GUIDE DE SÉCURISATION DES MULTIFONCTIONS

imageRUNNER ADVANCE

Canon

INTRODUCTION

Les périphériques multifonctions de Canon offrent des fonctionnalités d'impression, de copie, de numérisation, d'envoi et de télécopie. Les imprimantes multifonction sont des serveurs informatiques à part entière, qui fournissent un certain nombre de services réseau et un espace de stockage considérable sur disque dur.

Lorsqu'une entreprise intègre ces appareils à son infrastructure, elle doit régler certaines questions dans le cadre de sa stratégie de sécurité globale de l'entreprise, notamment en termes de confidentialité, d'intégrité des données et de disponibilité de vos systèmes réseau.

Bien entendu, le processus de déploiement varie d'une entreprise à l'autre, et toutes n'ont pas les mêmes besoins en matière de sécurité. Nous travaillons déjà ensemble pour que les appareils Canon vous soient expédiés avec des paramètres de sécurité pré-configurés adaptés. Mais nous allons plus loin en vous fournissant un certain nombre de paramètres de configuration qui vous permettront d'accorder parfaitement votre appareil aux exigences spécifiques de votre entreprise.

Ce guide réunit toutes les informations dont vous avez besoin pour discuter avec Canon ou un partenaire de Canon des paramètres les plus adaptés à votre environnement. Il convient de noter que tous les périphériques ne possèdent pas le même niveau de capacité et que différents logiciels système peuvent fournir des fonctionnalités différentes. Une fois que vous avez décidé de la configuration définitive, vous pouvez l'appliquer à votre imprimante ou parc d'imprimantes. N'hésitez pas à contacter Canon ou un partenaire de Canon pour obtenir de l'aide ou davantage de renseignements.

À qui s'adresse ce guide ?
Ce guide s'adresse à tous ceux qui s'intéressent à la conception, à l'intégration et à la sécurisation des imprimantes multifonction de bureau au sein d'une infrastructure réseau. Il peut s'agir d'ingénieurs informatique et réseau, de spécialistes en sécurité informatique et de professionnels de maintenance.

Portée et champ d'application
Ce guide apporte des explications et des conseils concernant les paramètres de configuration pour deux types d'environnements réseau courants, afin que les entreprises puissent mettre en place une solution multifonction en toute sécurité, en s'appuyant sur de bonnes pratiques. Il explique également comment (à partir de la version 3.8 de la plateforme logicielle du système) la fonctionnalité Syslog peut fournir un retour d'informations en temps réel des multifonctions. Ces paramètres ont été testés et validés par l'équipe Sécurité de Canon.

Nous ne tenons pas compte des exigences réglementaires spécifiques à chaque secteur d'activité et qui peuvent nécessiter la prise en compte d'autres questions de sécurité. Ces questions ne sont pas traitées dans le guide.

Ce guide se base sur les fonctionnalités typiquement disponibles sur la plateforme imageRUNNER ADVANCE. Il convient de noter que le contenu du guide s'applique à tous les modèles et toutes les séries de la gamme imageRUNNER ADVANCE, mais que tous les modèles ne disposent pas exactement des mêmes fonctionnalités.

Mise en œuvre de paramètres de sécurité adaptés à votre environnement sur vos imprimantes multifonction
Pour analyser les conséquences de l'intégration d'une imprimante multifonction à votre réseau en termes de sécurité, nous avons choisi deux scénarios courants :

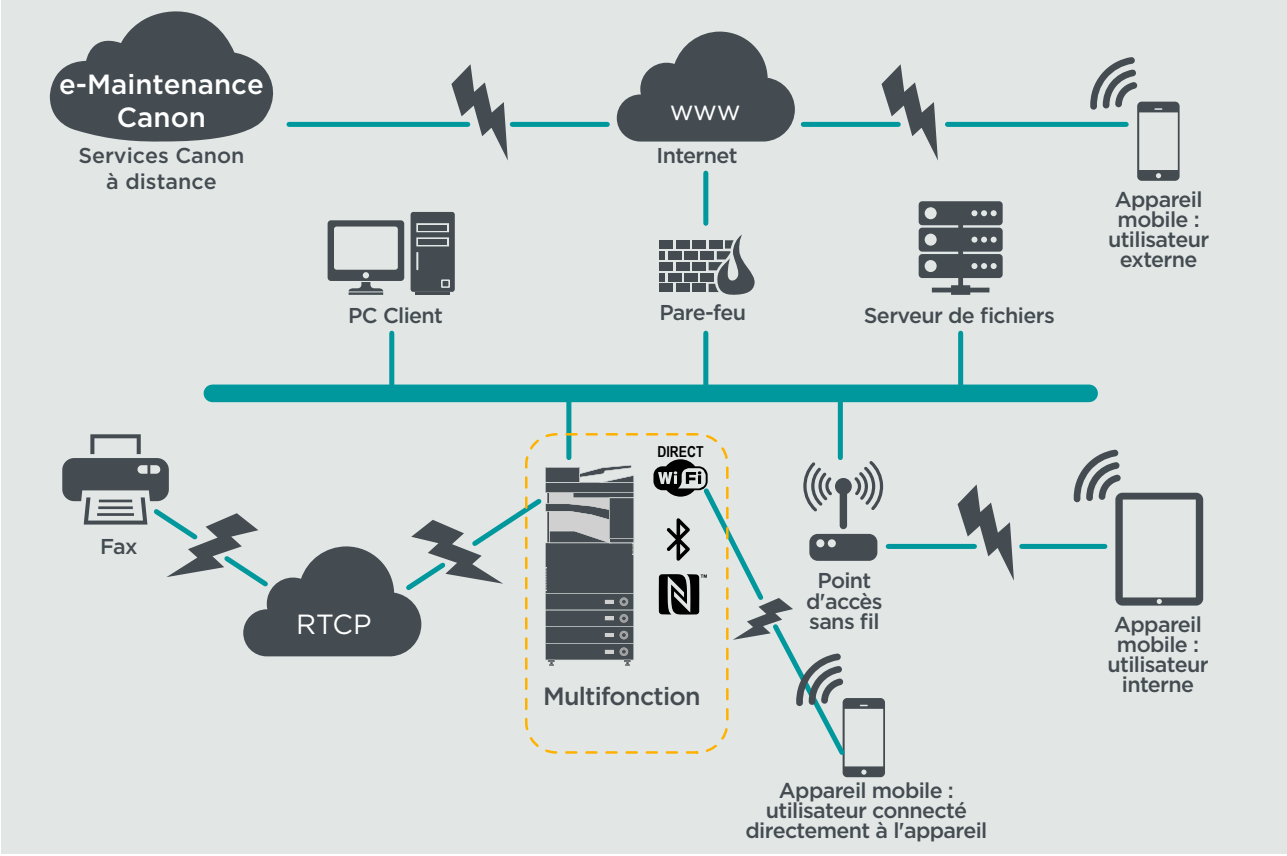
- **L'environnement d'une petite entreprise**
- **L'intégration dans l'environnement d'une grande entreprise**

ENVIRONNEMENT TYPIQUE D'UNE PETITE ENTREPRISE

Il s'agit en général d'une petite entreprise dotée d'un réseau non segmenté.
Elle utilise une à deux imprimantes multifonction en interne et ces appareils ne sont pas accessibles via Internet.

Bien que l'impression mobile soit disponible, celle-ci requiert l'ajout de composants supplémentaires à la solution. Les utilisateurs qui sollicitent les services de l'imprimante en dehors du réseau local doivent se connecter de manière sécurisée. Cette démarche n'est pas décrite dans ce guide. Néanmoins, la vigilance est de mise concernant la sécurité des données qui transitent entre le périphérique distant et l'infrastructure d'impression.

Schéma 1 Le réseau d'une petite entreprise



Les modèles imageRUNNER ADVANCE de dernière génération offrent une connexion réseau sans fil permettant de connecter l'imprimante à un réseau Wi-Fi. Cette fonctionnalité peut également être utilisée pour établir une connexion Wi-Fi Direct entre l'imprimante et un appareil mobile, sans connexion au réseau.

Des options Bluetooth et NFC sont disponibles sur plusieurs modèles et permettent d'établir une connexion Wi-Fi Direct avec, respectivement, des appareils iOS et Android uniquement.

POINTS À CONSIDÉRER POUR LA CONFIGURATION

Veuillez noter que si une fonctionnalité des imageRUNNER ADVANCE n'est pas mentionnée ci-dessous, c'est que nous considérons que ses paramètres par défaut sont suffisants pour le type d'entreprise et d'environnement réseau étudié.

Tableau 1 Points à considérer pour la configuration dans l'environnement d'une petite entreprise

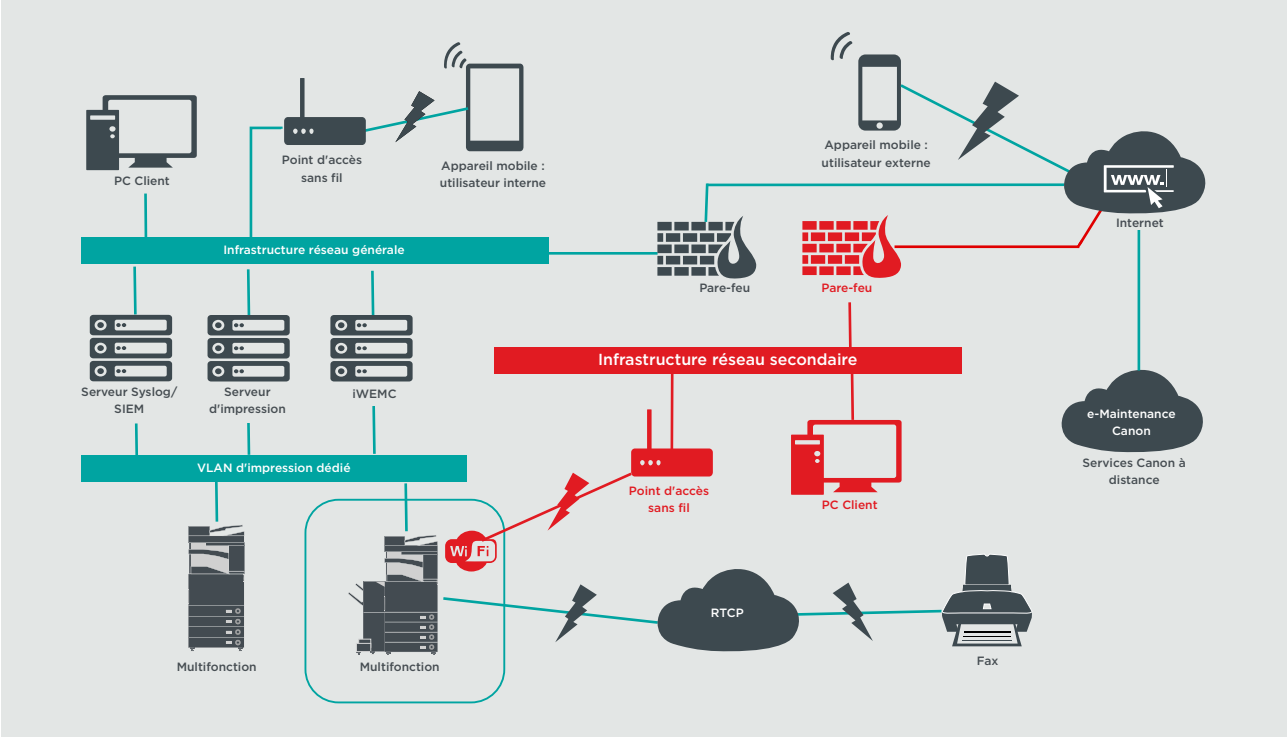
Fonctionnalité imageRUNNER ADVANCE	Description	Points à considérer
Mode service	Permet d'accéder aux paramètres de Mode service.	À protéger par un mot de passe autre que celui par défaut, complexe et de longueur maximale
Système de gestion des services	Permet d'accéder à divers paramètres de périphérique non-standard.	À protéger par un mot de passe autre que celui par défaut, complexe et de longueur maximale
Navigation/envoi SMB	Stockez et récupérez du contenu sur les lecteurs réseau partagés Windows/SMB.	Conformément à la politique de sécurité, les administrateurs système devraient interdire aux utilisateurs de créer des comptes locaux sur le client dans le cadre du partage de documents avec un multifonction imageRUNNER ADVANCE via SMB.
Interface utilisateur distante	Outil de configuration Web	L'administrateur imageRUNNER ADVANCE devrait activer le protocole HTTPS pour l'interface utilisateur à distance et désactiver l'accès via HTTP. Activez l'authentification à l'aide d'un code PIN unique sur chaque appareil.
SNMP	Intégration du système de surveillance du réseau	Désactivez la version 1 et activez uniquement la version 3.
Envoi vers un e-mail et/ou I-Fax	Envoyez des e-mails comportant des pièces jointes depuis l'appareil multifonction.	Activez le protocole SSL. N'utilisez pas l'authentification POP3 avant un envoi SMTP. Utilisez l'authentification SMTP.
POP3	Récupération et impression automatique des documents d'une boîte de messagerie	Activez le protocole SSL. Activez l'authentification POP3.
Carnet d'adresses/répertoire LDAP	Utilisez le service de répertoire pour rechercher un numéro de téléphone fixe ou une adresse e-mail à laquelle envoyer un document numérisé.	Activez le protocole SSL. N'utilisez pas les informations de connexion au domaine pour vous connecter au serveur LDAP ; utilisez des informations de connexion réservées à ce serveur.
Impression FTP	Téléchargez des documents vers/depuis le serveur FTP intégré.	Activez l'authentification FTP. N'oubliez-pas que les données qui circulent sur le réseau à l'aide du protocole FTP ne sont pas cryptées.
Envoi WebDAV	Numérisez et stockez des documents sur un emplacement distant.	Activez l'authentification pour les lecteurs partagés WebDAV.
PDF crypté	Permet de chiffrer des documents.	Conformément à la politique de sécurité, les documents sensibles devraient être chiffrés uniquement à l'aide du format PDF version 1.6 (AES-128).
Impression sécurisée	Les travaux d'impression sont envoyés à l'appareil mais restent bloqués dans la file d'attente tant que le code PIN correspondant n'a pas été saisi.	Activez la protection des travaux d'impression par code PIN.
Notification d'événement Syslog	Le protocole de journalisation système est un protocole standard du secteur utilisé pour envoyer des messages d'événement ou de journal système à un serveur spécifique appelé « Syslog ».	Envisagez d'indiquer les données de Syslog imageRUNNER à l'outil d'analyse Syslog de votre réseau existant ou à la plateforme SIEM (Security Event Management System) de votre entreprise.
Système de vérification au démarrage	Fournit la garantie que les composants logiciels système n'ont pas été compromis. Aura un impact minimal sur le temps de démarrage du système.	Activez la fonction.
Navigateur Web intégré	Accédez à Internet via un navigateur.	Créez une règle d'administration imposant l'utilisation d'un proxy Web permettant de filtrer le contenu afin d'éviter que les utilisateurs n'accèdent à du contenu malveillant ou viral. Désactivez la création de favoris.
Bluetooth et NFC (disponible à partir des modèles de troisième génération)	Utilisée pour établir une connexion Wi-Fi Direct.	Activez Wi-Fi Direct pour permettre la connexion directe avec un appareil mobile. Il n'est pas possible d'utiliser Wi-Fi Direct lorsque la connexion au réseau est effectuée via le Wi-Fi.
LAN sans fil	Fournit un accès sans fil.	Utilisez le mode d'accès protégé au Wi-Fi WPA-PSK/WPA2/PSK et des mots de passe complexes.
IPP	Permet de se connecter et d'envoyer des travaux d'impression via IP.	Désactivez IPP.
TPM	Fonction qui stocke les données de sécurité, telles que les mots de passe ou les clés de cryptage, dans le matériel pour assurer une protection maximale	Cette fonction est désactivée par défaut. Lorsqu'elle est activée, il est recommandé de créer une sauvegarde.

