Canon

imageWARE
Remote

Technology/Security Whitepaper

Version 2.5.1

IMPORTANT NOTICE

This document was created based on the latest technical information available at the time of its publishing. This information is subject to change without notice.

Table of Contents:

1. Overview

About this Whitepaper

This document is intended for IT administrators who would like to study the security features, system architecture and network impact of Canon U.S.A.'s imageWARE Remote service.

This document is NOT confidential.

About imageWARE Remote

imageWARE Remote is a service developed by Canon Inc. that is being made available to Canon U.S.A.'s dealers and authorized service providers, enabling them to provide better service to their customers.

Both services use the same underlying technology - either eRDS (**e**mbedded **R**emote **D**iagnostic **S**ystem), or RDS Plug-in (imageWARE Enterprise Management Console **R**emote **D**iagnostic **S**ystem Plug-in) to capture device information and transmit such information to a server managed by Canon Inc. via the Internet, where it is accessible by the service provider via a web interface (the Canon Inc. **U**niversal **G**ate**w**ay or "**UGW"**).

The RDS Plug-in solution requires imageWARE Enterprise Management Console to be installed as a base operating platform and this requires a computer to host the software.

The eRDS solution on the other hand does not require any additional hardware or software since the solution is already embedded within the imageRUNNER device.

Once activated, eRDS/RDS Plug-in will submit both meter readings and service information to the UGW.

Supported Devices

RDS Plug-in

The majority of devices with a standard management information base ("MIB") are supported. Please refer to the list of support models on Canon's eSupport website. Third party devices are supported through the standard MIB.

eRDS

Most All Canon imageRUNNER, imageRUNNER ADVANCE devices and present day imageCLASS, imagePRESS (except 6000), and imagePROGRAF devices.

2. Embedded RDS Overview

What is eRDS?

Most of Canon's devices ship equipped with embedded Remote Diagnostic System (eRDS) capability.

eRDS is a monitoring technology that runs inside of the Canon devices mentioned above that allows it to connect directly to the Canon Universal Gateway Server (UGW) for the purpose of collecting counter, jam, error, and alarm data in order to improve the level of customer support and service that Canon service providers can offer to their customers. eRDS provides the following benefits:

Automatic Meter Reading

eRDS captures and provides meter data automatically via the network to the UGW, reducing the need for manual collection of meter readings by the customer and reporting them to the service provider for billing purpose.

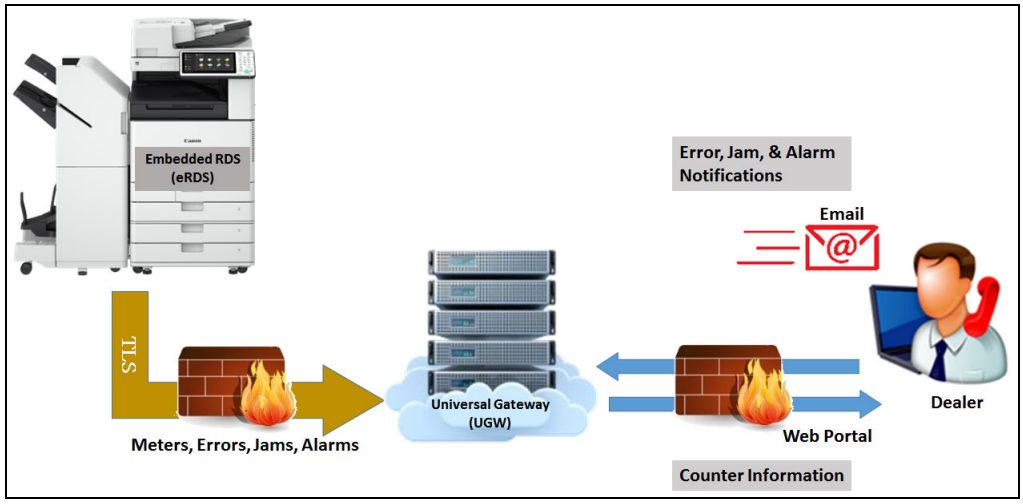
Enhanced Service Offering

Automatic error, jam, and alarm notifications can be used to improve service provider's response time.

