Version 1.1
17 août 2010

Document de présentation technique sur la sécurité des appareils imageRUNNER ADVANCE

OBJET DU PRÉSENT DOCUMENT

Canon reconnaît l'importance de la sécurité de l'information et est au fait des défis auxquels est confrontée votre entreprise. Ce document de présentation technique contient des renseignements sur la sécurité de l'information dans le cadre de l'utilisation des systèmes imageRUNNER ADVANCE de Canon. Il fournit des détails sur la technologie de sécurité imageRUNNER ADVANCE pour les environnements réseautés et autonomes et présente, dans l'optique de la sécurité des documents et de l'information, un aperçu de l'architecture des systèmes imageRUNNER ADVANCE, du cadre conceptuel et des technologies de Canon.

Ce document de présentation technique vise principalement les employés administratifs du client qui sont chargés de la configuration et de l'entretien des systèmes imageRUNNER ADVANCE. Les renseignements qui y sont énoncés peuvent faciliter la compréhension des nombreuses fonctions de configuration liées à la sécurité qui sont offertes par ces systèmes de Canon. Les systèmes imageRUNNER ADVANCE intègrent plusieurs fonctions (de série et en option) qui, lorsqu'elles sont utilisées par le client, peuvent favoriser une gestion et une protection efficaces des données traitées par le système et qui y sont enregistrées. Il incombe toutefois au client de choisir la ou les méthode(s) les plus appropriée(s) pour protéger ses données.

Canon ne peut garantir que l'emploi des renseignements contenus dans le présent document préviendra les attaques malicieuses ou l'utilisation inadéquate de vos systèmes imageRUNNER ADVANCE.

Les produits illustrés comportent des accessoires ou du matériel en option. Les fonctions abordées dans ce document de présentation technique comprennent des solutions de série et en option pour les systèmes imageRUNNER ADVANCE. Les spécifications et les dates de disponibilité peuvent être modifiées sans préavis.

Table des matières

Section 1 – Introduction

« Si vous considérez ces machines comme de simples copieurs ou de simples imprimantes, vous vous demandez en tout premier lieu si vous avez réellement besoin de sécurité. Vous découvrez ensuite que le matériel de bureau traditionnel intègre désormais des innovations et des capacités technologiques importantes qui en font une partie intégrante d'un réseau d'entreprise relié à l'intranet et à Internet. Les organismes gouvernementaux, les entreprises et les sociétés sans but lucratif passent graduellement des appareils autonomes traditionnels à des appareils qui intègrent les fonctions de ces derniers et les relient aux réseaux d'entreprise, ce qui donne lieu à de nouvelles préoccupations quant à la sécurité et à la gestion de l'information.

Les fonctions mises au point pour les systèmes imageRUNNER ADVANCE de Canon sont conçues pour prévenir la perte de données, protéger contre l'infiltration et assurer l'intégrité de l'information. »

– Dennis Amorosano, Directeur principal,
Marketing des solutions et soutien d'entreprise, Canon U.S.A., Inc.

La technologie associée au matériel de bureau continue de se développer en suivant le rythme toujours croissant de l'évolution du marché. Au cours des dernières années seulement, la technologie du matériel de bureau traditionnel a fait un bond en avant, élargissant les capacités fonctionnelles tout en devenant une partie intégrante des réseaux d'entreprise et d'Internet. En conséquence, un nouveau niveau de sensibilisation en matière de sécurité s'impose.

L'attention qu'accorde Canon aux tendances commerciales émergentes et aux détails entourant les exigences de sécurité des clients s'est traduite par la mise au point, dans les systèmes imageRUNNER ADVANCE, de caractéristiques conçues pour contenir les pertes de données et la menace potentielle du piratage.

Section 1 – Introduction

1.1 – Vue d'ensemble du marché de la sécurité

Dans le monde numérique, les risques pour les réseaux et les appareils empruntent davantage de formes et proviennent de plus d'endroits que jamais auparavant. De nos jours, les administrateurs des TI jouent le rôle additionnel d'agent de sécurité afin de protéger adéquatement l'information et les biens contre les menaces – allant du vol d'identité et de la perte de propriété intellectuelle à l'infection par les virus et les chevaux de Troie – provenant tant de l'extérieur que de l'intérieur.

Presque chaque jour, de nouvelles menaces de destruction exposent des vulnérabilités jusque-là inconnues, démontrant que l'on n'est jamais trop en sécurité. Les administrateurs des TI ont besoin d'une stratégie de sécurité globale qui puisse être appliquée à chaque niveau de l'organisation – depuis les serveurs, les ordinateurs de bureau et les appareils comme des PMF aux réseaux qui les relient.

Comme s'il n'était pas déjà assez difficile de gérer les risques pour les ordinateurs, les réseaux et les périphériques, la réglementation gouvernementale accrue ajoute une couche additionnelle de normes de conformité rigoureuses à respecter. La législation américaine, notamment la loi *Sarbanes-Oxley* (SOX), la loi *Gramm-Leach-Bliley* (GLB), la loi sur l'assurance-maladie (HIPAA) et la loi sur la confidentialité de l'éducation (FERPA), de même que la législation canadienne, notamment la *Loi sur la protection des renseignements personnels et les documents électroniques* et la législation provinciale sur la confidentialité, exigent des administrateurs des TI qu'ils accordent la priorité à la sécurité, la confidentialité, la précision et la fiabilité de l'information reçue.

1.2 – Vue d'ensemble de la sécurité de l'imagerie et de l'impression

Les appareils multifonction modernes partagent de nombreuses similitudes avec les ordinateurs personnels. Ils comportent de nombreux composants identiques comme une unité centrale, de la mémoire et des disques durs, et certains utilisent même des systèmes d'exploitation courants comme Windows ou Linux. Comme tous les appareils réseautés, ces appareils peuvent recueillir de l'information sensible et la stocker sur leur disque dur et dans leur mémoire. Dans nombre d'entreprises, toutefois, les appareils multifonction ne bénéficient pas de la même attention pour ce qui est de la sécurité des données.

Le Document de présentation technique sur la sécurité des appareils imageRUNNER ADVANCE de Canon a été conçu pour donner de l'information détaillée sur la manière de régler divers problèmes de sécurité avec les systèmes imageRUNNER ADVANCE. Les systèmes imageRUNNER ADVANCE de Canon possèdent de nombreuses capacités de sécurité de série. De nombreuses options de sécurité peuvent également y être ajoutées en vue de conférer un niveau supérieur de confidentialité, d'intégrité et de disponibilité aux données vitales de votre entreprise.

1.3 – Secteurs clés de concentration de la sécurité

Canon reconnaît les besoins essentiels de prévention de la perte de données, de protection de l'appareil contre l'utilisation non voulue et de réduction du risque de compromission de l'information. En conséquence, tous les systèmes imageRUNNER ADVANCE comportent de nombreuses fonctions de sécurité de série afin de protéger l'information.

Les capacités de sécurité imageRUNNER ADVANCE de Canon sont réparties en cinq secteurs clés :

- Sécurité de l'appareil
- Sécurité de l'information
- Sécurité du réseau
- Surveillance de la sécurité / outils de gestion
- Ouverture de session et vérification

Canon consacre énormément de temps et de ressources à améliorer continuellement les capacités de sécurité de ses appareils imageRUNNER. Les administrateurs disposent de capacités évoluées de restriction d'accès aux fonctions de l'appareil tout en maintenant une disponibilité et une productivité accrues.

Section 2 – Sécurité de l'appareil

2.1 – Sécurité du contrôleur imageRUNNER ADVANCE

La série imageRUNNER ADVANCE est construite sur une nouvelle plate-forme qui améliore considérablement la sécurité et la productivité. La nouvelle architecture se fonde sur un nouveau système d'exploitation tournant sous une version intégrée de Linux, qui devient la plate-forme la plus largement adoptée pour les appareils sophistiqués. La version source utilisée dans les appareils imageRUNNER ADVANCE a été élaguée de tous les gestionnaires et services non nécessaires de façon à conserver seulement ceux qui sont essentiels à son fonctionnement.

La nature du système Linux intégré et l'élagage du système d'exploitation réduisent considérablement l'exposition aux exploits par rapport à un système d'exploitation Linux ou Windows pour ordinateur de bureau ou serveur. Canon s'efforce de développer des produits qui répondent aux exigences de sécurité de ses clients ou les dépassent. Certaines des activités reliées à la sécurité comprennent l'essai indépendant, par des sociétés consultantes en sécurité, d'appareils imageRUNNER ADVANCE de Canon à différentes étapes de leur mise au point en vue d'éliminer toute vulnérabilité potentielle avant la production. Aussi, Canon a collaboré à des initiatives de l'industrie, comme la mise au point de la famille de normes IEEE P2600 sur la sécurité des systèmes et des unités d'impression.

2.2 – Authentification

Les systèmes imageRUNNER ADVANCE de Canon comportent de nombreuses options d'authentification auxquelles peut recourir l'administrateur afin que seuls les utilisateurs en libre-service et les utilisateurs autorisés du réseau accèdent à l'appareil et à ses fonctions, comme l'impression, la reproduction, la numérisation et l'envoi. En plus de limiter l'accès aux utilisateurs autorisés, l'authentification permet de contrôler l'utilisation de la production couleur et calcule le nombre total d'impressions par service ou utilisateur.

Authentification fondée sur l'appareil

Mode d'identification de service
Fonction intégrée aux systèmes imageRUNNER ADVANCE, le mode d'identification de service permet à l'administrateur de contrôler l'accès à l'appareil. Lorsque ce mode est activé, l'utilisateur final doit saisir un mot de passe pour accéder à l'appareil. Il est possible de configurer jusqu'à 1 000 identificateurs de service et chacun peut être configuré avec des limites d'impression, de reproduction et d'accès à la boîte aux lettres avancée, aux boîtes aux lettres et à la télécopie.

L'accès à la boîte aux lettres avancée, aux boîtes aux lettres et à la télécopie peut être activé « On » ou désactivé « Off » à l'écran « Limit Functions » (limitation des fonctions) sous « Department ID Management » (Mode de gestion de l'identification de service).

Le réglage peut être effectué sous Settings / Registration > Management Settings > User Management > Department ID Management (Réglages / Enregistrement > Paramètres de gestion > Gestion de l'utilisateur > Gestion de l'identification de service).

Ouvertures de session Single Sign On (SSO) et SSO Hybrid (SSO-H)
Single Sign On (SSO) est un service d'ouverture de session de la plate-forme d'application intégrée multifonction (MEAP) que l'on peut utiliser de façon autonome avec les données de l'utilisateur enregistrées localement à l'appareil ou conjointement avec un environnement réseauté Active Directory. SSO prend en charge les modes suivants :

- Authentification de l'appareil local – les justificatifs d'ouverture sont stockés dans l'appareil.
- Authentification de domaine – dans ce mode, l'authentification de l'utilisateur peut être liée dans un environnement Active Directory au sein d'un réseau.
- Authentification de domaine + Authentification de l'appareil local

Pour une ouverture de session en mode Authentification de domaine, l'utilisateur doit s'authentifier avec succès à l'aide des justificatifs d'ouverture valides au panneau de commande du système, de l'interface utilisateur à distance ou d'un navigateur Web s'il accède par un réseau avant d'accéder à quelque fonction que ce soit de l'appareil.

SSO est livré de série avec les systèmes imageRUNNER ADVANCE prêts pour MEAP et peut prendre en charge jusqu'à 200 domaines de confiance en plus des utilisateurs appartenant au même domaine que l'appareil.

Les systèmes imageRUNNER ADVANCE de Canon sont également livrés avec SSO-H, qui prend en charge l'authentification directe dans un domaine Active Directory en utilisant Kerberos ou NTLM v. 2 comme protocole d'authentification. SSO-H ne nécessite pas de logiciel supplémentaire pour procéder à l'authentification de l'utilisateur car il peut communiquer directement avec les contrôleurs de domaines du service d'annuaire Active Directory. En mode Authentification de l'appareil local, SSO-H peut prendre en charge jusqu'à 5 000 utilisateurs.

Authentification par carte

Authentification avec carte uniFLOW
Combinés au logiciel uniFLOW Output Manager, les systèmes imageRUNNER ADVANCE peuvent procéder à l'authentification sécuritaire des utilisateurs au moyen de cartes sans contact, de cartes à puce, de cartes magnétiques et de NIP. uniFLOW prend en charge HID Prox, MIFARE, Legic, Hitag et les cartes magnétiques en mode natif en utilisant son propre lecteur, ainsi que d'autres par le biais d'intégrations personnalisées. Certains modèles de lecteur de carte RF IDeas peuvent aussi être intégrés pour prendre en charge l'authentification en utilisant des cartes d'authentification à radiofréquences.