ENVIRONNEMENT D'UNE GRANDE ENTREPRISE

En général, ce type d'environnement se compose de plusieurs sites, plusieurs bureaux et présente une architecture réseau segmentée. Plusieurs multifonctions sont déployés sur un VLAN distinct, accessible pour un usage interne via le ou les serveur(s) d'impression. Ces multifonctions ne sont pas accessibles depuis Internet.

Souvent, ce type d'environnement bénéficie d'une équipe dédiée qui gère les réseaux, les exigences du back-office ainsi que les problèmes informatiques généraux. Toutefois, ce personnel n'a généralement pas de formation spécifique en ce qui concerne les imprimantes multifonction.

Schéma 2 Fonctionnement dans une grande entreprise



Les types de connexion signalés en rouge seront disponibles sur les modèles de 3ème génération.

POINTS À CONSIDÉRER POUR LA CONFIGURATION

Veuillez noter que si une fonctionnalité des imageRUNNER ADVANCE n'est pas mentionnée ci-dessous, c'est que nous considérons que ses paramètres par défaut sont suffisants pour le type d'entreprise et d'environnement réseau étudié.

Tableau 2 Points à considérer pour la configuration dans l'environnement d'une grande entreprise

Fonctionnalité imageRUNNER ADVANCE	Description	Points à considérer
Mode service	Permet d'accéder aux paramètres de Mode service.	À protéger par un mot de passe autre que celui par défaut, complexe et de longueur maximale
Système de gestion des services	Permet d'accéder à divers paramètres de périphérique non-standard.	À protéger par un mot de passe autre que celui par défaut, complexe et de longueur maximale
Navigation/envoi SMB	Stockez et récupérez du contenu sur les lecteurs réseau partagés Windows/SMB.	Conformément à la politique de sécurité, les administrateurs système devraient interdire aux utilisateurs de créer des comptes locaux sur leur ordinateur dans le cadre du partage de documents avec un multifonction imageRUNNER ADVANCE via SMB.
Interface utilisateur distante	Outil de configuration Web	Une fois la configuration initiale des imprimantes effectuée, désactivez le HTTP et le HTTPS pour désactiver l'interface utilisateur à distance.
SNMP	Intégration du système de surveillance du réseau	Désactivez la version 1 et activez uniquement la version 3.
Envoi vers un e-mail et/ou I-Fax	Envoyez des e-mails comportant des pièces jointes depuis l'appareil multifonction.	Activez le protocole SSL. Activez : - La vérification des certificats sur le serveur SMTP ou, si cela n'est pas possible : - Utilisez cette fonctionnalité uniquement dans un environnement doté d'un collecteur de système de détection d'intrusion réseau. N'utilisez pas l'authentification POP3 avant un envoi SMTP, utilisez l'authentification SMTP.
POP3	Récupération et impression automatique des documents d'une boîte de messagerie	Activez le protocole SSL. Activez : - La vérification des certificats sur le serveur POP3 ou, si cela n'est pas possible : - Utilisez cette fonctionnalité uniquement dans un environnement doté d'un collecteur de système de détection d'intrusion réseau. Activez l'authentification POP3.
Carnet d'adresses/répertoire LDAP	Utilisez le service de répertoire pour rechercher un numéro de téléphone ou une adresse e-mail à laquelle envoyer un document numérisé.	Activez le protocole SSL. Activez : - La vérification des certificats sur le serveur LDAP ou, si cela n'est pas possible : - Utilisez cette fonctionnalité uniquement dans un environnement doté d'un collecteur de système de détection d'intrusion réseau. N'utilisez pas les informations de connexion au domaine pour l'authentification sur le serveur LDAP ; utilisez des informations de connexion réservées au serveur LDAP.
IPP	Permet de se connecter et d'envoyer des travaux d'impression via IP.	Désactivez IPP.
Envoi WebDAV	Numérisez et stockez des documents sur un emplacement distant.	Activez l'authentification sur les lecteurs partagés WebDAV et activez le SSL. Créez une règle d'administration de l'imprimante autorisant le chargement uniquement pour les fichiers dotés d'extensions typiques des fichiers d'impression.
IEEE802.1X	Mécanisme d'authentification pour l'accès au réseau	Prise en charge d'EAPOL version 1
PDF crypté	Permet de chiffrer des documents.	Conformément à la politique de sécurité, les documents sensibles devraient être chiffrés uniquement à l'aide du format PDF version 1.6 (AES-128).
Impression sécurisée cryptée	Renforcez la protection offerte par l'impression sécurisée en chiffrant le fichier et le mot de passe au cours de la transmission.	Configurez le nom de l'utilisateur sur l'onglet Imprimante de la boîte de dialogue de configuration de l'imprimante sur le client, de sorte que ce nom d'utilisateur soit différent de celui utilisé par le même utilisateur pour se connecter au serveur LDAP/domaine. Vérifiez que l'option « Limiter l'accès aux travaux d'impression » est désactivée.
Validation automatique des certificats	Le processus de validation automatique améliore l'efficacité de l'extraction et du déploiement des certificats numériques.	Nécessite une solution de certificats réseau à exploiter
Notification d'événement Syslog	Le protocole de journalisation système est un protocole standard du secteur utilisé pour envoyer des messages d'événement ou de journal système à un serveur spécifique appelé « Syslog ».	Envisagez d'indiquer les données de Syslog imageRUNNER ADVANCE à l'outil d'analyse Syslog de votre réseau existant ou à la plateforme SIEM (Security Event Management System) de votre entreprise
Système de vérification au Démarrage	Fournit la garantie que les composants logiciels système n'ont pas été compromis. Aura un impact minimal sur le temps de démarrage du système.	Activez la fonction.
LAN sans fil	Fournit un accès sans fil.	Utilisez le mode d'accès protégé au Wi-Fi WPA-PSK/WPA2/PSK et des mots de passe complexes.
Wi-Fi Direct	Utilisée pour établir une connexion Wi-Fi Direct.	Désactivez Wi-Fi Direct.
Navigateur Web intégré (disponible sur les modèles de 3e génération, 2e édition)	Accédez à Internet via un navigateur.	Appliquez les restrictions appropriées ou désactivez toute option permettant de télécharger des fichiers envoyés via le navigateur.

Les modèles imageRUNNER ADVANCE de dernière génération offrent une connexion réseau sans fil permettant de connecter l'imprimante à un réseau Wi-Fi tout en étant connecté à un réseau filaire. Cela peut s'avérer utile lorsque le client doit partager un périphérique sur deux réseaux. Cela peut-être le cas dans les écoles, qui disposent d'un réseau réservé au personnel et d'un autre pour les élèves.

La plate-forme imageRUNNER ADVANCE offre un environnement riche en fonctionnalités garantissant une grande flexibilité d'utilisation. Compte tenu de tous les protocoles et services disponibles à cette fin, il est important de s'assurer que seuls les fonctionnalités, les services et les protocoles requis sont activés pour répondre aux besoins de l'utilisateur. Il s'agit d'une bonne pratique de sécurité qui réduira le champ d'attaque potentiel et empêchera l'exploitation des données qui s'y trouvent. Alors que de nouvelles vulnérabilités continuent d'apparaître, nous devons rester vigilants à ce que l'appareil ne soit pas compromis, que ce soit de manière intrinsèque ou extrinsèque. Il est utile de pouvoir surveiller l'activité de l'utilisateur pour faciliter l'identification et l'application de mesures correctives, le cas échéant.

La plate-forme logicielle imageRUNNER ADVANCE version 3.8 offre d'autres fonctionnalités s'ajoutant à celles disponibles depuis plusieurs années. Ces fonctionnalités offrent notamment la possibilité de surveiller le périphérique en temps réel à l'aide de Syslog et du système de vérification au démarrage. L'association de ces fonctionnalités aux solutions de sécurité réseau existantes, comme une plate-forme de gestion des événements et des informations de sécurité ou une solution de journalisation, augmente la visibilité sur les incidents et facilite leur identification à des fins légales.

Module de plateforme sécurisée (TPM)

Chaque modèle imageRUNNER ADVANCE comprend un module de plateforme sécurisée (TPM), c'est-à-dire une puce de sécurité standard ouverte résistante aux températures élevées (les modèles imageRUNNER ADVANCE DX disposent d'un module TPM 2.0). Ce module est responsable du stockage des mots de passe, des certificats numériques et des clés cryptographiques.

Tous les modèles imageRUNNER ADVANCE actuels équipés d'un disque dur ou d'un disque SSD offrent un cryptage complet, dont la clé de cryptage est stockée dans la puce de sécurité Canon MFP, conformément à la norme de sécurité FIPS 140-2 de niveau 2 (établie par le gouvernement des États-Unis), et non dans le TPM.

Par défaut, la fonctionnalité TPM est désactivée. Toutefois, vous pouvez l'activer en accédant au menu Fonctions supplémentaires de votre imageRUNNER ADVANCE. Il est fortement recommandé de sauvegarder le module TPM immédiatement après son activation, en prévention d'une panne. Notez que ce module ne peut être sauvegardé qu'une seule fois sur une clé USB.

