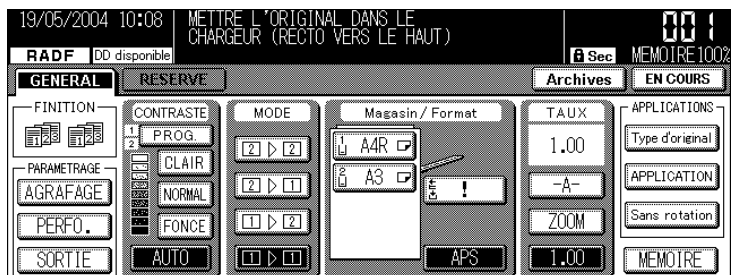
Vous trouverez ci-dessous une explication détaillée sur la façon dont vous pouvez accéder en mode Accès sécurisé à une boîte d'utilisateur pour laquelle une ID d'utilisateur et un mot de passe ont été définis.

DÉTAILS

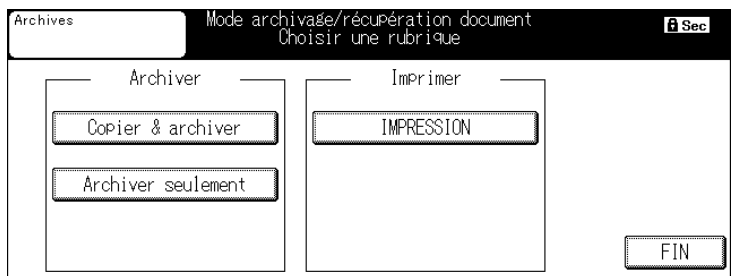
- La méthode permettant d'accéder aux données qui se trouvent dans une boîte d'utilisateur pour laquelle une ID d'utilisateur ou un mot de passe n'ont pas été définis est la même en mode normal et en mode Accès sécurisé.
- Une boîte d'utilisateur pour laquelle un mot de passe a été défini, mais qui n'a pas d'ID d'utilisateur, disposera d'un niveau de sécurité plus élevé, à condition que le mot de passe ait été défini conformément aux spécifications du mode Accès sécurisé.
- Une boîte système pour laquelle un mot de passe a été défini disposera d'un niveau de sécurité plus élevé, à condition que le mot de passe ait été défini conformément aux spécifications du mode Accès sécurisé.

Procédure

1. Appuyez sur la touche [COPIEUR] du panneau de commande pour afficher l'écran de base Copie.
2. Appuyez sur Archives.



3. Appuyez sur la touche de votre choix.



DÉTAILS

La fonction de réimpression disponible en mode normal ne peut pas être utilisée en mode Accès sécurisé. Dans ce mode, les touches Copier & Réimprimer et Réimprimer n'apparaissent pas.

4. Entrez l'ID d'utilisateur (lorsque vous accédez à une boîte d'utilisateur pour laquelle une ID d'utilisateur a été définie).

Utilisez les touches numériques du panneau de commande pour entrer l'ID d'utilisateur attribuée par le responsable (4 à 8 chiffres) et appuyez sur VALID.



Les boîtes d'utilisateur pour lesquelles l'ID d'utilisateur entrée a été définie et celles pour lesquelles aucune ID n'a été définie apparaîtront.

🔍 DÉTAILS

- Si vous entrez une ID d'utilisateur qui n'est pas reconnue et que vous appuyez sur la touche VALID., le message d'avertissement "ID d'utilisateur incorrecte" apparaîtra. Entrez l'ID d'utilisateur correcte.
- Si l'authentification échoue, cette tentative sera notée dans le journal d'audit.

5. Sélectionnez la boîte d'utilisateur de votre choix.

Appuyez sur la touche de la boîte d'utilisateur de votre choix parmi celles qui s'affichent, afin de la mettre en surbrillance. Pour sélectionner une boîte d'utilisateur qui n'apparaît pas à l'écran, appuyez sur une lettre de recherche (touches "A-" à "W-") ou sur Autres, ou entrez le numéro de boîte à l'aide des touches numériques et appuyez sur VALID. pour la rechercher, puis appuyez sur la touche trouvée pour la mettre en surbrillance.



Appuyez sur VALID.

Si vous sélectionnez une boîte d'utilisateur pour laquelle un mot de passe a été défini, l'écran d'entrée du mot de passe apparaîtra.

6. Entrez le mot de passe.

Appuyez sur la touche CODE pour afficher l'écran Saisie des données.

DÉTAILS

Utilisez les touches numériques du panneau de commande pour entrer le mot de passe sans appuyer sur CODE, s'il est uniquement constitué de numéros



Utilisez les touches de l'écran tactile et les touches numériques du panneau de commande pour entrer le mot de passe (8 caractères alphanumériques) et appuyez sur VALID.



DÉTAILS

- Respectez la casse (majuscules/minuscules) des caractères alphanumériques.
- Si vous entrez un mot de passe incorrecte ou moins de 8 caractères alphanumériques et que vous appuyez sur la touche VALID., le message d'avertissement "Mot de passe incorrect" s'affichera et les touches seront bloquées pendant 5 secondes. Attendez cinq secondes et entrez l'ID d'utilisateur correcte.
- Le système n'accepte pas de mot de passe consistant en un seul caractère répété plusieurs fois de suite.
- Si l'authentification échoue, cette tentative sera notée dans le journal d'audit.
- Les boîtes d'utilisateur pour lesquelles un mot de passe a été défini et la boîte système pour laquelle un mot de passe a été défini seront gérées conformément aux spécifications du mode Accès sécurisé précédemment évoquées.

Appuyez sur la touche VALID. de l'écran de saisie du mot de passe.

Pour ce qui est des opérations suivantes pour la sauvegarde des données dans une boîte d'utilisateur et la sortie des données, reportez-vous au guide d'utilisateur des Archives.

Empêcher l'accès et la modification des données de la zone Archives (suite)

Supprimer des données dans la boîte d'utilisateur en mode Accès sécurisé

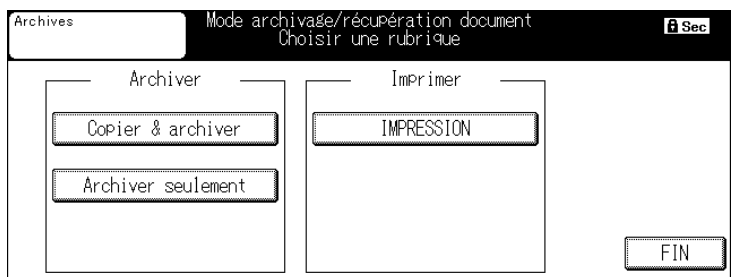
Vous trouverez ci-dessous des explications détaillées sur la façon dont vous pouvez supprimer un document enregistré dans une boîte d'utilisateur.

