



iW Management Console



White Paper

August 2006

White Paper Version: 1.02

Contents

1. Canon's Device Management	3
2. Product Overview	4
2.1. Product characteristics	4
2.2. Function overview	4
2.3. Target user	6
3. Installation	7
3.1. Device search	7
3.2. Device setting	10
3.3. Device monitoring	13
3.4. Setting for the device address book	16
3.5. Delivery of the printer driver	19
4. Use Case and Introduction Effect	22
5. Technology	24
5.1. Technical feature	24
5.2. Plug-in structure	24
5.3. Security	25
5.4. Communication protocol and port number	26
5.5. Network traffic	31
6. Environment	32
6.1. Operating environment	32
6.2. Supported device	34

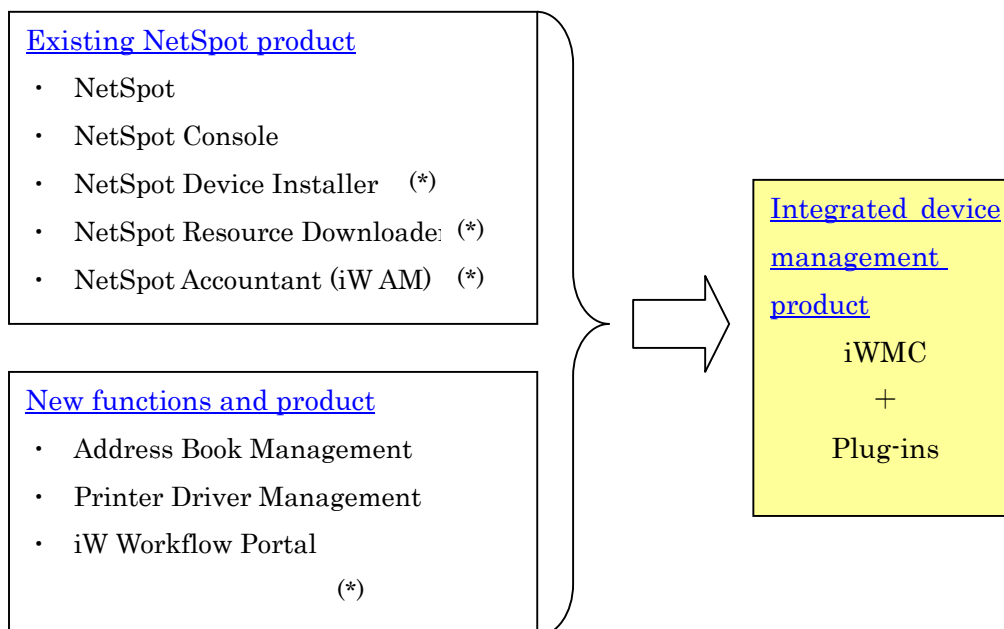
1. Canon's Device Management

Canon has involved in the device management from the early stage and provided NetSpot series as its flagship. In response to customer requests, Canon currently offers a variety of NetSpot lineup due to lineup enhancement.

When we considered the product from the customer's viewpoint, however, we also found new challenges.

- Products are categorized by function, which may bring burdens to IT administrators who try to manage the entire system. In addition, it might be difficult for them to decide which product to use for the specific use.
- IT environment is changing with dramatic speed, which diversifies customer needs as well. Even if some function is enough at some point, further enhancements will be required in the future. In order to meet these diversified customer needs, continuous function additions are required.

Considering these conditions, the idea of an integrated device management product, which combines "simplicity" and "function enhancement", has emerged and resulted in the planning of "iW Management Console". This white paper describes "iW Management Console V1.0.0 and V1.1.0".



(*) Plan to support sequentially by later versions.

2. Product Overview

2.1. Product characteristics

The iW Management Console (described as iWMC later in this white paper) is a Web-based integrated device management software. IT administrators effectively manage devices such as MFP and printer by using the following functions provided by iWMC, which enables a reduction of TCO of device management.

Not only Canon's devices, but also competitor's printers that support standard MIB are supported, which enables the acquisition and display of the information.

A series of device management settings can be registered as tasks by iWMC. Execution time and interval can be specified for the registered tasks; therefore, settings which require time and those which cannot be executed while the device is operating during the day will be executed during the night, and users can also receive the result via e-mail. These functions dramatically reduce the operation time of IT administrators. One of the functionalities of setting tasks is being able to edit or reuse them after they have been created.

2.2. Function overview

2.2.1. Device search

Search devices connected to the network and store them to the database of iWMC. Stored device information can be used for the classification of devices and filtering. When a new device is installed, it is possible to search for the device by specifying the device's IP address and add its device to the database.

2.2.2. Device setting

The device information such as a device name and installation site and the network settings such as an IP address and subnet mask address can be set to the searched device. If devices are classified by group, device settings within the same group can be set in one single operation.

2.2.3. Device monitoring

Obtain device information periodically and display the obtained device information as a list. When an administrator's e-mail address is set, errors will be sent to the

administrator in the case of an error occurring. A day of the week, time, and error types (such as a paper jam and toner replacement) to be monitored can be specified in details.

2.2.4. Device address book setting

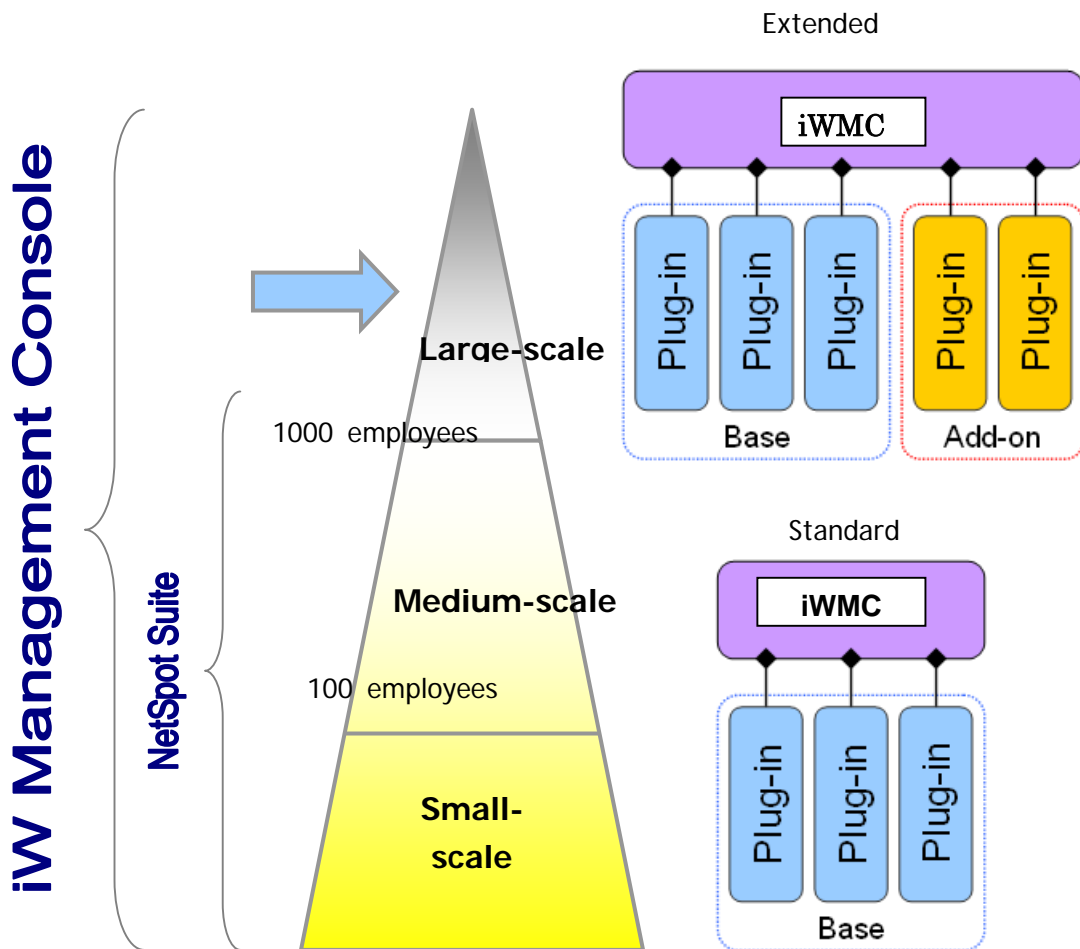
Fax numbers to be used for fax and send and an address book for e-mail address can be controlled by the MFPs. It is possible to obtain an address book from the device, which already has set addresses, and distribute it to multiple devices after editing as needed. E-mail addresses can also be imported from Lotus Notes and Microsoft Exchange and set to the device.

