RICOH
imagine. change.
imaginer. changer.

Solutions de sécurité Ricoh

Version 21

Des solutions complètes et fiables pour protéger l'information sensible

Solutions de sécurité Ricoh

Ne sous-estimez pas les risques et les coûts associés au vol de renseignements

L'information est votre actif le plus précieux. Par « information », nous voulons dire les documents classifiés, confidentiels ou autrement sensibles, allant des plans d'étage d'une ambassade aux évaluations du personnel. Les risques de vols de renseignements sont bien réels. Par exemple, une étude par Verizon faite en 2011 a découvert que dans cette même année, 174 millions de dossiers numériques avaient été compromis par des intrus qui avaient eu accès aux données, soit une hausse de plus de 4 000 % par rapport à 2010.[1] Quelles soient élaborées au sein d'un gouvernement, d'une entreprise ou dans un cadre privé, il est urgent d'adopter des stratégies efficaces de protection des ressources d'information.

Bien que la technologie ait transformée les pratiques des entreprises en permettant l'échange de données presque instantané, cette dernière a entraîné de nouveaux défis en matière de sécurité. Particulièrement, les personnes qui souhaitent affaiblir vos intérêts peuvent intercepter les renseignements rapidement et facilement lorsqu'ils sont sous forme numérique. Le risque peut vous exposer à une baisse de votre avantage concurrentiel, à un litige éventuel ou miner la confiance des actionnaires. Voici la liste de quelques secteurs à risque élevé :

Secteurs à risque élevé	Renseignements vulnérables
Gouvernement fédéral	Sécurité nationale, secrets militaires et commerciaux
Financier	Fusions et acquisitions, transactions boursières
Pharmaceutique	Études cliniques, demandes de brevets, résultats financiers trimestriels
Bureau général	Listes de clients, rémunération des cadres, plans de restructuration
Haute technologie	Conception de nouveaux produits (R et D), propriété intellectuelle
Laboratoires	Méthodes d'essai, rapports de recherche
Cabinets d'avocats	Mémoires, dépositions, contrats
Comptabilité	Données d'audits, rapports financiers
Médical/hôpitaux	Facturation, dossiers médicaux

Leadership en matière de sécurité de l'information

Ricoh, une multinationale se spécialisant en technologies de bureau, en solutions d'impression de production, en systèmes de gestion de documents et en service TI, a pour mission de vous aider à résoudre les défis de sécurité de toute nature dès leur apparition. En fournissant des options de sécurité personnalisées à nos clients, nous avons mis au point une suite exhaustive de solutions de sécurité. Ces solutions aident à protéger les données imprimées et électroniques de menaces opportunistes ou ciblées, tant internes qu'externes.

En évaluant vos faiblesses, en fixant des objectifs de sécurité et en prenant les mesures appropriées, vous minimiserez le risque de graves atteintes à la sécurité tout en vous aidant à documenter vos initiatives de conformité à la sécurité.

Verizon® 2012 « Data Breach Investigations Report », une étude effectuée par l'équipe d'évaluation des risques de Verizon en collaboration avec la police fédérale d'Australie, l'unité chargé de la criminalité nationale néerlandaise, le service de sécurité de l'information et de rapports irlandais, l'unité policière centrale de la criminalité en ligne et les services secrets des États-Unis. http://www.verizonbusiness.com/resources/reports/rp_data breach investigations report 2012_en_xg.pdf

Ce guide décrit les solutions de sécurité de Ricoh conçues afin de répondre du mieux possible à vos objectifs en matière de protection de vos systèmes de bureau numériques. Cette approche multicouches aidera à fermer la porte à ceux qui souhaitent exploiter les vulnérabilités. En fait, que vos systèmes Ricoh soient réseautés ou non, ces solutions entièrement intégrées et rentables vous aideront à vous protéger contre les failles de sécurité fréquentes, sans interruptions aux flux de documents normaux (autorisés).

Guide des solutions de sécurité de Ricoh

Niveau de risque	**FAIBLE**			**ÉLEVÉ**
Couche de sécurité	**1**	**2**	**3**	**4**
Objectif de sécurité...	• Limiter l'accès aux appareils non autorisés • Contrôle de la production de l'appareil...	Plus... • Appareils en réseau sécurisés • Données d'impression en réseau sécurisées	Plus... • Données et ports physiquement sécurisés • Chiffrement des communications Web • Authentification des utilisateurs...	Plus... • Ressources de surveillance et de contrôle • Audit de l'activité de tous les appareils
Solutions de sécurité Ricoh	• Codes d'utilisateur • Impression sécurisée • Sécurité de la mémoire vive	• Codes d'utilisateur • Impression sécurisée • Sécurité de la mémoire vive • Chiffrement du disque dur • Chiffrage des données • Système DOSS • Web Image Monitor • Web SmartDeviceMonitor	• Codes d'utilisateur • Impression sécurisée • Sécurité de la mémoire vive • C hiffrage des données • Système DOSS • Disque dur amovible • Sécurité des ports réseau • Chiffrement du disque dur • Chiffrage de 128 bits sur SSL/HTTPS • Authentification NT • Web Image Monitor • Web SmartDeviceMonitor	• Codes d'utilisateur • Impression sécurisée • Sécurité de la mémoire vive • SmartDeviceMonitor • Chiffrage des données • Système DOSS • Disque dur amovible • Sécurité des ports réseau • Chiffrement de 128 bits sur SSL/HTTPS • Authentification NT • Contrôle de l'impression et de la copie • Web Image Monitor • Web SmartDeviceMonitor • Chiffrement du disque dur • IPv6 • Kerberos • Impression verrouillée améliorée • Print Copy Scan (PCS) Director • Trousse d'authentification par carte

Solutions de sécurité Ricoh

Limiter l'accès non autorisé aux appareils

Codes d'utilisateur
Des codes d'utilisateur (standard dans la plupart des systèmes de Ricoh) permettent aux gestionnaires de système de gérer et de suivre l'utilisation des appareils d'impression numérique Ricoh. Un code d'utilisateur peut être attribué à quelqu'un selon les fonctions auxquelles on l'autorise à accéder. Ce niveau de contrôle vous permet de surveiller l'utilisation du système (p. ex. produire des rapports sur le nombre d'impressions par fonction et par code d'utilisateur).

Contrôle de la production de l'appareil

Impression verrouillée
L'impression verrouillée (offerte sous les pilotes d'impression avancées de Ricoh) conserve la confidentialité en retardant l'impression d'un document jusqu'à ce que l'utilisateur autorisé (auteur/créateur) entre son NIP (numéro d'identification personnel) au panneau de commande de l'appareil. Cela élimine la possibilité que des gens volent un document ou le retirent du bac de papier. (L'impression verrouillée exige l'installation d'un disque dur, qui peut être optionnel sous certains modèles.)

Chiffrement par mot de passe de l'impression verrouillée
En tant que nouvelle fonction, le mot de passe utilisé pour l'impression verrouillée peut être chiffré afin d'aider à protéger contre le branchement clandestin.

Enhanced Locked Print (impression verrouillée améliorée)
Enhanced Locked Print vous permet de profiter des avantages d'un appareil multifonction centralisé partagé sans compromettre la sécurité des documents. Les utilisateurs archivent, récupèrent et gèrent les documents confidentiels à l'aide d'un nom d'utilisateur et d'un mot de passe. Il s'agit d'une solution rapide et simple pour protéger les données confidentielles et exclusives de votre entreprise.

- L'utilisateur peut envoyer de façon sécuritaire des documents à une imprimante où ils sont retenus jusqu'à ce que l'utilisateur autorisé les imprime.
- Les documents ne peuvent être recueillis à l'imprimante par un autre utilisateur, ce qui en protège la confidentialité.
- Les documents stockés à l'imprimante sont chiffrés (l'information ne peut pas être compromise si le disque dur est volé).
- Enhanced Locked Print est installé sous l'appareil multifonction soit par logiciel intégré (carte SD) soit à distance par interface Web.
- Les administrateurs et les utilisateurs peuvent configurer Enhanced Locked Print à l'aide d'une interface de type fureteur Web.

