KONICA MINOLTA

The essentials of imaging

bizhub PRO C5501

Guide de l'utilisateur - Sécurité

Table des matières

1 Introduction

1 Introduction

1.1 Guide de l'utilisateur – Sécurité

La version du logiciel de contrôle est la suivante.

Programme de contrôle image (Contrôle image I1) version :
A0E70Y0-00I1-G00-40

À propos de la fonction d'affichage de la version du micro-logiciel

La version du logiciel de contrôle du bizhub PRO (programme de contrôle image/Programme de commande du contrôleur) mentionnée ci-dessus peut être confirmée en sélectionnant la rubrique "08 Version logiciel" du mode Service (mode réservé au technicien).

Si vous affichez la version du micro-logiciel, la version du programme de contrôle image se présente comme suit.

Version du programme de contrôle image (Contrôle image I1) :
G00 + 2 chiffres après le tiret (p. ex. : G00-**)

Gardez ces éléments à l'esprit quand vous vérifiez la version du logiciel.

RÉFÉRENCES :

- KONICA MINOLTA, le logo KONICA MINOLTA, et "The essentials of imaging" sont des marques déposées ou des marques commerciales de KONICA MINOLTA HOLDINGS, INC.
- bizhub PRO est une marque déposée de KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

DÉCHARGE :

- Aucune partie de ce manuel ne peut être utilisée ni reproduite sans autorisation.
- Le fabricant et le revendeur ne sauraient être tenus pour responsable de la moindre influence causée par l'utilisation de ce système d'impression et de ce Guide de l'utilisateur.
- Les informations contenues au présent sont susceptibles d'être modifiées sans préavis.

1.2 Composition du Guide de l'utilisateur

Cette machine est livrée avec les Guides de l'utilisateur suivants sous forme papier.

Guide de l'utilisateur bizhub PRO C5501 – Copieur

Ce guide décrit un aperçu de la machine et des opérations de copie.

Veuillez consulter ce guide pour les informations sur la sécurité, la mise sous tension et hors tension de la machine, l'alimentation en papier, le dépannage de la machine en cas de bourrage papier par exemple et les opérations de copie disponibles sur la machine.

Guide de l'utilisateur bizhub PRO C5501 – Référence de l'administrateur POD

Ce guide vous fournit des informations détaillées sur la gestion de la machine et la manière de personnaliser la machine en fonction de votre utilisation quotidienne.

Veuillez consulter ce guide pour la configuration et la gestion de la machine ainsi que pour l'enregistrement des paramètres de papier pour copie et de magasin.

Guide de l'utilisateur bizhub PRO C5501 – Sécurité (ce manuel)

Ce guide décrit les fonctions de sécurité.

Veuillez consulter ce guide pour savoir comment utiliser le mode Sécurité renforcée et pour l'exploitation détaillée de la machine en mode Sécurité renforcée.

Pour opérer en toute sécurité, veuillez impérativement lire "Chapitre 1 Informations de Sécurité" dans le "Guide de l'utilisateur bizhub PRO C5501 – Copieur" avant d'utiliser la machine.

2 Fonctions de sécurité

2 Fonctions de sécurité

Le périphérique bizhub PRO C5501 possède deux modes de sécurité.

Copie normal

Utilisez ce mode si la machine est utilisée par une seule personne et qu'il y a une faible chance d'accès et de fonctionnement illicite. C'est le mode par défaut à la sortie de l'usine.

Pour utiliser la Copie normal, veuillez consulter le Guide de l'utilisateur de chaque machine individuelle.

Sécurité renforcée

Utilisez ce mode si la machine est connectée au sein d'un réseau local ou à des réseaux externes par l'intermédiaire d'un câble téléphonique ou d'autres moyens. Un administrateur machine gère le périphérique en fonction de ce Guide de l'utilisateur pour que les utilisateurs puissent bénéficier d'un environnement de travail sûr.
Votre administrateur machine est la seule personne habilitée à activer ou désactiver le mode Sécurité renforcée et à procéder à d'autres changements et votre technicien S.A.V. va désigner un administrateur machine.