Usage Statistics, Parts Lifetime and Consumables Management

Service providers have access to information on parts usage of customers' registered eRDS capable Canon devices. This can be used to offer pre-emptive service to the customer, before consumable and durable parts reach the end of their expected life cycle. In addition, information about toner usage allows the service provider to make suggestions about re-ordering or stock quantities.

eRDS Architecture



This simplified figure shows the architecture of the eRDS system.

The eRDS system on the device pushes the data out via secure TLS connection to the UGW server.

Once the data is on the UGW server:

- Meter readings are available on the UGW server to view or download by the service provider.
- Error/jam/alarm notifications can be sent directly to the service provider by e-mail upon occurrence.
- The service provider can also log onto UGW to obtain information on any error/jam/alarm notification.

3. RDS Plug-in Overview

What is the RDS Plug-in?

The RDS Plug-in is an alternative solution to eRDS for users that need to support legacy devices as well as third party, non-Canon, devices. However, the use of RDS Plug-in requires the deployment of a computer to host the imageWARE Enterprise Management Console (iWEMC).

The RDS Plug-in communicates with user selected devices from the iWEMC device list to collect counter, jam, error, and alarm data. As described later, the RDS Plug-in will push the collected data to the UGW server at specified intervals.

Similar to the eRDS version, the RDS Plug-in connects to the UGW for the purpose of collecting counter, jam, error, and alarm data in order to improve the level of customer support and service that Canon service providers can offer to their customers. The RDS Plug-in provides the same benefits as eRDS, as listed below:

Automatic Meter Reading

The RDS Plug-in captures and provides meter data automatically via the network to the UGW, reducing the need for manual collection of meter readings by the customer and reporting them to the service provider for billing purpose.

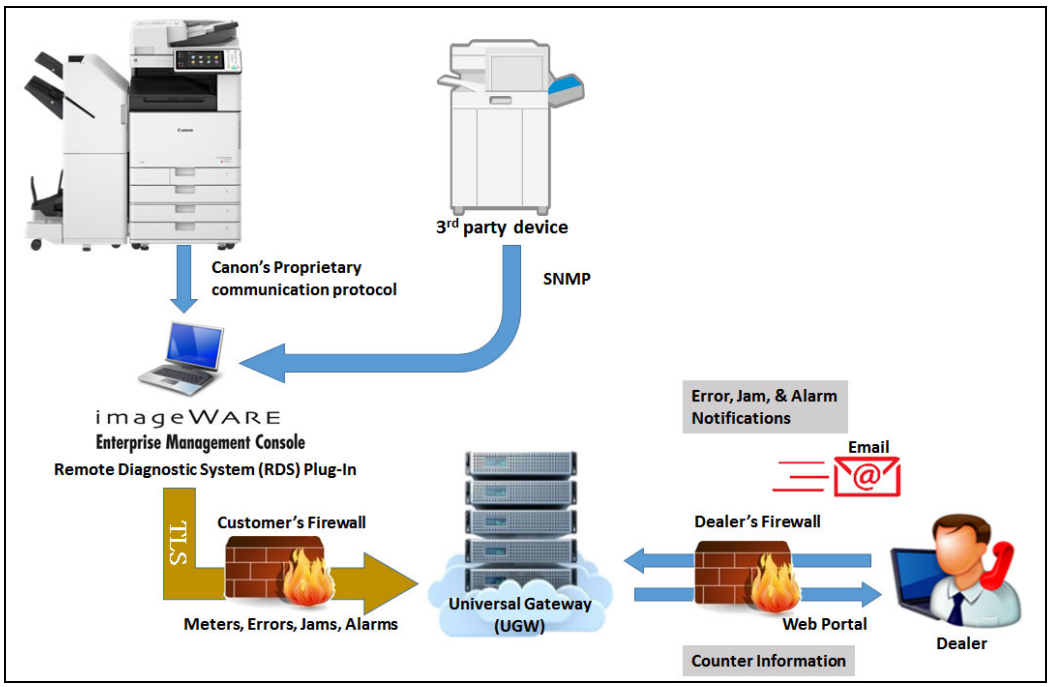
Enhanced Service Offering

Automatic error, jam, and alarm notifications can be used to improve service provider's response time.

