AU-211P CAC/PIV Solution

Users Guide

1 Introduction

Thank you for choosing this device.

This guide provides descriptions of the installation, operating procedures and precautions for using Authentication Unit (IC Card Type) AU-211P. Carefully read this User's Guide before using this device.

The actual screens that appear may be slightly different from the screen images used in this User's Guide.

Trademark/copyright acknowledgements

- Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- All other company names and product names mentioned in this User's Guide are either registered trademarks or trademarks of their respective companies.

Restrictions

- Unauthorized use or reproduction of this User's Guide, whether in its entirety or in part, is strictly prohibited.
- The information contained in this User's Guide is subject to change without notice.

1.1 Safety Information

Carefully read this information.

- Before using this device, carefully read this information and follow it to operate the device correctly.

Important information

- The reprinting or reproduction of the content of this publication, either in part or in full, is prohibited without prior permission.
- The content of this publication is subject to change without notice.
- This publication was created with careful attention to content; however, if inaccuracies or errors are noticed, please contact your sales representative.
- The marketing and authorization to use our company's product mentioned in this information are provided entirely on an "as is" basis.
- Our company assumes no responsibility for any damage (including lost profits or other related damages) caused by this product or its use as a result of operations not described in this information. For disclaimers and warranty and liability details, refer to the User's Guide Authentication Unit (IC Card Type AU-211P).
- This product is designed, manufactured and intended for general business use. Do not use it for applications requiring high reliability and which may have an extreme impact on lives and property. (Applications requiring high reliability: Chemical plant management, medical equipment management and emergency communications management)
- Use with other authentication devices is not guaranteed.
- In order to incorporate improvements in the product, the specifications concerning this product are subject to change without notice.

For safe use

	• Do not use this product near water, otherwise it may be damaged. • Do not cut, damage, modify or forcefully bend the USB cable. A malfunction may occur as a result of a damaged or cut USB cable. • Do not disassembly this device, otherwise it may be damaged.

Regulation notices

USER INSTRUCTIONS FCC PART 15 - RADIO FREQUENCY DEVICES (For U.S.A. Users)

FCC: Declaration of Conformity	
Product Type	Authentication Unit (IC Card Type)
Product Name	AU-211P
(This device complies with Part 15 of the FCC Rules.) Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device.	

NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interface by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING:

The design and production of this unit conform to FCC regulations, and any changes or modifications must be registered with the FCC and are subject to FCC control. Any changes made by the purchaser or user without first contacting the manufacturer will be subject to penalty under FCC regulations.

INTERFERENCE-CAUSING EQUIPMENT STANDARD (ICES-003 ISSUE 4) (For Canada Users)

(This device complies with RSS-Gen of IC Rules.) Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

5 How to Use the Authentication Unit

This chapter explains how to log in and authenticate a CAC/PIV card user onto the network via the MFP. This chapter also explains how to log a user off the network/MFP.

5.1 Login and Logout

5.1.1 Login

Use the following steps to log into the MFP.

1 Insert a CAC/PIV card in the reader.

2 Enter the PIN code.

- You can use the keypad on the MFP to enter the PIN code.

- Or you can press the [PIN] button, a keyboard screen appears use this keyboard screen to enter a PIN code.

Detail

If an incorrect PIN code is entered, "No. of Allowable Auth Failure" appears on the screen. After 3 consecutive authentication failures the CAC/PIV card will be locked for security reasons. For details on how to unlock the CAC/PIV card, contact your PKI card administrator.

3 Press [OK].

This starts authentication. Successful authentication grants a user access the MFP.

Detail

When Account Track is enabled, use the CAC/PIV card to perform user authentication before account authentication. When Account Track is enabled on the MFP that supports this system, user authentication is forcibly associated with account authentication.

Detail

You can log in as a public user if Public User Access is enabled.

If logging into the MFP as an administrator or User Box administrator, press [ID & PW], and enter the password

Detail

If you log into the MFP as an administrator, you can check or delete the desired job. If you log into the MFP as a User Box administrator, you can view the contents of all the created User Boxes regardless of whether a password has been specified.

5.1.2 Logout

To log out the MFP, pull the CAC or PIV card out of this unit.

Detail

If a PKI card is used to log in to the MFP, you cannot log out by pressing the [ID] key on the control panel.

If the MFP sub power is turned off while logging in using the PKI card, you will be logged out of the MFP.

5.2 Specific MFP Functions Using CAC/PIV Card Authentication

This section explains the specific MFP functions using the CAC/PIV card authentication.