Pour activer le mode Sécurité renforcée, le technicien S.A.V. doit définir un mot de passe d'authentification CE et un mot de passe administrateur pour le périphérique.
Veuillez contacter votre technicien S.A.V. si vous voulez utiliser le mode Sécurité renforcée.

Si vous voulez éviter que l'on accède ou que l'on manipule vos données de manière intempestive, veillez à utiliser le mode Sécurité renforcée.

L'icône Sécurité 

s'affiche sur l'écran tactile si le mode Sécurité renforcée est activé.

Environnements dans lesquels le mode Sécurité renforcée est recommandé

- La machine est surveillée par une ligne téléphonique ou un réseau.

Créer un environnement sûr

Pour votre sécurité, nous recommandons que les superviseurs et l'administrateur machine utilisent le mode Sécurité renforcée et établissent l'environnement d'utilisation suivant.

- Qualifications pour devenir administrateur machine
  Le superviseur doit déléguer l'administration du périphérique à une personne fiable possédant suffisamment de connaissances, de compétences techniques et d'expérience en tant qu'administrateur machine.
- Garantie du technicien S.A.V. (CE)
  Un superviseur ou un administrateur machine peut utiliser le mode Sécurité renforcée après avoir confirmé qu'un contrat d'entretien a été signé avec le technicien S.A.V. (CE). Indiquez clairement dans le contrat d'entretien que le technicien S.A.V. ne va pas s'engager dans des actions frauduleuses.
- Réseau local sécurisé (LAN)
  Assurez-vous que la machine est connectée au réseau local protégé par un pare-feu destiné à interdire l'accès à la machine depuis un réseau extérieur.

3 Sécurité renforcée

3 Sécurité renforcée

3.1 Description du mode Sécurité renforcée

La sécurité renforcée s'applique aux fonctions suivantes.

- Configuration carte réseau machine
  Si le mode Sécurité renforcée est activé, la seule fonction disponible est Archange.
- Interdiction d'accès extérieur
  Aucun accès n'est possible par les lignes téléphoniques, sauf Archange.
- Création, enregistrement, et analyse d'un journal des événements
  Permet de créer et d'enregistrer un historique des opérations concernant les fonctions de sécurité. La date et l'heure, les informations identifiant la personne responsable de l'opération, les détails de l'opération et les résultats de l'opération seront enregistrés afin de permettre une analyse des accès non-autorisés. Ce journal sera écrasé si la zone de rapport est supprimée.
- Identification Administrateur machine
  Un technicien S.A.V. définira les données d'identification de l'administrateur machine. L'administrateur machine doit saisir un code d'accès pour se voir autoriser l'accès. Seule une chaîne d'identification peut être enregistrée par machine.
- Mode Fonctions administrateur
  Si le mode Fonctions administrateur a été activé après l'authentification Administrateur réussie, le changement de configuration de diverses fonctions de la machine sera disponible sur la machine. Assurez-vous de bien quitter le mode Fonctions administrateur si vous quittez la machine alors que le mode Fonctions administrateur est activé.

3.2 Données protégées par le mode Sécurité renforcée

Les données protégées par le mode Sécurité renforcée sont les données documentaires enregistrées dans la machine.

Pour activer/désactiver le mode Sécurité renforcée

L'administrateur machine peut activer ou désactiver le mode Sécurité renforcée.

Si le mode Sécurité renforcée est désactivé, toutes les données sont potentiellement accessibles, alors soyez vigilants.

4 Fonctions de sécurité concernant l'administrateur machine

4 Fonctions de sécurité concernant l'administrateur machine

C'est l'administrateur machine qui active ou désactive le mode Sécurité renforcée.

