Security White Paper

Canon Universal Gateway (UGW) 2 – including eMaintenance (eM) and Canon Data Collection Agent (CDCA)

Date issued	December 2021
Author	
Document version	version v1.1

1 Purpose

1.1 Overview

This paper outlines Canon's approach to security for Universal Gateway 2 (hereinafter referred to as “UGW2”) including eMaintenance (hereinafter referred to as “eM”) supported by the UGW2 system.

This document describes the security features of the Universal Gateway 2 (below, UGW2), eMaintenance (eM) and Canon Data Collection Agent (CDCA).

UGW2 is a cloud-based service that communicates with customers' Multi-Functional Printing Devices via the Internet to support device management. In addition, UGW2 is composed of several services for device management, and users can select and use the services.

Canon believes that it is crucial to provide information on the data handled by UGW2 and on the security functions to ensure that users can use UGW2 with peace of mind.

In this security white paper, we first present an overall configuration diagram of the UGW2 and then disclose information on the types of data handled, the traffic generated, the network protocol used, and other data used in the service. In addition, the security functions implemented in the UGW2 are described.

1.2 Governance

This document is subject to version control. Reference should only be made to versions contained within the Portfolio and Business Development SharePoint site.

The content remains the property of Canon Europe and is not intended for external use unless prior written approval has been given by the Document Author.

This document does not require localization.

2 Overview & Introduction

2.1 Document overview

Previous Version of Document	1.0
Current Version of Document	1.1

3 System Overview

UGW2 is a platform used for managing selected Canon devices of customers. It consists of several services which are used to manage Canon devices and provide functionality as well as useful information about the installed devices to a customer. Further information on what the services provide can be found in Chapter 4.

UGW2 also has common management service. Common management service is utilized across UGW2 services and provides functions to manage dealer tenants, customer tenants, user accounts, devices, etc.

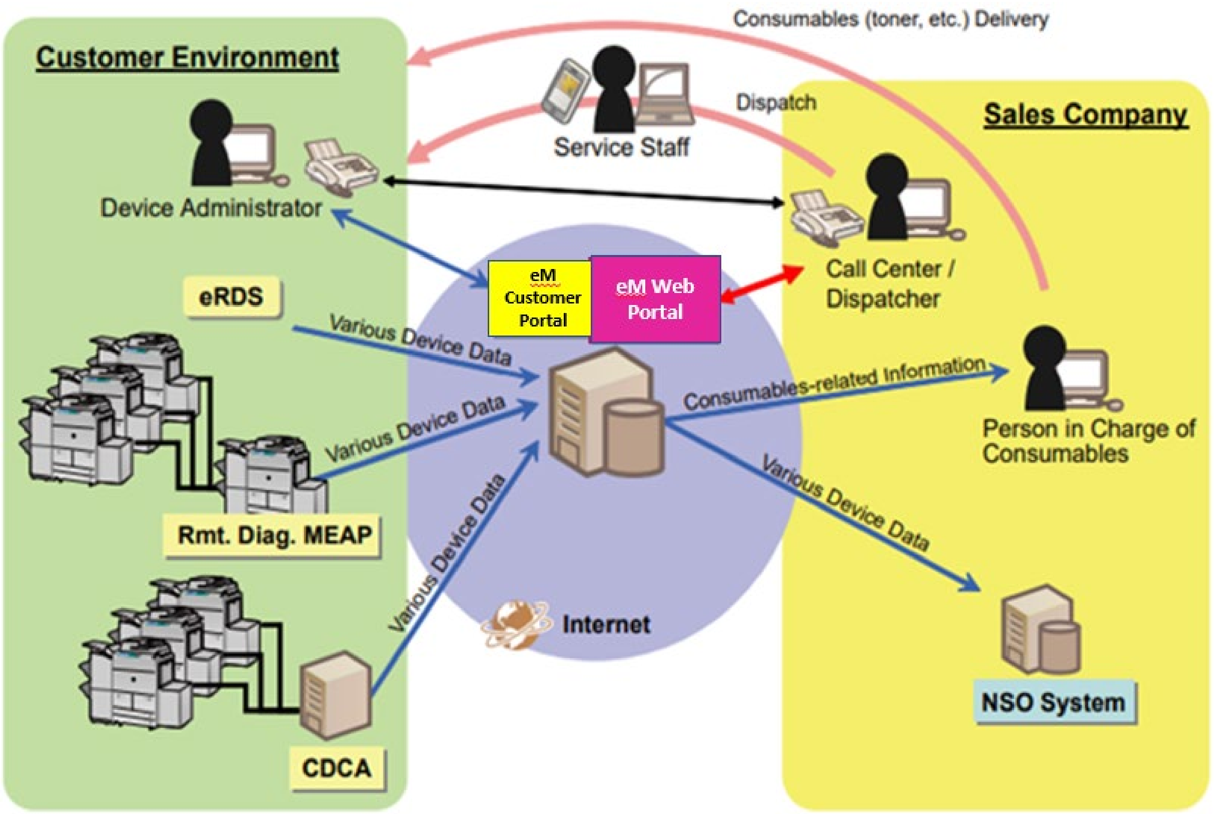
In addition, UGW2 is equipped with a platform that collects and accumulates operating information from a large number of devices. Each service provides functions by using data collected and accumulated in the UGW2 platform.

The collected data for eMaintenance and UGW2 is hosted on Amazon Web Services, on servers based in Europe.

For further information on where the different elements of UGW2 and eM are installed please refer to the diagram in Chapter 4.