Pour plus d'informations sur le module TPM, accédez au lien ci-dessous via votre navigateur Web et saisissez **Utilisation du TPM** dans la zone de recherche. Vous pourrez ainsi accéder à des informations liées aux domaines suivants :

- Activation du module TPM
- Sauvegarde et restauration du module TPM

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Système de vérification au démarrage

Cette fonctionnalité est un mécanisme matériel qui s'assure que toutes les parties du logiciel système imageRUNNER ADVANCE de troisième génération 3ème édition sont vérifiées grâce à la fonctionnalité Root of Trust (ROT) afin de garantir que le système d'exploitation se charge comme Canon l'a prévu. Si une personne malveillante cause une altération ou tente de modifier le système ou si une erreur se produit lors du chargement du système, le processus s'arrête et un code d'erreur s'affiche.

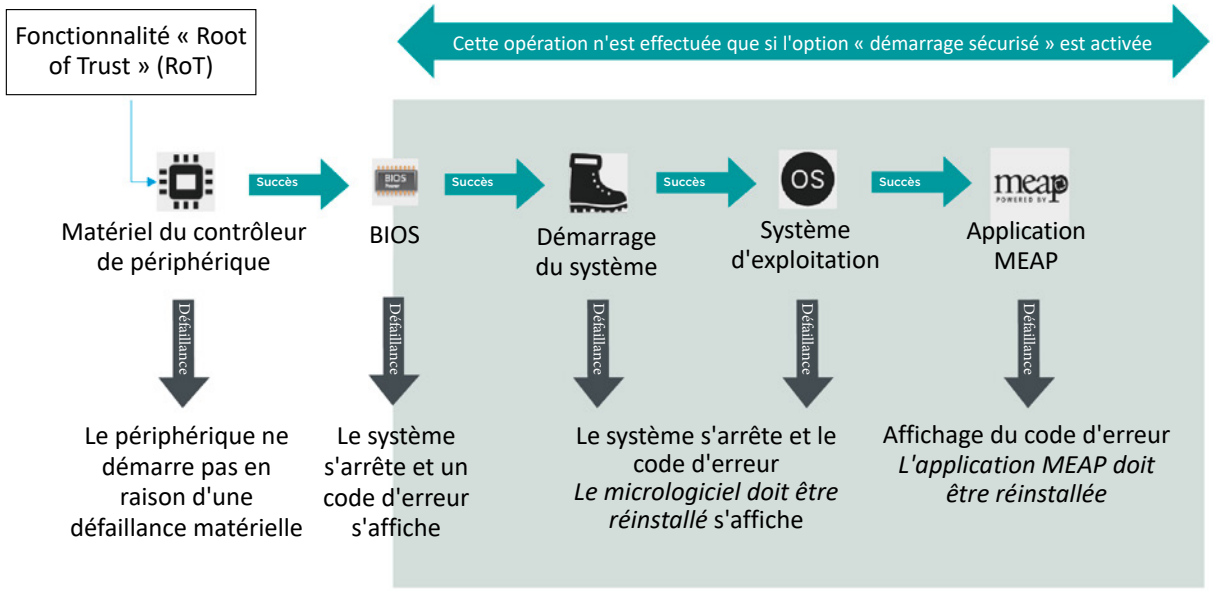


Schéma 3 Processus de vérification du système au démarrage

Ce processus est transparent pour l'utilisateur, en dehors du message indiquant qu'une version système non autorisée est en cours de chargement. La technologie imageRUNNER ADVANCE de troisième génération 3ème édition dispose d'une option d'activation de la vérification du système au démarrage. Cette option doit être activée pour que cette fonction de sécurité soit exécutée.

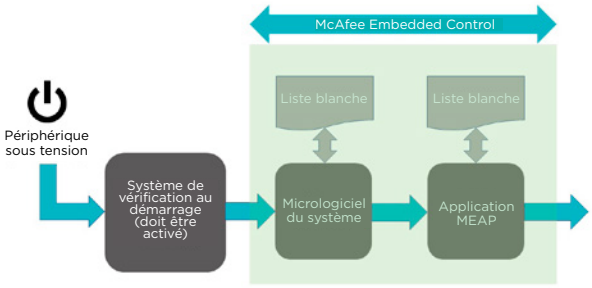


Schéma 4 Processus de démarrage du périphérique à partir du démarrage et pendant l'exécution

McAfee Embedded Control

Avec l'ajout de McAfee Embedded Control à partir de la plateforme 3.9, une couche supplémentaire de protection des périphériques est fournie aux modèles imageRUNNER ADVANCE de troisième génération 3e édition. Les modifications non autorisées apportées au micrologiciel système ou à l'environnement MEAP peuvent, selon leur gravité, arrêter le périphérique avec un code d'erreur ou consigner l'événement dans le journal d'audit pour que l'administrateur puisse l'analyser.

Avec l'ajout de McAfee Embedded Control à partir de la plateforme 3.9, une couche supplémentaire de fichiers programmes non répertoriés dans la liste blanche est considérée comme non autorisée et ne sera pas autorisée à s'exécuter. Cela permet d'éviter que des vers, des virus, des logiciels espions et autres programmes malveillants compromettent le périphérique. Un journal de toutes les exécutions qui ont été empêchées est disponible dans le journal d'audit en cas d'activation. McAfee Embedded Control offre les avantages suivants :

- Prévention de l'altération de logiciels pendant l'exécution grâce à la mise en œuvre de la « liste blanche » produite par McAfee
- Selon la gravité, l'imprimante sera arrêtée avec un code d'erreur ou l'événement sera consigné dans le journal d'audit pour que l'administrateur puisse en prendre connaissance
- McAfee Embedded Control est une fonctionnalité standard sur les modèles de troisième génération 3e édition
- Désactivé par défaut : pour démarrer le service, activez la fonctionnalité de vérification du système au démarrage et McAfee Embedded Control
- Lorsque ces deux derniers sont activés, le temps de préchauffage est plus long (jusqu'à 60 secondes)
- Si le mode de démarrage rapide du périphérique est activé, même avec la vérification du système au démarrage, McAfee Embedded Control est sans effet

McAfee Embedded Control vérifie la valeur indiquée dans la liste blanche avant l'exécution du module. Il vérifie en outre la valeur générée par l'exécution du module pendant le fonctionnement. Si les deux valeurs sont identiques, la vérification est réussie. Si elles sont différentes, la vérification est un échec et l'exécution du module échoue. Voici ce qui se produit si la vérification est un échec :

(a) Le processus de vérification du micrologiciel commence lorsque le module d'exécution répertorié dans la liste blanche est démarré. Si la vérification échoue, l'exécution est bloquée et un code d'erreur (E614-xxxx) s'affiche.

(b) Lorsqu'une tentative d'exécution d'un module logiciel non répertorié est détectée, l'exécution s'arrête et l'événement est consigné dans le journal d'audit.

(c) Lorsqu'une tentative de réécriture ou de suppression d'un module logiciel répertorié dans la liste blanche est détectée, cette tentative est bloquée et le code d'erreur est consigné dans le journal d'audit.

(d) La validation de la liste blanche elle-même est effectuée au démarrage. Si une altération de la liste blanche est détectée, l'exécution est bloquée et un code d'erreur s'affiche. Le code d'erreur s'affiche en fonction de l'emplacement du module logiciel sur lequel une altération a été détectée. Exemple de code d'erreur : E614-xxxx pour un micrologiciel, E602-xxxx pour une application MEAP.

(e) Si nécessaire, la liste blanche est mise à jour lorsque le micrologiciel système est mis à jour ou lorsque des applications MEAP autorisées sont installées. Pour garantir la cohérence, lorsque le module logiciel est mis à jour, la liste blanche et le journal des transactions qui consigne l'historique des modifications apportées à la liste blanche sont également mis à jour.

Toutes les activités consignables qui concernent les processus relatifs à la vérification du système au démarrage et à McAfee Embedded Control sont répertoriées dans le journal de gestion du périphérique. Un administrateur de sécurité peut être informé de ces activités en temps réel grâce à l'intégration à un système SIEM.

Effacement des données sécurisé

Le multifonction gère les données pour effectuer des tâches de copie, de numérisation, d'impression et de télécopie, ainsi que les carnets d'adresses, les journaux système et l'historique des tâches, qui pourraient contenir des informations sensibles. La plateforme imageRUNNER ADVANCE fournit une fonction d'effacement sécurisé des données qui garantit non seulement la suppression de l'entrée de la table d'allocation des fichiers pour les données supprimées, mais également le remplacement des secteurs stockant les données par des données factices, empêchant ainsi toute récupération.

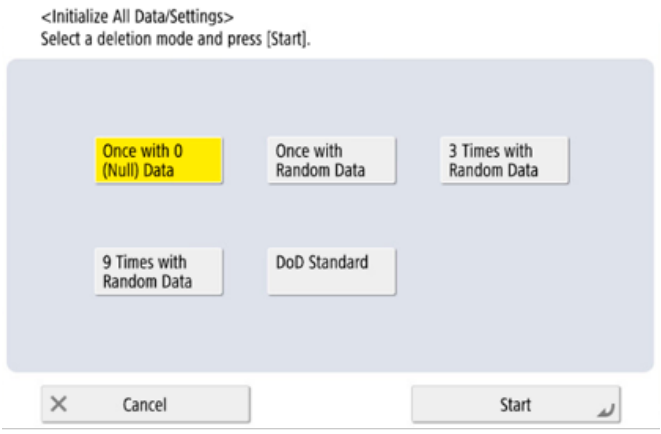


Schéma 5 Options d'écrasement des données pour le modèle imageRUNNER ADVANCE équipé d'un disque dur

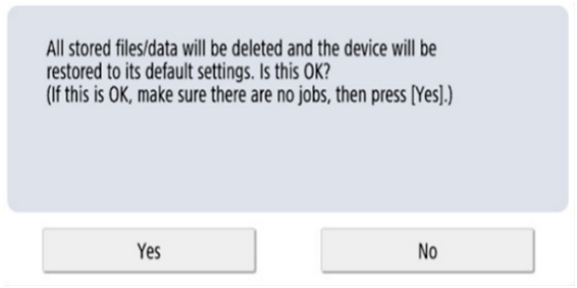


Schéma 6 Initialisation de toutes les données SSD pour le modèle imageRUNNER ADVANCE

En fonction du modèle de périphérique, un disque dur (HDD) ou un disque SSD (Solid-State Drive) est utilisé. Puisqu'un disque dur utilise un plateau de rotation physique sur lequel les données sont enregistrées, un certain nombre d'écrasements, généralement trois, sont nécessaires pour garantir l'écrasement efficace des données. Cependant, la technologie SSD gère le stockage différemment, en répartissant la mémoire de manière uniforme sur l'ensemble de l'espace disponible. Ainsi, il est inutile d'écraser plusieurs fois les données.

Technologie SSD

Contrairement à un disque dur, un disque SSD élimine le besoin d'effectuer des opérations de maintenance, car l'autosuffisance a été intégrée dès la phase de conception à l'aide d'algorithmes et de mesures de sécurité intégrée pour s'assurer que les données sont éliminées efficacement, tout en optimisant la durée de vie. Les données sont stockées électriquement dans des cellules de mémoire à semi-conducteurs, ce qui a l'avantage d'offrir un accès rapide, mais pose le problème suivant : chaque cellule n'a qu'un nombre limité d'écritures.

Répartition de l'usure

Pour contrer le problème de l'usure excessive d'un bloc de mémoire particulier, un processus appelé la répartition de l'usure est utilisé pour garantir que le nombre d'écritures soit réparti le plus uniformément possible. Deux principes sont utilisés : la répartition dynamique et la répartition statique.

La répartition dynamique de l'usure attribue des blocs de stockage de manière à ce que les réécritures soient repositionnées sur les nouveaux blocs vides. Un compteur d'usure est ensuite incrémenté pour permettre au contrôleur SSD d'effectuer le suivi de l'usure. La répartition statique de l'usure permet de déplacer les données existantes non modifiées vers un nouveau bloc mémoire, répartissant ainsi l'usure de manière plus uniforme sur l'ensemble du stockage disponible. Le principe consiste à répartir le nombre de réécritures uniformément sur tous les blocs de mémoire, peu importe si les données stockées ne changent que de temps en temps ou qu'elles évoluent en permanence. Le processus « TRIM » contribue à prolonger la durée de vie et à assurer un mappage ultrarapide des données.