Pour ce faire, il faut définir sur la machine un mot de passe d'identification CE à 8 chiffres et un code d'accès administrateur machine. Demandez à votre technicien S.A.V. de définir un code d'administrateur. Pour changer ce mot de passe, l'administrateur machine lui-même doit appliquer la procédure décrite dans le Guide de l'utilisateur Référence de l'administrateur POD.

Pour protéger les données dans la machine contre les accès non autorisés et l'altération, il est recommandé de désigner un administrateur machine et d'activer le mode Sécurité renforcée.

...

Rappel

Ne pas utiliser votre nom, date d'anniversaire, code employé, etc. pour le code d'accès, qui serait facile à retrouver pour d'autres personnes.

Veillez à ne divulguer ce code à personne ou à ne pas laisser quelqu'un d'autre en prendre connaissance.

4.1 Activer/désactiver le mode Sécurité renforcée

La section suivante décrit comment activer/désactiver le mode Sécurité renforcé.

...

Remarque

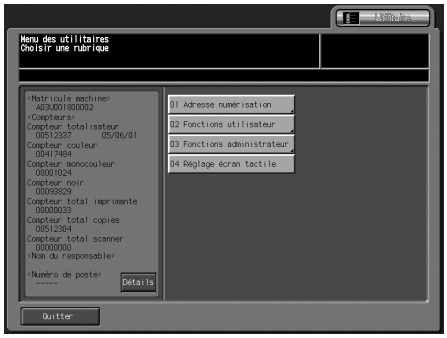
Les codes d'accès sont sensibles à la casse.

Si vous entrez un code d'accès erroné ou de moins de 8 caractères alphanumériques et que vous appuyez sur la touche [Valider], le message d'avertissement "Code erroné" apparaît, et les touches seront verrouillées pendant cinq secondes. Entrez le bon code d'accès au bout des cinq secondes.

Si l'identification se solde par un échec, les informations seront enregistrées dans le journal des événements.

1 Appuyez sur [Utilitaire/Compteur] sur le panneau de contrôle pour afficher l'écran Utilitaires.

2 Appuyez sur [03 Fonctions administrateur].

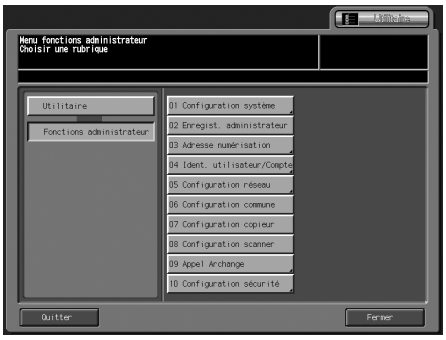


L'écran de saisie du code d'accès s'affiche.

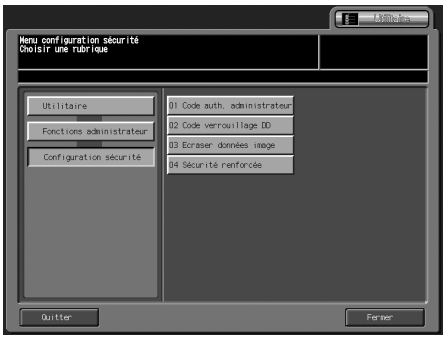
3 Entrez le code d'accès.
Sur le clavier de l'écran tactile, entrez le code d'accès Administrateur machine à 8 chiffres et appuyez sur [Valider].

L'écran Menu fonctions administrateur s'affiche.

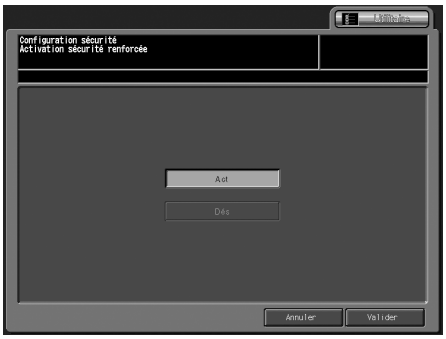
4 Sécurité renforcéeAppuyez sur [10 Configuration sécurité].



