Universal Gateway 2

Security White Paper

Revision 1.1.5

Contents

1 Introduction

This paper outlines Canon's approach to security for Canon Universal Gateway 2 (UGW2).

UGW2 is a cloud service that supports device management by communicating with customers' Canon multi-function printers, single function printers and so forth via the Internet. UGW2 comprises a plurality of services for device management, from which users can select the one to use.

Canon believes that it is crucial to disclose information on data handled by UGW2 and security measures implemented in UGW2 help ease the concerns of customers when using UGW2.

This paper first gives the overall configuration, and then the types of the data handled by the systems, network traffic expected to occur, network protocols used for providing the services, and lastly the implemented security measures.

This paper was written for Canon sales companies only. When providing the information to customers, it is prepared on the assumption that each sales company reviews the content and adjusts it to suit the customer.

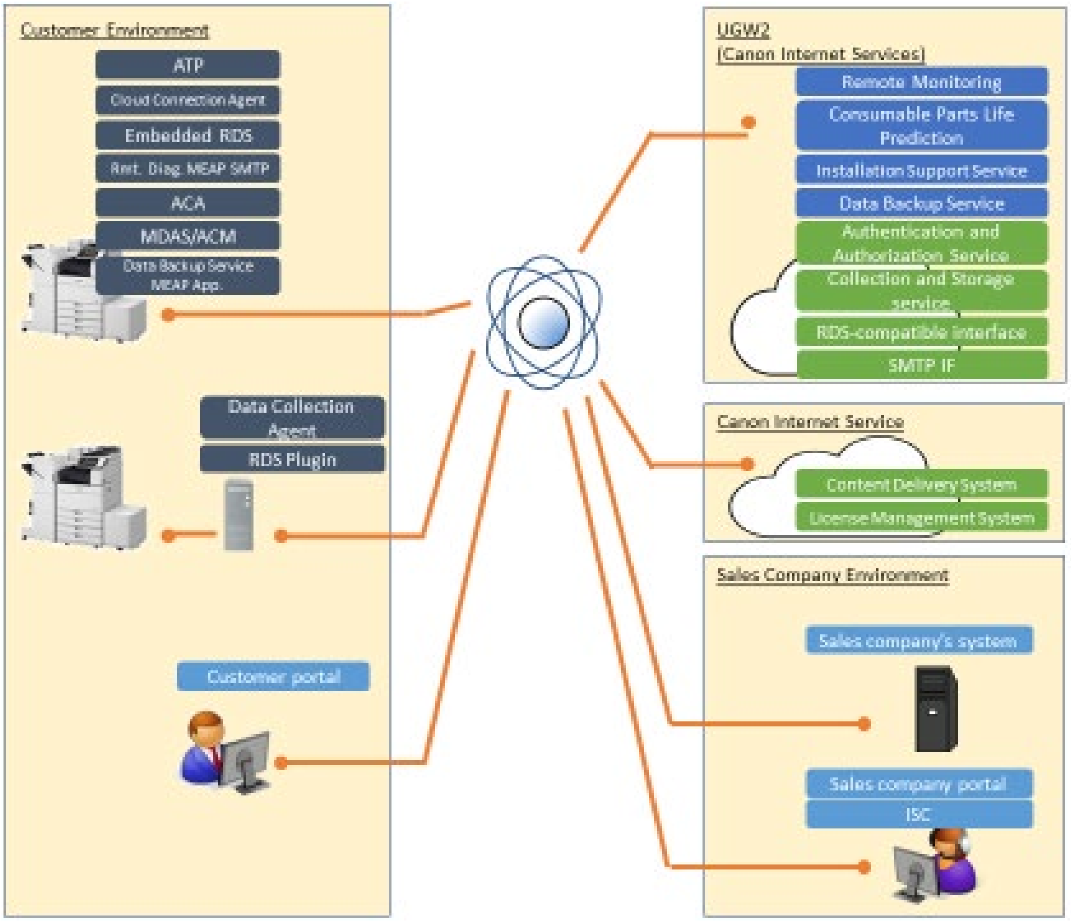
2 System Overview

Each of the services constituting UGW2 provides functions and information appropriate for users and systems of the sales companies and customer's users by linking with customer devices. UGW2 includes UGW2 Common Management (Authentication and Authorization Service and Collection and Storage Service) that transversely and collectively manages sales company, customers, user accounts and devices to make them available to all the services. Thanks to UGW2 Authentication and Authorization Service, once the user accounts and the devices are provisioned in one service, they will be able to be used in all the service. In addition, UGW2 has UGW2 Collection and Storage Service that collects and stores operational data of a large number of devices. The services share data stored on the UGW2 Platform for providing their functions.

3 System Configuration

UGW2 consists of:

- Services for device management Authentication and Authorization Service Collection and Storage Service Client applications for each of the services
- UGW2 Common Management Service
- Client applications for each of the services



3.1 Universal Gateway 2 (Canon Internet Services)

imageWARE Remote helps by providing maintenance service pursuant to a maintenance agreement between a sales company and a customer, and supplies the following information to the sales company and the customer.

- Counter information, including billing counter information etc.
- Event information related to events such as errors, alarms, and paper jams
- The replacement time of toner cartridges/consumable parts

3.1.1 UGW2 Common Management Service

UGW2 Common Management Service manages sales company, customers, user accounts, devices, etc., and also has authentication and authorization functions for clients (browsers, devices and applications etc.) accessing UGW2.

3.1.2 RDS-Compatible Interface

RDS-compatible Interface supports the communication protocols of imageWARE Remote client applications (Embedded RDS and RDS Plugin), and collects operational data of the devices.

3.1.3 Integrated Database

Integrated Database (DB) collects operational data of the devices, which is used for determining the status of the Canon Group's MFP business in the actual market.

3.1.4 UGW2 Collection and Storage Service

It is a scalable infrastructure that communicates with agent software Cloud Connection Agent to securely and stably collect operational information for structured devices. It also aggregates and accumulates collected data, including data collected via the RDS compatible interface.

3.1.5 Installation Support Service (ISS)

This service enables sales companies to efficiently perform the initial installation of a customer's device.

