Reissued: 2-June-16

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

RTB Reissue

The items in ***bold italics*** were corrected or added.

Subject: Card Authentication Package v2 Installation Manual			Prepared by: Kohsuke Tomoyama
From: Solution Support Sect., Solution Support Dept.			
Classification:	☐ Troubleshooting	☐ Part information	☐ Action required
	☐ Mechanical	☐ Electrical	☒ Service manual revision
	☐ Paper path	☐ Transmit/receive	☐ Retrofit information
	☐ Product Safety	☐ Other ( )	☐ Tier 2

This RTB has been issued to announce the release of the Card Authentication Package v2 Installation Manual.

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Card Authentication Package v2 Installation Manual

Document version: 1.3.1

Main Chapters

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Installation

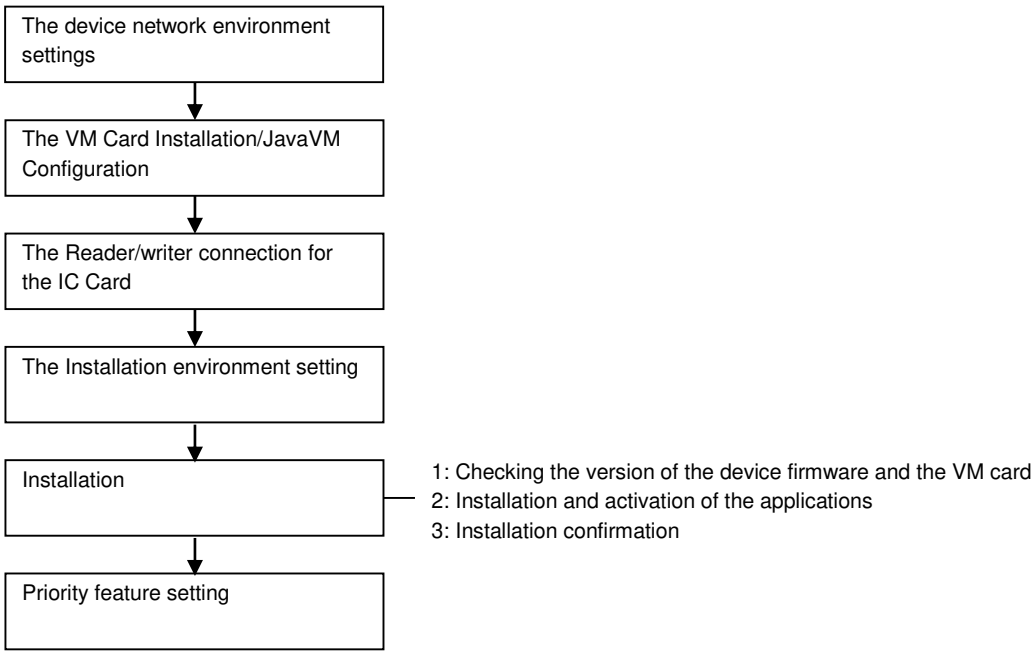
Installation

Before installation, please make sure all firmwares (GW firmware, Smart Operation Panel firmware, and Smart Operation Panel applications) are the latest version. Regarding the firmware update procedures, please refer to the device service manual.

Installation (WVGA/4.3-inch operation panel models)

- Depending on the device model, the actual operation panel screen may look different from the screenshots used in this document.

Installation Flowchart

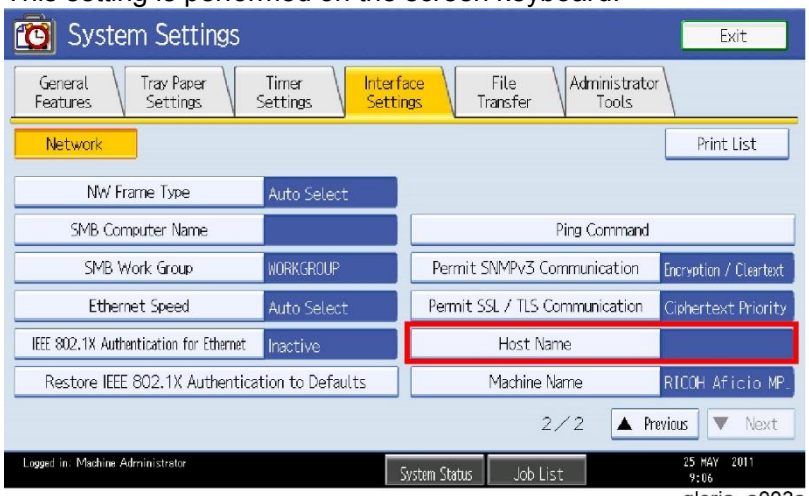
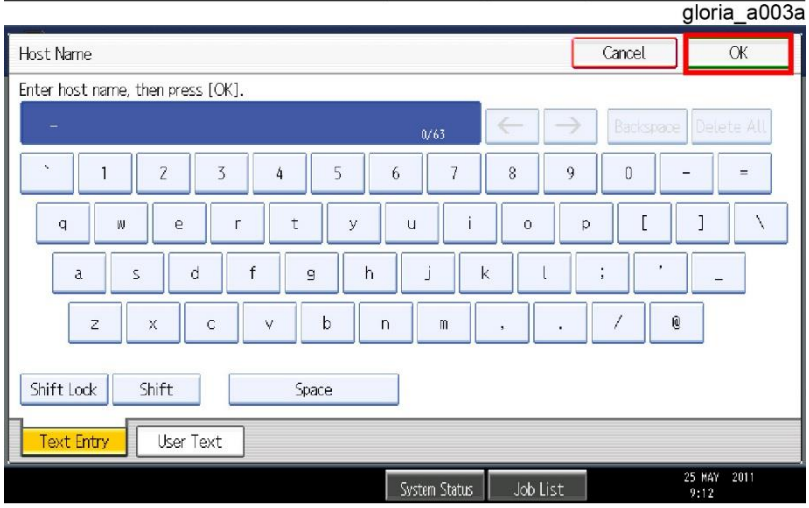


Installation Environment Settings

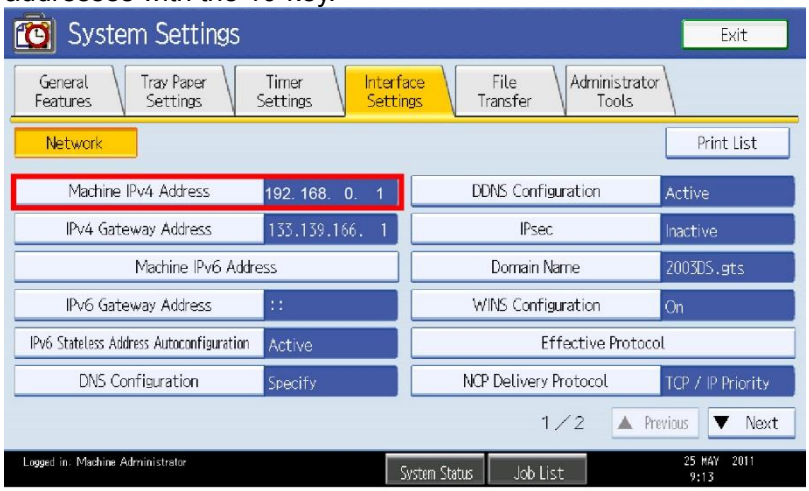
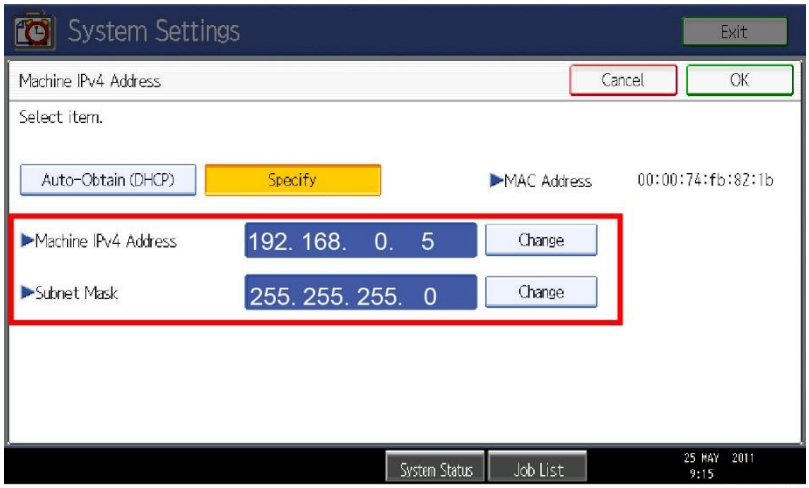
1. **Network information**

* Setting from System Settings of the device
* In the case of Smart Operation Panel models, [User Tools] must be selected first and then the [User Tools / Counter / Enquiry] screen is displayed.

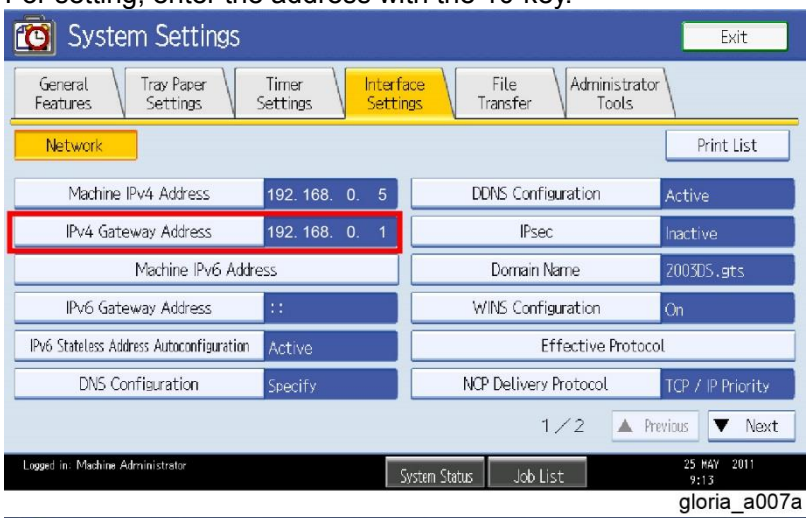
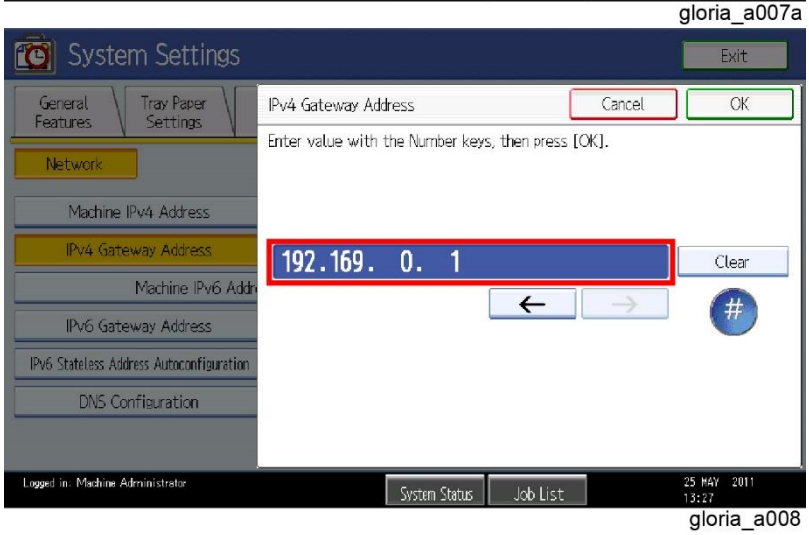
Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Item	Detailed descriptions	Default/Remarks
Host Name	Set the host name shown on [Interface Settings] tab. This setting is performed on the screen keyboard.  gloria_a003a  gloria_a004a	-