La gamme imageRUNNER ADVANCE propose plusieurs options de configuration, qui permettent de définir la zone ainsi que le mode d'écrasement. Ces options peuvent varier selon les modèles. Les modèles qui utilisaient le stockage sur disque dur fournissaient auparavant une fonction de suppression complète des données qui effaçait la totalité des données.

- La clé de cryptage du disque SSD est stockée dans le périphérique spécifique. Si elle est retirée de ce périphérique spécifique, les données sont chiffrées selon la norme **AES de 256 bits** et ne peuvent être ni lues, ni écrites
- La puce de sécurité 2.10 des multifonctions Canon est conforme à la norme **FIPS 140-2 de niveau 2** (norme gouvernementale établie par les États-Unis).

Initialiser toutes les données/tous les paramètres

- **Limité à [Once with 0 (Null) Data/Une fois avec 0 (Zéro) donnée]**
- Le disque SSD est un disque à semi-conducteurs, tandis qu'un disque HDD utilise des disques magnétiques rotatifs.
- En outre, après avoir écrit une fois avec 0 donnée, il est pratiquement impossible de lire les données écrites, car la table d'accès est réécrite et l'emplacement des données est inconnu.
- Puisque les données stockées sont chiffrées, il est impossible de lire ou d'écrire des données sur un PC ou après une installation sur un autre multifonction.

Validation automatique des certificats

Dans les versions antérieures à la version 3.8 de la plateforme logicielle système imageRUNNER ADVANCE, l'administrateur devait installer manuellement les certificats de sécurité mis à jour sur chaque périphérique.
Cette tâche est laborieuse, car elle nécessite de se connecter à chaque périphérique, l'un après l'autre, pour effectuer une mise à jour manuelle. Les certificats doivent être installés manuellement à l'aide de l'interface utilisateur à distance (RUI) de chaque périphérique, ce qui rend le processus beaucoup plus long. Grâce au service de validation automatique des certificats introduit à partir de la version 3.8 de la plateforme, cette surcharge de travail appartient au passé.

Le processus de validation automatique améliore l'efficacité de l'extraction des certifications. Il permet d'extraire automatiquement les certificats à l'aide du service NDES (Network Device Enrollment Service) pour Microsoft Windows et du protocole SCEP (Simple Certificate Enrollment Protocol).

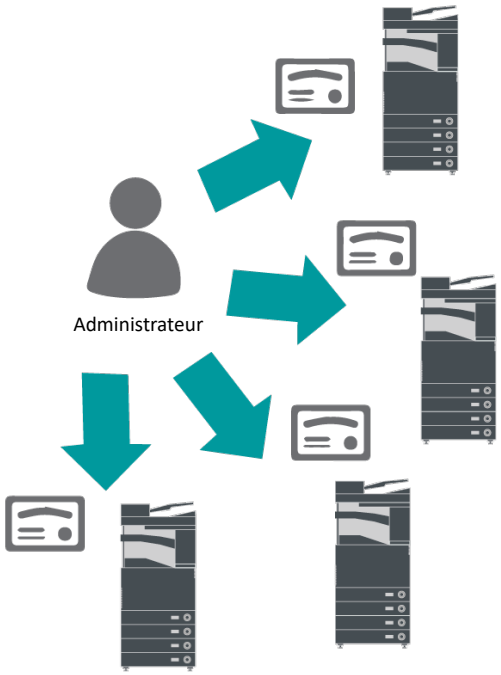


Schéma 7 Validation des certificats

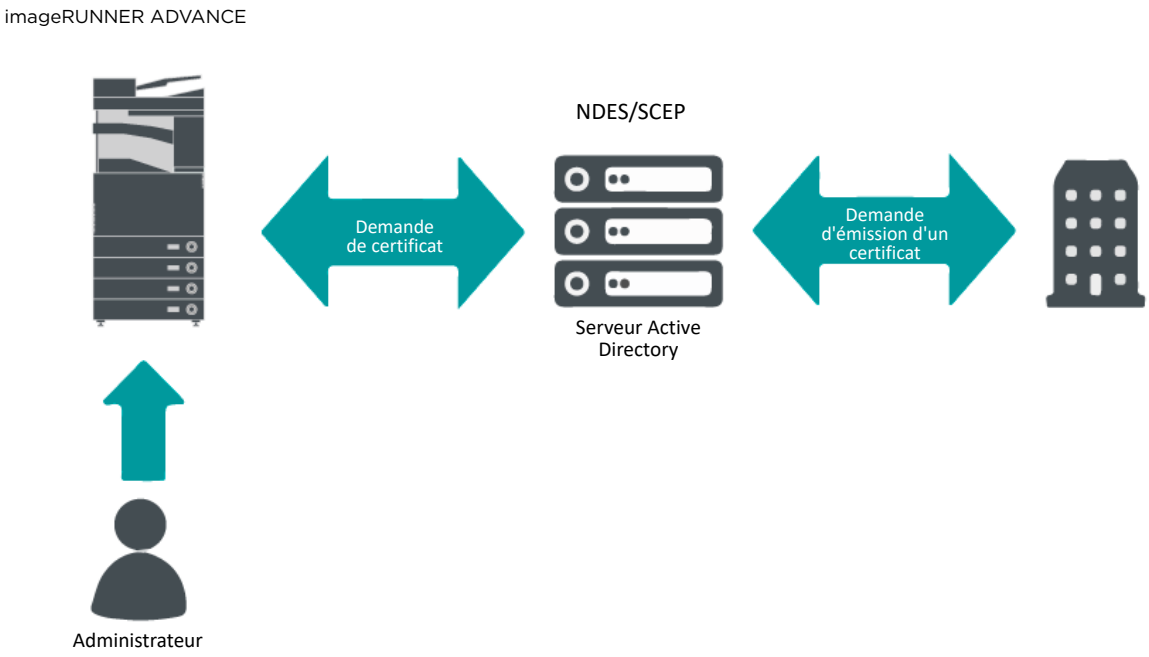


Schéma 8 Processus de validation des certificats

SCEP est un protocole qui prend en charge les certificats émis par une autorité de délivrance de certificats (CA). NDES permet aux périphériques réseau d'extraire ou de mettre à jour des certificats d'après le protocole SCEP.

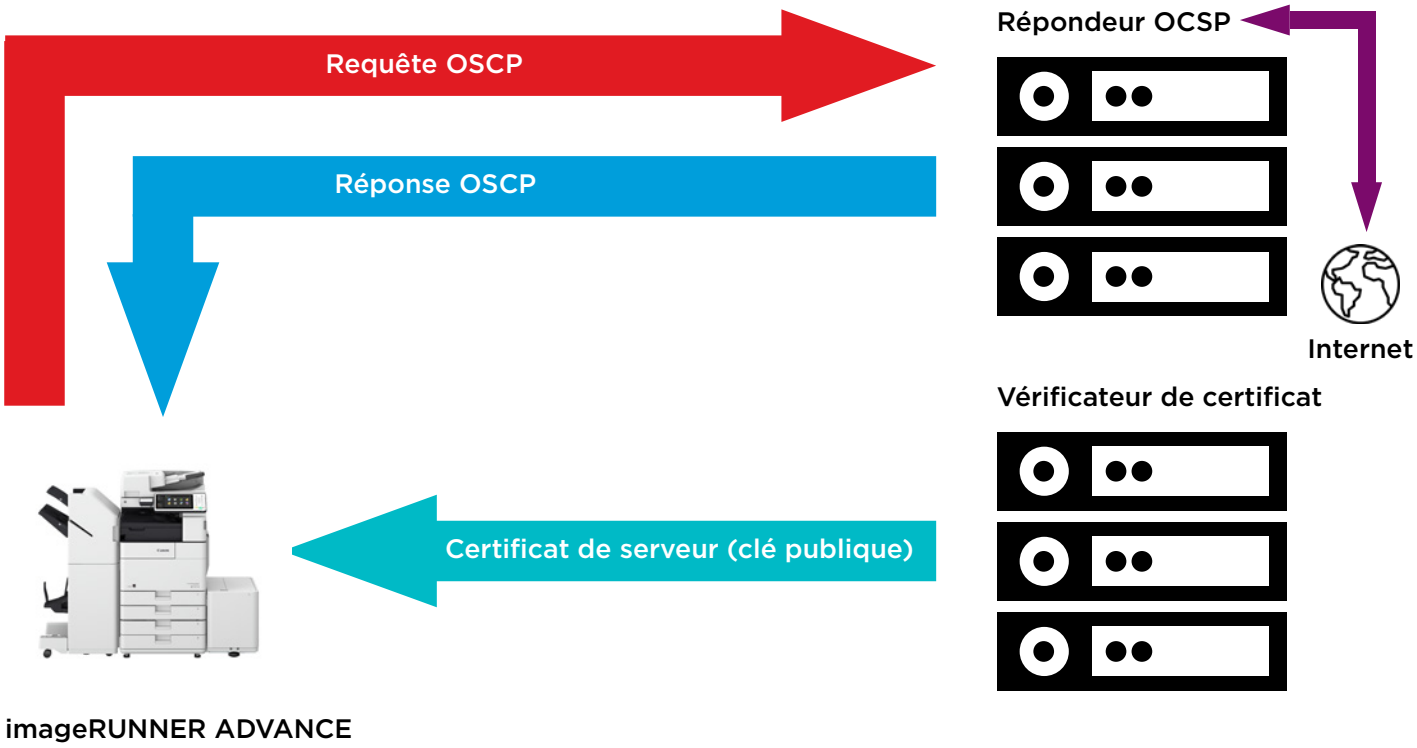
NDES est un service de rôle des services relatifs aux certificats Active Directory.

Protocole de vérification de l'état du certificat en ligne

Plusieurs facteurs justifient la nécessité de révoquer un certificat numérique. Par exemple, la clé privée associée peut avoir été perdue, volée ou compromise, ou un nom de domaine peut avoir été modifié.

Le protocole de vérification de l'état du certificat en ligne (ou OCSP) est un protocole Internet standard utilisé pour vérifier l'état de validation d'un certificat numérique X.509 fourni par un serveur de certification. En envoyant une requête OCSP au répondeur OCSP (généralement un émetteur de certificat), et en désignant un certificat spécifique, le répondeur OCSP indique dans sa réponse si le certificat est « bon », « révoqué » ou « inconnu ».

Schéma 9 Processus d'établissement de liaison OCSP



À partir de la version 3.10 de la plate-forme imageRUNNER ADVANCE, le protocole OCSP fournit un mécanisme de vérification en temps réel de l'état des certificats numériques X.509 installés. Les versions précédentes de la plate-forme prenaient uniquement en charge la méthode basée sur une liste de certificats révoqués (ou CRL), inefficace et entraînant une surcharge importante des ressources réseau.

Informations relatives à la sécurité et gestion des événements

La technologie imageRUNNER ADVANCE permet de diffuser des événements de sécurité en temps réel à l'aide du protocole Syslog, conforme aux normes RFC 5424, RFC 5425 et RFC 5426.

Ce protocole est utilisé par un large éventail de types de périphérique comme moyen de collecter en temps réel des informations qui peuvent être utilisées pour identifier d'éventuels problèmes de sécurité.

Pour faciliter la détection des menaces et des incidents de sécurité, le périphérique doit être configuré de manière à pointer vers un serveur SIEM (Security Incident Event Management) tiers.

Les événements Syslog produits par le périphérique peuvent être utilisés pour créer des actions suite à la collecte et l'analyse en temps réel d'événements à partir d'une grande variété de sources de données contextuelles (schéma 7). La génération de rapports de conformité et l'examen des incidents peuvent également être pris en charge grâce à l'utilisation de solutions supplémentaires, par exemple un serveur SIEM. Un exemple est illustré sur le schéma 8.

La dernière génération de périphériques imageRUNNER ADVANCE offre une fonctionnalité Syslog qui prend en charge une large gamme d'événements pouvant être collectés. Il est ainsi possible de corréler et d'analyser des événements sur plusieurs sources disparates.