Procédure

1. Appuyez sur la touche Archives de l'écran de base Copie, Télécopieur ou Imprimante.



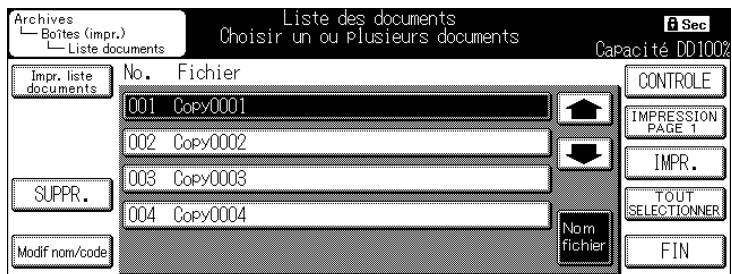
2. En mode Copie, appuyez sur IMPRESSION.



CONSEIL

Pour les modes Télécopieur et Imprimante, reportez-vous au guide d'utilisateur du mode correspondant.

3. Suivez les étapes 4 ~ 6 page 9 et 10 pour afficher l'écran Liste des documents.



4. Sélectionnez les données (documents) à supprimer.

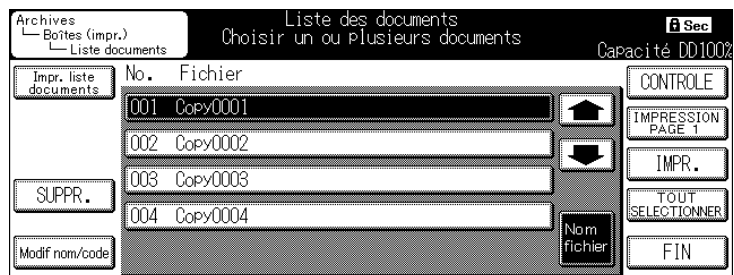
Appuyez sur la touche correspondant au document que vous souhaitez supprimer.



🔍 DÉTAILS

- Si un mot de passe a été défini pour le document sélectionné, une fenêtre s'affichera et vous devrez entrer le mot de passe du document. Appuyez sur CODE pour afficher l'écran Saisie des données, entrez le mot de passe (maximum 8 chiffres) à l'aide des touches de l'écran tactile et appuyez sur VALID.
- Utilisez les touches numériques du panneau de commande pour entrer le mot de passe du document sans afficher l'écran Saisie des données, s'il est uniquement constitué de numéros.

5. Appuyez sur SUPPR.



Une fenêtre s'affiche pour vous demander de confirmer la suppression.



Appuyez sur OUI. Le document sélectionné sera supprimé et l'affichage repassera à l'écran Liste des documents.

Empêcher l'accès et la modification des données de la zone Archives (suite)

Enregistrer des données numérisées / modifier le mot de passe de boîte en mode Accès sécurisé

Vous pouvez sélectionner une boîte d'utilisateur pour recevoir les données de numérisation. Qu'un mot de passe ait été défini ou non, accédez à une boîte à laquelle un numéro a été attribué, définissez un mot de passe sécurisé en mode Accès sécurisé et enregistrez les données dans la boîte d'utilisateur.

Les utilisateurs normaux peuvent changer le mot de passe déjà défini pour une boîte d'utilisateur disposant d'un numéro de boîte, conformément aux spécifications du mode Accès sécurisé.



Rappel

Les utilisateurs normaux doivent changer dès que possible le mot de passe attribué par le responsable, afin de pouvoir protéger leurs données.

Enregistrez les données numérisées et changez le mot de passe de la boîte en suivant les procédures ci-dessous.

Procédure

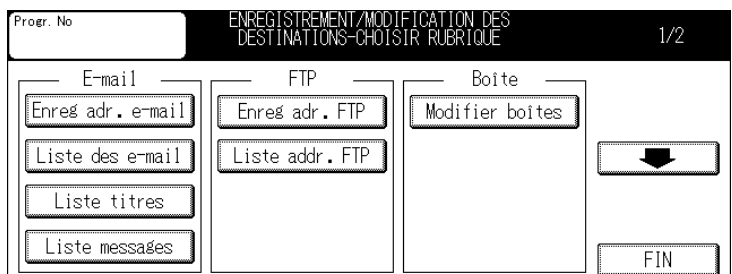
1. Appuyez sur la touche [SCANNER/ARCHIVES] du panneau de commande.

L'écran de base Scanner apparaît.



2. Appuyez sur Boîte, puis sur Prog. touches, à droite de l'écran.

L'écran de saisie de la destination apparaît.



Empêcher l'accès et la modification des données de la zone Archives (suite)

Progr. No ENREGISTREMENT/MODIFICATION DES DESTINATIONS-CHOISIR RUBRIQUE 2/2

PC (SMB)

Config. PC (SMB)

Liste adresses

FIN

🔍 DÉTAILS

- Vous ne pouvez pas créer un nouveau numéro de boîte. Si vous souhaitez le modifier, contactez le responsable.
- Le mot de passe apparaîtra sous la forme suivante : "*****". Entrez 8 caractères alphanumériques de votre choix. Si la boîte ne dispose pas encore d'un mot de passe, saisissez-en un. Sans mot de passe, une boîte ne peut pas être enregistrée comme destination d'envoi des données.

3. Appuyez sur Modifier boîtes.

L'écran de saisie du numéro de boîte apparaît.

Progr. No Entrer un numéro de boîte Sec

Modifier boîtes

No boîte 1

SUPPR.

ANNUL.

VALID.

4. Entrez un numéro de boîte de 1 à 999999999 à l'aide des touches numériques du panneau de commande et appuyez sur VALID.

L'écran de saisie/modification de boîte apparaît.

Progr. No Modifier boîtes Sec

Modifier boîtes

No boîte 2

Nom KMBT

CODE *****

pour recherche A- D- G- J- M- P- T- W- Autres

ENREG.