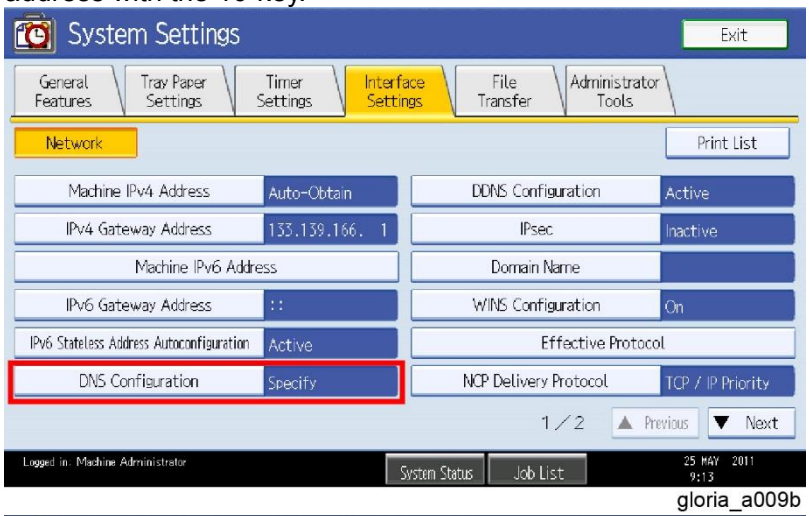
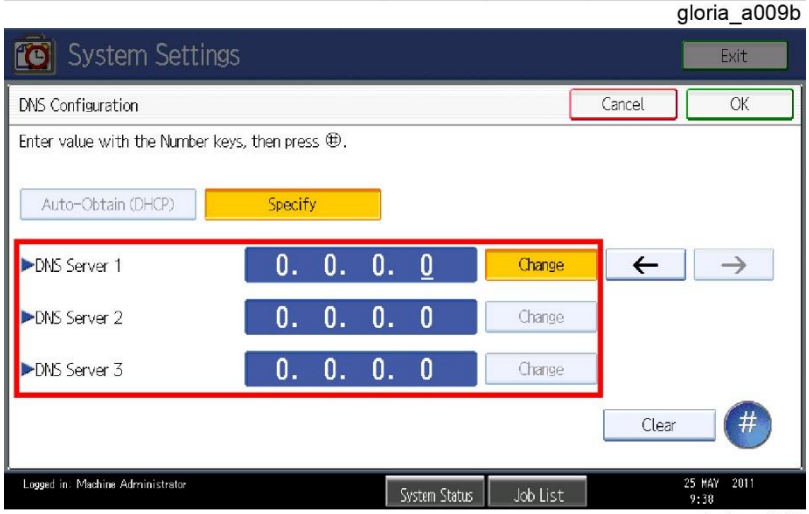
Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

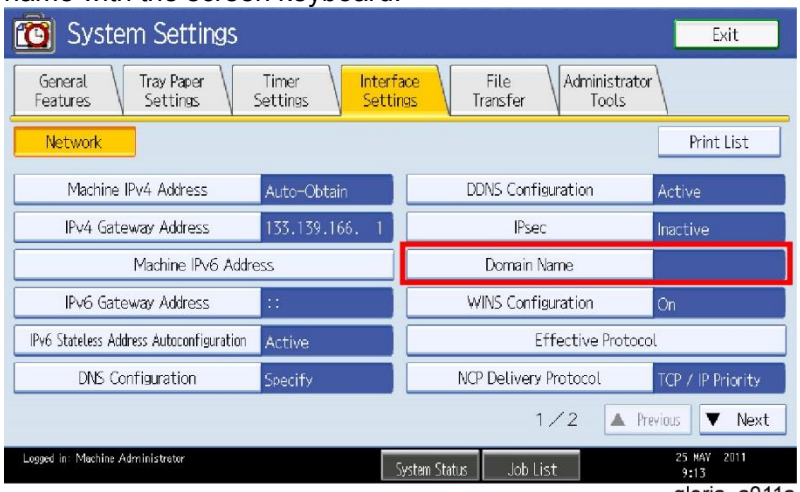
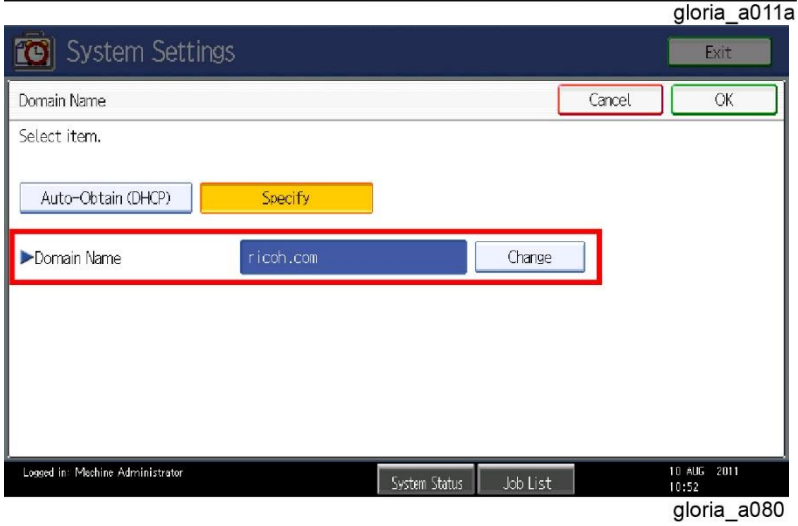
Item	Detailed descriptions	Default/Remarks
IP Address/ Subnet Mask	Set the IP address and the subnet mask that appear when [Machine IPv4 Address] in [Interface settings] tab is selected. For setting, press [Specify] and [Change], and then enter the addresses with the 10-key.  gloria_a005a  gloria_a006	-

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Item	Detailed descriptions	Default/Remarks
Default Gateway	Set the address that appears when [IPv4 Gateway Address] in [Interface Settings] tab is selected. For setting, enter the address with the 10-key.  gloria_a007a  gloria_a008	-

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Item	Detailed descriptions	Default/Remarks
DNS Server 1/DNS Server 2/DNS Server 3	Set the server address that appears when [DNS Configuration] in [Interface Settings] tab is selected. For setting, press [Specify] and [Change], and then enter the address with the 10-key.  gloria_a009b  gloria_a010	-

Item	Detailed descriptions	Default/Remarks
Domain Name	Set the name that appears when [Domain Name] in [Interface Settings] tab is selected. For setting, press [Specify] and [Change], and then enter the name with the screen keyboard.  gloria_a011a  gloria_a080	-

2) Timer Setting

* Setting in [Timer Settings] of [System Settings]

Item	Detailed descriptions	Default/Remarks
Auto Logout Timer	The default value is [Off], however press [Auto Logout Timer] in [Timer Settings] tab and select [On] to enter the log out time if necessary to change it. The range of entering the automatic logout time is from 60 to 999 seconds.	Default: [Off]

Note

- If the JavaVM is installed to the device's Flash Memory (FM), this procedure is not necessary. In this case, please proceed to the "JavaVM Configuration".

1. Set [Auto Off timer] to 5 minutes in [User Tools / Counter / Enquiry] screen → [System Settings] → [Timer Settings] tab.

Note

- [Auto Off Timer] at the device side should be set to 5 minutes to prevent the device from entering the Auto Off mode while the Java ™ Platform is installing or activating.

2. Set [System Auto Reset Timer] to [Off] in [User Tools / Counter / Enquiry] screen → [System Settings] → [Timer Settings] tab.

Note

- This setting should be restored after the installation.

3. Turn off the main power of the device.
4. Insert the VM card into the SD card slot.

Note

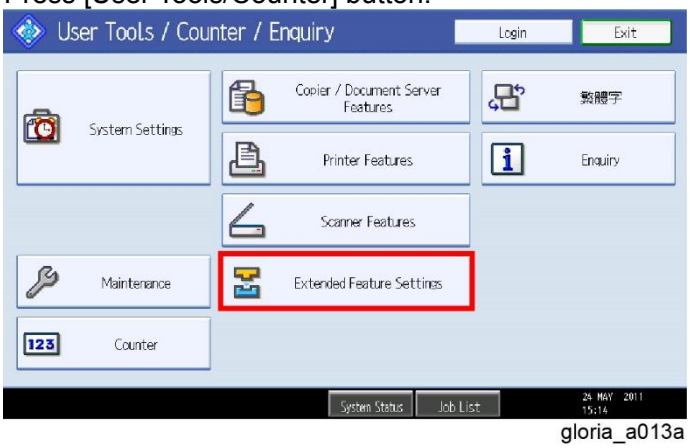
- For which the SD card slot should be inserted into, see the service manual of each machine.

5. Turn on the main power of the device.

Note

- The Java ™ Platform is installed automatically if the main power of the device is turned on after the VM card insertion.
- It takes for approx. from 3 to 4 minutes to install it automatically.
- Never turn off the power of the device during the installation, otherwise it may damage the VM card. Turn off the power after the confirmation in step 8 has been done.