Basic functions

Function	Description	See
Address Search (LDAP)	Logs into the LDAP server using the Kerberos authentication ticket that is obtained by Active Directory authentication with the CAC/PIV card when searching for the destination via the LDAP server. The user can perform authentication only once to obtain access privileges, and configure the single sign-on environment to be convenient.	p. 72
Scan to SMB (Network Share)	Logs into the destination computer using the Kerberos authentication ticket that is obtained by Active Directory authentication with the CAC/PIV card when sending scanned data via SMB. The user can perform authentication only once to obtain access privileges, and configure the single sign-on environment to be convenient.	p. 76
Scan to E-mail (S/MIME)	Encrypts an e-mail or adds a digital signature using the CAC/PIV card when sending an e-mail. This function prevents tapping, fabrication or spoofing of an e-mail.	p. 79
PKI Card Print (confidential printing)	The user can encrypt print data using the CAC/PIV card before sending the data to the MFP. The print data is saved temporarily in the MFP. Once the same user performs authentication at the MFP with the CAC/PIV card, the data is decrypted and printed. The print data is encrypted when it is sent from the printer driver and can only be printed when authentication at the MFP using the CAC/PIV card is successful; therefore, you can ensure the confidentiality of documents.	p. 82

Ensuring a higher level of security

To ensure a higher level of security, use the Scan To Me and Scan To Home functions.

Note

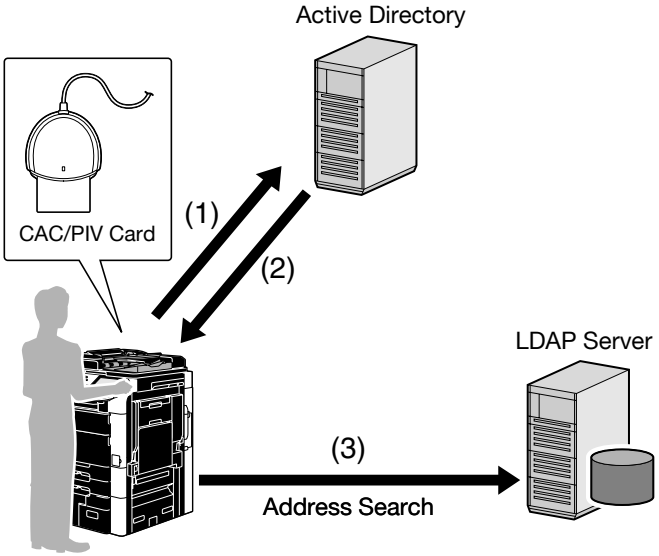
To use these functions, ask your service engineer to configure settings. For details, contact your service representative.

Function	Description	See
Scan To Me	Sends scanned data to the user's e-mail address. The user can obtain the user's e-mail address using the LDAP protocol, and easily send data to the obtained address. This function is effective when frequently sending scanned data to a user's address. When this function is enabled, the user cannot use some functions to ensure higher level security. For details, refer to the relevant page.	p. 90
Scan To Home	Sends scanned data to the user's computer. The user can obtain the position of the user's Home folder from Active Directory, and easily send data to the Home folder of the user's computer. This function is effective when frequently sending scanned directly to their Home folder. When this function is enabled, the user cannot use some functions to ensure higher level security. For details, refer to the relevant page.	p. 95

5.3 Address Search (LDAP)

5.3.1 Overview

This function will allow a CAC/PIV card user to log in to an LDAP server and perform an address name search. The process utilizes a Kerberos authentication ticket that is obtained by Active Directory and authenticates with the CAC/PIV card when searching for a destination via the LDAP server.



(1) Insert the CAC/PIV card into the MFP to perform Active Directory authentication.

(2) Obtain the Kerberos authentication ticket.

(3) Use the Kerberos authentication ticket to log in to the LDAP server and search for the destination.

...

Note

This function is not available when you log in to the MFP as a public user or User Box administrator.

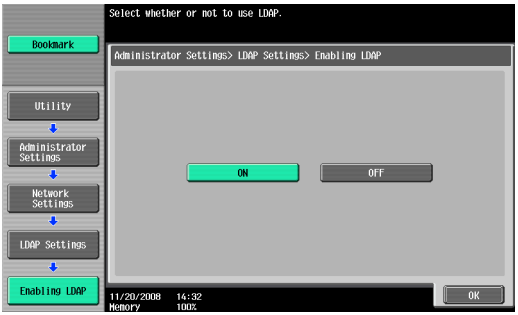
5.3.2 LDAP Related Settings

This section explains how to configure the address search (LDAP) settings on the MFP that supports this system.

Enabling LDAP

Configure settings to use the LDAP server.