2.2.5. Installation of printer driver

Push installation is supported to install a printer driver from iWMC to each client PC. Pull installation is also supported to install a printer driver by accessing to the iWMC via web browser from each client PC and selecting a driver.

2.3. Target user

iWMC targets a large-scale enterprise, which cannot be supported by the conventional NetSpot Suite, and effectively manages a large number of devices by providing group functions, filtering functions, and simultaneous setting functions for multiple devices. A plug-in structure enables separate installation of required functions accordance with user's environment as needed.



3. Installation

3.1. Device search

3.1.1. Device search method

The followings are search methods provided by iWMC

- IP broadcast search
- IP addressing search
- Search by NetBIOS name or DNS name
- Multicast search

“IP broadcast search” executes broadcast search by using SNMPv1 protocol. Network type can be specified either from “Search within local network” or “Search within specified network”.

“Search within local network” (example: “255.255.255.255”) enables search for devices connected to the same network with the PC that installed iWMC. “Search within specified network” (example:” 172.24.255.255”) enables search for devices connected to the specified network.

This search method is appropriate for the environment where the number of managed devices is between 100 and 200 and broadcast packet can be used within the network.

“IP addressing search” executes search for the device with specified IP address by using SNMPv1 protocol. There are three types of IP address specification methods: “IP address direct specification”, “IP address range specification”, and “IP address import from a file”.

“IP address direct specification” directly specifies the IP address for the target device, such as “172.24.93.164”. “IP address range specification” specifies the range of IP address with hyphen such as “172.24.16.1-172.24.16.255”, and search the device within the range. “IP address import from a file” enables import of IP address list of target addresses from a CSV file.

This search method is appropriate when the IP address of the target device is fixed, when the number of target devices is several hundreds, or when the broadcast packet cannot be used within the network.

Please note: when the number of target devices is several hundred, the search time

will take several minutes or hours.

When creating multiple tasks for the device search, adjust start time so as not to overlap execution time.

“Search by NetBIOS name or DNS name” executes search for the device specified with NetBIOS name or DNS name. Specify the device name, for instance, either “devname” or “devname.abc.com”.

iWMC obtains the device IP address specified with NetBIOS name or DNS name by doing a name resolution and then obtain the device information from the IP address through SNMPv1 protocol.

This search method is appropriate when target devices are managed by NetBIOS or DNS name.

“Multicast search” executes multicast search by SLP protocol. According to the network settings, it is possible to search the device within a certain range where multicast packet can reach.

As an optional setting, the number of hops (TTL), the number of routers the multicast packet will go through, can be specified. Specify an appropriate value according to the settings of router on the network. In addition, a scope name can be specified by SLP protocol. If the scope name for the target device is changed, specify an appropriate scope name.

This search method only applies to searching for Canon’s devices. This search method is appropriate when only Canon’s devices are targeted for management, when the number of target devices is between 100 and 200, and when multicast packet can be used on the network.

When a different search method other than “Multicast search” is specified; “Community name specification” and “Search for device compatible with standard MIB” can be specified as an option. A community name that is used by SNMPv1 protocol can be specified for “Community name specification”. The same community name set to the target device has to be specified.

“Search for device compatible with standard MIB” specifies whether the search applies to devices compatible with standard MIB other than Canon devices.

3.1.2. Device search task creation

Follow the following procedures for the device search task creation.

- (1) Select “Device search task creation” from “Device search/management” on the menu.
- (2) Select the most appropriate search method for the network from the previous methods. Multiple search methods can be specified.
- (3) Specify the task name and the time to start a search.
For example, select “Execute search periodically” and set the date and time by selecting a month from the execution cycle combo box when you execute device search once a month at night and update the list of target devices.
- (4) Check the task and register it.

After registration, iWMC schedule function executes a device search automatically. The result of the task execution can be confirmed by “Execution task list” from “Device search/management”.

The searched device list can be confirmed either “Device list” from “Device monitoring” or “Device search result management” from “Device search/management”.

3.2. Device setting

3.2.1. Setting item

The following item values can be set all at once for multiple devices by iWMC.

Device information

Device name	User friendly name of the device
Installation site	Location of the device
Administrator name	Administrator name of the device
Contact information of administrator	Contact information of the device administrator
Comment on administrator	Additional information on the device administrator
Name of service person	Name of the device service person
Contact information of service person	Contact information of the device service person
Comment on service person	Additional information on the device service person

TCP/IP protocol setting

Frame type	Frame type
Address setting by DHCP	Address setting by DHCP (ON/OFF)
Address setting by BOOTP	Address setting by BOOTP (ON/OFF)
Address setting by RARP	Address setting by RARP (ON/OFF)
The number of IP address *1	Set IP address, which is set to the IP address pool, to the device
Setting	The "IP address setting" page to create IP address pool is displayed when clicking
Subnet mask	IP address to be set to the device as subnet mask
Gateway address acquisition method	Gateway address acquisition method (Auto/Manual)
Gateway address	IP address to be set to the device as gateway address
LPD print service	LPD print service (ON/OFF)
LPD banner	LPD banner setting (ON/OFF/Auto)

RAW port	RAW port (ON/OFF)
RAW mode two-way communication	RAW mode two-way communication (ON/OFF)
IPP	IPP setting (ON/OFF)
Primary DNS server address	IP address to be set to the device as primary DNS server address
Secondary DNS server address	IP address to be set to the device as secondary DNS server address
DNS dynamic update	DNS dynamic update setting (ON/OFF)
DNS host name *2	Name to be set to the device as DNS host name (accept up to 57 one-byte characters)
DNS domain name	Name to be set to the device as DNS domain name (accept up to 64 one-byte characters)
SNTP server	Name to be set to the device as SNTP server name (accept up to 255 one-byte characters)

Device information delivery setting

Address book reception restriction function *3	Set either Valid (ON) or Invalid (OFF) for the address book reception restriction function
--	--

- *1 When the check mark is set to either [Address setting by DHCP], [Address setting by BOOTP], or [Address setting by RARP], and “ON” is selected, [The number of IP address] cannot be selected.
- *2 In order to avoid duplication of the DNS host name, the last 6 characters of the device MAC address will be added after the input DSN host name automatically.
- *3 When delivering the address book, “Address book reception restriction function” should be valid in advance.