Schéma 10 Capture des données Syslog

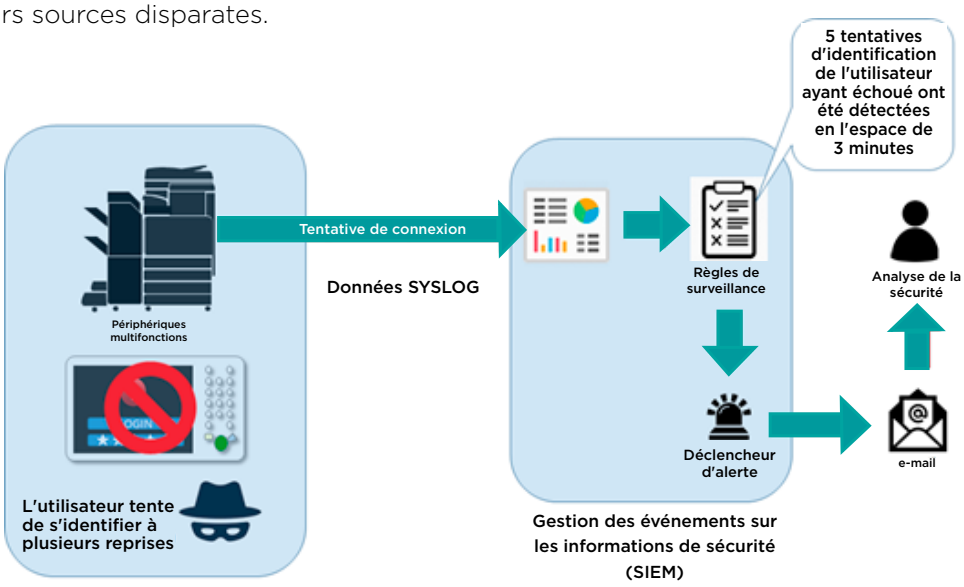


Schéma 11 Exemple d'utilisation des données Syslog imageRUNNER ADVANCE

Pour obtenir la liste des cibles d'opération SIEM, accédez au lien suivant via votre navigateur Web et téléchargez le document **« SIEM_spec (imageRUNNER ADVANCE) »**.
https://www.canon-europe.com/support/product-specific-security-measures/

Gestion des journaux du périphérique

Outre la fonctionnalité Syslog fournie par la plateforme logicielle système version 3.8, la gamme imageRUNNER ADVANCE dispose des journaux suivants, qui peuvent être gérés sur le périphérique. Ces journaux peuvent être exportés au format CSV via l'interface utilisateur à distance (RUI).

Tableau 3 Exemples de fichiers journaux pouvant être gérés par le multifonction.

Type de journal	Numéro indiqué comme « Type de journal » dans le fichier CSV	Description
Journal	4098	Ce journal contient des informations au sujet de l'état d'authentification de l'utilisateur (connexion/déconnexion et réussite/échec de l'authentification de l'utilisateur), de l'enregistrement/la modification/la suppression des informations utilisateur gérées avec l'authentification de l'utilisateur, et de la gestion (ajout/modification/suppression) des rôles grâce au SYSTÈME DE GESTION DES ACCÈS
Journal des travaux	1001	Ce journal contient des informations au sujet de l'achèvement des travaux de copie/télécopie/numérisation/envoi/impression
Journal des transmissions	8193	Ce journal contient des informations relatives aux transmissions
Journal d'enregistrement dans l'espace avancé	8196	Ce journal contient des informations au sujet de l'enregistrement de fichiers dans l'espace avancé, sur le réseau (espace avancé d'autres imprimantes) et sur le support de mémoire
Journal des opérations de boîte aux lettres	8197	Ce journal contient des informations au sujet des opérations effectuées sur les données de la boîte aux lettres, de la boîte mémoire RX et de la boîte fax confidentielle
Journal d'authentification de la boîte aux lettres	8199	Ce journal contient des informations au sujet de l'état d'authentification de la boîte aux lettres, de la boîte mémoire RX et de la boîte fax confidentielle
Journal des opérations de l'espace avancé	8201	Ce journal contient des informations relatives aux opérations de données effectuées dans l'espace avancé
Journal de gestion de l'imprimante	8198	Ce journal contient des informations au sujet du démarrage et de l'arrêt de l'imprimante, des modifications apportées aux paramètres à l'aide de (Paramètres/Enregistrement), des modifications apportées aux paramètres à l'aide de la fonction de diffusion des informations sur le périphérique et du paramétrage horaire. Le journal de gestion de l'imprimante enregistre également les modifications apportées aux informations utilisateur ou aux paramètres de sécurité lors de l'inspection ou de la réparation de l'imprimante par votre revendeur Canon agréé
Journal d'authentification réseau	8200	Ce journal est enregistré lorsque la communication IPsec échoue
Journal Exporter/Importer tout	8202	Ce journal contient des informations au sujet de l'importation/exportation des paramètres à l'aide de la fonction Exporter/Importer tout
Journal de sauvegarde de la boîte aux lettres	8203	Ce journal contient des informations au sujet des sauvegardes de données dans les boîtes de réception utilisateur, la boîte mémoire RX, la boîte fax confidentielle, l'espace avancé, ainsi que des données en attente et du formulaire enregistré pour la fonction de superposition des images
Journal des opérations de l'écran de gestion des applications/logiciels	3101	Il s'agit d'un journal des opérations pour les SMS (Service Management Service), l'enregistrement et les mises à jour de logiciels, les programmes d'installation d'applications MEAP, etc.
Journal de la politique de sécurité	8204	Ce journal contient des informations au sujet de l'état des paramètres de la politique de sécurité
Journal de gestion des groupes	8205	Ce journal contient des informations au sujet de l'état des paramètres (enregistrement/modification/suppression) des groupes d'utilisateurs
Journal de la maintenance du système	8206	Ce journal contient des informations au sujet des mises à jour du micrologiciel, de la sauvegarde/restauration de l'application MEAP, etc.
Journal d'impression relatif à l'authentification	8207	Ce journal contient des informations et l'historique des opérations concernant les travaux d'impression en attente forcée
Journal de synchronisation des paramètres	8208	Ce journal contient des informations au sujet de la synchronisation des paramètres de l'imprimante. Synchronisation des paramètres de plusieurs imprimantes multifonctions Canon
Journal de gestion des journaux d'audit	3001	Ce journal contient des informations au sujet du début et de la fin de cette fonction (fonction Gestion des journaux d'audit), de l'exportation des journaux, etc.

Les journaux peuvent contenir jusqu'à 40.000 enregistrements. Lorsque le nombre d'enregistrements dépasse 40.000, les enregistrements les plus anciens sont les premiers à être supprimés.

ASSISTANCE À DISTANCE POUR L'APPAREIL

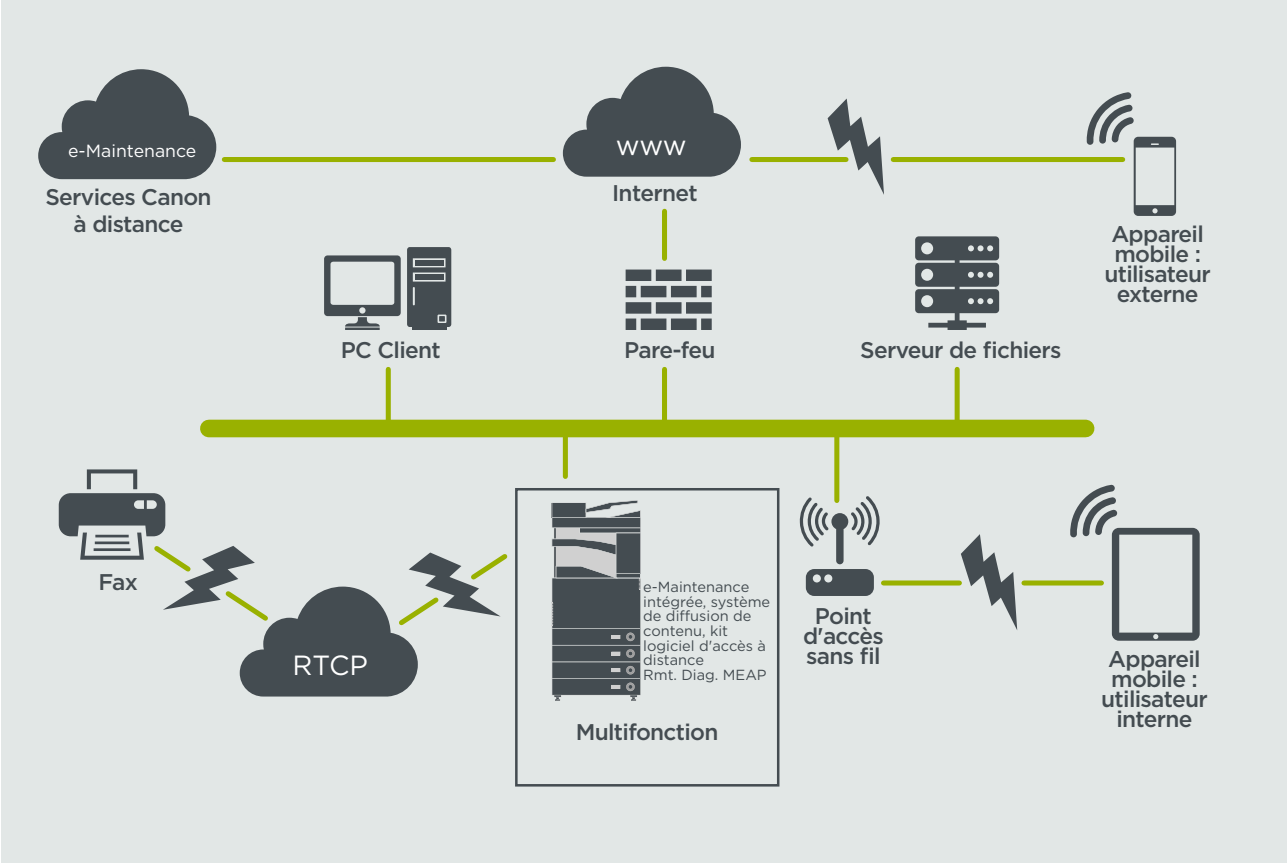
Pour que Canon ou un partenaire de Canon puisse fournir une assistance efficace, la plateforme imageRUNNER ADVANCE est capable d'envoyer des données de maintenance ainsi que de recevoir des mises à jour du micrologiciel ou des applications. Il est important de noter qu'aucune image ou métadonnées d'images ne sont envoyées.

Ci-dessous se trouvent deux possibilités de déploiement des services d'assistance à distance de Canon au sein du réseau d'une entreprise.

Scénario de déploiement 1 : connexion dispersée

Ce paramètre permet à chaque imprimante multifonction de se connecter directement à un service distant via Internet.

Schéma 12 Connexion dispersée



Scénario de déploiement 2 : connexion à gestion centralisée

Dans les grandes entreprises dotées d'un environnement comportant plusieurs imprimantes multifonction, il est nécessaire de pouvoir gérer efficacement des appareils à partir d'un point central, notamment en ce qui concerne la connexion aux services à distance de Canon. Cette stratégie de gestion centralisée est possible lorsque chaque imprimante se connecte via un point de connexion unique à iW Enterprise Management Console (iWEMC). Pour la communication entre la fonctionnalité Gestion du micrologiciel dans iWEMC et les périphériques multifonctions, le port UDP 47545 est utilisé.