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [LDAP Settings] - [Enabling LDAP].

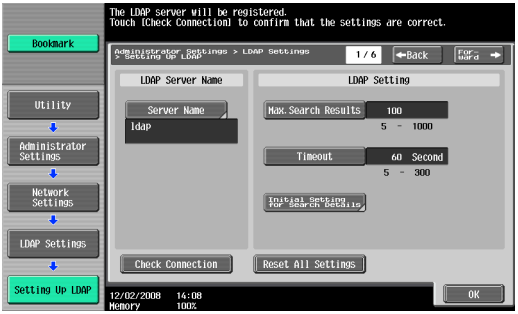


Item	Description
Enabling LDAP	Select [ON].

Setting Up LDAP

Register the desired LDAP server to search for the destination.

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [LDAP Settings] - [Setting Up LDAP].



Item	Description
LDAP Server Name	Specify the LDAP server name (up to 32 characters).
Max. Search Results	Enter the maximum number of items that can be received as address search (LDAP) results.
Timeout	Specify the timeout period for address search (LDAP).
Initial Setting for Search Details	Specify address search (LDAP) conditions.
Server Address	Specify the conditions of address search (LDAP).
Search Base	Specify the search starting point in the directory structure under the LDAP server (up to 255 characters). This search function also covers subdirectories under the specified starting point.
SSL Setting	Select "ON" to encrypt communication between the MFP and LDAP server with SSL.
Port Number	Specify the LDAP port number.
Port Number (SSL)	Enter the desired port number for SSL communication.
Referral Setting	Select whether to use the referral function. Match the LDAP server environment.
Domain Name	Specify the domain name to log in to the LDAP server (up to 64 characters).

Detail

On the MFP that supports this system, "Authentication Type" is automatically set to "GSS-SPNEGO". "Select Server Authentication Method" is automatically set for user authentication.

5.3.3 Performing an Address Search (LDAP) at the MFP

Use the Fax/Scan screen on the MFP control panel, and press [Address Search]. The procedures can vary depending on whether a single or multiple LDAP servers are registered.

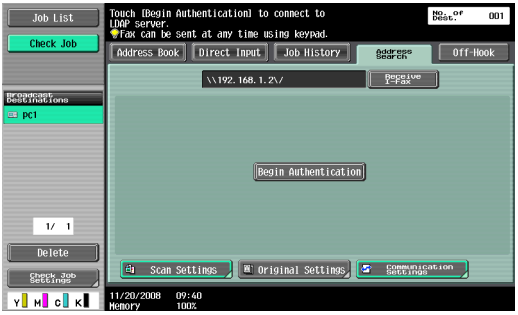
Note

If address search (LDAP) setting incorrectly configured properly, [Address Search] will not appear. Check that the address search (LDAP) setting is configured correctly.

When a single LDAP server is registered

Press [Begin Authentication] to perform authentication with the Kerberos authentication ticket and connect to the LDAP server.

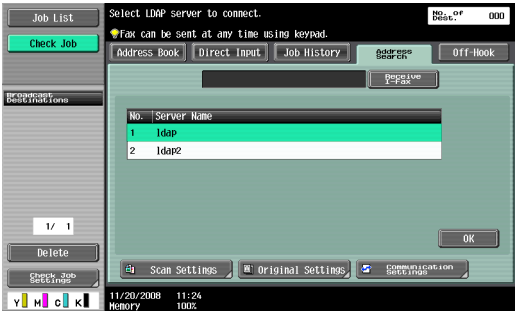
After connecting to the LDAP server, select the desired method to search for the destination.



When multiple LDAP servers are registered

Select the LDAP server to search, and press [OK]. Perform authentication using the Kerberos authentication ticket, and connect to the LDAP server.

After connecting to the LDAP server, select the desired method to search for the destination.



...

