

INFORMATION SECURITY WITH CANON EMAINTENANCE

Canon's eMaintenance takes care of the management and administration of all your Canon networked MFP and SFP devices while adhering to strict security protocols.



PART 1: FREQUENTLY ASKED QUESTIONS

This document aims to answer the main security questions you might have regarding eMaintenance. For further information on the security embedded in eMaintenance please contact your local Canon representative.

Who owns my data?

In all cases your data is owned by you, Canon is only an agreed data processor of customers' eMaintenance data.

Who can access my data?

Canon provides a layered approach to regulating access to data including:

- Physical access controls – Only authorised persons allowed to physically access premises, buildings, or rooms where Personal Data is stored.
- System access controls – Systems processing Personal Data can only be accessed with authorisation based on user roles and associated permissions.
- Data access controls – Persons entitled to use data processing systems gain access only to the Personal Data that they have a right to access.
- Data transmission controls – Except as necessary for the provision of services in accordance with the relevant agreement, Personal Data must not be read, copied, modified, or removed without authorisation during transfer.
- Data input controls – Canon implements measures which make it possible to retrospectively examine and establish whether and by whom Personal Data has been entered, modified, or removed from Canon's data processing systems.
- Job controls – All Canon employees and contractual sub-processors or other service providers are contractually bound to respect the confidentiality of all sensitive information.
- Data separation controls – Personal Data is only stored and accessible from each customer's individual eMaintenance tenant.

Data access is controlled using the following measures:

- As part of Canon's Security Policy, Personal Data requires at least the same protection level as "confidential" information.
- Access to Personal Data is granted on a need-to-know basis. Personnel have access to the information that they require to fulfil their duty.
- Security measures that protect applications processing Personal Data are regularly checked. To this end, Canon conducts internal and external security checks and penetration tests on its IT systems.
- Personal Data must not be read, copied, modified or removed without authorisation in the course of processing, use and storage.

Is my data encrypted?

Data stored within the AWS cloud service is encrypted.

When data is transferred between Canon and its customers this is always conducted across secure encryption transport protocols.

Personal data that may be stored when using the optional Data Backup Service or Installation Support Service, such as device address book data, is encrypted using AES-256.

How is my data separated from other customers' data?

Personal Data is processed using the following separation controls:

Canon uses appropriate technical controls to achieve customer data logical separation.

Where applicable, a multi-layer tree structure ensures a parent's tenant has access to their children's tenant, however children cannot access other tenants at the same level or at a higher level (such as that of the parents).



What data is collected by eMaintenance?

The majority of data collected and used by eMaintenance is non-personally identifiable device data such as customer, device name, serial number, location, IP address, status and alerts.

The following information is not collected by eMaintenance: Information related to user's operation such as username*, date/time, document name, job contents (image data/print data) for COPY, PRINT, SCAN, and SEND.

Does Canon audit its cloud security?

Canon conducts various audits as indicators of the information security implementation status of the cloud services it provides, in order to ensure that Canon and its customers can use the services with confidence.

In order to verify the eMaintenance security measures, penetration tests are performed regularly by a third party.

*When using the optional Data Backup Service or Installation Support Service personal data such as username and email address may be collected if contained in the device address book, but only with specific agreement with the customer.

Is the eMaintenance cloud infrastructure secure?

The eMaintenance service is hosted on the AWS platform located in Frankfurt, Germany.

Does eMaintenance have any certification against any of the major security standards?

Canon Inc.'s Digital Printing Development Centre is certified according to the international standard ISO/IEC 27001. The certification gained is related to Canon Inc.'s development of the Monitoring Service (including eMaintenance Suite) for Multi-Function Devices (MFDs) and Printers.

By attaining ISO/IEC 27001 and ISO/IEC 27017, Canon Inc. can confirm its security processes have been 3rd party certified to an internationally recognised standard.