Usage Statistics, Parts Lifetime and Consumables Management

Service providers have access to information on parts usage of customers' registered eRDS capable Canon devices. This can be used to offer pre-emptive service to the customer, before consumable and durable parts reach the end of their expected life cycle. In addition, information about toner usage allows the service provider to make suggestions about re-ordering or stock quantities.

RDS Plug-in Architecture



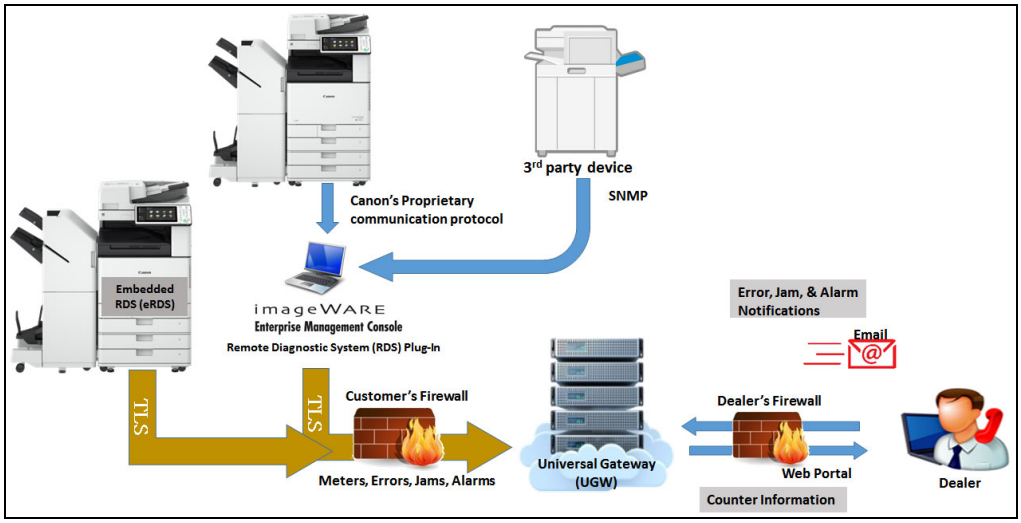
This simplified figure shows the architecture of the RDS Plug-in system.

The RDS Plug-in pulls data from Canon devices via a Canon specific proprietary protocol, as described later in the communication protocol chart. For third party devices, the RDS Plug-in pulls data via the standard MIB by Simple Network Management Protocol ("SNMP").
The RDS Plug-in pushes the collected data out via secure TLS connection to the UGW server.

Once the data is on the UGW server:

- Meter readings are available on the UGW server for download by the service provider.
- Error/jam/alarm notifications can be sent directly to the service provider by e-mail upon occurrence.
- The service provider can also log onto UGW to obtain information on any error/jam/alarm notification.

eRDS & RDS Plug-in combined Architectures



This simplified figure shows the architecture of the eRDS system and of the RDS Plug-in system combined.

4. eRDS Network Security

LAN

Communication Target and Protocol

The eRDS communicates only with the UGW and is unable to communicate with other devices that are connected to a customer's Local Area Network.

Communication between UGW Server and eRDS Devices

Communication Target

The eRDS enabled Canon devices communicates only with the UGW when sending device information. The authentication method is described later.

Communication Protocol

The eRDS enabled Canon devices communicates with the UGW by using the HTTPS protocol. The eRDS enabled Canon devices acts as the "Client", and will never become a Web server for the purposes of eRDS communication.
Please note that some eRDS enabled Canon devices may act as a Web server for other non-eRDS related features.

Data to be collected and forwarded

The data to be collected by eRDS and forwarded to UGW is shown in Table 1. The eRDS enabled Canon device sends the data shown in Table 1 to the UGW at the specified timing.
In the "regular counter transmission", the maximum size of the transmitted data package is about 250 KB. This transmission occurs only once every 16 hours.

