

Canon

i m a g e W A R E
Remote

Technology/Security Whitepaper

Version 2.0

November 2010

IMPORTANT NOTICE

This document was created based on the latest technical information available as of July 2010. This information is subject to change without notice.

Table of Contents:

1. Overview

About this Whitepaper	4
About imageWARE Remote	4
Supported Devices	5

2. Embedded RDS Overview

What is eRDS?	5
eRDS Architecture.....	6

3. RDS Plug-in Overview

What is RDS Plug-in?	7
RDS Plug-in Architecture.....	8

4. eRDS Network Security

LAN	9
Communication between UGW Server and eRDS Devices	9
Data Encryption	12
eRDS activation	12
Authentication Procedures	12

5. RDS Plug-in Network Security

RDS Plug-in Overview	15
Destination identification	16
Communication protocol between device and RDS (device to RDS)	16
Communication protocol between the RDS and the UGW	16
Timing and data size chart for data retrieval from device to RDS	17
Timing and data size chart for transmitting data from RDS to UGW	17
Data encryption	19
RDS failure recovery measures	20
Authentication Procedures	20

6. General Considerations

Customer Requirements	21
Image Data	21
Failures	21
Data Storage Time.....	22

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 service providers, enabling them to provide better service to their customers.

imageWARE Remote consists of two components: imageWARE Remote Meter Reading (collects meter reads automatically from enabled imageRUNNER devices) and imageWARE Remote Service Monitor (provides information about device status, error notifications and statistics about parts lifetime and consumables). Both services use the same underlying technology - either eRDS (**e**mb**e**ded **R**emote **D**ia**g**nostic **S**ystem), or RDS Plug-in (imageWARE Enterprise Management Console **R**emote **D**ia**g**nostic **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**ateway or "**U**GW").

The RDS Plug-in solution requires imageWARE Enterprise Management Console to be installed as a base operating platform and this requires a server 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. However, depending on the business model selected by the Service Provider, the UGW will allow for access of meter reading only (imageWARE Remote Meter Reading) or both meter reading and service information will be made available (imageWARE Remote Service Monitor).

***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

All Canon imageRUNNER devices, from the 70 Series and later, are supported. This includes the entire imageRUNNER ADVANCE line. The embedded RDS technology is already available on these devices and needs to be activated in service mode to start working. At the time of imageWARE Remote launch, Canon imageRUNNER 30 Series devices will only support eRDS if they are equipped with a Canon Multi-PDL printer board.

For a list of supported models, please refer to Canon’s eSupport website or contact your Canon representative directly to obtain the most current information regarding imageWARE Remote.

2. Embedded RDS Overview

What is eRDS? Canon’s imageRUNNER series devices ship equipped with embedded Remote Diagnostic System (eRDS) capability.

eRDS is a technology that allows the imageRUNNER devices to connect directly to the 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