Authentification avancée – carte de proximité
En utilisant une application MEAP, les systèmes imageRUNNER ADVANCE peuvent être personnalisés pour authentifier automatiquement l'utilisateur à l'aide de cartes sans contact comme celles que l'on utilise dans les environnements d'entreprise. Les données de l'utilisateur peuvent être enregistrées localement dans un tableau sécurisé qui élimine le besoin d'un serveur externe, ou intégrées avec un serveur d'authentification existant en personnalisant ce dernier. Les cartes HID Prox, HID iClass, Casi-Rusco, MIFARE et AWID sont prises en charge. On peut également recourir à la personnalisation pour prendre en charge d'autres types de cartes.

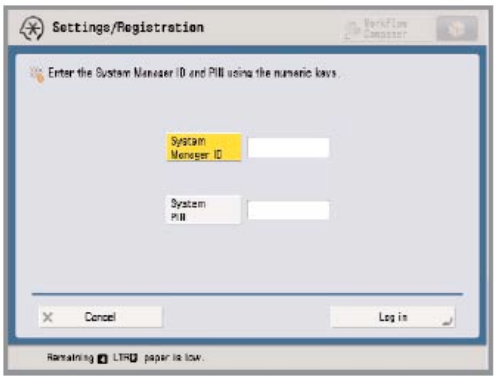
Système de lecteur de carte de contrôle
Les systèmes imageRUNNER ADVANCE de Canon peuvent prendre en charge un système de lecteur de carte de contrôle en option pour donner accès à l'appareil et en gérer l'utilisation. Le système de lecteur de carte de contrôle en option nécessite l'utilisation de cartes intelligentes que l'on doit insérer dans le système pour pouvoir accéder aux fonctions, ce qui automatise le processus d'authentification du service. Le système de lecteur de carte de contrôle en option gère jusqu'à 300 services ou utilisateurs.

2.3 – Contrôle d'accès

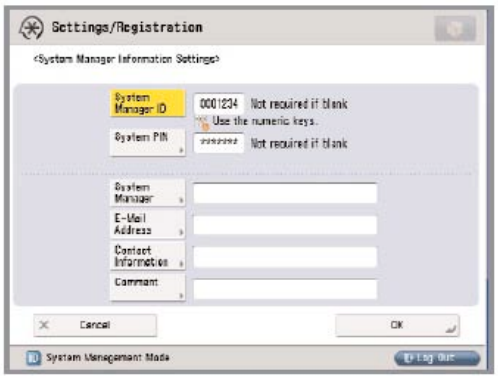
Les systèmes imageRUNNER ADVANCE de Canon prennent en charge de nombreuses options de contrôle d'accès afin de vous aider à gérer l'utilisation des paramètres et des fonctions de l'appareil en plus des capacités particulières de certaines fonctions. Les solutions de contrôle d'accès des appareils imageRUNNER ADVANCE peuvent aider à l'authentification, à l'autorisation et à la vérification. Canon offre des solutions permettant de verrouiller tout l'appareil ou des fonctions précises (p, ex., le balayage-courriel), tout en laissant les autres applications disponibles à l'utilisation générale. Avec la puissance et la souplesse de MEAP, certaines solutions peuvent être personnalisées pour répondre à vos besoins particuliers.

Paramètres de système protégés par mot de passe

Les écrans de paramètres des systèmes imageRUNNER ADVANCE prennent en charge la protection par mot de passe afin de restreindre la modification des réglages de l'appareil au panneau de commande et à l'interface utilisateur à distance. Entre autres options, l'administrateur du système peut établir l'information réseau, configurer le système, activer et désactiver le réseau et les protocoles d'impression. Canon recommande fortement d'établir un mot de passe d'administrateur au moment de l'installation, étant donné qu'il commande les paramètres critiques de l'appareil.



Écran du gestionnaire du système



Écran de stockage d'identificateur et de mot de passe

Système de gestion des accès

Le système de gestion des accès, offert de série dans les systèmes imageRUNNER ADVANCE, peut servir à contrôler l'accès aux fonctions de l'appareil. On peut imposer des restrictions aux utilisateurs et aux groupes afin de restreindre l'utilisation de fonctions entières ou de caractéristiques particulières d'une fonction. Les restrictions d'accès sont gérées en unités appelées « rôles ». Les rôles contiennent des renseignements qui déterminent les fonctions de l'appareil pouvant être utilisées ou non.

Les rôles peuvent être établis selon le titre du poste de l'utilisateur ou ses responsabilités ou par groupe, ce qui permet à l'administrateur de créer des rôles propres à certains services ou groupes de travail. Comme l'administrateur n'est pas contraint de restreindre l'utilisation d'une fonction dans son intégralité, les rôles peuvent être aussi précis qu'il le faut pour un certain nombre de besoins d'entreprise. En plus des rôles de base, qui comportent des restrictions d'accès, on peut enregistrer jusqu'à 100 nouveaux rôles personnalisés pour un maximum de 5 000 utilisateurs. L'administrateur peut également décider s'il permet ou non aux utilisateurs non inscrits d'ouvrir une session en tant qu'invités et il peut établir les réglages pour les rôles d'invités.

Section 2 – Sécurité de l'appareil

Les divers niveaux d'accès de base (rôles) disponibles sont décrits ci-dessous.

Privilèges selon le niveau d'accès	
Rôle prédéterminé	**Privilèges d'accès**
Administrateur	Jouit du privilège d'utiliser toutes les fonctions de l'appareil.
Administrateur de réseau	Gère surtout les réglages propres au réseau à l'affichage Réglages et enregistrement.
Administrateur de l'appareil	Peut préciser les paramètres de gestion du type de papier et les paramètres des fonctions d'envoi et de réception.
Utilisateur autorisé	Jouit du privilège d'utiliser toutes les fonctions de l'appareil, à l'exception de la fonction de gestion de l'appareil.
Utilisateur général	Jouit du privilège d'utiliser toutes les fonctions de l'appareil, à l'exception des fonctions de gestion de l'appareil et de précision/enregistrement au carnet d'adresses.
Utilisateur limité	N'accède ni à la gestion de l'appareil ni aux fonctions d'envoi et imprime et reproduit seulement recto verso.
Invité	N'accède ni à la gestion de l'appareil ni aux fonctions d'envoi et imprime et reproduit seulement recto verso.

Les fonctions suivantes peuvent être restreintes.

Fonctions de l'appareil	Valeurs	Description
Impression	Autorisé, non autorisé	Autorise ou interdit l'utilisation des applications relatives à la fonction d'impression.
Reproduction	Autorisé, non autorisé	Autorise ou interdit l'utilisation des applications relatives à la fonction de reproduction.
Envoi/stockage sur le réseau		Établit des restrictions sur l'envoi à l'externe de documents numérisés et de documents de la boîte de réception de l'utilisateur, ainsi que sur la sauvegarde de documents sur des serveurs de fichiers ou sur le réseau.
Envoi de courrier électronique	Autorisé, non autorisé	Autorise ou non l'envoi de courrier électronique.
Envoi de télécopie Internet	Autorisé, non autorisé	Autorise ou non l'envoi de télécopie Internet.
Envoi de télécopie		Autorise ou non l'envoi de télécopie.
Envoi par protocole de transfert de fichier	Autorisé, non autorisé	Autorise ou non l'envoi par protocole de transfert de fichier.
Envoi par logiciel NetWare (IPX)	Autorisé, non autorisé	Autorise ou non l'envoi par logiciel NetWare (IPX).
Envoi par Windows (SMB)	Autorisé, non autorisé	Autorise ou non l'envoi par Windows (SMB).
Envoi par protocole WebDAV	Autorisé, non autorisé	Autorise ou non l'envoi par protocole WebDAV.
Envoi à partir de la boîte de réception	Autorisé, non autorisé	Établit des restrictions sur la sauvegarde de documents numérisés dans les boîtes aux lettres de l'utilisateur.
Précision du domaine d'adresse / envoi aux adresses reçues d'un téléphone cellulaire	Autorisé, non autorisé	Pour les appareils imageRUNNER ADVANCE, ces restrictions s'appliquent aussi aux adresses reçues d'un téléphone cellulaire.
Utilisation de l'emplacement de stockage du carnet d'adresses / du registre pour le réseau	Aucune restriction, non autorisé, lecture seulement	Pour les appareils imageRUNNER ADVANCE, ces restrictions s'appliquent aussi à l'enregistrement, à la modification et à la suppression de données stockées sur le réseau.
Envoi à une nouvelle adresse / envoi aux adresses reçues d'un téléphone cellulaire	Autorisé, non autorisé	Pour les appareils imageRUNNER ADVANCE, ces restrictions s'appliquent aussi aux adresses reçues d'un téléphone cellulaire.
Ajout de la signature de l'appareil aux fichiers envoyés	Autorisé, non autorisé	Autorise ou non l'ajout de la signature d'un appareil à l'envoi de fichiers PDF.
Envoi du format du fichier	Autorisé, non autorisé	Autorise ou non l'envoi des formats de fichier auxquels la signature d'un appareil ne peut être ajoutée.
Fonctions de sauvegarde (boîte aux lettres/retenue/support à mémoire)	Autorisé, non autorisé	Autorise ou non l'utilisation des fonctions de sauvegarde.
Accès Internet	Autorisé, non autorisé	Autorise ou interdit l'utilisation des applications relatives à la fonction d'accès Internet.
Fonctions utilitaires	Autorisé, non autorisé	Autorise ou interdit l'utilisation des applications relatives aux fonctions utilitaires.
Autres	Autorisé, non autorisé	Autorise ou interdit l'utilisation d'autres applications.
Applications MEAP	Autorisé, non autorisé	Autorise ou non l'utilisation d'applications MEAP.

** Nécessite l'activation de SSO-H.*

Section 2 – Sécurité de l'appareil

Lorsque le système de gestion des accès est activé, l'utilisateur doit ouvrir une session à l'appareil avec l'authentification SSO. Le système de gestion des accès prend en charge l'authentification avec le système d'authentification d'appareil local aussi bien qu'avec Active Directory en utilisant SSO-H*, qui prend en charge l'authentification Kerberos. Une fois que l'utilisateur a ouvert une session avec son nom et son mot de passe, l'appareil détermine le rôle attribué à cet utilisateur particulier. Les restrictions s'appliquent en fonction de ce rôle. Si une fonction est entièrement restreinte, elle s'affiche de manière estompée après l'authentification de l'utilisateur.

Authentification au niveau de la fonction
L'authentification au niveau de la fonction des systèmes imageRUNNER ADVANCE de Canon peut limiter l'utilisation de fonctions particulières selon les utilisateurs autorisés en exigeant qu'ils s'authentifient pour utiliser des fonctions sensibles. L'authentification au niveau de la fonction fait partie du système de gestion des accès et fonctionne avec SSO-H pour l'authentification. Elle permet à l'administrateur de choisir précisément les fonctions autorisées aux utilisateurs en libre-service et en réseau, sans entrée de justificatifs par rapport à celles pour lesquelles un utilisateur doit ouvrir une session. Par exemple, l'administrateur peut permettre à tous les utilisateurs de faire des reproductions en noir et blanc mais leur demander d'ouvrir une session s'ils veulent utiliser la couleur ou la fonction Numérisation et envoi.

Numérisation et envoi – sécurité

Certaines informations des appareils où la fonction Numérisation et envoi est autorisée, comme les numéros de télécopieur et les adresses électroniques, peuvent être considérées comme confidentielles et sensibles. Ces appareils disposent de fonctions de sécurité additionnelles pour bloquer l'accès à l'information confidentielle.

Mot de passe du carnet d'adresses
Des mots de passe d'administrateur et d'utilisateur peuvent être établis pour accéder aux fonctions de gestion du carnet d'adresses. Un administrateur de système peut choisir les données du carnet d'adresses qui peuvent être consultées par les utilisateurs et masquer les détails à caractère confidentiel. Ces mots de passe peuvent être établis séparément, de sorte que des personnes autres que le gestionnaire du système puissent administrer le carnet d'adresses.

L'établissement d'un mot de passe pour accéder à un carnet d'adresses restreint la capacité de stockage, d'édition ou de suppression d'adresses électroniques individuelles et de groupe du carnet d'adresses. Ainsi, seules les personnes qui possèdent le bon mot de passe peuvent accéder au carnet d'adresses et y apporter des modifications.

On utilise le même mot de passe pour la fonction Importation/Exportation du carnet d'adresses avec l'interface à distance.

** Nécessite la console de gestion d'entreprise imageWARE et le module d'extension du système de gestion des accès pour effectuer l'authentification par le biais d'Active Directory.*

Affichage Mot de passe du carnet d'adresses

Affichage Activation/désactivation du code d'accès au carnet d'adresses

Code d'accès au carnet d'adresses
L'utilisateur final peut aussi mettre un code d'accès à des adresses du carnet d'adresses. Lorsqu'il enregistre une adresse, il peut entrer un code d'accès en vue de restreindre l'affichage de cette entrée au carnet d'adresses. Cette fonction limite l'affichage et l'utilisation d'une adresse du carnet d'adresses aux utilisateurs possédant le bon code. Le code d'accès peut être activé et désactivé selon le niveau de sécurité jugé nécessaire.