[Table 1]

Data to be sent*	Description	Timing to send	Amount of data
Error data	Includes the error code, error subcode, date of occurrence, total counter at occurrence, paper feeding slot, and paper size.	When an error occurs	5 KB
Jam data	Includes the jam code, date of occurrence, total counter at occurrence, paper feeding slot, and paper size.	When a jam occurs	5 KB
Alarm data	Includes the alarm level, alarm code, alarm subcode, date of occurrence, and total counter at	When an alarm occurs	5 KB

	occurrence.		
Status data	The data when a status change occurs.	When status change occurs	5 KB
Billing counter data	The counter data typically used for billing, such as Total, Copy, Print, B/W, and Color.	Every 16 hours	Approx. 450 KB (Billing counter: 110 KB, Detailed counter: 72 KB, Parts counter: 103 KB, Mode counter: 164 KB)
Detailed Counter data	The detailed counter data for each paper size such as Total, B/W, and Color.		
Parts counter data	The counter data indicating the amount of usage by part. The number of parts varies by model.		
Mode Counter data	The counter data by operation mode. The number of modes varies by model.	Every 25 days	
ROM version data	The ROM version data of Main, Scan, Print, Feeder, Finisher, Fax, PDL, and Tray.	Every 7 days	Approx. 5 KB
Debug log data	The log data output by an application for analyzing a malfunction.	When the size of the debug log reaches a specified size.(512KB)	145 KB
Environment log data	Environment log data of the device (e.g. temperature, humidity)	The data is sent once every 12 hours.	Approx. 6 KB
Service mode menu information	All Adjust values that have been set by a technician during the initial install and all Display values which are measured values related to image formation.	Only at the time of the first communication test.	Approx. 435 KB
	All Display values which are measured values related to image formation.	When specific alarms or errors occur.	Approx. 127 KB

Service Browser Information	Status of Service Browser and Option Browser.	When clicking the button to enable the browser in the service mode menu.	Approx. 3 KB
Settings information inquiry	Inquiry for the settings information flag status of the device configured for a remote update by the Contents Delivery System.	Once every 12 hours	Approx. 2 KB
S.M.A.R.T. data	Self-diagnosis report, as provided the hard disk as defined by the S.M.A.R.T.(Self-Monitoring Analysis and Reporting Technology) standard	Once every 30 days	Approx. 5 KB

The transmission start time is determined by UGW based on the return value of the communication test.

* Not all features are available for all eRDS enabled Canon devices.

Data Encryption

From eRDS to the UGW server, data is encrypted at the transport layer though a TLS connection, which is typically used to secure connections over the Internet. Therefore, the data does not need to be encrypted at the application layer.
The key length used in the HTTPS communications are as follows:

Public Key length: RSA 2048bit
Symmetric Key length: AES 128bit (imageRUNNER ADVANCE 1st Generation)
: AES 256 bit ((eRDS released after 4th Qtr. of 2012) imageRUNNER ADVANCE 2nd Generation or later)

Secure Hash Algorithm Server Certificate:

- SHA2
- SHA1 (SHA1 is used only with the device that supports the communications in which a server certificate is used. However, the SHA1 server certificate will be discontinued by the end of 2019.)
- See last page Supported Device List for details.

eRDS activation

eRDS must be integrated in the main unit firmware of the Canon device. In order to enable eRDS on most Canon devices, the setting must be activated from service mode, therefore a user cannot accidentally activate this option. Starting with Canon devices such as, 3rd Generation imageRUNNER ADVANCE and imagePROGRAF TX series, eRDS is enabled by default and can be activated in User Mode.

Authentication Procedures

Server Authentication

The UGW uses TLS Authentication together with application authentication. The eRDS function will not transmit information to servers other than the UGW using these methods.

1) TLS Authentication

TLS Authentication is performed according to the following procedures. Please note the following steps describe the TLS protocol and are not specific to Canon's eRDS technology.