FIN

🔍 DÉTAILS

Entrez un numéro de boîte existant. Seul le responsable peut enregistrer un nouveau numéro de boîte.

5. Appuyez sur CODE.

L'écran Saisie des données apparaît.



6. Entrez le mot de passe et appuyez sur VALID.

Si la boîte n'avait pas de mot de passe, celui que vous avez entré sera défini pour la boîte.

Si la boîte avait déjà un mot de passe, celui que vous avez entré remplacera l'ancien.

Pour plus d'informations sur les opérations de numérisation, reportez-vous au guide d'utilisateur Réseau/Scanner.

DÉTAILS

- Si le mot de passe entré existe déjà, il passera sur la valeur par défaut "*****". Entrez un nouveau mot de passe.
- Les mots de passe sont sensibles à la casse (majuscules/minuscules).
- Si vous entrez un mot de passe incorrect ou de moins de 8 caractères alphanumérique et que vous appuyez sur la touche VALID., le message d'avertissement "Mot de passe incorrect" apparaîtra. Entrez le mot de passe correct.
- N'utilisez pas votre nom, date de naissance, numéro d'employé, etc. Ce type de mot de passe peut être facilement découvert.
- Si la définition du mot de passe échoue, cet échec sera noté dans le journal d'audit.

Sortie de données dans la boîte d'impression confidentielle

Impression confidentielle à partir d'un PC :

Pour définir la sortie des données à l'aide de la fonction d'impression confidentielle sur un PC, entrez une ID d'utilisateur composée de 4 à 8 chiffres. En mode Accès sécurisé, entrez également un mot de passe composé de 8 caractères alphanumériques.

DÉTAILS

- Les mots de passe sont sensibles à la casse (majuscules/minuscules).
- Si vous entrez moins de 8 caractères alphanumériques et que vous appuyez sur la touche VALID., le mot de passe ne sera pas accepté.
- La définition de l'ID d'utilisateur pour la boîte d'impression confidentielle n'est pas obligatoire, mais elle est tout de même recommandée, afin d'améliorer le niveau de sécurité.

Sortie d'impression confidentielle sur l'appareil :

Appuyez sur la touche [IMPRIMANTE] du panneau de commande pour sélectionner le mode Imprimante, puis appuyez sur la touche Saisie code. L'écran Saisie code / Entrer l'ID utilisateur avec le clavier apparaît.

A l'aide des touches numériques du panneau de commande, entrez l'ID d'utilisateur définie lorsque vous avez lancé l'impression confidentielle sur le PC.

Appuyez sur Code pour afficher l'écran Saisie des données, puis entrez le mot de passe à l'aide de l'écran tactile et des touches numériques du panneau de commande.



Empêcher l'accès et la modification des données de la zone Archives (suite)

Appuyez sur VALID. Vous repasserez à l'écran Saisie code / Entrer l'ID utilisateur avec le clavier.

Dans cet écran, appuyez sur la touche VALID.

L'impression confidentielle démarrera.



DÉTAILS

- Les mots de passe sont sensibles à la casse (majuscules/minuscules).
- Si vous entrez un mot de passe incorrecte ou moins de 8 caractères alphanumériques et que vous appuyez sur la touche VALID., le message d'avertissement "Mot de passe incorrect" s'affichera et les touches seront bloquées pendant 5 secondes. Attendez cinq secondes et entrez le mot de passe correct.
- Si l'authentification échoue, cette tentative sera notée dans le journal d'audit.

Sortie de données dans la boîte de télécopie confidentielle

Enregistrement d'un mot de passe confidentiel/numéro de protection d'accès pour la boîte de télécopie confidentielle :

Lorsque vous enregistrez la boîte de télécopie confidentielle, appuyez sur la touche Code réception et entrez 1 à 4 chiffres à l'aide des touches numériques du panneau de commande.

Appuyez sur Clé boîte pour afficher l'écran Saisie des données. En mode Accès sécurisé, entrez le numéro de protection d'accès composé de 8 caractères alphanumériques et appuyez sur VALID.

La touche d'enregistrement de l'écran Créer ou modifier boîte aux lettres / Réception ne fonctionnera pas tant que vous n'aurez pas entré un numéro de protection d'accès à 8 chiffres.

Progr. No
Boîte réception

CREER OU MODIFIER BOITE AUX LETTRES
RECEPTION - CHOISIR UNE RUBRIQUE

No de la boîte 001 (00 A 20)

Code réception 1234

Nom

Clé boîte *****

Vérifier code OUI NON

ENREG. FIN

Saisie des données [Clavier]

← →

1 2 3 4 5 6 7 8 9 0 - =

q w e r t y u i o p []

a s d f g h j k l : ;

z x c v b n m - . /

ESP.

SUPPR. Standard Basculer ANNUL. VALID.

🔍 DÉTAILS

- Vous pouvez également utiliser les touches numériques du panneau de commande pour entrer le numéro.
- Lorsque vous entrez un numéro de protection d'accès, tous les caractères s'affichent sous forme de *.
- Il n'est pas obligatoire d'entrer un mot de passe pour la boîte de numérisation. Le fait d'entrer un mot de passer permet d'améliorer le niveau de sécurité.
- Les numéro de protection d'accès sont sensibles à la casse (majuscules/minuscules).
- Si vous entrez moins de 8 caractères alphanumériques pour le numéro de protection d'accès et que vous appuyez sur la touche VALID., il ne sera pas accepté.
- La définition d'un mot de passe confidentiel/numéro de protection d'accès pour la boîte de télécopie confidentielle n'est pas obligatoire, mais elle permet d'améliorer le niveau de sécurité.