4 System Configuration

UGW2 consists services which are useful for managing customers' devices, common functional services for supporting the services, and agent software for the services. (Refer to the following conceptual diagram.)



eMaintenance (eM)
This service supports maintenance contracts between Canon NSO/Partner (dealer) and their customers . eM provides the following information:

- Billing counters and other counter information
- Event occurrence information such as error, alarm and jam
- Consumption rate of toner, parts, etc., and consumables inventory management

UGW2 common function
It manages Canon NSO/Partner tenants, customer tenant, user accounts, devices, etc., and provides authentication and authorization services for clients accessing UGW2 (browsers, devices, applications, etc.).

UGW2 platform/RDS Compatible Interface
Agent software (Embedded RDS, RDS Plugin, Rmt.Diag.MEAP SMTP) supporting eMaintenance and device operation information sent from the SMTP interface are transferred to the of the local UGW2.

UGW2 platform/SMTP interface

This interface supports the communication protocol of Remote Monitoring Service-enabled client applications (Diag.MEAP SMTP, CDCA (SMTP mode), RDS Plugin SMTP) and transfers operating information from the device to an RDS-compatible interface.

4.2 Agent Software

4.2.1 Device Embedded Agents

Access Token Provider (ATP)

ATP is a device embedded agent software for UGW2 common functions. ATP communicates with the UGW2 common functions and performs authentication and authorization processing on the device side.

Embedded RDS (eRDS)

eRDS is a device embedded agent software for eMaintenance. This monitoring software runs on the device itself. eRDS sends device management information to the RDS compatible interface.

Remote Diagnostic (Rmt. Diag.) MEAP SMTP/HTTP (RDS MEAP)

RDS MEAP is a device embedded agent software for eMaintenance and a monitoring program using MEAP platform. RDS MEAP enables monitoring of the installed device itself and other devices and send management information about the device to an RDS compatible interface.

4.2.2 PC Installed Agent

Remote Diagnostic System (RDS) Plugin

RDS Plugin is a PC-installed agent for eMaintenance. This monitoring software is installed on a general-purpose PC. It can monitor 1 ~ 3000 devices and sends device management information to the RDS compatible interface.

Canon Data Collection Agent (CDCA)

CDCA is a PC-installed agent for eMaintenance. This monitoring software is installed on a general-purpose PC and can monitor 1 ~ 1000 devices. Operating modes include HTTPS mode and SMTP mode (v 1.1 and later), where HTTPS mode sends device management information to RDS-compatible interface and SMTP mode sends the information to SMTP interface.

4.3 Device extension application

MEAP-integrated Delivery Assistant Service (MDAS)

Application Configuration Management (hereinafter referred to as ACM)

MDAS and ACM are MEAP applications for importing and exporting MEAP application settings.

5 Management Information & communication specifications

5.1 Data traffic between the monitor and the device

Data Source	Individual Data Summary	Data Transmission size	Data transmission timing
RDS Plug-in v2.x	Event Occurrence Notification	About 1 kbytes	each time an event occurs
	status monitoring	About 1 kbytes	Once every 5 minutes
	Service Call Log	Approximately 0.7 kbytes	each time an event occurs
	alarm log	Approximately 0.7 kbytes	each time an event occurs
	jam log	Approximately 0.7 kbytes	each time an event occurs
	billing counter	Approximately 11kbytes	Up to once per hour
	part counter	About 4 kbytes	Up to once per hour
	Counters by mode	Approximately 7 kbytes	Up to once per hour
	Firmware Version	About 3 kbytes	Up to once per hour
	Environment log	Approximately 6 kbytes	Once every 3 hours
	Event Occurrence Notification	Approximately 0.2 kbytes	each time an event occurs
	status monitoring	About 1 kbytes	Once every 5 minutes
	Service Call Log	Approximately 0.7 kbytes	each time an event occurs
	alarm log	Approximately 0.7 kbytes	each time an event occurs
	jam log	Approximately 0.7 kbytes	each time an event occurs
	part counter	Approximately 4 Kbytes	Once every 6 hours
	Counters by mode	Approximately 7 Kbytes	Once every 6 hours
	Firmware Version	About 3 kbytes	Up to once per hour
	Environment log	Approximately 6 kbytes	Once every 3 hours
RDS Plug-in V3.x polling monitoring	Event Occurrence Notification	Approximately 0.2 kbytes	each time an event occurs
	status monitoring	About 1 kbytes	Once every 5 minutes
	Service Call Log	Approximately 0.7 kbytes	each time an event occurs
	alarm log	Approximately 0.7 kbytes	each time an event occurs
	jam log	Approximately 0.7 kbytes	each time an event occurs
	part counter	Approximately 4 Kbytes	Once every 6 hours
	Counters by mode	Approximately 7 Kbytes	Once every 6 hours
	Billing counter • Department Counter (HTTP Mode) • Total Resource Counter • Service Mode Counter	In the case of 1000 divisions: Approximately 712 Kbytes When there is no department registration: Approximately 15 Kbytes	Once every 6 hours
	Firmware Version	About 3 Kbytes	Once every 6 hours