This standard demonstrates Canon Inc.'s commitment to information security within the company and our online service offering:

- **Confidentiality** – ensuring that information is accessible only to those authorised to have access.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods.

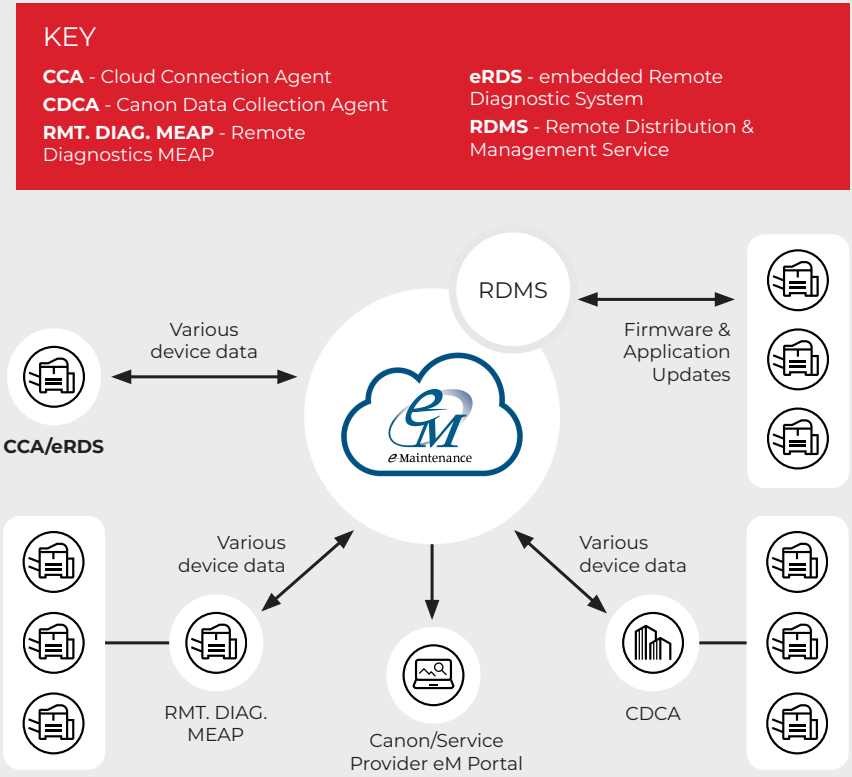


- **Availability** – ensuring that authorised users have access to information when needed.

ISO/IEC 27001 requires regular review and means that the Monitoring Service functions are being developed and delivered by a safe and secure organisation which has been confirmed by third-party certification according to agreed international standards.

Part of ISO/IEC 27001 includes ISO/IEC 27017 which defines additional security controls specifically for cloud service providers. It outlines an information security framework for organisations using cloud services.

Canon has chosen to comply with this code of practice for information security controls because it keeps their cloud service customers safer by providing a consistent and comprehensive approach to information security.



PART 2: eM INFRASTRUCTURE REQUIREMENTS

eM uses a number of local agents and software applications to provided communications between the Canon devices and the eM service. Dependent on a number of factors such as device type, local infrastructure set up and service requirement, each customer may have one or more of these enabled.

The options are as follows:

Cloud Connection Agent (CCA)

CCA is the latest device-embedded agent for eMaintenance, which runs internally on the device without the need for a separate data collection agent to be installed on your network. As it can collect a wider range of device data, CCA connectivity is required to benefit from all the latest (and future) eMaintenance functionality and services, including AI-based Predictive Diagnosis and Repair. CCA can be added to existing devices running eRDS.

Canon Data Collection Agent (CDCA)

This is a PC-installed agent for eMaintenance. This monitoring software is installed on a local PC on the customers' network.

Remote Diagnostics MEAP (RMT. DIAG. MEAP)

This is a device embedded agent software for eMaintenance using MEAP platform which can be used to monitor the host device and other Canon devices on the network. Ideal for smaller networks that don't require a CDCA server.