3.1.6 Data Backup Service (DBS)

It is a service for sales companies to back up and restore customer’s device configuration information.

3.2 Agent Software

3.2.1 Device Embedded Agents

3.2.1.1 *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.

3.2.1.2 *Cloud Connection Agent*

Cloud Connection Agent is a device embedded agent software that sends device event information and log files to the UGW2 collection and storage service, and controls the device.

3.2.1.3 *Embedded RDS (eRDS)*

eRDS is an imageWARE Remote client application, which is a monitoring system that runs on the devices. It transmits data managed by the devices to the RDS-compatible Interface.

3.2.1.4 *Auto Configuration Agent (ACA)*

ACA is a device embedded agent software and MEAP application for ISS. ACA works with ATP, MDAS/ACM to download installation data, firmware, and MEAP applications from ISS and apply them to the device. It can also apply installation data exported to USB memory to the device. ACA is installed on the device by the user during device pre-installation and is deleted after user's confirmation of the pre-installation completion.

3.2.1.5 Data Backup Service MEAP Application (DBSA)

DBSA is a device embedded agent software and MEAP application for DBS. DBSA retrieves configuration information for the device that DBSA is installed on and sends it to DBS.

It also receives the device configuration information from DBS and restores it to the device. DBSA works with ATP, Cloud Connection Agent, eRDS, and ACM.

3.2.2 PC Installed Agents

3.2.2.1 RDS Plugin (RDS)

RDS is an imageWARE Remote client application, which is a monitoring system that is installed and runs on PCs. It monitors 1 to 3000 devices and transmits data managed by the devices to the RDS-compatible Interface.

3.2.2.2 Canon Data Collection Agent (CDCA)

CDCA is an imageWARE Remote enabled client application. CDCA is a type of monitoring program that you install on your PC. CDCA is a monitoring device that can monitor 1 to 1000 devices and sends management information about the devices to the RDS-compatible interface.

3.3 Other Client Software

3.3.1 Installation Support Client (ISC)

This PC application is compatible with ISS and installed on a general-purpose PC. ISC can create, edit, and store the installation model on the ISS. In addition, ISC creates installation data that ACA can read and stores on the ISS or USB memory.

3.4 Device Extension Application

3.4.1 MEAP-integrated Delivery Assistant Service (MDAS)/Application Configuration Management (ACM)

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

3.5 Cooperative System

3.5.1 Content Delivery System (CDS)

CDS is a service that manages and delivers firmware and MEAP applications.

3.5.2 License Management System (LMS)

LMS is a service to issue and manage licenses for software products.

4 Manage Data and Communication Specifications

The types of the data handled by UGW2, the network traffic expected to occur, and the network protocols used for providing the services are listed in the table shown in the Appendix.

5 Recommended Settings for Internet Connection Control

You need to be connected to the Internet to use the UGW2 features. If you need to add a domain name to the allowed list to communicate through a firewall or other security server, we recommend that you use wildcards to specify the following domain names:. If you cannot use wildcards, you must set the FQDN to use. For all FQDNs, refer to the attached UGW2 management information and communication specifications.

5.1 Monitoring Service or Data Backup Service

- *.srv.ygles.com
- *.amazonaws.com
- a01.ugwdevice.net
- b01.ugwdevice.net

5.2 Installation Support Service

- a02.c-cdsknn.net
- *.microsoft.com
- Recommended Edge Update Settings
  - https://docs.microsoft.com/en-us/deployedge/microsoft-edge-security-endpoints
  - https://docs.microsoft.com/ja-jp/deployedge/microsoft-edge-security-endpoints

6 Information Security Policy and Technical Measures

All data handled by UGW2 described herein is considered our information assets to be protected. This chapter provides Canon's information security policies and technical measures to protect information assets from the viewpoint of the three information security components: Confidentiality, Integrity, and Availability.

6.3 Confidentiality

Confidentiality in UGW2 is designed to help ensure that only authorized users have access to information assets. The information security policies related to confidentiality are as follows.

- UGW2 manages users and the systems appropriately, and allows only the right users and the right systems (including devices) to access information assets.
- UGW2 is designed to establish secure communication channels on the Internet to help prevent data leakage.
- 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.

The following describes the technical measures implemented in UGW2 to maintain the confidentiality of information assets pursuant to the above policies.

6.3.1 Encryption Using HTTPS

Encrypted communication over HTTPS communication occurs between the web browser and the device management service, and between the device and the service registry service. 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 Encryption: RSA 2048
- Symmetric Key Encryption (Maximum)
- AES 256 (Depend on the Web browser)

The communication protocol supports TLS 1.2.

Note: The Cloud Connection Agent does not follow the TLS settings of the device

6.3.2 Device Management

Confidentiality in Device Management Services and Service Registry Services means ensuring that only authorized users are permitted to access to protected asset information. The security policy for confidentiality is as follows:

- Device Management Services and Service Registry Services manage the users and systems that have access to the protected asset information and help ensure that only the appropriate users or systems have access to the protected asset information.
- Device management and service registry services create a reliable channel for communication over the Internet to ensure that data is not compromised.

To achieve this security goal, we have implemented the following technologies in our device management services.

6.3.3 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.

If your browser requires sensitive information, such as changing the password string set by the WebUI, send a special string to the browser instead of the sensitive information.

(Appears in the browser as a password string "*******")

6.3.3.1 Installation Support Service Stored Data

Encryption of Data Held by ISS Services

The data received by the ISS service from ISC and ACA is kept encrypted.

Information Type	Encryption Method
Installation model information	Symmetric cipher: AES 256
Installation results information	Symmetric cipher: AES 256

Encryption of USB Memory Data

The installation model and results that ISC and ACA read and write to the USB memory are encrypted.

Information Type	Encryption Method
ACA management information	Symmetric cipher: AES 128
Installation model information	Common Key Encryption: AES 128[1]
Device Content Information	Encrypted by an external system[2]
Device content file	Common Key Encryption: AES 128/Encrypted by External Systems[2]

Encrypting File Server Data

The firmware file that ISC stores on the file server is encrypted.