Sécurité de la mémoire vive
Certains systèmes MFP de Ricoh utilisent la mémoire vive (RAM) et non le disque dur pour les tâches de traitement de documents par copieur. Bien qu'un disque dur soit offert en option, la sécurité est mieux assurée par une configuration de base dans laquelle les travaux traités passent par une mémoire vive volatile (qui efface l'information dès que le système est éteint). Ne pouvant stocker les données de façon permanente comme cela se fait lorsqu'il y a un disque dur, l'appareil ne présente pas une menace grave pour la sécurité des données. Ainsi, ces systèmes MFP sont tout désignés pour les environnements à faible volume où la sécurité des informations est une priorité absolue.

Appareils en réseau sécurisés

SmartDeviceMonitor (pour Admin*)
SmartDeviceMonitor est un utilitaire compris avec toutes les imprimantes Ricoh, les appareils multifonctions avec fonction d'impression et la trousse imprimante/numériseur. Cette suite logicielle polyvalente simplifie l'installation, le suivi et la gestion des systèmes de production en réseau Ricoh, tout en prenant en charge les principales caractéristiques de sécurité.

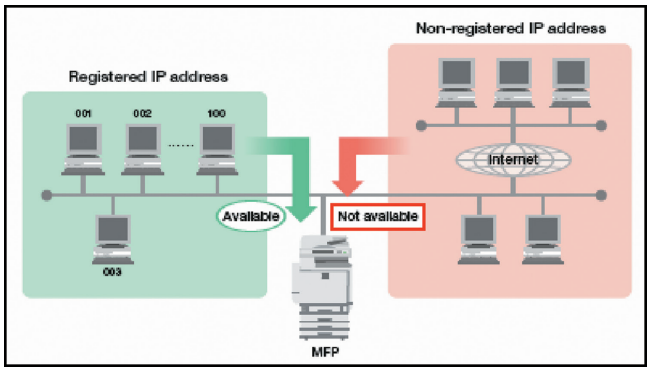
- **Modifier le nom de communauté**
  Afin de pallier les vulnérabilités de SNMP (Simple Network Management Protocol), l'administrateur système peut modifier le nom de communauté des appareils Ricoh de « Public » à tout autre nom plus sécurisé. Lorsque cette mesure de sécurité est prise, le nom de communauté (du logiciel) doit être le même que celui de l'appareil de production Ricoh en réseau.
- **Limiter l'accès des utilisateurs**
  Les administrateurs système peuvent contrôler les privilèges des utilisateurs grâce à l'outil de gestion des utilisateurs. Ceci active un menu qui affiche les périphériques autorisés par code et nom d'utilisateur. Tous les périphériques Ricoh compatibles sous le réseau sont énumérés et en cliquant l'appareil, on accède à un menu qui limite ou permet l'accès à l'appareil pour chaque utilisateur.

Web Image Monitor
Web Image Monitor est un utilitaire Web intégré de gestion d'appareils.

- **Établir l'intervalle d'adresses IP (filtre IP)**
  Les administrateurs systèmes peuvent restreindre les hôtes des adresses IP appartenant à un certain intervalle de se connecter au contrôleur d'impression. Les commandes ou les tâches qui proviennent d'adresses IP non autorisées sont alors ignorées par le contrôleur d'impression.
- **Sécurité des ports réseau**
  L'administrateur système peut activer ou désactiver les ports IP, contrôlant de la sorte des services en réseau offerts par le contrôleur d'impression à l'utilisateur.

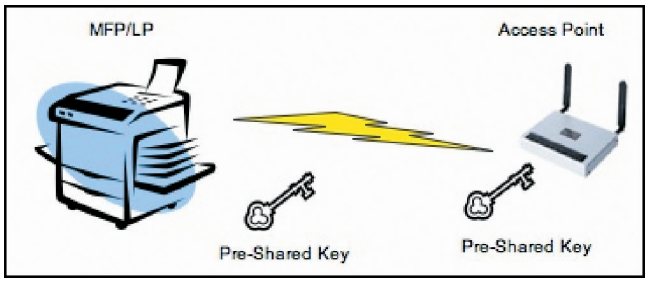
* Remarque: SmartDeviceMonitor pour Admin est hébergé sur le bureau client et permet aux utilisateurs d'établir le statut et la disponibilité des périphériques Ricoh en réseau. Lorsqu'il est installé, une icône apparaît sur le bureau de l'utilisateur sous la barre de tâches Windows, qui permet de vérifier l'état du système en un coup d'œil.

Filtrage d'adresses IP (protocole Internet)
Dans un réseau LAN, chaque ordinateur réseauté possède une adresse IP qui représente son numéro de matériel unique. Tout comme les adresses de résidence ayant un numéro d'immeuble ou d'appartement, cela permet de router les courriels et les pièces jointes, d'acheminer les télécopies au bon destinataire et d'envoyer des données d'impression aux appareils de production en réseau depuis un PC expéditeur. La capacité des appareils Ricoh à bloquer ou limiter un utilisateur ou un groupe d'utilisateurs selon l'adresse IP améliore la gestion des PC et des utilisateurs, aide à répartir le volume entre les divers appareils et rehausse la sécurité réseau en limitant l'accès aux fichiers sauvegardés sous les appareils.



Registres de tâches / registres d'accès
Une liste exhaustive de tous les travaux réalisés par l'appareil est sauvegardée en mémoire. On peut consulter cette liste sous Web SmartDeviceMonitor afin de surveiller l'utilisation de l'appareil par tâche ou par utilisateur. Lorsqu'elle est utilisée de pair avec les modes d'authentification des utilisateurs externes, il est possible de déterminer quel utilisateur abuse de l'appareil. Il est également possible de déterminer quel appareil a été utilisé et par qui en faisant le suivi d'une transmission non autorisée.

Prise en charge WPA (accès Wi-Fi protégé)
Utilisée de pair avec l'option le LAN sans fil IEEE 802.11a/b/g, WPA est une norme de sécurité qui corrige certaines lacunes des communications sans fil. Elle procure un sentiment de tranquillité aux entreprises, aux petites entreprises et même aux utilisateurs à la maison à l'effet dont les données sont protégées en ne donnant accès à leur réseau qu'aux utilisateurs autorisés. Les caractéristiques d'authentification et de chiffrement «Personal» et «Enterprise» bloquent les intrusions à partir de portables sans fil dans tout environnement, prévenant l'interception des trains de données et des mots de passe ou l'utilisation d'une connexion sans fil comme point d'entrée dans le réseau de données du client.



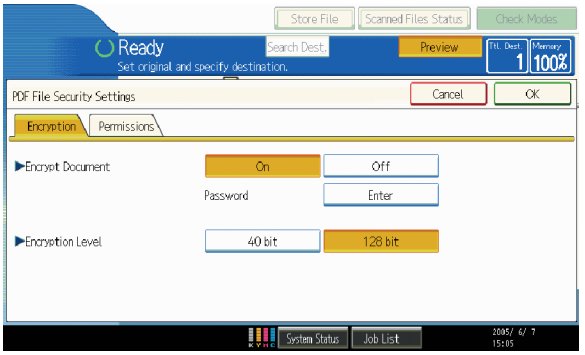
Authentification filaire 802.1X
802.1X offre l'authentification au port réseau pour les communications point à point entre les appareils en réseau et un port LAN En offrant une connexion point à point à un port LAN, la communication est désactivée lorsque l'authentification est refusée.

Chiffrage des données
Lorsque des données critiques traversent le réseau, il est possible qu'un pirate intercepte le train de données brutes et les mots de passe. L'arrivée de la technologie réseau sans fil, quoiqu'elle s'avère très commode pour la navigation et l'impression pour des millions d'utilisateurs, expose aussi les réseaux aux attaques d'intrus munis de portables sans fil par tout point d'accès dans leur rayon. Sans protection, l'information intelligible peut facilement être volée ou modifiée puis réintégrée au réseau. Les appareils Ricoh sont munis des capacités de chiffrement suivantes afin de vous aider à réduire le niveau de risque.