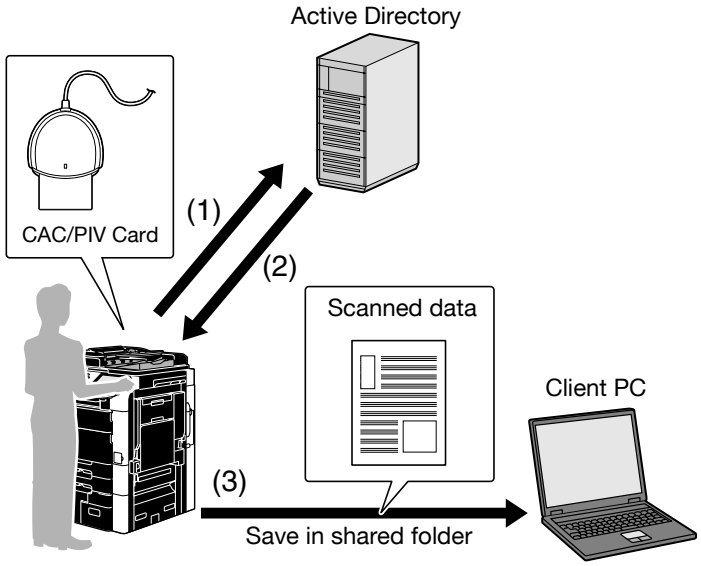
Note

For details on the address search (LDAP) function, refer to the User's Guide [Network Scan/Fax/Network Fax Operations] supplied together with the MFP.

5.4 Scan to SMB (Network Share)

5.4.1 Overview

This function allows a user to scan a document into the destination computer via SMB using a Kerberos authentication ticket that is obtained by Active Directory and authenticates with the CAC/PIV.



(1) Insert the CAC/PIV card into the MFP to perform Active Directory authentication.

(2) Obtain the Kerberos authentication ticket.

(3) Use the Kerberos authentication ticket to log in to the destination computer and save scanned data.

...

Note

This function is not available while logged into the MFP as a public user or as a User Box administrator.

5.4.2 Scan to SMB Related Settings

This section explains how to configure the Scan to SMB settings on the MFP.

Client Settings

Configure the setting to perform SMB TX.

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [SMB Settings] - [Client Settings].

Item	Description
ON/OFF	Select [ON].
SMB Auth Setting	Select [Kerberos] or [Kerberos/NTLMv2/v1] as the SMB TX authentication method. The default is [Kerberos]. In an NTLM authentication environment, select [Kerberos/NTLMv2/v1].
DFS Setting	To perform SMB TX in a DFS (Distributed File System) environment, select "Enable".
Password Authentication Restriction	This system applies the user account of the CAC/PIV card to perform authentication even if the user ID or password is registered in the SMB TX address included in the address book. In this item, specify the action to be taken when authentication has failed using the user account of the CAC/PIV card. If "Limit" is selected, it results in an authentication failure. If "Do Not Limit" is selected, enter the user ID and password on the control panel when sending data.

Note

Specify the WINS server or direct hosting service to fit your environment. For details, refer to the User's Guide [Network Administrator] supplied together with the MFP.

5.4.3 Performing Scan to SMB at the MFP

Use the Fax/Scan screen on the MFP control panel to specify the target SMB address.

When SMB TX starts, you can use the Kerberos authentication ticket to log into the destination computer and save scanned data in a shared holder.

Note

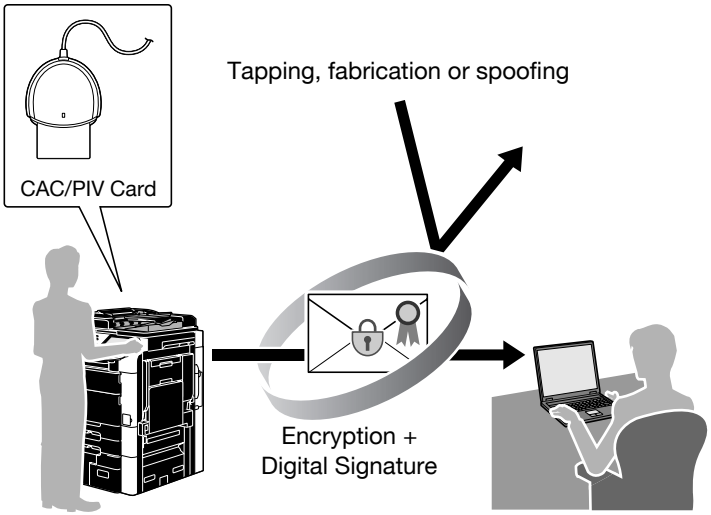
For details on how to register the SMB address or use SMB TX, refer to the User's Guide [Network Scan/Fax/Network Fax Operations] supplied together with the MFP.

5.5 Scan to E-mail (S/MIME)

5.5.1 Overview

This function allows a CAC/PIV card user to authenticate and Scan to Email from the MFP. A user will be able to add a digital signature when sending an e-mail. Sending an e-mail with a digital signature enables you to prove you are the e-mail sender.

If a certificate is registered in the target address, you can combine this function with e-mail encryption when sending an e-mail. Sending an encrypted e-mail prevents information from being leaked to a third party on the transmission route.



Note

This function is not available when you log into the MFP as a public user or User Box administrator.