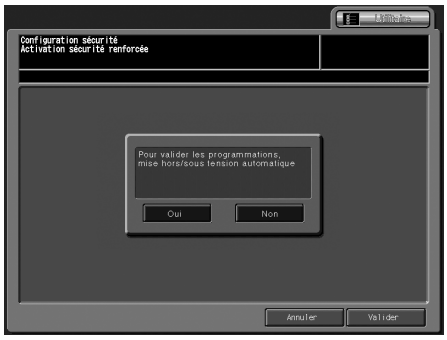
5 Appuyez sur [04 Sécurité renforcée].



6 Activez ou désactivez le mode Sécurité renforcée
Pour activer le mode Sécurité renforcée, appuyez sur [Act] pour le sélectionner. Pour le désactiver, sélectionnez [Dés].



7 Appuyez sur [Valider].



L'écran de confirmation de redémarrage s'affiche.

8 Appuyez sur [Oui].

La machine va redémarrer et la nouvelle configuration sera activée.

4.2 Code verrouillage DD

Quand le mode Sécurité renforcée est activé, un code de protection (8 à 32 caractères alphanumériques, sensibles à la casse) peut être défini sur le disque dur pour protéger les données qui y sont enregistrées.

Si vous accédez au disque dur depuis l'extérieur, la consultation des données ne sera pas possible sans la saisie du code de protection correct.

Rappel

Ne pas utiliser votre nom, date d'anniversaire, code employé, etc. pour le code d'accès, qui serait facile à retrouver pour d'autres personnes.

Veillez à ne divulguer ce code à personne ou à ne pas laisser quelqu'un d'autre en prendre connaissance.

Remarque

Le code de protection du disque dur ne fonctionne que si le mode Sécurité renforcée est activé. S'il est désactivé, le message "Veuillez activer le mode Sécurité renforcé" s'affiche.

Remarque

Les codes d'accès sont sensibles à la casse.

Si vous entrez un code d'accès erroné ou de moins de 8 caractères alphanumériques et que vous appuyez sur la touche [Valider], le message d'avertissement "Code erroné" apparaît, et les touches seront verrouillées pendant cinq secondes. Entrez le bon code d'accès au bout des cinq secondes.

Si l'identification se solde par un échec, les informations seront enregistrées dans le journal des événements.

Détails

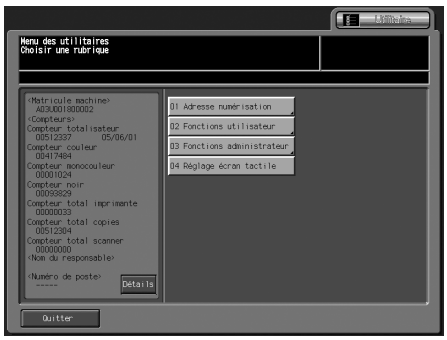
Le numéro de série de la machine sera imprimé dans le coin supérieur droit du journal des événements. Pour plus de détails, voir "Imprimer journal des événements" à la page 4-10 et "Analyser le journal des événements" à la page 4-12 pour voir un modèle du journal.

Si l'identification se solde par un échec, les informations seront enregistrées dans le journal des événements.

Le code d'accès actuel ne peut pas être réutilisé comme nouveau code d'accès.

1 Appuyez sur [Utilitaire/Compteur] sur le panneau de contrôle pour afficher l'écran Utilitaires.

2 Appuyez sur [03 Fonctions administrateur].

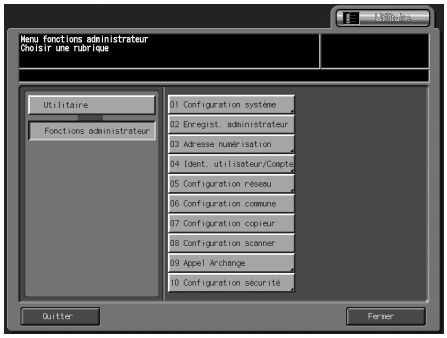


L'écran de saisie du code d'accès s'affiche.