	Environment log	Approximately 6 Kbytes	Once every 6 hours
RDS Plug-in V3.x Bit Connection Monitoring	Service Call Log	About 5 kbytes	each time an event occurs
	alarm log	About 5 kbytes s	each time an event occurs
	jam log	About 5 kbytes	each time an event occurs
	US > Alerts	About 5 kbytes	Whenever the monitored status changes
	part counter	Approximately 103 kbytes	Once every 8 hours
	Counters by mode	Approximately 164 kbytes	Once every 16 hours
	Billing counter • Department Counter (HTTP Mode) • Total Resource Counter • Service Mode Counter	In the case of 1000 divisions: Approximately 712 Kbytes When there is no department registration: Approximately 15 Kbytes	Once every 6 hours
	Firmware Version	About 5 kbytes	Once every 8 hours
	environment log	Approximately 6 kbytes	Once every 6 hours
	Service Mode Menu Information (ADJUST information, which is set values, and DISPLY values, which are measured values related to image formation)	Approximately 281 kbytes	During the initial communication test
	Service Mode Menu Information (ADJUST information, which is various settings in the service mode menu)	Approximately 154 kbytes	When service mode menu settings are changed
	Service Mode Menu Information DISPLAY value, which is a measurement related to image formation	Approximately 127 kbytes	each time a particular event occurs
	Enable Browser Options	About 3 kbytes	When Service Man Browser is enabled
	hard disk status diagnostic information	About 5 kbytes	Once in 30 days
	Inquire about setting information	Approximately 2 kbytes	Once every 12 hours
CDCA	status monitoring	Approximately 1.2 kbytes (Events included: 0.2 kbytes)	1.Once every 5 minutes (Do not retrieve during sleep) When a status change event occurs (Also retrieve during sleep)
	Service Call Log	Approximately 0.9 kbytes (Events included: 0.2 kbytes)	1. Once every 5 minutes (Do not retrieve during sleep) When getting log write events (Also retrieve during sleep)
	alarm log	Approximately 0.9 kbytes (Events included: 0.2 kbytes)	1. Once every 5 minutes (Do not retrieve during sleep) When getting log write events (Also retrieve during sleep)
	jam log	Approximately 0.9 kbytes (Events included: 0.2 kbytes)	1. Once every 5 minutes (Do not retrieve during sleep) When getting log write events (Also retrieve during sleep)
	Part Counter	Approximately 4 Kbytes	1. When acquisition has not been completed for 8 hours or more and less than 24 hours since the
	Counters by Mode	Approximately 7 Kbytes	
	Billing counter	In the case of 1000 divisions:	

	• Department Counter (HTTP Mode) • Total Resource Counter Service Mode Counter	Approximately 712 Kbytes When there is no department registration: Approximately 15 Kbytes	last acquisition (not acquired during Sleep) 2. When it has not been acquired for more than 24 hours since the last acquisition (Also retrieve during sleep) Service mode counters and all resource counters are also retrieved when status monitoring, service call logs, alarm logs, and jam logs are retrieved
	Firmware Version	About 3 Kbytes	
	environment log (HTTPS mode)	Approximately 6 Kbytes	
Rmt. Diag. MEAP (HTTP/SMTP) Polling monitoring	Status monitoring	Approx.1.2kbytes (events included: 0.2 kbtes)	Once per minute (also available during sleep)
	Service call log	Approx.0.9kbytes	Every time a log write event occurs
	Alarm log	Approx.0.9kbytes	Every time a log write event occurs
	Jam log	Approx.0.9kbytes	Every time a log write event occurs
	Parts counter	Approx.4Kbytes	Acquired at the following times: • During the transmission test • On startup • Once every 16 hours (HTTP)/Once every 24 hours (SMTP) • Once every 7 days (HTTP counters by mode)/once every 24 hours (SMTP)
	Mode Counter	Approx.7Kbytes	
	Billing counter • Department Counter (HTTP Mode) • Total Resource Counter Service Mode Counter	In the case of 1000 divisions: Approximately 712 Kbytes When there is no department registration: Approximately 15 Kbytes	
	Firmware Version	Approx.3Kbytes	
RDS Agent V2.6 (SMTP)	Status monitoring	Approx.1kbytes	Once per minute
	Service call log	Approx.1kbytes	Every time an event occurs
	Alarm log	Approx.1kbytes	Every time an event occurs
	Jam log	Approx.1kbytes	Every time an event occurs
	Parts counter	Approx.4kbytes	Once every 4 hours
	Mode Counter	Approx.7kbytes	Once every 4 hours
	Billing counter	Approx.11kbytes	Once every 4 hours
	Firmware Version	Approx.3kbytes	Once every 4 hours

5.2 Protocol used and destination FQDN - eMaintenance

Protocol	Port Number	Data	Application	Access Destination FQDN
HTTPS	TCP/443	eRDS RDS Plug-in (HTTP Version) Rmt. Diag. MEAP HTTP CDCA (HTTPS mode)	Data transmission and control	• a01.ugwdevice.net • b01.ugwdevice.net
SMTP	TCP/25 (587 ※3)	RDS Plug-in (SMTP version) Rmt. Diag. MEAP SMTP CDCA (SMTP mode) *4 RDS Agent V2.6 (SMTP)	data transmission	A local mail server or a mail server provided by Canon
HTTPS	TCP/443	ATP Browser Sales Company System Client	authentication and authorization	• www-ec1.srv.ygles.com • camapi-ec1.srv.ygles.com • cam-ec1.srv.ygles.com • camapis-ec1.srv.ygles.com • ec1-oip-lfscl-extacs.s3.amazonaws.com • ec1-oip-intvs.s3.amazonaws.com

HTTPS	TCP/443	ATP Browser Sales Company System Client	authentication and authorization	- camapi.srv.ygles.com - cam.srv.ygles.com - www.srv.ygles.com
HTTPS	TCP/443	Browser Sales Company System Client	Device Registration Management	mds-ec1.srv.ygles.com
HTTPS	TCP/443	Sales Company System Client	Provision of master information	mds.srv.ygles.com
HTTPS	TCP/443	Browser Sales Company System Client	eMaintenance (Portal/API)	- rcm-ec1.srv.ygles.com - rcmapi-ec1.srv.ygles.com - ec1-oip-extacs.s3.eu-central-1.amazonaws.com - ec1-rcm-lfscl-extdstb-1.s3.eu-central-1.amazonaws.com