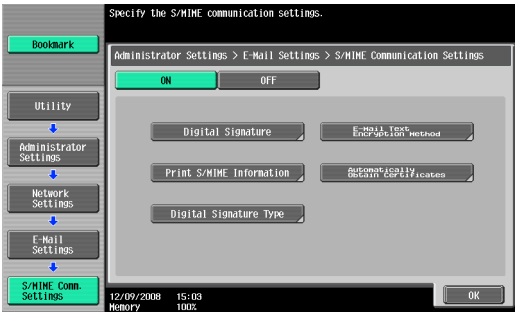
5.5.2 Scan to Email Related Settings

This section explains how to configure settings to encrypt an e-mail or add a digital signature on the MFP.

S/MIME Communication Settings

Configure settings to encrypt an e-mail and add a digital signature.

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [E-Mail Settings] - [S/MIME Communication Settings].



Item	Description
ON/OFF	Select [ON].
Digital Signature	To add a digital signature, select "Always add signature" or "Select when sending". The default is "Select when sending". If "Select when sending" is selected, specify whether to add a digital signature before sending an e-mail. If "Always add signature" is selected, a digital signature is automatically added using the CAC/PIV card when sending an e-mail.
Digital Signature Type	Select the digital signature type.
E-Mail Text Encryption Method	Select the e-mail text encryption method.

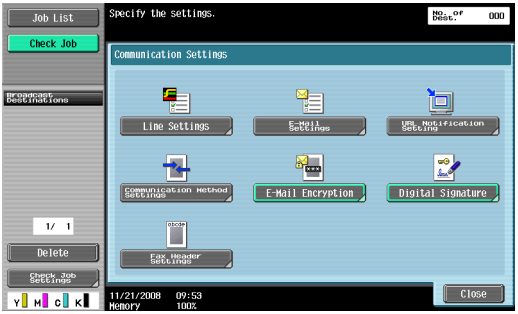
Note

For details on how to configure the settings required to send an e-mail, refer to the User's Guide [Network Administrator] supplied together with the MFP.

5.5.3 Encrypting an E-Mail and Adding a Digital Signature

Display the Fax/Scan screen on the MFP control panel, and press [Communication Settings].

- To encrypt an e-mail, press [E-Mail Encryption], and specify the e-mail address with the certificate registered.
- If "Select when sending" is selected to add a digital signature, press [Digital Signature] and specify the e-mail address. If "Always add signature" is selected, a digital signature will be automatically added.



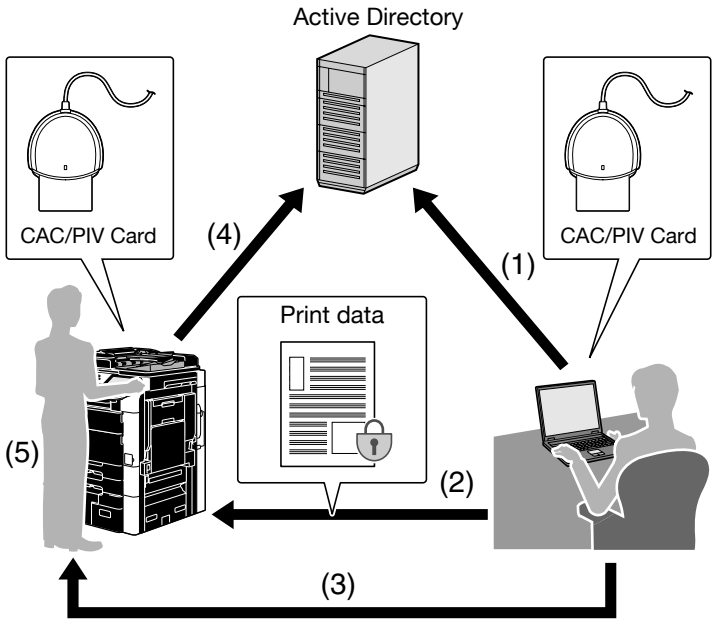
Detail

- *For details on how to send an e-mail, refer to the User's Guide [Network Scan/Fax/Network Fax Operations] supplied together with the MFP.*
- *For details on how to register the certificate in the e-mail address, refer to the User's Guide [Network Administrator] supplied together with the MFP.*
- *When adding a digital signature with a PIV card, enter the PIN code when sending an e-mail. If the PIV card is locked as a result of an incorrectly entered PIN code, the e-mail sending job will be discarded.*

5.6 PKI Card Print

5.6.1 Overview

This function encrypts print data using the CAC/PIV card before sending the data from the printer driver to the MFP. The print data is saved in the PKI Encrypted Document User Box of the MFP, when the user authenticates at the MFP using their CAC/PIV card the print data is decrypted and print is outputted. The print data is encrypted when it is sent from the printer driver and can only be printed when authentication at the MFP using the CAC/PIV card is successful; therefore, this ensures the confidentiality of the documents.