L'utilisateur suit le chemin Settings / Registration > Register Destinations > Register New Destinations (Réglages/enregistrement > Enregistrement des destinations > Nouvelle destination) puis enregistre l'adresse électronique, le numéro de télécopie ou de télécopie Internet, l'adresse de fichier ou de groupe et établit le code d'accès de cette entrée du carnet d'adresses.

Fonction de restriction de destination
La transmission de données vers une nouvelle destination par le biais de la fonction Numérisation et envoi et par télécopieur peut être restreinte afin d'interdire les transmissions ailleurs que vers les destinations enregistrées ou autorisées par le gestionnaire du système.

En plus de la restriction vers toutes les nouvelles destinations, l'administrateur peut restreindre l'ajout de nouvelles adresses pour des types de destination particuliers accessibles aux utilisateurs pour la numérisation et l'envoi ou la télécopie de documents. On peut établir des permissions pour activer ou désactiver l'entrée de nouvelles adresses dans les cas suivants :

- Entrées dans le carnet d'adresses
- Serveurs LDAP
- Boîtes de réception d'utilisateur
- Boutons d'accès direct
- Boutons Favoris
- Adresses électroniques de l'utilisateur (bouton d'envoi à soi-même, si l'ouverture de session SSO est utilisée)

Fonctions de sécurité du gestionnaire d'impression

Comptabilisation des travaux d'impression

La comptabilisation des travaux d'impression est une fonction de série des gestionnaires d'impression Canon. Elle exige de l'utilisateur qu'il entre un mot de passe défini par l'administrateur avant d'imprimer, ce qui restreint l'accès à l'appareil aux personnes ayant la permission d'imprimer. Les restrictions d'impression peuvent être établies en utilisant les justificatifs d'un identificateur de service ou au moyen du système de gestion des accès.

Blocage de l'interface USB

Le blocage de l'interface USB permet à l'administrateur du système de protéger les systèmes imageRUNNER ADVANCE contre les accès non autorisés par l'interface USB intégrée. L'accès à l'interface USB de l'appareil donnant accès par le bureau et le mode hôte de l'appareil pour les autres dispositifs USB peuvent chacun être activés ou désactivés.

Suivre le chemin Settings / Registration > Preferences > External Interface > USB Settings (Réglages/Enregistrement > Préférences > Interface externe > Réglages USB).

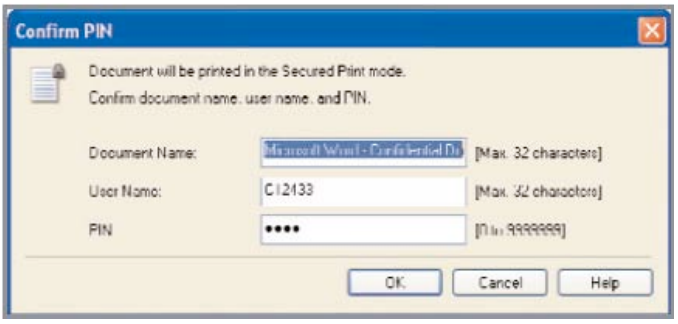
Section 3 – Sécurité de l'information

Canon prend très au sérieux sa mission qui consiste à protéger l'information confidentielle de votre entreprise. Depuis vos documents, télécopies et courriels jusqu'aux données sous-jacentes sur votre disque dur interne et en mémoire, Canon a établi de nombreux contrôles afin d'assurer que votre information ne soit pas compromise.

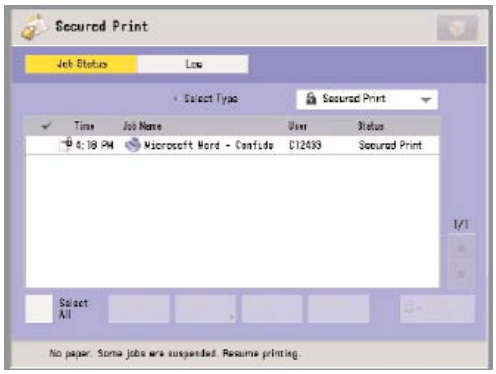
3.1 – Sécurité des documents

Impression sécurisée

Impression sécurisée / Impression sécuritaire à données cryptées*
L'impression sécuritaire à données cryptées et l'impression sécurisée sont des fonctions d'impression qui maintiennent un travail dans la file d'attente jusqu'à ce que l'utilisateur saisisse le mot de passe approprié à l'appareil. Ainsi, l'utilisateur se trouve à proximité de l'appareil avant l'impression, ce qui réduit les risques de laisser un document sans surveillance. L'imageRUNNER ADVANCE demande à l'utilisateur d'entrer un mot de passe dans la fenêtre du gestionnaire d'impression lorsqu'il envoie un travail à partir d'un ordinateur personnel connecté. Le même mot de passe est également demandé au niveau de l'appareil pour imprimer le travail. L'utilisation du logiciel d'impression sécuritaire à données cryptées relève la sécurité d'un cran, car le cryptage des données à 256 bits (AES) protège les données d'impression acheminées sur le réseau. Sur les systèmes équipés de l'impression sécuritaire à données cryptées en option, l'administrateur peut utiliser la fonction de restriction d'impression afin de permettre d'imprimer seulement les travaux cryptés à l'appareil indiqué.



Affichage d'impression sécurisée du gestionnaire d'imprimante



Affichage d'état du travail à imprimer

Impression sécurisée uniFLOW
La suite uniFLOW Output Manager, exclusive à Canon, est un logiciel modulaire en option conçu pour réduire les coûts, améliorer la productivité et accroître la sécurité. Du point de vue de la sécurité, uniFLOW Output Manager favorise une impression sécuritaire en retenant dans le serveur les travaux acheminés à n'importe quel système imageRUNNER ADVANCE jusqu'à ce que l'utilisateur demande l'impression.
À son bureau, l'utilisateur imprime des documents en choisissant le serveur uniFLOW comme imprimante. À l'appareil indiqué, l'utilisateur peut s'authentifier à l'aide d'une des nombreuses méthodes prises en charge. L'utilisateur accède ensuite à l'application uniFLOW MEAP client à partir du panneau de commande de l'appareil et libère le travail de la file de documents en attente.

** Nécessite l'impression sécuritaire à données cryptées en option.*

Protection de l'espace de stockage des documents

Sécurité de la boîte aux lettres

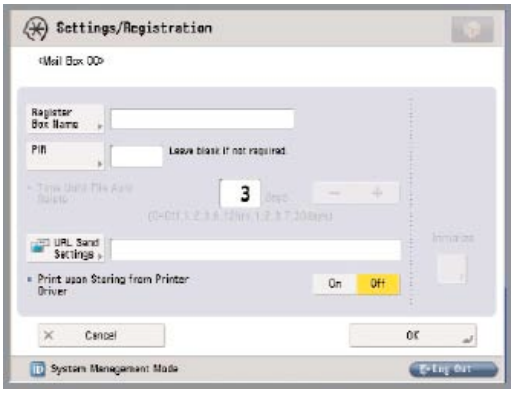
Chaque système imageRUNNER ADVANCE est livré de série avec des boîtes aux lettres pour le stockage de données numérisées et imprimées. La sécurité des boîtes aux lettres repose sur la capacité de concevoir un mot de passe unique pour y accéder. Une fois qu'un document est stocké dans la boîte aux lettres (si celle-ci est protégée par mot de passe), tout utilisateur doit taper son mot de passe pour le récupérer.

L'administrateur peut également recourir à la fonction de restriction d'impression pour limiter l'impression directe du bureau d'un ordinateur vers l'appareil. Cela oblige l'utilisateur à stocker tous ses travaux d'impression dans la boîte aux lettres et à se rendre à l'appareil afin de lancer l'impression.

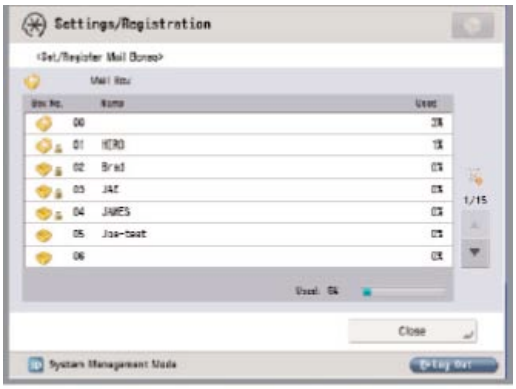
Sécurité de boîte aux lettres avancée

La fonction de boîte aux lettres avancée permet au système imageRUNNER ADVANCE de servir d'espace de stockage et de partage de fichiers. Les utilisateurs peuvent stocker des fichiers dans un dossier partagé ou dans leur espace personnel dans leur format de fichier d'origine, comme Word ou PDF. L'espace personnel de chaque utilisateur est protégé par des justificatifs de sécurité et l'utilisateur doit ouvrir une session pour y accéder. L'utilisateur peut aussi stocker des documents pour que d'autres y aient accès dans le même dossier partagé et dans des sous-dossiers.

La boîte aux lettres avancée permet également aux utilisateurs d'accéder à leurs fichiers stockés à partir du bureau de leur ordinateur au moyen de Windows Explorer en désignant le dossier comme un lecteur réseau. Après avoir accédé au dossier, l'utilisateur doit s'authentifier à l'aide d'une boîte d'ouverture de session Windows.



Affichage du mot de passe d'établissement / stockage dans la boîte



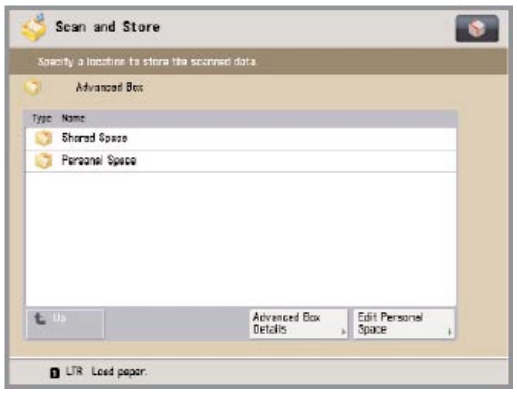
Affichage de destination de stockage dans la boîte aux lettres

Affichage du mot de passe d'établissement / stockage dans la boîte aux lettres

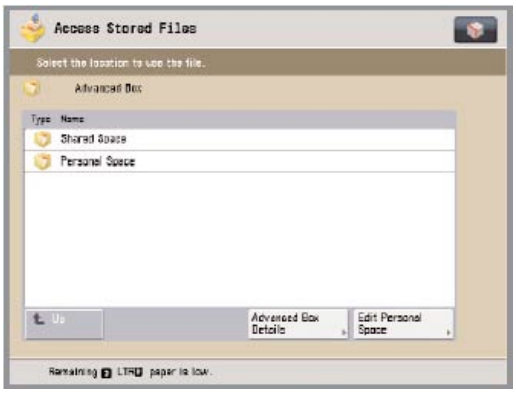
L'administrateur peut gérer les fonctions de la boîte aux lettres avancée par le biais de l'interface utilisateur à distance et exécuter les actions suivantes :

- Créer des comptes d'utilisateur et en définir le type (administrateur ou utilisateur final)
- Activer l'authentification et l'espace personnel
- Enregistrer les appareils du réseau pour y accéder à distance
- Sélectionner les formats de fichier permis pour le stockage (format imprimable seulement, formats Office communs, ou tous). Le fait de se limiter aux formats imprimables seulement, comme TIFF, JPEG et PDF réduit le risque d'infection par des virus qui sont ordinairement joints aux fichiers .exe. De plus, la boîte aux lettres avancée peut être analysée par un logiciel anti-virus lorsqu'elle est partagée comme un lecteur réseau.

Afin de prévenir le stockage de fichiers exécutables pouvant contenir des virus et d'autres codes malveillants, l'administrateur du système peut limiter aux formats imprimables comme PDF, TIFF et JPEG les types de documents pouvant être sauvegardés.



Affichage de numérisation et stockage dans la boîte aux lettres avancée



Affichage d'accès aux fichiers stockés dans la boîte aux lettres avancée

Autres fonctions de sécurité des documents

Filigrane et filigrane de sécurité
Afin de dissuader la copie ou l'envoi non autorisés d'information confidentielle, les systèmes imageRUNNER ADVANCE prennent en charge la capacité d'incorporer un texte défini par l'utilisateur dans l'arrière-plan de travaux d'impression ou de reproduction. Le filigrane apparaît lorsqu'on photocopie le document. La fonction de filigrane de sécurité en option peut être activée pour tous les travaux d'impression ou attribuée par l'utilisateur par le biais du gestionnaire d'impression. L'utilisateur peut également choisir la position où le filigrane personnalisé ou préétabli apparaîtra sur la copie.

