

SMARTSHIELD



Technologie de sécurité d'impression
intégrée

Pour les imprimantes ColorWave et
PlotWave

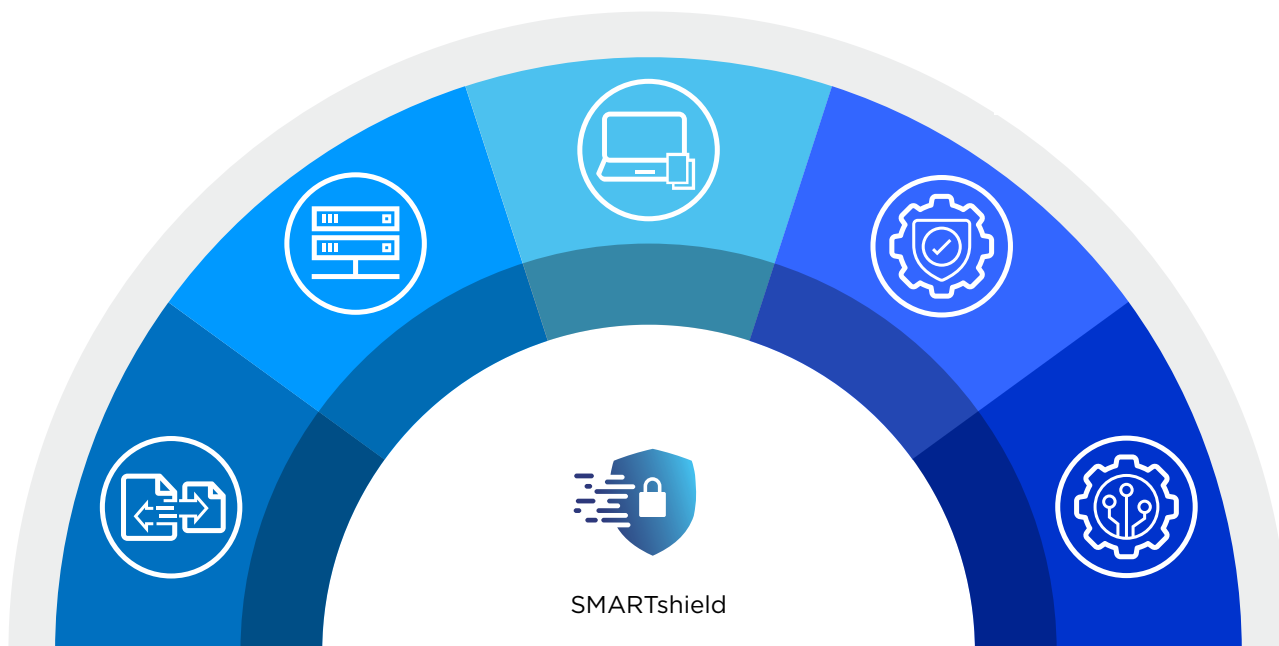
Canon

SÉCURITÉ D'IMPRESSION DE PREMIER ORDRE

Nos imprimantes grand format leaders sur le marché répondent aux préoccupations de sécurité des utilisateurs de documents techniques qui traitent des données clients confidentielles.

SMARTshield est une suite de fonctions de sécurité intégrées dans le flux de production d'impressions des derniers systèmes PlotWave et ColorWave. Conçue pour protéger vos systèmes aujourd'hui et demain.