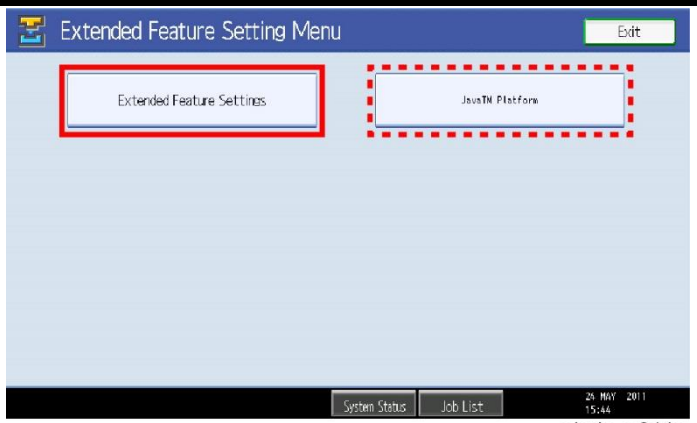
6. Press [User Tools/Counter] button.



gloria_a013a

7. Press [Extended Feature Settings] after [User Tools / Counter / Enquiry] screen appears.

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

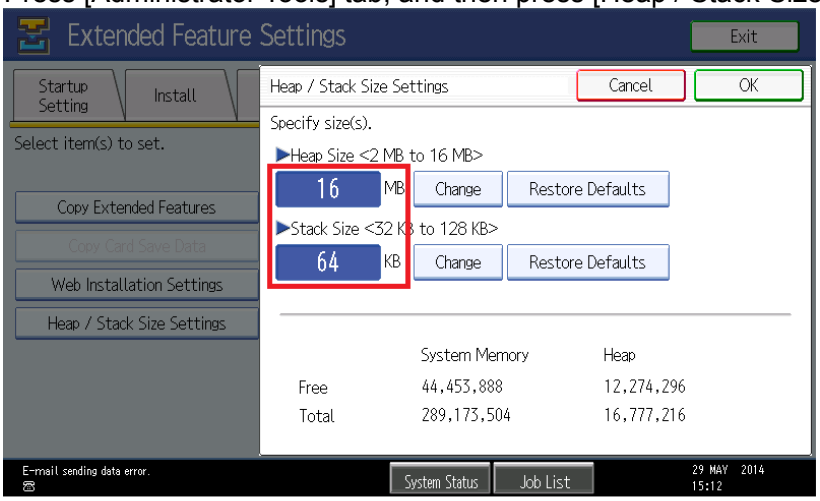


gloria_a014a

8. Confirm on [Extended Feature Setting Menu] screen that [JavaTM Platform] appears after the installation is completed normally.

JavaVM Configuration

1. Press [User Tools/Counter] button.
2. Press [Extended Feature Settings] after [User Tools / Counter / Enquiry] screen appears.
3. Press [Extended Feature Settings].
4. Press [Administrator Tools] tab, and then press [Heap / Stack Size Settings].

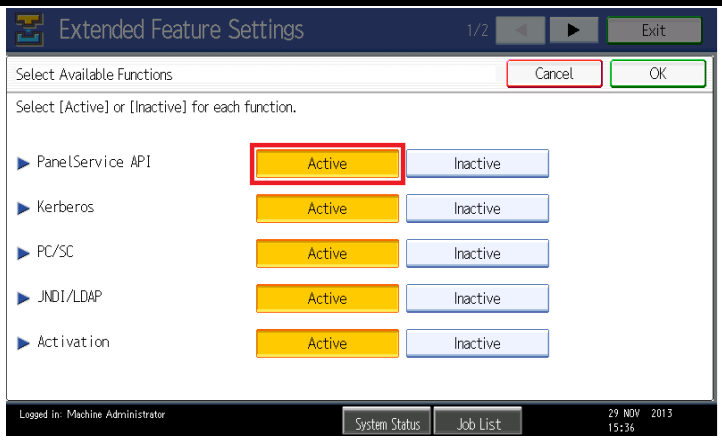


gloria_a015

5. Set the heap size and stack size.

Model	Heap size	Stack size
11S or earlier	16MB (Default: 10MB)	64KB (Default: 64KB)
11A or later	48MB (Default: 16MB)	Do not change from default size (Default: 256KB)

6. Press the [Administrator Tools] tab, and then press [Select Available Functions].
7. Set [PanelService API] as [Active].



8. Finish [User Tools].
9. Push the power button at the side of operation section, and turn off the main power after the power indicator has finished blinking.

Note

- The VM card should be operated with setting in the SD card slot.
- Restore the original setting after installation if the change of [System Auto Reset Timer] is performed.

IC Card Reader/Writer connection

Note

- The Installation should be executed after the main power is turned off.

Connect the IC card Reader/Writer to the device.

Note

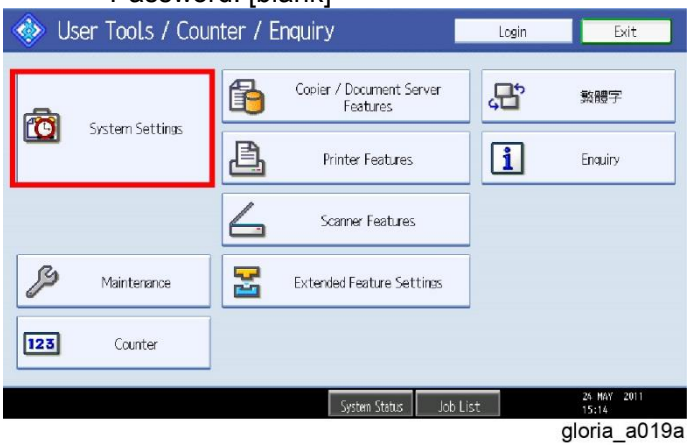
- Connect the USB cable to the left USB port for Aficio MP C5000/C4000/C3300/C2800, Aficio MP C2550/2050.
- For other machines, either port can be connectable.
- Regarding NFC Card Reader installation, please refer to the service manual for each model.

Authentication Management Settings

1. Log in the device as an administrator.

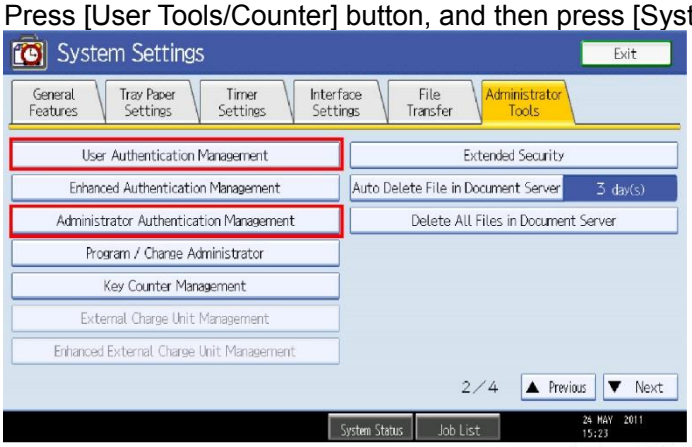
Note

- The initial value of login data is as follows:
- Login user name: admin
- Password: [blank]



gloria_a019a

2. Press [User Tools/Counter] button, and then press [System Settings].

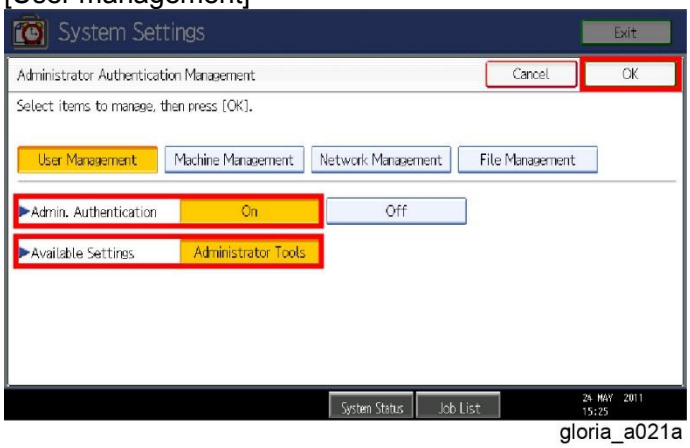


gloria_a020a

3. Press [Administrator Tools] tab, and set items below:
   [Administrator Authentication Management]
   [User Authentication Management]

1) Administrator Authentication Management

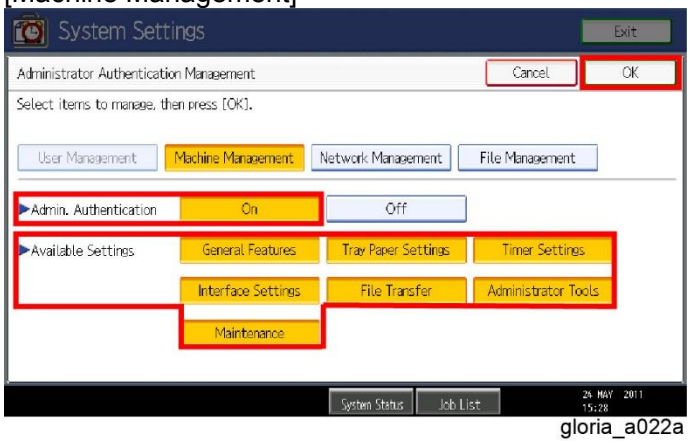
[User management]



gloria_a021a

1. Set [Admin. Authentication] to [On].
2. Press [Administrator Tools] of [Available Settings].
3. Press [OK] of the upper right, and enable the change.

[Machine Management]

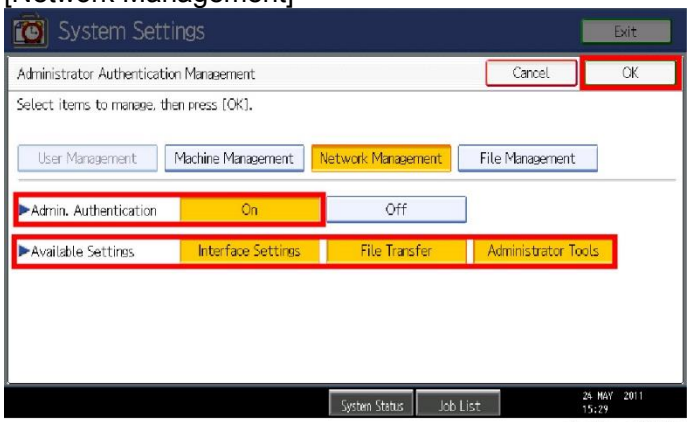


gloria_a022a

1. Set [Admin. Authentication] to [On].
2. For setting all items in [Available Settings] to values, press [General Features], [Tray Paper Settings], [Timer Settings], [Interface Settings], [File Transfer], [Administrator Tools] and

[Maintenance].
3. Press [OK] of the upper right, and enable the change.

