LA SÉCURITÉ DES INFORMATIONS AVEC LA eMAINTENANCE CANON

La eMaintenance de Canon prend en charge la gestion et l'administration de toutes vos imprimantes multifonction et monofonction Canon en réseau tout en respectant des protocoles de sécurité stricts.

PARTIE 1 : QUESTIONS FRÉQUENTES

Ce document a pour objectif de répondre aux principales questions sur la sécurité que vous pourriez avoir concernant eMaintenance. Pour plus d'informations sur la sécurité intégrée à eMaintenance, veuillez contacter votre représentant Canon local.

Qui est propriétaire de mes données ?

Dans tous les cas, vous êtes propriétaire de vos données, Canon n'étant qu'un sous-traitant agréé des données eMaintenance de ses clients.

Qui peut accéder à mes données ?

Canon propose une approche à plusieurs niveaux de la régulation de l'accès aux données, notamment :

- **Contrôles d'accès physique :** seules les personnes autorisées sont autorisées à accéder physiquement aux locaux, aux bâtiments ou aux salles où des données personnelles sont stockées.
- **Contrôles d'accès au système :** les systèmes traitant des données à caractère personnel ne sont accessibles qu'avec une autorisation basée sur les rôles utilisateur et les autorisations associées.
- **Contrôles d'accès aux données :** les personnes autorisées à utiliser des systèmes de traitement des données n'ont accès qu'aux données à caractère personnel pour lesquelles elles disposent d'un droit.
- **Contrôles de la transmission des données :** sauf si nécessaire pour la prestation de services conformément à l'accord concerné, les données à caractère personnel ne doivent pas être lues, copiées, modifiées ou supprimées sans autorisation pendant le transfert.
- **Contrôles de l'entrée des données :** Canon met en place des mesures qui permettent d'examiner rétrospectivement et d'établir si et par qui les données à caractère personnel ont été saisies, modifiées ou supprimées des systèmes de traitement des données de Canon.
- **Contrôle des tâches :** tous les employés de Canon et sous-traitants contractuels ou autres prestataires de services sont contractuellement tenus de respecter la confidentialité de toutes les informations sensibles.
- **Contrôles de la séparation des données :** les données à caractère personnel sont uniquement stockées et accessibles depuis le tenant eMaintenance individuel de chaque client.

L'accès aux données est contrôlé à l'aide des mesures suivantes :

- Dans le cadre de la politique de sécurité de Canon, les données à caractère personnel des clients nécessitent au moins le même niveau de protection que les informations « confidentielles ».
- L'accès aux données à caractère personnel est accordé sur la base de la nécessité de les connaître. Le personnel a accès aux informations dont il a besoin pour remplir ses fonctions.
- Les mesures de sécurité qui protègent les applications traitant des données à caractère personnel sont régulièrement vérifiées. À cette fin, Canon effectue des contrôles de sécurité internes et externes ainsi que des tests de pénétration sur ses systèmes informatiques.
- Les données à caractère personnel ne doivent pas être lues, copiées, modifiées ou supprimées sans autorisation dans le cadre du traitement, de l'utilisation et du stockage.

Mes données sont-elles chiffrées ?

Les données stockées dans le service cloud AWS sont chiffrées.

Lorsque des données sont transférées entre Canon et ses clients, cela est toujours effectué via des protocoles de transport de chiffrement sécurisés.

Les données à caractère personnel pouvant être stockées lors de l'utilisation du service de sauvegarde des données ou du service d'assistance à l'installation en option, telles que les données du carnet d'adresses de l'appareil, sont chiffrées à l'aide d'AES-256.

Comment mes données sont-elles séparées des données des autres clients ?

Les données à caractère personnel sont traitées à l'aide des contrôles de séparation suivants :

Canon utilise des contrôles techniques appropriés pour assurer la séparation logique des données à caractère personnel des clients.

Le cas échéant, une arborescence multicouche garantit que le tenant d'un parent a accès au tenant de ses enfants, mais les enfants ne peuvent pas accéder à d'autres tenants au même niveau ou à un niveau supérieur (comme celui des parents).