(1) Insert the CAC/PIV card into the computer to perform Active Directory authentication.

(2) Encrypt print data using the CAC/PIV card to send it from the printer driver to the MFP.

(3) Take the CAC/PIV card to the MFP.

(4) Insert the CAC/PIV card into the MFP to perform Active Directory authentication.

(5) Decrypt print data using the CAC/PIV card, and print it.

5.6.2 Installing the Printer Driver

To use PKI Card Print, install a printer driver compatible with this system in the computer.

Required System Environment

The printer drivers are available in the following environment.

Type	Page description language	Supported Operating System
PCL driver	PCL-XL	Windows 2000 Professional (SP4 or later) Windows XP Home Edition (SP1 or later) Windows XP Professional (SP1 or later) Windows XP Professional x64 Edition Windows Vista Home Basic * Windows Vista Home Premium * Windows Vista Business * Windows Vista Enterprise * Windows Vista Ultimate * Windows 2000 Server (SP4 or later) Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Enterprise Edition Windows Server 2003, Standard x64 Edition Windows Server 2003, Enterprise x64 Edition Windows Server 2003 R2, Standard x64 Edition Windows Server 2003 R2, Enterprise x64 Edition * Available in 32-bit (x86) or 64-bit (x64) environment.
PS driver	PostScript	Windows 2000 Professional (SP4 or later) Windows XP Home Edition (SP1 or later) Windows XP Professional (SP1 or later) Windows XP Professional x64 Edition Windows Vista Home Basic * Windows Vista Home Premium * Windows Vista Business * Windows Vista Enterprise * Windows Vista Ultimate * Windows 2000 Server (SP4 or later) Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Enterprise Edition Windows Server 2003, Standard x64 Edition Windows Server 2003, Enterprise x64 Edition Windows Server 2003 R2, Standard x64 Edition Windows Server 2003 R2, Enterprise x64 Edition * Available in 32-bit (x86) or 64-bit (x64) environment.

Installing the printer driver

Install the printer driver using Add Printer Wizard of the Windows printer.

<Windows XP or Server 2003>

Click the Start Menu, and then [Printers and Faxes].

- For Windows XP, click [Add a printer] under the [Printer Tasks] menu.
- For Windows Server 2003, double-click [Add Printer].

After the Add Printer Wizard appears, complete the installation by following the on-screen instructions.

<Windows Vista>

Installing the printer driver in Windows Vista requires administrator authority.

Click the Start Menu, and then [Control Panel]. Then click [Printer] from [Hardware and Sound], and click [Add a printer] on the toolbar.

After the Add Printer Wizard appears, complete the installation by following the on-screen instructions.

<Windows 2000>

Click the Start Menu, and then [Settings] - [Printers]. Double-click [Add Printer].

After the Add Printer Wizard appears, complete the installation by following the on-screen instructions.

...

Note

The printer driver installation method varies depending on how the printer driver is connected to the MFP or which protocol is used. For details, refer to the User's Guide [Printer Operations] supplied together with the MFP.

5.6.3 Specifying the Print Data Deletion Time

The data encrypted with the CAC/PIV card is deleted from the PKI Encrypted Document User Box of the MFP after saved in the User Box and printed on the MFP.

However, if unprinted print data in the PKI Encrypted Document User Box exceed the User Box upper limit, new data cannot be saved in the User Box. To avoid this problem, you can configure the setting to automatically delete data that remains saved in the User Box for a specific length of time.

Note

The PKI Encrypted Document User Box can contain up to 200 documents.

PKI Encrypted Document Delete Time Setting

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [System Setting] - [User Box Settings] - [PKI Encrypted Document Delete Time Setting].

To specify the deletion time, press [Yes], and enter the time required to automatically delete print data.

5.6.4 Performing PKI Card Print

The following explains how to handle PKI Card Print.

Sending print data (Printer driver setting)

Use the following steps to configure the printer driver setting when encrypting print data using the CAC/PIV card and sending it to the MFP.