Information Type	Encryption Method
Device content file	Common Key Encryption: AES 128/Encrypted by External Systems[2]

Encrypt the Exported Installation Model File

The installation model file that ISC exports is encrypted.

Information Type	Encryption Method
Installation model information	Symmetric cipher: AES 128

[1] The security level of the device configuration files imported into ISC maintains the security level you choose when exporting from the device. The newly created device configuration files in ISC has a security level 1. The device configuration files conform to the device specifications

[2] Encrypted by LMS/CDS, etc.

6.3.3.2 Data Stored in the Backup Service

Encrypt and retain backup data.

Information Type	Encryption Method
Backup Data	Symmetric cipher: AES 256

6.3.4 Storing Credentials

UGW2 maintains the following credentials in a lossy 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.

6.3.4.1 Storing Installation Support Service Credentials

Storage of Authentication Information Held by ISS Services

The ISS service maintains the following credentials:

Information Type	Encryption Method
File Server Information	Encryption by keys using AWS Key Management Service (KMS)

Storage of Authentication Information Maintained by ISC

ISC maintains the following credentials.

Information Type	Encryption Method
Client credentials	Encryption with Windows DPAPI
Authorization token	Encryption with Windows DPAPI

Account management is delegated to Microsoft Edge.

The management of file server and proxy credentials is delegated to the Windows Credential Manager.

Storage of Credentials Maintained by ACA

ACA maintains the following credentials.

Information Type	Encryption Method
Proxy authentication information	Symmetric Key Encryption (Maximum) — AES 128

6.3.5 Authentication and Access Control

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

Accessed	Authentication	Access Control
Sales Company Portal	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" 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 sales company to which it belongs and the sales company under its control. (However, if the sales company to which the account belongs is the direct sales company, the data managed by the indirect sales company 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" for more information about user authentication. Successful accounts will have access to information determined by the sales company 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.
Sales Company System API	Through the Internet, the sales company system sends credentials.	If authentication is successful, the sales company system receives an access token that allows it to send data to UGW2. Sales company systems can send and receive information from various service systems by sending an access token with a request to UGW2.
UGW2 Collection and Storage Service	Through the Internet, the device sends credentials	If authentication is successful, Cloud Connection Agent can send data to UGW2.

6.3.6 Measures Against Malicious Code Attacks

Device management services are designed to prevent malicious user code entry attacks to prevent user device information from being exposed. The Device Management Services web page performs server-side sanitizing and input validation to help avoid various input attacks such as SQL injection. This should prevent unauthorized theft of device information stored by Device Management Services.

6.3.7 Authentication Information Protection

Measures to prevent leakage of authentication information are implemented in UGW2. The following authentication information will be irreversibly converted and stored in UGW2 (no algorithm is disclosed).

- Account authentication information which are used when accessing UGW2 Portals
- Authentication information used by the systems (including devices) when accessing 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

6.3.8 Access Control and Authentication

UGW2 implements access control and authentication mechanisms designed to ensure that only the right users and the right systems (including devices) can access to information assets.

6.3.8.1 User Authentication

User authentication with a user ID and password is provided.

Authentication Cookie

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 : 120 minutes (2 hours)
- Authentication cookie timeout : 1440 minutes (24 hours)

Authentication Logs

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 five (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

6.3.8.2 Access Control to Customer Data

In order for users of the distributor to have access to customer data, they must register or share customers on the portal for Sales Company. At the time of customer registration, the ID of the customer is issued and the service license is issued all at once.

6.3.8.3 Access Control by Each Client Application

The client applications, namely e-RDS, RDS, and CDCA, provide access control and authentication mechanisms ensuring that only the right users can access to information assets.

Access Destination	Authentication	Access Control
Cloud Connection Agent	Enter a special authentication operation from the device's operation panel.	If the authentication is successful, the CE setting screen including Cloud Connection Agent setting screen can be operated.
Embedded RDS (eRDS)	Perform a specific operation in the authentication process on the device control panel.	Once the authentication has succeeded, access to the service menu for service technicians, including the eRDS configuration menu, becomes possible.
RDS Plugin (RDS)	Enter authentication information into RDS or a web browser of another PC through a network.	The customer's IT administrator provisions an administrator account and groups for RDS. Once the authentication has succeeded, access to the screens predetermined according to the granted permissions becomes possible.
ACA	Automatic device authentication with ATP when searching for installation models	If the authentication is successful, it is possible to obtain an installation model that matches the installation number (Serial number of the device running or ACA) entered on the ACA screen among the installation models held by the tenant corresponding to the organization number entered on ACA screen, and to upload the installation results.
ISC	Enter credentials from login screen	Once authenticated, the installation model can be viewed and edited based on the authorized user.
DBSA	Enter device registration key in ATP	If the authentication succeeds, the backup data can be transmitted to the customer tenant.

Access Destination	Authentication	Access Control
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 eight (8) characters (V1.1 and later).

6.3.9 Authorization

UGW2 implements an OAuth 2.0 authorization server for allowing the user to impart its granted permissions to a linked service so that the service can access information assets covered by the permissions.

6.3.9.1 Grant Types

The following grant types are supported in UGW2 Common Management Service.

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

6.3.9.2 Access Tokens

Only bearer token types are supported in UGW2 Common Management Service.

The table below shows expiration time for each access token type. The entropy of access tokens follows the UGW2 specifications.

Token Type	Expiration Time
Authorization Code	600 sec (10 minutes)
Access Token	3,600 sec (1 hour)
Refresh Token	34,560,000 sec (400 days)[3]

[3] A refresh token will be invalidated when an access token is refreshed, and a new refresh token will be issued.

6.3.9.3 Client Authentication

For Client Credentials Grant, a client ID and client secret are used via Basic authentication, and for urn: ietf: params: oauth: grant-type: jwt-bearer, a key pair is used for authentication. A client ID is generated randomly using UUID format indicating it is a client. A client secret is a random string that consists of 20 characters contains at least one upper case letter, one lower case letter, one number, and one special symbol. For the specifications that treat client secrets as passwords, client secrets are treated in the same manner as user passwords. However, unlike user passwords, client secret never expires.