Quelles données sont collectées par eMaintenance ?

La majorité des données collectées et utilisées par eMaintenance sont des données d'appareil à caractère non personnel telles que le client, le nom de l'appareil, le numéro de série, l'emplacement, l'adresse IP, l'état et les alertes.

Les informations suivantes ne sont pas collectées par eMaintenance : informations relatives au fonctionnement de l'utilisateur telles que le nom d'utilisateur*, la date/l'heure, le nom du document, le contenu du travail (données d'image/ données d'impression) pour la COPIE, l'IMPRESSION, la NUMÉRISATION et l'ENVOI.

Canon vérifie-t-il la sécurité de son cloud ?

Canon effectue divers audits comme les indicateurs de l'état de mise en œuvre de la sécurité des informations des services Cloud qu'elle fournit, afin de garantir que Canon et ses clients peuvent utiliser les services en toute confiance.

Afin de vérifier les mesures de sécurité eMaintenance, des tests de pénétration sont effectués régulièrement par un tiers.

*Lors de l'utilisation du service facultatif de sauvegarde des données ou du service d'assistance à l'installation, les données à caractère personnel telles que le nom d'utilisateur et l'adresse e-mail peuvent être collectées si elles sont contenues dans le carnet d'adresses de l'appareil, mais uniquement dans le cadre d'un accord spécifique avec le client.

L'infrastructure cloud eMaintenance est-elle sécurisée ?

Le service eMaintenance est hébergé sur la plate-forme AWS située à Francfort, en Allemagne.

eMaintenance dispose-t-elle d'une certification par rapport à l'une des principales normes de sécurité ?

Le Centre de développement de l'impression numérique de Canon Inc. est certifié conforme à la norme internationale ISO/IEC 27001. La certification obtenue est liée au développement par Canon Inc. du service de surveillance (y compris la suite eMaintenance) pour les appareils multifonctions (MFD) et les imprimantes.

En respectant les normes ISO/IEC 27001 et ISO/IEC 27017, Canon Inc. peut confirmer que ses processus de sécurité ont été certifiés par un tiers et sont conformes à une norme internationalement reconnue.

Cette norme démontre l'engagement de Canon Inc. en matière de sécurité des informations au sein de l'entreprise et de notre offre de services en ligne :

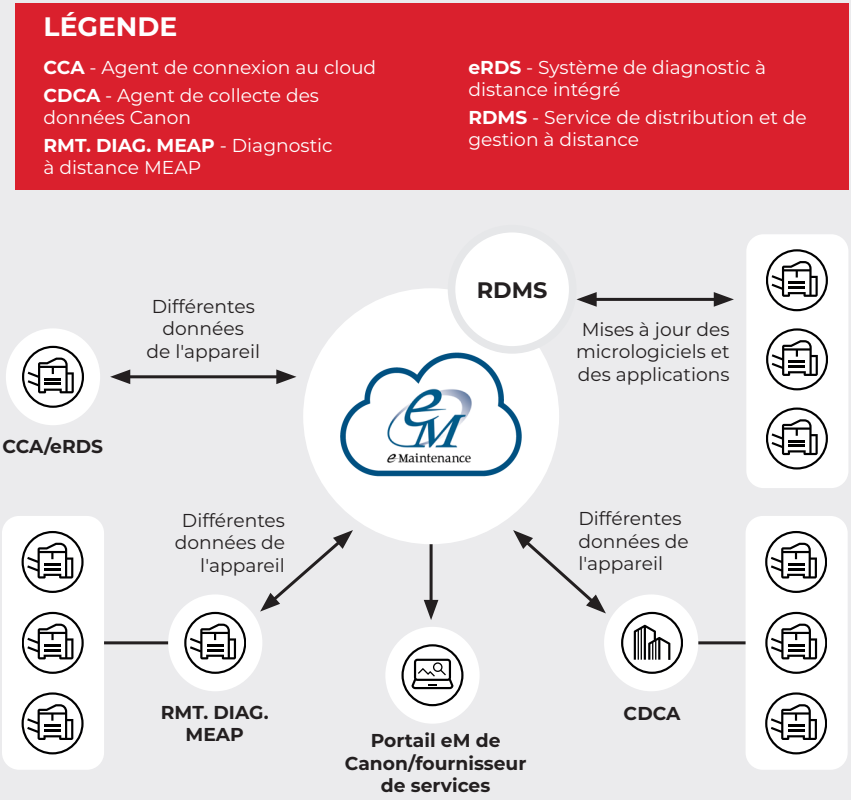
- **Confidentialité :** s'assurer que les informations sont accessibles uniquement aux personnes autorisées.
- **Intégrité :** protéger l'exactitude et la totalité des informations et des méthodes de traitement.