- "Root Certificates" published by Verisign are installed in an imageRUNNER when it ships from the factory.
- When the eRDS enabled Canon device starts communicating, eRDS will receive the "Server Certificate" published by Verisign from the UGW by HTTPS.
- The eRDS device compares the "Server Certificates" with the "Root Certificates".
- If these certificates match, the eRDS device successfully authenticates the other communicating party as the UGW server.
- The encryption method is negotiated using HTTPS, afterwards,

HTTPS communications begin and the data is encrypted

2) Application level authentication
Application-level authentication further secures the eRDS communication between the Canon device and the UGW.
The URL of the UGW Server is pre-populated into the firmware of the eRDS enabled Canon device.
Service personnel can change this URL. However, the firmware will only attempt a transmission if the domain name of the URL is in the UGW's DNS domain.
In the event that a user changes the URL to something outside of the UGW DNS domain, the eRDS enabled Canon device will not transmit any data.

Client Authentication
This section describes the client authentication used by the UGW.

1) Client authentication by TLS (OSI Layer 4 to 5)
Client authentication by TLS is not performed.

2) Client authentication by application (OSI Layer 7)
The UGW will receive information only from devices whose serial numbers have been registered on the UGW by the service provider. Prior to registration on the Universal Gateway, a communication test needs to be performed on the eRDS enabled Canon device, establishing communication between the UGW and the device.
Reverse engineering is impossible because of TLS encryption and the use of the Canon proprietary Simple Object Access Protocol ("SOAP") schema communication protocol. Therefore, a rogue client cannot be developed.

Content Delivery System Linkage

In order for UGW to use the firmware distribution command function* of the Content Delivery System, devices to be updated must be enabled on the device.
Using the UGW firmware distribution command function, set an update settings information flag to devices (eRDS) to be updated.
eRDS regularly checks with UGW for the update settings information flag.
Finding the update settings information flag, eRDS notifies the CDS Updater of the device that there is an update command. The CDS Updater, upon receiving an update command, starts the update communication with the Content Delivery System.
* For more information on security of the function to invoke an application (firmware distribution command function) on the CDS management server

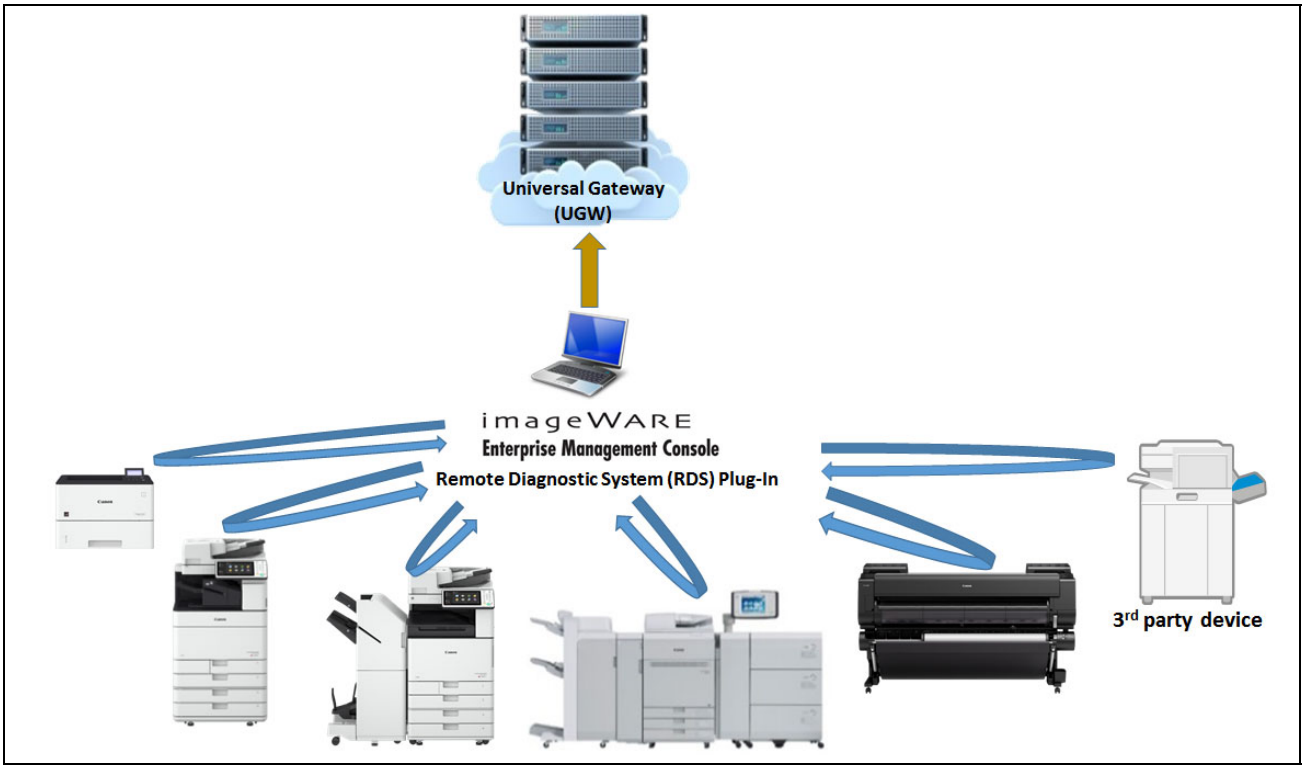
from the UGW Web Portal, refer to the "Content Delivery System Security White Paper".