Solutions de sécurité Ricoh

Chiffrement du répertoire d'adresses
Le chiffrement du répertoire d'adresses protège les informations de contact en chiffrant les données sauvegardées sous le répertoire du système. Même si le disque dur est retiré de l'appareil, les données sont illisibles. Cette fonction élimine le risque que les employés, les clients ou les fournisseurs d'une entreprise ou d'un service soient la cible de courriels malveillants ou que leur ordinateur soit contaminé par un virus. De plus, puisque les données de répertoire correspondent généralement aux noms et aux mots de passe d'utilisateurs qui sont aussi utilisés ailleurs sous le réseau, la protection du répertoire d'adresses d'une imprimante ou d'un appareil multifonction rehausse la sécurité du réseau dans son ensemble.

Transmission PDF chiffrée
Le format PDF d'Adobe est devenu la norme universelle pour la création de documents qui peuvent être ouverts et partagés par tout utilisateur, peu importe la plateforme. Adobe fournit gratuitement l'application Acrobat® Reader® en téléchargement. Un fichier PDF est en fait le cliché d'un document. Il ne peut être modifié (à moins d'utiliser l'application Adobe Acrobat complète) et est donc intéressant pour les auteurs qui veulent partager leurs documents approuvés tout en limitant les modifications. Une autre caractéristique intéressante du format PDF est le fait que la taille des fichiers est grandement réduite par rapport aux fichiers d'origine, ce qui les rend plus faciles à transmettre par courriel.



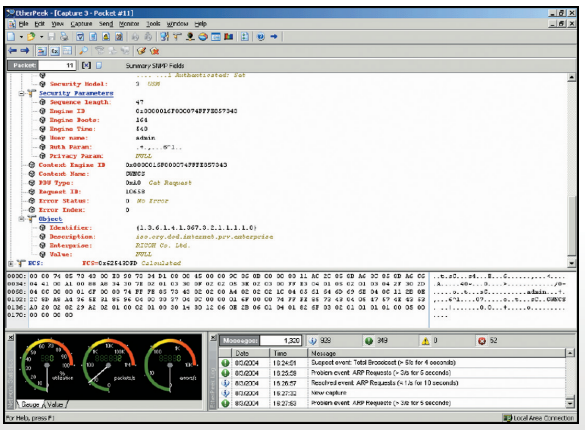
Quoiqu'Adobe offre certaines caractéristiques de sécurité intégrées à l'application Acrobat pour verrouiller les documents et les protéger à l'aide de mots de passe, rien n'empêche les fichiers d'être interceptés en format déchiffrable sur le réseau. Voilà où la fonction de transmission PDF chiffrée de Ricoh ajoute de la valeur en brouillant et en chiffrant les données qui seraient autrement parfaitement transparentes pendant la transmission. L'utilisateur peut opter pour le chiffrement de 40 bits ou de 128 bits et peut fixer les droits du destinataire quant à la révision du document ou à l'extraction de contenu. (Voir aussi le chiffrement du mot de passe PDF.)

Chiffrement du disque dur (DD)
Cette fonction peut chiffrer le disque dur du système afin de protéger contre le vol des données. Même si le disque dur est volé, les données ne sont pas divulguées. La méthode de chiffrement utilisée est la norme AES (Advanced Encryption Standard) à 256 bits.

Clé de chiffrement du pilote
Les appareils Ricoh offrent cette caractéristique qui chiffre le mot de passe d'authentification de l'utilisateur lorsque ce dernier utilise les pilotes PCL ou RPCS afin que des intrus ne puissent avoir accès au système en utilisant un mot de passe volé.

Chiffrement du mot de passe PDF
Cette fonction corrige une vulnérabilité des transmissions PDF chiffrées où le mot de passe de l'utilisateur est clairement indiqué dans la fenêtre. Cette fonction chiffre les mots de passe allant jusqu'à 32 caractères pour une transmission et un stockage plus sécurisés des fichiers PDF. L'affectation d'un mot de passe de groupe pour l'appareil destinataire et les PC branchés se fait par DeskTopBinder Lite.

Communication chiffrée SNMP v3
Simple Network Management Protocol version 3 (SNMP v3) est une norme de gestion de réseau couramment utilisée dans les environnements TCP/IP. SNMP procure une méthode de gestion des hôtes comme les imprimantes, les numériseurs, les postes de travail et les serveurs et regroupe les ponts et les pivots au sein d'une «communauté» depuis un ordinateur central qui héberge le logiciel de gestion du réseau. Il permet par exemple aux administrateurs de modifier les paramètres des appareils à l'aide de SmartDeviceMonitor depuis un PC en réseau. Les communications chiffrées vous aident à maintenir la sécurité de l'environnement.



Les versions précédentes (v1 et v2) de SNMP servaient à configurer et à surveiller les appareils à distance. La dernière version, SNMP v3, affiche des améliorations à l'authentification des utilisateurs et au chiffrement des données qui rehaussent la sécurité pour mieux protéger les données et les réseaux. En activation, SNMP v3 empêche les utilisateurs non autorisés de voir le mot de passe ou le contenu d'un fichier en format texte lisible, protégeant ainsi des informations précieuses.

Kerberos
Kerberos est un protocole d'authentification en réseau conçu pour renforcer l'authentification des applications clients/serveurs en implantant une cryptographie à clé secrète. Plusieurs protocoles Internet ne protègent pas les mots de passe. Les pirates utilisent des logiciels appelés « renifleurs » pour extraire les mots de passe et ainsi accéder aux réseaux. La transmission d'un mot de passe non chiffré sur un réseau peut donc le rendre vulnérable à des attaques. L'authentification Kerberos limite les risques reliés aux mots de passe non chiffrés et sécurise les réseaux.

Communication IPSec
IPsec (IP security) est une suite de protocoles pour sécuriser les communications IP (Internet Protocol) en authentifiant ou en chiffrant chaque paquet IP dans un train de données. IPsec comprend aussi des protocoles pour établir des clés de chiffrement. Les entreprises qui ont besoin d'un niveau élevé de sécurité munissent leurs réseaux d'IPsec pour protéger les données. Ces entreprises utilisent aussi IPsec pour l'impression.

S/MIME pour Scan to E-mail
S/MIME (Secure/Multipurpose Internet Mail Extensions) est une norme de chiffrement à clé publique et de signature de courriels encapsulée sous MIME (Multipurpose Internet Mail Extensions). MIME est une norme Internet qui étend le format des courriels afin qu'ils puissent prendre en charge les textes en jeu de caractères autre que US-ASCII, les pièces jointes qui ne sont pas des textes, les corps de message en plusieurs parties et les entêtes en jeu de caractères autre qu'ASCII.

Cette fonction est utilisée pour chiffrer les données confidentielles transmises sous Scan to E-mail afin de protéger les données d'un branchement clandestin.

Données d'impression en réseau sécurisées

Chiffrement des données par IPP
Un autre excellent moyen d'aborder la sécurité des données est le chiffrement. À l'aide de l'utilitaire pour client, SmartDeviceMonitor de Ricoh, les données d'impression peuvent être chiffrées sous Secure Sockets Layer/Transport Layer Security (SSL/TLS) par Internet Printing Protocol (IPP), ce qui sécurise les données entre les postes de travail et les imprimantes et appareils multifonctions du réseau. (Le protocole TLS aide à garantir la confidentialité et l'intégrité des données entre les applications client/serveur qui communiquent entre elles sur Internet.) Cela veut dire que toute tentative d'exploiter des données d'impression échouera, c.-à-d. les données interceptées sont indéchiffrables. Veuillez vérifier la compatibilité des modèles dans les tableaux de caractéristiques des produits ci-inclus.

Suppression des données latentes

Système de sécurité par écrasement des données (DOSS) :
Afin d'empêcher la perte des données, les mesures de sécurité de l'information d'une entreprise devraient inclure une technologie qui supprime les images numériques latentes sous le disque dur de l'appareil multifonction. Le système de sécurité par écrasement des données de Ricoh parvient à ce but en supprimant les données temporaires stockées sous le disque dur de l'appareil multifonction par écrasement de l'image latente avec des séquences aléatoires de « 1 » et de « O. ».