- **Disponibilité :** veiller à ce que les utilisateurs autorisés aient accès aux informations en temps voulu.

La norme ISO/IEC 27001 exige un examen régulier, et indique que les fonctions du service de surveillance sont développées et fournies par une organisation fiable et sécurisée qui a été confirmée par une certification tierce conformément aux normes internationales convenues.

Une partie de la norme ISO/IEC 27001 inclut la norme ISO/IEC 27017 qui définit des contrôles de sécurité supplémentaires spécifiquement destinés aux fournisseurs de services cloud. Elle décrit un cadre de sécurité des informations pour les entreprises qui utilisent des services cloud.

Canon a choisi de se conformer à ce code de pratique pour les contrôles de sécurité des informations, car il maintient la sécurité des clients de ses services cloud en leur proposant une approche cohérente et complète de la sécurité des informations.



PARTIE 2 : EXIGENCES EN MATIÈRE D'INFRASTRUCTURE eM

eM utilise un certain nombre d'agents locaux et d'applications logicielles pour des communications fournies entre les appareils Canon et le service eM. En fonction d'un certain nombre de facteurs tels que le type d'appareils, la configuration de l'infrastructure locale et les exigences de service, chaque client peut bénéficier d'un ou plusieurs de ces éléments.

Les options sont les suivantes :

CCA (Agent de connexion au cloud)

Le CCA est le dernier agent intégré à l'appareil pour eMaintenance. Il s'exécute en interne sur l'appareil sans qu'il soit nécessaire d'installer un agent de collecte de données distinct sur votre réseau. Étant donné qu'elle peut collecter une plus large gamme de données des appareils, la connectivité CCA est nécessaire pour bénéficier de tous les services et fonctionnalités eMaintenance les plus récents (et futurs), y compris le diagnostic et la réparation prédictifs basés sur l'IA. CCA peut être ajouté aux appareils existants exécutant eRDS.

CDCA (Agent de collecte des données Canon)

Il s'agit d'un agent installé sur PC pour eMaintenance. Ce logiciel de surveillance est installé sur un PC local du réseau du client.

RMT. DIAG. MEAP (Diagnostic à distance MEAP)

Il s'agit d'un logiciel agent intégré à l'appareil pour eMaintenance utilisant la plate-forme MEAP qui peut être utilisé pour surveiller l'appareil hôte et les autres appareils Canon sur le réseau. Idéal pour les petits réseaux qui ne nécessitent pas de serveur CDCA.

eRDS (Service de diagnostic à distance intégré)

eRDS est un agent intégré d'appareil hérité pour eMaintenance. Ce logiciel de suivi s'exécute en interne sur l'appareil même. eRDS envoie les informations de gestion des appareils au service eMaintenance et peut être configuré pour recevoir les mises à jour du micrologiciel et des licences d'application MEAP.

RMDS (Service de distribution et de gestion à distance)

Permet aux fournisseurs de services Canon agréés de gérer les produits et les licences pour les applications MEAP et les options iR, ainsi que de mettre à jour le micrologiciel et les licences d'application MEAP.

Service de sauvegarde des données

Ce service facultatif effectue une sauvegarde planifiée régulière des paramètres stockés sur l'appareil de stockage interne sous forme chiffrée vers le cloud. En cas de défaillance du disque dur/SSD/contrôleur nécessitant un remplacement, le service de sauvegarde des données peut restaurer les données sur l'appareil, ce qui réduit considérablement le délai de réparation.