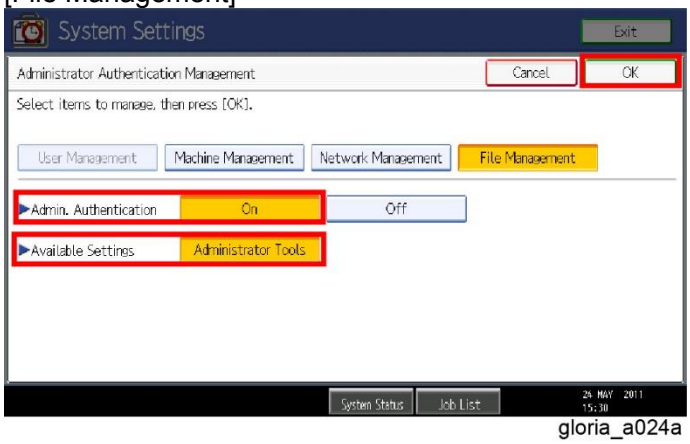
[Network Management]



gloria_a023a

1. Set [Admin. Authentication] to [On].
2. For setting all items in [Available Settings] to values, press [Interface Setting], [File Transfer], and [Administrator Tools].
3. Press [OK] of the upper right, and enable the change.

[File Management]

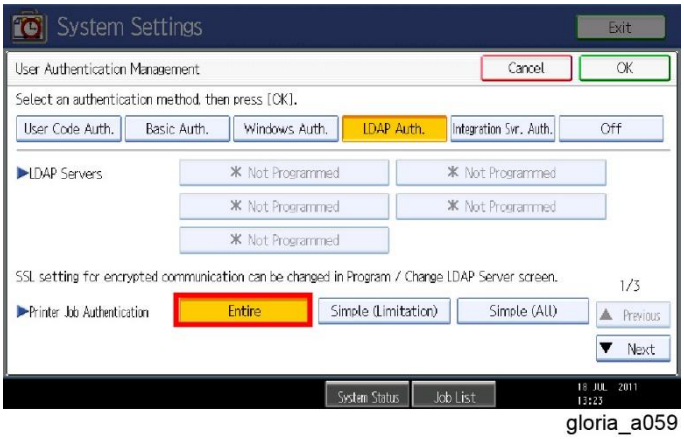


gloria_a024a

1. Set [Admin. Authentication] to [On].
2. Press [Administrator Tools] of [Available Settings].
3. Press [OK] of the upper right, and enable the change.

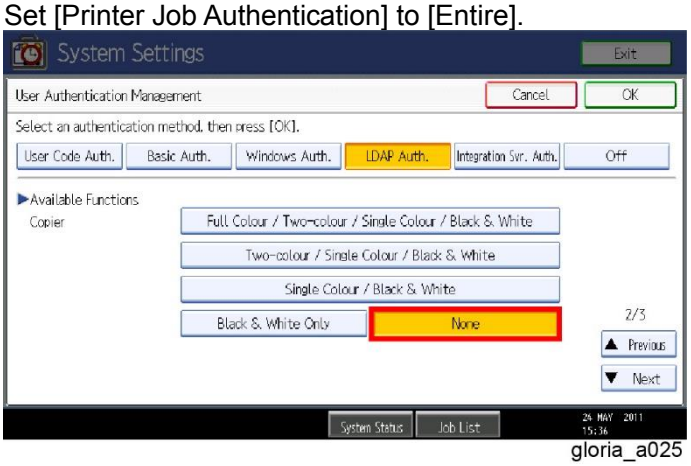
2) User Authentication Management

1. Confirm whether the method of the authentication is “Custom” or “LDAP”.



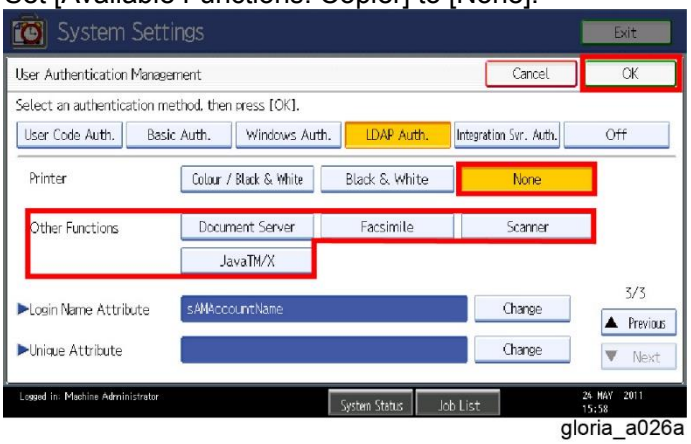
gloria_a059

2. Set [Printer Job Authentication] to [Entire].



gloria_a025

3. Set [Available Functions: Copier] to [None].



gloria_a026a

4. Set [Available Functions: Printer] to [None].
5. Reset [Document Server], [Facsimile], [Scanner] and [JavaTM/X] in [Available Functions: Other Functions].
6. Press [OK] of the upper right, and enable the change.

Turn the power off and on after the settings of [Administrator Authentication Management] and [User Authentication Management] are finished.

Card Authentication Package V2 Installation

Install the following applications using Remote Install Manager to install Card Authentication Package v2. For the installations procedures of these applications, see the service manual of Remote Install Manager. (☛ Remote Install Manager)

Note

- Regarding the installation method for Smart Operation Panel models (Compatibility mode), it is necessary to perform offline installation via RIM. It is not possible for the eDC-I system to judge which application module type (MP**: Compatibility mode / Z**: Hybrid mode) should be installed to devices equipped with the Smart Operation Panel. It is possible for Hybrid mode to perform online/offline installation via RIM.

Note

- In the case of Smart Operation Panel models (Hybrid mode), it is necessary to install 2 modules for CAP before activation when conducting offline installation: one for CAP authentication and one for CAP User Config. Tool. CAP User Config. Tool is used only when the authentication type is Local DB or CAP-ES (Internal user). If authentication type

is AD, LDAP, or CAP-ES (only external user), it is not necessary to install the module for CAP User Config. Tool.

In the case of Standard Operation Panel and Smart Operation Panel (Compatibility mode):

Application	Version	Note
CAP V2 MP11/MP21/MP31/SP31	V2.x	MP11 (WVGA models) MP21 (4-line LCD LP models) MP31 (12A or older 4.3-inch operation panel MFP models) SP31 (12S or later 4.3-inch operation panel LP models)
CAP LAUNCHER	V2.x	
CAP	V2.x	
CAP REG	V2.x	

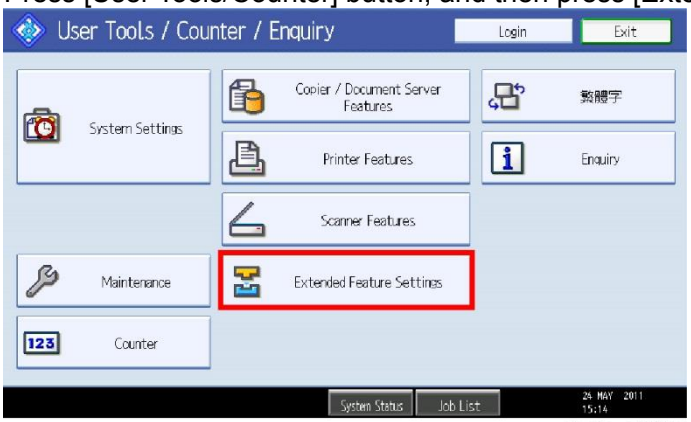
In the case of Smart Operation Panel (Hybrid mode):

Application	Version	Note
CAP V2 Z11	V2.x	
CAP	V2.x	
CAP V2 Auth. UI	V1.x	Smart Operation Panel application.
CAP User Config.	V1.x	Smart Operation Panel application.
CAP NFC Plug-in	V1.x	Smart Operation Panel application. Only for v2.3.0 or later.

Activation Check

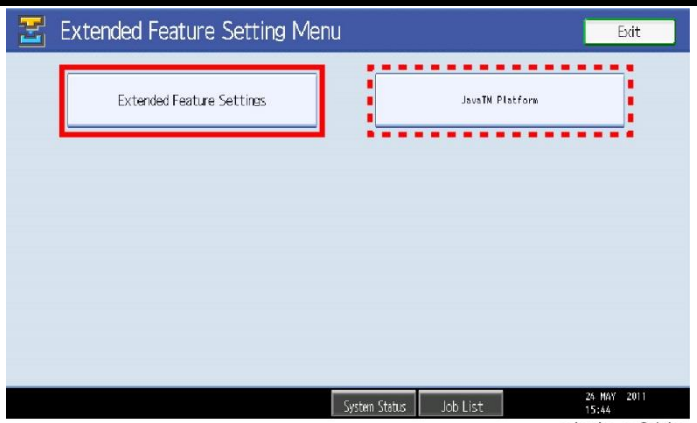
1. In the case of CAP v2 (Hybrid mode), restart the device manually to enable authentication internally.

2. Press [User Tools/Counter] button, and then press [Extended Feature Settings].



gloria_a013a

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k



gloria_a014a

3. Confirm on [Extended Feature Setting Menu] screen that [JavaTM Platform] appears.

Note

- If [JavaTM Platform] is not shown, the Java ™ Platform has not been activated yet. Wait for a while until [JavaTM Platform] appears.

4. Press [Extended Feature Settings].

gloria_a057a

5. Press [Startup Setting] tab, and confirm that the condition of each application is the same as below:
In the case of Standard Operation Panel and Smart Operation Panel (Compatibility mode):

Application	Status
CAP V2 MP11/MP21/MP31/SP31	Starting Up
CAP LAUNCHER	Suspend Note The Launcher is disabled by default. Please set it as the “Priority”. The Launcher is not supported on 4.3-inch operation panel models.
CAP	Starting Up
CAP REG	Stop
JavaTM Platform	Starting Up

In the case of Smart Operation Panel (Hybrid mode):

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Application	Status
CAP V2 Z11	Starting Up
CAP	Starting Up
JavaTM Platform	Starting Up

In the case of Smart Operation Panel (Hybrid mode), please also check whether the following applications are installed in Home screen → Screen Features → Screen Device Settings Information → Software Version List:

Application	Note
CAP V2 Auth. UI	
CAP User Config.	
CAP NFC plug-in	Only for v2.3.0 or later.

Note

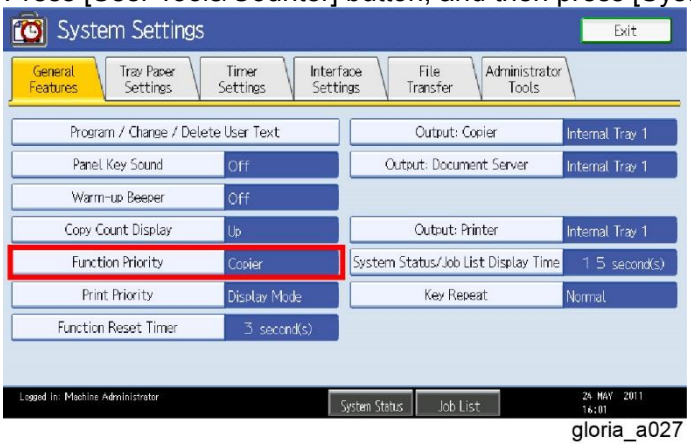
The following SP modes are automatically set whenever the applications are started up (Every time when the machine power is turned on). In the case of Smart Operation Panel models, press the [x] button on the login screen and select the [Printer] icon after logging out, and then go into SP mode. It is not possible to log in to SP mode from User Tools or Quick application (such as Quick Copy) and when logged in to the device.