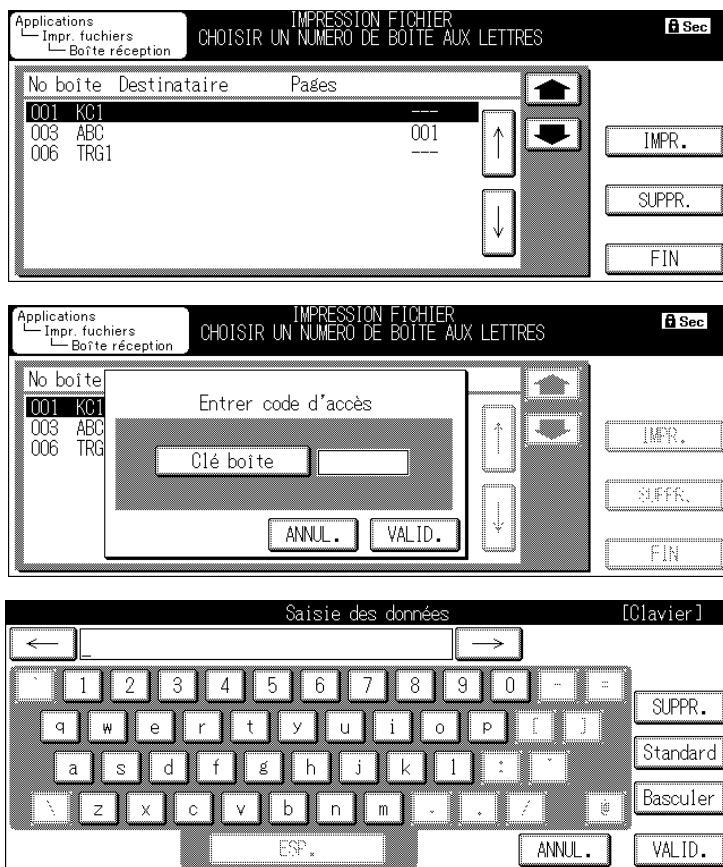
Empêcher l'accès et la modification des données de la zone Archives (suite)

Sortie de données dans la boîte de télécopie confidentielle :

Appuyez sur la touche [FAX] du panneau de commande pour sélectionner le mode Télécopieur et passez à l'écran Impr. fichiers d'Applications pour afficher l'écran Impression fichier.

Appuyez sur IMPR. ou SUPPR. L'écran d'entrée du numéro de protection d'accès apparaît.

Appuyez sur la touche Clé boîte pour afficher l'écran Saisie des données et entrez le mot de passe.



En mode Accès sécurisé, entrez 8 caractères alphanumériques et appuyez sur VALID. Vous repassez à l'écran Impression fichier.

DÉTAILS

- Vous pouvez également utiliser les touches numériques du panneau de commande pour entrer le numéro.
- Les mots de passe sont sensibles à la casse (majuscules/minuscules).
- Si vous entrez moins de 8 caractères alphanumériques et que vous appuyez sur la touche VALID., le message d'avertissement "Mot de passe incorrect" s'affichera et les touches seront bloquées pendant 5 secondes. Attendez cinq secondes et entrez le mot de passe correct.
- Si l'authentification échoue, cette tentative sera notée dans le journal d'audit.

Pour plus d'informations, reportez-vous aux différents guides d'utilisateur.

Fonctions de sécurité de responsable

Le responsable peut activer ou désactiver le mode Accès sécurisé.

Pour cela, il est nécessaire de définir un mot de passe de responsable à 8 chiffres pour l'appareil. Demandez à votre représentant de service après-vente agréé de définir un mot de passe de responsable.

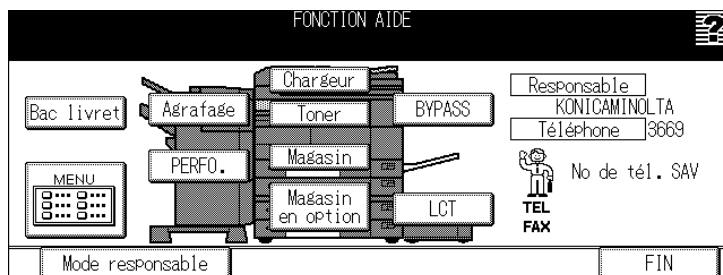
Pour protéger les données de la machine et éviter qu'on puisse y accéder ou les modifier, il est recommandé de désigner un responsable et d'utiliser le mode Accès sécurisé.

Activation/Désactivation du mode Accès sécurisé

Vous trouverez ci-dessous une explication sur la façon dont vous pouvez activer ou désactiver le mode Accès sécurisé.

Procédure

1. Appuyez sur la touche [COPIEUR] du panneau de commande pour afficher l'écran Copieur.
2. Appuyez sur la touche [AIDE].
3. Appuyez sur la touche Mode responsable de l'écran d'aide.



L'écran de saisie du mot de passe apparaît.

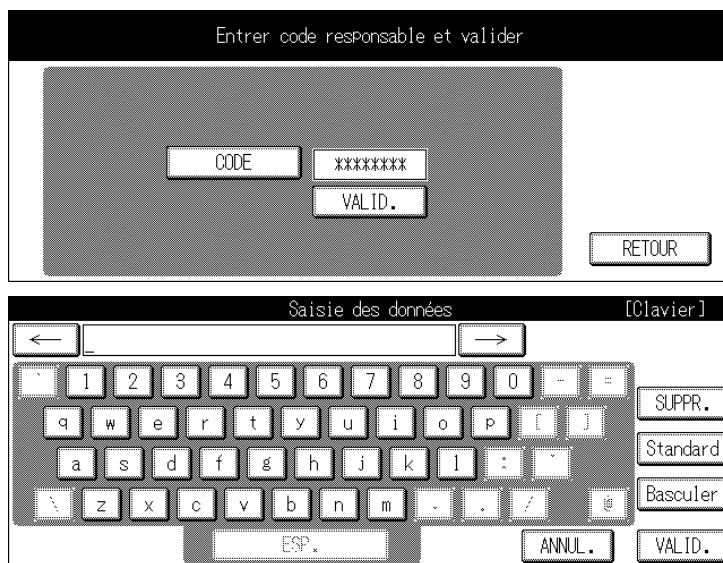
Appuyez sur CODE. Si le mode Accès sécurisé n'a pas été défini, entrez un mot de passe de responsable de 1 à 8 chiffres à l'aide de l'écran tactile et des touches numériques du panneau de commande, et appuyez sur VALID.

Si le mode Accès sécurisé a été défini, appuyez sur CODE, entrez le mot de passe de responsable (8 caractères alphanumériques) à l'aide de l'écran tactile et des touches numériques du panneau de commande, et appuyez sur VALID. (Voir page 23 pour plus de détails.)