In order to set IP address to the device, the IP address pool should be created in advance. If “IP addresses for the target devices to be managed by iWMC” or “IP addresses for the devices, which are already used within the network” are included in the IP address pool, these IP addresses cannot be set to the device by iWMC.

Device reboot is required to validate the change of “TCP/IP protocol setting” except some exception. Specify the device reboot when registering a task or create a task to reboot the device.

3.2.2. Device group utilisation

The device group can be specified to the target by the device setting management task. If the target device is not fixed yet when creating a task, it is convenient to create a blank device group and specify it to the target. When the target device is fixed, add its target device to the previously specified device group.

If the devices with the same authentication information are managed by group unit, a task can be easily created by its group unit.

3.2.3. Authentication information sharing

The device authentication information inserted the user, whilst creating tasks for the purpose of device settings (device settings and device reboot), are stored in iWMC. Therefore, when a user creates a task for device settings, re-entry of user authentication is not required for the same device, as the user authentication is already stored in iWMC.

3.2.4. Success and failure measurement of a task

iWMC measures success and failure of a device setting delivery task based on the following requirements.

Device setting delivery task

Condition for the failure	When setting items implemented to the device cannot be delivered or when none of the information defined by the device setting delivery task for the target device is delivered.
Condition for the success	Other than the above conditions

Device setting acquisition task

Condition for the failure	When setting items implemented to the device cannot be delivered or when none of the information is obtained from the iWMC.
Condition for the success	Other than the above conditions

Device reboot task

Condition for the failure	When a device cannot be rebooted
Condition for the success	Other than the above conditions

As shown in the above, success and failure of the task depends on the implementation of the device.

3.3. Device monitoring

3.3.1. Display of monitoring result

Execution results of monitoring conditions are reflected in the device list when updating the display. In case of the iWMC 1.0, the icon changes indicating the device changes, while the status icon and the status message are replaced with iWMC 1.1.

With devices which are not selected as a target device for monitoring, the information will not be changed unless it is actually updated by a user. In order to maintain the latest device list information, it is required to specify all devices displayed on the device list for the monitoring target.

3.3.2. Grey-out display of the device

Immediately after reading the information from a CSV file, or when the target device for monitoring fails the communication, the device list information is greyed out.

Due to the lack of device information, which is shortly after reading from a CSV file, it is impossible to specify for the target of a task, which can be created by the iWMC.

As for the greyed out device due to reading information from a CSV file, the device can be activated by updating device information from the device list.

When the device specified for the monitoring fails communication, it will be changed to the grey out display; however, even if the device other than the monitoring target fails communication, it will not be greyed out.

3.3.3. Filter

Filtering function can be applied to narrow down the list of the items displayed on the device list.

For example, in order to apply filter to the item displayed on the “device name” of the device list, the filter item named “device name” of the filter is used.

Firstly, check the check box of “device name” of the filtering item, and input string of the device name, which requires filtering, to the “device name” text box of the filtering item. Lastly, click the “apply” button of the upper part of the filter and then the filter is applied. When the input string is matched with one part of the actual device name, the device name is displayed on the device list after filtering.

When multiple filter items are checked, only devices that satisfy input conditions to the checked filter items are displayed on the device list after filtering.

3.3.4. E-mail notification

The result of the device monitoring is sent to the administrator via e-mail.

Either one of the following two or both can be selected for the e-mail format to be sent.

- Standard format
- Format for mobile terminal

A simplified “standard” format email is sent in a format suitable for mobile terminals.

An e-mail that simplified the e-mail to be sent by “standard format” is sent with “format for mobile terminal”.

The difference between “standard format” and “format for mobile terminal” is only whether there is a limit for the number of characters for an e-mail to be sent (format for mobile terminal) or not (standard format). In either way, an e-mail is sent by the monitoring target device.

If there is no change for errors occurred in the monitoring target device, iWMC does not send an e-mail.

3.3.5. Creation of monitoring conditions

When monitoring the device status, execute the following procedures.

- (1) Select the target device to monitor the status.
- (2) Set the error condition to send notification via e-mail and the period for the status monitoring.
- (3) Set the name for the monitoring condition and the destination to send the monitoring result.

In the above second procedure, unnecessary e-mail delivery on holidays or during out-of-hours can be prevented by setting “monitor day” and “monitor time” for the “monitor period” properly.

In the above third procedure, it is possible to select from two types of notifications for monitoring the result: “standard format” or “format for mobile terminal”. It is also possible to create the monitoring condition that does not send any e-mail by not selecting any format. In this case, the monitoring result of the target device status is

not sent via e-mail, but reflected in the device list. Periodical update of the device list display allows an administrator to monitor the device status.

iWMC executes polling for the individual monitoring target devices to monitor their status with a 10-minute interval. However, when a PC spec that operates iWMC is lower, or when a computer is under high load by operating multiple monitoring conditions with one PC, the polling interval for individual monitoring target devices may exceed 10 minutes.

3.4. Setting for the device address book

Additional installation of the Device Address Book Management Plug-In enables delivery to the destination via network to multiple devices.

3.4.1. Import of the address book from outside

By utilising the device's address book management function, the address book can be imported from outside. The data format of importable address book is as follows.

- Microsoft Exchange Server (5.x/2000)
- Lotus Notes (4.x/5.x)
- Extended LDIF format
- CSV format

Refer to the help for iWMC for the data format when importing the "CSV format" address book.

In addition, "extended LDIF format" (extension is ".abk" (Canon Address Book)) is the designated format to exchange address book data among devices and enables import of the data to devices by using the remote UI.

3.4.2. Export of the address book to outside

By utilising the device's address book management function, the address book can be exported externally. The data format of exportable address book is only in an "extended LDIF format".

3.4.3. Acquisition of data from the device

In order to get the address book from the device, SSL setting is required at the device side in advance. It is also required to turn off the receiving restriction function for the address book.

Receiving restriction function of the address book can be controlled from iWMC device setting management of the device main unit panel.

The following procedures are performed to get the address book from the device.

- (1) Select the source device to retrieve the address book.
- (2) Input authentication information of the target device selected in the step (1) and specify the address book to retrieve.
- (3) Click the "Execute" button.

Only one device can be selected in step (1).