Accès au réseau requis

Pour permettre à eMaintenance de fonctionner, les clients doivent accéder aux URL appropriées disponibles sur leur réseau pour les appareils Canon. Veuillez contacter votre représentant Canon pour obtenir la liste des URL spécifiques requises pour votre environnement.

URL DE CONNEXION eMAINTENANCE INDIVIDUELLE

Canon recommande l'utilisation de caractères de remplacement dans les exclusions de pare-feu tels que :
*.srv.ygles.com *.amazonaws.com
*.c-cdsknn.net *.ugwdevice.net

CCA	
hbp-ec1l.srv.ygles.com - Port 443	rgt.srv.ygles.com - Port 443
kinesis.eu-central-1.amazonaws.com - Port 443	camapi.srv.ygles.com - Port 443
cognito-identity.eu-central-1.amazonaws.com - Port 443	camapi-ec1.srv.ygles.com - Port 443
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com - Port 443 ou Port 8883	hbpm-ec1l.srv.ygles.com - Port 443
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX et versions ultérieures (mode standard)	**CDCA v2.XX et versions ultérieures (mode CCA)**
rgt.srv.ygles.com	hbp-ec1l.srv.ygles.com
hbpm-ec1l.srv.ygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ec1.srv.ygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ec1.srv.ygles.com	a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com
camapi.srv.ygles.com	rgt.srv.ygles.com
camapis.srv.ygles.com	hbpm-ec1l.srv.ygles.com
mds-ec1.srv.ygles.com	camapi-ec1.srv.ygles.com
gdlp01.c-wss.com	camapis-ec1.srv.ygles.com
www-ec1.srv.ygles.com	camapi.srv.ygles.com
cam-ec1.srv.ygles.com	camapis.srv.ygles.com
	mds-ec1.srv.ygles.com
	gdlp01.c-wss.com
	www-ec1.srv.ygles.com
	cam-ec1.srv.ygles.com
Pour RMT. DIAG. MEAP (mode CCA v4.0 et ultérieur)	**Pour RMT. DIAG. MEAP (mode HTTP)**
hbp-ec1l.srv.ygles.com	a01.ugwdevice.net - Port 443
kinesis.eu-central-1.amazonaws.com	b01.ugwdevice.net - Port 443
cognito-identity.eu-central-1.amazonaws.com	
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srv.ygles.com	
hbpm-ec1l.srv.ygles.com	
camapis-ec1.srv.ygles.com	
camapis.srv.ygles.com	
camapi-ec1.srv.ygles.com	
camapi.srv.ygles.com	
mds-ec1.srv.ygles.com	
eRDS	
a01.ugwdevice.net - Port 443	
b01.ugwdevice.net - Port 443	
cnvextdata-an1s.srv.ygles.com - Port 443 requis uniquement pour l'activation à distance de CCA sur les appareils existants avec eRDS	
Pour RDMS	
device.c-cdsknn.net - Port 443	a02.c-cdsknn.net - Port 443
device02.c-cdsknn.net - Port 443	
Pour le service de sauvegarde des données	
hbp-ec1l.srv.ygles.com - Port 443	b01.ugwdevice.net - Port 443
kinesis.eu-central-1.amazonaws.com - Port 443	cnvextdata-an1s.srv.ygles.com - Port 443
cognito-identity.eu-central-1.amazonaws.com - Port 443	camapi-ec1.srv.ygles.com - Port 443
a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com - Port 443 ou Port 8883	camapis-ec1.srv.ygles.com - Port 443
rgt.srv.ygles.com - Port 443	camapi.srv.ygles.com - Port 443
hbpm-ec1l.srv.ygles.com - Port 443	camapis.srv.ygles.com - Port 443
a01.ugwdevice.net - Port 443	dcf-ec1.srv.ygles.com - Port 443

Février 2025 - V.01

Canon Inc.
canon.com

Canon Europe
canon-europe.com

French edition

Canon France SAS
14 Rue Emile Borel
CS 28646
75809 PARIS CEDEX 17
Tél : 01 85 14 40 00

canon.fr
canon.be
canon.lu
canon.ch