- Le processus d'écrasement des données aléatoire de Ricoh en trois étapes rend pratiquement impossible l'accès aux fichiers de copie et d'impression stockés et leur reconstruction
- S'utilise avec le système de disque dur amovible, offrant ainsi une approche multicouche à la sécurité des documents sensibles
- Une icône s'affiche sur l'écran indiquant que le processus est en cours ou terminé.
- Se conforme aux méthodes recommandées par la National Security Agency (NSA) pour la gestion de l'information classifiée.
- **Soutien les clients avec leur conformité aux exigences des normes HIPAA, GLBA et FERPA**
- DOSS de type A, B, C, D, F, H et I est certifié ISO 15408 à un niveau d'évaluation d'assurance 3

Exigences de conformité aux lois sur la sécurité
Les entreprises qui utilisent et stockent certaines données sensibles telles que des renseignements médicaux, financiers ou certains types de renseignements qui identifient personnellement les individus peuvent faire l'objet d'exigences réglementaires incluant la **Health Insurance Portability and Accountability Act (HIPAA), la Gramm-Leach-Bliley Act (GLB) ou la Family Education Rights Privacy Act**. Bien qu'aucun système ne puisse garantir de façon absolue la sécurité des données, l'utilisation de solutions Ricoh comme DOSS et l'option de disque dur amovible peut aider les clients à faire face aux risques que posent les données latentes sensibles.

Solutions de sécurité Ricoh

Données et ports physiquement sécurisés

Systèmes de disque dur amovible (RHD)
Commode et facile à utiliser, le système de disque dur amovible de Ricoh interface avec le disque dur de série d'un système numérique. Cette solution dote le disque dur interne d'un boîtier externe rigide muni d'un système de verrouillage à clé. Un système d'étiquetage à numéros permet de repérer facilement le disque dur en entreposage ou lorsqu'on le replace dans l'appareil. Un étui rembourré antistatique est inclus pour protéger le disque dur pendant le transfert et l'entreposage.

Afin d'offrir encore plus de sécurité et de polyvalence dans le traitement de documents classifiées et non classifiés, on peut obtenir un disque dur amovible supplémentaire en option. Les systèmes numériques de Ricoh peuvent donc travailler avec deux disques durs amovibles interchangeables : l'un pour les documents classifiés et l'autre pour les documents non classifiés. Lorsque les documents classifiés sont copiés ou imprimés, le disque dur peut être retiré et placé dans un endroit sûr tandis que l'autre disque dur peut être inséré.

- Le disque dur amovible est entreposé en un lieu accessible pour en faciliter la récupération et l'entreposage avec autorisation.
- Maximise la sécurité en séparant physiquement les données de l'appareil, empêchant de la sorte l'accès aux données latentes.
- Les systèmes de Ricoh à disque dur amovible n'affectent en rien les fonctions de copie, d'impression et de numérisation des appareils.
- Fonctionne de pair avec le système de sécurité par écrasement des données de Ricoh, offrant une approche multicouche à la protection des documents sensibles.
- Les fonctions disponibles lorsque le disque dur amovible est installé incluent la copie, l'impression, la numérisation et le serveur de documents*. Lorsqu'un disque dur amovible est installé, l'option de télécopie n'est pas disponible.

***Serveur de documents :** capacité que possèdent certains systèmes de production Ricoh de stocker les tâches sur le disque dur du système (numérisation, impression, télécopie ou copie); supporte aussi l'impression de documents sécurisée.

Sécurité des ports réseau
Généralement, les systèmes prêts à mettre en réseau sont livrés au client avec tous les ports « ouverts » afin de faciliter leur ajout aux réseaux. Si cela facilite l'installation de ces systèmes, cela pose aussi un risque au niveau de la sécurité.

Afin de rehausser la sécurité du réseau, le gestionnaire peut désactiver un protocole comme SNMP ou FTP à l'aide de Web Image Monitor ou de SmartDeviceMonitor. Cela empêche le vol des noms et mots de passe des utilisateurs, en plus d'aider à éliminer les menaces externes comme la destruction/falsification de données stockées, les attaques pour déni de service (DoS) et les virus qui peuvent pénétrer le réseau par un port d'imprimante ou d'appareil multifonction inutilisé.

Chiffrement de la communication des données

Chiffrement de 128 bits sur SSL
GlobalScan et DocumentMall prennent tous deux en charge le chiffrement de 128 bits sur SSL (Secure Sockets Layer). La technologie SSL utilise une clé privée pour chiffrer les données numérisées de l'appareil MFP Ricoh au serveur GlobalScan ou DocumentMall, créant de la sorte une connexion sécurisée. Toute URL (Uniform Resource Locator) qui a besoin d'une connexion SSL, comme GlobalScan et DocumentMall, commencera avec https:, le « s » signifiant « sécurisé ».

Authentification des utilisateurs

Prévention de l'utilisation non autorisée des systèmes :
L'authentification est une caractéristique de sécurité des appareils multifonctions qui empêche les utilisateurs ou les groupes d'utilisateurs non autorisés d'avoir accès aux fonctions du système ou de modifier les paramètres. Cette importante capacité permet à l'administrateur système de gérer les droits d'accès et de protéger les fonctions de base installées sur votre MFP contre une utilisation trafiquée non approuvée.

- **L'authentification de l'utilisateur** vous permet de limiter l'accès à l'équipement à ceux qui ont un nom d'utilisateur et un mot de passe valides.

GlobalScan est une solution Web de gestion de documents et de contenu qui permet à certains systèmes Ricoh d'effectuer des fonctions de numérisation réseau, particulièrement « scan-to-email ou folder », ainsi qu'effectuer des fonctions de gestion de document, de télécopie et de ROC au moyen de plugiciels facultatifs. Ce puissant système de distribution et de saisie de documents papier facile à utiliser s'intègre harmonieusement à votre infrastructure de courrier existante afin de propulser la productivité de votre groupe de travail en combinant la fonction de numérisation dans une plateforme de copieur accessible.
Les fonctions de sécurité avancée de GlobalScan incluent : Secure LDAP, Secure SMTP, authentification Kerberos et les PDF protégés par mot de passe.

DocumentMall, une application peu dispendieuse et munie de plusieurs fonctions de sécurité, offre via Internet un accès sécurisé à vos documents à partir de partout au monde, 24 heures par jour, 7 jours par semaine, permettant ainsi de partager et de collaborer facilement entre frontières dispersées géographiquement.

- **L'authentification Windows** vérifie l'identité de l'utilisateur de l'appareil multifonction en comparant les données de connexion (nom/mot de passe de l'utilisateur) à la banque de données d'utilisateurs autorisés sous le serveur réseau Windows, afin d'accorder ou d'interdire l'accès aux fonctions de l'appareil multifonction.
- **L'authentification LDAP** valide l'utilisateur auprès du serveur LDAP (Light-weight Directory Access Protocol), ne donnant accès au répertoire d'adresses qu'aux utilisateurs entrant un nom/mot de passe valide pour trouver et sélectionner des adresses courriel stockées sous le serveur LDAP.
- **Authentification de l'administrateur** – l'administrateur gère les paramètres du système et l'accès des utilisateurs aux fonctions de l'appareil multifonction. Jusqu'à quatre gestionnaires peuvent partager les tâches d'administration, ce qui permet de répartir la charge de travail et de limiter les opérations non autorisées par un seul gestionnaire, quoiqu'une même personne puisse assumer tous les rôles. De plus, un rôle de superviseur peut être créé pour établir ou modifier les mots de passe des gestionnaires.
- **Authentification de base** - authentifie l'utilisateur à l'aide du nom/mot de passe enregistré sous le répertoire d'adresses de l'appareil multifonction. Une personne sans nom/mot de passe valide ne peut accéder à l'appareil.
- **Authentification du code d'utilisateur** - utilise le système de code d'utilisateur de série de Ricoh pour authentifier l'utilisateur. L'opérateur de l'appareil multifonction n'a qu'à entrer son code d'utilisateur, qui est comparé aux données enregistrées dans le répertoire de l'appareil multifonction. Une personne sans nom/mot de passe valide ne peut accéder à l'appareil. L'authentification de base et l'authentification du code d'utilisateur peuvent être utilisées dans les environnements autres que Windows et les bureaux qui ne sont pas en réseau.
- **Authentification CAC de l'US Department of Defense** - Common Access Card (CAC) est un système spécialisé d'authentification par carte d'identité de l'US Department of Defense (DoD) conçu pour les utilisateurs du gouvernement qui doivent se conformer à la directive présidentielle 12 du Homeland Security (HSPD-12). Cette directive oblige les employés et les sous-traitants du gouvernement fédéral à rehausser la sécurité de façon efficiente en réduisant la fraude liée à l'identité grâce a à une plus grande protection des renseignements personnels. Les seuls clients utilisant la solution d'authentification CAC de Ricoh est l'U.S. Department of Defense (DoD) [forces terrestres, navales et aériennes, Marines, garde côtière et agences affiliées].
- La **Personal Identity Verification (PIV)** est la version civile de la carte CAC du gouvernement américain.
- La **solution d'authentification par jeton SIPRNet** est la version pour les réseaux contrôlés.