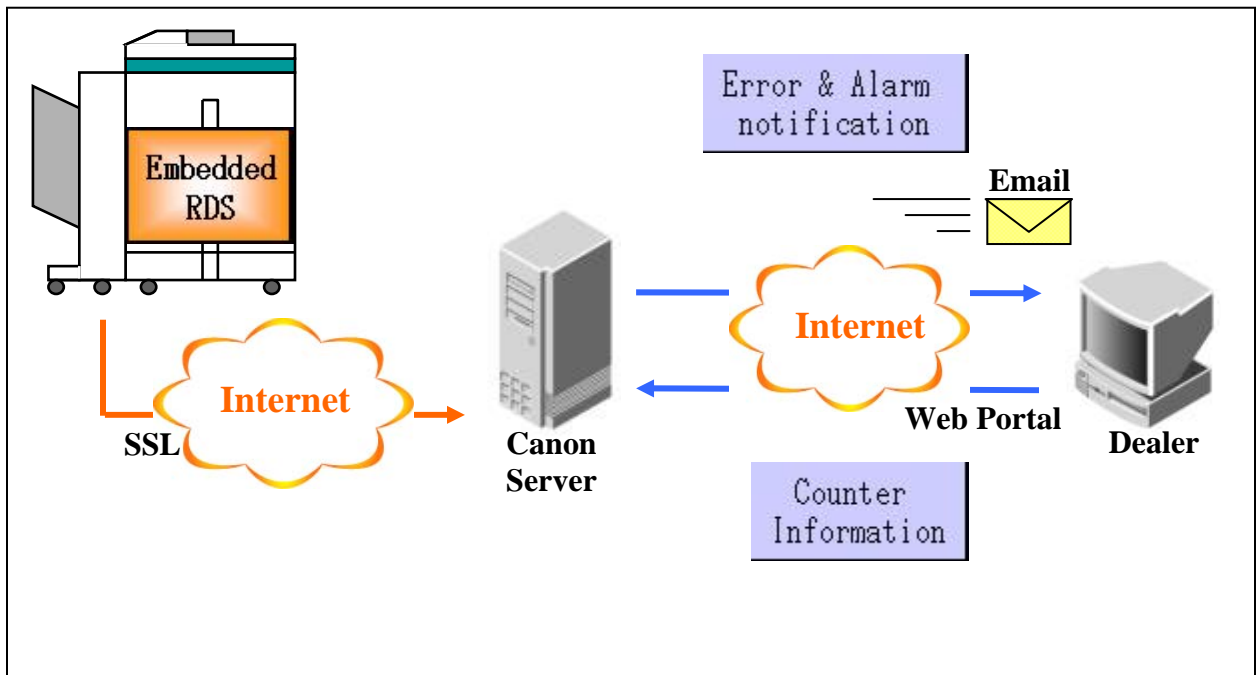
Automatic error, jam, and alarm notifications can be used to improve service provider’s response time.

Usage Statistics, Parts Lifetime and Consumables Management

As part of the imageWARE Remote Service Monitor feature, service providers have access to information on parts usage of customers’ registered imageRUNNER 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 SSL connection to the UGW server (push process)

Once the data is on the UGW server:

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

3. RDS Plug-in Overview

What is RDS Plug-in? 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 server to host the imageWARE Enterprise Management Console (iWEMC).

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

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.