5.3 Protocol used and destination FQDM

Monitoring Device	Protocol	Port Number	Data Source
RDS Plug-in	SNMP	UDP/161	monitoring device
	SNMP	UDP/50703 -65000 *	device
	Unique to Canon	TCP/47546	monitoring device
	Unique to Canon	UDP/47545	monitoring device
	Unique to Canon	TCP/9007	monitoring device
	Unique to Canon	UDP/50702 *	device
	SLP	UDP/427	monitoring device
	SLP	UDP/11427	device
	HTTPS	TCP/443	monitoring device
	HTTPS	TCP/443	device
CDCA	HTT P	TCP /80	monitoring device
	HTT P	TCP /8000	monitoring device
	HTT P	TCP /8080	monitoring device
	SNMP	U DP/161	monitoring device
	Unique to Canon	U DP/47545	monitoring device
	Unique to Canon	TCP /S pecified port from the device	monitoring device
	Unique to Canon	U DP/11427	device
	Unique to Canon	U DP/47545(DefaultValue)	device
	Unique to Canon	TCP /AutoAssignment	device
	Unique to Canon	U DP/AutoAssignment	device
	SNMP	U DP/AutoAssignment	device
Rmt. Diag. MEAP (HTTP/SMTP)	SNMP	U DP /161	monitoring device
	Unique to Canon	U DP /47545	monitoring device
	Unique to Canon	S pecified port from the TCP /device	monitoring device
RDS Agent V2.6 (SMTP)	SNMP	UDP/161	monitoring device
	Unique to Canon	UDP/47545	monitoring device
	Unique to Canon	TCP/9007	monitoring device
	SLP	UDP/427	monitoring device
	SLP	UDP/11427	device

5.4 Types of data and data traffic sent by client applications

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	eMaintenance
ATP	Device Identification Serial Number	Approximately 4 KB	During communication by ATP	Yes
ATP	Communication Test Results	Approximately 4 KB	During communication test with ATP	Yes
ATP(When checking the connection destination)	Device Basic Information • Device Name • Serial Number • Country Code • Country destination	Approximately 2 KB	Before transmission of communication test result	
eRDS	service mode counter	Approximately 110 KB	Once every 16 hours	Yes
	Total Resource Counter	Approximately 72 KB	Once every 16 hours	Yes
	part counter	Approximately 103 KB	Once every 16 hours	Yes
	Counters by mode	Approximately 164 KB	Once in 25 days (Some counters for certain models may be used once every 150 days.)	
	Inquire about setting information	Approximately 2 KB	During the initial communication test Once every 12 hours	Yes
	Service Call Log	Approximately 5 KB	each time an event occurs	Yes
	jam log	Approximately 5 KB	each time an event occurs	Yes
	alarm log	Approximately 5 KB	each time an event occurs	Yes
	US > Alerts	Approximately 5 KB	Whenever the monitored status changes	Yes
	Firmware Version	Approximately 5 KB	Once every 7 days (The model that transmits device configuration information does not transmit the firmware version.)	Yes
	Environmental information (Temperature/Humidity)	Approximately 6 kbytes	Once every 12 hours	
	Service Mode Menu Information	Approximately 281 KB	During the initial communication test	
		Approximately 154 KB	When service mode menu settings are changed	
		Approximately 127 KB	each time a particular event occurs	
	Enable Browser Options	Approximately 3 KB	When Service Man Browser is enabled	Yes
	Storage information (HDD/EMMC)	Approximately 5 KB	Once in 30 days	
	calibration log	Approximately 3 KB	time of calibration	Yes

	Device configuration information	Approximately 232 KB	The first communication test and when device configuration information is updated.	Yes
	Debug Log	Approximately 145 KB	When the log information reaches the specified number	
RDS Plug-in (HTTPS)	Charging Counter Information • Department Counter • Total Resource Counter • Service Mode Counter	In the case of 1000 divisions: Approximately 973 KB When there is no department registration: Approximately 149 KB	Send once every 12 hours	
	Part Counter Information	Approximately 105 KB	Send once every 16 hours	
	Counter Information by Mode	Approximately 169 KB	Send once every 7 days	
	Inquire about setting information	Approximately 2 KB	Once every 12 hours	
	Service Call Log	Approximately 5 KB	each time an event occurs	
	jam log	Approximately 5 KB	each time an event occurs	
	alarm log	Approximately 5 KB	each time an event occurs	
	US > Alerts	Approximately 5 KB	Whenever the monitored status changes	
	Firmware Version	Approximately 8 KB	Send once every 7 days	
	Environmental information (Temperature/Humidity)	Approximately 20 KB	Send once every 12 hours	
	Service Mode Menu Information (Bit connector only)	Approximately 150 KB	When registering a device to RDS	
		Approximately 100 KB	service mode menu setting value change	
		Approximately 50 KB	specific alarms, when errors occur	
	Enable Browser Options (Bit connector only)	Approximately 3 KB	When the browser enable button is pressed in the service mode menu	
	Storage information (HDD/EMMC) (Bit connector only)	Approximately 4.2 KB	Once in 30 days	
	Debug Log	Up to approximately 245 KB	When the log exceeds the specified number of lines (512 lines)	
RDS Plug-in (SMTP system)	service mode counter	Approximately 7 KB	once a day	Yes
	counter by paper			Yes
	environment log			
	part counter	Approximately 7 KB	Once every 7 days	Yes
	Counters by mode			
	Firmware Version			Yes
	Service Call Log	Approximately 1 KB	each time an event occurs	Yes
	jam log	Approximately 1.5 KB	Every time the jam log exceeds the specified number of times or specified rate	Yes