- SP5-401-103: [0] → [3]
- SP5-401-162: bit0 [0] → [1], bit5 [0] → [1] *
- SP5-401-230: bit0 [0] → [1]
- SP5-401-240: bit0 [0] → [1]

*The bit6 of SP5-401-162 is changed from [0] to [1] at the first time when an IC card is touched. However, this is a normal action.

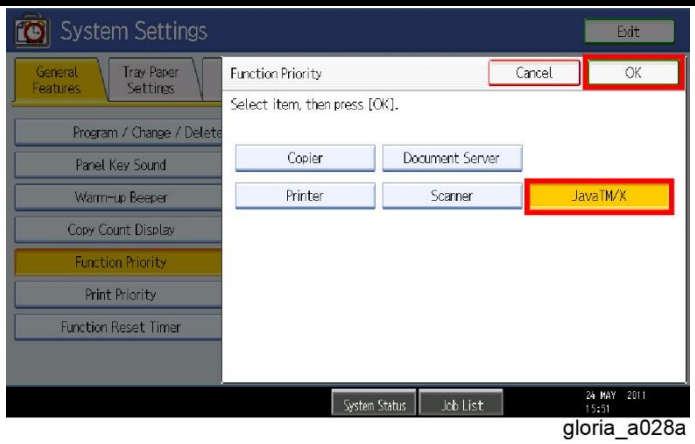
Priority Feature Setting (In the case of Standard Operation Panel models)

1. Press [User Tools/Counter] button, and then press [System Settings].



gloria_a027

2. Press [General Features] tab, and then press [Function Priority].



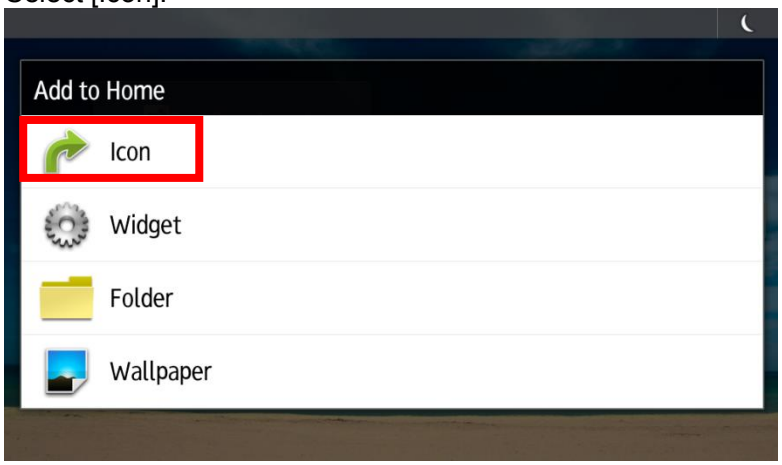
gloria_a028a

3. Select [Java TM/X] and press [OK].

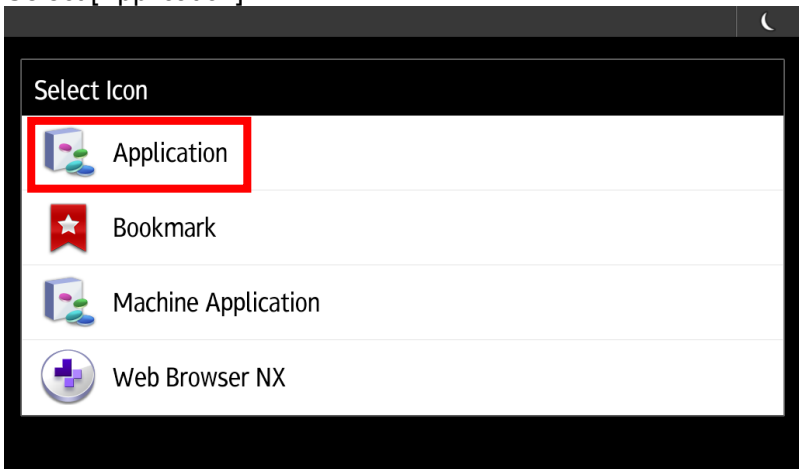
Smart Operation Panel model specific settings

Icon Setting (Only for Hybrid mode):
CAP User Config. Tool can be displayed on the Home screen.

1. Log in to the MFP as an Administrator.
2. Press and hold the Home screen. The [Add to Home] screen will appear.
3. Select [Icon].

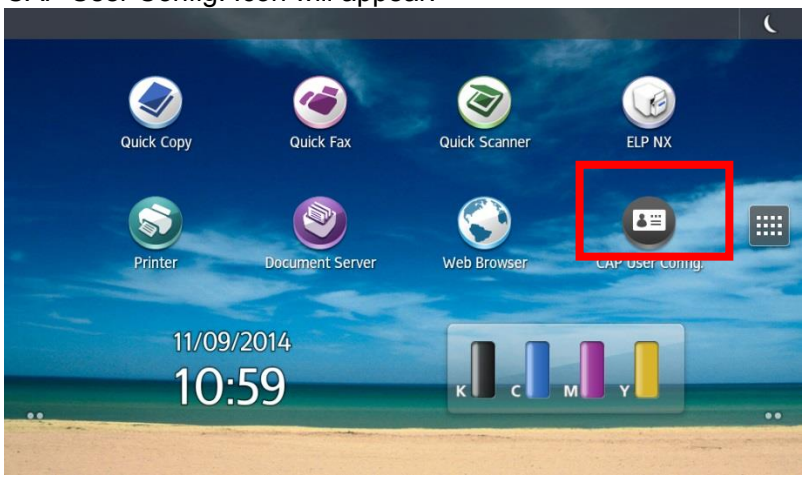


4. Select [Application].



5. Select [CAP User Config.].

6. CAP User Config. Icon will appear.

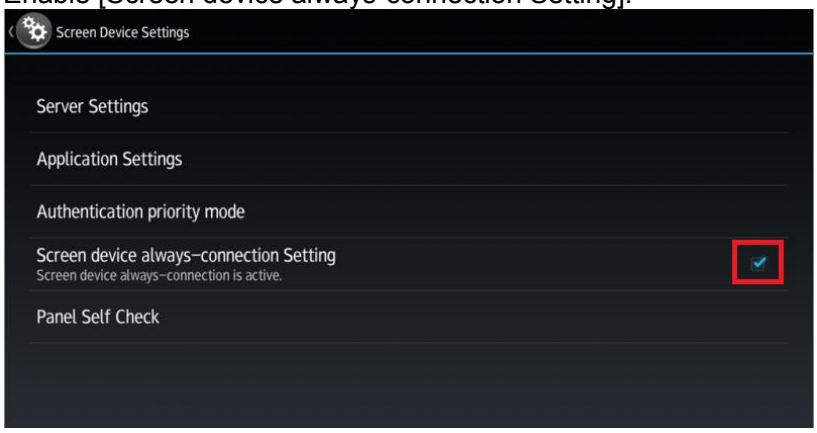


Screen device always-connection Setting (15S or later models)

1. Shift to Screen service mode.

   Note

   For information on how to enter Screen service mode, contact the supervisor in your branch office.
2. Select [Screen Device Settings].
3. Enable [Screen device always-connection Setting].

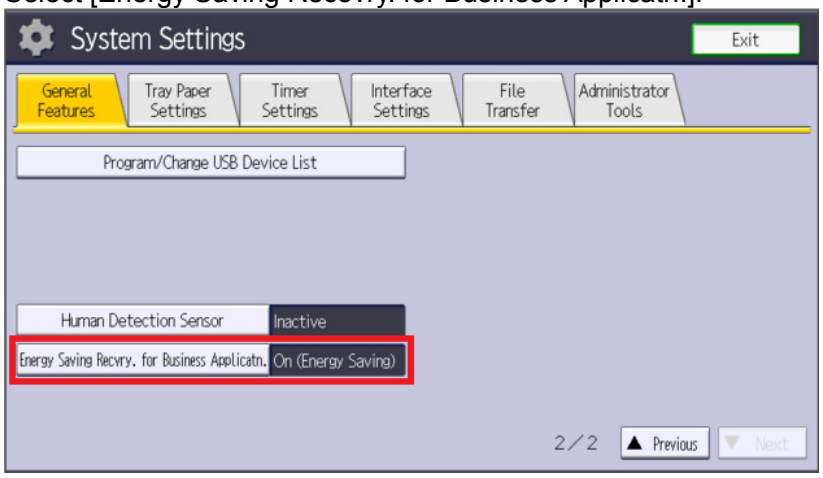


Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

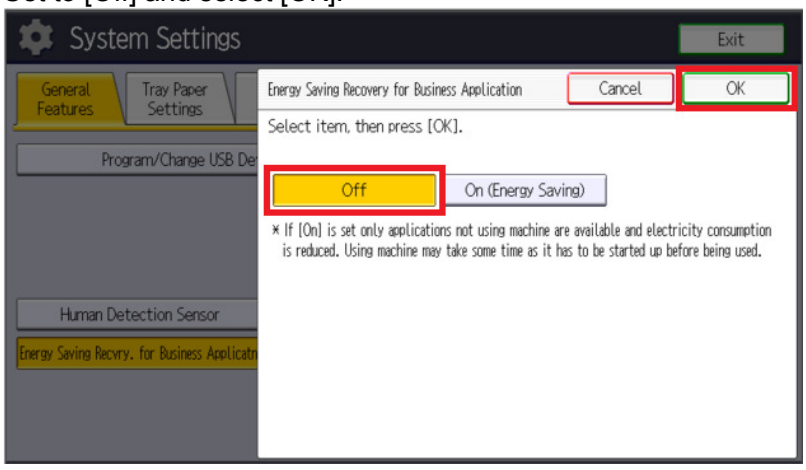
Recommendation: Energy Saving Recovery for Business Application setting (15S or later models)

If the setting is “On”, login may be little slow at the first time after recovering the energy saving. We recommend setting this as “Off”.

1. Log in to the MFP as an Administrator.
2. Select [User Tools].
3. Select [Machine Features].
4. Select [System Settings].
5. Select [Energy Saving Recovry. for Business Applicatn.].



