Canon

imageWARE Enterprise Management Console V4.1

Security White Paper

Revision 1.3

Contents

1 Introduction..4

2 System Configuration 5

2.1 Components.. 6

2.1.1 Manager.. 6

2.1.1.1 Web Application 6

2.1.1.2 Scheduler 6

2.1.1.3 L-CDS 7

2.1.1.4 Database 7

2.1.2 Agent 8

2.1.2.1 Asynchronous Communication Function (poster)... 8

2.1.2.2 Task Controller 9

2.1.2.3 Database 9

2.1.2.4 Protocol Layers 9

2.1.2.5 Manager Public File Caching (cache)... 9

2.1.2.6 Reverser Proxy Function for the L-CDS 9

2.1.3 Device.. 10

3 Managed Data and Communication Specifications 11

3.1 Data Types.. 11

3.2 Details of Each Type 12

3.2.1 Device Information 12

3.2.2 Address Book Data 16

3.2.3 Application Information 16

3.2.4 Device Settings.. 17

3.2.5 Firmware Information 18

3.2.6 Agent Information... 18

3.2.7 LDAP Server Credentials 19

3.2.8 Information Sent by Email 19

3.3 Credentials Used to Communicate With Devices 20

3.4 Data Retention Period 22

3.5 Data Traffic 22
3.5.1 Communication Performed When Using the Basic Functionality 23
3.5.2 Communication Performed When Using the Address Book Management Functionality 25
3.5.3 Communication Performed When Using the Application Management Functionality 25
3.5.4 Communication Performed When Using the Device Settings Management Functionality 26
3.5.5 Communication Performed When Using the Firmware Management Functionality 27
3.6 Ports and Protocols 28
3.6.1 Listening Port and Protocol 28
3.6.2 Communication Performed When Using the Installer 30
3.6.3 Communication Performed When Using the Basic Functionality 30
3.6.4 Communication Performed When Using the Address Book Management Functionality 33
3.6.5 Communication Performed When Using the Application Management Functionaltiy 34
3.6.6 Communication Performed When Using the Device Settings Management Functionality 35
3.6.7 Communication Performed When Using the Firmware Management Functionality 36
4 Information Security Policy and Technical Measures 38
4.1 Confidentiality 38
4.1.1 User Authentication and Access Control 39
4.1.2 Agent Authentication 40
4.1.3 Password Hashing 40
4.1.4 Data Encryption 41
4.1.5 Security Measures Against Malicious Code Attacks 41
4.1.6 Communication Channel Encryption 41
4.2 Integrity 42
4.2.1 Security Measures Against Data Falsification 42
4.2.2 Security Measures Against Malicious Code Attacks 42
4.3 Availability 43
4.3.1 User Authentication and Access Control 43
4.3.2 Security Measures Against Malicious Code Attacks 43
5 Revision History 44

1 Introduction

This paper outlines Canon's approach to security for imageWARE/iW Enterprise Management Console (hereinafter referred to as “iW EMC”).

iW EMC is web-based comprehensive device management software, allowing IT administrators to manage Canon devices such as MFPs and printers efficiently, which leads to reduce the total cost of ownership (TCO) of device management.

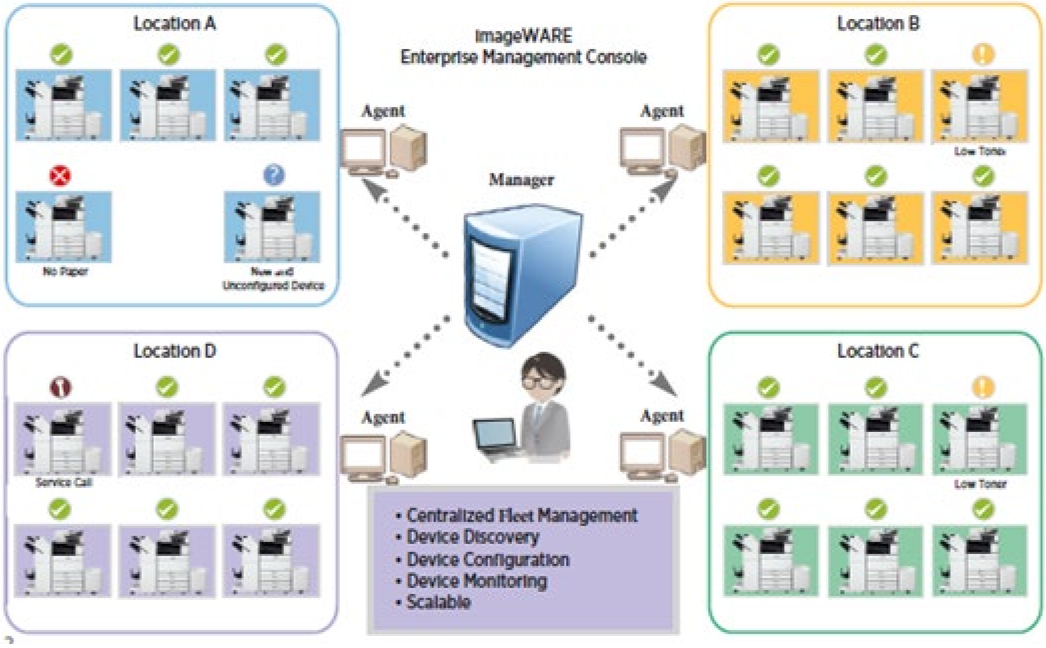
Canon believes that it is crucial to disclose information on data handled by iW EMC and security measures implemented in iW EMC to ensure that our customers can use iW EMC with complete peace of mind.