If a wrong target device authentication information is inserted in the step (2), it may fail in retrieving the address book. Verification whether the authentication information is correct is recommended by clicking “test authentication” button after inputting the authentication information.

Retrieving the address book will be executed immediately; therefore, when a large number of addresses are included in the address book to be retrieved, it would require quite some time to complete the transfer of the address book.

When it succeeds in retrieving the address book, the display will shift to the edit page of the address book. When the display shifts to the edit page of the address book, the retrieved address book information has already been stored to the database.

If there are multiple address books, it is required to retrieve the address book one by one.

3.4.4. Creation of address book delivery task

In order to deliver the address book to the device, SSL setting is required at the device side in advance. It is also required to turn off the retrieving restriction function for the address book

Retrieving restriction function of the address book can be controlled from iWMC device setting management of the device main unit panel.

The following procedures are performed to deliver the address book to the device.

- (1) Select the destination device to deliver address book.
- (2) Input authentication information of the target device selected in the step (1).
- (3) Select the address book to deliver.
- (4) Set the task name and its schedule.

In the step (1), multiple devices can be selected. When the same values are set to “system administrator ID” and “password” for target devices, the same “system administrator ID” and “password” can be applied to all the target devices by inputting “system administrator ID” of “authentication information collective setting for multiple devices” and “password” and then clicking the “set selected devices” button in the

step (2). If the same values are set to “system administrator ID” and “password” for multiple devices, however, the security strength will decrease. Therefore, change the operation according to the environment.

If wrong target device authentication information is input in the step (2), it may fail in the delivery of the address book. Verification whether the authentication information is correct is recommended by clicking “test authentication” button after inputting the authentication information.

The address book delivery function enables setting of the delivery schedule.

3.5. Delivery of the printer driver

Additional installation of the Printer Driver Installation Plug-in enables single management of the entire printer drivers to be installed to client PCs by the iWMC.

3.5.1. Two ways of the printer driver delivery

There are following two ways to deliver a printer driver.

- Push installation

The way to install the printer driver remotely by using the single task from iWMC to multiple client computers.

- Pull installation

The way to install the desired printer driver manually by accessing iWMC from each client computer.

“Push installation” is an appropriate installation method when an IT administrator needs to manage the rollout of printer drivers to each client computer. Task processing enables installation of a printer driver at night.

On the other hand, “pull installation” is an appropriate installation method when an IT administrator does not want to spend much time for management. This method reduces burden for the IT administrator because a user of each client computer installs a desired printer driver manually from the printer driver list that was been prepared by the IT administrator in advance. However, when the number of client computer is large, an operation to avoid access concentration is required.

3.5.2. Establishment of FTP server (for both Push and Pull installation)

The printer driver to for delivery is stored on an FTP server. Firstly, specify the FTP server to use as a storage location of the printer driver after installation of the Printer Driver Installation Plug-in.

The FTP server can either be created on the iWMC server computer or on a different server on the customer network. Both types of FTP configurations are acceptable. Established FTP server can be activated by specifying IP Address, Port Number, Virtual Directory Name, User Name, Password, and Transfer Mode (Passive or Active) by the iWMC.

3.5.3. Registration of the driver set (for both Push and Pull installation)

The printer driver to be delivered should be registered to the FTP server in advance. As to the upload of the printer driver, download a driver upload tool “Driver Set Uploader” by using the iWMC from the client computer of an IT manager. Registration of the printer driver to be uploaded can be performed by specifying the Setup.exe of each driver installer from the “Driver Set Uploader”.

3.5.4. Creation of association (for both Push and Pull installation)

The registered driver set is associated with the searched device by a search function. Desired name can be applied to the association. Installation of the printer driver can be executed by selecting the association when creating a task in case of the push installation and by selecting the desired association by a client computer for the pull installation.

3.5.5. Agent installation (Push)

In order to execute a push installation, the agent service should be installed into a client computer to deliver the printer driver in advance. Communication between the agent and iWMC enables a client computer to download the printer driver from the FTP server and install it.

The following 3 methods are provided to install the agent to a client computer.

- Task installation
For Windows 2000 client except Windows XP Home Edition
- Quick installation
For Windows 2000 client except Windows XP Home Edition
- Manual installation
For all clients including Windows 9x and Windows XP Home Edition

“Task installation” is an appropriate installation when the number of client computer to install the agent is large. It is possible to install the agent into multiple client computers with a single task.

“Quick installation” is an appropriate installation when the number of client computer to install the agent is small. Installation of the agent is executed by each client computer.

“Manual installation” is to install the agent by connecting to the iWMC from each client computer, downloading the execution file to install the agent, and executing its execution file by each client computer.

As for “task installation” and “quick installation”, it is required to install and register

the information on client computers to be selected by CSV file in advance.
Registered client computers can be managed by group in the same manner with the device group, which enables installation of the agent by group.
Installation of the agent can be executed by the user ID and password with administrative privileges of the client computer (domain administrative privileges in the case of the domain).

3.5.6. Task creation (Push)

There are following two functions for the task regarding the push installation.

- Agent task installation
- Printer driver delivery installation

“Agent task installation” is the function to deliver the agent by a task as described in “Agent installation (Push)”.

On the other hand, “printer driver delivery installation” is executed as a task of the iWMC by selecting a client computer or device, selecting the information associated with the selected client computer or device (refer to the previously described “Creation of association (for both Push and Pull installation)”), and scheduling a task.

4. Case examples and iWMC Openings

Case1	In the past, MFP and LBP were managed by the administrative division, however, currently; all devices connected to the network are managed by the IT division. The administrative division hired temporary employees and placed them for the device management. Nowadays, however, the cost reduction is intense, which makes it difficult to hire new temporary employees at the IT division. It is an urgent issue that output devices on the network need to be managed efficiently.
Solution	Established the help desk to control the entire devices by the center console. As for the incidents such as running out of toner or paper, users can deal with the matters by receiving phone calls from the person who is in front of the center console at site.
Introduction effect	Jobs conducted by temporary employees with labor-intensive method can be dealt with a few numbers of employees at the help desk, which reduces the burden of IT administrators.

Case 2	At the time of replacement of PC and MFP, the IT administrator made a plan, but found out the following workload would increase dramatically. <ul style="list-style-type: none"> • Installation of the printer driver to each client PC • Import of the address book to each MFP
Solution	Group MFPs and import the address book by group with single task. Group client PCs and execute push installation by group with single task as well.
Introduction effect	Centralized management by the IT administrator enables distribution of the MFP's address book and delivery of the printer driver to each client PC, which dramatically decreases workload of the IT administrator. Use of the group function also reduces workload of the IT administrator. A few inquiries from each client user also contribute to workload reduction of the IT administrator.

Case 3	After the installation of the color MFP, the volume of color print has increased more than expected, which causes cost increase. One of the factors seems to be the fact that even black and white documents are printed in color mode.
Solution	Reduce the color print cost by customising the default value of the printer driver to make black and white print default. Customised driver can be distributed by iWMC. By utilising its customized driver, change of the default value is thoroughly applied to all users.
Introduction effect	Unexpected color print by users will almost be prevented, which will reduce the print cost.