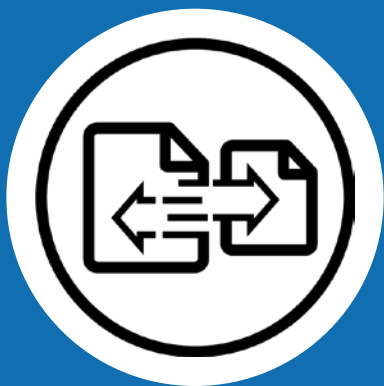
Aujourd'hui plus que jamais, les entreprises et les organismes gouvernementaux équipés d'imprimantes grand format doivent protéger leurs informations les plus importantes, confidentielles et sensibles au sein de leur bureau et sur leurs réseaux. Il s'agit des informations envoyées à l'imprimante par des postes de travail individuels et d'autres périphériques, ainsi que des données stockées sur l'imprimante même. Il est également essentiel que les systèmes soient protégés contre tout accès non autorisé aux données d'impression, aux informations imprimées et au système informatique de l'utilisateur final via des imprimantes. Les entreprises ont donc besoin d'une imprimante grand format sécurisée qui facilite la vie de l'administrateur informatique, des utilisateurs et des membres de la direction de l'entreprise.

SMARTshield est une technologie de sécurité d'impression entièrement intégrée à toutes nos imprimantes grand format et mise au point spécifiquement pour répondre à ces besoins.

SMARTshield propose plusieurs mesures de sécurité conçues pour empêcher que les données et les informations soient accessibles à des personnes non autorisées.

Grâce à SMARTshield, tous vos risques de sécurité, à chaque étape du flux de production, sont pris en compte.

SMARTshield vous protège aujourd'hui et demain.



ENVOI SÉCURISÉ

Protégez vos données lors de l'envoi de fichiers à votre imprimante, depuis n'importe quel périphérique.

Grâce aux applications de flux de production ClearConnect, les utilisateurs peuvent envoyer des fichiers depuis leur bureau ou n'importe quel appareil mobile. Avec un tel niveau de flexibilité et d'accès mobile, il est essentiel que les données importantes soient envoyées à l'imprimante en toute sécurité à tout moment et depuis tous les périphériques.



Compatibilité IPSec (Internet Protocol Security)



Compatibilité IPv6 et IPv4



HTTPS





STOCKAGE ET SUPPRESSION SÉCURISÉS

Protégez les données confidentielles stockées sur le disque dur de l'imprimante.

Il est impératif d'empêcher que les données confidentielles stockées sur l'imprimante soient volées ou sortent accidentellement de l'entreprise ou du service. SMARTshield crypte les données et limite l'accès via l'identification de l'utilisateur, ce qui garantit la sécurité de toutes vos données. En effaçant correctement les données, les utilisateurs sont certains que leurs fichiers confidentiels ne peuvent pas être consultés par des collègues non autorisés.

- Effacement sécurisé des fichiers
- Déchiquetage électronique
- Disque dur amovible
- Démarrage sécurisé
- Cryptage des données
- Destruction du disque dur à la fin du contrat





AUTORISATION

L'autorisation utilisateur SMARTshield évite que des utilisateurs non autorisés n'aient accès aux fichiers confidentiels.

De plus, en exigeant l'authentification des utilisateurs, vous gardez un contrôle plus strict de leurs activités. Il est également possible de limiter les fonctionnalités et les protocoles auxquels les utilisateurs peuvent accéder et de surveiller les dépenses engagées par chacun d'eux.



- Verrouillage des accès au panneau de contrôle
- Impression sécurisée via des identifiants de domaine (Active Directory)
- Impression sécurisée via une carte à puce (lecteur en option)
- Impression de fichiers uniquement disponibles dans votre boîte de réception intelligente
- Numérisation vers votre dossier d'accueil personnel
- Impression à partir de votre dossier d'accueil personnel
- Désactivation des ports et des interfaces
- Logiciels tiers tels que uniFLOW



PRÉVENTION DU PIRATAGE

Pour toute entreprise, l'un des plus grands défis en matière de sécurité consiste à se protéger des pirates informatiques. Avec autant de précieuses données imprimées, il est essentiel de limiter l'accès à l'imprimante et aux données stockées sur le contrôleur (ou le disque dur).