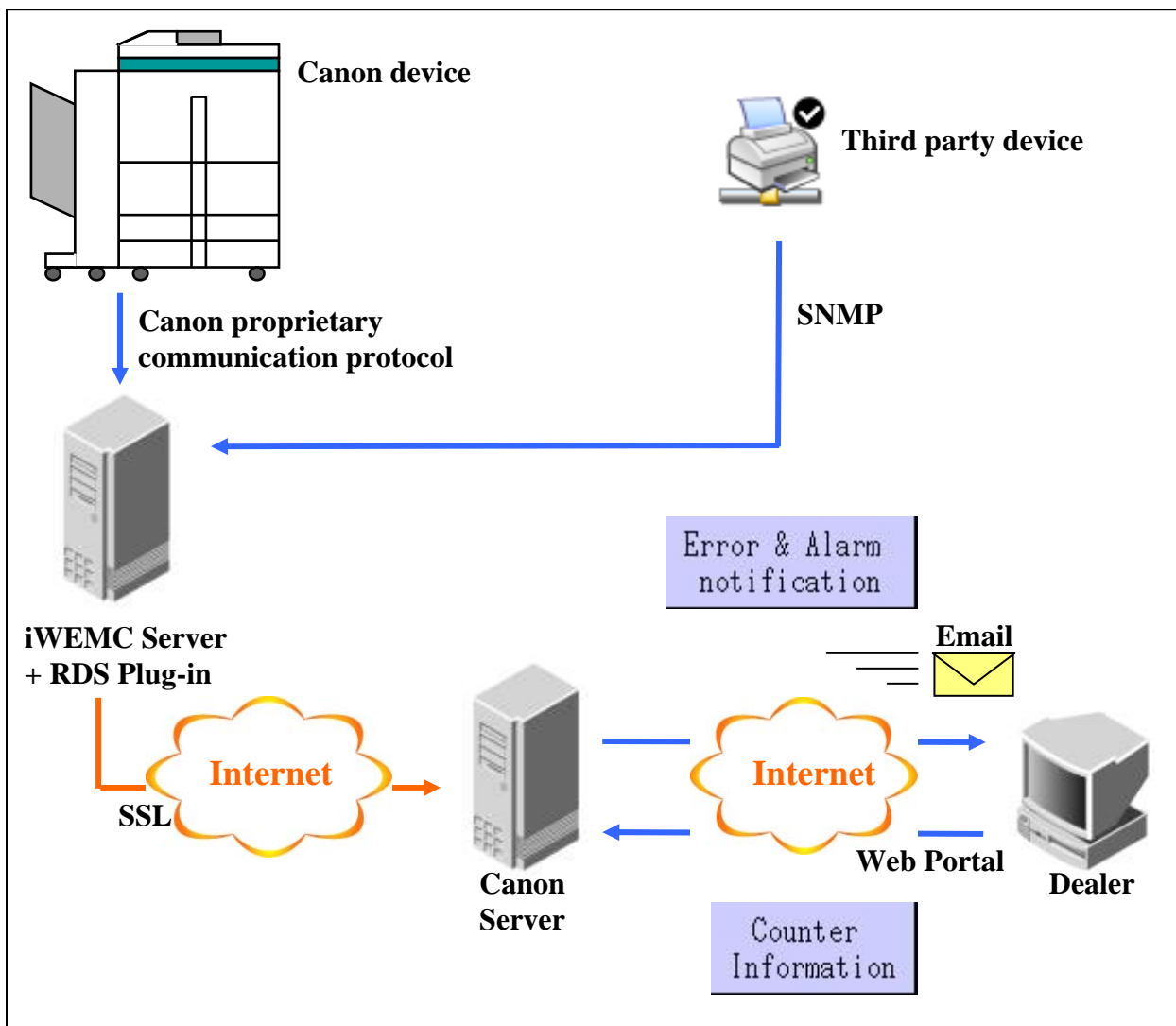
Enhanced Service Offering

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

Usage Statistics, Parts Lifetime and Consumables Management

As part of the imageWARE Remote Service Monitor feature, service providers have access to information on parts usage of customers' registered imageRUNNER 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 SSL connection to the UGW server (push process)

Once the data is on the UGW server:

- Meter readings are available on the UGW server for download by the service provider (pull

- process).
- Error/jam/alarm notifications can be sent directly to the service provider by e-mail upon occurrence (push process).
- The service provider can also log onto UGW to obtain information on any error/jam/alarm notification (pull process).

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 imageRUNNER communicates only with the UGW when sending device information. The authentication method is described later.

Communication Protocol

The eRDS enabled imageRUNNER communicates with the UGW by using the HTTPS protocol. The eRDS enabled imageRUNNER acts as the “Client”, and will never become a HTTP server for the purposes of eRDS communication. Please note that some imageRUNNERS may act as a HTTP 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 imageRUNNER 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	4 KB

imageWARE

Remote

Jam data	Includes the jam code, date of occurrence, total counter at occurrence, paper feeding slot, and paper size.	When a jam occurs	4 KB
Alarm data	Includes the alarm level, alarm code, alarm subcode, date of occurrence, and total counter at occurrence.	When an alarm occurs	4 KB
Status data	The data when a status change occurs.	When status change occurs	4 KB
Billing counter data	The counter data typically used for billing, such as Total, Copy, Print, B/W, and Color.	Every 16 hours	Approx. 250 KB (Billing counter: 62 KB, Detailed counter: 42 KB, Parts counter: 33 KB, Mode counter: 111 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.		
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)	13.5 KB
Environment log data	Environment log data of the device (e.g. temperature, humidity)	The data is sent once every twelve 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	Only at the time of the first communication test. UGW3.0 or later.	Approx. 150 KB

imageWARE

Remote

	image formation.		
	All Display values which are measured values related to image formation.	When specific alarms or errors occur. UGW3.0 or later.	Approx. 50 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. 4.2 KB