Case 4	Editing of the MFP's address book becomes burden for the IT administrator every time the organisation is changed.
Solution	Import the address book of Lotus Notes and MS Exchange, which is managed as the master, to iWMC. Set the task to deliver the address book during the night when MFP is not used by users.
Introduction effect	Maintenance burden will be decreased dramatically since the IT administrator does not have to exercise dual management of the address books. The delivery of the address book during which users do not use MFP allows users not to stop their work or will not decrease user's working efficiency as well.

5. Technology

5.1. Technical feature

iWMC has been developed based on the .NET Framework technology which has been introduced into the latest Windows system. Utilisation of the .NET Framework technology recognises multi lingual languages due to satellite assembly and implementation of the UI by using Web control provided by ASP.NET.

Standard SNMP, which is the protocol for the device management, and standard web service including XML and SOAP for the web-based system are used for the communication between iWMC and devices. In addition to the utilisation of the standard MIB such as MIB II, Printer MIB, and HOST RESOURCES MIB, which are defined by the RFC, Canon MIB, which is the extended protocol developed by Canon, is used for the SNMP protocol, which enables support of full items to manage devices. It is possible to search and monitor devices manufactured by competitors as long as these devices support the standard MIB.

5.2. Plug-in structure

iWMC adopted a plug-in structure which allows addition of plug-ins structured by the predefined architecture.

Installation of iWMC basic set enables iWMC system administrator to utilise basic management functions (device search, device monitoring, and device setting management) to manage devices. The addition of plug-ins according to the purposes of the IT administrator and capability of the target device enables more complicated device management.

iWMC system administrator can install additional plug-in file set on client computer via iWMC server computer by using “plug-in management” of “environmental setting”. Currently, “Device Address Book Management Plug-in” and “Printer Driver Installation Plug-in” are offered as additional plug-ins of the iWMC.

5.3. Security

[\[Login management\]](#)

iWMC is a web application which enables the client computer to use iWMC on the server computer, accessed via a web browser. When accessing iWMC, the user authentication screen is displayed at first. Only when the user inputs the correct user name and password, can iWMC functions be used. It is recommended to update the password regularly in the same way as other IT systems.

[\[Access restriction by user\]](#)

By using account management functions of the iWMC, access level can be set by user group for each function of the iWMC. When managing the device by the same Administrators' using the iWMC, this function enables setting of the access authority for each administrator to perform minimum functions, which improves the security level of the entire system. The setting to allow access by only a limited administrator (usually one person as a system administrator) for the iWMC environment setting (system setting, account management, and system log) is recommended.

[\[Data hiding\]](#)

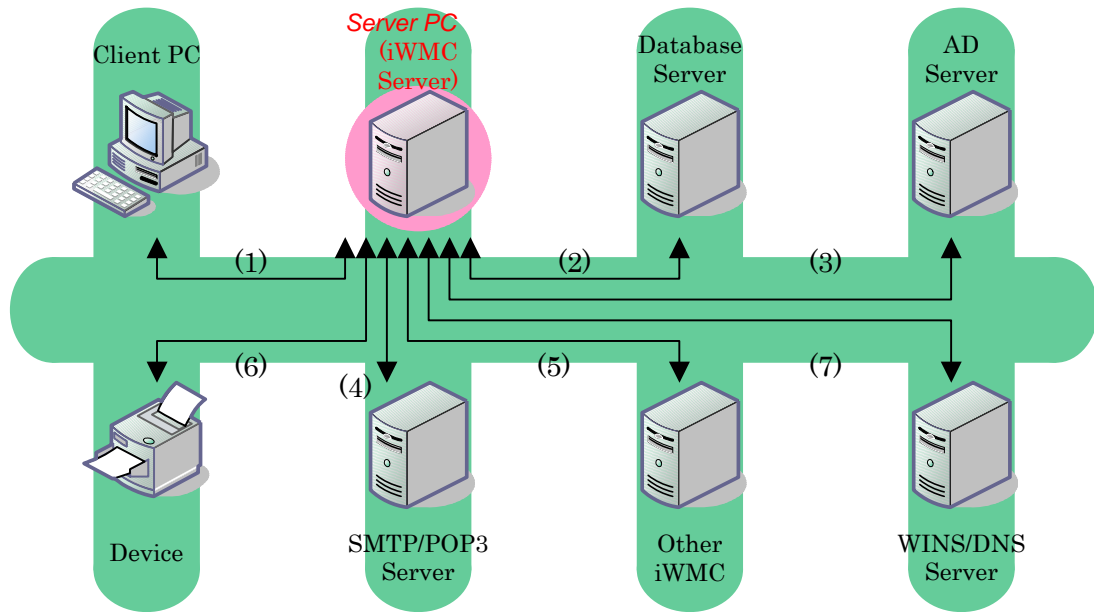
iWMC's internal data (environment setting information, task information and so on) is stored in the database (SQL or MSDE) specified during the installation of the iWMC. Therefore, its contents cannot be referred to from the Windows file system. Access to the database is protected by a user name and password.

[\[Authentication when sending an e-mail\]](#)

iWMC system administrator configures the SMTP server setting, which enables sending of the configured e-mail message after appropriate authentication (SMTP authentication and POP before SMTP (POP or APOP)) for the SMTP server is verified.

5.4. Communication protocol and port number

With reference to iWMC basic set, the PC on which iWMC is installed communicates with the network objects shown below.



Communication environment of the iWMC basic set

With reference to the communication routes shown in above diagram, the following protocol and port number are used.

Port No.	Protocol	Network Service	Direction	Description
80	TCP	HTTP	(1) inbound	It is required to access to the iWMC server/ISS from the client PC. Port number can be modified by the IIS setting.
443	TCP	HTTPS	(1) inbound	It is required to access to the iWMC server from the client PC (when using the SSL). Port number can be modified by the IIS setting.
1443	TCP	SQL over TCP	(2) outbound	It is required for the iWMC Server to access the SQL/MSDE installed into the remote PC. It is not required when using the SQL/MSDE installed into the iWMC Server. The port number can be modified by the SQL/MSDE setting.

389	TCP	LDAP	(3) outbound	It is required to obtain user list information from the Active Directory. It is not required when the unique authentication for the iWMC is selected when installing the iWMC.
25	TCP	SMTP	(3) outbound	It is required to send a notification via e-mail. The port number can be modified by [Communications Settings] of [Configuration].
110	TCP	POP3	(4) outbound	It is required to authenticate via POP before SMTP when sending a notification via e-mail. It is not required when authentication via POP before SMTP is not executed. The port number can be modified by [Communications Settings] of [Configuration].
427	UDP	SLP	(5) inbound	It is required to be searched from the other iWMC server by the SLP multicast (distributed service search function).
427	UDP	SLP	(5) outbound	It is required to be searched from the other iWMC server by the SLP multicast (distributed service search function).
427	UDP	SLP	(6) outbound	It is required to search devices by SLP Multicast.
161	UDP	SNMP	(6) outbound	It is required to search devices by SNMP broadcast or unicast, to authenticate when delivering the device setting or rebooting, or to obtain the device setting, deliver the setting, and obtain and set the data when rebooting.
53	UDP	DNS	(7) outbound	It is required to convert the DNS host name to IP address when searching the device by specifying the DNS host name (FQDN).
137	UDP	NetBIOS Name Resolution	(7) outbound	It is required to convert the NetBIOS name to IP address when searching the device by specifying the NetBIOS name.