Il est également essentiel de vous assurer que votre imprimante ne peut pas être piratée ni utilisée contre votre réseau. SMARTshield relève le défi et protège du piratage sur plusieurs fronts :

- Désactivation des protocoles inutilisés
- SNMP v3
- Authentification IEEE 802.1x
- Antivirus McAfee (facultatif)
- Contrôle des applications de liste blanche McAfee (facultatif)





SÉCURITÉ AUJOURD'HUI ET DEMAIN

La sécurité est un domaine en perpétuel mouvement. Les pirates tentent constamment de trouver de nouvelles façons d'accéder à vos précieuses informations. SMARTshield a été conçu pour assurer la sécurité de vos informations, aujourd'hui et demain.

Et bien sûr, nos experts en sécurité surveillent en permanence les risques les plus récents afin de garantir la sécurité de vos données et de vos imprimantes. Les fonctionnalités actuelles incluent :

- Logiciel de contrôleur Windows 10 IoT Enterprise LTSC
- Support jusqu'en 2029 minimum
- Mises à jour de sécurité du contrôleur à distance
- Service à distance



Parce que nous comprenons vos préoccupations en matière de sécurité, nous avons mis au point une suite de fonctionnalités qui protègent votre entreprise des risques auxquels elle est confrontée à chaque étape de votre flux de production. Non seulement aujourd'hui, mais également demain.

Canon est votre partenaire pour un environnement d'impression sûr.

COMPATIBLE AVEC SMARTSHIELD

SMARTshield est intégré aux systèmes suivants :

ColorWave 3600



ColorWave 3800



Série PlotWave 3000



Série PlotWave 5000



PlotWave 7500



SMARTSHIELD

EN DÉTAIL

ENVOI SÉCURISÉ

**Compatibilité IPsec
(Internet Protocol
Security)**

Compatibilité IPv6 et IPv4

HTTPS

IPSec est un protocole qui assure l'authentification, la confidentialité et l'intégrité des données communiquées sur le réseau entre le contrôleur et d'autres périphériques.

Internet Protocol version 4 (IPv4) est l'un des protocoles de base des méthodes normalisées d'interconnexion de réseaux sur Internet et d'autres réseaux à commutation de paquets. Il utilise des adresses 32 bits. IPv6 est la version la plus récente et dans la mesure où elle utilise des adresses de 128 bits, elle fonctionne avec beaucoup plus de périphériques.

Afin d'éviter que le trafic réseau pour WebTools Express, Publisher Express et Publisher Select utilisant le protocole HTTP ne soit intercepté ou modifié, le protocole HTTPS peut être utilisé au lieu du trafic HTTP avec le contrôleur. De plus, il est possible d'intégrer dans le contrôleur des certificats de confiance émis par une autorité de certification pour empêcher toute tentative d'interception, c'est-à-dire empêcher qu'une partie malveillante se trouvant sur le chemin du serveur du contrôleur ne se fasse passer pour le contrôleur.

STOCKAGE ET SUPPRESSION SÉCURISÉS

**Effacement sécurisé des
fichiers**

**Déchetage
électronique**

Disque dur amovible

Démarrage sécurisé

Cryptage des données

**Destruction du disque dur
à la fin du contrat**

Supprimez automatiquement les travaux d'impression, de numérisation et de copie de la boîte de réception intelligente après l'heure définie par l'utilisateur. L'effacement des fichiers est sécurisé lors de l'activation du déchetage électronique.

La fonction de déchetage électronique est une fonction de sécurité qui permet au système d'écraser les données d'impression/de copie/de numérisation de l'utilisateur une fois celles-ci supprimées du système. Ainsi, toutes les données utilisateur supprimées, y compris le contenu et les attributs des fichiers, ne peuvent pas être récupérées, par exemple en cas de vol du disque.

Le kit de disque dur amovible en option permet aux administrateurs de retirer physiquement le disque dur interne du périphérique afin de le stocker dans un endroit sécurisé en dehors des heures de travail. Le lecteur est ensuite facilement réinstallable pour être utilisé pendant les heures de travail normales.

Le démarrage sécurisé est une norme de sécurité qui permet de s'assurer que le périphérique démarre uniquement via des logiciels fiables. Lorsque l'imprimante démarre, le logiciel du contrôleur vérifie la signature de chaque logiciel de démarrage.