DÉTAILS

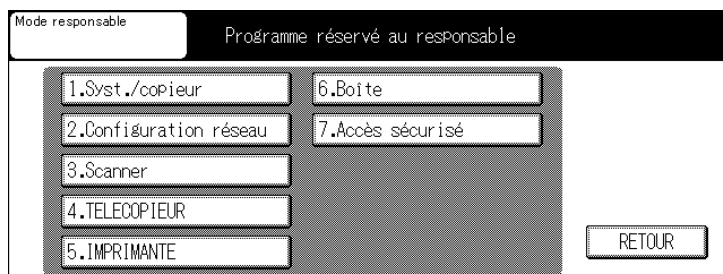
Utilisez les touches numériques du panneau de commande pour entrer le mot de passe sans appuyer sur CODE, s'il est uniquement constitué de numéros.

Fonctions de sécurité de responsable (suite)



Sur l'écran d'entrée du mot de passe, appuyez sur VALID. L'écran Mode responsable apparaît.

4. Sur l'écran Mode responsable, appuyez sur la touche 7. Accès sécurisé.



L'écran de configuration du mode Accès sécurisé apparaît.

5. Appuyez sur la touche 1. Accès sécurisé.



L'écran Accès sécurisé apparaît.

6. Activez ou désactivez le mode Accès sécurisé.

Si vous souhaitez activer le mode Accès sécurisé, appuyez sur la touche OUI pour la mettre en surbrillance. Si vous souhaitez le désactiver, appuyez sur la touche NON pour la mettre en surbrillance.
Appuyez sur VALID.



Le message de confirmation du redémarrage apparaît.



DÉTAILS

Si vous appuyez sur VALID. sans changer le réglage, le message de confirmation du redémarrage n'apparaîtra pas et vous repasserez à l'écran de configuration du mode Accès sécurisé.

7. Appuyez sur OUI.

L'appareil redémarre et le nouveau réglage est activé.

Rappel

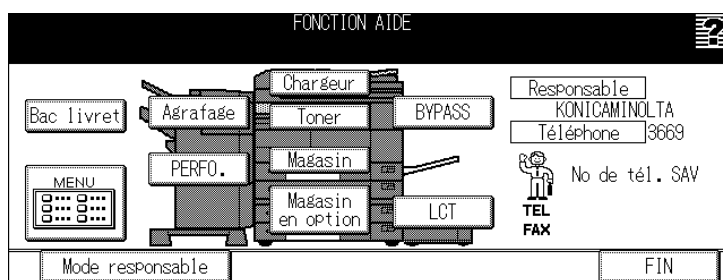
Si vous allumez ou éteignez l'alimentation principale ou secondaire sans appuyer sur la touche OUI, le changement n'apparaîtra pas dans les réglages. Pour changer le réglage, vous devez toujours appuyer sur la touche OUI.

Enregistrer/modifier l'ID d'utilisateur et le mot de passe dans la boîte d'utilisateur

Vous trouverez ci-dessous des explications sur la façon dont vous pouvez accéder à l'écran qui permet d'enregistrer ou de modifier une boîte d'utilisateur en mode Accès sécurisé, ainsi que les précautions d'usage.

Procédures

1. Appuyez sur la touche [COPIEUR] du panneau de commande pour afficher l'écran Copieur.
2. Appuyez sur la touche [AIDE].
3. Appuyez sur la touche Mode responsable de l'écran d'aide.

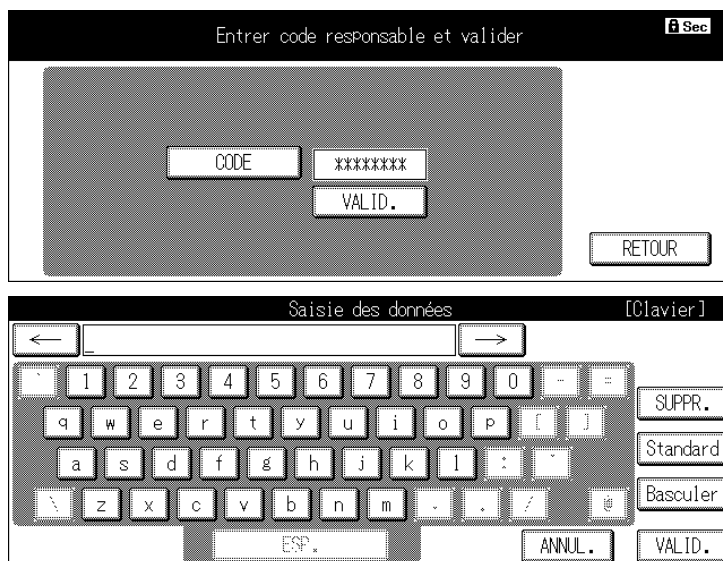


L'écran de saisie du mot de passe apparaît.

Appuyez sur CODE et, à l'aide de l'écran tactile et des touches numériques du panneau de commande, entrez le mot de passe de responsable (8 caractères alphanumériques) attribué par le représentant de service après-vente, puis appuyez sur VALID.

🔍 DÉTAILS

Utilisez les touches numériques du panneau de commande pour entrer le mot de passe sans appuyer sur CODE, s'il est uniquement constitué de numéros.

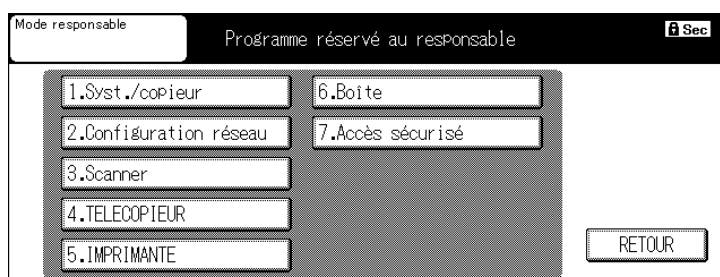


DÉTAILS

- Les mots de passe sont sensibles à la casse (majuscules/minuscules).
- Si vous entrez un mot de passe incorrecte ou moins de 8 caractères alphanumériques et que vous appuyez sur la touche VALID., le message d'avertissement "Mot de passe incorrect" s'affichera et les touches seront bloquées pendant 5 secondes. Attendez cinq secondes et entrez le mot de passe correct.
- Si l'authentification échoue, cette tentative sera notée dans le journal d'audit.

Sur l'écran d'entrée du mot de passe, appuyez sur VALID. L'écran Mode responsable apparaît.

4. Appuyez sur la touche 6. Boîte.



L'écran des paramètres de boîte apparaît.