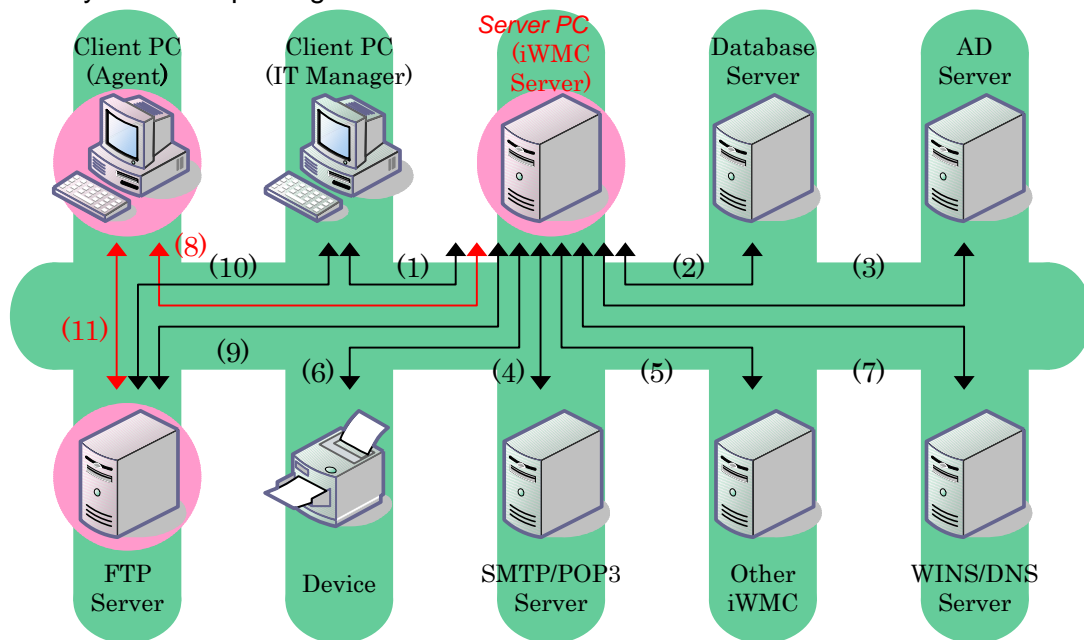
47545	UDP	CPCA	(6) outbound	It is required for the authentication when delivering the device setting or when rebooting.
80	TCP	HTTP	(6) outbound	It is required for the access to the web page stored in the device (Remote UI) or the EFI Web Tools (when mounting the EFI controller on the device).
8080	TCP	HTTP	(6) outbound	It is required for the access to the web page stored in the device (Remote UI) (when mounting the EFI controller on the device).
–	ICMP	ICMP Echo (ping)	(*) outbound	It is required to check address duplication when setting the IP address in order to deliver the device setting.

In the above table, “Direction” indicates the communication direction from the viewpoint of the server computer where iWMC is installed. When “Direction” is “inbound”, “Port No.” indicates the port number of the receiving side, while “Direction” is “outbound”; “Port No.” indicates that of the destination.

“Device Address Book Management Plug-in” utilises the following protocols besides protocols used by the basic package.

Port No.	Protocol	Network Service	Direction	Description
80	TCP	HTTP/UDDI	(6) inbound	It is required for the Universal Description, Discovery and Integration (UDDI) .
443	TCP	HTTPS	(6) inbound	It is required to implement SOAP communication.

“Printer Driver Installation Plug-in” utilises the following protocols besides protocols used by the basic package.



Communication environment when adding Printer Driver Installation Plug-in

The Agent program for the “Printer Driver Installation Plug-in” responsible for delivering printer driver is installed onto the client computer (described as “Client PC (Agent) ” in the above figure). The Agent program is installed manually for Windows 9x. For other Windows OS, it is installed remotely from the server computer on which iWMC is installed.

The printer driver file to be installed by the “Printer Driver Installation Plug-in” is stored in the “FTP server” described in the figure. The IT administrator accesses iWMC via web browser installed in the “Client PC (IT Manager) ” and uploads the printer driver file stored in the “Client PC (IT Manager) ” to the FTP server by using the “no-touch deployment Windows Form Application”.

Below are the “Printer Driver Installation Plug-in” protocols;

Port No.	Protocol	Network Service	Direction	Description
135	TCP	Remote Procedure Call	(8) outbound	It is required to install the Agent program into the client PC remotely from the iWMC by using WMI (Windows Management Instrumentation) .
445	TCP	SMB Direct Hosting	(8) outbound	It is required to install the Agent program into the client PC remotely from the iWMC by using WMI (Windows Management Instrumentation) .
11017	UDP	SNMP	(8) outbound	It is required for the iWMC server to send executive instruction of the task to the Agent installed in the client PC.
80	TCP	HTTP	(8) inbound	It is required for the Agent installed into the client PC to send the client PC information to the iWMC via the web service. “Inbound” is the direction looked from the iWMC server side and “outbound” is the one looked from the Agent program installed into the client PC.
21	TCP	FTP	(9) outbound	It is required for the iWMC to access to the FTP server. The port number can be modified by the FTP server setting.
20	TCP	FTP	(9) outbound	It is required for the iWMC server and the FTP server to transfer data with the standard mode (PORT mode).

21	TCP	FTP	(10) outbound	It is required to access to the FTP server from the printer driver file management program installed by the “no-touch deployment”. The port number can be modified by the FTP server setting.
20	TCP	FTP	(10) outbound	It is required for the printer driver file management program installed by the “no-touch deployment” and the FTP server to transfer data with the standard mode (PORT mode).
21	TCP	FTP	(11) outbound	It is required for the Agent program installed into the client PC to access to the FTP server. The port number can be modified by the FTP server setting.
20	TCP	FTP	(11) outbound	It is required for the Agent program installed into the client PC and the FTP server to transfer data with the standard mode (PORT mode).

5.5. Network traffic

Network traffic is quite small when monitoring the device at the normal status.

- When the device is at the normal status : [About 3.5 Kbytes / 1 device](#)
- When an error occurs in the device : [About 4 Kbytes / 1 device](#)

Even if 1,000 units of devices are connected to the network, the iWMC obtains the device status one by one, which does not have an impact on traffic if the number of devices is increased.