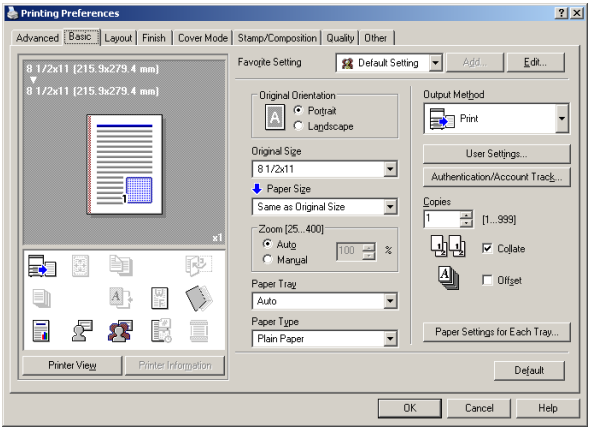
1 Click [Print] in the menu of the application software.

2 Select the desired printer ("KONICA MINOLTA C353 Series PS" or "KONICA MINOLTA C353 Series PCL").

3 Click [Properties] or [Preferences].

4 The Basic tab appears.

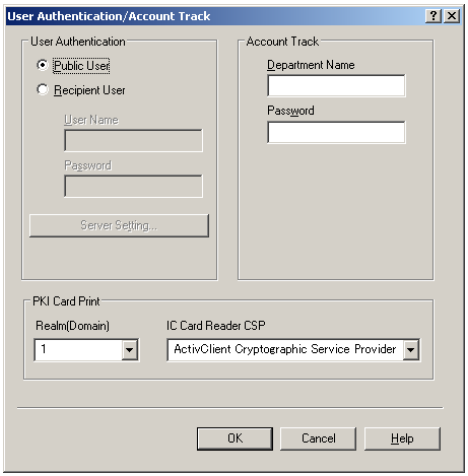
5 Click [Authentication/Account Track].



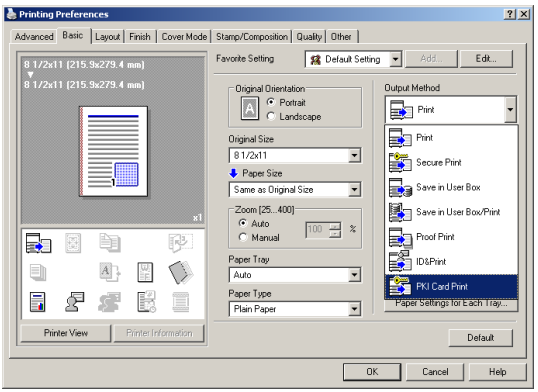
6 Select the "Realm(Domain)" and "IC Card Reader CSP", and click [OK].

- The value of "Realm(Domain)" corresponds to the registration number of the Active Directory. For example, if the registration number of an Active Directory is set to "2", the value of "Realm(Domain)" is also set to "2".
- PKI Card Print uses authentication information of the CAC/PIV card; therefore, it disables the authentication information specified in "User Authentication".

– If Account Track is enabled, enter the "Department Name" and "Password" under "Account Track". To enable Account Track, configure the printer driver setting separately. For details on setting, refer to the User's Guide [Printer Operations] supplied together with the MFP.



7 Under "Output Method", select "PKI Card Print", and click [OK].



8 Send print data.

Detail

If the MFP is associated with PageScope Authentication Manager, and the user is not registered in PageScope Authentication Manager or the user has no print privileges, an authentication failure will occur, and the print job will be discarded.

MFP printing

The following explains how to print data on the MFP.

The MFP provides two printing methods: (1) printing data simultaneously with authentication and (2) selecting and printing data in the PKI Encrypted Document User Box after authentication.

- Using method (1), you can insert the CAC/PIV card into the MFP and perform authentication to easily print the relevant user's data.
- Using method (2), you can select only the required data from the PKI Encrypted Document User Box to print it. You can also delete unnecessary data.

Note

- *Selecting method (1) prints all print documents stored in the user's PKI Encrypted Document User Box.*
- *The printed data is deleted from the PKI Encrypted Document User Box after printing.*

<Printing data simultaneously with authentication>

When the PKI Encrypted Document User Box contains print data, [Print & Access] appears on the login screen.

➔ Press [Print & Access], and insert the CAC/PIV card into the authentication unit attached to the MFP.

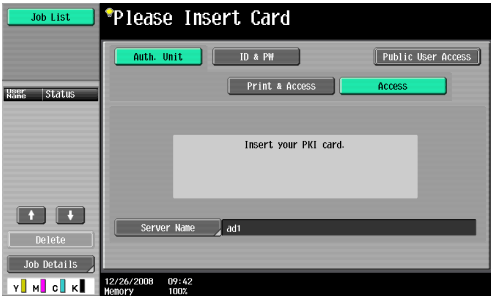
– If the CAC/PIV card is inserted, the PIN code entry screen appears. When authentication succeeds after entering the PIN code, the system prints all the relevant user's data and logs into the MFP.