Le cryptage du disque dur du contrôleur PowerSync crypte tous les fichiers présents sur l'ensemble du disque (y compris ceux du système d'exploitation et toutes les données ; cryptage de l'espace utilisé). Le mécanisme de cryptage est basé sur un TPM (Trusted Platform Module) et un système Microsoft BitLocker conforme à la certification FIPS 140-2. La méthode de cryptage AES 256 est utilisée.

À la demande du client, le disque dur interne du contrôleur PowerSync peut être retiré et physiquement détruit, ce qui garantit qu'aucune donnée d'impression du client ne reste sur l'imprimante une fois qu'elle a quitté les locaux du client.

AUTORISATION

**Verrouillage des accès au
panneau de contrôle**

**Impression sécurisée
via des identifiants de
domaine (Active Directory)**

**Impression sécurisée
via une carte à puce
(hors lecteur)**

**Impression de fichiers
uniquement disponibles
dans votre boîte de
réception intelligente**

**Numérisation vers
votre dossier d'accueil
personnel**

**Impression à partir de
votre dossier d'accueil
personnel**

**Désactivation des ports et
de l'interface**

**Logiciels tiers tels que
uniFLOW**

Lorsque vous activez la fonction de gestion des accès, le panneau de contrôle utilisateur ClearConnect n'est accessible qu'après le déverrouillage par le biais d'identifiants de domaine ou d'une carte à puce.

Les travaux d'impression « sensibles » envoyés par le propriétaire du travail ne sont pas imprimés tant que ce dernier ne s'est pas authentifié sur le panneau de contrôle utilisateur du système avec les bons identifiants utilisateur et qu'il n'en a pas demandé l'impression.

Les travaux d'impression « sensibles » envoyés par le propriétaire du travail ne sont pas imprimés tant que ce dernier ne s'est pas authentifié sur le panneau de contrôle utilisateur du système en insérant la carte à puce et qu'il n'en a pas demandé l'impression.

Lors de la désactivation de l'impression directe dans WebTools Express, le fichier d'impression attend dans votre boîte de réception intelligente jusqu'à ce qu'il soit activé à partir du panneau de contrôle ClearConnect ou de WebTools Express. Cette fonction évite que l'impression ne soit accidentellement utilisée par d'autres utilisateurs.

La fonction de numérisation vers le dossier d'accueil est disponible avec la méthode d'authentification par nom d'utilisateur et mot de passe. Après s'être authentifié sur le panneau de l'imprimante, l'utilisateur peut numériser un fichier dans son répertoire d'accueil sur le réseau, tel que configuré pour son compte dans MS Windows Active Directory.

La fonction d'impression à partir du dossier d'accueil est disponible avec la méthode d'authentification par nom d'utilisateur et mot de passe. Après s'être authentifié sur le panneau de l'imprimante, l'utilisateur peut imprimer depuis son répertoire d'accueil sur le réseau, tel que configuré pour son compte dans MS Windows Active Directory.

Pour sécuriser le contrôleur POWERSync contre tout accès non autorisé, tous les ports et interfaces réseau inutilisés sont désactivés.

Les systèmes d'impression PlotWave et ColorWave dotés d'une interface utilisateur ClearConnect peuvent être intégrés aux environnements uniFLOW du client. Les utilisateurs bénéficient ainsi de fonctionnalités supplémentaires qui leur permettent de contrôler et de réduire les coûts d'impression et de copie, de renforcer la sécurité des documents et d'améliorer la productivité des employés.



PRÉVENTION DU PIRATAGE

Désactivation des protocoles inutilisés

Les administrateurs réseau ont la possibilité de configurer les protocoles spécifiques qui sont accessibles. Par conséquent, les communications non souhaitées entre les appareils et l'accès au système via des protocoles de transport spécifiques indésirables peuvent être efficacement bloqués.