Ressources de surveillance et de contrôle

Print Copy Scan (PCS) Director

Print Copy Scan (PCS) Director est une solution de gestion de l'impression complète qui permet aux utilisateurs d'analyser, de comprendre et, finalement, d'économiser sur les coûts associés à l'impression et la photocopie. Cette solution peut être mise en place pour surveiller les activités d'impression des services ou de l'entreprise, limiter le nombre d'impressions et de copies qu'un utilisateur peut faire, ainsi que renforcer des méthodologies d'impression basées sur des règles afin de réduire le coût total de propriété.

Print Copy Scan (PCS) Director identifie et contrôle le coût de l'impression à l'échelle de l'entreprise.

Audit de l'activité de tous les appareils

Print and Copy Control v3 de Ricoh pour Equitrac Office et Express

Ricoh Print and Copy Control permet au client de mieux contrôler l'accès et de surveiller les données de copie/impression à l'aide d'un logiciel intégré au disque dur de certains systèmes de production Ricoh. Au nombre des avantages :

Options d'authentification sécurisées

Protégez les données sensibles et prévenez l'utilisation non autorisée à l'aide de la méthode d'authentification qui correspond aux besoins de votre entreprise.

- Simplicité et sécurité. Les employés accèdent à l'appareil multifonction en utilisant leur badge d'identité d'entreprise et des lecteurs de cartes optionnels qui s'installent en quelques minutes. Ricoh PCC prend en charge MIFARE®, Legic®, HID® Prox (125 KHz) et les cartes à bande magnétique.
- Accès commode personnalisé. Surveillez la production de documents à l'aide de l'accès NIP sécurisé – par utilisateur, par projet ou même par équipe de travail.
- Accès instantané à l'échelle de l'entreprise. L'utilisateur entre son identité réseau existante et son mot de passe pour « déverrouiller » l'appareil multifonction.

Convivial et sécurisé

- Impression commode et sécurisée. La production de documents Follow-You™ vous permet de produire des documents à partir de tout appareil MFP en réseau, ce qui permet d'éviter les appareils achalandés ou non disponibles et d'imprimer au besoin dans diverses divisions, étages ou édifices.
- Contrôle minuté. Le gestionnaire peut programmer la suppression automatique de toutes les tâches du serveur à une heure déterminée.
- Sécurité renforcée. Les travaux sont conservés sous un serveur sécurisé et non pas sous le disque dur du système. Les documents ne sont produits qu'après libération par l'utilisateur, ce qui évite qu'un document traine à un appareil.

Solutions de sécurité Ricoh

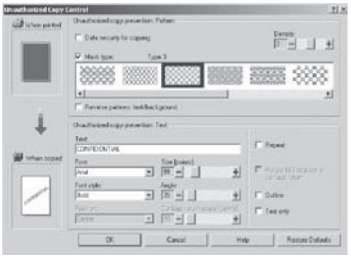
Contrôle des copies non autorisées

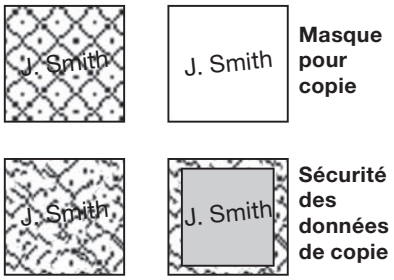
Le pilote d'imprimante de Ricoh offre une caractéristique unique qu'aucun autre fabricant n'offre, le contrôle des copies non autorisées. Cette fonction intègre des motifs et du texte sous le texte imprimé, ce qui contribue à éliminer le risque de copie non autorisée de documents sensibles.

Cette nouvelle fonction est idéale pour les petites entreprises qui utilisent le système principalement pour la télécopie, la copie et l'impression, soit des entreprises qui copient des rapports de personnel, des régimes de rémunération, des dossiers médicaux, des rapports financiers, etc.

Le contrôle des copies non autorisées comprend deux fonctions :

1. Masque pour copie[2] – une caractéristique standard qui intègre un masque et un message dans l'impression d'origine. Ce message apparait lorsque l'on fait des copies sous un système numérique Ricoh ou concurrent; le nom de l'auteur, par exemple, permettrait d'identifier l'émetteur.
2. Sélectionnez la sécurité des données de copie[1] pour que toutes les copies produites avec un MFP muni d'une unité de sécurité des données de copie soient grisées, laissant une marge de 0,16 po (4 mm) de motif de masquage.





Remarques :

[1] Unité de sécurité des données de copie facultative requis. N'est pas compatible avec certaines configurations comprenant la télécopie. Un ratio de réduction de copie de moins de 50 % sera désactivé.

[2] Certains appareils MFP numériques peuvent ne pas détecter les modèles de masquage.

Impression obligatoire des renseignements sur la sécurité

La fonction d'impression obligatoire des renseignements sur la sécurité comprend de l'information sur la personne ayant imprimé le document, quand et à partir de quel appareil.

Le type de renseignements sur la sécurité inclus avec l'impression obligatoire des renseignements sur la sécurité comprend :

- La date et l'heure auxquelles la tâche a été imprimée
- Le nom ou les données de connexion de l'utilisateur qui a imprimé la tâche
- Adresse IP de l'appareil ayant imprimé la tâche
- Numéro de série de l'appareil ayant imprimé la tâche

Les administrateurs peuvent sélectionner quel type de renseignement devrait être imprimé sur le document produit. La position d'impression peut être modifiée pour le coin supérieur gauche, supérieur droit ou inférieur gauche. (Réglage par défaut : inférieur droit.)

Fonctions de sécurité des télécopieurs commerciaux pour le bureau général

Télécopieur commercial autonome

Accès restrictif

L'option d'accès restreint vous permet de surveiller de près l'utilisation des appareils et de dissuader les passants d'utiliser l'appareil. Les utilisateurs autorisés doivent entrer un code avant de pouvoir utiliser l'appareil. En outre, cette fonction peut être reliée à la caractéristique « minuterie mode nuit » afin que l'accès restreint soit en marche ou éteint durant certaines heures, empêchant ainsi l'accès après les heures de bureau.

Authentification du serveur de domaine

Lorsque la sécurité et le suivi des utilisateurs deviennent un problème pour les gestionnaires des TI, l'authentification du serveur de domaine est standard sur le FAX4430NF et le FAX5510NF*. L'authentification limite l'accès aux systèmes de télécopie, ce qui augmente la sécurité puisque l'utilisation de l'appareil est surveillée. Seulement les utilisateurs ayant un compte de contrôleur de domaine Windows peuvent accéder à l'appareil. L'authentification du serveur limitera l'accès au télécopieur non seulement pour la fonction scan-to-email, mais aussi pour la fonction standard de télécopie, et de télécopie par IP et télécopie LAN.

Protection par NIP de sécurité
Afin d'empêcher l'exposition d'un NIP ou d'un no d'identité personnel, tout caractère après une certaine position dans le numéro du destinataire sera masqué sur l'affichage et dans le rapport de communications.