- [Given the above facts, iWMC has little impact on the customer's network traffic.](#)

6. Environment

6.1. Operating environment

Computer to install the iW Management Console	
CPU	Pentium3 processor: 1GHz or larger (Recommended Pentium4 processor: 2GHz or larger)
Memory	256MB or larger (recommended 512MB or larger)
Hard disk	More than 100MB free space for installation When using the disk for the database server simultaneously, more than 1GB free space is required for the database in addition to the above space (recommended 2GB or larger)
OS*	Microsoft Windows 2000 Professional/Server + Service Pack 4 Microsoft Windows XP Professional + Service Pack 2 Microsoft Windows Server 2003 + Service Pack 1 Microsoft Windows Server 2003 R2
Software Runtime	Microsoft .NET Framework v1.1 (Service Pack 1) Microsoft .NET Framework Language Pack Microsoft Web Services Enhancements 2.0 SP3 for Microsoft.NET
Database	Microsoft SQL Server 2000 (Service Pack 4 or later) Microsoft SQL Server 2005 Microsoft SQL Server 2000 Desktop Engine (Service Pack 4 or later) Microsoft SQL Server 2000 Desktop Engine Release A Microsoft SQL Server 2005 Express Edition
Web Server	Microsoft Internet Information Services 5.0 or later
The number of devices and users managed by a single server	Device: 1,000 units User: 10,000 users

*) When using the driver management plug-in, server OS is recommended.

Client (computer which accesses to the iW Management Console)	
Display	SVGA 800×600 or more (recommended XGA 1024×768 or more) High color: 65,536 colors or more (recommended full color: 16,777,216 colors or more)
Web browser	Microsoft Internet Explorer 5.5 SP2/6.0SP1
OS	Microsoft Windows 98 Second Edition/ME Microsoft Windows 2000 Professional/Server + Service Pack 4 Microsoft Windows XP Home Edition/Professional + Service Pack 2 Microsoft Windows Server 2003 + Service Pack 1 Microsoft Windows Server 2003 R2

Computer to install the printer driver

Memory	128MB
Hard disk	10MB for the installation of the Agent (only push installation) 30MB free space per driver
OS	Microsoft Windows 98 Second Edition/ME Microsoft Windows 2000 Professional/Server + Service Pack 4 Microsoft Windows XP Home Edition/Professional + Service Pack 2 Microsoft Windows Server 2003 + Service Pack 1 Microsoft Windows Server 2003 R2

6.2. Supported device

Supported Canon devices are listed below.

With reference to other vendor's devices, the expression "models which support the Standard MIB" described in the 3.3 is used.

When operations of some models are verified; list them specifically.

This is the information as of July 31, 2006. Contact your appropriate sales company for the latest information.

Device Name	Feature of iWMC					
	Device Setting & Monitoring	Address Book Plug-in	Printer Driver Management Plug-in			
			PCL	PS	UFR II	FAX
iR3250	Yes	—	—	—	—	—
iR5000-6000	Yes	—	Yes	Yes	—	—
iR5000	Yes	—	Yes	Yes	—	—
iR6000	Yes	—	Yes	Yes	—	—
iR5000-L1	Yes	—	Yes	—	—	—
iR6000-L1	Yes	—	Yes	—	—	—
iR5000i	Yes	—	Yes	Yes	—	—
iR6000i	Yes	—	Yes	Yes	—	—
iR5020	Yes	—	Yes	Yes	—	—
iR6020	Yes	—	Yes	Yes	—	—
iR2200	Yes	—	Yes	Yes	—	Yes
iR2800	Yes	—	Yes	Yes	—	Yes
iR3300	Yes	—	Yes	Yes	—	Yes
iR2200i	Yes	—	Yes	Yes	—	Yes
iR3300i	Yes	—	Yes	Yes	—	Yes
iR2220	Yes	—	Yes	Yes	—	Yes
iR3320	Yes	—	Yes	Yes	—	Yes
iR8500	Yes	—	Yes	Yes	—	—
iR85	Yes	—	—	—	—	—
iR7200	Yes	—	Yes	Yes	—	—
iR105	Yes	—	Yes	Yes	—	—

Device Name	Feature of iWMC					
	Device Setting & Monitoring	Address Book Plug-in	Printer Driver Management Plug-in			
			PCL	PS	UFR II	FAX
iR8500-M1	Yes	—	Yes	—	—	—
iR85-M1	Yes	—	—	—	—	—
iR7200-M1	Yes	—	Yes	—	—	—
iR105-M1	Yes	—	Yes	—	—	—
iR8500-M2	Yes	—	Yes	—	—	—
iR85-M2	Yes	—	—	—	—	—
iR7200-M2	Yes	—	Yes	—	—	—
iR105-M2	Yes	—	Yes	—	—	—
iR85PLUS	Yes	Yes 1	Yes	Yes	Yes	—
iR8070	Yes	Yes 1	Yes	Yes	Yes	—
iR105PLUS	Yes	Yes 1	Yes	Yes	Yes	—
iR9070	Yes	Yes 1	Yes	Yes	Yes	—
iR85PLUS-M3	Yes	—	Yes	—	—	—
iR8070-M3	Yes	—	Yes	—	—	—
iR8070-S1	Yes	—	Yes	—	—	—
iR105PLUS-M3	Yes	—	Yes	—	—	—
iR9070-M3	Yes	—	Yes	—	—	—
iR2870	Yes	Yes 1	Yes	Yes	Yes	Yes
iR2270	Yes	Yes 1	Yes	Yes	Yes	Yes
iR2830	Yes	—	Yes	—	Yes	Yes
iR4570	Yes	Yes 1	Yes	Yes	Yes	Yes
iR3570	Yes	Yes 1	Yes	Yes	Yes	Yes
iR3530	Yes	—	Yes	—	Yes	Yes
iR6570	Yes	Yes 1	Yes	Yes	Yes	Yes
iR5570	Yes	Yes 1	Yes	Yes	Yes	Yes

*1) Firmware update is necessary

Device Name	Feature of iWMC					
	Device Setting & Monitoring	Address Book Plug-in	Printer Driver Management Plug-in			
			PCL	PS	UFR II	FAX
iR6570-S1	Yes	—	Yes	—	—	Yes
iR5570-S1	Yes	—	Yes	—	—	Yes
iR6570-M3	Yes	—	Yes	—	—	Yes
iR5570-M3	Yes	—	Yes	—	—	Yes
iR7105	Yes	Yes	Yes	Yes	Yes	—
iR7095	Yes	Yes	Yes	Yes	Yes	—
iR7086	Yes	Yes	Yes	Yes	Yes	—
iR7105-S1	Yes	—	Yes	—	—	—
iR7095-S1	Yes	—	Yes	—	—	—
iR7086-S1	Yes	—	Yes	—	—	—
iR C3200	Yes	—	Yes	Yes	—	Yes
CLC 3200-C1	Yes	—	Yes	—	—	Yes
iR C3220	Yes	—	Yes	Yes	—	Yes
CLC 3220-C1	Yes	—	Yes	—	—	Yes
CLC 3220-C2	Yes	—	Yes	—	—	Yes
CLC 3220-NX3000	Yes	—	—	—	—	—
CLC 3220-Z3000	Yes	—	—	—	—	—
iR C2620	Yes	—	Yes	Yes	—	Yes
CLC 2620-C1	Yes	—	Yes	—	—	Yes
CLC 2620-NX3000	Yes	—	—	—	—	—
CLC 2620-Z3000	Yes	—	—	—	—	—
CLC5151-H1	Yes	—	Yes	—	—	Yes
CLC5151 -GX100	Yes	—	—	—	—	—
iR C4580	Yes	Yes	Yes	Yes	Yes	Yes
CLC4040-H1	Yes	—	Yes	—	—	Yes
CLC4040-GX100	Yes	—	—	—	—	—