Embedded Remote Diagnostic Service (eRDS)

eRDS is a legacy device embedded agent for eMaintenance. This monitoring software runs internally on the device itself. eRDS sends device management information to the eMaintenance service and can be set up to receive firmware and MEAP application licenses updates.

Remote Distribution & Management Service (RDMS) & Setting Distribution

Enables authorised Canon Service providers to manage products and licenses for MEAP applications and device options & settings as well as update firmware and MEAP application licenses.

Data Backup Service (DBS)

This optional service takes a regular scheduled backup of the settings stored on the internal storage device in an encrypted form to the cloud. In the case of HDD/SSD/Controller failure requiring replacement, the Data Backup Service can restore the data to the device greatly reducing the repair time.

Remote Access

Permits remote service agent access to a device screen but only after one time code generated by the device is provided by the customer. Information is displayed on the screen showing that the device is being remotely accessed. Termination of the connection can be initiated by the end user, service agent or by automatic timeout.

Installation Support Service (ISS)

This is primarily used when a device is first built to apply its initial settings. It can also be used once the device is on-site to modify device settings locally.

INDIVIDUAL eMAINTENANCE CONNECTION URLs

Canon recommend the use of wildcards in Firewall exclusions such as:
*.srv.ygles.com *.ugwdevice.net
*.c-cdsknn.net *.c-wss.com

Connection Type						Service						
CCA*	eRDS	CDCA V1.x	CDCA V2.xx CCA CCA Mode/Standard	RMTDIAG MEAP V4.0	RMTDIAG MEAP V4.0 CCA	RDMS	Data Backup*	Remote Screen Access	Remote Setting Distribution	ISS	Access Destination FQDN	Application
	✓			✓							a01.ugwdevice.net	Data transmission & control
						✓				✓	a02.c-cdsknn.net	RDMS(API) Firmware
										✓	asd-ec18.srv.ygles.com	RDMS(API)
	✓	✓		✓							b01.ugwdevice.net	Data transmission & control
✓			✓		✓		✓			✓	camapi.srv.ygles.com	Authentication & authorization
✓			✓		✓		✓			✓	camapi-ec1.srv.ygles.com	Authentication & authorization
			✓		✓		✓				camapis.srv.ygles.com	Authentication & authorization
			✓		✓		✓				camapis-ec1.srv.ygles.com	Authentication & authorization
	✓										cnvextdata-an1s.srv.ygles.com	CCA comms check
							✓				dcf-ec1.srv.ygles.com	Backup Services API
						✓					device.c-cdsknn.net	RDMS(API)
						✓					device02.c-cdsknn.net	RDMS(API)
			✓								gdlp01.c-wss.com	Update Software
✓			✓		✓		✓	✓	✓		hbp-ec1l.srv.ygles.com	Data transmission
✓			✓		✓		✓				hbpm-ec1l.srv.ygles.com	Data transmission
										✓	iss-ec1.srv.ygles.com	ISS Portal API
										✓	issdata-ec1.srv.ygles.com	ISS Portal API
			✓		✓						mds-ec1.srv.ygles.com	Device registration
✓			✓		✓		✓				rgt.srv.ygles.com	Obtaining destination info
									✓		sadapi-ec18.srv.ygles.com	RDMS(API) Device settings

Note: All connection are via HTTPS on Port 443

*When using CCA or DBS the following url's are required if CCA Version in the device is 3.1.10 or Earlier

a2etju7iem1tgc-ats.iot.eu-central-1.amazonaws.com
cognito-identity.eu-central-1.amazonaws.com
kinesis.eu-central-1.amazonaws.com

Canon Inc.
canon.com

Canon Europe
canon-europe.com

English Edition
© Canon Europa N.V. 2026

Canon Europe Limited
4 Roundwood Avenue
Stockley Park
Uxbridge
UB11 1AF

Version 1.00