5. RDS Plug-in Network Security

RDS Plug-in Overview

The RDS Plug-in (imageWARE Enterprise Management Console + RDS Plug-in) communication functions can be divided into two major components:

1) Retrieval of data from the device
2) Send the retrieved device data to the UGW server



Destination identification

When retrieving device data, the RDS Plug-in will only communicate with the registered device. The RDS Plug-in will not communicate with any other device on the LAN. When sending the retrieved device data, the RDS Plug-in communicates only with the UGW server registered in the RDS Plug-in configuration settings. The IT administrator for iWEMC can regulate access to the configuration settings through user privileges.

Communication protocol between device and RDS Plug-in (device to RDS Plug-in)

Table 2 lists the communication protocols and port numbers used to facilitate the data retrieval from device to RDS Plug-in. As shown in the table, the communication protocols are proprietary to Canon except for SNMP. All of the listed protocols are used for managing devices. SNMP is also an RFC-defined protocol for managing network devices. These protocols are not capable of accessing or retrieving image data or content information such as Address Book data.

[Table 2]

Protocol	Port Number	Client/Server
Device communication, proprietary to Canon	TCP/47546 (b9ba)	Client
Device communication, proprietary to Canon	UDP/47545 (b9b9)	Client
Device communication, proprietary to Canon	TCP/9007 (232f)	Client
SNMP	UDP/161	Client
HTTPS	TCP/443	Client
HTTPS	TCP/443	Server
SLP	UDP/427	Client
SMTP	TCP/25	Server
SMTP AUTH	TCP/587	Server

Communication protocol between the RDS Plug-in and the UGW

The RDS Plug-in communicates with UGW using HTTPS and always works as a requester, never as a Web server.

Timing and data size chart for data retrieval from device to RDS Plug-in

The table below lists the timing and the size of the data retrieved from a device by the RDS Plug-in.

[Table 3]

	Retrieval of the device data
Polling packets	Frequency: Every time an event occurs Amount of data: 0.2 KB/device
Counter-related data	Frequency: once per hour or less often Amount of data: 15 KB/device (with 1000 departments registered 712 KB)

Quality-related data	Frequency: Every time an event occurs, as determined by polling packets (see above) Amount of data: 0.7 KB
Firmware version data	Frequency: once every 6 hours Amount of data: approx. 3 KB/device
Environment data	Frequency: once every 6 hours Amount of data: 6 KB/device

Timing and data size chart for transmitting data from RDS Plug-in to UGW

Table 4 lists the device data that will be sent from the RDS Plug-in to the UGW.