	Alarm Log Level 2/Level 3	Approximately 2 KB	Each time the level 2 alarm log exceeds the specified number of times or specified rate Every time a Level 3 event occurs	Yes
	Debug Log	Approximately 245 KB	When the log information reaches the specified number	
Rmt. Diag. MEAP SMTP	service mode counter	Approx.80KB	It is transmitted in the following three times: 1. During the transmission test 2. On Start-up 3. Once a day	Yes
	counter by paper	Approx.4KB		Yes
	part counter			Yes
	Counters by mode	Approx.70KB		
	Service Call Log	Approximately 2 KB	each time an event occurs	Yes
	jam log	Approximately 2 KB	each time an event occurs	Yes
	Alarm Log Level 2/Level 3	Approximately 2 KB	each time an event occurs	Yes
	Firmware Version	Approximately 2 KB	It is transmitted in the following times: 1. During the transmission test 2. On Startup 3. Once a day	Yes
	Debug Log	Approximately 55 KB	When the log information reaches the specified number	
Rmt. Diag. MEAP HTTP	Service Call Log	Approximately 5k bytes	each time an event occurs	Yes
	jam log	Approximately 5k bytes	each time an event occurs	Yes
	alarm log	Approximately 5k bytes	each time an event occurs	Yes
	US > Alerts	Approximately 5k bytes	Whenever the monitored status changes	Yes
	service mode counter	Approximately 110 kbytes	It is transmitted in the following times: • During the transmission test • On Startup • Send once every 16 hours • Send once every 7 days (Counters by mode)	Yes
	Total Resource Counter	Approximately 72 kbytes		Yes
	department counter	In the case of 1000 divisions: Approximately 973 Kbytes		Yes
	part counter	Approximately 103 kbytes		Yes
	Counters by mode	Approximately 128 kbytes		
	Firmware Version	About 5 kbytes		Yes
	Debug Log	Up to 128 Kbytes	It is transmitted in the following four instances: 1. Immediately after successful transmission test 2. Device startup after successful submission test 3. 10 minutes after the exception occurred 4. After the specified 200 logs	

Browser	Sales Organization Tenant Information Tenant identification information (Tenant ID) Tenant Name language code time zone Locale address information* Mail address setting information* Other	Approximately 5 KB	Sales Organization Tenant Information Operation	Yes
	Customer Tenant Info Tenant identification information (Tenant ID) Tenant Name* language code time zone Locale address information* Industry cutoff date Invoice To Information* Contact Information* Other	Approximately 5 KB	During the Customer Tenant information operation	Yes
	User Information User ID Password Email address Name Locale Phone Number Other	Approximately 3 KB	During the user information operation	Yes
	Authorization Information Authorization Code Access Token Refresh Token	Approximately 2 KB	During each API call	
	Administrator Information Admin Name Administrator Contact Information	Approximately 1 KB	During the administrator information operation	Yes
	contract information Contract Number contract period information Contract Category Other	Approximately 1 KB	When operating contract information	Yes
	RDS Information RDS Version RDS ID Communication setting information** date of installation** date of removal** Contract Category** site information** Configuration Information** Administrator Information** Other**	Approximately 2 KB	When operating RDS information	Yes
	Inventory subinventory information inventory subinventory Customer Name address information Other	Approximately 3 KB	During inventory subinventory operations	Yes

	Device Information Service Type** Embedded RDS Settings Device ID Product Name Device Name** date of installation** date of removal** site information** Toner/Ink Management Information** Other**	Approximately 5 KB	When operating device information	Yes
	Managing Installation Data File Server Information	Approximately 2 KB	During file server information operation	
CDCA (HTTPS mode)	Charging Counter Information • Service Mode Counter • Total Resource Counter • Department Counter	In the case of 1,000 divisions: Approximately 973 KB When there is no department registration: Approximately 149 KB	Send once every 12 hours	Yes
	Part Counter Information	Approximately 105 KB	Send once every 16 hours	Yes
	Counter Information by Mode	Approximately 169 KB	Send once every 7 days	
	Service Call Log	Approximately 5 KB	each time an event occurs	Yes
	jam log	Approximately 5 KB	each time an event occurs	Yes
	alarm log	Approximately 5 KB	each time an event occurs	Yes
	US > Alerts	Approximately 5 KB	Whenever the monitored status changes	Yes
	Firmware Version	Approximately 8 KB	Send once every 7 days	Yes
	Environmental information (Temperature/Humidity)	Approximately 20 KB	Send once every 12 hours	
CDCA (SMTP mode)	Charging Counter Information • Service Mode Counter • Total Resource Counter	Approximately 7 KB	Transmission time: specified in CDCA UI (Default 6:00 PM) Transmission interval: specified in CDCA UI (Every 12 hours/every 24 hours)	Yes
	Part Counter Information	Approximately 7 KB	Transmission time: specified in CDCA UI (Default 6:00 PM) Transmission interval: specified in CDCA UI (Every 12 hours/every 24 hours)	Yes
	Counter Information by Mode	Approximately 7 KB	Transmission time: specified in CDCA UI (Default 6:00 PM) Transmission interval: specified in CDCA UI (Every 12 hours/every 24 hours)	
	Service Call Log	Approximately 2 KB	each time an event occurs	Yes
	Jam log	Approximately 2 KB	each time an event occurs	Yes
	Alarm log	Approximately 2 KB	each time an event occurs	Yes
	US > Alerts	Approximately 2 KB	Whenever the monitored status changes	Yes
	Firmware Version	Approximately 7 KB	Transmission time: specified in CDCA UI (Default 6:00 PM) Transmission interval: specified in CDCA UI (Every 12 hours/every 24 hours)	Yes

RDS Agent V2.6 (SMTP)	Service mode counter	Approx.7KB	Every 24 hours	Yes
	Paper Size Counter	Approx.7KB	Every 24 hours	Yes
	Parts counter	Approx.7KB	Every 24 hours	Yes
	Mode Counter	Approx.7KB	Every 24 hours	
	Device Firmware Information	Approx.7KB	Send on the 8th, 18th and 28th of every month	Yes
	Service call log	Approx.1KB	Each time an event occurs	Yes
	Alarm log	Approx.2KB	Follow the specified conditions	Yes
	Jam Log	Approx.1.5KB	Follow the specified conditions	Yes

The following data is not sent to UGW2
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.