6. Set to [Off] and select [OK].



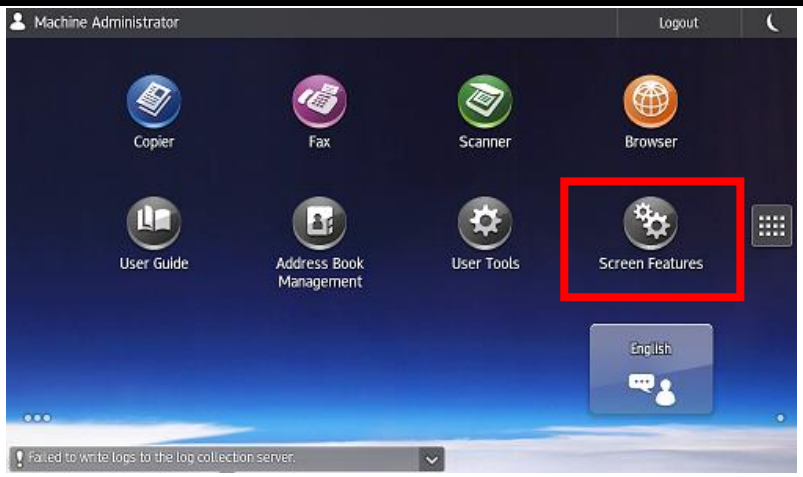
Priority Feature Setting (Only for Compatibility mode):

It is possible to select CAP LAUNCHER as a default application when a user logs in to the device.

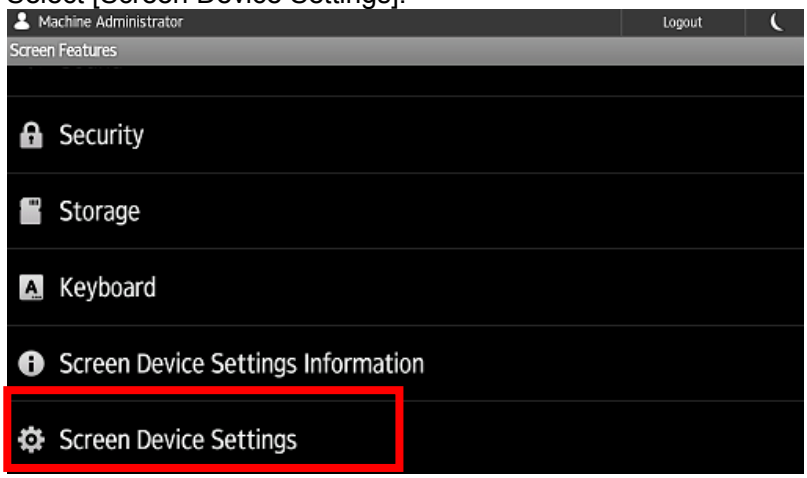
How to configure Function Priority:

1. Log in to the MFP as an Administrator.
2. Select [Screen Features].

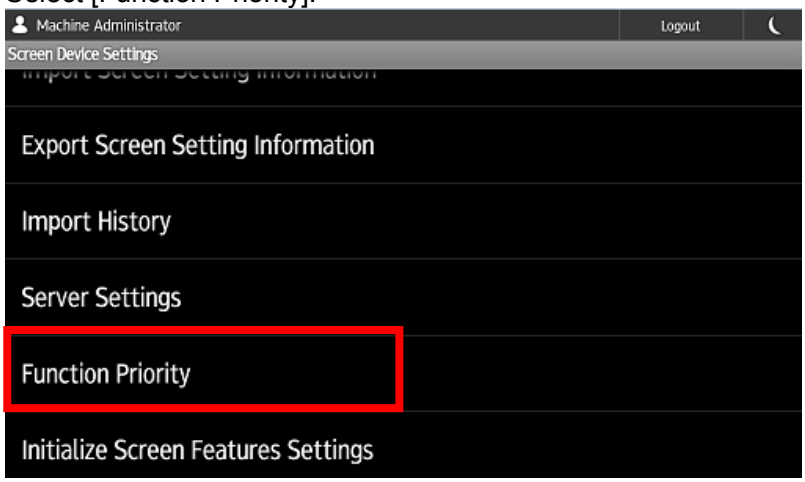
Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k



3. Select [Screen Device Settings].

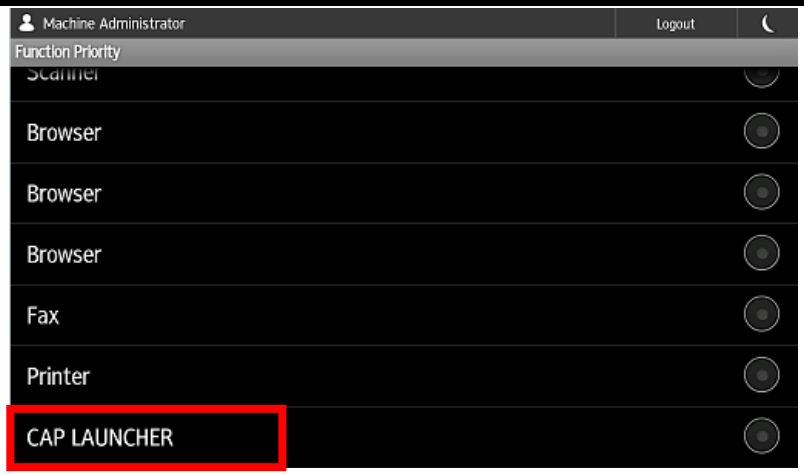


4. Select [Function Priority].



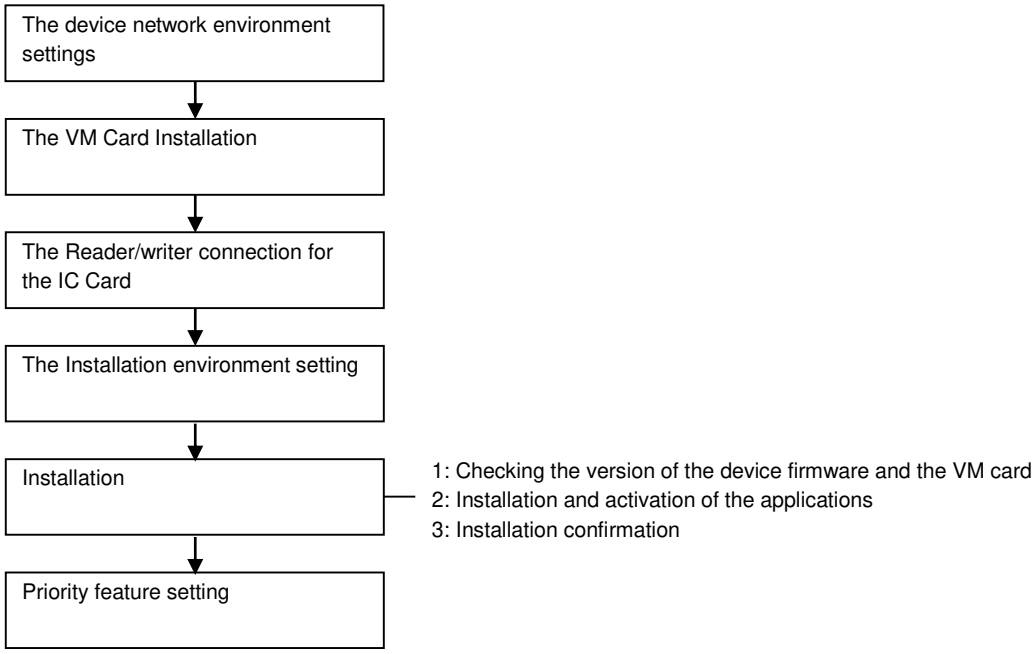
5. Select [CAP LAUNCHER].

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k



Installation (4-line MFP/4-line LP/LP)

Installation Flowchart



Installation Environment Settings

Set the following network information from system settings in the device.

- Host Name
- IP Address
- Subnet Mask
- Default Gateway
- DNS Server 1
- DNS Server 2
- DNS Server 3

- Domain Name

VM Card Installation

1. Set [Energy Saver Timer] to 5 minutes in [User Tools / Counter / Enquiry] screen → [System Settings] → [Timer Settings] tab.

   Note
   - [Energy Saver Timer] at the device side should be set to 5 minutes to prevent the device from entering the Energy Saver mode while the Java ™ Platform is installing or activating.
2. Insert the VM card into the SD card slot.

   Note
   - For which the SD card slot should be inserted into, see the service manual of each machine.
3. Turn on the main power of the device.

   Note
   - The Java ™ Platform is installed automatically if the main power of the device is turned on after the VM card insertion.
   - It takes for approx. from 3 to 4 minutes to install it automatically.
   - Never turn off the power of the device during the installation, otherwise it may damage the VM card. Turn off the power after the confirmation in step 8 has been done.
4. Access to the machine with Web Image Monitor.
5. Log in the machine as an administrator.

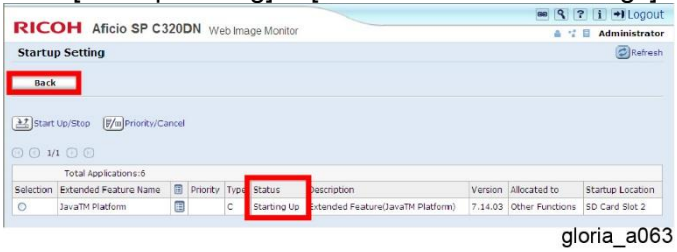
   Note
   - The initial value of login data is as follows:
   - Login user name: admin
   - Password: [blank]

gloria_a061

6. Click [Configuration] in the left menu.

gloria_a062

7. Click [Startup Setting] in [Extended Feature Settings] menu.

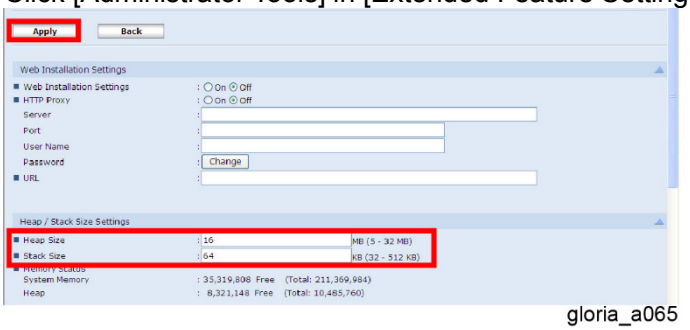


gloria_a063

8. Confirm that the status of [JavaTM Platform] is [Starting Up].
9. Click [Back].

gloria_a064

10. Click [Administrator Tools] in [Extended Feature Settings] menu.



gloria_a065

11. Set [Heap Size] to 16 MB, and set [Stack Size] to 64 KB.
12. Click [Apply].
13. Log out from Web Image Monitor.
14. Select [Shutdown] from the menu of the device.