This paper first gives the overall configuration of iW EMC, and then the types of the data handled, network traffic expected to occur, network protocols, and lastly the security measures implemented in each components of the iW EMC system.

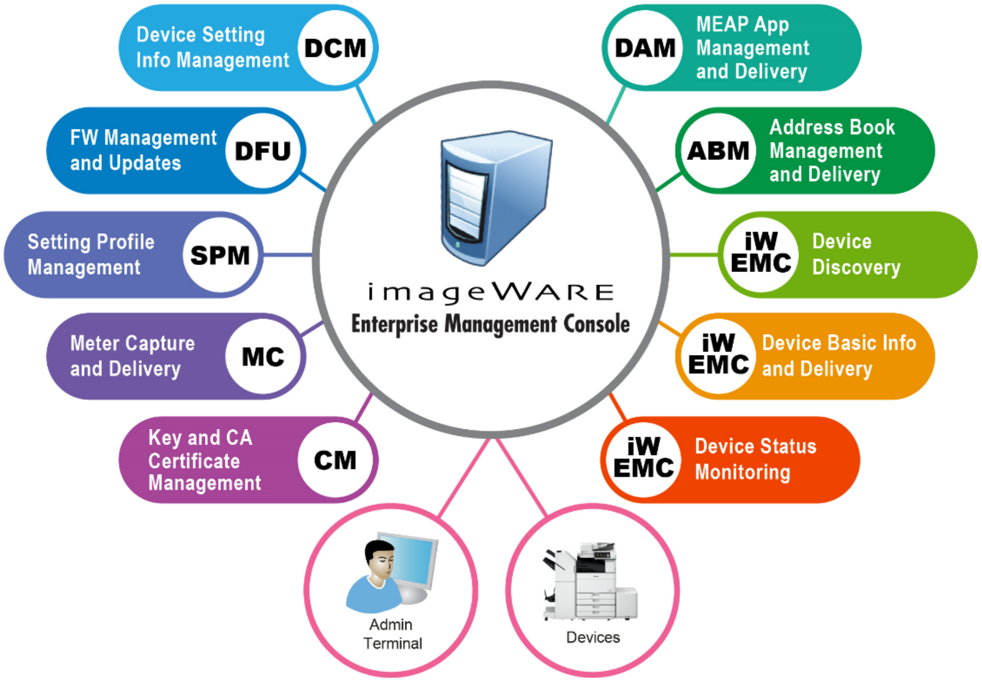
This document is written for our sales companies only. Please do not distribute the document as-is, but read it carefully and modify the contents and expressions to make sure it’s suitable for the customers in your region.

2 System Configuration

Below is the system configuration of iW EMC.



imageWARE Enterprise Management Console v4 Built-in Features


Device Setting Info Management
DCM
FW Management and Updates
DFU
Setting Profile Management
SPM
Meter Capture and Delivery
MC
Key and CA Certificate Management
CM
DAM
MEAP App Management and Delivery
ABM
Address Book Management and Delivery
iW EMC
Device Discovery
iW EMC
Device Basic Info and Delivery
iW EMC
Device Status Monitoring
imageWARE
Enterprise Management Console
Admin Terminal
Devices

2.1 Components

The components of the iW EMC system are described below.

2.1.1 Manager

A Manager is a Windows service controlling the entire system and providing the UI of iW EMC, which consist of:

- WEB application, which provides Web UI
- Scheduler, which allows system to run tasks and/or send notification to Agent automatically.
- L-CDS, the SOAP service which provides reply to firmware renewal request from devices.
- Database

2.1.1.1 Web Application

- The WEB application is integrated with a SMTP server sending notification emails and the iW EMC Online Manual.
- Event notifications to external systems are handled using WebHooks.
- Access rights management with LDAP server, and Single-Sign-On with Integrated Windows Authentication are available.

2.1.1.2 Scheduler

The scheduler scans the database on a regular basis to manage execution of tasks exceeding their deadline and send notifications to Agents.

2.1.1.3 L-CDS

The L-CDS is service which provides Contends Delivery Service in local network. When it received the firmware renewal request from the device, it judges if it’s valid or not, and will reply the specific URL for downloading the firmware if it’s valid.

2.1.1.4 Database

Manager uses the SQLite in the process. The Microsoft SQL Server can be used as an option instead of the SQLite.

2.1.2 Agent

An Agent runs as Windows service, and it consists of:

- Asynchronous communication function to send data to Manager
- Framework to control tasks
- Database to store data temporally
- Protocol library for the communication with devices
- Cache function for public files.
- Reverser proxy function for L-CDS

2.1.2.1 Asynchronous Communication Function (poster)

The poster takes care of asynchronous communication to the Manager with no Response is necessary, such as sending credentials for communication with devices, and sending results of the sub-tasks. The poster receives this type of requests once, and sends them to the Manager asynchronously.

2.1.2.2 Task Controller

It controls the defined tasks based on the iW EMC framework.

2.1.2.3 Database

Asynchronous HTTP requests, and Data retrieved form devices are stored in the database on the agent side. SQLite, which is an in-process database, is used.

2.1.2.4 Protocol Layers

Communication with each device is performed through the protocol layers.