Cet écran comprend les éléments suivants :

- (1) Boîte système
- (2) Boîtes utilisateur
- (3) Liste boîtes utilisateur



DÉTAILS

Si le mode Accès sécurisé est activé, la touche 4. Réimprimer n'apparaîtra pas et vous ne pourrez pas utiliser cette fonction.

Pour les autres réglages, reportez-vous aux différents guides d'utilisateur.

Fonctions de sécurité de responsable (suite)

Un mot de passe doit être défini dans chaque boîte et n'oubliez pas de prendre en compte les remarques suivantes si le mode Accès sécurisé est activé.

Mot de passe Boîte système :

8 caractères alphanumériques (sensibles à la casse)

Les mots de passe de moins de 8 caractères ne seront pas acceptés.

Vous ne pouvez pas utiliser un mot de passe existant déjà.

ID d'utilisateur pour Boîte utilisateur :

4 à 8 chiffres

Mot de passe pour Boîte utilisateur :

8 caractères alphanumériques (sensibles à la casse)

Les mots de passe de moins de 8 caractères ou consistant en un seul caractère répété plusieurs fois de suite ne seront pas acceptés.



Rappel

N'utilisez pas votre nom, date de naissance, numéro d'employé, etc. Ce type de mot de passe peut être facilement découvert.

Suppression d'un mot de passe d'une boîte d'utilisateur :

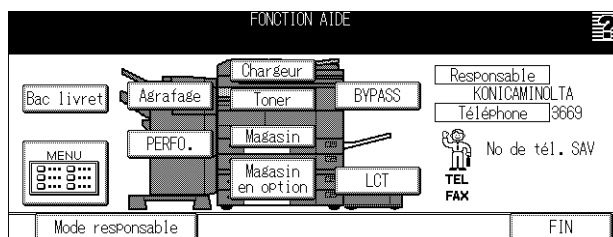
Le responsable peut supprimer le mot de passe d'une boîte d'utilisateur. Les boîtes d'utilisateur dont le mot de passe a été effacé ne peuvent plus être utilisées en mode Accès sécurisé. Veillez à prendre cela en compte, si le responsable supprime un mot de passe.

Impression du journal d'audit

Si le mode Accès sécurisé est activé, un journal d'audit sera automatiquement créé. Vous trouverez ci-dessous une explication sur la façon dont vous pouvez imprimer le journal d'audit automatiquement créé.

Procédure

1. Appuyez sur la touche [COPIEUR] du panneau de commande pour afficher l'écran Copieur.
2. Appuyez sur la touche [AIDE].
3. Dans l'écran d'aide, appuyez sur la touche Mode responsable.

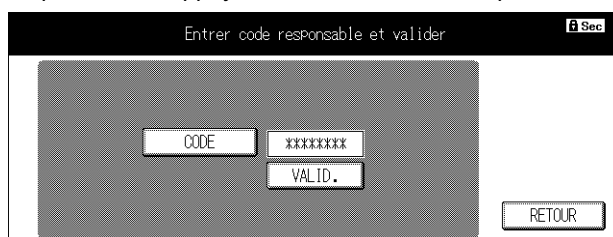


L'écran de saisie du mot de passe apparaît.

Appuyez sur CODE et, à l'aide de l'écran tactile et des touches numériques du panneau de commande, entrez le mot de passe (8 caractères alphanumériques) attribué par le représentant de service après-vente, puis appuyez sur VALID.

🔍 DÉTAILS

Utilisez les touches numériques du panneau de commande pour entrer le mot de passe sans appuyer sur CODE, s'il est uniquement constitué de numéros

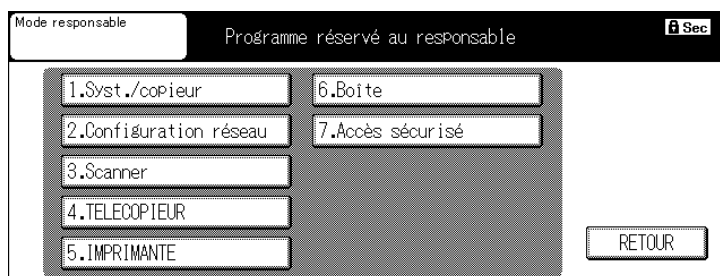


🔍 DÉTAILS

- Les mots de passe sont sensibles à la casse (majuscules/minuscules).
- Si vous entrez un mot de passe incorrect ou moins de 8 caractères alphanumériques et que vous appuyez sur la touche VALID., le message d'avertissement "Mot de passe incorrect" s'affichera et les touches seront bloquées pendant 5 secondes. Attendez cinq secondes et entrez le mot de passe correct.
- Si l'authentification échoue, cette tentative sera notée dans le journal d'audit.

Sur l'écran d'entrée du mot de passe, appuyez sur VALID. L'écran Mode responsable apparaît.

4. Sur l'écran Mode responsable, appuyez sur la touche 7. Accès sécurisé.



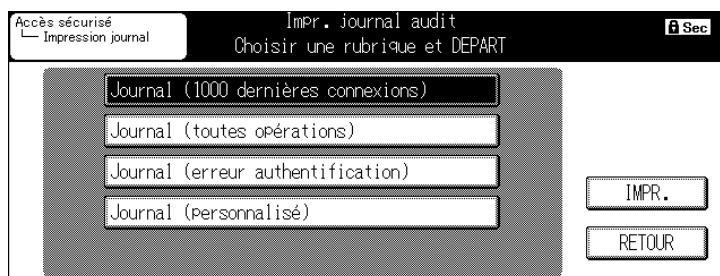
L'écran de configuration du mode Accès sécurisé apparaît.

5. Appuyez sur la touche 2. Impr. journal audit.



L'écran Impr. journal audit apparaît.

Sélectionnez le format de sortie de votre choix et appuyez sur la touche pour la mettre en surbrillance.



Journal (1000 dernières connexions) :

Les 1000 dernières connexions seront imprimées dans le rapport de journal d'audit.

Journal (toutes opérations) :

Toutes les entrées du journal d'audit (maximum 10 000) seront imprimées.

Si vous choisissez une des deux options ci-dessus, passez à l'étape 7.

Journal (erreur authentification) :

Seuls les journaux d'erreur créés en cas d'échec d'authentification seront imprimés. Il n'y a pas de limite au nombre d'entrées qui seront imprimées.

Vous pouvez associer ce format avec "Journal (personnalisé)" pour imprimer des journaux.

Si vous souhaitez imprimer uniquement les erreurs d'authentification, passez à l'étape 7.