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

**Data
Encryption**

From eRDS to the UGW server, data is encrypted at the transport layer through a SSL 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 : 1024bit

Symmetric Key length : 128bit

eRDS activation

eRDS is integrated in the main unit firmware of the imageRUNNER device. In order to enable eRDS, the setting must be activated from service mode, therefore a user cannot accidentally activate the option.

**Authentication
Procedures****Server Authentication**

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

1) SSL Authentication

SSL Authentication is performed according to the following procedures. Please note the following steps describe the SSL 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 imageRUNNER 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 imageRUNNER and the UGW.

The URL of the UGW Server is pre-populated into the firmware of the imageRUNNER.

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 imageRUNNER will not transmit any data.

Client Authentication

This section describes the client authentication used by the UGW.

1) Client authentication by SSL (OSI Layer 4 to 5)

Client authentication by SSL 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 imageRUNNER, establishing communication between the UGW and the device.

Reverse engineering is impossible because of SSL encryption and the use of the Canon proprietary Simple Object Access Protocol (“SOAP”) schema communication protocol. Therefore, a rogue client cannot be developed.

Service Browser (to display information for service technician)

The Service Browser is a feature available only on imageRUNNER ADVANCE units. The purpose of this feature is to provide comprehensive and up-to-date repair reference, specific to the problem at hand, for the service technician.

(1) To enable the Service Browser, the device must succeed in the communication test with UGW. Since the Service Browser can only be enabled and started up in the service mode, it cannot be operated by customers.

(2) As for the URL to connect to the FAQ portal, the “ugwdevice.net” domain is preregistered to My Favorites, which can be edited in the service mode level 2.

The communication path between the Service Browser and UGW (FAQ portal) is encrypted using SSL.

(3) To log onto UGW, besides the Web-Portal ID and password, the serial number information of the iR device installed with the Service Browser is used for authentication, so no third party can have an easy access.

(4) Device retrieves the service data from UGW, and stores on the local domain to process. The service data that the device gets is handled only with the service browser. It does not affect on the standard browser function and customer’s data.

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(****Enabled

as in the device has service mode switch activated for CDS? Or device has to be CDS capable? Or is there something to activate on the CDS server?****) on the Content Delivery System.

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.