6 Policies, Information & implemented Technologies

The assets to be protected on UGW2 are all the data content to be handled (For details, please refer to the detailed materials provided separately by our company.)

UGW2 handles the protection of the all data, assets and information related to the devices and Users that are managed. For further information in this area please refer to the detailed and focused materials which are found on SIMS.

The following section outlines the security policies of UGW2 and the technologies used to apply them. There is a focus around the areas of Confidentiality, Integrity and Availability of the platform.

6.1 Confidentiality

In UGW2, Confidentiality means ensuring access to protected asset information only to authorized users. Confidentiality's security policy is as follows.

- UGW2 manages the users and systems, including devices, that have access so to ensure that only the appropriate users or systems have access to the protected asset information.
- UGW2 creates a reliable channel (HTTPS Encrypted) when communicating over the Internet to ensure that data is not compromised.

Confidentiality in CDCA means that only authorized users are allowed access to the protected assets.

- CDCA controls who can access the protected asset and allows only the appropriate users or systems to access the protected asset information.
- CDCA takes measures to prevent data leakage on the communication path via the browser.

To achieve this Confidentiality security policy, we have implemented the following technologies on UGW2.

6.1.1 Data Encryption in HTTPS Communication

Encrypted HTTPS communication is used between the various software elements and UGW2. Therefore, even if the communication is intercepted on the transmission line, it is not easily decoded. The key lengths of public and symmetric ciphers that can be used in this HTTPS communication are as follows:

- Public key cryptography: RSA 2048
- Common Key Encryption: AES 256 Some clients are allowed to use 3DES EDE, AES 128.

The communication protocols support TLS 1.2 and onwards. Which communication protocol to use depends on user environment and system.

CDCA uses HTTPS to communicate with the browser.

6.1.2 Data Encryption in SMTP Communication

RDS, RDS MEAP and CDCA encrypts device monitoring information when sending mail using SMTP. Therefore, even if the mail data is intercepted on the transmission path, it is not easily decoded. The following encryption technologies are used to encrypt this data:

RDS MEAP (v3.1 and later), CDCA

- Public key cryptography: RSA 2048 bits
- Symmetric cipher: AES 256 bits

RDS MEAP (Up to v3.0), RDS

- Public key cryptography: RSA 2048 bits
- Symmetric cipher: AES 128 bits

6.1.3 Encryption of stored data

The CDCA encrypts and stores the authentication information and the information entered on UGW2 configuration screen in the database. CDCA uses RFC 2898 to generate a key and the Advanced Encryption Standard (256) algorithm to encrypt the data as it is stored in the database.

Sensitive editable data, such as current passwords are encrypted when presented to a user via the Web Browser. For example, if you request to change the password set by the WebUI a string of characters "**********" will be used as the current password so as to protect the current information.

6.1.4 Storing credentials

UGW2 maintains the following credentials in an encrypted state. (Algorithm not disclosed)

- Account credentials to access the portal screen of UGW2
- Credentials for the system (Include Devices) to access UGW2

The password for user authentication contains a salt generated from a random number and a string that is hashed using the SHA -256 algorithm with salt added to the password. The salt above is added to the password entered by the user at login, and the user is authenticated by comparing the hashed string using the SHA -256 algorithm with the stored hashed string.

6.1.5 Authentication and access control

UGW2 authenticates and controls access to protected asset information for the appropriate systems, devices and users.

Accessed	Authentication	Access control
Canon NSO/PartnerPortal	Enter credentials from a web browser via the Internet.	The user of the dealer tenant authenticates the user using the user ID and password. See "user authentication" in chapter 6.1.6 of this document for more information about user authentication. If authentication is successful and the account has function privileges (Read/Write), the information defined by the function is accessible. In addition, the data that an account can access is limited to the data managed by the Canon NSO/Partner to which it belongs and the Canon NSO/Partner under its control. (However, if the tenant to which the account belongs is the direct Canon NSO, the data managed by the indirect Partner cannot be

		accessed.). "Control access to customer data" for information about the controls that enable users of the sales company tenant to access customer data
Customer Portal	Enter credentials from a web browser via the Internet.	A customer tenant user authenticates with a user ID and password. See "user authentication" in chapter 6.1.6 of this document for more information about user authentication. Successful accounts will have access to information determined by the Canon NSO/Partner in advance. Also, data for non-Customer Tenant tenants to which the account belongs will not be accessible unless a reference customer preference is set.
Canon NSO / Partner System API	Through the Internet, the sales company system sends credentials.	If authentication is successful, the Canon NSO/Partner system receives an access token that allows it to send data to UGW2. Canon NSO/Partner systems can send and receive information from various service systems by sending an access token with a request to UGW2.

6.1.6 User authentication

User authentication with a user ID and password is provided.

Authentication Cookies

Upon successful login, it issues an authentication cookie valid within UGW2 domain (ex www-an1.srv.ygles.com). The authentication cookie timeout is as follows:

- Idle timeout: 30 minutes
- General timeout: 1440 minutes (24 hours).