6.3.9.4 Redirect URI

The redirect URI used for OAuth2.0 in UGW2 Common Management Service is required to be an absolute URI and must not include a fragment component. Moreover, it needs to be registered beforehand. 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.

6.3.9.5 Scopes

UGW2 Common Management Service supports only predefined scopes, and an authentication token that does not have any scopes associated cannot be issued. For scope types, refer to the specifications of each of the services.

6.3.10 Countermeasures Against Malicious Code Attacks

UGW2 prevents malicious user code entry attacks to help prevent the leakage of user credentials and customer information from each sales company. All interfaces, including UGW2 web screen, and sales company system APIs, perform server-side sanitizing and input validation to avoid various input attacks typified by SQL Injection. This prevents unauthorized theft of protected asset information managed by UGW2.

CDCA takes measures against malicious user input attacks to prevent the leakage of user credentials and customer information. CDCA web screen utilizes .NET Entity Framework 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.

6.4 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 helps ensure that the communication partner is correct when protected asset information is sent and received by communication.
- UGW2 helps ensure 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.

6.4.1 Data Validation

UGW2 checks the accuracy of the received information assets. The following items will be checked.

Transmission Source

Compare the device information included in the received data with the registered device information to check whether they match. UGW2 will not receive any data sent from devices other than the registered devices.

Data Contents

Check that the received data is in a specified format and required data is actually present. If the data is not in the specified format, it will be discarded.

6.4.2 Server Authentication

The client applications transmit device monitoring information to only UGW2. In HTTPS communications by UGW2 with the client applications and, DigiCert SSL certificates are used for server authentication. The identification of servers with UGW2's unique URL verification process allows the client applications to control transmission destinations.

- Root certification authority: VeriSign Class 3 Public Primary Certification Authority - G5 or DigiCert Global Root G2
- Signature algorithm for SSL certificates: 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.

6.4.3 Device Management

Integrity in device management and service registry services means providing that protected asset information is accurate and that protected asset information is complete. Our security policy is as follows.

- The Device Management Service and Service Registry Service ensure that the peer is correct when protected asset information is sent and received by communication.
- The Device Management and Service Registry services ensure that the protected asset information stored is correct and complete.

To achieve this integrity policy, we have implemented the following technologies in our device management services.

6.4.4 Countermeasures Against Unauthorized Access

To minimize the risk of third-party intrusion, the Device Management and Service Registry services stop unnecessary network services and close unnecessary ports through firewalls. This limits the route of entry through the network. All network access is logged in the access log. The UGW2 Device Management and Service Registry services provide access logs in the unlikely event of an unauthorized system intrusion.

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[4], we take measures such as using the form authentication function of .NET and changing the session ID at each log in.

6.4.5 Measures Against Malicious Code Attacks

Device management services prevent malicious user code entry attacks to prevent unauthorized rewriting of device management information. The Device Management Services web page performs server-side processing to avoid various input attacks such as SQL injection and cross-site request forgery. This prevents unauthorized rewriting of device information stored by the device management service.

6.4.6 Verification of Monitored Devices

RDS confirms whether a monitored device has been replaced by checking the unique device identifier (serial number or MAC address) before retrieving data from the device through the network.

[4] Session hijacking is 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.

6.4.7 Countermeasures Against Malicious Code Attacks

UGW2 detects and defends against malicious code attacks to prevent falsification of information assets. Preventative measures are taken against attacks such as SQL Injection and cross-site request forgery on the APIs provided by UGW2, and thus no falsification of the device monitoring information stored in the RDS-compatible Interface occurs.

6.5 Availability

Availability in UGW2 means ensuring that information assets are reliably accessible to authorized users. The information security policy related to availability is as follows.

- UGW2 allows authorized users to access their notifications and the systems when required

Availability in CDCA is the ability of authorized users to access protected asset information when they need it. Our security policy is as follows.

- CDCA can access the system when an authorized user is needed.

The following describes the technical measures implemented in the RDS-compatible Interface to maintain the availability of information assets pursuant to the above policy.

6.5.1 Self Monitoring

RDS/CDCA monitors devices 24 hours/365 days. It has a self-monitoring function, and even if a process is terminated abnormally due to a fatal fault, they are able to continue monitoring using the self-restoration function.

Monitoring system	The time required to detect an abnormal event	Response to the abnormal event detected
RDS Plugin (RDS)	A maximum of three minutes	Restart the process

6.5.2 Countermeasures Against Malicious Code Attacks

UGW2 detects and defends against malicious code attacks to provide stable system performance. To avoid various attacks such as cross-site scripting on the APIs provided by UGW2, sanitization is carried out at the server side. This helps protect the systems from various attacks such as tricking a user who accessed UGW2 into navigating to a malicious website or making it impossible for the customer to get necessary information.

6.5.3 Maintaining High Availability

High availability strategies are implemented in UGW2 to ensure the business continuity of the sales companies, customers, and partners.

The Managed Services offered by the cloud service provider for UGW2 is used as the execution environment for software and databases comprising the services, and delivers the following high availability features.

- The systems and the databases are constantly managed by the Managed Services so as to maintain stable performance. When the amount of traffic increases, auto scaling is performed to handle more traffic without impairing performance.
- Requests and data stored on the systems and the databases are automatically distributed to multiple data centers to prevent data loss and service downtime even if some of them fail.

Failover is provided for operations not using the Managed Services. Besides, redundancy technologies are used for all servers of the systems, if one of them fails, processing is distributed to the other servers operating normally. These strategies allow users who have logged into UGW2 to access information assets at any time.

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

6.5.4 Device Management

Availability in the Device Management Information Service and Service Registry Service is the ability of authorized users to access protected asset information when needed. Our security policy is as follows. The Device Management Information Service and Service Registry Service allow users to access the system when they need it. To achieve this security strategy for availability, we have implemented the following technologies for device management information services and service registry services.

6.5.5 Failover Enabled

To provide a stable system, the Device Management Information Service and Service Registry Service implement failover capabilities in the system. In the unlikely event that a single server fails, it is automatically distributed to the surviving server. This mechanism provides an environment in which users who have accessed the device management information service or the service registry service can access the information when they want to use it.