2.1.2.5 Manager Public File Caching (cache)

It is a function that allows files that can be typically retrieved from the public URL of the Manager to be retrieved from the URL of the Agent used for caching purposes. The Agent holds the files for a certain period of time, and returns them according to requests.

2.1.2.6 Reverser Proxy Function for the L-CDS

The reverse proxy receives the queries from devices and forward it to the L-CDS service and also forward the response from the L-CDS service back to the device.

2.1.3 Device

The devices managed by iW EMC will receive the several kinds of requests from iW EMC thru the Agent, such as application install or firmware update. Once the device receive the request, the device is initiated to execute the following process.

- When installing an application and license: The device retrieves application files and a license file from the HTTP/HTTPS server in the Agent by using "Manager Public File Caching".

- When updating firmware: The device sends the request to the L-CDS (in the Manager) thru the Reverse Proxy (in the Agent) for the URL of the firmware file. The L-CDS will reply to the device with the URL of the Public File Caching in the Agent, then device will retrieve the firmware file from there. In case the Agent does not have the requested firmware file in the cache, the Agent will retrieve it from the Manager in background and keep it in the cache so that the device can retrieve it from the Agent.

Note: In cases both of the Agent and the Manager are running in the same PC, and also the device is linked with the Agent, the device will communicate with the Manager directly instead of thru the Reverse Proxy.

3 Managed Data and Communication Specifications

iW EMC retrieves data from customers' devices or computers and so on, and stores it in the database. This chapter describes data types handled, network communications that will be performed, and network protocols to be used.

3.1 Data Types

The data types handled by iW EMC (send/ receive/store) include the following:

- Device information: sent and received between the devices and iW EMC
- Address book data: sent and received by the Address Book Management functionality on iW EMC
- Application information: sent and received by the Application Management functionality on iW EMC
- Device Settings: sent and received by the Device Settings Management function on iW EMC
- (Security policy, key, and certificate data are part of the device settings.)
- Firmware information: sent and received by the Firmware Management functionality on iW EMC
- Agent Information: data about each Agent which is managed by iW EMC
- LDAP server credentials: sent and received between the LDAP Sever and iW EMC when logging in with a LDAP account
- Information sent by Email: sent to a Mail server for an email notification for task results or device errors found during device monitoring
- Information linked with external systems: sent to external systems by iW EMC using the WebHook feature upon occurrence of events.
- Other data: In addition to the above listed data, iW EMC handles the following data: data that is entered in a web browser by users through various functions and stored in a Database server via the iW EMC server. Also data that is, by user operation, read out from the Database server and displayed in the web browser via the iW EMC server. The former data is self-explanatory as it is entered by the users themselves, and the latter data is omitted from This paper because it is generated based on the above listed data, namely: device information, address book data, application information, device settings, firmware information, Agent information, LDAP server credentials, information sent by Email, information linked with external systems, and other data.

3.2 Details of Each Type

The following tables list data used in each function by each data type.

3.2.1 Device Information

Purpose	Data	Data Sent to Device	Data Received from Device
Discover Devices	Data Common to All Device		
	Serial Number	NO	YES
	Manufacturer Name	NO	YES
	Product Name	NO	YES
	IPv4 Address	NO	YES
	Subnet Mask	NO	YES
	Gateway Address	NO	YES
	IPv6 Address	NO	YES
	Hostname	NO	YES
	MAC Address	NO	YES
	Device Name	YES	YES
	Installation Location	YES	YES
	Data Specific to Each Individual Device		
	Number of Color Prints	NO	YES
	Speed of Continuous Print	NO	YES
	Unit of the Speed of Continuous Print	NO	YES

Purpose	Data	Data Sent to Device	Data Received from Device
Retrieve Device Information	Application		
	ID	NO	YES
	Name	NO	YES
	Version	NO	YES
	Device Status	NO	YES
	Need for a License	NO	YES
	Expiration Date	NO	YES
	License Status	NO	YES
	Option		
	Name	NO	YES
	Location	NO	YES
	Type	NO	YES
	Firmware		
	Type	NO	YES
	Name	NO	YES
	Version	NO	YES
	Revision	NO	YES
	Supporting Languages	NO	YES

Purpose	Data	Data Sent to Device	Data Received from Device
Monitor Devices	Device Status		
	Power State	NO	YES
	Counter Value	NO	YES
	Status Message Being Displayed	NO	YES
	Error Information		
	Contents	NO	YES
	Level	NO	YES
	Response Level	NO	YES
	Group	NO	YES
	Group Index	NO	YES
	Elapsed Time	NO	YES
	Contents	NO	YES
	Paper Feeder Information		
	Index	NO	YES
	Name	NO	YES
	Type	NO	YES
	Paper Size	NO	YES
	Amount of Remaining Paper	NO	YES
	Paper Feeding Capacity	NO	YES
	Unit	NO	YES

Purpose	Data	Data Sent to Device	Data Received from Device
Monitor Devices cont’d	Consumables Information		
	Index	NO	YES
	Color	NO	YES
	Type	NO	YES
	Remaining Amount	NO	YES
	Maximum Capacity	NO	YES
	Unit	NO	YES
	Contents	NO	YES
	Finisher Consumables Information		
	Index	NO	YES
	Class	NO	YES
	Type	NO	YES
	Contents	NO	YES
	Remaining Amount	NO	YES
	Maximum Capacity	NO	YES
	Unit	NO	YES