Schéma 13 Connexion à gestion centralisée

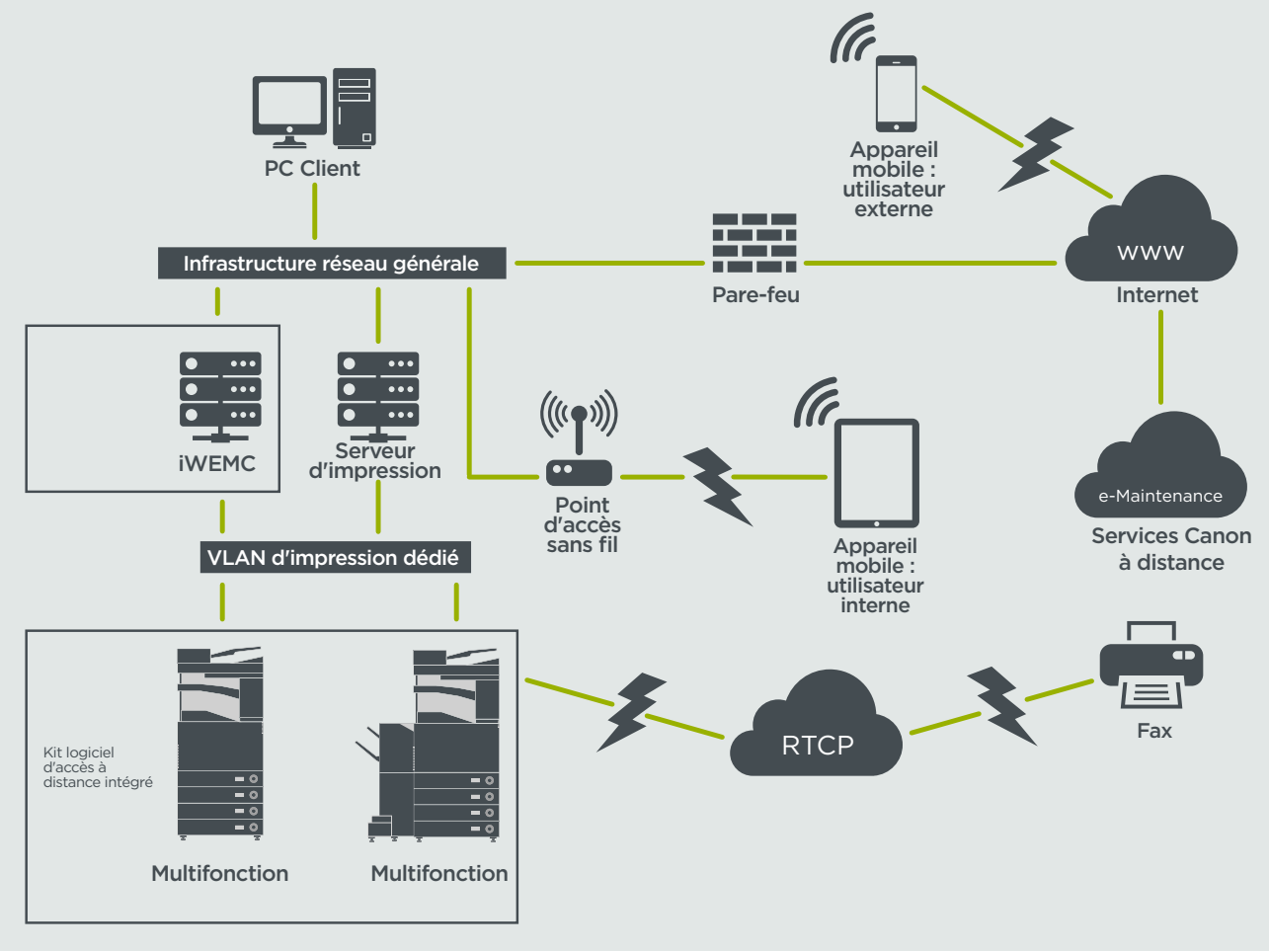


Schéma
14a. Liste des périphériques (ici, un seul périphérique) répertoriés sur iW Enterprise Management Console
14b. Informations et paramètres du périphérique

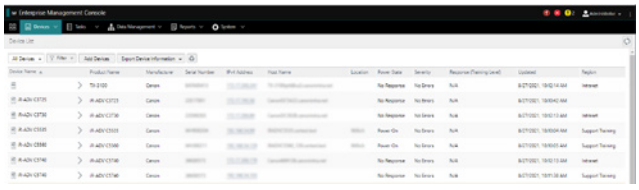


Schéma 14a

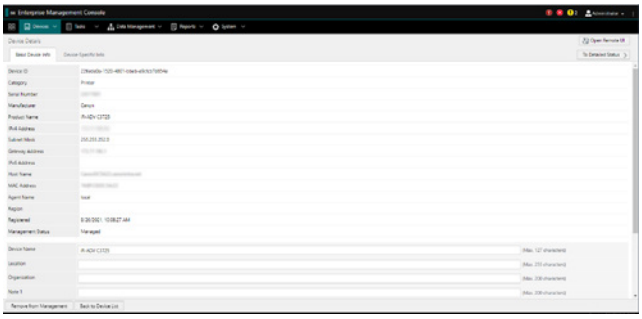


Schéma 14b

e-Maintenance

Le système e-Maintenance assure la relève automatique des compteurs d'utilisation des imprimantes à des fins de facturation, de gestion des consommables et de contrôle des imprimantes à distance, à l'aide d'informations sur l'état du périphérique et d'alertes en cas d'erreur.

Le système e-Maintenance se compose d'un serveur connecté à Internet (UGW2) et d'un logiciel intégré à l'imprimante multifonction (eRDS) et/ou d'un logiciel supplémentaire sur le serveur (CDCA) et/ou l'application MEAP (Rmt. Diag. MEAP) pour collecter les informations de maintenance du périphérique. L'eRDS est un logiciel de contrôle exécuté sur l'imprimante imageRUNNER ADVANCE. Si l'option de surveillance est activée dans les paramètres du périphérique, le logiciel eRDS obtient les informations relatives au périphérique et les envoie au serveur UGW2. L'agent de collecte des données Canon (CDCA) est un logiciel de contrôle installé sur un ordinateur de bureau, qui permet de surveiller jusqu'à 1000 périphériques. Il passe par le réseau pour obtenir les informations auprès de chaque périphérique avant de les envoyer au serveur UGW2. Rmt. Diag. MEAP est une application MEAP permettant l'envoi d'informations sur les périphériques à e-Maintenance par e-mail ou communication HTTPS. Elle peut gérer jusqu'à 31 périphériques.

Ci-dessous, le tableau 4 décrit les données transférées ainsi que les protocoles (selon les options sélectionnées lors de la conception et de l'installation) et les ports utilisés. À aucun moment des données d'image pour la copie, l'impression, la numérisation ou la télécopie ne sont transférées.

Tableau 4 Présentation des données traitées par e-Maintenance

Description	Données traitées	Protocole/Port	Port
	Adresse du service Web UGW2 Adresse/numéro de port du serveur Compte/mot de passe du proxy Adresse de destination des e-mails UGW2 Adresse du serveur SMTP Adresse du serveur POP État du périphérique, relevé du compteur et informations sur le modèle Numéro de série Autres informations sur le toner/l'encre Informations sur le micrologiciel Informations sur les demandes de réparation Informations sur la journalisation Appel de service Alarme de service Bourrage Environnement Journal des conditions	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Communication entre e-Maintenance (UGW2) et les périphériques (uniquement CDCA ou Rmt. Diag. MEAP, car eRDS est un logiciel intégré)		SNMP Spécifique à Canon SLP/SLP/HTTPS	UDP/161 TCP/47546, UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443

Système de diffusion de contenu

Le système de distribution de contenu (CDS) établit une connexion entre l'imprimante multifonction et le serveur Universal Gateway 2 (UGW2) de Canon. Fournit des mises à jour pour le micrologiciel et les applications de l'imprimante.

Tableau 5 Présentation des données traitées par le système de diffusion de contenu

Description	Données envoyées	Protocole/Port	Port
Communication entre le périphérique multifonction et UGW2	Numéro de série du périphérique Version du micrologiciel Langue Pays Informations relatives au contrat de licence d'utilisation	HTTP/HTTPS	TCP/80 TCP/443
Communication entre UGW2 et le périphérique multifonction	Fichier de test (données binaires aléatoires) pour tester la communication Données binaires sur le micrologiciel ou l'application MEAP	HTTP/HTTPS	TCP/80 TCP/443

Une URL d'accès au CDS spécifique est prédéfinie dans la configuration de l'imprimante.
Si vous devez gérer les applications et le micrologiciel de l'imprimante de manière centralisée au sein de l'infrastructure, iWEMC devra être installé en local avec la fonctionnalité Micrologiciel et la gestion des applications.

Kit logiciel d'accès à distance

Le kit logiciel d'accès à distance (RSOK) permet d'accéder à distance au panneau de commande de l'imprimante multifonction. Ce système de type serveur-client se compose d'un serveur VNC exécuté sur le périphérique multifonction et de l'application client Remote Operation Viewer VNC pour Microsoft Windows.

Schéma 15 Paramétrage du kit logiciel d'accès à distance (RSOK)

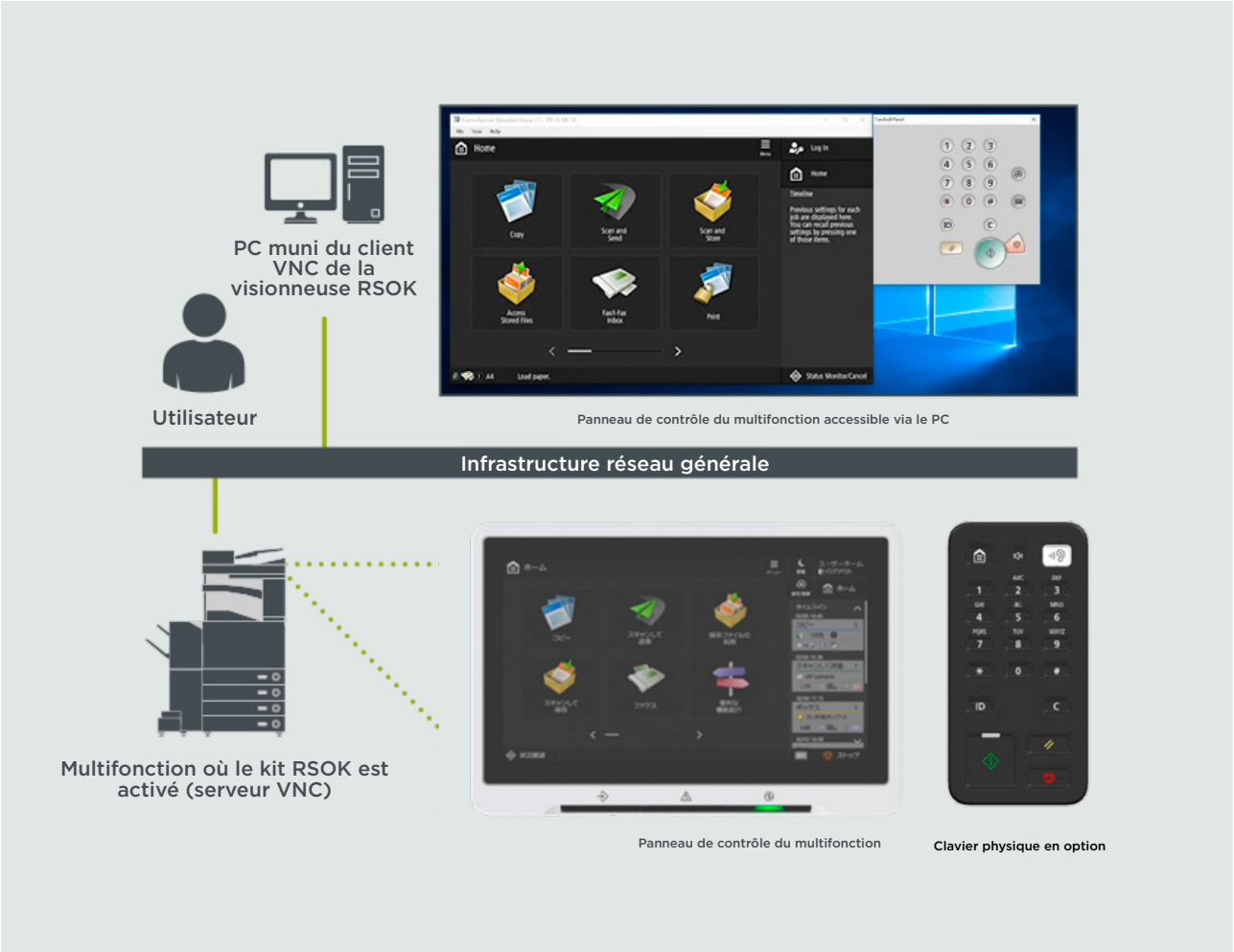


Tableau 6 Présentation des données traitées par le kit logiciel d'accès à distance

Description	Données envoyées	Protocole/Port	Port
Authentification du mot de passe VNC	Mot de passe de l'utilisateur	Chiffrement DES	5900
Application Operation Viewer	Panneau de commande de l'imprimante - données à l'écran - opération via une clé matérielle	Version Protocole 3.3 RFB	5900

ANNEXE

Fonctionnalités de sécurité imageRUNNER ADVANCE de Canon

La plateforme imageRUNNER ADVANCE offre une interface de configuration à distance par l'intermédiaire de services Web, appelée Interface utilisateur à distance (RUI). Cette interface permet d'accéder à de nombreux paramètres de configuration de l'imprimante multifonction et peut être désactivée le cas échéant ou protégée par un mot de passe pour éviter que des utilisateurs non autorisés y accèdent.