6.5.6 Measures Against Malicious Code Attacks

To provide a stable system, UGW2 prevents malicious user code entry attacks. UGW2 provides an API that performs server-side sanitizing to avoid various input attacks, such as cross-site scripting. This helps protect the system from attacks in which the user accessing the UGW2 is forced to communicate with an unintended website or cannot obtain the information the user needs.

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.

6.5.7 Countermeasures Against Email Virus

To provide stable performance, UGW2 implements a spam and virus filtering service that detects and blocks unwanted and unsafe emails such as spam emails and virus-infected emails. Thanks to the spam and virus filtering service, the unwanted and unsafe emails are eliminated before the services receive them.

6.6 Penetration Testing

Penetration testing is conducted on a regular basis by a third-party vendor to evaluate the security described herein.

7 Appendix

Amazon Web Services (AWS) Data Center

UGW2 runs in an AWS environment. Please refer to link below for more information regarding AWS compliance programs.

https://aws.amazon.com/compliance/programs/

Data Traffic Between the Monitor and the Device

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing
RDS Plug-in V3.x polling monitoring	Event Occurrence Notification	Approximately 0.2 KB	Each time an event occurs
	Status Monitoring	Approximately 1 KB	Once every 5 minutes
	Service Call Log	Approximately 0.7 KB	Each time an event occurs
	Alarm Log	Approximately 0.7 KB	Each time an event occurs
	Jam Log	Approximately 0.7 KB	Each time an event occurs
	Part Counter	Approximately 4 KB	Once every 6 hours
	Counters by mode	Approximately 7 KB	Once every 6 hours
	Billing Counter - Department Counter - Total Resource Counter - Service Mode Counter	In the case of 1000 divisions Approximately 712 KB When there is no department registration Approximately 15 KB	Once every 6 hours
	Firmware Version	Approximately 3 KB	Once every 6 hours
	Environment Log	Approximately 6 KB	Once every 6 hours

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing
RDS Plug-in V3.x Bit Connection Monitoring	Service Call Log	Approximately 5 KB	Each time an event occurs
	Alarm Log	Approximately 5 KB	Each time an event occurs
	Jam Log	Approximately 5 KB	Each time an event occurs
	US > Alerts	Approximately 5 KB	Whenever the monitored status changes
	Part Counter	Approximately 103 KB	Once every 8 hours
	Counters by mode	Approximately 164 KB	Once every 16 hours
	Billing Counter - Department Counter - Total Resource Counter - Service Mode Counter	In the case of 1000 divisions Approximately 712 KB When there is no department registration Approximately 15 KB	Once every 6 hours
	Firmware Version	Approximately 5 KB	Once every 8 hours
	Environment Log	Approximately 6 KB	Once every 6 hours
RDS Plug-in V3.x Bit Connection Monitoring Cont'd	Service Mode Menu Information (ADJUST information, which is set values, and DISPLY values, which are measured values related to image formation)	Approximately 281 KB	During the initial communication test
	Service Mode Menu Information (ADJUST information, which is various settings in the service mode menu)	Approximately 154 KB	When service mode menu settings are changed
	Service Mode Menu Information DISPLAY value, which is a measurement related to image formation	Approximately 127 KB	Each time a particular event occurs
	Enable Browser Options	Approximately 3 KB	When Service Man Browser is enabled
	hard disk status diagnostic information	Approximately 5 KB	Once in 30 days
	Inquire about setting information	Approximately 2 KB	Once every 12 hours

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing
CDCA v 1.0 polling monitoring	Status Monitoring	Approximately 1.2 KB (Events included: 0.2 KB)	1. Once every 5 minutes (Do not retrieve during sleep) 2. When a status change event occurs (Also retrieve during sleep)
	Service Call Log	Approximately 0.9 KB (Events included: 0.2 KB)	1. Once every 5 minutes (Do not retrieve during sleep) 2. When getting log write events (Also retrieve during sleep)
	Alarm Log	Approximately 0.9 KB (Events included: 0.2 KB)	1. Once every 5 minutes (Do not retrieve during sleep) 2. When getting log write events (Also retrieve during sleep)
	Jam Log	Approximately 0.9 KB (Events included: 0.2 KB)	1. Once every 5 minutes (Do not retrieve during sleep) 2. When getting log write events (Also retrieve during sleep)
	Part Counter	Approximately 4 KB	1. When acquisition has not been completed for 8 hours or more and less than 24 hours since the 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) 3. Service mode counters and all resource counters are also retrieved when status monitoring, service call logs, alarm logs, and jam logs are retrieved
	Counters by mode	Approximately 7 KB	
	Billing Counter - Service Mode Counter - Total Resource Counter - Department Counter	In the case of 1,000 divisions Approximately 712 KB When there is no department registration Approximately 15 KB	
	Firmware Version	Approximately 3 KB	
	Environment Log	Approximately 6 KB	

Protocol Used Between the Monitoring Device and the Device

Monitoring Device	Protocol	Port Number	Data Source	Remarks
RDS Plug-in	SNMP	UDP/161	Monitoring Device	
	SNMP	UDP/50703 - 65000 *	Device	*Fixed in RDS V 3.2.1 HTTP and later. Automatic allocation is performed for RDS V 3.2.0 and earlier.
	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	*Fixed in RDS V 3.2.1 HTTP and later. Automatic allocation is performed for RDS V 3.2.0 and earlier.
	SLP	UDP/427	Monitoring Device	
	SLP	UDP/11427	Device	
	HTTPS	TCP/443	Monitoring Device	
	HTTPS	TCP/443	Device	
CDCA V 1.0	HTTP	TCP/80	Monitoring Device	
	SNMP	UDP/161	Monitoring Device	
	HTTP	TCP/8000	Monitoring Device	
	HTTP	TCP/8080	Monitoring Device	
	Unique to Canon	TCP/9007	Monitoring Device	
	Unique to Canon	UDP/11427	Device	