Note

- Never turn off the power of the device before the shutdown, otherwise the HDD may be damaged.

15. Turn off the power.

Note

- The VM card should be operated with setting in the SD card slot.

IC Card Reader/Writer connection

Note

- The installation should be executed after the main power is turned off.

Connect the IC card Reader/Writer to the device.

Authentication Management Settings

1. Open Web Image Monitor.
2. Log in Web Image Monitor as an administrator.

Note

- The initial value of login data is as follows:
- Login user name: admin
- Password: [blank]

gloria_a061

3. Click [Configuration] in the left menu.

gloria_a072

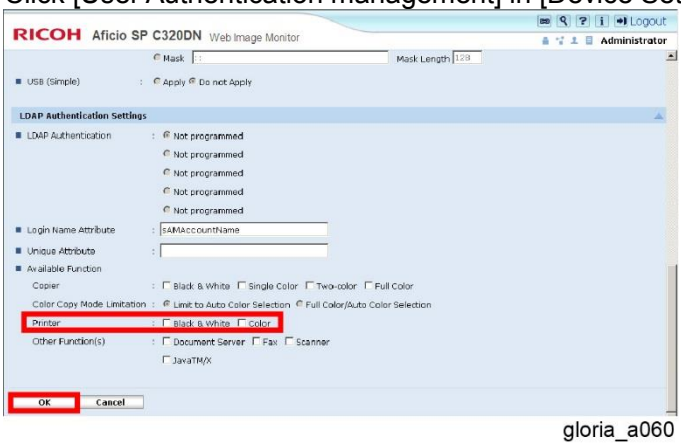
4. Click [Administrator Authentication Management] in [Device Settings] menu.

gloria_a073

5. Check [On] at the following items.
   [User Administrator Authentication]
   [Machine Administrator Authentication]
   [Network Administrator Authentication]
   [File Administrator Authentication]
6. Click [OK], and enable settings.

gloria_a074

7. Click [User Authentication management] in [Device Settings] menu.



gloria_a060

8. Remove all check marks in [Available Function: Printer] of [LDAP Authentication Settings] or [Custom Authentication Settings].
9. Click [OK], and enable settings.
10. Log out from Web Image Monitor.

11. Select [Shutdown] from the menu of the device.
12. Turn off and on the power of the device.

Card Authentication Package V2 Installation

For the Card Authentication Package V2 installation, install it with Remote Install Manager. See the service manual of Remote Install Manager. (☛ Remote Install Manager)

Automatic Startup Settings

The following applications should be set to start up automatically.

- CAP
- CAP LAUNCHER
- CAP V2 MP21/SP11

1. Open Web Image Monitor.
2. Log in to Web Image Monitor as an administrator.

Note

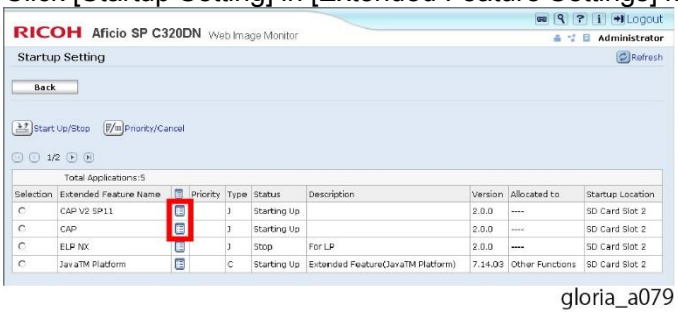
- The initial value of login is as follows:
- Login user name: admin
- Password: [blank]

gloria_a061

3. Click [Configuration] in the left menu.

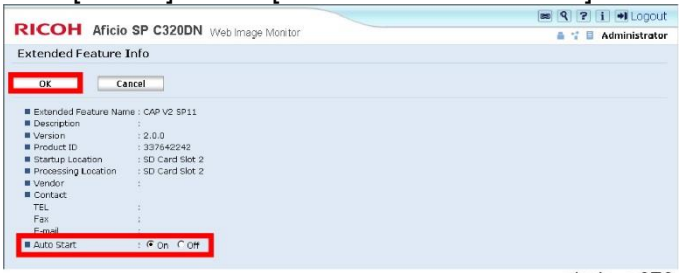
gloria_a071

4. Click [Startup Setting] in [Extended Feature Settings] menu.



gloria_a079

5. Click [Details] icon of [Extended Feature Name] for the target application.



gloria_a078

6. Check [On] at [Auto Start] and click [OK].
7. Reboot the device.

Installation Check

1. Turn on the power of the device.
2. Log in Web Image Monitor as an administrator.

Note

- The initial value of login data is as follows:
- Login user name: admin
- Password: [blank]

gloria_a061

3. Click [Configuration] in the left menu.

gloria_a071

4. Click [Extended Feature Info] in [Extended Feature Settings] menu.
5. Refer to the application list, and confirm that the condition of each application is the same as below:

Application	Status
CAP V2 MP21/SP11	Starting Up
CAP LAUNCHER	Suspend
CAP	Starting Up
CAP REG	Stop
JavaTM Platform	Starting Up

Priority Feature Setting

1. Press [Maintenance] → [General Settings] → [Function Priority] from the menu of the device.
2. Select [Java TM/X].

Note

- The procedure of this setting differs from devices so that see the service manual of the device.

When Migrate to Card Authentication Package v2 from v1

Migration from Card Authentication Package v1 to v2 requires the conversion of the user information from Card Authentication Package v1's format to v2's format.

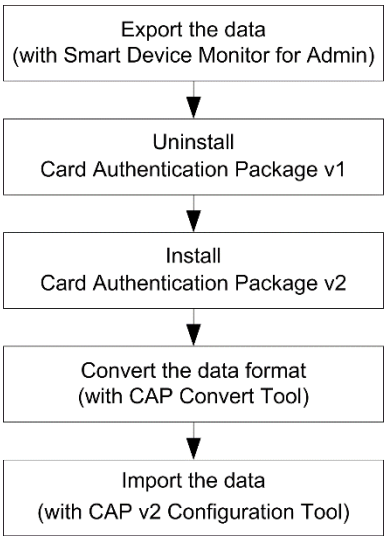
Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

The following explains the conversion procedure using CAP Convert Tool.

Note

- For CAP Convert Tool, JRE v6.0 or later is required on the host PC.

Conversion Flowchart



gloria_ap003

Export the Data

The following three files are required in order to convert the Card Authentication Package v1 data into v2 data.

- Card information file: card(date).csv
- User information file: (model name)_user.csv
- Address information file: (model name)_addr.csv

These exports have to be done before uninstalling v1.

1) Export the card information

1. Click [Maintenance] to show [Card ID Mapping Maintenance] screen.

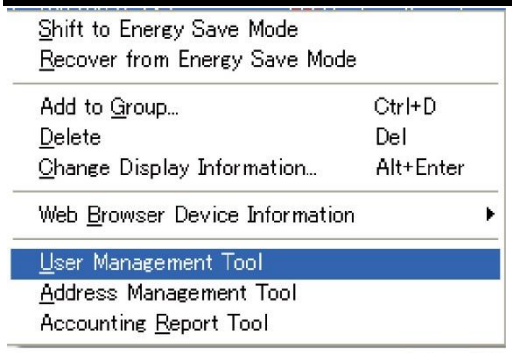
gloria_a051

2. Click [Export].

The export operation creates a CSV file containing the card information.

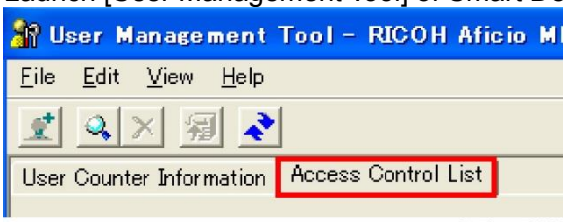
Example: cardmmdd.csv (mmdd: an exported month (mm) and day (dd))

2) Export the user information



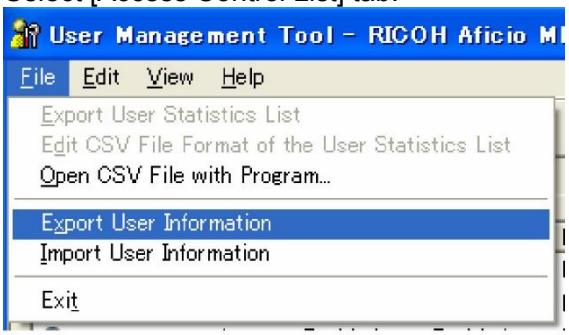
gloria_a052

1. Launch [User Management Tool] of Smart Device Monitor for Admin.



gloria_a053

2. Select [Access Control List] tab.

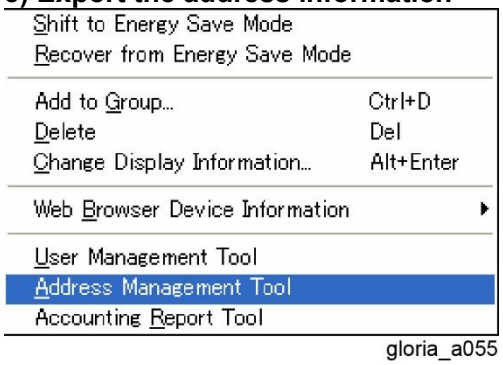


gloria_a054

3. Select [Export User Information] from [File] menu.

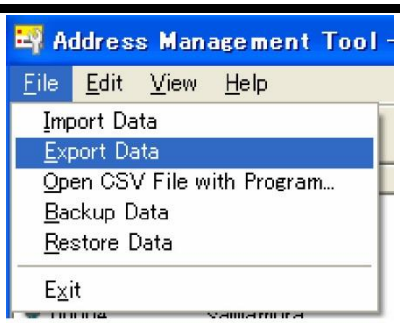
The user information is exported as a CSV file.
Example (for an Aficio MP C5000): Aficio_MP_C5000_user.csv

3) Export the address information



gloria_a055

1. Launch [Address Management Tool] of Smart Device Monitor for Admin.



gloria_a056

2. Select [Export Data] from [File] menu.

Three CSV files are created by the export process and one of them is needed for the conversion.

Example (for an Aficio MP C5000):

Aficio_MP_C5000_faxinfo.csv
Aficio_MP_C5000_taginfo.csv
Aficio_MP_C5000_addr.csv (Only this file is needed for the conversion.)