3.2.2 Address Book Data

Purpose	Data	Data Sent to Device	Data Received from Device
Backup Address Book Data	Address List	NO	YES
	Address List One Touch	NO	YES

Purpose	Data	Data Sent to Device	Data Received from Device
Distribute Address Book Data	Address List	YES	NO
	Address List One Touch	YES	NO

Purpose	Data	Data Sent to Device	Data Received from Device
Remove Address Book Data	Address List	YES	NO
	Address List One Touch	YES	NO

3.2.3 Application Information

Purpose	Data	Data Sent to Device	Data Received from Device
Uninstall an Application	License File	NO	YES

Purpose	Data	Data Sent to Device	Data Received from Device
Distribute an Application	MEP Application File	YES	NO
	License File	YES	NO

Purpose	Data	Data Sent to Device	Data Received from Device
Update a License	License File	YES	NO

3.2.4 Device Settings

Purpose	Data	Data Sent to Device	Data Received from Device
Backup Device Settings	Device Settings	NO	YES

Purpose	Data	Data Sent to Device	Data Received from Device
Distribute Device Settings	Device Settings	YES	NO

Purpose	Data	Data Sent to Device	Data Received from Device
Monitor Security Policies	The Number of Rewritings for Security Policies	NO	YES
	Security Policy Settings	NO	YES

Purpose	Data	Data Sent to Device	Data Received from Device
Distribute Security Policies	Security Policy Setting Password	YES	NO
	Security Policy Settings	YES	NO

Purpose	Data	Data Sent to Device	Data Received from Device
Change Security Policy Setting Password	Old Security Policy Setting Password	YES	NO
	New Security Policy Setting Password	YES	NO

3.2.5 Firmware Information

Purpose	Data	Data Sent to Device	Data Received from Device
Update Firmware	Firmware Data	YES	NO
	Device Serial Number	NO	YES
	Firmware Type	YES	YES
	Firmware Version	YES	YES
	Main Controller Version	NO	YES
	UGW Integration Flag	NO	YES
	Enable Scheduled Update Settings	NO	YES
	Language Code	NO	YES
	Country Code	NO	YES
	Region Code for the Device's Location	NO	YES

3.2.6 Agent Information

Purpose	Data	Data Sent to Device
Perform Agent Management	Version	YES
	Status	YES
	IP Address	YES
	Port Number	YES
	Module Version	YES
	Time Zone	YES

3.2.7 LDAP Server Credentials

Purpose	Data	Data Sent to LDAP Server	Data Received from LDAP Server
Connect to an LDAP Server	Domain Name	YES	NO
	User Name	YES	NO
	Password	YES	NO
	List of Groups to which Each User Belongs	NO	YES
Integrated Windows Authentication	Access Token (acquired by Web Browser)	YES	NO
	List of Groups to which Each User Belongs	YES	NO

Note: With the Integrated Windows Authentication, the system acquires the access token from the web browser running on the PC where the login account was authenticated through Windows AD server, and verifies it.

3.2.8 Information Sent by Email

Purpose	Data	Data Sent to Email Server
Configure Email Settings	Sender’s Email Address	YES
	SMTP User Name	YES
	SMTP Password	YES
	Main Body (status information, consumables information, device Information, task information)	YES
	Mail Attachment (counter values)	YES

3.3 Credentials Used to Communicate With Devices

This section describes the credentials that are used for various communications with devices. Actual authentication methods can vary due to factors such as the device type, device settings, device status, and iW EMC configuration. The following are all of the credentials which will be used for each purpose.

- Discover devices
  - SNMPv1 or SNMPv3 read-only access
- Retrieve device information
  - SNMPv1 or SNMPv3 read-only access
  - Canon proprietary protocol
- Retrieve device status
  - SNMPv1 or SNMPv3 read-only access
- Retrieve counters
  - SNMPv1 or SNMPv3 read-only access
  - Canon proprietary protocol
- Backup address book data/ distribute address book data/ remove address book data
  - SNMPv1 or SNMPv3 read-write access
  - Canon proprietary protocol
  - Either user authentication, domain authentication, department ID authentication
- Uninstall an application
  - SNMPv1 or SNMPv3 read-write access
  - Canon proprietary protocol
  - Service Management Service
- Update a license
  - SNMPv1 or SNMPv3 read-write access
  - A Canon specific proprietary protocol,
  - Service Management Service
- Distribute device settings
  - SNMPv1 or SNMPv3 read-write access
  - Canon proprietary protocol
  - Either user Authentication, domain authentication, password authentication, department ID authentication

- Retrieve device settings
    - SNMPv1 or SNMPv3 read-write access
    - User Authentication, domain authentication, password authentication, department ID authentication
- Change password for security policies
    - SNMPv1 or SNMPv3 read-write access
    - User authentication, domain authentication, password authentication, department ID authentication
- Monitor/distribute security policies
    - SNMPv1 or SNMPv3 read-write access
    - Canon proprietary protocol
    - User authentication, domain authentication, password authentication, department ID authentication
- Update firmware
    - SNMPv1 or SNMPv3 read-only access
    - User authentication, domain authentication, department ID authentication

3.4 Data Retention Period

Data retained by iW EMC is deleted at the following timings.