Si vous souhaitez imprimer des journaux associant ce format et "Journal (personnalisé)", sélectionnez cette touche et passez à l'étape 6.

Fonctions de sécurité de responsable (suite)

Journal (personnalisé) :

Affichez l'écran Paramétrage journal, spécifiez la date et l'heure de création des entrées de journal d'audit et le nombre à imprimer.

Si vous associez ce format avec "Journal (erreur authentification)", vous pouvez obtenir uniquement les entrées nécessaires pour la période à laquelle une erreur d'authentification a eu lieu.

Passez à l'étape 6.

6. Appuyez sur la touche Journal (personnalisé). L'écran Paramétrage journal apparaît.

Accès sécurisé
Impression journal
Paramétrage journal

Paramétrage journal
Entrer nombre d'opérations et date

Valeur actuelle 19/05/2004 12:58
jj/mm/aaaa hh/mm

Valeur Progr. 19/05/2004 12:57

Nbre opérations 01000 1-10000

ANNUL.

VALID.

Appuyez sur la touche Valeur progr. pour spécifier la période pour laquelle vous souhaitez un journal d'audit.

Utilisez les touches fléchées droite/gauche pour déplacer le curseur et entrez les chiffres à l'aide des touches numériques du panneau de commande.

Les entrées de journal à partir de la date et de l'heure entrées seront imprimés.

Appuyez sur la touche Nbre opérations pour spécifier le nombre à imprimer.

Entrez un chiffre à l'aide des touches numériques du panneau de commande.

Le nombre maximum d'entrées de journal est de 10 000 pour les appareils équipés d'un disque dur et de 2400 les appareils sans disque dur.

Appuyez sur la touche VALID. pour repasser à l'écran Impr. journal audit.

7. Dans cet écran, appuyez sur la touche IMPR.

Les entrées de journal d'audit spécifiées seront imprimées.

Accès sécurisé
Impression journal

Impr. journal audit
Choisir une rubrique et DEPART

Journal (1000 dernières connexions)

Journal (toutes opérations)

Journal (erreur authentification)

Journal (personnalisé)

IMPR.

RETOUR

🔍 DÉTAILS

- Pour arrêter l'impression, appuyez sur la touche [ARRÊT] du panneau de commande.
- Si l'impression se termine normalement, vous pourrez imprimer une autre liste en continu à partir de l'écran Impr. journal audit.

Fonctions de sécurité de responsable (suite)

Analyse du journal d'audit

Les journaux d'audit doivent être analysés régulièrement par le responsable ou en cas d'accès ou de modification non autorisée des données enregistrées sur la machine, lorsqu'elle est en mode Accès sécurisé.

Vous pouvez imprimer les entrées de journal d'audit sous quatre formats différents (voir pages 27 et 28). Lorsque vous imprimez des journaux pour les analyser, prenez en compte toutes les caractéristiques individuelles.

Journal (1000 dernières connexions)

P.1
2004/01/14 16:31
27NA90005
TC: 753
ROM Ver. 10 0000

Date	ID	ID opération	RÉSULT AT	Date	ID	ID opération	RÉSULT AT
04/01/14 20:42:48	-2	02	ECHEC	04/01/14 20:42:59	-2	02	ECHEC
04/01/14 20:43:15	-2	02	ECHEC	04/01/14 20:43:21	-2	02	ECHEC
04/01/14 20:43:35	-2	02	ECHEC	04/01/14 20:44:07	-2	02	ECHEC
04/01/14 20:44:20	-2	02	ECHEC	04/01/14 20:44:27	-2	02	ECHEC
04/01/14 20:44:32	-2	02	ECHEC	04/01/14 20:44:47	-2	02	ECHEC
04/01/14 09:20:00	-2	02	ECHEC	04/01/15 09:20:13	-2	02	ECHEC
04/01/14 09:20:35	-2	02	ECHEC	04/01/15 09:20:47	-2	02	ECHEC
04/01/14 09:20:56	-2	02	ECHEC	04/01/15 09:21:07	-2	02	ECHEC
04/01/14 09:21:32	-1	01	OK	04/01/15 09:22:15	-2	02	ECHEC
04/01/14 09:22:25	-2	02	ECHEC	04/01/15 09:22:49	-1	01	OK
04/01/14 09:23:19	-2	02	ECHEC	04/01/15 09:23:24	-2	02	ECHEC
04/01/14 09:23:57	-1	01	OK	04/01/15 09:24:07	-1	06	OK
04/01/14 09:24:20	-2	02	OK	04/01/15 09:24:24	-2	03	OK
04/01/14 09:25:18	-2	03	OK	04/01/15 09:25:23	-2	03	OK
04/01/14 19:08:24	-2	03	OK				

Informations du journal d'audit

Le journal d'audit contient les informations suivantes.

1. Date et heure : date et heure à laquelle une opération a été effectuée, donnant lieu à la création d'une entrée dans le journal.
2. ID : permet de spécifier la personne qui a effectué l'opération ou qui est en rapport avec un problème de protection.
"-1" : Opération effectuée par le CE (représentant de service après-vente).
"-2" : Opération effectuée par le responsable.
Autres chiffres : Indique des interventions liées à la sécurité, les ID d'opérations suivantes permettent d'avoir plus de précisions sur la source du problème de sécurité.
N° de boîte : Le N° de la boîte pour laquelle l'opération a été effectuée.
ID d'utilisateur Confidentiel : ID spécifiée par un PC au moment de l'impression confidentielle (ID de 1 à 5 chiffres spécifiée par l'utilisateur).
N° de boîte Confidentiel : N° de boîte vers laquelle une réception de télécopie confidentielle a été effectuée (N° de boîte Confidentiel de 1 à 9 chiffres).
3. ID opération : ID permettant de spécifier l'opération.
Vérifiez le détail de l'opération en rapport avec l'ID d'opération dans le tableau ci-dessous.
4. Résultat : Résultat d'une opération.
Pour l'authentification du mot de passe, la réussite ou l'échec seront indiqués par OK et ECHEC.
Pour les opérations sans authentification de mot de passe, toutes les entrées de journal seront indiquées comme OK.