Réseau fermé
Avec le réseau fermé, les codes ID des appareils communicants sont vérifiés. S'ils ne sont pas identiques, la communication est terminée, empêchant ainsi la transmission possible, intentionnellement ou accidentellement, de documents confidentiels aux mauvais endroits, p. ex. à l'extérieur du réseau. (Remarque : les réseaux fermés exigent que tous les systèmes de télécopie soient des systèmes Ricoh ayant la faculté de fonctionner avec un système fermé)

Transmission et réception confidentielles
Cette caractéristique permet à l'utilisateur de transmettre et de recevoir à une boîte de réception protégée par un mot de passe. Les messages sont imprimés uniquement après que le destinataire entre le bon mot de passe, ce qui offre ainsi un niveau de sécurité accru lors de communication entre appareils.

Mémoire verrouillée
Lorsque la mémoire verrouillée est activée, les documents provenant de tous les expéditeurs (ou d'expéditeurs particuliers) sont retenus dans la mémoire. Lorsque le no d'identité de la mémoire verrouillée est entré sur le panneau de contrôle, les documents sont alors imprimés; il s'agit d'un autre moyen de sécurité qui empêche les documents de rester sans surveillance dans le plateau de réception à la vue de tous.

Télécopieur commercial en réseau

Acheminement d'adresse secondaire UIT-T
Utiliser une adresse secondaire annexée à un numéro de télécopieur permet d'acheminer une télécopie directement à l'ordinateur d'un destinataire via leur adresse courriel. Lorsque la télécopie est reçue à un ordinateur, la confidentialité est conservée, c.-à-d. le message peut-être vu uniquement par le destinataire.

Télécopie par IP
Les systèmes de télécopie Ricoh munis de NIC, peuvent supporter la télécopie par IP sécurisée T.38 en temps réel dans l'intranet d'une entreprise, non seulement en évitant les lignes téléphoniques dispendieuses, mais aussi en travaillant en toute sécurité derrière le pare-feu.

Tableau de compatibilité des solutions de sécurité Ricoh

	Fonctions de sécurité des télécopieurs commerciaux							
	Réseau fermé	Transmission et réception confidentielles	Télécopieur IP	Acheminement d'adresse secondaire UIT-T	Verrouillage de mémoire	Accès restrictif	Protection par NIP de sécurité	Authentification du serveur de domaine
Télécopieur Super G3								
FAX 1190L					■	■		
FAX3320L	■	■			■	■	■	
FAX4430L	■	■			■	■	■	
FAX4430NF	■	■	■	■	■	■	■	■
FAX5510L	■	■			■	■		
FAX5510NF	■	■	■	■	■	■		■

Solutions de sécurité Ricoh

Déclaration relative à la sécurité de l'information ISO 27001

ISO/IEC 27001 est une norme internationale vérifiable établissant les exigences pour les systèmes de gestion de la sécurité de l'information (ISMS). Cette norme est conçue afin d'identifier, de gérer et de minimiser une vaste gamme de menaces auxquelles l'information est régulièrement sujette, et exige que les processus et les procédures soient chiffrés dans le but d'identifier et de réduire les risques de sécurité susceptibles de compromettre les systèmes d'information.

Ricoh reconnaît l'importance d'aider à protéger les ressources d'information de notre entreprise, de nos clients, de nos partenaires d'affaires et de nos employés. Ricoh s'engage à développer, à mettre en œuvre et à continuellement améliorer notre système de gestion de la sécurité de l'information (ISMS) afin d'identifier et de protéger les ressources d'information de nos activités commerciales. Ricoh a choisi la norme de certification ISO 27001 dans des emplacements et des services clés afin de démontrer notre engagement envers la sécurité de l'information.

ISO 27001:2005
ISO 27001 est une norme internationale publiée en 2005 établissant les exigences pour les systèmes de gestion de la sécurité de l'information (ISMS). Elle est complétée par la norme ISO/IEC 17799:205 (Technologie de l'information -- Techniques de sécurité -- Code de bonne pratique relatif à la gestion de la sécurité de l'information). Le code de pratique est un document de référence qui définit les meilleures pratiques en matière de gestion de la sécurité de l'information, et découle directement de la norme britannique BS 7799.

Déclaration relative à la certification IEEE 2600/ISO 15408 de Ricoh

Certification IEEE 2600/ISO 15408
La norme IEEE 2600 est une norme de sécurité de la technologie de l'information élaborée par l'industrie de l'équipement de bureau. La norme définit les exigences minimales pour les fonctions de sécurité utilisées par les produits multifonctions (MFP) dans les environnements d'exploitation qui exigent un niveau élevé de sécurité des documents. La vérification indépendante confiée à une tierce partie et acceptée par l'industrie offerte via le test de sécurité ISO 15408 est combinée à un profil de protection fixe afin de fournir une référence commune pour l'évaluation de la sécurité des MFP. Les appareils MFP obtenant la certification pour la norme IEEE 2600 sont conçus avec des fonctions de sécurité évoluées pour être conformes au profil de protection établi. Dans le but d'assurer que le MFP démontre sa conformité à la norme établie, un laboratoire tiers indépendant teste et assure la vérification que les affirmations d'un fournisseur sur les fonctions de sécurité sont exactes, et présente un rapport de validation. Les clients peuvent alors utiliser les rapports de validation IEEE 2600 publiés pour le MFP certifié ou conforme dans leurs propres plans de sécurité de l'information afin de prouver que des efforts raisonnables ont été consentis afin de protéger l'information.

Principales fonctions, avantages et offres à nos clients
- Validation des fonctions de sécurité du MFP par un laboratoire tiers indépendant qui est reconnu par le gouvernement américain
- Vérification par un tiers indépendant que les affirmations d'un fournisseur sur les fonctions de sécurité de ses MFP sont exactes
- Une norme complète établit une référence commune quant aux attentes en matière de sécurité pour les produits MFP
- Plus besoin d'évaluer les affirmations individuelles en matière de sécurité de différents fournisseurs
- Les clients peuvent utiliser l'information générée par le test de certification comme preuve pour leurs plans de sécurité de l'information

Zones du MFP ayant été testées selon la norme IEEE

Les zones fonctionnelles du MFP suivantes ont été validées selon la norme IEEE 2600. Ces zones ont été identifiées comme étant les plus vulnérables aux violations de données éventuelles.

- Identification des utilisateurs et systèmes d'authentification
- Technologie de chiffrement des données disponibles pour les systèmes MFP
- Validation du micrologiciel du système du MFP
- Séparation de la ligne de télécopie analogue et du contrôleur de copie/impression/numérisation
- Validation des algorithmes de chiffrements de données
- Opération DOSS

Déclaration relative à la certification des produits

Ricoh Americas Corporation offre une gamme de produits dynamique et en évolution. Veuillez visiter http://www.ricoh.com/about/security/products/mfp/cc/ pour les plus récents renseignements relatifs à la certification des produits.

Ricoh est une entreprise tournée vers l'avenir qui possède une gamme de produits dynamique et qui s'améliore constamment afin de satisfaire aux exigences changeantes de nos clients. La certification IEEE P2600/ISO 15408 des produits Ricoh est un processus constant avec des mises à jour et des efforts continus. Cela dit, la plus récente information en matière de certification peut ne pas être indiquée sur ce site Web. Veuillez communiquer avec votre professionnel des ventes Ricoh pour connaître l'information la plus à jour concernant la certification IEEE P2600/ISO 15408.

Aperçu de la sécurité du panneau de commande intelligent (PCI)

Plusieurs des appareils MFP et des produits d'impression Ricoh lancés récemment seront maintenant dotés d'un panneau de commande intelligent (PCI). Cette nouvelle interface utilisateur améliorera la productivité en utilisant la technologie d'innovation des styles de travail de Ricoh, et fournira un panneau de contrôle commun pour l'ensemble de la gamme d'appareils. Afin d'aider à soutenir un fonctionnement sécurisé de cette nouvelle technologie, Ricoh a mis en œuvre les procédures et fonctions de sécurité suivantes pour le nouveau PCI :

- La fonction de gestion pour le panneau de commande intelligent peut être protégée par mot de passe afin de contribuer à limiter l'accès à la capacité de modifier les fonctions administratives du PCI.
- Le PCI est doté de capacités semblables aux « tablettes intelligentes », mais n'a pas toutes les mêmes fonctionnalités car il a été modifié en vue de son utilisation par les MFP et les imprimantes de Ricoh seulement.
- Le système d'exploitation Ricoh permet uniquement aux applications signées par Ricoh d'être installées. Les applications qui tentent d'être téléchargées sans signature numérique Ricoh ne seront pas installées et seront supprimées.
- Ricoh utilise des modules Android précis, en personnalise d'autres et évite les modules qui ne sont pas nécessaires au fonctionnement du PCI ou qui présentent des problèmes connus.
- Le groupe de spécialistes de Ricoh surveille les sites Web de notification d'organismes de sécurité publique pour être à l'affût des alertes de risques et de problèmes de sécurité éventuels.