[Table 4]

Data type *	Description	Transmission schedule	Amount of data
Error data	Includes the error code, error subcode, date of occurrence, total counter at occurrence, paper feeding slot, and paper size.	The data is sent when the RDS Plug-in detects a service call error and obtains the error log.	Approx. 5 KB
Jam data	Includes the jam code, date of occurrence, total counter at occurrence, paper feeding slot, and paper size.	The data is sent when the RDS Plug-in detects a jam and obtains the jam log.	Approx. 5 KB
Alarm data	Includes the alarm level, alarm code, alarm subcode, date of occurrence, and total counter at occurrence.	The RDS Plug-in detects an Alarm Level 2 or Level 3 and obtains the alarm log. Also, when the RDS Plug-in detects inconsistency in IP-MAC, it creates an alarm log by setting its level to 3 and sends a false alarm.	Approx. 5 KB
Status data	Device status change event	When status change occurs.	Approx. 5 KB
Billing counter data	The counter data used for billing that includes the detailed counter data such as the total counter for each paper size.	The data is sent once every 12 hours.	Approx. 149 with No departments 973 KB with 1000 departments (min/max) (Measured on iR-ADV C5051)
Parts counter data	The counter data indicating the amount of usage by part. The number of parts varies by model.	Once every 16 hours	Approx. 105 KB (Measured on iR-ADV C5051)
Mode Counter data	The counter data by operation mode. The number of modes varies by model.	The data is sent once every 7 days	Approx. 169 KB (Measured on iR-ADV C5051)
ROM version data	The ROM version data of Main, Scan, Print, Feeder, Finisher, Fax, PDL, and Tray.	The data is sent once every 7 days	Approx. 8 KB (Measured on iR-ADV C5051)

Debug log data	The log data output by an application for analyzing a malfunction.	When the number of log lines reaches a specified number (512lines)	Approx. 245 KB (Measured on iR-ADV C5051)
Environment log data	Environment log data of the device (e.g. temperature, humidity)	The data is sent once every 12 hours.	Approx. 20 KB (Measured on iR-ADV C5051)
Service mode menu data	All adjust values which are various set values and all Display values which are measured values related to image formation.	When registering a device to RDS	Approx. 150 KB
	All adjust values which are various set values.	When changing set value of the service mode menu	Approx. 100 KB
	All Display values which are measured values related to image formation.	When specific alarms or errors occur.	Approx. 50 KB
Service Browser data	Status of Service Browser and Option Browser.	When clicking the button to enable the browser in the service mode menu.	Approx. 3 KB
S.M.A.R.T. data	Self-diagnosis report, as provided the hard disk as defined by the S.M.A.R.T.(Self-Monitoring Analysis and Reporting Technology) standard	Once every 30 days	Approx.4.2 KB

* Not all features are available for all RDS plug-in enabled Canon devices. The standard MIB models will send the “Billing Counter” and “Status Information” only.

Data Encryption

Between the RDS Plug-in and UGW server, data is encrypted at the transport layer though a TLS connection, which is typically used to secure connections over the Internet. Therefore, the data need not be encrypted at the application layer.
The key length used in the HTTPS communications are as follows:

Public Key length: RSA 2048bit
Symmetric Key length: AES 256 bit (RDS Plug-in v3.1 or later)

In the connection between the device and RDS Plug-in, data is not encrypted. Since the communication protocol and format utilizes a closed binary data/proprietary format, even in the event that your local network has been wiretapped, the data will not be passed in clear text.

The data managed internally within the RDS Plug-in utilizes DBMS. Therefore, even if a user can somehow gain access to the Windows files, access to the data stored by DBMS will not be granted unless the user has access privileges.

Secure Hash Algorithm Server Certificate:

- SHA2
- SHA1 (SHA1 is used only with the device that supports the communications in which a server certificate is used. However, the SHA1 server certificate will be discontinued by the end of 2019.)
- See last page Supported Device List for details.

RDS Plug-in failure recovery measures

In the event that there is a physical failure on the computer hosting iWEMC RDS Plug-in, the settings for the RDS Plug-in can be restored with the XML configuration file. Therefore, it is important for the server administrator to maintain a backup of the configuration file.
However, the jam log and alarm log kept by the RDS Plug-in are not included in this configuration file and may be lost.

Authentication Procedures

Server Authentication

The UGW utilizes TLS authentication together with application authentication. The RDS Plug-in will only transmit data to the UGW server using these methods.

1) TLS Authentication

TLS Authentication is performed according to the following procedures. Please note the following steps describe the TLS protocol and are not specific to Canon technology.