Fonctions de sécurité de responsable (suite)

Tableau des différents éléments enregistrés dans le journal d'audit

N°	Opération	ID	ID opération	Résultat
1	Authentification CE	ID CE	01 : CE_ID (fixe)	OK/ECHEC
2	Authentification responsable	ID responsable	02 : ID responsable (fixe)	OK/ECHEC
3	Définir/changer Mode Accès sécurisé	ID responsable	03 : Définir/changer mode sécurisé	OK
4	Imprimer journal d'audit	ID responsable	04 : Imprimer journal d'audit	OK
5	Changer/enregistrer mot de passe CE	ID CE	05 : Changer/enregistrer mot de passe CE	OK
6	Changer/enregistrer mot de passe responsable	ID CE	06 : Changer/enregistrer mot de passe responsable	OK
7	Créer boîte d'utilisateur	N° boîte	07 : Créer boîte d'utilisateur	OK
8	Changer/enregistrer mot de passe boîte par responsable	N° boîte	08 : Changer/enregistrer mot de passe boîte par responsable (1)	OK
9	Supprimer boîte d'utilisateur	N° boîte	09 : Supprimer boîte d'utilisateur	OK
10	Changer attributs de boîte d'utilisateur	N° boîte	10 : Changer attributs de boîte d'utilisateur	OK
11	Authentification mot de passe pour boîte d'utilisateur	N° boîte	11 : Authentification mot de passe pour boîte d'utilisateur	OK/ECHEC
12	Changer attributs de boîte d'utilisateur par utilisateur	N° boîte	12 : Changer attributs de boîte d'utilisateur	OK
13	Accès à un document	N° boîte	13 : Accès à un document	OK
14	Supprimer document	N° boîte	14 : Supprimer document	OK
15	Changer attribut du document	N° boîte	15 : Changer attribut du document	OK
16	Authentification mot de passe pour impression confidentielle	ID utilisateur Confidentiel	16 : Authentification mot de passe pour impression confidentielle	OK/ECHEC
17	Authentification mot de passe pour impression confidentielle télécopie	N° boîte Confidentiel	17 : Authentification mot de passe pour impression confidentielle télécopie	OK/ECHEC
18	Accès à document impression confidentielle	ID utilisateur Confidentiel	18 : Accès à document impression confidentielle	OK
19	Supprimer document impression confidentielle	ID utilisateur Confidentiel	19 : Supprimer document impression confidentielle	OK
20	Créer boîte télécopie Confidentiel	N° boîte Confidentiel	20 : Créer boîte télécopie Confidentiel	OK
21	Changer mot de passe pour boîte confidentielle télécopie	N° boîte Confidentiel	21 : Changer mot de passe pour boîte confidentielle télécopie	OK
22	Changer attribut de boîte confidentielle télécopie	N° boîte Confidentiel	22 : Changer attribut de boîte confidentielle télécopie	OK
23	Accès à document dans boîte confidentielle télécopie	N° boîte confidentielle	23 : Accès à document dans boîte confidentielle télécopie	OK
24	Supprimer document dans boîte confidentielle télécopie	N° boîte confidentielle	24 : Supprimer document dans boîte confidentielle télécopie	OK

Le but de l'analyse du journal d'audit est de comprendre les éléments suivants et de prendre les mesures de protection adéquates.

Quelqu'un a-t-il accédé à des données pour les modifier, les détruire, les voler, etc. ?

Objet de l'attaque

Détails de l'attaque

Résultats de l'attaque

Pour des méthodes d'analyse plus spécifiques, reportez-vous à la page suivante.

Fonctions de sécurité de responsable (suite)

Spécification des actions non autorisées : authentification de mot de passe

Si des journaux ont ECHEC comme résultat pour des authentifications de mot de passe (ID opération : 01, 02, 11, 16, 17), il se peut que des éléments protégés par des mots de passe aient fait l'objet d'une attaque.

- Les entrées de journaux indiquant un échec d'authentification de mot de passe (ECHEC) indiquent qui a effectué l'opération et si des opérations non autorisées ont été effectuées lors de l'échec d'authentification du mot de passe.
- Même si l'authentification du mot de passe a réussi (OK), l'entrée indique si un utilisateur légitime a créé l'ID d'opération. Il est nécessaire de contrôler soigneusement ce qui s'est passé lorsqu'une authentification réussit après une série d'échecs, surtout en dehors des horaires de bureau.

Spécification des opérations non autorisées : opérations autres que des authentifications de mot de passe en accès sécurisé.

Tous les résultats d'opérations autres que des authentifications de mot de passe seront positifs (OK), il est donc nécessaire de déterminer s'il y a eu des opérations non autorisées par ID et ID d'opération.

- Étant donné que vous ne pouvez pas spécifier ce qui a été attaqué uniquement à partir de l'ID, il est nécessaire de se reporter à l'ID d'opération et au tableau de la page précédente pour déterminer si les opérations non autorisées ont été faites sur une boîte d'utilisateur, une impression confidentielle ou des données dans un boîte confidentielle de télécopie.
- Contrôlez l'heure et vérifiez si l'utilisateur du sujet en question a effectué des opérations non autorisées.

(Exemple)

Si un document enregistré dans un boîte a été imprimé à l'aide d'une autorisation frauduleuse, l'entrée de journal d'audit suivante sera créée.

1. Authentification de mot de passe pour la boîte :
ID opérations = 11
N° boîte = Boîte avec laquelle l'authentification a été faite
Résultat = OK/ECHEC
2. Accès au document dans la boîte :
ID opérations = 13
N° boîte = Boîte avec laquelle l'authentification a été faite

Vérifiez la date et l'heure à laquelle l'opération ci-dessus a été effectuée et vérifiez si l'opération sur le document dans la boîte spécifiée a été faite par un utilisateur de boîte autorisé.

Actions à prendre si des opérations non autorisées sont découvertes

- Si vous découvrez qu'un mot de passe a été découvert après analyse du journal d'audit, changez immédiatement ce mot de passe.
- Il est possible qu'un mot de passe ait été décodé et/ou modifié, et que les utilisateurs autorisés ne puissent plus accéder à une boîte. Le responsable doit contacter l'utilisateur pour voir ce qu'il en est et, si tel est le cas, le responsable doit changer le mot de passe et supprimer les données enregistrées dans la boîte.
- Si vous ne parvenez pas à trouver les documents qui devraient être dans une boîte ou si vous trouvez un document dont le contenu a été modifié, il se peut que des opérations non autorisées aient eu lieu. Des contre-mesures similaires sont nécessaires.