Monitoring Device	Protocol	Port Number	Data Source	Remarks
CDCA V 1.0 Cont'd	Unique to Canon	UDP/47545 (Default Value)	Device	
	Unique to Canon	UDP/47545	Monitoring Device	
	Unique to Canon	TCP/47546	Monitoring Device	
	Unique to Canon	TCP/Auto Assignment	Device	
	Unique to Canon	UDP/Auto Assignment	Device	
	SNMP	UDP/Auto Assignment	Device	

Types of Data and Data Traffic Sent by Client Applications

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
ATP	Device Identification • Serial Number	Approximately 4 KB	During communication by ATP	Yes	Yes			Yes	Yes	Indefinite
ATP	Communication Test Results	Approximately 4 KB	During communication test with ATP	Yes	Yes					Indefinite
ATP when checking connection destination	Device Basic Information • Device Name • Serial Number • Country Code • Country Destination	Approximately 2 KB	Every 12 hours		Yes					Not stored
Cloud Connection Agent	Device Basic Information • Device Name • Serial Number • Network Configuration Information • Firmware Information	Approximately 2 KB	Every 12 hours	Yes	Yes	Yes (does not transfer to Japan)			Yes	Indefinite
	Counter Information	Approximately 40 KB	Every 12 hours	Yes		Yes				Indefinite
	Service Call Error Information	Approximately 1 KB	When an event occurs	Yes		Yes				Indefinite
	Self-Diagnosis Information When an Error Occurs	Approximately 1 KB	When an event occurs	Yes		Yes				Indefinite
	Alarm Information	Approximately 1 KB	When an event occurs	Yes		Yes				Indefinite
	Jam Information	Approximately 1 KB	When an event occurs	Yes		Yes				Indefinite
	Alert Information	Approximately 1 KB	When an event occurs	Yes		Yes				Indefinite
	MEAP Information	Approximately 40 KB	Every 12 hours	Yes		Yes				Indefinite
	Hardware Option Information	Approximately 1 KB	Every 12 hours	Yes		Yes				Indefinite
	Calibration Information	Approximately 1 KB	When an event occurs	Yes		Yes				Indefinite
	Storage Information (HDD/EMMC)	Approximately 1 KB	Every 12 hours			Yes				Indefinite
	Environmental Information (Temperature/Humidity)	Approximately 1 KB	When environmental information is output			Yes				Indefinite
	Event Information Filter Configuration Information	Approximately 1 KB	Start of various UGW2 services	Yes						The tenant registration on the device is removed.
	Device Log File	Approximately 1 GB	When a log transmission instruction is received			Yes				Indefinite

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
Cloud Connection Agent (when checking the connection destination)	Device Basic Information • Device Name • Serial Number • Country Code • Country Destination	Approximately 2KB	When the device starts, every 24 hours		Yes					Not stored
eRDS	Service Mode Counter	Approximately 110 KB	Once every 16 hours	Yes		Yes				Indefinite
	Total Resource Counter	Approximately 72 KB	Once every 16 hours	Yes		Yes				Indefinite
	Part Counter	Approximately 103 KB	Once every 16 hours	Yes		Yes				Indefinite
	Inquire About Setting Information	Approximately 2 KB	During the initial communication test Once every 12 hours	Yes						Not stored
	Service Call Log	Approximately 5 KB	Each time an event occurs	Yes		Yes				Indefinite
	Jam Log	Approximately 5 KB	Each time an event occurs	Yes		Yes				Indefinite
	Alarm Log	Approximately 5 KB	Each time an event occurs	Yes		Yes			Yes	Indefinite
	US > Alerts	Approximately 5 KB	Whenever the monitored status changes	Yes		Yes				Indefinite
	Firmware Version	Approximately 5 KB	Once every 7 days (The model that transmits device configuration information does not transmit the firmware version.)	Yes		Yes				Indefinite
	Enable Browser Options	Approximately 3 KB	When Service Man Browser is enabled	Yes						Indefinite
	Calibration log	Approximately 3 KB	Time of calibration	Yes						Indefinite
	Device Configuration Information	Approximately 232 KB	The first communication test and when device configuration information is updated.	Yes						Indefinite

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
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	Yes		Yes				Indefinite
	Part Counter Information	Approximately 105 KB	Send once every 16 hours	Yes		Yes				Indefinite
	Counter Information by Mode	Approximately 169 KB	Send once every 7 days			Yes				Indefinite
	Inquire about setting information	Approximately 2 KB	Once every 12 hours	Yes						Not stored
	Service Call Log	Approximately 5 KB	Each time an event occurs	Yes		Yes				Indefinite
	Jam Log	Approximately 5 KB	Each time an event occurs	Yes		Yes				Indefinite
	Alarm Log	Approximately 5 KB	Each time an event occurs	Yes		Yes				Indefinite
	US > Alerts	Approximately 5 KB	Whenever the monitored status changes	Yes		Yes				Indefinite
	Firmware Version	Approximately 8 KB	Send once every 7 days	Yes		Yes				Indefinite
	Enable Browser Options (Bit connector only)	Approximately 3 KB	When the browser enable button is pressed in the service mode menu	Yes						Indefinite

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
Browser	Sales Organization Information - Identification information - Company Name - language code - time zone - Locale - address information* - Mail address setting information* - Other	Approximately 5 KB	Sales Organization Information Operation	Yes	Yes	Yes *1 (data with “*” is not transferred to Japan)				Tenant Information - Delete after 400 days of tenant deletion *1:Data retention period is indefinite
	Customer Info Identification information - Customer Name* - language code - time zone - Locale - address information* - Industry - cutoff date - Invoice To Information* - Contact Information* - Other	Approximately 5 KB	During the Customer information operation	Yes	Yes	Yes *1 (data with “*” is not transferred to Japan)				Tenant information (Exclude Log Information): Deleted 400 days after tenant deletion ･Log Information Login log: deleted 1100 days after log output or 400 days after tenant deletion Service usage log － deleted 1100 days after log output or 400 days after tenant deletion *1:Data retention period is indefinite
	User Information - User ID - Password - Email address - Name - Locale - Phone Number - Other	Approximately 3 KB	During the user information operation	Yes	Yes					Delete Immediately After Deleting User Delete as soon as tenant is deleted
	Client Information - Client ID - Client Secret - Device Serial Number - Device Product Name * - Device name * - Device location * *This information is set only for clients registered from the old ATP.	Approximately 2 KB	During the client information operation		Yes					