Data	Deletion
Status Information	Delete data which is older than the period set between 30 days to 2000 days. (Default: 100 days)
Task Results	Delete data which is older than the period set between 30 days to 2000 days. (Default: 100 days)
Audit Log	Delete data which is older than the period set between 30 days to 2000 days. (Default: 100 days)

3.5 Data Traffic

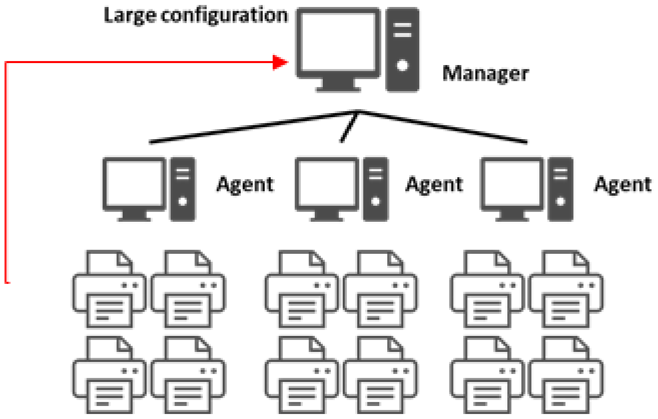
By using iW EMC, the following types of communications are performed among a Manager and Agents, and devices (Communication traffic that occur).

- Communication performed when using the Basic functionality
- Communication performed when using the Address Book Management functionality.
- Communication performed when using the Application Management functionality.
- Communication performed when using the Device Settings Management functionality
- Communication performed when using the Firmware Management functionality

3.5.1 Communication Performed When Using the Basic Functionality

The following table shows the volume and frequency of communication performed against one device by using the Basic functionality. No communication is performed between the device and the Manager.

Purpose	Manager - Agent	Agent - Device	Device - Manager	Frequency
Discover Devices	Approx. 36.7 Kbytes	Approx. 19.1 Kbytes		User-specified frequency
Retrieve Device Status	Approx. 12.7 Kbytes	Approx. 14.8 Kbytes		5 minutes to 1440 minutes (Default: 10 minutes)
Retrieve Counters	Approx. 13.6 Kbytes	Approx. 7.4 Kbytes		1 hour to 24 hours (Default: 4 hours)
Retrieve Device Information	Approx. 26.0 Kbytes	Approx. 40.8 Kbytes		1 day to 20 days (Default: 1 day)



Note: The communications volume will vary according to the device model, the error type, and the number of errors that are occurring simultaneously. Furthermore, the communications volume between Manager - Agent, and between Agent - Device will differ due to difference in the processing or in the protocols used.

In discover devices, the number of packets sent per second to the IP addresses of all devices subject to discovery is proportional to the total number of the numbers shown below:

- The number of SNMP community names configured for each of SNMPv1 read-only access and SNMPv1 read-write access.
- The number of SNMP community strings configured for each of SNMPv3 read-only access and SNMPv3 read-write access.

The number of packets per second is calculated according to the formula below.

30 x (2 x [Total number of community strings configured for SNMPv1/SNMPv3] + 1)

For example, if one community name is configured for SNMPv1 read-write access and two community strings are configured for SNMPv3 read-write access, it is calculated by the following formula:

30 x (2 x 2 + 1) = 150

That means that, about 150 packets are sent per second. The coefficient ”30” can be changed by rewriting a configuration file. The smaller the coefficient value, the longer the discovery time.

3.5.2 Communication Performed When Using the Address Book Management Functionality

The following table shows the volume and frequency of communication performed against one device by using the Address Book Management functionality. No communication is performed between the device and the Manager. The communications volume between the Manager and an Agent, and between the Agent and the device will differ due to difference in the processing or data compression and decompression for address book data. Also, if a communication retry occurs due to the device status or the communication status, the communications volume between the Agent and the device will increase.

Purpose	Manager - Agent	Agent - Device	Device - Manager	Remarks
Retrieve Address Book Data	Approx. 64.8 Kbytes	Approx. 1.1 Mbytes		1600 addresses (max.)
Distribute Address Book Data	Approx. 529.2 Kbytes	Approx. 1.4 Mbytes		1600 addresses (max.)

3.5.3 Communication Performed When Using the Application Management Functionality

The following table shows the volume and frequency of communication performed against one device by using the Application Management functionality. No communication is performed between the device and the Manager. The communication volume depends on the data size of the application to distribute.

Purpose	Manager - Agent	Agent - Device	Device - Manager	Remarks
Distribute an Application	Approx. 33.3 Kbytes	Approx. 73.4 Kbytes		The size of data to distribute is 16.6 Mbytes.
Distribute a License	Approx. 32.7 Kbytes	Approx. 68.6 Kbytes		1 license

3.5.4 Communication Performed When Using the Device Settings Management Functionality

The following table shows the volume and frequency of communication performed against one device by using the Device Settings Management functionality. No communication is performed between the device and the Manager. The communications volume between the Manager and the Agent, and between the Agent and the device will differ due to difference in the processing or data compression and decompression for device settings. The communications volume depends on the data size of the device settings to be distributed or retrieved, and the processing time on the device side.