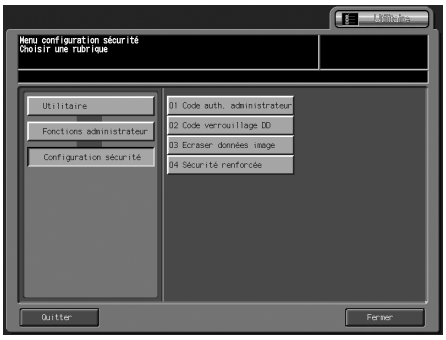
3 Entrez le code d'accès.
Sur le clavier de l'écran tactile, entrez le code d'accès Administrateur machine à 8 chiffres et appuyez sur [Valider].

L'écran Menu fonctions administrateur s'affiche.

4 Appuyez sur [10 Configuration sécurité].

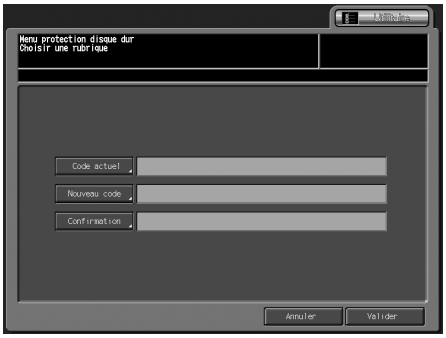


5 Appuyez sur [02 Code verrouillage DD].



L'écran Menu protection disque dur s'affiche.

6 Appuyez sur [Code actuel] pour saisir le mot de passe actuellement utilisé et appuyez ensuite sur [Valider].
Le premier mot de passe : numéro de série alphanumérique à 13 chiffres de la machine



7 En cas de réussite de l'authentification, appuyez sur [Nouveau code] pour saisir le nouveau mot de passe.
La touche ne sera pas active avant que l'authentification ne se soit soldée par un succès.

– Appuyez sur [Valider] pour revenir à l'écran précédent.

8 Appuyez sur [Confirmation] pour réintroduire le même code qu'à l'étape précédente.

– Appuyez sur [Valider] pour revenir à l'écran précédent.

9 Appuyez sur [Valider].

4.3 Imprimer journal des événements

Un journal des événements sera automatiquement créé en cas d'accès aux données archivées sur la machine.

Vous pouvez imprimer toutes les données du journal comme suit.

...

Remarque

Les codes d'accès sont sensibles à la casse.

Si vous entrez un code d'accès erroné ou de moins de 8 caractères alphanumériques et que vous appuyez sur la touche [Valider], le message d'avertissement "Code erroné" apparaît, et les touches seront verrouillées pendant cinq secondes. Entrez le bon code d'accès au bout des cinq secondes.

Si l'identification se solde par un échec, les informations seront enregistrées dans le journal des événements.

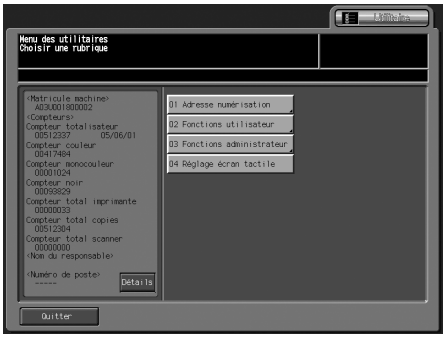
...

Remarque

Pour arrêter l'impression, appuyez sur [Arrêt] sur le panneau de contrôle, puis appuyez sur [Annuler] sur l'écran de confirmation.