Solutions de sécurité Ricoh

Tableaux de compatibilité des solutions de sécurité Ricoh

	Protection du réseau			Accès à l'appareil										Chiffrement des données									Protection des documents								Cert. de sécurité
	Web Image Monitor	SmartDeviceMonitor	Protocole réseau « on/off »	Authentification de l'administrateur	Registre des tâches/register des accès	Filtrage d'adresses IP	Enregistrement de compte d'utilisateur	Authentification de l'utilisateur;	WPA (accès protéger Wi-Fi)	Kerberos	Authentification câblée 802.1X	Gouv. fédéral des É.-U. Authentification CAC/PIV	Authentification par jeton SIPRNet du Department of Defense (DoD) des États-Unis	Protocole SSL (Secure Socket Layer) à 128 bits	Chiffrement du répertoire d'adresses	Transmission PDF chiffrée	Clé de chiffrement du pilote	Chiffrement du mot de passe PDF	Chiffrement SNMP v3	S/MIME pour Scan to E-mail	Communication IPSec	Chiffrement du disque dur	Chiffrement par mot de passe de l'impression verrouillée	Système de sécurité par écrasement des données	Impression verrouillée/sécurisée/verrouillée améliorée	Protection par mot de passe des documents stockés	Sécurité basée sur la mémoire vive* (si le DD est facultatif)	Disque dur amovible	Contrôle des copies non autorisées	Masque pour copie	Option de sécurité des données de copies	Impression obligatoire des renseignements sur la sécurité	Certification IEEE 2600/ISO 15408
Couleur multifonction																																
Pro C550EX / C700EX*	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■		
Pro C900s	■	■	■	■	■	■	■	■						■	■	■		■		■	■			■									
Aficio MP C300/SR/ C400/SR	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■							
Aficio MP C305SPF	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	
Aficio SP C242SF	■	■	■	■				■													■		■				■						
Aficio MP C300HT/ HW	■	■	■	■	■		■	■		■	■	■		■	■							■	■	■	■	■					■		
Aficio MP C3003/ C3503	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■
Aficio MP C4503/ C5503/C6003	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■
Aficio MP C6502/ C8002	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■
Pro C5100S/ Pro C5110S*	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	
SP C250SF/ C252SF	■		■			■															■					■							
MP C306SPF	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■	■	■	
MP C306/C406	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■	■	■	■
MP C3004/C3504	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■	■	■	
MP C4504/C6004	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■	■	■	
MP C401	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■	■		■
MP C2003/C2503	■		■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■				■	■		■
MP C2004/C2504	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■	■	■	

* Remarque : Les modèles Pro C550EX/Pro C700EX et Pro C5100S/Pro C5110S ainsi que les contrôleurs Fiery ont des fonctions de sécurité séparées. Les fonctions de sécurité indiquées ci-dessus concernent le contrôleur GW de l'unité centrale seulement. Si celle-ci est configurée avec le Fiery, les fonctions de sécurité du Fiery auront préséance.

	Protection du réseau			Accès à l'appareil										Chiffrement des données										Protection des documents							Cert. de sécurité
	Web Image Monitor	SmartDeviceMonitor	Protocole réseau « on/off »	Authentification de l'administrateur	Registre des tâches/registre des accès	Filtrage d'adresses IP	Enregistrement de compte d'utilisateur	Authentification de l'utilisateur;	WPA (accès protéger Wi-Fi)	Kerberos	Authentification câblée 802.1X	Gouv. fédéral des É.-U. Authentification CAC/PIV	Authentification par jeton SIPRNet du Department of Defense (DoD) des États-Unis	Protocole SSL (Secure Socket Layer) à 128 bits	Chiffrement du répertoire d'adresses	Transmission PDF chiffrée	Clé de chiffrement du pilote	Chiffrement du mot de passe PDF	Chiffrement SNMP v3	S/MIME pour Scan to E-mail	Communication IPSec	Chiffrement du disque dur	Chiffrement par mot de passe de l'impression verrouillée	Système de sécurité par écrasement des données	Impression verrouillée/sécurisée/verrouillée améliorée	Protection par mot de passe des documents stockés	Sécurité basée sur la mémoire vive* (si le DD est facultatif)	Disque dur amovible	Contrôle des copies non autorisées	Masque pour copie	Option de sécurité des données de copies	Impression obligatoire des renseignements sur la sécurité	Certification IEEE 2600/ISO 15408
Noir et blanc																																
Pro 907EX/1107EX/ 1357EX	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■		
Aficio MP 201F/ 201SPF	■	■	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]			■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■[1]	■			■	■		
Aficio SP 5200S/ 5210SF/5210SR	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■			■		■		
Aficio MP 301SPF	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	
Aficio SP 3400/ 3410 SF	■	■	■																						■		■						
Aficio SP 3510 SF	■	■	■																		■				■		■						
Aficio SP 4410SF (SFgx)	■	■	■	■	■	■	■					■									■			■	■		■						
Aficio MP 6002/ 7502/9002 SPF	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■
Pro 8100EX/8100S/ 8110S/8120S	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	
Aficio MP 2554SP/ 3054SP/3554SP	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	■	■
MP 401SPF	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	
SP 4510SF	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■	
Aficio MP 4054/ 5054/6054	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	■	■
SP 3600SF/3610SF			■	■		■		■	■					■							■						■						
MP 305SPF	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■	■	■	
MP 501/601	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■		■	
MP 6503/7503/ 9003	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■	■	■	
MP 402	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■				■		■	

[1]Trousse imprimante/numériseur requise. [2]Trousse imprimante/numériseur et IEEE 802.11b requis.

Solutions de sécurité Ricoh

	Protection du réseau			Accès à l'appareil										Chiffrement des données										Protection des documents								Cert. de sécurité
	Web Image Monitor	SmartDeviceMonitor	Protocole réseau « on/off »	Authentification de l'administrateur	Registre des tâches/registre des accès	Filtrage d'adresses IP	Enregistrement de compte d'utilisateur	Authentification de l'utilisateur;	WPA (accès protéger Wi-Fi)	Kerberos	Authentification câblée 802.1X	Gouv. fédéral des É.-U. Authentification CAC/PIV	Authentification par jeton SIPRNet du Department of Défense (DoD) des États-Unis	Protocole SSL (Secure Socket Layer) à 128 bits	Chiffrement du répertoire d'adresses	Transmission PDF chiffrée	Clé de chiffrement du pilote	Chiffrement du mot de passe PDF	Chiffrement SNMP v3	S/MIME pour Scan to E-mail	Communication IPSec	Chiffrement du disque dur	Chiffrement par mot de passe de l'impression verrouillée	Système de sécurité par écrasement des données	Impression verrouillée/sécurisée/verrouillée améliorée	Protection par mot de passe des documents stockés	Sécurité basée sur la mémoire vive* (si le DD est facultatif)	Disque dur amovible	Contrôle des copies non autorisées	Masque pour copie	Option de sécurité des données de copies	Impression obligatoire des renseignements sur la sécurité	Certification IEEE 2600/ISO 15408
Imprimante couleur																																
Aficio SP C231N/ C232DN	■	■	■																							■						
Aficio SP C420DN	■	■	■	■	■	■	■	■	■					■		■		■	■			■		■	■	■	■		■	■	■		
Aficio SP C420DN-KP HotSpot	■	■	■	■	■	■	■	■	■					■		■		■	■			■		■	■	■	■		■	■	■		
Aficio SP C820DN	■	■	■	■	■	■	■	■	■	■	■			■		■		■	■		■	■	■	■	■	■	■		■	■	■		
Aficio SP C821DN	■	■	■	■	■	■	■	■	■	■	■			■		■		■	■		■	■	■	■	■	■	■		■	■	■		
Aficio GX2500	■	■																								■						
Aficio GX3000*	■	■	■	■		■																				■		■				
Aficio GX e3300N*	■	■	■	■		■																				■		■				
Aficio GX3050N*	■	■	■	■		■																				■		■				
Aficio GX e3350N*	■	■	■	■		■																				■		■				
Aficio GX5050N*	■	■	■	■		■																				■		■				
Aficio GX e5550N*	■	■	■	■		■																				■						
Aficio GX7000	■	■																								■						
Pro C900	■	■	■	■	■	■	■	■						■	■	■		■		■	■			■									
Aficio SP C430DN/ SP C431DN	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■		■	■	■	■	■	■	■						
Aficio SP C431DN-HS	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■		■	■	■	■	■	■							
Aficio GX e7700N	■	■	■	■		■																				■						
Pro C651EX/C751EX	■	■	■	■	■	■	■	■	■	■	■			■	■	■		■	■	■	■	■		■		■							
Aficio SP C830DN/ SP C831DN	■	■	■	■	■	■	■	■		■	■			■	■	■	■		■		■		■	■	■		■		■	■			
Aficio SP C730DN	■	■	■	■	■	■	■	■		■	■			■	■	■	■		■		■		■	■	■				■	■			
SP C250DN/ SP C252DN	■		■			■															■						■						
SP C440DN	■	■	■	■	■	■	■	■	■	■	■			■	■		■	■			■	■	■	■	■		■					■	
SP C340DN/ C342DN	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■		■			■			

