



Canon

SEGURIDAD DE LA INFORMACIÓN CON CANON eMAINTENANCE

Canon eMaintenance se encarga de la gestión y administración de todos los dispositivos MFP y SFP en red de Canon sin dejar de lado el cumplimiento de estrictos protocolos de seguridad.



PARTE 1: PREGUNTAS FRECUENTES

El objetivo de este documento es responder a las principales preguntas de seguridad que puedas tener sobre eMaintenance. Para obtener más información sobre la seguridad integrada en eMaintenance, ponte en contacto con tu representante local de Canon.



¿Quién es el propietario de mis datos?

En todos los casos en los que tus datos sean propiedad tuya, Canon será el encargado del tratamiento de datos acordado para los datos de eMaintenance de los clientes.



¿Quién puede acceder a mis datos?

Canon ofrece un enfoque de varias capas para regular el acceso a los datos, a saber:

- **Controles de acceso físico:** Solo las personas autorizadas pueden acceder físicamente a las instalaciones, edificios o salas donde se almacenan los datos personales.
- **Controles de acceso al sistema:** Solo se puede acceder a los sistemas que procesan datos personales con autorización en función de los roles y los permisos de usuario.
- **Controles de acceso a datos:** Solo las personas autorizadas para usar dichos sistemas pueden acceder a los datos personales.
- **Controles de transmisión de datos:** A menos que sea necesario para la prestación de servicios en función del acuerdo pertinente, los datos personales no se podrán leer, copiar, modificar ni ser eliminados sin autorización durante la transferencia.
- **Controles de introducción de datos:** Canon aplica medidas que permiten examinar de forma retrospectiva y determinar si se han introducido, modificado o eliminado datos personales de sus sistemas de tratamiento de datos, así como la persona o personas que lo hayan hecho.

- **Controles de trabajo:** Todos los empleados de Canon y los subencargados contractuales, así como otros proveedores de servicios, están obligados contractualmente a respetar la privacidad de toda la información confidencial.
- **Controles de separación de datos:** Los datos personales solo se almacenan y son accesibles desde el inquilino de eMaintenance de cada cliente.

El acceso a los datos se controla mediante las siguientes medidas:

- Como parte de la política de seguridad de Canon, los datos personales de clientes requieren como mínimo el mismo nivel de protección que la información «confidencial».
- El acceso a los datos personales se concede según sea necesaria esta información. Los miembros del personal tienen acceso a la información que necesitan para realizar su trabajo.
- Las medidas de seguridad de las aplicaciones que tratan datos personales se comprueban periódicamente. Con este fin, Canon realiza comprobaciones de seguridad internas y externas, así como pruebas de penetración en sus sistemas de TI.
- Los datos personales no se podrán leer, copiar, modificar ni ser eliminados sin autorización durante su procesamiento, uso y almacenamiento.



¿Están cifrados mis datos?

Los datos almacenados en servicios en la nube de AWS están cifrados.

Cuando los datos se transfieren entre Canon y sus clientes, siempre se realizan a través de protocolos de transporte con cifrado seguro.

Los datos personales que puede que se almacenen al usar el servicio de copia de seguridad de datos opcional o el servicio de asistencia a la instalación, como los datos de la libreta de direcciones del dispositivo, se cifran mediante AES-256.



¿Cómo se separan mis datos de los de otros clientes?

Los datos personales se procesan mediante los siguientes controles de separación:

Canon utiliza los controles técnicos adecuados para llevar a cabo la separación lógica de los datos de los clientes.

Llegado el caso, una estructura de árbol multicapa garantiza que el inquilino del principal tenga acceso al de sus secundarios, pero los secundarios no pueden acceder a otros inquilinos del mismo nivel ni de niveles superiores (como el de los principales).



¿Qué datos recopila eMaintenance?

La mayoría de los datos recopilados y utilizados por eMaintenance son datos del dispositivo no identificables personalmente, como el cliente, el nombre del dispositivo, el número de serie, la ubicación, la dirección IP, el estado y las alertas.

eMaintenance no recopila la siguiente información: datos relacionados con la operación del usuario, como el nombre de usuario*, la fecha y la hora, el nombre del documento, el contenido del trabajo (datos de imagen/ datos de impresión) para COPIAR, IMPRIMIR, ESCANEAR y ENVIAR.



¿Audita Canon su seguridad en la nube?

Canon lleva a cabo varias auditorías, como indicadores del estado de implementación de la seguridad de la información de los servicios en la nube que proporciona, con el fin de garantizar que Canon y sus clientes puedan utilizar los servicios con confianza.

Con el fin de verificar las medidas de seguridad de eMaintenance, un tercero realiza pruebas de penetración periódicamente.

*Al utilizar el servicio de copia de seguridad de datos opcional o el servicio de asistencia a la instalación, se pueden recopilar datos personales, como el nombre de usuario y la dirección de correo electrónico, si están incluidos en la libreta de direcciones del dispositivo, pero solo si así se ha acordado específicamente con el cliente.