Cryptage des fichiers PDF
Le mode Cryptage des fichiers PDF de l'ensemble de fonctions de sécurité Numérisation et envoi en option permet à l'utilisateur de définir les autorisations d'accès aux fichiers PDF envoyés à une adresse électronique ou à un serveur de fichiers, de les crypter et d'en établir le mot de passe pour une sécurité accrue. Seuls les utilisateurs qui entrent le bon mot de passe peuvent ouvrir, imprimer ou modifier le fichier PDF reçu.

Le mode Cryptage des fichiers PDF peut être utilisé uniquement si la destination est une adresse de courriel ou un serveur de fichiers. Si la destination est un numéro de télécopieur, une adresse de télécopie Internet ou une boîte de réception, l'utilisateur ne peut pas envoyer le travail en tant que fichier PDF crypté. Les fichiers PDF cryptés peuvent être sauvegardés à l'aide des algorithmes 40 bits RC4, 128 bits RC4 ou 128 bits AES. Un fichier PDF crypté à 128 bits AES ne peut être ouvert qu'avec Acrobat 7.0 ou une version ultérieure.

Section 3 – Sécurité de l'information

Signature numérique pour PDF (appareil et utilisateur)
Avec la fonction Numérisation et envoi, l'utilisateur peut ajouter des signatures numériques qui attestent la source et l'authenticité d'un document PDF ou XPS. Lorsque le destinataire ouvre un fichier PDF ou XPS sauvegardé avec une signature numérique, il peut voir les propriétés du document et examiner le contenu de la signature, notamment l'autorité de certification, le nom de produit du système, le numéro de série et la date/heure de création du fichier. Si la signature est une signature d'appareil, elle contient également le nom de l'appareil qui a créé le document, alors qu'une signature d'utilisateur atteste l'identité de l'utilisateur authentifié qui a envoyé ou sauvegardé le document.

Les modes Signature numérique de l'appareil pour PDF et XPS utilisent le certificat de signature de l'appareil et la biclé qui constituent la signature de l'appareil pour ajouter une signature numérique au document, ce qui permet au destinataire de vérifier quel appareil a numérisé le document. Si la signature numérique de l'utilisateur pour PDF en option est activée, l'utilisateur peut composer une signature numérique incorporant son nom et son adresse courriel afin de confirmer qu'il est la source du document et d'indiquer si des changements ont été apportés. Afin de pouvoir utiliser le mode de signature numérique de l'utilisateur, l'authentification SSO doit être activée et un certificat valide doit être installé dans l'appareil.

Les systèmes imageRUNNER ADVANCE de Canon prennent également en charge une fonction appelée Signature numérique visible pour PDF, qui affiche obligatoirement la signature numérique à la première page du fichier PDF, ce qui évite au destinataire d'avoir à ouvrir les propriétés du document. L'utilisateur peut sélectionner la signature visible à l'écran de Numérisation et envoi et déterminer sa position et son orientation sur la page. En plus de mettre la signature numérique davantage en évidence, cela assure qu'elle apparaît sur toutes les versions imprimées du document.

Numérotation des jeux de reproduction
Tous les systèmes imageRUNNER ADVANCE ont la capacité d'ajouter des numéros de jeux de reproduction et de les imprimer sur la page à l'endroit défini par l'utilisateur. La numérotation des jeux de reproduction offre une méthode de suivi des documents en établissant le numéro du jeu que reçoit un destinataire.

Gestion des droits Adobe LiveCycle ES*
Une fois créé, un fichier PDF peut en général être échangé ouvertement s'il n'est pas crypté et/ou sécurisé par un mot de passe. Les organisations qui exigent un contrôle plus précis de leurs données peuvent intégrer un système imageRUNNER ADVANCE avec un serveur de gestion des droits Adobe LiveCycle^{MD}ES. Le logiciel de gestion des droits Adobe LiveCycle ES rend possible l'application des politiques de document dynamiques sur le choix des utilisateurs authentifiés autorisés à en voir le contenu, à définir les dates d'expiration, à suivre la diffusion et à définir les filigranes. Une fois que les privilèges du document ont été précisés, le logiciel communique avec le serveur de gestion des droits Adobe LiveCycle^{MD}sur Internet afin d'appliquer la plus récente politique.

Numérisation verrouillée et suivi des documents
La fonction Numérisation verrouillée et suivi des documents en option des systèmes imageRUNNER ADVANCE permet d'intégrer dans l'arrière-plan des documents des données de suivi comme le nom d'utilisateur, la date et le nom de l'appareil. Les utilisateurs ne peuvent pas lire l'information, seul l'administrateur du système y ayant accès. Les données de suivi peuvent également contenir de l'information sur la politique qui détermine si le document peut être reproduit ou numérisé sur d'autres systèmes imageRUNNER ADVANCE dont la fonction Numérisation verrouillée de document est activée.

Veuillez consulter la description plus détaillée de la fonction Numérisation verrouillée et suivi des documents à la section 6 – Ouverture de session et vérification, à la page 30.

** Les formats de fichiers PDF/A-1b et PDF crypté ne sont pas compatibles avec le serveur de gestion des droits Adobe LiveCycle^{MD}ES.*

La fonction de numérisation verrouillée permet d'appliquer les limitations suivantes à un document :

- Limitation complète : Personne ne peut utiliser les fonctions de reproduction/envoi/télécopie.
- Authentification par mot de passe : Autorise la reproduction/envoi/télécopie à la saisie du bon mot de passe.
- Authentification de l'utilisateur : Autorise la reproduction/envoi/télécopie seulement pour l'utilisateur autorisé à l'origine qui ouvre une session à l'appareil avec l'identificateur d'utilisateur et le mot de passe appropriés.

L'administrateur de système peut obliger l'application d'un code de Numérisation verrouillée et suivi des documents à tout travail d'impression, et permettre ou interdire toute reproduction, numérisation, envoi et télécopie de documents contenant le code de suivi caché.

Pour plus d'information sur l'aspect suivi de la fonction Numérisation verrouillée et suivi des documents, veuillez consulter la section *Ouverture de session et vérification* du présent document.

3.2 – Sécurité des données*

Les systèmes imageRUNNER ADVANCE sont dotés de série d'un large éventail de fonctions de sécurité pour l'appareil et le réseau. Canon reconnaît que chaque client a des besoins différents. En conséquence, elle offre diverses options de sécurité avancées afin d'aider les entreprises à atteindre leurs objectifs en matière de confidentialité interne et de conformité aux règlements applicables à certains environnements.

Ces options ont été mises au point conformément aux exigences de sécurité accrues des principaux clients et des organismes gouvernementaux. Canon offre des fonctions de sécurité avancées qui protègent les données stockées dans l'appareil et durant la transmission.

Données au repos

Protection des données du disque dur et de la mémoire vive
L'exploitation normale de tous les systèmes imageRUNNER ADVANCE nécessite un disque dur et une mémoire vive.
Les partitions du disque dur des imageRUNNER ADVANCE sont formatées selon l'un des types de systèmes de fichiers suivants :

- Système de fichiers iR
- Système de fichiers compatible avec le système FAT 32

Le « système de fichiers iR » est un système exclusif à Canon conçu uniquement pour le traitement rapide et efficace des fichiers image. Ce système de fichiers n'est pas compatible avec les systèmes de fichiers couramment utilisés dans les ordinateurs personnels. En conséquence, l'analyse de ses données au niveau des secteurs est extrêmement difficile.

Le « système de fichiers compatible avec le système FAT 32 » est le système qu'utilise l'imageRUNNER Advance pour les zones du disque où sont stockés les fichiers du micrologiciel, des applications MEAP, de la boîte aux lettres et de la boîte aux lettres avancée.

** Certains systèmes imageRUNNER ADVANCE configurés avec la trousse d'écriture miroir du disque dur en option pour le contrôleur d'impression externe peuvent contenir plus d'un disque dur.*

En général, il est difficile d'analyser les données de ces systèmes de fichiers au niveau du secteur. Toutefois, Canon reconnaît que des pirates très motivés et expérimentés pourraient tenter d'obtenir cette information à partir des environnements où l'information sensible est traitée, en analysant les disques durs de ces appareils. Afin de protéger vos renseignements sensibles et confidentiels, les appareils imageRUNNER ADVANCE de Canon comportent un utilitaire de formatage de disque de série ainsi que des accessoires optionnels plus évolués, comme la trousse de suppression des données du disque dur, la trousse de cryptage des données du disque dur ou la trousse de disque dur amovible.

Formatage du disque dur de série*
Les meilleures pratiques, et souvent les politiques d'entreprise, recommandent habituellement que l'administrateur nettoie complètement les systèmes avant de relocaliser les appareils, ou encore à la fin de leur durée utile ou de leur contrat de location. La fonction de formatage du disque dur, offerte de série dans tous les appareils imageRUNNER ADVANCE, est plus qu'une simple fonction de formatage de disque dur. Non seulement cette fonction supprime-t-elle la table d'allocation de fichiers associée à toutes les zones client sur le disque, mais elle écrase aussi toutes les zones de données client sur le disque dur avec des caractères nuls. Les données d'information suivantes sont écrasées :

- données stockées dans les boîtes aux lettres et la boîte aux lettres avancée;
- données stockées dans les boîtes de réception de télécopie / télécopie Internet (boîte de réception de télécopies confidentielle / boîte de réception en mémoire);
- données d'adresse stockées dans le carnet d'adresses;
- paramètres de numérisation enregistrés pour la fonction d'envoi;
- paramètres du mode mémoire enregistrés pour la fonction de reproduction ou de boîtes aux lettres;
- applications MEAP et fichiers de licence;
- données sauvegardées des applications MEAP;
- mot de passe du service d'ouverture de session du SGS (service de gestion du système) de MEAP;
- information d'authentification de l'utilisateur enregistrée dans le système d'authentification d'appareil local de SSO-H (Single Sign-On H);
- documents non envoyés (documents réservés ou réglés avec le mode d'envoi différé);
- historique des travaux;
- réglages/paramètres d'enregistrement;
- formats enregistrés pour le mode de superposition d'image;
- paramètres de réacheminement mémorisés;
- biclé et certificat du serveur enregistrés sous [Certificate Settings] (Réglages du certificat) dans [Device Management] (Gestion de l'appareil) dans les réglages de gestion (à l'écran Réglage et enregistrement).

La fonction de formatage du disque dur livrée de série dans chaque appareil imageRUNNER ADVANCE écrase une fois les données avec des caractères nuls. Si la trousse de suppression des données du disque dur en option est installée, la fonction de formatage du disque dur exécute des options d'écrasement additionnelles, y compris le choix d'effectuer l'écrasement en trois passes conformément à la norme DoD 5022.22M.

** Veuillez consulter le bulletin imageRUNNER n° 5.10 du 26 avril 2010 intitulé Hard Disk Drive Format Technology Procedures for imageRUNNER, imageRUNNER ADVANCE and imagePRESS devices (Technologie de formatage du disque dur des appareils imageRUNNER, imageRUNNER ADVANCE et imagePRESS) pour en savoir davantage.*

Trousse de cryptage des données du disque dur
La trousse de protection du disque dur en option, certifiée niveau 3 (EAL3) sur l'échelle d'assurance des critères communs, protège toutes les données stockées sur le disque interne à l'aide d'algorithmes conformes aux normes de l'industrie. La trousse de protection du disque dur des systèmes imageRUNNER ADVANCE utilise une carte d'extension spéciale qui crypte chaque bit de données avant de l'écrire sur le disque dur en faisant appel au cryptage AES à 256 bits (Advanced Encryption Standard).

Veuillez consulter l'information sur les trousses de protection des données du disque dur en option pour les imageRUNNER ADVANCE de Canon à la Section 9.2.

Trousse de suppression des données du disque dur
La trousse de suppression des données du DD en option permet à l'administrateur du système de configurer l'imageRUNNER ADVANCE pour écraser les données du DD du serveur d'images interne et les données précédentes comme tâche de routine de traitement des travaux. Cette fonctionnalité peut être réglée de manière à écraser les données :

1. une fois avec des données d'intégrité;
2. une fois avec des données aléatoires;
3. trois fois avec des données aléatoires;
4. ou en trois passes conformément à la norme américaine DoD 5022.22M.

Veuillez consulter l'information sur les trousses de protection des données du disque dur en option pour les imageRUNNER ADVANCE de Canon à la Section 9.2.

Moment de l'écrasement des données
Le moment de la suppression dépend du mode et des options de finition choisis lors de l'impression. De façon générale, si un bourrage ou un autre événement anormal met fin à l'opération en cours, les données de la page seront stockées jusqu'à ce que le travail puisse être terminé puis seront écrasées.