Purpose	Manager - Agent	Agent - Device	Device - Manager	Remarks
Distribute Device Settings	Approx. 97.3 Kbytes	Approx. 722.7 Kbytes		Settings/registration basic Information only
	Approx. 50.6 Mbytes	Approx. 51.0 Mbytes		The size of data to distribute is 37.1 Mbytes.
Retrieve Device Settings	Approx. 104.0 Kbytes	Approx. 548.9 Kbytes		Settings/registration basic Information only
	Approx. 49.0 Mbytes	Approx. 50.8 Mbytes		Retrieve the 37.1 Mbytes of data that was distributed and back it up.
Retrieve Security Policies	Approx. 26.2 Kbytes	Approx. 103.5 Kbytes		All items
Distribute Security Policies	Approx. 22.5 Kbytes	Approx. 208.8 Kbytes		All items
Retrieve Keys/ Certifications	Approx.100Kbyte	Approx.70Kbyte		Assumption: In case 3 keys and 80 certificates
Add a Key	Approx. 25Kbyte	Approx. 50Kbyte		Assumption: In case 3 keys reside in device, and adding 1 key.
Add a Certificate	Approx.105Kbyte	Approx.200Kbyte		Assumption: In case 3 certificates reside in device, and adding 1 certificate.
Delete a Key and a Certificate	Approx.100Kbyte	Approx. 210Kbyte		Assumption: In case3 keys and 80 certificates reside in device, and adding 1 key and 1 certificate.

3.5.5 Communication Performed When Using the Firmware Management Functionality

The following table shows the volume and frequency of communication performed against one device by using the Firmware Management functionality. No communication is performed between the device and the Manager. The communication volume depends on the data size of the firmware to distribute.

Purpose	Manager - Agent	Agent - Device	Device - Manager	Remarks
Distribute Firmware	Approx. 518.2 Kbytes	Approx. 87.7 Kbytes		The size of data to distribute is approx. 808.0 Mbytes.

3.6 Ports and Protocols

This section provides port numbers and communication protocols used for communications performed through iW EMC for each case.

3.6.1 Listening Port and Protocol

The following table shows the listening ports and protocols of the Manager:

Port No.	Protocol	Network	Purpose
80	TCP	HTTP	WEB Server
443	TCP	HTTPS	WEB Server (encrypted communication)
81	TCP	HTTP	SOAP service of the L-CDS
444	TCP	HTTPS	SOAP service of the L-CDS (encrypted communication)

Note: Each port number can be defined during installation.

The following table shows the listening ports and protocols of the Agent:

Port No.	Protocol	Network	Purpose
10080[1]	TCP	HTTP	WEB Server
8443[2]	TCP	HTTP	WEB Server
10081[1]	TCP	HTTP	SOAP service of the L-CDS
844[1]	TCP	HTTP	SOAP service of the L-CDS (encrypted communication)
11427	UDP	Canon Specific	Receives power status notification from devices

The Agent will uses the port which the OS is not currently using, and will listen the UDP packets when searching Printers and when acquiring device status.

The subsections below describe how each port is used.

[1] Can be changed in Setting file.

[2] Can be defined during installation.

3.6.2 Communication Performed When Using the Installer

The following table shows a port number and a communication protocol to be used for detecting the presence of an external SQL Server.

Port No.	Protocol	Network	Source	Destination	Purpose
1434[3]	UDP	Microsoft SQL Server	Installer	External PC	Detect an external SQL server

3.6.3 Communication Performed When Using the Basic Functionality

The following table lists network protocols and port numbers that are used for the Basic functionality.

Port No.	Protocol	Network	Source	Destination	Purpose
8443	TCP	HTTPS	Manager	Agent	Establish communication between the Manager-the Agent
443	TCP	HTTPS	Agent	Manager	
161	UDP	SNMP	Agent	Device	Discover Devices
Arbitrary port[4] number	UDP	SNMP	Device	Agent	
53	UDP	DNS	Agent	DNS Server	
137	UDP	NetBIOS Name Resolution	Agent	DNS Server	
5355	LLMNR	DNS	Agent	External PC	
161	UDP	SNMP	Agent	Device	Retrieve Device Information

[3] Default value. It follows the database server settings.

[4] An unused port number in an OS will be assigned. (complies with IANA recommendations: 49152-65535) The port number can not be fixed. The Agent waits for reception of a UDP packets through this port number, and instructs the device to return a response to this port number.

Port No.	Protocol	Network	Source	Destination	Purpose
161	UDP	SNMP	Agent	Device	Configure Device Settings
47545	UDP	Canon Proprietary	Agent	Device	Retrieve Counters
161	UDP	SNMP	Agent	Device	Retrieve Counters
161	UDP	SNMP	Agent	Device	Retrieve Device Status
Arbitrary port [5]number	UDP	SNMP	Device	Agent	
47545	UDP	Canon Proprietary	Agent	Device	Retrieve Alert Information
8000	TCP	HTTP	Agent	Device	Retrieve Application Information
8443	TCP	HTTPS	Agent	Device	
161	UDP	SNMP	Agent	Device	Retrieve Option Information
161	UDP	SNMP	Agent	Device	Retrieve Firmware Information
47545	UDP	Canon Proprietary	Agent	Device	
161	UDP	SNMP	Agent	Device	Send a Restart/ Shutdown Command
47545	UDP	Canon Proprietary	Agent	Device	
11427	UDP	Canon Proprietary	Device	Agent	Send a Power State Notification
80	TCP	HTTP	PC	Manager	Use an External API
443	TCP	HTTPS	PC	Manager	
443	TCP	HTTPS	PC	Manager	Access the Manager via Web Browser
80	TCP	HTTP	Manager	Device	Display RUI
8000	TCP	HTTP	Manager	Device	

[5] An unused port number in an OS will be assigned. (complies with IANA recommendations: 49152-65535) The port number can not be fixed. The Agent waits for reception of a UDP packets through this port number, and instructs the device to return a response to this port number.