Uninstall Card Authentication Package v1

For the Card Authentication Package v1 uninstallation, see the service manual for Card Authentication Package v1. (☛ Card Authentication Package v1 Service Manual)

Install Card Authentication Package v2

For the Card Authentication Package v2 installation, install it with Remote Install Manager. See the service manual of Remote Install Manager. (☛ Remote Install Manager)

Convert the Data Format

1. Before running CAP Convert Tool, put the tool and the files into the same directory.
   - CAP Convert Tool: DataConvertFromCap.exe
   - Card information file: card(date).csv
   - User information file: (model name)_user.csv
   - Address information file: (model name)_addr.csv
2. CAP Convert Tool is a command-line tool. Open a command prompt and switch to the directory where the files are located.
3. Enter the following command.
   DataConvertFromCap.exe (User information file name) (Address information file name) (Card information file name) [Character-code]

   Note
   - If any character code is not specified, “Cp1252” will be used as a default.
   - For a list of supported character encoding types, refer to the 2nd column of the following list:
   - http://download.oracle.com/javase/1.5.0/docs/guide/intl/encoding.doc.html
4. A message is displayed when the conversion is complete. The message includes the following information:
   - User information registered (total item)
   - Convert user information items (succeeded)
   - Input format error items (failed)
   - Conversion error items (failed)

   If there is no error, close the command prompt.

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Import the Data

A successful conversion creates the following two files:

- DataConvertFromCap.csv
  This is the user information file for Card Authentication Package v2.
  To import the data, use CAP v2 Configuration Tool.
- DataConvertFromCap.log
  This log contains the conversion results and the error information.

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Uninstallation

Uninstallation

Uninstallation (WVGA/4.3-inch operation panel models)

- Depending on the device model, the actual operation panel screen may look different from the screenshots used in this document.

Setting in the Device

Set [Enhanced Authentication Management] in [Security Management] to [Off].

Note

- The SC636 error will occur when ignoring the process above.

SP Mode Cancellation

Restore the SP values described below. In the case of Smart Operation Panel model, press the [x] button on the login screen and select the [Printer] icon after logging out, and then go into SP mode. It is not possible to log in to SP mode from User Tools or Quick application (such as Quick Copy) and when logged into the device.

- SP5-401-103: [3] → [0]
- SP5-401-162: bit0 [1] → [0], bit5 [1] → [0], bit6 [1] → [0]
- SP5-401-230: bit0 [1] → [0]
- SP5-401-240: bit0 [1] → [0]

Note

- The machine should be rebooted after the settings are changed.
- The setting changes are not necessary if the reinstallation is executed.

Priority Feature Cancellation

In the case of Normal Operation Panel models:

1. Press [User Tools/Counter] button, and then press [Screen Device Settings].
2. Press [General Features] tab, and then press [Function Priority].
3. Select an item on the screen other than [Java TM/X] and press [OK].

In the case of Smart Operation Panel models:

1. Press [Screen Features] button, and then press [System Settings].
2. Press [Function Priority].
3. Select an item on the screen other than [CAP User Config.] and press [OK].

Authentication Management Settings

1. Log in the device as an administrator.

Note

- The initial value of login data is as follows:
- Login user name: admin
- Password: [blank]

2. Press [User Tools/Counter] button, and then press [System Settings].
3. Press [Administrator Tools] tab, and set items below:
   [User Authentication Management]
   [Administrator Authentication Management]

1) User Authentication Management

4. Set the method of the authentication is “Off”.
5. Press [OK] of the upper right.

2) Administrator Authentication Management

[User management]

6. Set [Admin. Authentication] to [Off].

[Machine Management]

7. Set [Admin. Authentication] to [Off].

[Network Management]

8. Set [Admin. Authentication] to [Off].

[File Management]

9. Set [Admin. Authentication] to [Off].
10. Press [OK] of the upper right.

Turn the power off and on after the settings of [Administrator Authentication Management] and [User Authentication Management] are finished.

Card Authentication Package V2 Uninstallation

For the Card Authentication Package V2 uninstallation, uninstall it with Remote Install Manager. See the service manual of Remote Install Manager. (☛ Remote Install Manager)

Uninstallation (4-line MFP/4-line LP/LP)

Setting in the Device

Set [Enhanced Authentication Management] in [Security Management] to [Off].

Note

- The SC636 error will occur when ignoring the process above.

Setting with Web Image Monitor

1. Open Web Image Monitor.
2. Log in the machine as an administrator.

Note

- The initial value of login data is as follows:
- Login user name: admin
- Password: [blank]

gloria_a061

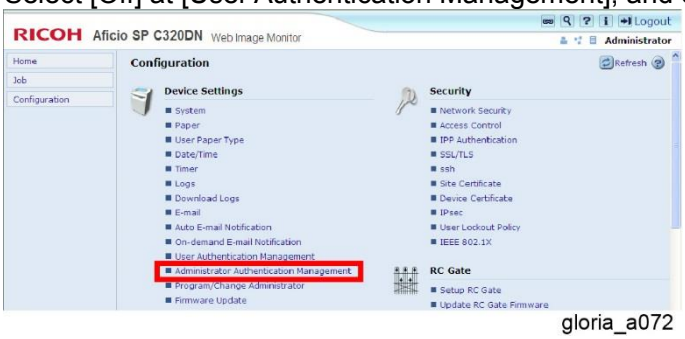
3. Click [Configuration] in the left menu.

gloria_a074

4. Click [User Authentication Management] in [Device Settings] menu.

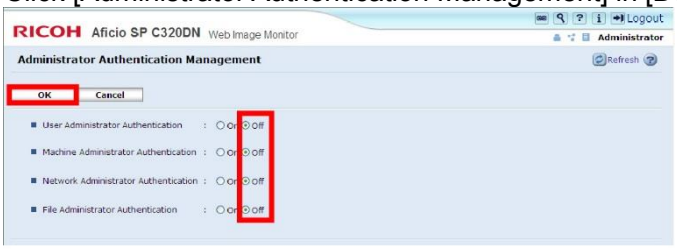
gloria_a075

5. Select [Off] at [User Authentication Management], and click [OK].



gloria_a072

6. Click [Administrator Authentication Management] in [Device Settings] menu.



gloria_a076

7. Check [Off] at the following items, and click [OK].
   - User Administrator Authentication
   - Machine Administrator Authentication
   - Network Administrator Authentication
   - File Administrator Authentication
8. Turn off and on the power of the device.
9. Execute the uninstallation with Remote Install Manager. For details, see the service manual of Remote Install Manager. (☛ Remote Install Manager)

SP Mode Cancellation

Restore the SP values described below.

- SP5-401-103: [3] → [0]
- SP5-401-162: bit0 [1] → [0], bit5 [1] → [0]
- SP5-401-230: bit0 [1] → [0]

- SP5-401-240: bit0 [1] → [0]

Note

- The machine should be rebooted after the settings are changed.
- The setting changes are not necessary if the reinstallation is executed.

Priority Feature Cancellation

1. Press [Maintenance] → [General Settings] → [Function Priority] from the menu of the device.
2. Select an item on the screen other than [Java TM/X].

Note

- The procedure of this setting differs from devices so that see the service manual of the device.

Model: Card Authentication Package v2	Date: 12-Mar-12	No.: RD602007k

Appendix

VM Card Update

VM Card Update

Note
- The steps below should be followed when updating the VM card if CAPv2 is installed.

1. Disable Enhanced Authentication Management (SP5-401-160: [1] → [0]).

Note
- Proceed to step 2 without rebooting the device.

2. Update the VM card using Remote Install Manager.
3. Reboot the device two times (some settings are automatically set during the 1st reboot that require a 2nd reboot to enable).

Procedure for changing the HDD

1. Export the user/device settings via the Configuration Tool for back up. (If possible)
   File --> Export --> Select User Information and Device Settings for export --> Click the "Export" button.
2. Uninstall all the applications (CAP) using Remote Install Manager.
3. Change out the HDD.

Note
- Please refer to the device service manual to change out the HDD.

4. Reinstall all the applications (CAP) using Remote Install Manager.
5. Import the user/device setting in Configuration Tool.
3. File --> Import --> Browse for the User Information and Device Settings --> Click the "Import" button.

Procedure for changing the controller board

This procedure is available in the case that Java VM is installed to the device's flash memory (FM) on the controller board.

1. Export the user/device settings via the Configuration Tool for back up. (If possible.)
   File --> Export --> Select User Information and Device Settings for export --> Click the "Export" button.
2. Uninstall all applications (CAP) via Remote Install Manager.

Note
- In the case that the controller board needs to be replaced when using Hybrid mode:
  If it is necessary to replace the controller board, the Smart Operation Panel applications

will remain. Therefore, the applications should be uninstalled using RIM.

3. Disable the Java VM (SP5-730-001: [1] -> [0]). Then restart the device.
4. Change out the controller board.

Note

- Please refer to the device service manual to change out the Controller Board.

5. Reinstall all the applications (CAP) using Remote Install Manager.
6. Import the user/device setting in configuration tool.
   File --> Import --> Browse for the User Information and Device Settings --> Click the "Import" button.

Procedure for changing the Smart Operation Panel

This procedure is available when changing to a Smart Operation Panel from a Standard Operation Panel or if a Smart Operation Panel needs to be replaced.

1. Export the user/device settings via the Configuration Tool for back up. (If possible.)
   File --> Export --> Select User Information and Device Settings for export --> Click the "Export" button.
2. Uninstall all applications (CAP) via Remote Install Manager.

Note

- In the case that the Smart Operation Panel needs to be replaced when using Hybrid mode:
  If it is necessary to replace the Smart Operation Panel, the DSDK applications installed in the Java VM will remain. Therefore, these applications should be uninstalled via Web image Monitor. The uninstallation method via Web Image Monitor is as follows.
  WIM -> Configuration -> “Uninstall” in Extended Feature Settings

- The reason for why the DSDK applications must be uninstalled via WIM is as follows:
  As per the specification for the eDC-i system, the DSDK applications installed in the Java VM and the Smart Operation Panel applications are regarded as 1 application. When the Smart Operation Panel is replaced (the DSDK applications are left and the Smart Operation Panel applications disappear), the eDC-i system will judge that both the DSDK applications and the Smart Operation Panel applications are deleted. This will cause an error to occur when uninstalling via RIM. Therefore, it is necessary to uninstall the remaining DSDK applications via WIM in order to clear the error in RIM.

- In the case that the Smart Operation Panel needs to be replaced when using Hybrid mode:
  It is necessary to forcibly deactivate the license key in advance. Please contact the marketing section in your branch office regarding the deactivation method.

3. Reinstall all applications (CAP).
4. Import the user/device settings via the Configuration Tool.
   File --> Import --> Browse for the User Information and Device Settings --> Click the "Import" button.