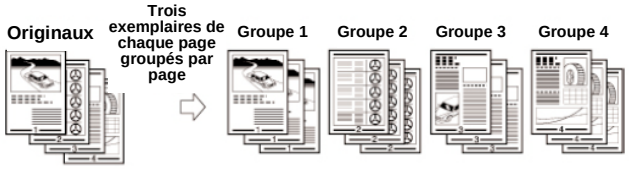
Section 3 – Sécurité de l'information

Les exemples d'écrasement de données suivants illustrent ce qui se passe avec certains modes de travail de l'appareil, avec trois jeux de trois originaux.

1. Modes reproduction et impression

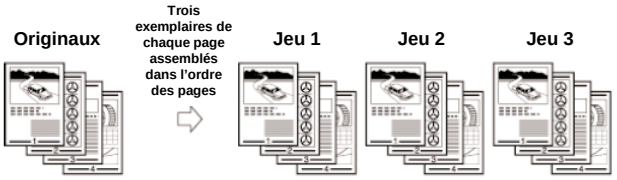
a. Triage de groupe

Lorsque l'utilisateur programme un travail à trier en jeux de groupes sans préciser d'options de finition, les pages de données sont écrasées chaque fois qu'un jeu est complet.



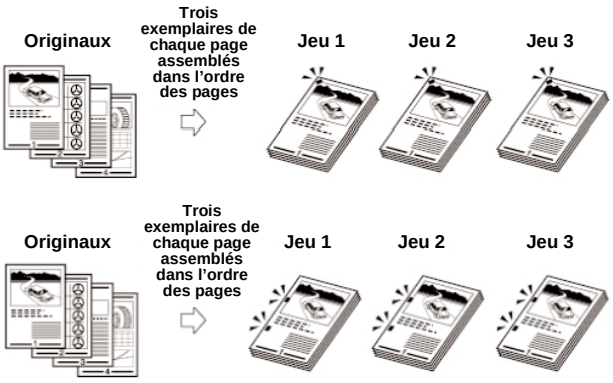
b. Triage-assemblage

Lorsque l'utilisateur programme un travail à trier en jeux assemblés sans préciser d'options de finition, les pages de données sont écrasées chaque fois que la dernière page du dernier jeu est imprimée.



c. Triage-agrafage

Lorsque l'utilisateur programme un travail à trier en jeux agrafés, les pages de données sont écrasées page par page une fois que l'impression de tous les jeux agrafés est terminée.



d. Reproduction à distance ou en cascade

Lorsque l'utilisateur programme un travail de reproduction à distance ou en cascade, selon les réglages choisis, les pages de données sont écrasées page par page, immédiatement, ou sont écrasées page par page une fois que le travail est terminé.

2. **Impression à partir de la boîte aux lettres**

    a. **Impression à partir de la boîte aux lettres**
    Lorsque l'utilisateur imprime un travail stocké dans la boîte aux lettres, toutes les pages sont écrasées immédiatement après la fin du travail.

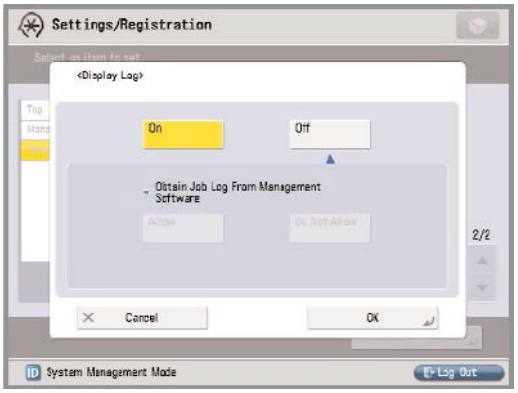
3. **Envoi et numérisation**

    b. **Données d'envoi et de numérisation**
    Lorsque l'utilisateur envoie ou numérise un travail vers une autre destination, toutes les pages de données sont supprimées ou écrasées immédiatement une fois que tout le travail est envoyé.

    c. **Données de télécopie et de télécopie Internet**
    Lorsque la fonction « Rapport d'activités de télécopie » est activée (On), les données sont écrasées immédiatement, dès que l'appareil reçoit une confirmation de transmission réussie.
    En cas d'échec de transmission, les données demeurent pendant que l'appareil effectue un autre essai de transmission. Si la fonction « Rapport d'activités de télécopie » est désactivée (Off), les données sont immédiatement supprimées.

Incidence de l'utilisation de la trousse de suppression des données du disque dur sur le rendement
Il importe de noter que les réglages de la trousse de suppression des données du DD peuvent avoir une incidence sur le rendement de l'appareil, dépendant du type de travail soumis à l'appareil et du niveau de protection par écrasement des données. Si l'on envoie une bonne quantité de gros travaux à l'appareil et que l'option d'écrasement des données à trois reprises est sélectionnée, on doit s'attendre à des retards, même minimes, pour des vitesses supérieures à 50 images par minute (ipm). Pour les appareils ayant une vitesse inférieure à 50 ipm, les réglages de la trousse de suppression des données du DD n'auront aucune incidence sur le rendement.

Trousse de disque dur amovible
La trousse de disque dur amovible en option des imageRUNNER constitue, pour un administrateur de système, un moyen de verrouiller physiquement le disque dur interne dans l'appareil pendant les heures d'exploitation normales, ce qui diminue le risque de vol. Une fois l'appareil arrêté, le disque peut être déverrouillé et retiré pour être remisé dans un endroit sûr.



Affichage de dissimulation du registre de travaux

Fonction de dissimulation du registre de travaux
La fonction de dissimulation du registre de travaux, livrée de série, cache les travaux traités par le système pour éviter que des utilisateurs en libre-service ou des utilisateurs du réseau, depuis l'interface utilisateur à distance, ne les visualisent. L'administrateur peut quand même accéder au registre de travaux, bien qu'il soit caché, et l'imprimer afin de montrer l'utilisation des fonctions de reproduction, de télécopie, d'impression et de numérisation de l'appareil.
L'administrateur peut sélectionner [On] ou [Off] pour la fonction de dissimulation du registre de travaux, sous Settings / Registration > Management Settings > Device Management > Display Log (Réglages / Enregistrement / Paramètres de gestion > Gestion du périphérique > Affichage du registre).

Le registre paraît lorsque [On] est sélectionné. Si l'on a choisi [Off] à l'affichage du registre des travaux, les fonctions et réglages suivants ne paraissent pas à l'écran et ne sont pas activés :

- reproduction, envoi, télécopie et registre d'impression au moniteur système;
- réception au moniteur système du rapport de gestion d'envoi lorsque le système est équipé de la trousse de numérisation et d'envoi de Canon, disponible en option;
- rapport de gestion de télécopie;
- impression automatique désactivée [Off], ce qui désactive le rapport d'envoi et de télécopie quotidien.

Le réglage par défaut de la fonction de dissimulation du registre de travaux est [Off] (désactivé).

Essentials (Workflow Composer)
La suite Essentials pour l'imageRUNNER ADVANCE de Canon comprend la composante Workflow Composer qui permet à l'utilisateur et à l'administrateur de créer des flux de travaux personnalisés afin d'automatiser les tâches redondantes et d'intégrer les systèmes dorsaux au moyen de connecteurs. L'administrateur peut créer des flux de travaux à l'intention des utilisateurs afin de réduire les erreurs d'envoi de documents et de limiter aux personnes désignées l'accès aux opérations qui interagissent avec les systèmes dorsaux.

Chaque système imageRUNNER ADVANCE comporte un module de plateforme sécurisé (TPM), une puce de sécurité aux normes ouvertes inviolable responsable du cryptage et du décryptage d'information comme les mots de passe, les certificats, les noms d'utilisateur et les clés de cryptographie. La puce TPM protège les données du disque dur interne car la clé de cryptage se trouve à un endroit distinct. Une fois activé, l'appareil ne démarrera pas pour se protéger des attaques physiques si la puce TPM est retirée.

La puce TPM est désactivée par défaut. Cette fonction peut être activée sur les appareils imageRUNNER ADVANCE de Canon à partir du menu Fonctions supplémentaires. Une fois activée, il est important de sauvegarder la puce TPM en cas de défaillance, par l'intermédiaire de la mémoire USB.

Données en transit

Impression sécuritaire à données cryptées
L'impression sécuritaire à données cryptées utilise le solide cryptage AES à 256 bits pour protéger les données de votre travail d'impression en cours de transmission sur le réseau. Afin de protéger le travail contre l'impression sans surveillance, la fonction d'impression sécuritaire à données cryptées le retient dans une file jusqu'à ce que l'utilisateur saisisse son mot de passe au panneau de commande.

Cryptage des fichiers PDF
La fonction de cryptage des fichiers PDF des systèmes imageRUNNER ADVANCE prend en charge le cryptage à 40 bits/128 bits RC4 et le cryptage 128 bits AES (Advanced Encryption Standard) afin de mieux sécuriser l'envoi des documents. Un fichier PDF crypté à 128 bits AES ne peut être ouvert qu'avec Acrobat 7.0 ou une version ultérieure.

Pour plus d'information, veuillez consulter la sous-section *3.1 – Sécurité des documents*, sous la section *Sécurité de l'information.*

3.3 – Sécurité des télécopies

Carte de télécopie Super G3 et carte de télécopie à plusieurs lignes

Les systèmes imageRUNNER ADVANCE de Canon qui prennent en charge la télécopie Super G3 avec la carte de télécopie Super G3 installée peuvent être branchés au réseau téléphonique public commuté pour l'envoi et la réception de données de télécopie. Afin de maintenir la sécurité des réseaux des clients par rapport à cette interface potentielle, Canon a conçu ses cartes de télécopie Super G3 pour qu'elles fonctionnent en tenant compte des impératifs de sécurité suivants.

Mécanisme de communication de la carte de télécopie Super G3
Le modem de la carte de télécopie Super G3 n'est pas doté de la capacité de transmission des données, mais seulement de la transmission des télécopies. Résultat : la communication TCP/IP par la ligne téléphonique est impossible. De plus, il n'existe aucun module fonctionnel tel un service d'accès à distance permettant la communication entre une ligne téléphonique et une connexion réseau dans l'appareil.

Transmission de télécopie
La fonction de télécopie d'un ordinateur personnel peut télécopier des documents depuis l'ordinateur par un réseau en utilisant le gestionnaire de télécopie de l'ordinateur. Cependant, le transfert de données d'un ordinateur personnel par un réseau vers l'appareil et le transfert des données (transmission de télécopie) de la ligne téléphonique par la carte de télécopie G3 sont structurellement séparés.

Réception de télécopie
Bien que l'on puisse accéder, par le réseau, à une télécopie reçue au moyen de la fonction de boîte aux lettres confidentielle intégrée à l'appareil ou acheminer automatiquement la télécopie reçue vers un réseau, il n'est pas possible de porter atteinte au réseau dans l'un et l'autre cas car on n'accède à ces capacités qu'une fois la communication de la télécopie terminée. Étant donné que les données stockées dans la boîte aux lettres confidentielle ont un format exclusif à Canon, il n'y a aucune menace d'infection par un virus. Même si l'appareil recevait un fichier de données prétendant être un fichier de données image de télécopie mais que celui-ci contenait un virus, les données reçues devraient d'abord être décodées. En essayant de décoder le virus, la ligne téléphonique serait déconnectée, un code d'erreur au décodage apparaîtrait et les données reçues seraient supprimées. Les cartes de télécopie Super G3 ne peuvent pas recevoir de fichiers de données; elles ne peuvent que recevoir et décoder des transmissions de télécopies. Ainsi, les fichiers infestés de virus qui sont envoyés à un appareil imageRUNNER ADVANCE par sa ligne téléphonique ne peuvent être traités.

Invitation à émettre une télécopie
L'invitation à émettre une télécopie est la seule fonction qui permet aux utilisateurs de traiter des documents stockés dans une case d'invitation à émettre. Toute action liée aux documents ainsi stockés est exécutée au moyen des protocoles de télécopie G3, qui ne fournissent aucun moyen d'accéder au réseau local.

Autres fonctions de télécopie

Transfert des télécopies / Acheminement des télécopies dans la boîte aux lettres
La fonction de transfert des télécopies permet aux appareils imageRUNNER ADVANCE équipés d'une carte de télécopie de transférer des télécopies entrantes à des destinataires particuliers. Pour cela, il faut définir des conditions préalables ou stocker les télécopies dans une boîte de réception en mémoire sécurisée en vue de l'impression ultérieure plutôt que de laisser les messages d'arrivée s'empiler dans un plateau à la vue de tous.

Acheminement des télécopies dans la boîte aux lettres avancée et Avis de réception de télécopie
Tout comme pour la fonction de transfert des télécopies, les systèmes imageRUNNER ADVANCE prennent en charge la capacité de définir des règles d'acheminement distinctes en fonction de la ligne de réception de la télécopie. Chaque télécopie peut être acheminée vers un espace partagé ou personnel particulier d'une boîte aux lettres avancée, une base de données, un serveur de fichiers, une boîte de réception de télécopies confidentielles ou un autre télécopieur. Lorsqu'elle est utilisée avec la fonction de transmission de travail vers la boîte aux lettres avancée, la fonction d'avis de réception de télécopie envoie immédiatement un courriel au destinataire désigné pour lui signaler l'arrivée d'une nouvelle télécopie.