Log

Log information such as the logged-in user's ID, login success/failure, method, and access source. Tenant administrators can retrieve the login log of their tenant.

Password

- The account is locked after 5 consecutive failed login attempts within 12 minutes.
- The account will be unlocked after 12 minutes.
- The password has an expiration date of 90 days. After the expiration date, you must change your password to log in.
- Ability to reset a lost password is implemented. The password can be reset by the user or by the tenant administrator.

Password policy for dealer tenant users

- Character type: All uppercase and lowercase letters and numbers
- Minimum number of characters: 8 characters
- Maximum number of characters: 512 characters
- Available Symbols: ! “# $% & ‘ () * +, -. /:; < > =? @ [] ^ _ `{} | ~
- Duplication with the previous password: Cannot have the same password as the current and previous first password

Password policy for customer portal users

- Character type: using lower case letters and numbers
- Minimum number of characters: 6 characters
- Maximum number of characters: 512 characters
- Available Symbols: ! “# $% & ‘ () * +, -. /:; < > =? @ [] ^ _ `{} | ~
- Duplication with the previous password: Cannot have the same password as the one currently in use

6.1.7 Control access to customer data

In order for users of dealer tenants to have access to customer data, they must register or share customers by web portal in advance. At the time of customer registration, the customer tenant ID and the service license are issued all at once.

6.1.8 Access control by each software

The software authenticates and controls access to protected asset information for the right people.

Accessed	Authentication	Access control
eRDS	Enter a special authentication operation from the device's operation panel	If the authentication is successful, the CE setting screen including the e-RDS setting screen can be operated.
RDS Plugin	Enter authentication information from the RDS console or another PC via a network using a web browser.	Customer IT administrator creates an administrative account and group for RDS. If the authentication succeeds, the user can access a screen determined according to the authority given to the group to which the account belongs.
Rmt. Diag. MEAP SMTP	Enter a special authentication operation from the device's operation panel.	If the device administrator successfully authenticates, Rmt. Diag. MEAP SMTP setting screen can be operated.
CDCA	Enter authentication information from the RDS console or another PC via a network using a web browser.	CE or customer IT administrator sets the password for the administrator account during the CDCA installation. Successful authentication provides access to the CDCA screen. The minimum password length is 8 characters (V1.1 and later).

6.1.9 Authorization

UGW2 provides the authorization server functionality in OAuth 2.0 so that users with the appropriate authority can make the delegation and the associated services can access the delegated scope of protected asset information.

Grant Type

UGW2 common functions support the following Grant Types.

- Authorization Code Grant
- Client Credentials Grant
- urn: ietf: params: oauth: grant-type: jwt-bearer

Token
UGW2 common functions only support bearer tokens as Token Types. The following table shows the expiration dates for various tokens. The randomness of each token follows the UGW2 specification.

Token Type	Expiration date
Authorization Code	600 seconds (10 minutes)
Access Token	3600 seconds (1 hour)
Refresh Token	34.56 million seconds (400 days) *1

Client Authentication
UGW2 performs basic authentication on the Client ID and Client Secret pair for Client Credentials Grant, or key pair authentication for urn: ietf: params: oauth: grant-type: jwt-bearer.
The Client ID is issued with a sufficiently random UUID and tenant ID format to indicate that it is the client.
Client Secret is a 20-character string that is random and contains at least 1 uppercase, lowercase, number, or symbol. Other specifications that treat Client Secret as a password are similar to user passwords. However, unlike user passwords, Client Secret never expires.

Redirect URI
The Redirect URI used by UGW2 common function with OAuth 2.0 is an absolute URI and does not allow fragments. It must also be registered in advance.

The match between the Redirect URI registered at the time of authorization and the Redirect URI of the request is determined by a case-insensitive exact match in the schema and host portion and a case-sensitive exact match in the path portion and beyond.

Scope
UGW2 common functions support only the predefined Scope. Also, an authorization token without Scope cannot be issued.
Check the specifications of the various services of UGW2 for various scopes.

6.1.10 Countermeasures against Malicious Code Attacks

UGW2 has measures in place that helps to prevent malicious user code entry attacks and leakage of user credentials and customer information.

To prevent unauthorized theft of protected asset information managed by UGW2, all interfaces, including UGW2 web screen, Canon NSO/Partner system API's, and HubPort perform server side sanitizing and input validation. This helps to avoid various input attacks typified by SQL Injections.

*1 *The Refresh Token is disabled each* time the Access Token is refreshed, and a new Refresh Token is issued.

CDCA takes measures against malicious user input attacks to prevent the leakage of user credentials and customer information. CDCA web screen utilizes .NET EntityFramework to access the database to avoid various input attacks such as SQL Injection.
In addition, the input values are verified by both JavaScript on the web browser and the web server to prevent unauthorized input by users.

6.2 Integrity

In UGW2, Integrity means ensuring that protected asset information is accurate and free of defects. Our security policy for Integrity is as follows.

- UGW2 ensures that the communication partner is correct when protected asset information is sent and received by communication.
- UGW2 ensures that the protected asset information it stores is correct and complete

Integrity in CDCA means that the data is consistent, correct, and accessible.
CDCA's security policy for this is as follows:

- CDCA verifies that the communication partner is correct when protected asset information is transmitted and received by communication.
- CDCA verifies that the protected asset information it stores is correct and complete.

To achieve this Integrity security policy, we have implemented the following technologies on UGW2.

6.2.1 Verification of received data

UGW2 verifies that the received protected asset information is correct. Verification items are as follows.

- Verifying Source Information
  UGW2 verifies that the device information in the received data matches the device registered on UGW2. It does not receive information from devices that are not registered with UGW2.

