Canon

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 authorized 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 authorization 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 authorization 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 authorization 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.
- The customer (including its approved Controllers) will have access only to their own data based on secure authentication and authorisation.
- 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.

*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.

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.

Is the eMaintenance cloud infrastructure secure?

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

For further information on security in the AWS infrastructure please follow this link:

https://docs.aws.amazon.com/whitepapers/latest/introduction-aws-security/compliance.html

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 27001:2013. The certification gained is related to Canon INC's development of the Monitoring Service (including eMaintenance Suite) for Multi-Function Devices (MFD's) and Printers.

By attaining ISO/IEC 27001:2013 and ISO/IEC 27017:2015, Canon INC can confirm its security processes have been 3rd party certified to an internationally recognized standard.

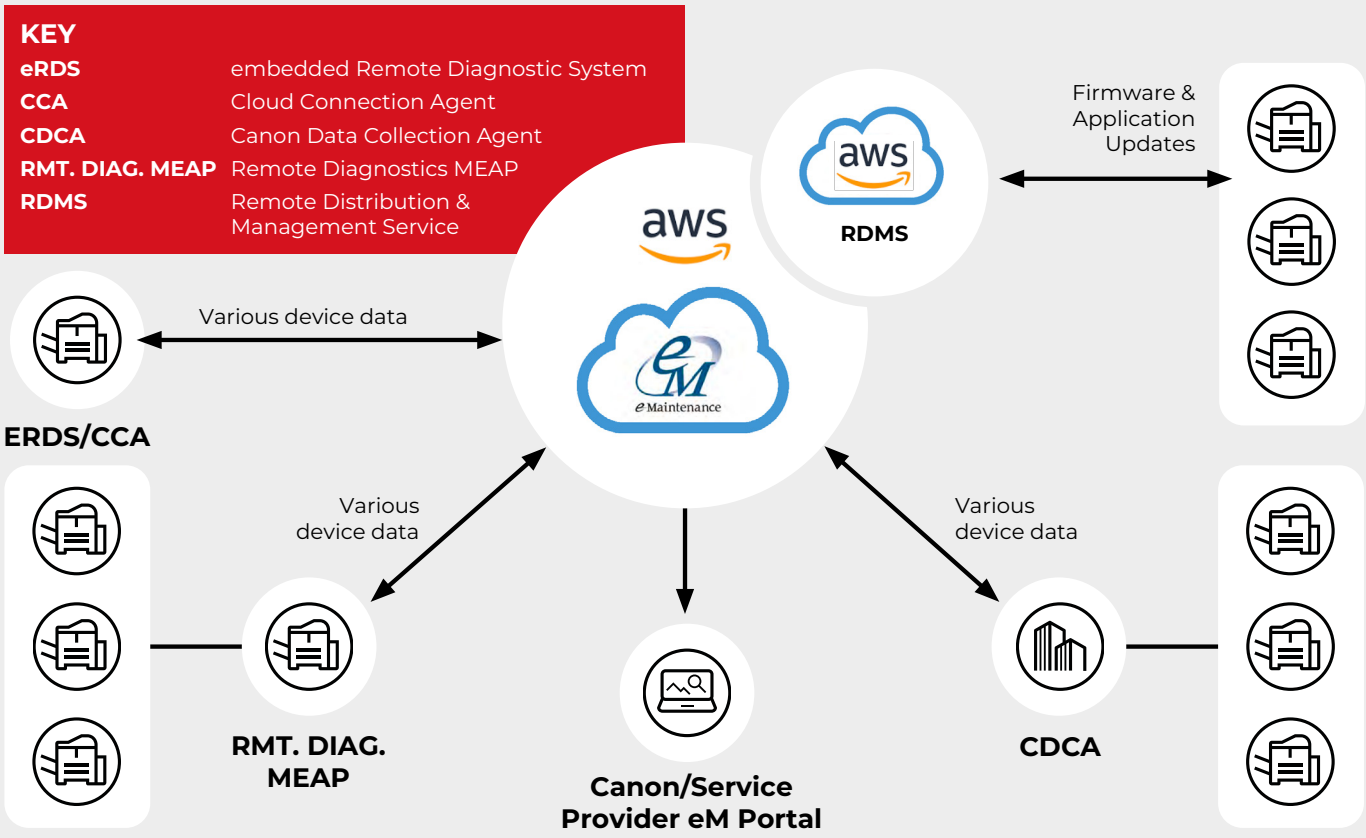
This standard demonstrates Canon INC's commitment to information security within the company and our online service offering:

- Confidentiality – ensuring that information is accessible only to those authorized to have access.
- Integrity – safeguarding the accuracy and completeness of information and processing methods.
- Availability – ensuring that authorized users have access to information when needed.

ISO/IEC 27001:2013 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 27001:2013 includes ISO/IEC 27017:2015 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. Dependant 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:

eRDS (embedded Remote Diagnostic Service)

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 updates.

CCA (Cloud Connection Agent)

CCA is the latest device embedded agent for eMaintenance. This monitoring software runs internally on the device itself. CCA sends a wider range of device management information to the eMaintenance service enabling enhanced functionality and services to be provided and can be set up to receive firmware and MEAP application updates.

CDCA (Canon Data Collection Agent)

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

RMT. DIAG. MEAP (Remote Diagnostics MEAP)

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.

RDMS (Remote Distribution & Management Service)

Enables authorized Canon Service providers to manage products and licenses for MEAP applications and iR options as well as update firmware and MEAP applications.

Data Backup Service

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.

Required Network Access

To enable eMaintenance to function, customers will be asked to make access to the appropriate URLs available through their network for the Canon devices. Please ask your Canon representative for the list of specific URLs required for your environment.

INDIVIDUAL eMAINTENANCE CONNECTION URLs

Canon recommend the use of wildcards in Firewall exclusions such as:

*.srv.ygles.com
*.amazonaws.com
*.c-cdsknn.net
*.ugwdevice.net

eRDS	
a01.ugwdevice.net - Port 443	
b01.ugwdevice.net - Port 443	
cnvextdata-an1s.srv.ygles.com - Port 443 is only required when switching from eRDS to CCA	
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 or Port 8883	
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX and newer (standard Mode)	**CDCA v2.XX and newer (CCA Mode)**
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
For RDMS	
device.c-cdsknn.net - Port 443	a02.c-cdsknn.net - Port 443
device02.c-cdsknn.net - Port 443	
For Data Backup Service	
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 or 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

Canon Inc.
canon.com

Canon Europe
canon-europe.com

English Edition

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