*Les modèles GX3000/3050N/5050N n'utilisent pas le même Web Image Monitor que les autres imprimantes Ricoh. Le navigateur est développé par Silex Technology et sera légèrement différent des autres modèles. Les modèles GX3000/GX e3300N/GX3050N/GX e3350N/GX5050N/GX e5550N sont compatibles à la fonction «filtrage d'adresses IP » seulement. Le «filtrage d'adresse Mac » n'est pas supporté. La fonction d'impression verrouillée/ sécuritaire est disponible uniquement si le disque dur est installé.

	Protection du réseau			Accès à l'appareil										Chiffrement des données										Protection des documents									Cert. de sécurité
	Web Image Monitor	SmartDeviceMonitor	Protocole réseau « on/off »	Authentification de l'administrateur	Registre des tâches/registre des accès	Filtrage d'adresses IP	Enregistrement de compte d'utilisateur	Authentification de l'utilisateur;	WPA (accès protéger Wi-Fi)	Kerberos	Authentification câblée 802.1X	Gouv. fédéral des É.-U. Authentification CAC/PIV	Authentification par jeton SIPRNet du Department of Defense (DoD) des États-Unis	Protocole SSL (Secure Socket Layer) à 128 bits	Chiffrement du répertoire d'adresses	Transmission PDF chiffrée	Clé de chiffrement du pilote	Chiffrement du mot de passe PDF	Chiffrement SNMP v3	S/MIME pour Scan to E-mail	Communication IPSec	Chiffrement du disque dur	Chiffrement par mot de passe de l'impression verrouillée	Système de sécurité par écrasement des données	Impression verrouillée/sécurisée/verrouillée améliorée	Protection par mot de passe des documents stockés	Sécurité basée sur la mémoire vive* (si le DD est facultatif)	Disque dur amovible	Contrôle des copies non autorisées	Masque pour copie	Option de sécurité des données de copies	Impression obligatoire des renseignements sur la sécurité	Certification IEEE 2600/ISO 15408
Imprimantes noir et blanc																																
Aficio SP 3300D/ SP 3300DN	■	■	■																								■					
Aficio SP 4100NL	■	■	■	■	■	■	■	■	■					■					■				■	■	■	■	■		■	■	■	
Aficio SP 4100N-KP HotSpot	■	■	■	■	■	■	■	■	■					■					■				■	■	■	■	■		■	■		
Aficio SP 4110N-KP HotSpot	■	■	■	■	■	■	■	■	■					■					■				■	■	■	■	■		■	■	■	
Aficio SP 4210N	■	■	■				■	■	■		■			■					■		■		■	■		■		■	■	■		
Aficio SP 5100N	■	■	■			■	■	■						■		■		■								■						
Aficio SP 6330N	■	■	■	■	■	■			■																	■		■				
Aficio SP 8200DN	■	■	■	■	■		■	■	■						■				■		■	■	■	■	■	■	■	■	■	■		
Aficio SP 9100DN	■	■	■			■	■	■	■					■		■		■					■	■	■			■	■			
Aficio SP 5200DN	■	■	■	■	■	■	■		■	■	■			■	■	■	■	■	■		■					■						
Aficio SP 5210DN	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■		■	■	■	■	■	■						
Aficio SP 1210N																										■						
Aficio SP 4310N	■	■	■		■		■	■	■		■			■	■			■	■		■	■		■	■		■		■	■	■	
Aficio SP 1210N	■	■	■																						■		■					
Aficio SP 3400n/ SP 3410D	■	■	■			■	■																		■		■					
Aficio SP 3510DN	■	■	■			■	■																		■		■					
Aficio SP 8300DN	■	■	■	■	■		■	■	■	■	■			■			■		■	■	■		■	■	■		■		■	■		
SP 4510DN	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■	■				■	
SP 4520DN	■		■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■	■				■	
SP 6430DN	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■		■	■	■	■	■	■		■			■	■	
SP 3600DN			■	■		■		■	■					■							■					■						
SP 5300DN/ 5310DN	■	■	■	■	■	■	■	■	■	■	■			■	■	■	■	■	■	■	■	■	■	■	■	■	■			■		
Grand format																																
Aficio MP W5100	■	■	■	■	■		■	■		■				■	■	■	■	■	■	■	■	■	■	■	■				■	■		
Aficio MP W7140	■	■	■	■	■		■	■		■				■	■	■	■	■	■	■	■	■	■	■	■				■	■		
Aficio MP CW2200	■	■	■	■	■		■							■	■	■	■	■	■	■	■	■	■	■	■				■	■	■	
Aficio MP W3601	■	■	■	■	■		■	■	■	■				■	■	■		■	■		■	■		■	■							

Le contenu de ce document, de même que l'apparence, les fonctions et les caractéristiques des produits de Ricoh peuvent changer de temps à autre sans préavis. Les produits illustrés comportent des options. Même après avoir pris toutes les précautions possibles pour assurer l'exactitude de l'information, Ricoh ne fait aucune déclaration ni ne garantit l'exactitude de l'information contenue dans le présent document et n'accepte aucune responsabilité à l'égard de toute erreur ou omission dans ledit texte.Les seules garanties relatives aux produits et services de Ricoh sont exposées dans les énoncés de garantie formelle s'y rattachant.Aucun élément du présent document ne doit être interprété comme une garantie supplémentaire. Vos résultats réels, incluant la vitesse d'impression et autres mesures de rendement, varieront selon votre utilisation des produits et services, ainsi que les conditions et facteurs touchant le rendement.IL N'Y A PAS DE GARANTIE QUE VOUS RÉALISEREZ DES RÉSULTATS SEMBLABLES À NOS RÉSULTATS. RICOH N'OFFRE AUCUN AVIS JURIDIQUE, COMPTABLE OU FISCAL, ET NE REPRÉSENTE NI NE GARANTIT QUE SES PRODUITS OU SERVICES GARANTISSENT OU ASSURENT VOTRE CONFORMITÉ AUX LOIS, RÈGLEMENTS OU AUTRES EXIGENCES. Le client est responsable de ses choix de produits, de solutions et d'architectures techniques et de sa propre conformité aux différentes lois comme la Gramm-Leach-Bliley Act, la Sarbanes-Oxley Act et la Health Insurance Portability and Accountability Act (HIPAA).

RICOH

imagine. change.

imaginer. changer.

www.ricoh.ca

Ricoh Canada Inc., 300-5520 Explorer Drive, Mississauga, ON L3P 7S7, 1-888-742-6417