- Check the contents of the received data
  UGW2 verifies that the format is correct and that the required information is available. If the received data does not conform to the correct format, the received data is discarded.

6.2.2 Server authentication

Various types of software send information only to UGW2. The software uses Digisert's certificate for server authentication when communicating HTTPS with UGW2. In addition, the software uses a unique verification process for the destination URL to identify the server and control the data destination.

- Root Certification authority: VeriSign Class 3 Public Primary Certification Authority – G5 or DigiCert Global Root G2
- Server certificate signing algorithm: SHA -256 with RSA

Data handled by CDCA is stored in the database by encrypting the data and the common key itself with the common key as described in "Data encryption". In addition, we recommend SSL as the communication path through the Web browser, and the communication contents of the Web service are encrypted using the public key.

6.2.3 Measures against unauthorized acces

UGW2 stops unnecessary network services and closes unnecessary ports by firewalls to minimize third-party risk in intrusion. This limits the intrusion path through the network. All network access is logged in the access log. UGW2 maintains an access log in the unlikely event of an unauthorized intrusion to the system.

6.2.4 Verifying Monitoring Devices

RDS verifies that the device has not been replaced in order to obtain correct monitored device information. Agent software with eMaintenance obtains device identification information (Serial number or Mac address) and verifies that the device has not been replaced before retrieving information from the device over the network.

6.2.5 Countermeasures against Malicious Code Attacks

To prevent unauthorized rewriting of protected asset information, UGW2 prevents malicious user code entry attacks. The API provided by UGW2 performs processing to avoid input attacks by SQL Injection and cross-site request forgery. This prevents the device monitoring information stored in the compatible IF from being tampered with.

To prevent unauthorized rewriting of device management information, CDCA takes measures against malicious user input attacks. On the CDCA Web screen, to avoid various input attacks such as SQL Injection and session hijacking (*), we take measures such as using the form authentication function of .NET and changing the session ID at each log in.

(*) Session hijacking: An attack in which a series of communications (Session) between a pair of devices on a network is intercepted, and data is stolen or manipulated from one device by pretending to be the other.

6.3 Availability

In UGW2 and CDCA, Availability means that authorized users have access to protected asset information when they need it. Our security policy for Availability is as follow.

- UGW2 can notify and access the system when users need it.
- CDCA can access the system when an authorized user is needed.

To achieve this Availability security policy, we have implemented the following technologies on UGW2.

6.3.1 Self-monitoring of processes

RDS is a system that monitors a device continuously for 24 hours, 365 days, without interruption. To achieve this, each device has its own process monitoring function. In the unlikely event that a catastrophic failure occurs, and the processing process fails, the self-recovery feature allows monitoring to continue.

Monitoring device	Time until abnormality detection	Response - error detection
RDS Plug-in	Up to 3 minutes	Restart Process

6.3.2 Measures to maintain high Availability

To ensure business continuity among Canon NSO/Partner customers, and business partners, UGW2 implements the following measures to maintain high availability. Because UGW2 utilizes managed services from cloud computing providers, the software and database execution environments that make up UGW2 have high availability as shown below.

- The systems and databases are managed and operated to ensure a certain level of performance. As traffic grows, it can handle more traffic while automatically scaling and maintaining performance.
- The systems and databases are automatically requested and stored in multiple data centres and are designed and operated to prevent data loss and service downtime in the event of a system failure.

For processes that are not using managed services, failover function is implemented. All servers that make up the system are redundancy so that even if one server fails, the other server is activated and takes over automatically. This function provides an environment where users who have accessed UGW2 can access the information when they want to use it.

CDCA provides authentication and access control for logged-in users, allowing them to access the system at any time according to their privileges.

6.3.3 Countermeasures against Malicious Code Attacks

To provide a stable system, UGW2 avoids code entry attacks from malicious users. UGW2 provides an API that performs server-side sanitizing to avoid various input attacks such as cross-site scripting. This protects the system from attacks in which the user accessing.

UGW2 is forced to communicate with an unintended website or cannot obtain the information needed by the user.

As mentioned above, CDCA utilizes .NET API for sanitizing and validates input values to avoid various input attacks such as SQL Injection.
As a result, we are taking countermeasures against attacks in which users who access CDCA are forced to communicate with unintended websites and cannot obtain necessary information.

6.3.4 Response to illegal mail in mail server

To provide a stable system, UGW2 introduces spam-antivirus filters to eliminate malicious e-mail such as virus and spam. This eliminates malicious mail before the service begins the mail capture process.

6.4 Penetration test

In order to verify the above security measures, penetration test is performed regularly by a third party. The penetration test will be implemented once a year periodically.

6.5 Certifications

Please refer to the link below for the authentication that the data center used by this service has obtained.
https://aws.amazon.com/compliance/programs/

7 Glossary

Acronym	Name
ACM	Application Configuration Management
AES	Advanced Encryption Standard
API	Application Programming Interface
ATP	Access Token Provider
CDCA	Canon Data Collection Agent
EDE	Encrypt-decrypt-encrypt
eM	eMaintenance
eRDS	Embedded Remote Diagnostic System
HTTPS	Hypertext Transfer Protocol Secure
MDAS	MEAP-integrated Delivery Assistant Service
NSO	National Sales Organisation
RDS	Remote Diagnostic System
Rmt. Diag.	Remote Diagnostic
SMTP	Simple Mail Transfer Protocol
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SRA	Rivest Shamir Adleman
SSL	Secure Sockets Layer
UGW2	Universal Gateway 2
3DEA	Triple Data Encryption Algorithm
UI	User Interface
URI	Uniform Resource Identifier