Confirmation de la destination de la télécopie
Afin de prévenir l'envoi par inadvertance d'une télécopie au mauvais destinataire, les appareils imageRUNNER ADVANCE offrent une fonction de confirmation du numéro de télécopie entré pour une protection additionnelle. Lorsque l'administrateur active cette fonction, les utilisateurs doivent entrer de nouveau le numéro de télécopieur du destinataire avant l'envoi afin de confirmer qu'il correspond au numéro original spécifié. Si les numéros ne correspondent pas, l'utilisateur est invité à entrer de nouveau le numéro original et à le confirmer.

Espace de stockage des télécopies

Sécurité des télécopies dans la boîte aux lettres et la boîte aux lettres avancée
Les télécopies entrantes dans les systèmes imageRUNNER ADVANCE peuvent être acheminées automatiquement vers une boîte aux lettres ou une boîte aux lettres avancée désignée, laquelle peut être protégée par un mot de passe afin que les personnes non autorisées n'en voient pas le contenu.

Les personnes non autorisées utilisent le plus souvent un réseau, avec ou sans fil, pour accéder à un appareil connecté. Canon confère aux administrateurs une foule de puissantes commandes pour limiter l'accès aux utilisateurs et aux appareils autorisés, pour activer et désactiver des services du système et pour protéger le caractère confidentiel de l'information transmise par le réseau grâce à de solides technologies de cryptage.

Section 4 – Sécurité du réseau

4.1 – Sécurité du réseau et de l'impression (trousse d'imprimante réseau Canon seulement)

Les systèmes imageRUNNER ADVANCE intègrent de nombreuses fonctions de sécurité du réseau hautement configurables qui aident à sécuriser l'information lorsque la trousse d'imprimante réseau en option est installée. Les fonctions de sécurité du réseau de série comprennent la capacité de permettre uniquement aux utilisateurs et aux groupes autorisés d'imprimer à l'appareil, ce qui limite les communications de l'appareil aux adresses IP/MAC désignées et contrôle la disponibilité des protocoles et des ports du réseau de la manière voulue.

Activation et désactivation de protocoles et d'applications

Par le biais des utilitaires de paramétrage et d'installation de l'appareil de Canon, l'administrateur de réseau peut configurer certains protocoles et ports de service de l'appareil. Cela bloque efficacement les communications non voulues avec l'appareil de même que l'accès au système par le biais de protocoles de transmission particuliers.

Les systèmes imageRUNNER ADVANCE de Canon donnent la possibilité de désactiver les ports TCP/IP non utilisés afin de rehausser la sécurité des appareils. La désactivation des ports a un effet sur les fonctions et les applications offertes par l'appareil. Voici la liste des ports configurables*.

Nom	Port	Description	Chemin de la configuration	Fonctions touchées par ce port
FTP	TCP 21	Transfert de fichiers [Commande]	Settlings / Registration > Preferences > Network > TCP / IP Settings > FTP Print Settings (Réglages / Enregistrement > Préférences > Réseau > Réglages TCP/IP > Paramètres d'impression FTP)	S'il est désactivé, les options d'impression/numérisation FTP sont également désactivées.
SMTP	TCP 25	Simple Mail Transfer Protocol Protocole SMTP	Settings / Registration > Preferences > Function Settings > Send > Email / I-Fax Settings Communication Settings (Réglages / Enregistrement > Préférences > Réglage des fonctions > Envoi > Réglages courriel / télécopie Internet > Réglages de communication)	Ce port active les fonctions de courriel et de télécopie Internet.
HTTP	TCP 80	World Wide Web HTTP Protocole HTTP	Settings / Registration > Preferences > Network > TCP / IP Settings > Use HTTP (Réglages / Enregistrement > Préférences > Réseau > Réglages TCP/IP > Utiliser HTTP)	Aucun accès à l'interface utilisateur à distance de l'imageRUNNER si ce port est désactivé. L'impression IPP cesse si ce port est désactivé.
netbios-ssn	TCP 139	NETBIOS Session Service Protocole de session NetBIOS	Settings / Registration > Preferences > Network > SMB Server Settings > Use SMB (Réglages / Enregistrement > Préférences > Réseau > Réglages du serveur SMB > Utiliser SMB)	Touche la numérisation vers un dossier Windows.
HTTPS	TCP 443	Protocole HTTP sur TSL/SSL. Peut être utilisé avec les fonctions suivantes :		S'il est activé, tout le trafic réseau entre l'ordinateur personnel de l'utilisateur et l'appareil imageRUNNER par l'interface utilisateur à distance est sécurisé.
		Interface utilisateur à distance	Settings / Registration > Management Settings > License / Other > Remote UI > Select On > Use SSL, Select On or Off (Réglages / Enregistrement > Paramètres de gestion > Licence / Autre > IU à distance > Activer (ON) > Utiliser SSL, Activer (ON) ou Désactiver (OFF))	
		Réglages MEAP	Settings / Registration > Management Settings > License / Other > MEAP Settings > SSL Settings > Select On or Off (Réglages / Enregistrement > Paramètres de gestion > Licence / Autre > Réglages MEAP > Réglages SSL, Activer (ON) ou Désactiver (OFF))	
		Paramètres d'impression IPP	Settings / Registration > Preferences > Network > TCP/IP Settings > IPP Print Settings > Select On > Use SSL, Select On or Off (Réglages / Enregistrement > Préférences > Réseau > Réglages TCP/IP > Paramètres d'impression IPP > Activer (ON) > Utiliser SSL, Activer (ON) ou Désactiver (OFF))	
		Paramètres de transmission de l'information aux appareils	Settings / Registration > Management Settings > Device Management > Device Information Delivery Settings > Restrict Receiving for Each Function > Select On or Off (Réglages / Enregistrement > Paramètres de gestion > Gestion des appareils > Paramètres de transmission de l'information aux appareils > Restrictions de réception pour chaque fonction > Activer (ON) ou Désactiver (OFF))	

		Confirmation des NIP des identificateurs de service	Settings / Registration > Preferences > Network > TCP/IP Settings > Confirm Department ID PIN > Select On or Off (Réglages / Enregistrement > Préférences > Réseau > Réglages TCP/IP > Confirmation des NIP des identificateurs de service > Activer (ON) ou Désactiver (OFF))	
		Courriel / télécopie Internet : Authentification/cryptage	Settings / Registration > Function Settings > Send > E-Mail / I-FAX Settings > Communication Settings > Authent./Encryption > Allow SSL (SMTP Receive), Allow SSL (SMTP Send), and Allow SSL (POP) (Réglages / Enregistrement > Réglage des fonctions > Envoi > Réglages courriel / télécopie Internet > Réglages de communication > Authent./Cryptage > Autoriser SSL (Réception SMTP), Autoriser SSL (Envoi SMTP), et Autoriser SSL (POP))	
IMPRIMANTE	TCP 515	Fonction de file d'attente	Settings / Registration > Preferences > Network > Use Spool Function > Select On or Off (Réglages / Enregistrement > Préférences > Réseau > Utilisation de la fonction File d'attente > Activer (ON) ou Désactiver (OFF))	La désactivation de ce protocole fait cesser l'impression LPR.
IPP	TCP 631	IPP (Internet Print Protocol) (Protocole d'impression Internet)	Settings / Registration > Preferences > Network > TCP / IP Settings > IPP Print Settings > Select On or Off (Réglages / Enregistrement > Préférences > Réseau > Réglages TCP/IP > Paramètres d'impression IPP > Activer (ON) ou Désactiver (OFF))	La désactivation de ce protocole cause l'arrêt de l'impression IPP.
HTTP (Meap)	TCP 8000	Protocole HTTP pour MEAP	Settings / Registration > Management Settings > License / Other > MEAP Settings > SSL Settings > Select On or Off (Réglages / Enregistrement > Paramètres de gestion > Licence / Autre > Réglages MEAP > Réglages SSL, Activer (ON) ou Désactiver (OFF))	La désactivation met fin à l'accès à la page du SGS MEAP et à d'autres applications MEAP comme iWAM pour MEAP.
RAW	TCP 9100	Imprimante TCP / IP standard (RAW)	Settings / Registration > Preferences > Network > TCP / IP Settings > RAW Print Settings > Select On or Off (Réglages / Enregistrement > Préférences > Réseau > Réglages TCP/IP > Paramètres d'impression RAW > Activer (ON) ou Désactiver (OFF))	La désactivation met fin à l'impression suivant le protocole d'impression TCP/IP standard.
SNMP	UDP 161	Simple Network Management Protocol (Protocole de gestion de réseau simple)	Settings / Registration > Preferences > Network > TCP / IP Settings > SNTP Settings > Select On or Off (Réglages / Enregistrement > Préférences > Réseau > Réglages TCP/IP > Réglages SNMP > Activer (ON) ou Désactiver (OFF))	La désactivation a pour effet que les utilitaires de gestion comme iW EMC ne découvrent pas et ne peuvent pas gérer les appareils imageRUNNER.

** Les paramètres des ports utilisés et des ports par défaut peuvent varier selon le modèle.*

Filtrage d'adresse IP

Grâce à la fonction de réglage de transmission/impression, le gestionnaire du système peut limiter l'accès du réseau à l'appareil à des adresses ou à des plages d'adresses IP particulières pour l'impression et des réglages/furetage. Il est possible de préciser les réglages d'un maximum de huit adresses individuelles ou consécutives. Par la suite, le gestionnaire du système peut autoriser l'accès à une plage d'adresses, mais le refuser à des adresses particulières à l'intérieur de cette plage.

Filtrage d'adresse MAC (Media Access Control)

Le filtrage d'adresse MAC est utile aux réseaux de plus petite taille dont l'administrateur peut gérer les contrôles de systèmes particuliers, quel que soit le sous-réseau auquel ils sont connectés. Dans les environnements utilisant le protocole DHCP (Dynamic Host Configuration Protocol) d'attribution des adresses IP, le filtrage d'adresse MAC peut éviter les problèmes qui surviennent lorsque les locations DHCP arrivent à échéance et qu'une nouvelle adresse IP est accordée à un système. Tout comme pour les filtres d'adresse IP, les filtres d'adresse MAC peuvent servir à permettre ou à refuser l'accès à des adresses précises. On peut enregistrer un maximum de 100 adresses MAC et les ajouter, les modifier ou les supprimer facilement à l'interface utilisateur. Les filtres d'adresse MAC ont une priorité supérieure à celle des filtres d'adresse IP; l'accès aux systèmes nécessaires peut donc être permis ou refusé, même si l'adresse IP du système dicte le contraire.

Cryptage SSL

De nombreuses organisations se préoccupent énormément de la protection des données transférées entre les ordinateurs personnels et les serveurs ou entre ordinateurs. Cependant, quand vient le temps d'échanger ces mêmes données avec un PMF, elles sont presque toujours envoyées en clair. Il est donc possible de capter toutes les données au moment où elles sont envoyées à l'imprimante sur le réseau. Canon peut atténuer ce dilemme avec la prise en charge du cryptage avec couche de sockets sécurisés (SSL) pour certaines transmissions aller et retour à l'appareil imageRUNNER comme l'impression en protocole Internet (IPP), la télécopie Internet, l'IU à distance, l'accès Web et la transmission de l'information aux appareils (DIDF).

Prise en charge d'IPv6

La prise en charge du protocole IPv6 par tous les systèmes imageRUNNER ADVANCE offre une infrastructure réseau plus sûre, améliore l'acheminement et facilite davantage la gestion pour les administrateurs que le protocole IPv4.

Prise en charge d'IPSec

Les systèmes imageRUNNER ADVANCE de Canon prennent en charge une carte IPSec en option qui permet aux utilisateurs d'utiliser IPSec (Internet Protocol Security) afin d'assurer la confidentialité et la sécurité de l'information entrante et sortante de l'appareil, alors qu'elle est en transit sur des réseaux non sécurisés.

IPSec est une suite de protocoles servant à sécuriser les communications IP. IPSec prend en charge l'échange sécuritaire des paquets au niveau IP, où les paquets du flux de données sont authentifiés et cryptés. Il crypte les données de sorte qu'elles ne puissent être lues par des parties autres que le destinataire; il s'assure également que les données ne sont pas modifiées en cours de route et qu'elles proviennent d'une source digne de confiance et assure la protection contre la reprise de la session sécurisée. La fonctionnalité IPSec de l'appareil ne prend en charge que le mode transmission. En conséquence, l'authentification et le cryptage sont appliqués seulement à la partie données des paquets IP.

Voir dans le manuel de l'appareil imageRUNNER ADVANCE particulier les instructions additionnelles sur l'enregistrement des politiques de sécurité fondées sur IPSec.