Device Name	Feature of iWMC					
	Device Setting & Monitoring	Address Book Plug-in	Printer Driver Management Plug-in			
			PCL	PS	UFR II	FAX
iR C4080	Yes	Yes	—	—	—	—
iR 6800C EUR	Yes	—	Yes	Yes	—	Yes
iR 6800C EUR-D1/C6800-D1	Yes	—	Yes	—	—	Yes
iR 5800C EUR	Yes	—	Yes	Yes	—	Yes
iR 5800C EUR-D1/C6800-D1	Yes	—	Yes	—	—	Yes
iR 3100C EUR	Yes	—	Yes	Yes	—	Yes
iR 3100C EUR-E1/C3100-E1	Yes	—	Yes	—	—	Yes
iR 3170C EUR	Yes	—	Yes	Yes	Yes	Yes
iR 2570C EUR	Yes	—	Yes	Yes	Yes	Yes
iR C3380	Yes	Yes	Yes	Yes	Yes	Yes
iR C2880	Yes	Yes	Yes	Yes	Yes	Yes
iR 6870C EUR	Yes	Yes	Yes	Yes	Yes	Yes
iR 6870C EUR-G1/C6870-G1	Yes	—	Yes	—	—	Yes
iR 5870C EUR	Yes	Yes	Yes	Yes	Yes	Yes
iR 5870C EUR-G1/C5870-G1	Yes	—	Yes	—	—	Yes
iPR C1	Yes	Yes	Yes	Yes	Yes	—
iPR C1-Q1	Yes	—	—	—	—	—
iR1018/1022/1023	Yes	—	—	—	—	—
iR2020	Yes	—	Yes	—	Yes	Yes
iR2016	Yes	—	Yes	—	Yes	Yes
MF5630	Yes	—	—	—	—	—
MF5650	Yes	—	—	—	—	—
MF5730	Yes	—	—	—	—	—
MF5750	Yes	—	—	—	—	—

Device Name	Feature of iWMC					
	Device Setting & Monitoring	Address Book Plug-in	Printer Driver Management Plug-in			
			PCL	PS	UFR II	FAX
MF5770	Yes	—	—	—	—	—
MF3110	Yes	—	—	—	—	—
MF3200 Series	Yes	—	—	—	—	—
MF6500 Series	Yes	—	—	—	—	—
MF7100 Series	Yes	—	Yes	—	Yes	Yes
FAX-L900/L800	No	—	—	—	—	—
GP160	No	—	—	—	—	—
FAX-L1000	No	—	—	—	—	—
iR2000	Yes	—	Yes	—	—	—
iR1600	Yes	—	Yes	—	—	—
iR2010	Yes	—	Yes	—	—	Yes
iR1610	Yes	—	Yes	—	—	Yes
FAX-L2000	Yes	—	Yes	—	—	Yes
PC1200D/iR1200G/iC D600	Yes	—	—	—	—	—
PC1200D/iR1200G/iC D600	Yes	—	—	—	—	—
PC1200/iC D600/iR 1200G	Yes	—	—	—	—	—
PC1200/iC D600/iR 1200G	Yes	—	—	—	—	—
iR1200-1300	Yes	—	—	—	—	—
iR1510-1670	Yes	—	—	—	—	—
FAX-L400	Yes	—	Yes	—	—	Yes
I-SENSYS MF4100 Series	Yes	—	—	—	—	—
GP200-216:GP PS/PCL-D1	Yes	—	No	—	—	—
GP200-216:GP PCL-E1	Yes	—	No	—	—	—
GP200-225 PCL	Yes	—	No	—	—	—
GP200-225 PS/PCL	Yes	—	No	—	—	—
GP555-605-605P	Yes	—	Yes	—	—	—
GP300-405 PS/PCL	Yes	—	Yes	—	—	Yes
GP300-405 PCL	Yes	—	Yes	—	—	Yes

UK/FIGS	Feature of iWMC					
	Device Setting & Monitoring	Address Book Plug-in	Printer Driver Management Plug-in			
			PCL	PS	UFR II	FAX
iR400 PS/PCL	Yes	—	Yes	—	—	Yes
iR400 PCL	Yes	—	Yes	—	—	Yes
CP660PS	Yes	—	—	—	—	—
iR C2100S-2100	Yes	—	Yes	—	—	—
iR C2000 series	Yes	—	Yes	—	—	—
iR C624	Yes	—	—	—	—	—
CLC1180	Yes	—	—	—	—	—
CLC1160	Yes	—	—	—	—	—
CLC1150	Yes	—	—	—	—	—
CLC1130	Yes	—	—	—	—	—
CLC1100	Yes	—	—	—	—	—
CLC5000 series	Yes	—	—	—	—	—
CLC5000 series	Yes	—	—	—	—	—
CLC5000 series	Yes	—	—	—	—	—
CLC5000 series	Yes	—	—	—	—	—
C LBP 400	Yes	—	—	—	—	—
C LBP 460PS	Yes	—	—	—	—	—
LBP-1760	Yes	—	—	—	—	—
LBP-800	Yes	—	—	—	—	—
LBP-810	Yes	—	—	—	—	—
LBP-1760e	Yes	—	—	—	—	—
LBP-1000	Yes	—	—	—	—	—
LBP-2000	Yes	—	Yes	—	—	—
LBP-1210	Yes	—	—	—	—	—
LBP-2410	Yes	—	—	—	—	—
LBP-3260	Yes	—	—	—	—	—
LBP3360	Yes	—	Yes	—	Yes	—
LBP3460	Yes	—	Yes	—	Yes	—

UK/FIGS	Feature of iWMC					
	Device Setting & Monitoring	Address Book Plug-in	Printer Driver Management Plug-in			
			PCL	PS	UFR II	FAX
LBP5960	Yes	—	Yes	—	Yes	—
LBP5300	Yes	—	—	—	—	—
LBP3000	Yes	—	—	—	—	—
LBP3300	Yes	—	—	—	—	—
N2000	Yes	—	—	—	—	—
N1000	Yes	—	—	—	—	—
BIJ2300	Yes	—	Yes	—	—	—
BIJ1300	Yes	—	Yes	—	—	—
BIJ1350D	Yes	—	Yes	—	—	—
W2200	Yes	—	—	—	—	—
W6200PG	Yes	—	—	—	—	—
W7200	Yes	—	—	—	—	—
W7250	Yes	—	—	—	—	—
W8200PG	Yes	—	—	—	—	—
W8200	Yes	—	—	—	—	—
iPF5000	Yes	—	—	—	—	—
iPF500	Yes	—	—	—	—	—
iPF600	Yes	—	—	—	—	—
iPF9000	Yes	—	—	—	—	—
iPF700	Yes	—	—	—	—	—