Port No.	Protocol	Network	Source	Destination	Purpose
8080	TCP	HTTP	Manager	Device	Display RUI
Arbitrary port number	TCP	SMTP	Manager	Mail Server	Send an Email
Arbitrary port number	TCP	SMTPs	Manager	Mail Server	
389	TCP	LDAP	Manager	AD	Perform User Authentication
636	TCP	LDAP over TLS	Manager	AD	
1433[6]	TCP	SQL over TCP	Manager	DB	Access an External SQL Server
1434[6]	UDP	SQL Probe	Manager	DB	

[6] Default value. It follows the database server settings.

3.6.4 Communication Performed When Using the Address Book Management Functionality

The following table lists network protocols and port numbers that are used for the Address Book Management functionality.

Port No.	Protocol	Network	Source	Destination	Purpose
161	UDP	SNMP	Agent	Device	Verify performance /send a restart command/limit data reception for each function
80	TCP	HTTP	Agent	Device	Retrieve/distribute Address lists
443	TCP	HTTPS	Agent	Device	Retrieve/distribute Address lists (encrypted communication)

3.6.5 Communication Performed When Using the Application Management Functionality

The following table lists network protocols and port numbers that are used for the Application Management functionality.

Port No.	Protocol	Network	Source	Destination	Purpose
10080	TCP	HTTP	Device	Agent	The device retrieves an application/license from the Agent
8443	TCP	HTTPS	Device	Agent	The device retrieves an application/license from the Agent (encrypted communication)
80	TCP	HTTP	Device	Agent	The device retrieves an application/license from the Manager
443	TCP	HTTPS	Device	Manager	The device retrieves an application/license from the Manager (encrypted communication)
443	TCP	HTTPS	Agent	Manager	The Agent retrieves an application/license from the Manager (Cache)
8000	TCP	HTTP	Agent	Manager	To distribute /delete /start /stop the application /license
8443	TCP	HTTPS	Agent	Device	To distribute /delete /start /stop the application /license (encrypted communication)
161	UDP	SNMP	Agent	Device	To reboot the device

Note: In cases both of the Agent and the Manager are running in the same PC, the device will communicate with the Manager directly.

Note: Refer to the following section "Communication Performed When Using the Device Settings Management Functionality" for the distribution of the CA certificate to the device.

3.6.6 Communication Performed When Using the Device Settings Management Functionality

The following table lists network protocols and port numbers that are used for the Device Settings Management functionality.

Port No.	Protocol	Network	Source	Destination	Purpose
161	UDP	SNMP	Agent	Device	Verify the performance of device settings management /send a restart command
80	TCP	HTTP	Agent	Device	Retrieve/distribute device settings
8000	TCP	HTTP	Agent	Device	
443	TCP	HTTPS	Agent	Device	Retrieve/distribute device settings (encrypted communication)
8443	TCP	HTTPS	Agent	Device	

3.6.7 Communication Performed When Using the Firmware Management Functionality

The following table lists network protocols and port numbers that are used for the Firmware Management functionality.

Port No.	Protocol	Network	Source	Destination	Purpose
10081	TCP	HTTP	Device	Agent	Query about firmware from the device to the Agent
8444	TCP	HTTPS	Device	Agent	Query about firmware from the device to the Agent (encrypted communication)
10081	TCP	HTTP	Device	Manager	Query about firmware from the device to the Manager
8444	TCP	HTTPS	Device	Manager	Query about firmware from the device to the Manager (encrypted communication)
444	TCP	HTTPS	Agent	Manager	Query about firmware from the Agent to the Manager (Reverse proxy)
10080	TCP	HTTP	Device	Manager	The device retrieves the firmware from the Agent
8443	TCP	HTTPS	Device	Agent	The device retrieves the firmware from the Agent (encrypted communication)
10080	TCP	HTTP	Device	Manager	The device retrieves the firmware from the Manager
8443	TCP	HTTPS	Device	Manager	The device retrieves the firmware from the Manager (encrypted communication)
443	TCP	HTTPS	Agent	Manager	The Agent retrieves the firmware from the Manager (Cache)

Port No.	Protocol	Network	Source	Destination	Purpose
80	TCP	HTTP	Agent	Device	Update firmware
8000	TCP	HTTP	Agent	Device	
161	UDP	SNMP	Agent	Device	
443	TCP	HTTPS	Agent	Device	Update firmware (encrypted communication)
8443	TCP	HTTPS	Agent	Device	

Note: In cases both of the Agent and the Manager are running in the same PC, the device will communicate with the Manager directly.

Note: Refer to the previous section "Communication Performed When Using the Device Settings Management Functionality" for the distribution of the CA certificate to the device

4 Information Security Policy and Technical Measures

We shall take appropriate information security measures for the protection of data handled by iW EMC, which is considered information assets.

From the viewpoint of the three information security components: Confidentiality, Integrity, and Availability, this chapter provides our information security policies and technical measures to protect information assets.

4.1 Confidentiality

Confidentiality in iW EMC is to help ensure that only authorized users access information assets.

The information security policies related to confidentiality are as follows.