Méthode d'authentification et de cryptage :
L'une des méthodes suivantes doit être établie pour l'appareil.

- Protection AH (Authentication Header)
  Un protocole de certification d'authentification par détection des modifications aux données communiquées, y compris l'en-tête IP. Les données communiquées ne sont pas cryptées.

- Protection ESP (Encapsulating Security Payload)
  Un protocole qui assure la confidentialité par cryptage tout en attestant l'intégrité et en authentifiant seulement la partie données utiles des données communiquées.

Protocole d'échange de clés

Prend en charge le protocole d'échange de clés IKEv1 (Internet Key Exchange version 1) conforme à ISAKMP (Internet Security Association and Key Management Protocol). IKE comporte deux étapes; à la phase 1, l'association de sécurité (AS) utilisée pour le protocole IKE (IKE SA) est créée, et à la phase 2, l'AS utilisée pour IPSec (IPSec SA) est créée.

Afin d'établir l'authentification selon la méthode des clés prépartagées, il est nécessaire de choisir d'avance une clé prépartagée, qui est un mot-clé (24 caractères ou moins) utilisé pour les deux appareils pour l'envoi et la réception de données. Utilisez le panneau de commande de l'appareil pour régler la même clé prépartagée que le destinataire pour effectuer les communications IPSec et procéder à l'authentification avec la méthode de la clé prépartagée.

Pour choisir l'authentification avec la méthode de la signature numérique, il faut installer un fichier de biclé et un fichier de certificat de l'autorité de certification (AC) créé à l'avance sur un ordinateur personnel à l'aide de l'IU à distance, puis enregistrer les fichiers installés en utilisant le panneau de commande de l'appareil. L'authentification est menée avec les destinataires pour les communications IPSec en utilisant le certificat de l'AC.

Les types de biclés et le certificat de l'AC qui peuvent être utilisés pour l'authentification avec la méthode de signature numérique sont indiqués ci-dessous.

- Algorithme RSA
- Certificat X.509
- Biclé de format n° 12 PKCS

Réseau local sans fil

Les systèmes imageRUNNER ADVANCE de Canon prennent en charge les réseaux sans fil grâce à l'installation d'une carte de réseau local sans fil en option. La carte de réseau local sans fil est compatible avec le protocole IPv6 et prend en charge les plus récentes normes de cryptage de trafic sans fil y compris WEP, WPA et WPA2, en plus de la norme d'authentification IEEE802.1X.

La carte de réseau local sans fil et l'interface réseau standard des systèmes imageRUNNER ADVANCE ne peuvent pas être utilisées simultanément, ce qui élimine la possibilité d'utiliser l'appareil de façon mal intentionnée comme routeur ou pont d'interconnexion entre deux réseaux. La fonctionnalité de communication réseau est automatiquement désactivée pour l'interface de réseau standard lorsque la carte de réseau local sans fil est activée.

IEEE 802.1X

Le systèmes imageRUNNER ADVANCE de Canon prennent en charge le protocole IEEE 802.1x, qui est une norme sur le contrôle d'accès sur réseau par un port. Le protocole fournit l'authentification aux appareils branchés à un port de réseau local et établit une connexion de point à point seulement si l'authentification réussit. Le protocole d'authentification extensible EAP (Extensible Authentication Protocol) est lié aux réseaux avec et sans fil et permet d'utiliser de multiples méthodes d'authentification comme des cartes et des mots de passe à utilisation unique.

Le protocole IEEE 802.1X est déjà pris en charge par de nombreux commutateurs Ethernet; cela peut empêcher que des invités, des indésirables ou les systèmes ingérables qui ne peuvent réussir à s'authentifier se connectent à votre réseau.

Chaîne communautaire SNMP

Les chaînes communautaires sont comme des mots de passe pour les éléments de gestion d'appareils en réseau. Il existe une chaîne communautaire servant à l'accès en lecture seulement à un élément de réseau. La valeur par défaut de cette chaîne communautaire pour la plupart des appareils en réseau est souvent « public » (publique). En utilisant cette chaîne communautaire, une application peut récupérer des données à partir des éléments de la base d'information de gestion du système imageRUNNER ADVANCE. Il existe également une chaîne communautaire lecture/écriture dont la valeur par défaut est habituellement « private » (privée). En utilisant la chaîne communautaire lecture/écriture, une application peut modifier les valeurs des variables de la base d'information de gestion.

Les systèmes imageRUNNER ADVANCE de Canon utilisent les chaînes communautaires publique et privée comme chaînes communautaires SNMP par défaut, mais celles-ci peuvent être renommées selon une valeur définie par l'utilisateur pour une sécurité accrue. De plus, les systèmes prennent en charge SNMPv3, qui fournit une plus grande sécurité en protégeant les données contre le trafiquage, donnant ainsi l'assurance que l'accès est limité aux utilisateurs autorisés grâce à l'authentification et au cryptage des données envoyées sur le réseau.

Pour modifier les chaînes communautaires SNMP, allez à Settings / Registration > Preferences > Network > SNMP Settings (Réglages / Enregistrement > Préférences > Réseau > Réglages SNMP).

Blocage de l'interface USB

L'administrateur contrôle totalement l'activation et la désactivation de l'accès au port USB des imageRUNNER ADVANCE et contrôle de manière indépendante la capacité de connexion aux ordinateurs ou aux périphériques.

Pour obtenir plus d'information sur le blocage de l'interface USB, veuillez consulter la section *Sécurité de l'appareil*.

Numérisation-envoi – Préoccupations concernant la réception de virus par courriel

Les systèmes imageRUNNER ADVANCE dont la fonction Numérisation-envoi est activée rejettent toujours, dès la réception, tout virus joint à un message par courriel.

Les appareils dont la fonction Numérisation-envoi est activée prennent en charge les protocoles de réception de courrier électronique POP3 et SMTP. À la réception, le texte du courriel est séparé de tout fichier joint et, parmi les fichiers joints, seuls les fichiers image TIFF sont imprimés et transférés.

Trois scénarios sont possibles :

- **Données contenant un virus jointes au courriel :**
  À l'exception des fichiers TIFF, tous les fichiers joints reçus par courriel sont rejetés dès leur réception.
- **Virus prétendant être des fichiers TIFF :**
  Les fichiers image TIFF sont comprimés dans des formats comme MH, MR et MMR. Le système imageRUNNER ADVANCE comprime le format TIFF dès sa réception et code l'image de nouveau après l'avoir regénérée. Lorsqu'elle est traitée correctement, l'image originale est rejetée et une nouvelle image est créée, imprimée et transférée. Si une erreur survient durant le processus, les données du fichier TIFF ne sont pas transférées, mais supprimées, et un message signalant l'erreur à l'utilisateur est ajouté au texte du courriel puis est imprimé.
- **Le texte du courriel est un virus :**
  Les données texte du courriel donnent les données Date, Expéditeur, Code d'identification de message, Destinataire ou Objet écrites à la partie supérieure du courriel reçu en vue de l'impression et du transfert. Les données texte du courriel comportent des chaînes de caractères. Si des données binaires comme des données contenant un virus sont utilisées dans le texte du courriel, les données seront endommagées et les données contenant un virus seront rejetées. Même si les données comportant un virus sont des données visibles avec un format d'écriture, il n'est pas possible de les reconnaître comme une écriture parce que les données Date, Expéditeur, Code d'identification de message, Destinataire ou Objet sont jointes au haut de la page.

4.1 – Sécurité du serveur de courrier

Lorsque la fonction numérisation et envoi des appareils imageRUNNER ADVANCE est activée, le service de courrier interne est activé et prend en charge les protocoles POP et SMTP. Afin de protéger le service contre toute attaque ou utilisation inappropriée, l'administrateur peut activer des fonctions de sécurité additionnelles comme l'authentification SMTP et l'authentification POP préalable à l'authentification SMTP.

Authentification SMTP

Afin d'empêcher les utilisateurs non autorisés d'utiliser le serveur SMTP interne de l'appareil, l'administrateur peut activer l'authentification SMTP et désigner un nom d'utilisateur et un mot de passe pour la connexion au serveur.
De plus, l'administrateur peut activer SSL pour toutes les opérations d'envoi et de réception SMTP.

Authentification POP préalable à l'authentification SMTP

À titre de niveau de sécurité additionnel, les systèmes imageRUNNER ADVANCE prennent en charge la capacité permettant à l'administrateur d'activer ou de désactiver la fonction d'authentification POP préalable à l'authentification SMTP. L'authentification POP préalable à l'authentification SMTP rend obligatoire l'ouverture d'une session avec un serveur POP avant qu'il soit possible d'envoyer du courrier par SMTP.

Section 5 – Outils de gestion et de surveillance de la sécurité

Canon fournit de nombreux outils pour aider les organisations à mettre en œuvre les politiques internes de leur entreprise et à respecter les exigences réglementaires. Peu importe si l'on déploie un seul appareil imageRUNNER ADVANCE ou un parc complet de ces appareils, ces solutions permettent d'en vérifier l'utilisation et de limiter l'accès à leurs fonctions dans toute l'entreprise – tant au niveau du groupe qu'à celui de l'utilisateur.

5.1 – Console de gestion d'entreprise imageWARE

La console de gestion d'entreprise imageWARE (EMC) est un utilitaire Web hautement évolutif pour administrateur qui offre un point de contrôle centralisé pour tous les appareils en usage dans l'entreprise. Le logiciel facilite, pour les organisations, la gestion sécuritaire d'un ou de plusieurs appareils imageRUNNER ADVANCE à distance dans un réseau. En vue d'aider à mettre en œuvre et à gérer une infrastructure de PMF, la console de gestion d'entreprise imageWARE facilite la diffusion sécuritaire de la configuration de l'appareil et du carnet d'adresses au moyen du cryptage SSL, de même que la distribution de configurations standard et personnalisées aux postes de travail clients du réseau.

5.2 – Limitation des écrans de configuration de l'appareil

L'administrateur peut, à partir du panneau de commande et de l'interface utilisateur à distance, verrouiller l'accès des utilisateurs non autorisés aux affichages de configuration afin de protéger les données de configuration.

Pour plus d'information sur la limitation d'accès aux écrans de configuration de l'appareil, veuillez consulter la section *Sécurité de l'appareil*.

5.3 – Système de gestion des accès

Le système de gestion des accès donne à l'administrateur la capacité de restreindre l'accès aux fonctions du système au niveau de l'appareil ou de la fonction. Si l'on utilise l'authentification au niveau de l'appareil, les utilisateurs doivent ouvrir une session avant de pouvoir accéder au Menu principal. Si l'on utilise l'authentification au niveau de la fonction, les utilisateurs doivent entrer leurs justificatifs afin de pouvoir utiliser certaines fonctions souvent sensibles.

Pour plus d'information sur le système de gestion des accès, veuillez consulter la section *Sécurité de l'appareil*.

Section 6 – Ouverture de session et vérification

Bien peu de procédures de sécurité peuvent prévenir entièrement la fuite intentionnelle de données confidentielles tout en maintenant la productivité à un haut niveau, mais si une telle fuite venait à se produire, il serait important de pouvoir remonter jusqu'à la source. Canon a mis au point de nombreuses technologies de pointe en vue de fournir aux administrateurs des moyens puissants pour dissuader les fuites et enquêter sur les accès non autorisés.

6.1 – Numérisation verrouillée et suivi des documents

Les utilisateurs et administrateurs des systèmes imageRUNNER ADVANCE peuvent activer la fonction Numérisation verrouillée et suivi des documents en option afin de limiter l'utilisation des originaux imprimés. Si un document est reproduit, numérisé ou télécopié sur un autre appareil imageRUNNER ADVANCE avec la fonction Numérisation verrouillée et suivi des documents installée et activée, l'opération sera bloquée et un enregistrement de la reproduction non autorisée avec le nom de l'utilisateur sera consigné.

La capacité « verrouillage » de la fonction Numérisation verrouillée et suivi doit être séparée de la capacité « suivi » et les détails ci-après doivent être ajoutés.

VERROUILLAGE
Les limitations offertes sont les suivantes :

1. Interdit à tous : Personne ne peut utiliser les fonctions de reproduction / d'envoi / de télécopie.
2. Authentification par mot de passe : Autorise la reproduction / l'envoi / la télécopie à la saisie du bon mot de passe.
3. Authentification de l'utilisateur : Autorise la reproduction / l'envoi / la télécopie seulement pour l'utilisateur autorisé avec l'identificateur et le mot de passe appropriés.

SUIVI

1. Capacité de dissimuler des données de suivi dans un document comme un nom d'utilisateur, la date et l'heure et un nom d'appareil dans l'arrière-plan du document reproduit et imprimé.
2. L'analyseur de code de numérisation de document pour MEAP vous permet de savoir qui a copié ou imprimé le document, à quel moment et à quel appareil, en numérisant simplement le document à l'appareil.
3. Seul le personnel autorisé peut accéder aux données de suivi du document en saisissant un mot de passe.