1 Appuyez sur [Utilitaire/Compteur] sur le panneau de contrôle pour afficher l'écran Utilitaires.

2 Appuyez sur [03 Fonctions administrateur].

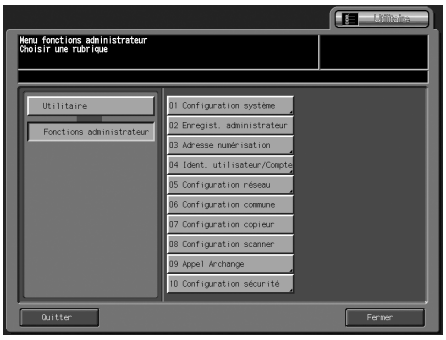


L'écran de saisie du code d'accès s'affiche.

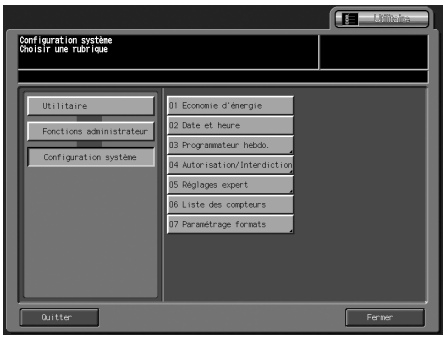
3 Entrez le [code d'accès].
Sur le clavier de l'écran tactile, entrez le code d'accès Administrateur machine à 8 chiffres et appuyez sur [Valider].

L'écran Menu fonctions administrateur s'affiche.

4 Appuyez sur [01 Configuration système].

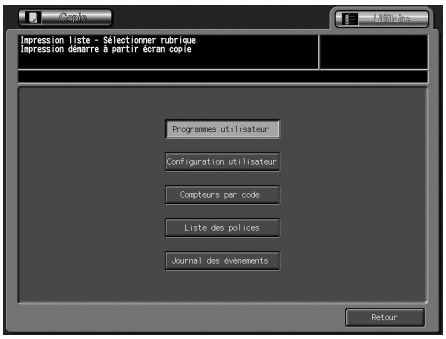


5 Appuyez sur [06 Liste des compteurs].



L'écran Impression liste s'affiche.

6 Appuyez sur [Journal des événements], et appuyez sur [Copie].



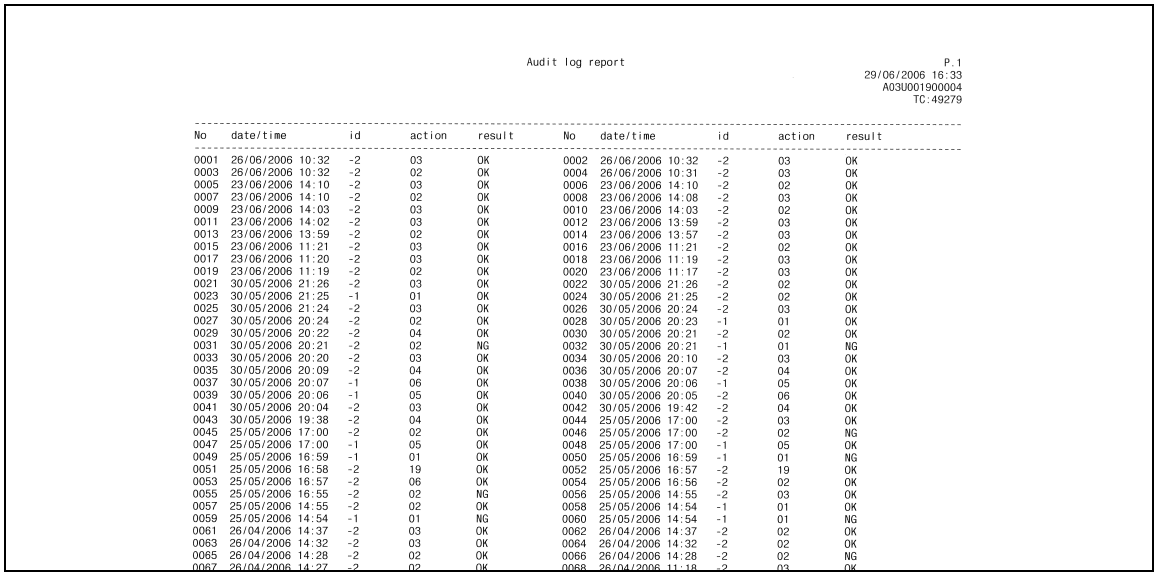
7 Appuyez sur [Départ] sur le panneau de contrôle.