- "Root Certificates" published by Verisign are packaged with the RDS Plug-in. After installing the RDS Plug-in, the certificate must be registered on the UI of the RDS Plug-in.
- When the RDS Plug-in starts communicating, it receives the "Server Certificate" published by Verisign from the UGW by HTTPS.
- The RDS Plug-in compares the "Server Certificates" with the "Root Certificates".
- If these certificates match, the RDS Plug-in successfully authenticates the other communicating party as the UGW server.
- The encryption method is negotiated using HTTPS, afterwards, HTTPS communications begin and the data is encrypted

2) Application level authentication

On the application level, the UGW server will be authenticated by the RDS Plug-in. Communication will proceed only when the UGW has been successfully authenticated. This further ensures that the RDS Plug-in will not communicate with any destination other than the UGW.

6. General Considerations

Customer Requirements

Network Connection

In order for the eRDS and/or the RDS Plug-in to work effectively, a continuous network connection is necessary. If the network connection is lost temporarily or permanently, the functions of imageWARE Remote (Meter Reading and Service Monitor) will not be available, resulting in the delayed reporting of meter reads. Additionally, service notifications will not be transmitted in a timely manner, jeopardizing the benefits of the Service Monitor feature.

Network Traffic

Although the data packages sent from the eRDS enabled Canon devices and/or the RDS Plug-in are very small, IT administrators will most likely note increased network traffic due to the communications between the eRDS/RDS Plug-in unit and the UGW. For the RDS Plug-in there will also be an increase in network traffic between the RDS Plug-in and the devices.

In addition, the hard coded URL of the UGW may become the most frequently addressed URL within the organization. This is due to the scheduled and event-related communications between the eRDS/RDS Plug-in and the Canon UGW server. To ensure uninterrupted performance of the imageWARE Remote services, it is important that this URL remains unchanged and will not be blocked.

Power

Power outages or device shutdowns by employees will result in an interruption of data transmission. No meter information can be transmitted to the UGW if the device is off. Upon return of power, the eRDS will start communicating with the UGW server again.

Image Data

The eRDS/RDS Plug-in is not capable of sending or receiving image data. The types of data collected and submitted by the eRDS/RDS Plug-in function are described in “Network Security”, Table 1 and Table 4.

Failures

After network failures or power outages, eRDS will automatically start communicating with the Canon UGW server once the situation is corrected. Execution of another “communication test” is not required.

Data Storage Time

UGW

Meter data will be stored in the Universal Gateway database for 12 months, however only the most recent meter data is accessible for download from the Web Portal by the service provider.
Service information/statistics are currently stored for 6 months. This storage time may be modified in the future.

RDS Plug-in

The RDS Plug-in does not retain any data other than what is necessary for the next scheduled data transmission to UGW.

Supported Device List

This table is based on available information at time of release of this document. Please refer to latest information on eSupport for up-to-date details.

Algorithm	*Supported imageRUNNERs*	
SHA1	Legacy iR (all)	Gen1 iR ADV (except iR ADV 4051 Series)
SHA2	Gen 2 iR ADV (all)	Gen3 iR ADV (all)
SHA2	iR ADV C9075, iR ADV C5051, iR ADV 6075, iR ADV 8105 (available mid 2018)	

Algorithm	*Supported imagePRESS and PRISMAsync*	
SHA1	imagePRESS C1	
SHA2	imagePRESS All (except iPR C1)	varioPRINT 135 and 140 Series

Algorithm	*Supported imageRUNNER LBP*
SHA1	CiR LBP5360, CiR LBP5960, CiR LBP5970/5975, iR LBP3460, iR LBP3560
SHA2	CiR LBP5280, CiR LBP5480, iR LBP3480, iR LBP3580, CiR LBP5460*

Algorithm	*Supported imageCLASS and other*
SHA1	Color imageCLASS LBP7110Cw, Color imageCLASS MF9150c, imageCLASS LBP6650dn
SHA2	All imageCLASS series not listed above

* Requires G5 Certificate be installed, can be downloaded from Symantec web site

No Laser Class Series SHA2 support

7. Operation Facility Measures

The operation facility is certified internet Data Center (iDC):

Certified Standard

ISO27001
ISO20000
ISO9001
ISO14001
Privacy mark