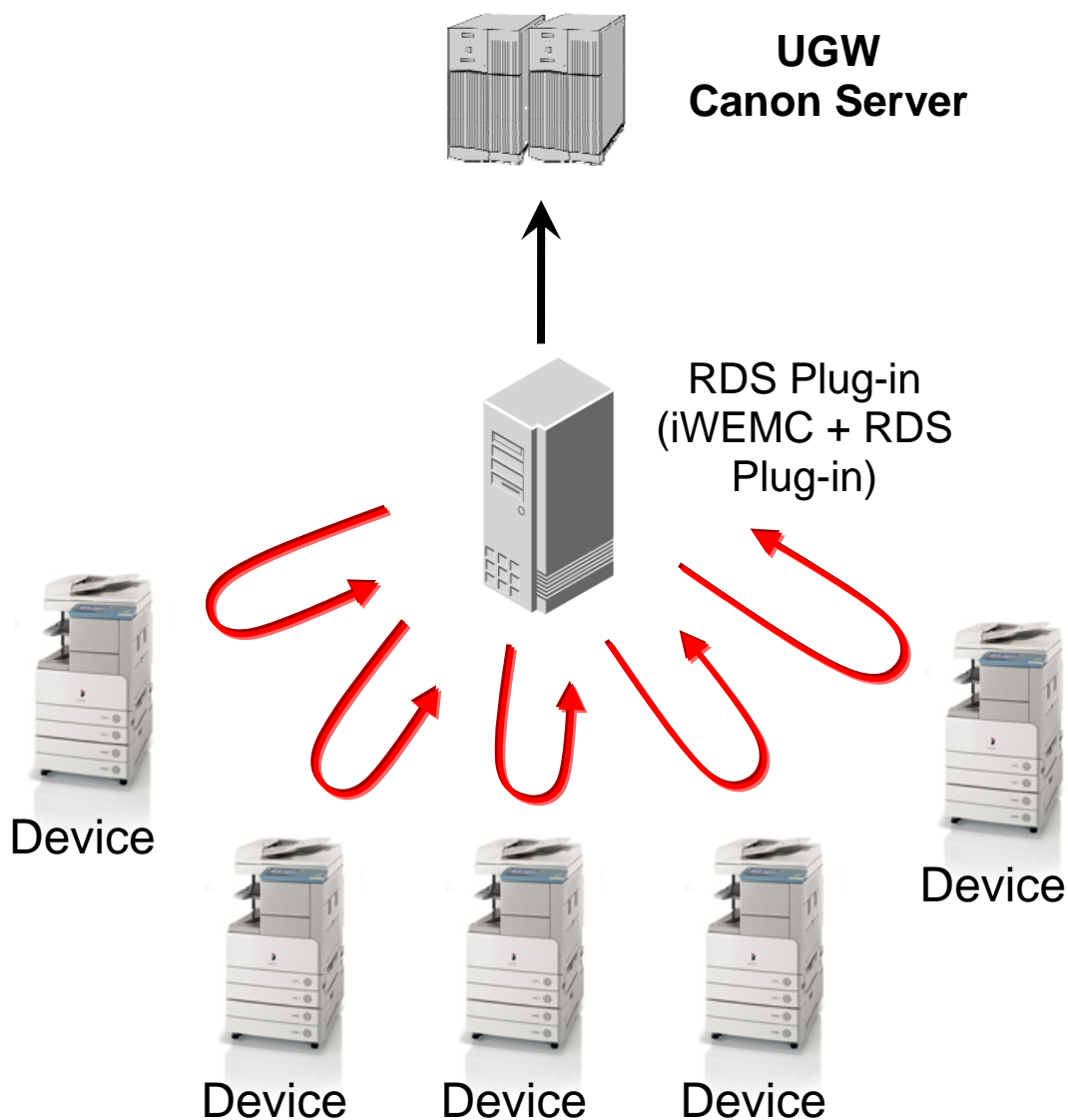
* For more information on security of the function to invoke an application (firmware distribution command function) on the CDS management server from the UGW Web Portal, refer to the “Content Delivery System Security White Paper”.

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

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: once every 5 minutes Amount of data: 0.2 KB/device
Counter-related data	Frequency: once per hour or less often Amount of data: 5 KB/device
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 per hour or less often Amount of data: approx. 0.2 KB/device
Environment data	Frequency: once every 3 hours Amount of data: 1 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. 4 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. 4 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	Approx. 4 KB

		creates an alarm log by setting its level to 3 and sends a false alarm.	
Status data	Device status change event	When status change occurs.	Approx. 4 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. 34 KB (Measured on iR C3200)
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. 38 KB (Measured on iR C3200)
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. 118 KB (Measured on iR C3200)
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 C3200)
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 C3200)
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 C3380 with 10 logs)
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

* 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 through a SSL 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 : 1024bit

Symmetric Key length : 128bit

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.

***RDS Plug-in
failure recovery
measures***

In the event that there is a physical failure on the server 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 SSL authentication together with application authentication. The RDS Plug-in will only transmit data to the UGW server using these methods.

1) SSL Authentication

SSL Authentication is performed according to the following procedures. Please note the following steps describe the SSL 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 imageRUNNER and/or 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 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 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.