4.4 Analyser le journal des événements

L'administrateur machine doit analyser régulièrement (une fois par mois) le journal des événements ou en cas de constat d'accès non autorisé ou d'altération des données enregistrées dans la machine en mode Sécurité renforcée.

La machine est prévue pour un maximum de 750 journaux par mois.

Si l'on envisage d'enregistrer plus de 750 journaux en un mois, il est recommandé d'analyser les journaux sur une période plus brève avant que le nombre des journaux non vérifiés atteigne cette limite.



Audit log report

P.1
29/06/2006 16:33
A03U001900004
TC:49279

No	date/time	id	action	result	No	date/time	id	action	result
0001	26/06/2006 10:32	-2	03	OK	0002	26/06/2006 10:32	-2	03	OK
0003	26/06/2006 10:32	-2	02	OK	0004	26/06/2006 10:31	-2	03	OK
0005	23/06/2006 14:10	-2	03	OK	0006	23/06/2006 14:10	-2	02	OK
0007	23/06/2006 14:10	-2	02	OK	0008	23/06/2006 14:08	-2	03	OK
0009	23/06/2006 14:03	-2	03	OK	0010	23/06/2006 14:03	-2	02	OK
0011	23/06/2006 14:02	-2	03	OK	0012	23/06/2006 13:59	-2	03	OK
0013	23/06/2006 13:59	-2	02	OK	0014	23/06/2006 13:57	-2	03	OK
0015	23/06/2006 11:21	-2	03	OK	0016	23/06/2006 11:21	-2	02	OK
0017	23/06/2006 11:20	-2	03	OK	0018	23/06/2006 11:19	-2	03	OK
0019	23/06/2006 11:19	-2	02	OK	0020	23/06/2006 11:17	-2	03	OK
0021	30/05/2006 21:26	-2	03	OK	0022	30/05/2006 21:26	-2	02	OK
0023	30/05/2006 21:25	-1	01	OK	0024	30/05/2006 21:25	-2	02	OK
0025	30/05/2006 21:24	-2	03	OK	0026	30/05/2006 20:24	-2	03	OK
0027	30/05/2006 20:24	-2	02	OK	0028	30/05/2006 20:23	-1	01	OK
0029	30/05/2006 20:22	-2	04	OK	0030	30/05/2006 20:21	-2	02	OK
0031	30/05/2006 20:21	-2	02	NG	0032	30/05/2006 20:21	-1	01	NG
0033	30/05/2006 20:20	-2	03	OK	0034	30/05/2006 20:10	-2	03	OK
0035	30/05/2006 20:09	-2	04	OK	0036	30/05/2006 20:07	-2	04	OK
0037	30/05/2006 20:07	-1	06	OK	0038	30/05/2006 20:06	-1	05	OK
0039	30/05/2006 20:06	-1	05	OK	0040	30/05/2006 20:05	-2	06	OK
0041	30/05/2006 20:04	-2	03	OK	0042	30/05/2006 19:42	-2	04	OK
0043	30/05/2006 19:38	-2	04	OK	0044	25/05/2006 17:00	-2	03	OK
0045	25/05/2006 17:00	-2	02	OK	0046	25/05/2006 17:00	-2	02	NG
0047	25/05/2006 17:00	-1	05	OK	0048	25/05/2006 17:00	-1	05	OK
0049	25/05/2006 16:59	-1	01	OK	0050	25/05/2006 16:59	-1	01	NG
0051	25/05/2006 16:58	-2	19	OK	0052	25/05/2006 16:57	-2	19	OK
0053	25/05/2006 16:57	-2	06	OK	0054	25/05/2006 16:56	-2	02	OK
0055	25/05/2006 16:55	-2	02	NG	0056	25/05/2006 14:55	-2	03	OK
0057	25/05/2006 14:55	-2	02	OK	0058	25/05/2006 14:54	-1	01	OK
0059	25/05/2006 14:54	-1	01	NG	0060	25/05/2006 14:54	-1	01	NG
0061	26/04/2006 14:37	-2	03	OK	0062	26/04/2006 14:37	-2	02	OK
0063	26/04/2006 14:32	-2	03	OK	0064	26/04/2006 14:32	-2	02	OK
0065	26/04/2006 14:28	-2	02	OK	0066	26/04/2006 14:28	-2	02	NG
0067	26/04/2006 14:27	-2	02	OK	0068	26/04/2006 11:18	-2	03	OK