¿Es segura la infraestructura en la nube de eMaintenance?

El servicio eMaintenance se aloja en la plataforma AWS ubicada en Fráncfort (Alemania).



¿Cuenta eMaintenance con alguna certificación relacionada con los principales estándares de seguridad?

El centro de desarrollo de impresión digital de Canon Inc. cuenta con la certificación ISO/IEC 27001 del estándar internacional. La certificación obtenida está relacionada con el desarrollo, por parte de Canon Inc., del servicio de supervisión (incluido eMaintenance Suite) para dispositivos multifunción (MFD) e impresoras.

Al acatar las normativas ISO/IEC 27001 e ISO/IEC 27017, Canon Inc. confirma que sus procesos de seguridad han sido certificados por terceros según lo estipulado en el estándar internacionalmente reconocido.

Este estándar demuestra el compromiso de Canon Inc. con la seguridad de la información dentro de la empresa y con nuestra oferta de servicios online:

- **Confidencialidad:** Garantizar que solo las personas autorizadas puedan acceder a información.
- **Integridad:** Proteger la precisión y la integridad de la información y de los métodos de procesamiento.



- **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a la información cuando sea necesario.

La norma ISO/IEC 27001 requiere una revisión periódica y significa que las funciones del servicio de supervisión están siendo desarrolladas y distribuidas por una organización segura que ha sido certificada por un tercero de acuerdo con las normas internacionales acordadas.

Parte de la norma ISO/IEC 27001 incluye la norma ISO/IEC 27017, que define controles de seguridad adicionales específicos para proveedores de servicios en la nube. Describe un marco de seguridad de la información para las organizaciones que utilizan servicios en la nube.

Canon ha elegido cumplir este código de prácticas para los controles de seguridad de la información porque proporciona un enfoque coherente y completo para mantener a sus clientes de servicios en la nube más seguros.

LEYENDA

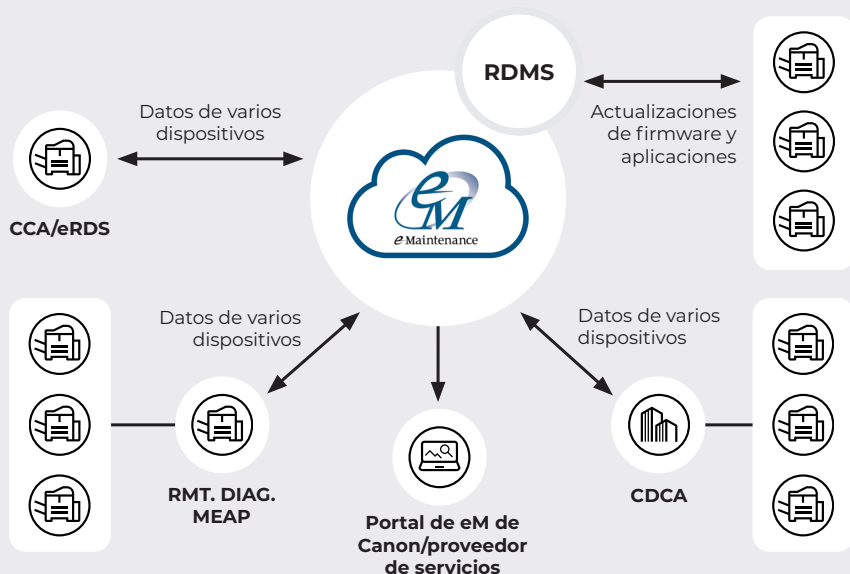
CCA: Cloud Connection Agent

CDCA: Canon Data Collection Agent

RMT, DIAG, MEAP: Remote Diagnostics MEAP

eRDS: embedded Remote Diagnostic Service

RDMS: Remote Distribution & Management Service



PARTE 2: REQUISITOS DE LA INFRAESTRUCTURA eM

eM utiliza una serie de agentes locales y aplicaciones de software para la comunicación entre los dispositivos Canon y el servicio eM. En función de factores como el tipo de dispositivo, la configuración de la infraestructura local y los requisitos del servicio, cada cliente puede tener uno o varios habilitados.

Las opciones son las siguientes:

CCA (Cloud Connection Agent)

CCA es el agente integrado en el dispositivo más reciente para eMaintenance, que se ejecuta internamente en el dispositivo sin necesidad de instalar un agente de recopilación de datos independiente en la red. Dado que puede recopilar una gama más amplia de datos de dispositivos, la conectividad CCA es necesaria para beneficiarse de todas las funciones y servicios de eMaintenance más recientes (y futuros), incluido el diagnóstico y la reparación predictivos basados en IA. CCA se puede añadir a dispositivos existentes que ejecuten eRDS.

CDCA (Canon Data Collection Agent)

Se trata de un agente instalado en un PC para eMaintenance. Este software de supervisión se instala en un PC local de la red del cliente.