Bien que la majorité des paramètres de l'appareil soient disponibles via l'Interface utilisateur à distance, certains restent uniquement accessibles sur le panneau de commande de l'imprimante multifonction. Nous vous recommandons de désactiver tous les services que vous n'utilisez pas et de renforcer le contrôle de ceux dont vous avez besoin. Pour une assistance en toute flexibilité, le kit logiciel d'accès à distance (RSOK) permet d'accéder à distance au panneau de commande de l'imprimante multifonction. Il s'appuie sur la technologie VNC composée d'un serveur (le multifonction) et d'un client (un ordinateur réseau). La visionneuse Canon spécifique installée sur le PC du client permet l'accès simulé aux touches du panneau de commande, si nécessaire.

Cette section présente les principales fonctionnalités de sécurité imageRUNNER ADVANCE et leurs paramètres de configuration.

Des manuels de l'utilisateur interactifs en ligne disponibles sur https://oip.manual.canon/ fournissent des informations ne se limitant pas aux fonctions de sécurité. Commencez par sélectionner le type de produit sur lequel vous souhaitez en savoir plus (par exemple imageRUNNER ADVANCE DX), puis cliquez sur l'icône de recherche avant de saisir vos critères de recherche. Vous trouverez ci-après quelques points généraux à prendre en compte afin de sécuriser votre appareil.

Gestion de l'imprimante multifonction

Pour réduire les risques de fuites d'informations personnelles et d'accès par des utilisateurs non autorisés, il est indispensable de prendre des mesures de sécurité efficaces et constantes. Désignez un administrateur chargé de gérer les paramètres des appareils afin de restreindre l'accès aux paramètres de gestion des utilisateurs et de la sécurité à quelques personnes autorisées.

Entrez le lien ci-dessous dans votre navigateur Web et accédez à la **configuration administrateur** dans la zone de recherche. Vous pourrez ainsi accéder à des informations liées aux domaines suivants :

- Gestion de base du périphérique
- Atténuation des risques de négligence, d'utilisation erronée ou abusive
- Gestion des périphériques
- Gestion de la configuration et des paramètres système

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Norme IEEE P2600

Plusieurs modèles imageRUNNER ADVANCE répondent à la norme IEEE P2600, qui est une norme internationale de protection des informations personnelles sur les imprimantes et les périphériques multifonctions.

Le lien ci-dessous répertorie les exigences en matière de sécurité fixées par la norme IEEE P2600 et explique de quelle manière les fonctions de chaque modèle répondent à ces exigences.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

Authentification IEEE 802.1X

Si une connexion à un réseau 802.1X est requise, le périphérique doit fournir des informations d'authentification prouvant qu'il est autorisé à se connecter au réseau.

Entrez le lien ci-dessous dans votre navigateur Web et indiquez **802.1X** dans la zone de recherche.
https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Application d'une politique de sécurité à l'imprimante

Sur les modèles imageRUNNER ADVANCE les plus récents, de nombreux paramètres de sécurité du périphérique et la politique de sécurité peuvent être gérés ensemble via l'interface utilisateur à distance. L'accès aux paramètres peut être réservé au seul administrateur de la politique de sécurité, qui dispose d'un mot de passe spécifique.

Entrez le lien ci-dessous dans votre navigateur Web et indiquez **Application d'une politique de sécurité à l'imprimante** dans la zone de recherche. Vous pourrez ainsi accéder à des informations liées aux domaines suivants :

- L'utilisation d'un mot de passe pour protéger l'accès aux paramètres de la politique de sécurité
- La configuration des paramètres de la politique de sécurité
- Les éléments du menu de paramétrage de la politique de sécurité

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Gestion des utilisateurs

Les clients qui ont besoin d'un niveau de sécurité et d'une efficacité accrus peuvent utiliser soit les fonctionnalités intégrées soit une solution de gestion de l'impression telle qu'uniFLOW.

Pour plus d'informations sur nos solutions de gestion de l'impression, veuillez contacter votre interlocuteur local ou consulter la brochure de la solution uniFLOW.

Configuration des paramètres de sécurité réseau

Les utilisateurs autorisés peuvent subir des pertes imprévues suite à des attaques de la part de tiers malveillants telles que le reniflage, l'usurpation ou l'altération de données circulant sur le réseau. Pour protéger les informations importantes et précieuses contre ces attaques, l'imprimante est dotée de nombreuses fonctionnalités de renforcement de la sécurité et de la confidentialité.

Entrez le lien ci-dessous dans votre navigateur Web et indiquez **Configuration des paramètres de sécurité réseau** dans la zone de recherche. Vous pourrez ainsi accéder à des informations liées aux domaines suivants :

Suivez le lien ci-dessous pour plus d'informations concernant :

- le blocage des accès non autorisés ;
- la connexion à un réseau LAN sans fil ;
- la configuration de l'environnement réseau.

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Gestion des données du disque dur ou du disque SSD

Le disque dur de l'imprimante multifonction héberge le système d'exploitation de l'appareil, les paramètres de configuration et les informations sur les travaux. La plupart des modèles de périphériques offrent un cryptage complet du disque (conforme à la norme FIPS 140-2). Son couplage avec le périphérique spécifique empêche les utilisateurs non autorisés de le lire. La puce de sécurité préparatoire des multifonctions Canon est certifiée en tant que module cryptographique dans le cadre du Programme de validation du module cryptographique (CMVP) établi par les États-Unis et le Canada, ainsi que le Programme de validation du module cryptographique japonais (JCMVP).

Entrez le lien ci-dessous dans votre navigateur Web et indiquez **Gestion des données du disque dur** dans la zone de recherche.

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Pour plus d'informations sur l'assainissement des données à l'aide de produits utilisant la technologie SSD, accédez au lien ci-dessous via votre navigateur Web et saisissez **Initialiser toutes les données** dans la zone de recherche.

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

PRÉSENTATION DES PARAMÈTRES DE LA POLITIQUE DE SÉCURITÉ

La troisième génération de modèles imageRUNNER ADVANCE est dotée de paramètres de politique de sécurité et d'un administrateur des paramètres de sécurité. L'administrateur doit se connecter en tant que tel puis, si l'option est activée, il doit fournir un mot de passe spécifique afin d'accéder aux paramètres de sécurité.

Le tableau ci-dessous répertorie les paramètres disponibles.

1. Interface	Notes
Politique de connexion sans fil	
Interdiction de l'utilisation de la connexion directe	<Use Wi-Fi Direct/Utiliser Wi-Fi Direct> est défini sur <Off/Désactivé>. Il est impossible d'accéder à l'imprimante à partir d'appareils mobiles.
Interdiction de l'utilisation du LAN sans fil	<Select Wired/Wireless LAN/Sélectionner LAN filaire/sans fil> est défini sur <Wired LAN/LAN filaire>. Il est impossible d'établir une connexion sans fil à l'imprimante multifonction via un routeur ou un point d'accès du LAN sans fil.
Politique USB	
Interdiction de l'utilisation en tant que périphérique USB	<Use as USB Device/Utiliser comme périphérique USB> est défini sur <Off/Désactivé>. Lorsque l'utilisation de l'appareil en tant que périphérique USB est interdite, il est impossible d'utiliser les fonctions d'impression et de numérisation à partir d'un ordinateur connecté via USB.
Interdiction de l'utilisation en tant que périphérique de stockage USB	<Use USB Storage Device/Utiliser le périphérique de stockage USB> est défini sur <Off/Désactivé>. Il est impossible d'utiliser des périphériques de stockage USB. Toutefois, les fonctions de maintenance suivantes restent disponibles, même lorsque l'option d'interdiction de l'utilisation en tant que périphérique de stockage USB est activée. • Mise à jour du micrologiciel à l'aide d'une clé USB (en mode de téléchargement) • Copie des données du journal secondaire du périphérique vers un périphérique USB (LOG2USB) • Copie d'un rapport depuis l'appareil vers un périphérique USB (RPT2USB).
Politique opérationnelle de communication réseau Remarque : ces paramètres ne s'appliquent pas à la communication avec les réseaux IEEE 802.1X, même si la case [Always Verify Server Certificate When Using TLS/Toujours vérifier le certificat de serveur lors de l'utilisation de TLS] est cochée	
Toujours vérifier les signatures pour les fonctions de serveurs SMS/WebDAV	Dans <SMB Server Settings/Réglages du serveur SMB>, les options <Require SMB Signature for Connection/Signature SMB requise pour la connexion> et <Use SMB Authentication/Utiliser l'authentification SMB> sont définies sur <On/Activé>. Dans <WebDAV Server Settings/Réglages du serveur WebDAV>, <Use TLS/Utiliser TLS> est défini sur <On/Activé>. Lorsque l'imprimante multifonction est utilisée en tant que serveur SMB ou WebDAV, les signatures de certificats numériques sont vérifiées au cours de la communication.
Toujours vérifier le certificat du serveur lorsque le protocole TLS est utilisé	<Confirm TLS Certificate for WebDAV TX/Confirmer certificat TLS pour TX WebDAV>, <Confirm TLS Certificate for SMTP TX/Confirmer certificat TLS pour TX SMTP>, <Confirm TLS Certificate for POP RX/Confirmer certificat TLS pour RX POP>, <Confirm TLS Certificate for Network Access/Confirmer certificat TLS pour l'accès réseau> et <Confirm TLS Certificate Using MEAP Application/Confirmer certificat TLS via Application MEAP> sont tous définis sur <On/Activé> et la case <CN> est cochée. En outre, les options <Verify Server Certificate/Vérifier le certificat du serveur> et <Verify CN/Vérifier CN> dans <SIP Settings/Réglages SIP> > <TLS Settings/Réglages TLS> sont définies sur <On/Activé>. Au cours de la communication TLS, une vérification des certificats numériques et de leurs noms communs est effectuée.
Interdiction de l'authentification en texte brut pour les fonctions de serveur	• <Use FTP Printing/Utiliser l'impression FTP> dans <FTP Print Settings/Réglages d'impression FTP> est défini sur <Off/Désactivé>. • <Allow TLS (SMTP RX)/Autoriser TLS (RX SMTP)> dans <E-Mail/I-Fax Settings/Réglages E-Mail/I-Fax> <Communication Settings/Réglages de communication> est défini sur <Always TLS/Toujours TLS>. <Dedicated Port Authentication Method/Méthode d'authentification de port dédié> dans <Network/Réseau> est défini sur <Mode 2>. • <Use TLS/Utiliser TLS> dans <WebDAV Server Settings/Réglage du serveur WebDAV> est défini sur <On/Activé>. Lorsque vous utilisez la machine en tant que serveur, les fonctions qui utilisent l'authentification en texte brut ne sont pas disponibles. Le protocole TLS sera utilisé si l'authentification en texte clair est interdite. En outre, vous ne pourrez pas utiliser les applications ou fonctions de serveur qui prennent uniquement en charge l'authentification en texte brut, telles que le FTP. L'accès à l'imprimante multifonction depuis le logiciel de gestion de l'imprimante ou le pilote peut être impossible.
Interdiction de l'utilisation du SNMPv1	Dans <SNMP Settings/Réglages SNMP>, <Use SNMPv1/Utiliser SNMPv1> est défini sur <Off/Désactivé>. Interdire l'utilisation du SNMPv1 peut vous empêcher d'obtenir ou de définir les informations sur l'appareil à partir du pilote d'impression ou du logiciel de gestion.
Politique d'utilisation des ports	
Restriction du port LPD	Numéro de port : 515 <LPD Print Settings/Réglages d'impression LPD> est défini sur <Off/Désactivé>. Il est impossible d'effectuer une impression LPD.
Restriction du port RAW	Numéro de port : 9100 <RAW Print Settings/Réglages d'impression RAW> est défini sur <Off/Désactivé>. Il est impossible d'effectuer une impression RAW.
Restriction du port FTP	Numéro de port : 21 Dans <FTP Print Settings/Réglages d'impression FTP>, <Use FTP Printing/Utiliser l'impression FTP> est défini sur <Off/Désactivé>. Il est impossible d'effectuer une impression FTP.
Restriction du port WSD	Numéro de port : 3702, 60000 Dans <WSD Settings/Réglages WSD>, les options <Use WSD/Utiliser WSD>, <Use WSD Browsing/Utiliser la navigation WSD> et <Use WSD Scan/Utiliser la numérisation WSD> sont toutes définies sur <Off/Désactivé>. Il est impossible d'utiliser les fonctions WSD.
Restriction du port BMLinkS	Numéro de port : 1900 N'est pas utilisé en Europe.
Restriction du port IPP	Numéro de port : 631 En cas de restriction du port IPP, les normes d'impression mobile Mopria, AirPrint et IPP ne sont pas disponibles.