SNMP V3

Version sécurisée de SNMP qui assure l'authentification et l'intégrité entre la station de gestion du réseau (NMS) et les imprimantes gérées.

Authentification des périphériques 802.1X IEEE

Mécanisme d'authentification par port (conformément à la norme IEEE802.1X) permettant à un périphérique d'être authentifié par une autorité centrale afin de communiquer sur le réseau avec les autres périphériques.

Antivirus McAfee (facultatif)

Possibilité d'installer le logiciel antivirus McAfee sur le contrôleur PowerSync comme mesure de protection supplémentaire contre les infections virales.

Contrôle des applications de liste blanche McAfee (facultatif)

Fonction de sécurité en option, activée via une licence. Lorsqu'elle est activée, elle crée une liste détaillée de tous les fichiers sur le contrôleur et empêche toute modification non autorisée, que ce soit par des programmes malveillants, des virus ou des utilisateurs non autorisés. Elle vérifie en permanence l'intégrité des fichiers par rapport à la liste et bloque toute modification non autorisée.

SÉCURITÉ AUJOURD'HUI ET DEMAIN

Logiciel de contrôleur Windows 10 IoT Enterprise LTSC

Le contrôleur PowerSync de l'imprimante utilise Windows 10 IoT Enterprise LTSC.

Support jusqu'en 2029 minimum

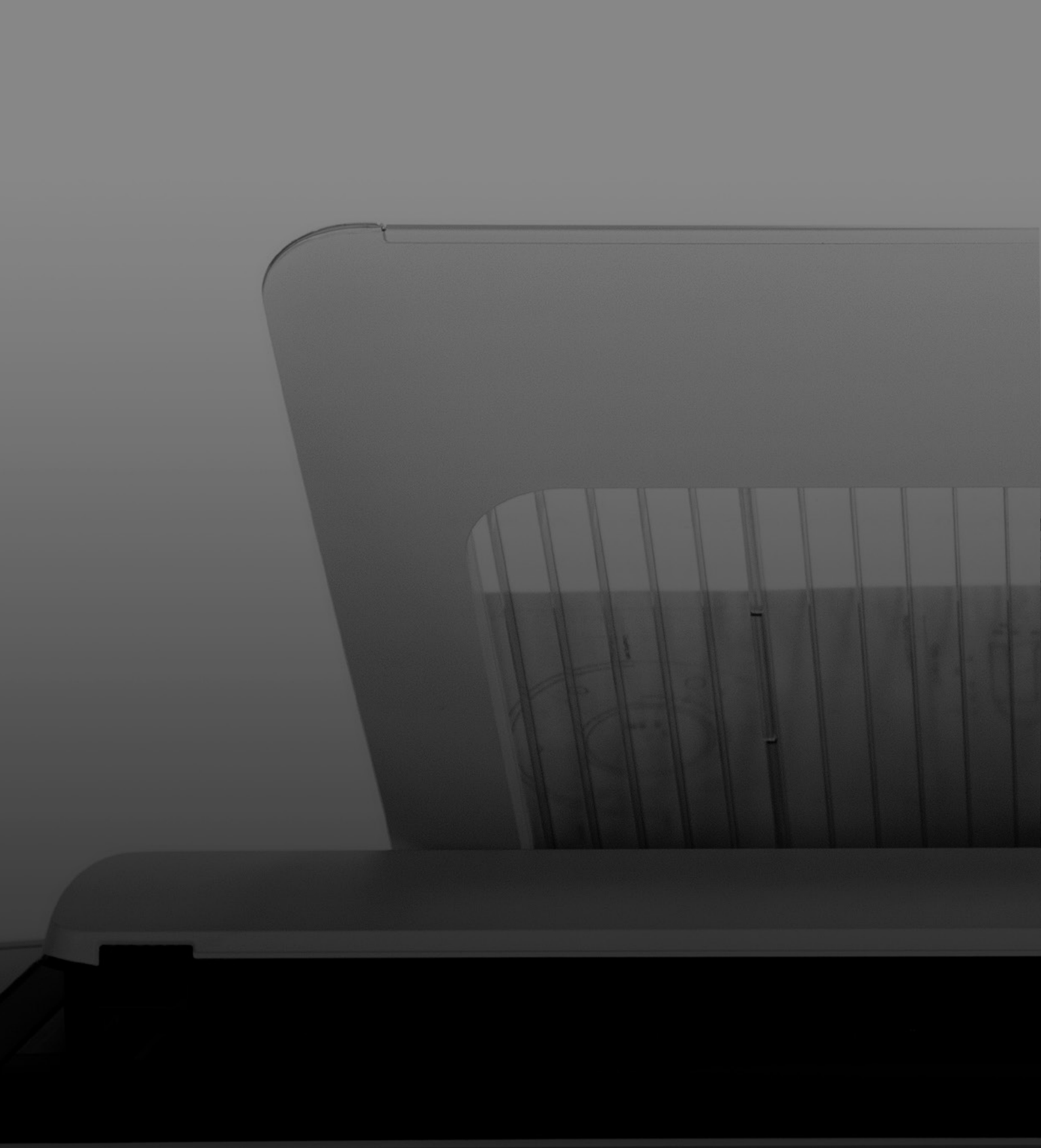
Microsoft garantit le support de Windows 10 IoT Enterprise LTSC jusqu'en 2029 minimum. Des mises à jour de sécurité seront donc fournies jusqu'à cette date.