L'analyseur de code de numérisation de document pour MEAP, disponible uniquement pour les utilisateurs faisant partie du groupe de l'administrateur de système, peut savoir qui a copié ou imprimé le document, à quel moment et à quel appareil, à la simple numérisation du document contenant le code de suivi à l'appareil.

Pour plus d'information sur la fonction Numérisation verrouillée et suivi des documents, veuillez consulter la section *Sécurité des documents*.

6.2 – Module d'extension de gestion comptable de la console de gestion d'entreprise imageWARE de Canon

Le module d'extension de gestion comptable de la console de gestion d'entreprise imageWARE de Canon apporte des capacités de suivi et de vérification améliorées dans l'environnement utilisateur. En plus d'assurer le suivi par identificateur de service ou par compte SSO, le module d'extension de gestion comptable de la console de gestion d'entreprise imageWARE, utilisé avec SSO, permet d'assurer individuellement le suivi de chaque utilisateur.

Le module d'extension de gestion comptable de la console de gestion d'entreprise imageWARE offre les capacités suivantes :

- suivi des travaux de reproduction, numérisation, envoi et télécopie;
- suivi par type de papier, par impression recto et recto verso ou par production de plusieurs pages sur une feuille;
- suivi par appareil;
- suivi par personne, groupe ou service;
- suivi par travaux de reproduction ou d'impression en noir et blanc ou en couleur;
- suivi par codes de facturation à plusieurs niveaux aux fins de facturation;
- analyse de la charge de travail des services/appareils;
- application des limites d'utilisation;
- exportation des rapports;
- saisie des codes de facturation au panneau de commande de l'appareil au moyen d'une application MEAP.

Le module d'extension de gestion comptable de la console de gestion d'entreprise imageWARE de Canon utilise l'identificateur de service des utilisateurs authentifiés pour la gestion et le suivi. Lorsque l'authentification SSO est utilisée, l'administrateur peut établir une correspondance entre les justificatifs de l'utilisateur et le compte Active Directory respectif en vue du suivi.

6.3 – imageRUNNER ADVANCE Tracker de Canon

L'option Essentials de l'imageRUNNER ADVANCE comprend la fonction de suivi Tracker qui permet aux utilisateurs, aux administrateurs et à d'autres services comptables de suivre, de gérer et de répartir les coûts en temps réel afin de prévenir l'utilisation inefficace et le gaspillage. Tracker est une solution sans serveur de recouvrement des coûts que l'on peut consulter au panneau de commande de l'appareil, sur Internet, dans des rapports par courriel automatisés ou par l'intégration au module d'extension de gestion comptable de la console de gestion d'entreprise imageWARE pour la création de rapports plus approfondis.

Section 7 – Solutions Canon et exigences réglementaires

Canon s'engage à offrir les périphériques multifonction les plus sécuritaires qui soient sur le marché d'aujourd'hui. Bon nombre de nos produits respectent ou dépassent les normes des organismes gouvernementaux et des entités privées liées à la certification en matière de sécurité et aux règlements de l'industrie.

7.1 – Critères communs

Depuis le 1er juillet 2002, le Département américain de la défense exige d'un groupe étendu de fournisseurs de matériel et de logiciel commerciaux qu'ils fassent évaluer leurs produits en fonction d'une norme connue sous le nom de Critères communs afin de déterminer s'ils conviennent aux utilisations du Département.

À la suite de l'élaboration des Critères communs, le National Institute of Standards and Technology et le National Security Agency ont, conjointement avec le Secrétariat d'État des États-Unis, travaillé en étroite collaboration avec leurs partenaires au projet des critères communs en vue de produire une entente de reconnaissance mutuelle des évaluations de sécurité des TI qui utilisent les critères communs. Cette entente porte un nom officiel : *Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security*. Il y est énoncé que chaque participant reconnaît les évaluations réalisées selon la méthodologie d'évaluation aux critères communs lorsque des certificats sont émis par les nations qui se reconnaissent mutuellement selon les niveaux d'assurance d'évaluation (Evaluated Assurance Levels, EAL) des critères communs EAL1 à EAL4. Les éléments des niveaux d'assurance d'évaluation EAL5 à EAL7 ne sont pas soumis à l'entente de reconnaissance mutuelle.

Liste des membres acceptant la reconnaissance mutuelle des critères communs : Australie, Autriche, Canada, République tchèque, Danemark, Finlande, France, Allemagne, Grèce, Hongrie, Inde, Israël, Italie, Japon, République de Corée, Royaume des Pays-Bas, Nouvelle-Zélande, Norvège, Singapour, Espagne, Suède, Turquie, Royaume-Uni et États-Unis.

7.2 – Certification aux critères communs

La norme *Common Criteria for Information Technology Security Evaluation* (Critères communs, ou CC), est une norme internationale (ISO/CEI 15408) qui définit les concepts et principes généraux d'évaluation de la sécurité des systèmes d'information et présente un modèle général d'évaluation. Elle fournit les structures de présentation des objectifs de sécurité des systèmes d'information, de sélection et de définition des exigences de sécurité des systèmes d'information et d'écriture des spécifications de haut niveau pour les produits et les systèmes. Elle précise les exigences fonctionnelles de sécurité de l'information de même que sept niveaux d'évaluation prédéfinis correspondant chacun à un paquet d'assurance pour la mise à l'essai et l'évaluation des fonctions du produit. Les sept niveaux EALS procurent au fournisseur et à l'utilisateur toute la souplesse voulue pour définir les exigences fonctionnelles et d'assurance uniques à leur environnement d'exploitation et obtenir le produit évalué convenant le mieux aux besoins.

Des sociétés de matériel et de logiciel de partout dans le monde utilisent le programme d'évaluation des Critères communs (CC) afin de fournir un moyen de comparaison du niveau d'assurance de leurs produits. Il importe toutefois de noter qu'alors que le programme d'évaluation s'avère très efficace pour valider les prétentions d'un fabricant, il ne mesure pas les capacités globales de sécurité ni les vulnérabilités dans leur ensemble. En conséquence, la certification aux critères communs doit être l'une des nombreuses considérations entrant dans le choix de produits liés à la sécurité au lieu d'être considérée comme LA norme.

Section 8 — Conclusion

Depuis son tout premier lancement, la série d'appareils imageRUNNER de Canon, qui connaît un énorme succès, a rapidement vu progresser ses capacités et ses fonctions. À chaque lancement, ces appareils sont davantage intégrés aux TI et à l'infrastructure de réseau. Comme tout appareil en réseau, les appareils d'imagerie et d'impression doivent être inclus dans le contexte plus vaste de la stratégie de sécurité de l'entreprise en vue d'assurer la confidentialité, l'intégrité et la disponibilité de l'information.

Afin de répondre aux besoins d'une solution de sécurité complète et personnalisable dans tout environnement, les systèmes imageRUNNER ADVANCE de Canon offrent un robuste ensemble de fonctions de série et de composants en option. Lorsqu'ils sont correctement déployés, ces appareils peuvent être protégés efficacement contre les utilisations non intentionnelles ou mal intentionnées. Combinés à des outils de suivi et de gestion avancés pour la vérification et l'administration centralisée, ces systèmes peuvent répondre aux demandes de productivité accrue et de haute sécurité.

Au fur et à mesure que les objectifs de confidentialité des entreprises et les lignes directrices et les règlements deviennent plus stricts, il importe d'évaluer le niveau de sécurité de tous les appareils d'imagerie et d'impression déployés. Après un examen minutieux, les appareils existants peuvent devoir être mis à niveau ou remplacés en fonction de l'environnement unique de chacun.
Canon s'engage à assurer la sécurité de l'information essentielle à toute entreprise et met continuellement au point de nouvelles technologies pour procurer une solution totale et fiable. Pour plus d'information, visitez le site http://www.canon.ca.

Section 9 — Annexe

9.1 – Référence rapide de recommandations de sécurité de Canon

Les besoins de chaque client sont différents et, alors que la responsabilité de la sécurité des données de l'entreprise repose finalement sur les épaules du client, les technologies de sécurité soulignées ci-dessous peuvent aider à prendre en charge les besoins de sécurité de l'information de votre organisation. Canon recommande de procéder aux interventions suivantes à titre de premières étapes appropriées pour sécuriser un système imageRUNNER ADVANCE dans la plupart des environnements. Alors que ces suggestions aident à améliorer la sécurité de l'appareil, ce sont avant tout les politiques de sécurité internes de l'entreprise qui doivent dicter les mesures de sécurité appropriées pour la mise en œuvre dans un environnement particulier.

1. Choisir une forme d'authentification de l'utilisateur et (ou) de commande d'accès
2. Établir le jeu identificateur d'administrateur et mot de passe
3. Désactiver les ports et applications non utilisés (p. ex., FTP, IUD)
4. Définir des mots de passe pour les boîtes aux lettres et les boîtes aux lettres avancées
5. Limiter l'impression et l'accès à l'IUD à des adresses MAC ou IP spécifiques
6. Définir des mots de passe pour la gestion du carnet d'adresses
7. Changer la chaîne communautaire SNMP
8. Désactiver le port USB s'il n'est pas utilisé
9. Utiliser la trousse d'effacement des données du disque dur en option ou la trousse de cryptage des données du disque dur afin d'assurer l'intégrité des données stockées sur les disques durs internes
10. Assurer le suivi des appareils utilisant imageWARE EMC

9.2 – Sécurité du disque dur de l'imageRUNNER ADVANCE de Canon

Fonctions

	Trousse de cryptage des données et d'écriture miroir C1	Trousse de suppression des données C1
Certification aux critères communs	EAL-3	S.O.
Appareils pris en charge	iR ADV C5051, C5045, C5035, C5030, C7065, C7055, C9075 PRO, C9065 PRO	iR ADV C5051, C5045, C5035, C5030, C7065, C7055, C9075 PRO, C9065 PRO
Activation	Installation de la carte de cryptage	Clé d'accès au système de gestion de licences
Désactivation	Désinstallation de la carte	Oui
Cryptage du disque dur	AES (256 bits)	–
Écrasement des données du DD	–	X
Forme d'écrasement	–	Valeur nulle : une fois Données aléatoires : une fois Données aléatoires : 3 fois Mode compatible à DoD 5022.22M
Mot de passe de la boîte aux lettres		
Mot de passe à 7 chiffres requis		
Échec d'authentification 1 Second verrouillage de l'IU		
Double saisie du mot de passe à l'enregistrement		
Mot de passe du gestionnaire du système		
Mot de passe à 7 chiffres requis	–	
Échec d'authentification 1 Second verrouillage de l'IU	–	
Initialisation du mot de passe en mode service	–	X
Double saisie du mot de passe à l'enregistrement	–	
Prise en charge de ScanGear	X	X
Prise en charge du gestionnaire de documents imageWARE^{MD}	X	X
MEAP^{MD}	X	X
Prise en charge du logiciel d'accès Internet	X	X
Cryptage de fichier joint sur la télécopie Internet	X	X
Affichage de la version de la trousse de sécurité	X	X

Légende : X = Fonction offerte – = Sans objet S.O. = Sans objet

L'information fournie dans ce document est l'information la plus récente disponible au moment de sa création. Canon Canada Inc. (« Canon ») rejette expressément par les présentes toute garantie de quelque nature que ce soit, expresse ou implicite, légale ou non, relativement à l'information fournie dans ce document.

Canon, ses filiales ou ses sociétés affiliées, leurs concédants, leurs distributeurs ou leurs détaillants ne seront tenus responsables en aucun cas des dommages directs, spéciaux, conséquents, fortuits ou indirects de quelque nature que ce soit (y compris, sans toutefois s'y limiter, la perte de profits ou de données ou les blessures personnelles), même si Canon, ses filiales ou ses sociétés affiliées, leurs concédants, leurs distributeurs ou leurs détaillants ont été avisés de la possibilité de tels dommages, et Canon, ses filiales ou ses sociétés affiliées, leurs concédants, leurs distributeurs ou leurs détaillants ne seront tenus responsables d'aucune réclamation d'un tiers contre vous découlant de l'utilisation ou du rendement des produits Canon ou des renseignements énoncés aux présentes.

Avis de non-responsabilité réglementaire :
Les énoncés exposés dans ce document reflètent les opinions de Canon Canada. Aucun de ces énoncés ne doit être considéré par les clients ou les détaillants de Canon comme un avis juridique, puisque Canon n'offre aucun conseil en matière de droit ou de conformité en ce qui concerne notamment, sans toutefois s'y limiter, la loi *Sarbanes-Oxley* et la *Loi sur la protection des renseignements personnels et des documents électroniques*. Chaque client doit demander à un conseiller juridique qualifié de déterminer l'avantage d'une solution particulière en ce qui a trait à la conformité aux lois et aux règlements.

Canon

1 800 OK Canon
www.canon.ca

Les spécifications et la disponibilité peuvent être modifiées sans préavis.