Informations du journal des événements

Le journal des événements contient les informations suivantes.

1. date/time : date et heure de l'opération qui a généré la création d'une rubrique de journal.
2. id : vous pouvez spécifier la personne qui a effectué l'opération ou concernée par la protection sécurisée.
   "-1" : opération par le technicien S.A.V. (CE)
   "-2" : opération par l'administrateur machine.
   Autre nombre entier : indique les motifs de la protection sécurisée.
3. action : permet de spécifier l'opération.
   Vérifiez les détails de l'opération que l'action indique dans le tableau suivant.
4. result : résultat d'une opération.
   Pour l'identification par code d'accès, la réussite ou l'échec se traduiront respectivement par OK et NG.
   Pour les opérations sans identification par code d'accès, toutes les entrées de journal seront indiquées comme étant OK.

4.5 Tableau des éléments enregistrés dans le journal des événements

N°	Opération	ID	Action archivée	Résultat
1	Identification technicien	ID CE	01	OK/NG
2	Identification du responsable	ID Administrateur machine	02	OK/NG
3	Configurer/modifier mode Sécurité renforcée	ID Administrateur machine	03	OK
4	Imprimer journal des événements	ID Administrateur machine	04	OK
5	Modifier/enregistrer code d'accès technicien	ID CE	05	OK
6	Modifier/enregistrer le code Administrateur machine	ID Technicien/ID Administrateur machine	06	OK
13	Modifier le code de protection du disque dur	ID Administrateur machine	19	OK

L'analyse du journal des événements permet de prendre des contre-mesures après avoir notamment vérifié :

Si on a accédé aux données ou si elles ont été manipulées en consultant
Objet de l'attaque
Détails de l'attaque
Résultat de l'attaque
Pour les méthodes spécifiques d'analyse, voir la page suivante.

Spécifier les actions non autorisées : identification par code d'accès

Si des rapports renvoient la mention NG comme résultat de l'identification par code d'accès (action : 01, 02), les éléments protégés par des codes d'accès ont peut-être fait l'objet d'une attaque.

- Les entrées de rapport faisant état d'un échec de l'identification (NG) indiquent le responsable de l'action et montrent si des actions non autorisées ont été faites lors d'un échec de l'identification par code d'accès.
- Même en cas de réussite de l'identification par code d'accès (OK), cela montre si un utilisateur légitimé a créé l'action. Vous devez faire très attention quand l'identification réussit après une série d'échecs, surtout à des horaires autres que les horaires de travail normaux.

Spécifier les actions non autorisées : actions autres que l'identification par code d'accès en mode Sécurité

Tous les résultats d'opération autres que l'identification par code d'accès seront indiqués comme réussis (OK), il faut donc déterminer par ID et par action s'il y avait des actions non autorisées.

- Vérifiez l'heure et regardez si l'utilisateur de l'opération spécifiée a procédé à une action non autorisée.

Mesures à prendre si vous découvrez des opérations non autorisées

Si vous découvrez qu'un code d'accès a été divulgué après avoir analysé le journal des événements, modifiez immédiatement le code d'accès.

5 Index

5 Index