Mises à jour de sécurité du contrôleur à distance

Via WebTools Express, l'administrateur système peut télécharger et installer à distance des mises à jour de sécurité. Vous bénéficiez ainsi d'une réaction rapide et d'un temps de fonctionnement élevé, car le technicien de maintenance n'a pas à intervenir physiquement sur l'imprimante.

On Remote Service

On Remote Service est un service développé par Canon pour garantir une disponibilité optimale de votre système Canon. Étant une application intégrée au contrôleur, Remote Service vous offre un support à distance, notamment le diagnostic, la lecture de compteurs et l'assistance à distance. Avantages de cette application : une disponibilité accrue de votre système, moins de tâches d'administration, un meilleur niveau de réparation dès la première intervention, des temps de réponse plus rapides et, surtout, une plus grande tranquillité d'esprit.



© 2020 Canon Production Printing

Canon est une marque déposée de Canon Inc. ColorWave, PlotWave et SMARTshield sont des marques déposées de Canon Production Printing Netherlands BV. Toutes les autres marques sont la propriété de leurs détenteurs respectifs et reconnues ici comme telles.

Aucune partie de cette publication ne peut être copiée, modifiée, reproduite ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, manuel ou autre, sans l'autorisation de Canon Production Printing. Les illustrations et les images de sortie sont simulées et ne s'appliquent pas nécessairement aux produits et services proposés sur chaque marché local. Le contenu de cette publication ne doit pas être interprété comme une garantie concernant des propriétés ou spécifications particulières ni concernant des performances techniques ou l'adéquation à un usage particulier. Le contenu de cette publication peut être soumis à des modifications à tout moment, sans préavis. Canon Production Printing ne saurait être tenu responsable des dommages directs, indirects ou consécutifs ni des pertes ou dépenses résultant de l'utilisation du contenu de cette publication.

Canon

Canon France S.A.
14 rue Emile Borel
75017 Paris
Tél. : 01 85 14 40 00
canon.fr

Canon Belgium NV/SA
Berkenlaan 3
1831 Diegem
Tel. 02-722 04 11
Fax 02-721 32 74
canon.be

Canon Luxembourg SA
West Side Village Complex
Building E
Rue Pafbruch 89E
L-8308 Capellen
Tél. : 48 47 961
Fax : 48 47 96 235
canon.lu

Canon (Suisse) SA
Richtstrasse 9
CH-8304 Wallisellen
Tel. +41 (0)22 567 58 58
canon.ch
French edition