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
Browser (cont'd)	Authorization Information - Authorization Code - Access Token - Refresh Token	Approximately 2 KB	During each API call		Yes					Authorization Code ー Delete after 10 minutes of issue ･Access Token ー Delete after one hour of publication ･Refresh Token ー Delete after 400 days of publication"
	Administrator Information - Admin Name - Administrator Contact Information	Approximately 1 KB	During the administrator information operation	Yes						Delete immediately after administrator deletion
	Contract information - Contract Number - Contract period information - Contract Category - Other	Approximately 1 KB	When operating contract information	Yes						Delete as soon as the contract is deleted
	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		Yes*1 Data with "*" is hashed and transferred to Japan.				RDS Information Deleted Immediately *1:Data retention period is indefinite
	Inventory subinventory information - inventory subinventory - Customer Name - address information - Other	Approximately 3 KB	During inventory subinventory operations	Yes						Inventory subinventory information Delete immediately after deletion
	"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	Yes	Yes*1 Data with "*" is hashed and transferred to Japan.				Delete device information immediately after deletion *1:Data retention period is indefinite
	Managing Installation Data -File Server Information"	Approximately 2 KB	During file server information operation					Yes		Deleting file server information ･Within 12 hours after tenant removal

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
ISC	ISC Configuration Information -Windows version -.NET Framework Version -ISC Version	Approximately 1 KB	During each API call					Yes		Indefinite
	Authorization Information -Authorization Code -Access Token -Refresh Token	Approximately 2 KB	During each API call					Yes		Authorization Code ー Delete after 10 minutes of issue ・Access Token ー Delete after one hour of publication ・Refresh Token ー Delete after 400 days of publication
	Installation model information -Installation Model Name -Other information entered by the user in ISC"	Approximately 400 KB Sample data Properties -Name, commented firmware -selected, updating Software Choose two options and two applications Common DCM files -Setting value of about 300 KB after exporting (except service mode) all categories from the device number of individual configurations Individual DCM files -Setting value of several KB"	During installation model saving operation					Yes		Within 15 minutes after removal of installation model (Internal backup data is deleted 8 days after operation) Within 12 hours after tenant removal
	Installation results information -Installation result -Device Settings Import Results Report"	Approximately 5 KB	During installation result upload operation					Yes		Indefinite. The DCM of the backup data of the installed model at the time of installation has been removed by deleting the most recent installation model. Within 12 hours after tenant removal"

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
ACA	ACA Configuration Information - {461}	Approximately 1 KB	During each API call					Yes		Indefinite
	Authorization Information -Access Token	Approximately 2 KB	During each API call					Yes		Access Token ― Delete after one hour of publication
	Installation data retrieval information -Organization Number -Installation number Device Serial Number	Approximately 2 KB	During installation data retrieval operation					Yes		Not stored
	Installation results information -Installation result -Device Settings Import Results Report"	Approximately 5 KB	During installation data retrieval operation					Yes		Indefinite. The DCM of the backup data of the installed model at the time of installation has been removed by deleting the most recent installation model. Within 12 hours after tenant removal"

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
DBSA	Backup Data -User Mode -Service Mode -Address Book -Personalization data (User Data) -MEAP application setting information -MEAP Application License Information -Advanced Box Folder Configuration (Tier 1) -Device Product Name -Firmware (controller) version -MEAP Application Identification -MEAP Application Version	Approximately 2000 KB Sample data - Users: 30 -5 MEAP applications Configuration file for each MEAP application: 200 KB	Once a week during a backup run operation						Yes	When the number of backup data items stored in DBS exceeds 4 (delete other backup data, leaving the last three.) When you delete backup data from the UGW2 When you delicense DBS from UGW2 When you remove a device from the UGW2 15 seconds after unregistering the device from the UGW2
	"Backup Service Configuration Information ・Schedule regular backups"	Approximately 1 KB	Once a day for configuration change operations, regular backups, and device registration with Customer Tenant						Yes	When you delicense DBS from UGW2 When you remove a device from the UGW2 15 seconds after unregistering the device from the UGW2"
	"Execution Results ・Results of Backup, Restore, and Migration"	Approximately 2 KB	Once a week, during a backup or restore operation						Yes	When you delicense DBS from UGW2
	"DBSA management information ・DBSA Debug Logs"	Approximately 32 KB	Once a day						Yes	Indefinite
DBSA (when checking the connection destination)	Device Basic Information -Device Name -Serial Number -Country Code -Region information	Approximately 2 KB	When the device starts Every 24 Hours		Yes					Not stored

Data Source	Individual Data Summary	Data Transmission Size	Data Transmission Timing	imageWARE Remote	UGW2 Common Function	UGW2 Collection and Storage	RDS Compatible Interface	ISS	DBS	Data Retention Period in UGW2
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		Yes				Indefinite
	Part Counter Information	Approximately 105 KB	Send once every 16 hours	Yes		Yes				Indefinite
	Service Call Log	Approximately 5 KB	Each time an event occurs	Yes		Yes				Indefinite
	jam log	Approximately 5 KB	Each time an event occurs	Yes		Yes				Indefinite
	alarm log	Approximately 5 KB	Each time an event occurs	Yes		Yes				Indefinite
	US > Alerts	Approximately 5 KB	Whenever the monitored status changes	Yes		Yes				Indefinite
	Firmware Version	Approximately 8 KB	Send once every 7 days	Yes		Yes				Indefinite
	Environmental Information (Temperature/Humidity)	Approximately 20 KB	Send once every 12 hours			Yes				Indefinite