RMT. DIAG. MEAP (Remote Diagnostics MEAP)

Se trata de un software de agente integrado en el dispositivo para eMaintenance que utiliza la plataforma MEAP y que permite supervisar el dispositivo host y otros dispositivos Canon en la red. Es ideal para redes más pequeñas que no requieren un servidor CDCA.

eRDS (embedded Remote Diagnostic Service)

eRDS es un agente integrado de dispositivos heredados para eMaintenance. Este software de supervisión se ejecuta internamente en el dispositivo. eRDS envía información de gestión de dispositivos al servicio eMaintenance y se puede configurar para recibir actualizaciones de firmware y licencias de aplicaciones MEAP.

RDMS (Remote Distribution & Management Service)

Permite a los proveedores de servicios autorizados de Canon gestionar productos y licencias para aplicaciones MEAP y opciones iR, así como actualizar el firmware y las licencias de dichas aplicaciones.

Servicio de copia de seguridad de datos

Este servicio opcional realiza una copia de seguridad programada periódica de la configuración almacenada en el dispositivo de almacenamiento interno en formato cifrado en la nube. En el caso de que se produzca un fallo en la unidad de disco duro/SSD/controladora que requiera sustitución, el servicio de copia de seguridad de datos puede restaurar los datos en el dispositivo, lo que reduce en gran medida el tiempo de reparación.

Acceso a la red necesario

Para que eMaintenance funcione, se pedirá a los clientes que accedan a las URL adecuadas disponibles a través de su red para los dispositivos Canon. Solicita a tu representante de Canon la lista de URL específicas necesarias para tu entorno.

URL DE CONEXIÓN DE eMAINTENANCE INDIVIDUALES

Canon recomienda el uso de comodines en las exclusiones del firewall, como:
*.srvygles.com *.amazonaws.com
*.c-cdsknn.net *.ugwdevice.net

CCA	
hbp-ec1.srvygles.com: Puerto 443	rgt.srvygles.com: Puerto 443
kinesis.eu-central-1.amazonaws.com: Puerto 443	camapi.srvygles.com: Puerto 443
cognito-identity.eu-central-1.amazonaws.com: Puerto 443	camapi-ec1.srvygles.com: Puerto 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com: Puerto 443 o Puerto 8883	hbpm-ec1.srvygles.com: Puerto 443
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX y posteriores (modo estándar)	CDCA v2.XX y posteriores (modo CCA)
rgt.srvygles.com	hbp-ec1.srvygles.com
hbpm-ec1.srvygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ec1.srvygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ec1.srvygles.com	a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com
camapi.srvygles.com	rgt.srvygles.com
camapis.srvygles.com	hbpm-ec1.srvygles.com
mds-ec1.srvygles.com	camapi-ec1.srvygles.com
gd1p01.c-wss.com	camapis-ec1.srvygles.com
www-ec1.srvygles.com	camapi.srvygles.com
cam-ec1.srvygles.com	camapis.srvygles.com
	mds-ec1.srvygles.com
	gd1p01.c-wss.com
	www-ec1.srvygles.com
	cam-ec1.srvygles.com
Para RMT. DIAG. MEAP (modo CCA v4.0 y posteriores)	Para RMT. DIAG. MEAP (modo HTTP)
hbp-ec1.srvygles.com	a01.ugwdevice.net: Puerto 443
kinesis.eu-central-1.amazonaws.com	b01.ugwdevice.net: Puerto 443
cognito-identity.eu-central-1.amazonaws.com	
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srvygles.com	
hbpm-ec1.srvygles.com	
camapis-ec1.srvygles.com	
camapis.srvygles.com	
camapi-ec1.srvygles.com	
camapi.srvygles.com	
mds-ec1.srvygles.com	
eRDS	
a01.ugwdevice.net: Puerto 443	
b01.ugwdevice.net: Puerto 443	
cnvextdata-anls.srvygles.com: El puerto 443 solo es necesario para la activación remota de CCA en dispositivos existentes con eRDS	
Para RDMS	
device.c-cdsknn.net: Puerto 443	a02.c-cdsknn.net: Puerto 443
device02.c-cdsknn.net: Puerto 443	
Para el servicio de copia de seguridad de datos	
hbp-ec1.srvygles.com: Puerto 443	b01.ugwdevice.net: Puerto 443
kinesis.eu-central-1.amazonaws.com: Puerto 443	cnvextdata-anls.srvygles.com: Puerto 443
cognito-identity.eu-central-1.amazonaws.com: Puerto 443	camapi-ec1.srvygles.com: Puerto 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com: Puerto 443 o Puerto 8883	camapis-ec1.srvygles.com: Puerto 443
rgt.srvygles.com: Puerto 443	camapi.srvygles.com: Puerto 443
hbpm-ec1.srvygles.com: Puerto 443	camapis.srvygles.com: Puerto 443
a01.ugwdevice.net: Puerto 443	dcf-ec1.srvygles.com: Puerto 443