- iW EMC manages authorized users appropriately, and ensures that only authorized users or systems are allowed to access information assets.
- We shall take appropriate measures designed to prevent data leakage that occurs on communication channels via a web browser.

The following subsections describe technical measures that are taken pursuant to the above policies.

4.1.1 User Authentication and Access Control

When accessing iW EMC via the web browser, the login screen is displayed and access to iW EMC is controlled using registered user accounts of iW EMC or registered users of LDAP. Users are assigned roles, and access to resources or operations is restricted based on the assigned roles. The table below provides the list of roles.

Role	Description
Admin	The Admin role has permissions to use all functions and to perform management of the iW EMC system. It can configure the settings associated with system operation (ex. Mail server settings), create/delete users, create/delete Agents, and add/remove functions.
Manager	The Manager role performs device management. It can configure the settings associated with devices and create/edit tasks.
User	The User role has permissions to view a list of devices and to view reports. It cannot rewrite data stored in iW EMC.

When logging in from the login screen, subsequent connections are authenticated using tickets stored in cookies.

Note: A Web API is used for communication between the web browser and iW EMC. You can also use basic authentication for calling the Web API. In doing so, the access can be restricted based on the above roles.

4.1.2 Agent Authentication

A secure communication can be established between a Manager and an Agent with HTTPS encryption.

Mutual authentication between the Manager and the Agent is performed as follows.

- The Agent contains a byte sequence which is made up of random digits, and it is shared with the Manager.
- The HTTP request sender calculates the hash value of specific header information using the byte sequence, and stores the hash value calculated in the HTTP header together with information that is used to identify the Agent.
- The receiver of the HTTP request extracts the information that is used to identify the Agent from the HTTP header and calculates its hash value, and then determines whether the hash value it has just calculated and the hash value stored in the HTTP header are matched.

4.1.3 Password Hashing

A user login password contains a salt composed of random digits and SHA-256 hash for the password with the salt added. During user authentication upon login, iW EMC appends the above salt to the password entered by the user and calculates its SHA-256 hash, and then determines whether the SHA-256 hash contained in the password and the SHA256 iW EMC has just calculated are matched.

4.1.4 Data Encryption

For storing confidential information such as credentials in the database, a key is created using a UUID, which is generated on a per Manager or Agent basis, and the string the user input, and then encryption using AES encryption algorithm (256 bits) is performed.

When the user is required to enter confidential information into the web browser such as when changing the password character strings which were specified through the UI, special characters will be sent to the web browser instead of sending the confidential information as it is.
(The password character strings are displayed as ”*******” in the web browser.)

4.1.5 Security Measures Against Malicious Code Attacks

iW EMC contains features to help detect and defend against malicious code attacks to prevent leakage of user credentials and customer data. For avoiding various attacks such as SQL injection, a Web API created with ASP.NET Core Entity Framework is used for accessing the database.

Also, validations can be performed using JavaScript both on the server side (web server) and on the client side (web browser), to prevent incorrect data from being entered by users.

4.1.6 Communication Channel Encryption

In iW EMC, HTTPS is used for secure communication between the Manager and each Agent. If HTTP is specified as a protocol, it is redirected to HTTPS.

Note: When updating firmware or obtaining applications/ licenses, devices communicate with iW EMC via HTTP to access required resource, and for such communication, an HTTP to HTTPS redirection is not performed.

4.2 Integrity

Integrity in iW EMC means that data is consistent, accurate, and accessible.

The information security policies related to integrity are as follows.

- iW EMC validates whether a communication destination is correct when information assets are sent and received.
- iW EMC validates that the stored information assets are accurate and complete.

The following subsections describe technical measures that are taken pursuant to the above policies.

4.2.1 Security Measures Against Data Falsification

As described in ”Data Encryption”, data handled by iW EMC is encrypted by using a common key and it will be stored together with the common key itself which is also encrypted, in the database. Furthermore, SSL is recommended for a communication channel via a web browser, and data that is sent and received by Web services is encrypted by a public key. Also, user operations executed from the web browser are logged to the system log.

4.2.2 Security Measures Against Malicious Code Attacks

iW EMC contains features to help detect and defend against malicious code attacks to prevent falsification of device information. For avoiding various attacks such as SQL injection and session hijacking, iW EMC uses forms authentication provided by ASP.NET Core and changes a session ID at each login.

Note: Session hijacking - A web attack taking over an ongoing active session between two communication end points over a network to gain unauthorized access to information or operations by pretending to be one of the communication end points.

4.3 Availability

Availability in iW EMC means that information assets are reliably available for access whenever users require.

The security policy related to availability is as follows.

- iW EMC allows authorized users to access the system whenever necessary.

The following subsections describe technical measures that are taken pursuant to the above policy.

4.3.1 User Authentication and Access Control

As described in “User Authentication and Access Control“, iW EMC authenticates users attempting to login and performs access control according to the assigned roles.

4.3.2 Security Measures Against Malicious Code Attacks

As described in “Security Measures Against Malicious Code Attacks“, to help avoid various attacks such as SQL injection in iW EMC, the NET Core Web API for sanitizing is used. In addition, validations checks are performed. These are designed to detect and defend against attacks that trick a user who accessed iW EMC into navigating to a malicious website or make it difficult for the user to get access to your data.

5 Revision History

Revision	Changed Contents	Author
1st Edition	1st Edition Published	CUSA