Protocol Used and FQDN

UGW2	ISS	DBS	Protocol	Port Number	Data Source	Application	Data Destination	Remarks
Use started after system change		Yes	HTTPS	TCP/443	Cloud Connection Agent	Data Transmission	hbp-uw2l.srv.ygles.com kinesis.us-west-2.amazonaws.com cognito-identity.us-west-2.amazonaws.com	Destination FQDN If you need permission settings, we recommend that you use wildcards to specify the following domain names: - *.srv.ygles.com - *.amazonaws.com If the above setting is possible, the setting is completed by adding the following domains. For remote monitoring and DBS use - a01.ugwdevice.net - b01.ugwdevice.net In the case of ISS use, - a02.c-cdsknn.net - *.microsoft.com If you cannot configure using wildcards, you must select and configure all FQDN s for each communication. When acquiring the connection destination information of UGW2, it communicates with the UGW common functions located in Europe.
		Yes	HTTPS	TCP/443	Cloud Connection Agent	Control	a20sc2usy86t4y-ats.iot.us-west-2.amazonaws.com	
Yes		Yes	HTTPS	TCP/443	eRDS RDS Plug-in (HTTP) CDCA V 1.0 Rmt Diag MEAP HTTP	Data Transmission & Control	a01.ugwdevice.net b01.ugwdevice.net	
Yes			HTTPS	TCP/443	Browser Sales Company System Client	Authentication & Authorization	www-uw2.srv.ygles.com camapi-uw2.srv.ygles.com cam-uw2.srv.ygles.com camapis-uw2.srv.ygles.com uw2-oip-lfscl-extacs.s3.amazonaws.com uw2-oip-intvs.s3.amazonaws.com camapi.srv.ygles.com cam.srv.ygles.com www.srv.ygles.com	
Yes	Yes	Yes	HTTPS	TCP/443	ATP Browser ISC ACA DBSA Sales Company System Client	Authentication & Authorization	camapi.srv.ygles.com cam.srv.ygles.com www.srv.ygles.com	
Yes			HTTPS	TCP/443	Browser Sales Company System Client	Device Registration Management	mds-uw2.srv.ygles.com	
Yes			HTTPS	TCP/443	Browser Sales Company System Client	imageWARE Remote	rcm-uw2.srv.ygles.com rcmapi-uw2.srv.ygles.com uw2-oip-extacs.s3.us-west-2.amazonaws.com uw2-rcm-lfscl-extdstb-1.s3.us-west-2.amazonaws.com	
	Yes		HTTPS	TCP/443	Browser ISC ACA	ISS (Portal/API)	iss-uw2.srv.ygles.com issdata-uw2.srv.ygles.com uw2-oip-extacs.s3-us-west-2.amazonaws.com uw2-oip-extacs.s3.us-west-2.amazonaws.com uw2-oip-extvs.s3-us-west-2.amazonaws.com uw2-oip-extvs.s3.us-west-2.amazonaws.com	
		Yes	HTTPS	TCP/443	Browser DBSA	Backup Services (Portal/API)	dcf-uw2.srv.ygles.com	

Note: Destination FQDN: If you need permission settings, we recommend that you use wildcards to specify the following domain names:

*.srv.ygles.com
*.amazonaws.com
*.ugwdevice.net

Protocol Used Between the Monitoring Device and the Device

Protocol	Protocol	Port Number	Data Source	Remarks
RDS Plug-in	SNMP	UDP/161	Monitoring Device	
	SNMP	UDP/50703 -65000[5]	Device	
	Proprietary to Canon	TCP/47546	Monitoring Device	
	Proprietary to Canon	UDP/47545	Monitoring Device	
	Proprietary to Canon	TCP/9007	Monitoring Device	
	Proprietary to Canon	UDP/50702[5]	Device	
	SLP	UDP/427	Monitoring Device	
	SLP	UDP/11427	Device	
	HTTPS	TCP/443	Monitoring Device	
	HTTPS	TCP/443	Device	

[5] Fixed in RDS V 3.2.1 HTTP and later. Automatic allocation is performed for RDS V 3.2.0 and earlier.

Protocol	Protocol	Port Number	Data Source	Remarks
CDCA v1.0	HTTP	TCP/80	Monitoring Device	Communication when viewing device/remote UI
	SNMP	UDP/161	Monitoring Device	"Communication during device search Communication when obtaining device capability information from a device Communication when obtaining device configuration information from a device Communication when retrieving MIB counters from a device Communication to obtain marker (toner/ink) information from the device"
	HTTP	TCP/8000	Monitoring Device	Communication when viewing device/remote UI
	HTTP	TCP/8080	Monitoring Device	Communication when viewing device/remote UI
	Proprietary to Canon	TCP/9007	Monitoring Device	
	Proprietary to Canon	TCP/Specified port from the device	Monitoring Device	Communication to obtain various counter information from a device (Alarm log/service call log/jam log/environment log/condition log) End Point specified by the device: 9007, 47546, etc.
	Proprietary to Canon	UDP/11427	Device	Communication at the time of power status notification
	Proprietary to Canon	UDP/47545 (Default Value)	Device	Communication at the time of status change event notification Communication at the time of log writing event notification
	Proprietary to Canon	UDP/47545	Monitoring Device	Communication to obtain various counter information from a device (Service mode counters, all resource counters, department counters, mode counters, and part counters) Communication when obtaining device capability information from a device Communication to obtain serial/extended serial information, marker (toner/ink) information, FW information, and toner bottle ID from a device Communication at the time of Wake Up notification (forced data acquisition) of a device
	Proprietary to Canon	TCP/47546	Monitoring Device	
	Proprietary to Canon	TCP/Auto Assignment	Device	Used to response to requests using Canon unique/TCP
	Proprietary to Canon	UDP/Auto Assignment	Device	Used to response to requests using Canon unique/TCP
	SNMP	UDP/Auto Assignment	Device	Used to respond to requests using SNMP/UDP

8 Revision History

Revision	Changed Contents	Author
1st Edition	1st Edition Published	CUSA
1.0.1	Updates to Chapters 3, 5, and Appendix	CUSA
1.0.2	Data Port to Cloud Connection Agent	CUSA
NOTE: No releases between 1.0.2 and 1.1.5		
1.1.5	• Revise description of communication protocol in 5.1.3 • Change direct to indirect in 5.1.6 • Update idle timeout for authentication cookies in 5.1.9.1 • Add minimum password length in 5.1.9.3 • Add new Section 5 • Remove redundant subsections in Section 6 • Add AWS and URL references	CUSA