Restriction du port SMB	Numéro de port : 137, 138, 139, 445 Dans <SMB Server Settings/Réglages du serveur SMB>, <Use SMB Server/Utiliser serveur SMB> est défini sur <Off/Désactivé>. Il n'est pas possible d'utiliser l'imprimante en tant que serveur SMB.
Restriction du port SMTP	Numéro de port : 25 Dans <E-Mail/I-Fax Settings/Réglages E-Mail/I-Fax> > <Communication Settings/Réglages de communication>, <SMTP RX/RX SMTP> est défini sur <Off/Désactivé>. La réception via SMTP n'est pas disponible.
Restriction d'un port dédié	Numéro de port : 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547 Les fonctions ou applications de copie, télécopie, numérisation ou impression à distance ne seront pas disponibles si le port dédié fait l'objet d'une restriction.
Restriction du port du logiciel d'accès déporté	Numéro de port : 5900 <Remote Operation Settings/Réglages de fonctionnement à distance> est défini sur <Off/Désactivé>. Il est impossible d'utiliser les fonctions de commande à distance.
Restriction du port SIP (Fax sur réseau IP)	Numéro de port : 5004, 5005, 5060, 5061, 49152 Les options <Use Intranet/Utiliser l'Intranet> dans <Intranet Settings/Réglages de l'intranet>, <Use NGN/Utiliser NGN> dans <NGN Settings/Réglages NGN> et <Use VoIP Gateway/Utiliser la passerelle VoIP> dans <VoIP Gateway Settings/Réglages de la passerelle VoIP> sont toutes définies sur <Off/Désactivé>. Il est impossible d'utiliser la télécopie sur IP.
Restriction du port mDNS	Numéro de port : 5353 Dans <mDNS Settings/Réglages mDNS>, les options <Use IPv4 mDNS/Utiliser mDNS IPv4> et <Use IPv6 mDNS/Utiliser mDNS IPv6> sont définies sur <Off/Désactivé>. <Use Mopria/Utiliser Mopria> est défini sur <Off/Désactivé>. Il est impossible d'effectuer des recherches sur le réseau ou de procéder à des réglages automatiques à l'aide de mDNS. Il est également impossible d'imprimer à l'aide de Mopria™ ou AirPrint.
Restriction du port SLP	Numéro de port : 427 Dans <Multicast Discovery Settings/Réglages de la découverte multidiffusion>, <Response/Réponse> est défini sur <Off/Désactivé>. Il est impossible d'effectuer des recherches sur le réseau ou de procéder à des réglages automatiques à l'aide de SLP.
Restriction du port SNMP	Numéro de port : 161 Cette restriction du port SNMP peut vous empêcher d'obtenir ou de définir les informations sur l'appareil à partir du pilote d'impression ou du logiciel de gestion. Dans <SNMP Settings/Réglages SNMP>, les options <Use SNMPv1/Utiliser SNMPv1> et <Use SNMPv3/Utiliser SNMPv3> sont définies sur <Off/Désactivé>.

2. Authentification	Notes
Politique opérationnelle d'authentification	
Interdiction des utilisateurs invités	• <Advanced Space Settings/Réglages Espace avancé> > <Authentication Management/Gestion de l'authentification> est défini sur <On/Activé>. • <Login Screen Display Settings/Réglages d'affichage sur écran de connexion> est défini sur <Display When Device Operation Starts/Afficher au démarrage de l'opération sur le périphérique>. • <Restrict Job from Remote Device without User Auth/Restreindre les tâches depuis un périphérique distant sans authentification utilisateur> est défini sur <On/Activé>. Les utilisateurs non enregistrés ne peuvent pas se connecter à l'imprimante. Les travaux d'impression envoyés depuis un ordinateur sont également annulés.
Paramétrage forcé de la déconnexion automatique	Ce paramètre permet de se déconnecter du panneau de contrôle. Il ne s'applique pas aux autres méthodes de déconnexion (plage réglable de 10 secondes à 9 minutes). <Auto Reset Time/Délai réinitialisation auto.> est activé. L'utilisateur est automatiquement déconnecté si aucune opération n'est effectuée pendant une période donnée. Sélectionnez [Time Until Logout/Délai de déconnexion] sur l'écran de paramétrage de l'interface utilisateur à distance.
Politique opérationnelle relative aux mots de passe	
Interdiction de la mise en cache des mots de passe pour les serveurs externes	Ce paramètre ne s'applique pas aux mots de passe que l'utilisateur accepte d'enregistrer, tels que les mots de passe permettant d'accéder aux carnets d'adresses, etc. <Prohibit Caching of Authentication Password/Interdire la mise en cache du mot de passe d'authentification> est défini sur <On/Activé>. Les utilisateurs devront toujours saisir un mot de passe pour accéder à un serveur externe.
Affichage d'un avertissement en cas d'utilisation du mot de passe par défaut	<Display Warning When Default Password Is in Use/Affichage d'un avertissement en cas d'utilisation du mot de passe par défaut> est défini sur <On/Activé>. Un message d'avertissement s'affiche dès que le mot de passe défini dans les paramètres d'usine de l'imprimante est utilisé.
Interdiction de l'utilisation du mot de passe par défaut pour l'accès à distance	<Allow Use of Default Password for Remote Access/Autoriser l'utilisation d'un mot de passe par défaut pour accès distant> est défini sur <Off/Désactivé>. Il est impossible d'utiliser le mot de passe par défaut défini en usine pour accéder à l'imprimante multifonction depuis un ordinateur.
Politique de paramétrage des mots de passe (n'inclut pas la gestion des identifiants de service et des codes PIN)	
Définition du nombre minimum de caractères utilisés dans le mot de passe	Plage de réglage du nombre minimum de caractères entre 1 et 32
Définition de la période de validité du mot de passe	Plage de réglage de la période de validité entre 1 et 180 jours
Interdiction d'utiliser 3 caractères identiques consécutifs	
Utilisation forcée d'au moins 1 caractère majuscule	
Utilisation forcée d'au moins 1 caractère minuscule	
Utilisation forcée d'au moins 1 chiffre	
Utilisation forcée d'au moins 1 symbole	
Politique de verrouillage	
Activation du verrouillage	Ne s'applique pas à l'ID de service, au code PIN de la messagerie, aux autres codes PIN ou à l'authentification pour l'impression sécurisée, etc. Seuil de verrouillage : réglable entre 1 et 10 fois Période de verrouillage : réglable entre 1 et 60 minutes

3. Clé/Certificat	Notes
Interdiction d'utiliser un chiffrement faible	S'applique à IPsec, TLS, Kerberos, S/MIME, SNMPv3 et au LAN sans fil. Lorsque ce paramètre est activé, la communication avec les périphériques qui prennent en charge uniquement le chiffrement faible peut être impossible.
Interdiction d'utiliser une clé/un certificat à chiffrement faible	S'applique à IPsec, TLS et S/MIME. Si vous utilisez une clé ou un certificat ne permettant qu'un cryptage faible pour TLS, cette clé ou ce certificat sera remplacé(e) par la clé ou le certificat préinstallé(e). Vous ne parviendrez pas à communiquer si vous utilisez une clé ou un certificat ne permettant qu'un cryptage faible pour des fonctions autres que TLS.
Utilisation de TPM pour stocker les mots de passe et les clés	Disponible uniquement sur les modèles sur lesquels TPM est installé. Sauvegardez toujours les clés TPM lorsque TPM est activé. Reportez-vous au manuel de l'utilisateur pour plus de détails. Remarques importantes en cas d'activation des paramètres TPM : • Prenez soin de remplacer le mot de passe de l'administrateur par défaut, afin d'empêcher tout tiers, autre que l'administrateur, d'effectuer une sauvegarde de la clé TPM. Si un tiers s'empare de la clé TPM de sauvegarde, toute restauration de la clé TPM sera impossible. • Pour accroître la sécurité, la clé TPM ne peut être sauvegardée qu'une seule fois. Si les paramètres TPM sont activés, veillez à sauvegarder la clé TPM sur un périphérique de stockage USB que vous conserverez en lieu sûr, afin qu'il ne soit ni perdu, ni volé. • Les fonctions de sécurité offertes par TPM ne garantissent pas une protection totale des données ou du matériel.

4. Journal	Notes
Enregistrement forcé d'un journal d'audit	• <Save Operation Log/Enregistrer le journal des opérations> est défini sur <On/Activé>. • <Display Job Log/Afficher le journal des tâches> est défini sur <On/Activé>. • <Retrieve Job Log with Management Software/Récupérer le journal des tâches avec le logiciel de gestion> dans <Display Job Log/Afficher le journal des tâches> est défini sur <Allow/Autorisé>. • <Save Audit Log/Enregistrer le journal d'audit> est défini sur <On/Activé>. • <Retrieve Network Authentication Log/Récupérer le journal d'authentification réseau> est défini sur <On/Activé>. Lorsque ce paramètre est activé, les journaux d'audit sont toujours enregistrés.
Application forcée des paramètres SNTP	Saisissez l'adresse du serveur SNTP. Dans <SNTP Settings/Réglages SNTP>, <Use SNTP/Utiliser SNTP> est défini sur <On/Activé>. La synchronisation de l'heure via SNTP est requise. Entrez une valeur pour [Server Name/Nom du serveur] sur l'écran de paramétrage de l'interface utilisateur à distance.
Rapport du journal Syslog	Activez les détails de destination Syslog lorsque vous utilisez un serveur Syslog ou SIEM • <Username and password/Nom d'utilisateur et mot de passe> • <SMB server name/Nom du serveur SMB> • <Destination path/Chemin de destination> • <Perform export time/Durée d'exportation>

5. Travail	Notes
Politique d'impression	
Interdiction d'imprimer immédiatement les travaux reçus	Lorsque l'impression immédiate des travaux reçus est interdite, les travaux sont stockés dans la mémoire du télécopieur/fax par Internet. • <Handle Files with Forwarding Errors/Gérer les fichiers comportant des erreurs de transmission> est défini sur <Off/Désactivé>. • <Use Fax Memory Lock/Utiliser le verrouillage mémoire du Fax> est défini sur <On/Activé>. • <Use I-Fax Memory Lock/Utiliser le verrouillage mémoire du I-Fax> est défini sur <On/Activé>. • <Memory Lock End Time/Heure de fin du verrouillage mémoire> est défini sur <Off/Désactivé>. • <Display Print When Storing from Printer Driver/Afficher l'impression lors de la sauvegarde depuis le pilote d'imprimante> dans <Set/Register Confidential Fax Inboxes/Définir/enregistrer des boîtes de réception confidentielles de fax> est défini sur <Off/Désactivé>. • <Settings for All Mail Boxes/Réglages pour toutes les boîtes mail> > <Print When Storing from Printer Driver/Imprimer lors de la sauvegarde depuis le pilote d'imprimante> est défini sur <Off/Désactivé>. • <Box Security Settings/Réglages de sécurité de la boîte> > <Display Print When Storing from Printer Driver/Afficher l'impression lors de la sauvegarde depuis le pilote d'imprimante> est défini sur <Off/Désactivé>. • <Prohibit Job from Unknown User/Interdire les tâches à un utilisateur inconnu> est défini sur <On/Activé>, et <Forced Hold/Attente forcée> est défini sur <On/Activé>. L'impression n'est pas exécutée sur-le-champ, même lorsque des opérations d'impression sont en cours
Politique d'envoi/réception	
Autorisation de l'envoi uniquement vers les adresses répertoriées	Dans <Limit New Destination/Limiter nouvelle destination>, les options <Fax>, <E-Mail>, <I-Fax> et <File/Fichier> sont définies sur <On/Activé>. L'envoi n'est possible qu'à destination d'adresses répertoriées dans le carnet d'adresses.
Confirmation forcée du numéro de fax	Avant d'envoyer un fax, les utilisateurs doivent resaisir le numéro de fax afin de confirmer qu'il s'agit du bon numéro.
Interdiction du transfert automatique	<Use Forwarding Settings/Utiliser les réglages de transfert> est défini sur <Off/Désactivé>. Il est impossible de transmettre automatiquement les télécopies.

6. Stockage	Notes
Suppression totale forcée des données	<Hard Disk Data Complete Deletion/Suppression totale des données du disque dur> est défini sur <On/Activé>.

Pour connaître toutes les caractéristiques techniques du périphérique imageRUNNER ADVANCE, consultez la page produit disponible à l'adresse https://www.canon-europe.com/business-printers-and-faxes/imagerunner-advance-dx/.

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

French edition v2.0