Detail

If necessary, this function also prints data in the ID & Print User Box. For details on ID & Print, refer to the User's Guide [Printer Operations] supplied together with the MFP.

<Selecting and printing data in the PKI Encrypted Document User Box >

1 Press [Access], and insert the CAC/PIV card into the authentication unit attached to the MFP.



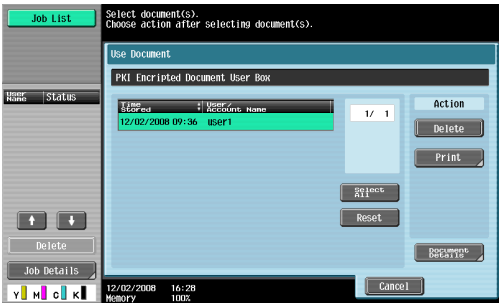
2 Enter the PIN code and to log into the MFP.

3 Press the [User Box] key, and then [Use Document] - [System User Box] - [Encrypted Document User Box] - [OK] - [PKI Encrypted Document User Box] - [OK].

A login user's print data list is displayed.

4 Select the desired data, and press [Print].

- Press [Delete] to delete the selected data.
- Press [Document Details] to view detailed information on the selected document.



5.7 Scan To Me

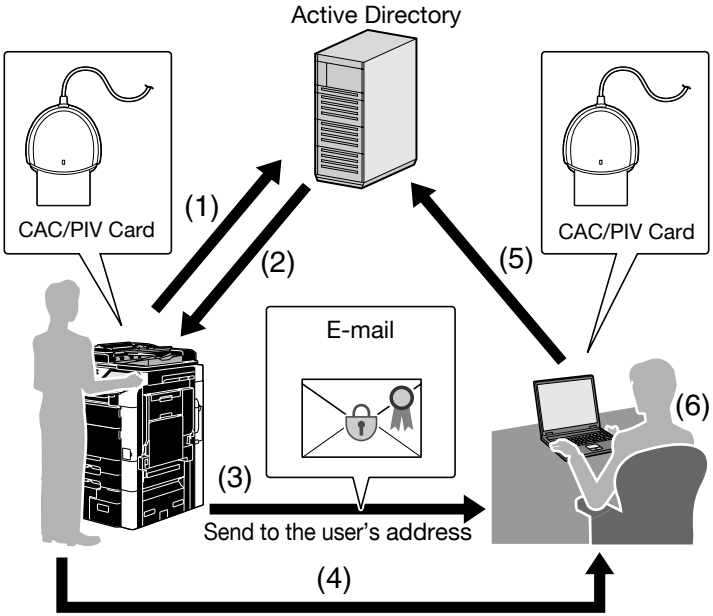
Note

To use this function, ask your service engineer to configure appropiate settings. For details, contact your service representative.

5.7.1 Overview

Scan To Me is a function where, after the CAC/PIV user has successfully authenticated, via the MFP, to the network, the users own email address is automaticvally populated in the 'To' field. The users email address is obtained from Active Directory. This function is useful is securing the email process, the user can only email from the MFP back to their own email address.

The user can also encrypt an e-mail using the CAC/PIV card or add a digital signature when sending an e-mail, ensuring a higher level of security.



(1) Insert the CAC/PIV card into the MFP to perform Active Directory authentication.

(2) Obtain the user's e-mail address.

(3) Send the e-mail to the user's e-mail address. If necessary, the user can use the CAC/PIV card to encrypt an e-mail or add a digital signature.

(4) Take the CAC/PIV card to the computer.

(5) Insert the CAC/PIV card into the computer to perform Active Directory authentication.

(6) Receive the e-mail. If the user encrypts an e-mail or adds a digital signature when sending, check the e-mail decoding or digital signature using the CAC/PIV card.

...

Note

This function is not available when you log in to the MFP as a public user or User Box administrator.

5.7.2 Before Using Scan To Me

Restrictions

Enabling Scan To Me provides a higher level of security by applying the following restrictions.

- The user cannot directly enter the address using e-mail TX, FTP TX, SMB TX, WebDAV TX, or Save in User Box.
- The user cannot use Annotation User Box.
- The user cannot save documents using the User Box function.
- The user cannot send documents from User Boxes.
- The user cannot use the URL notification function.
- The user cannot use the TSI distribution function.

Operation settings

To ensure a higher level of security when using Scan To Me, apply the following settings.

- Disable Address Search (LDAP) (when **no** LDAP server is registered).
- Disable saving a document in an external memory.
- When Public User Access is enabled, disable scanning in the public user mode.

Note

For details on settings, refer to the User's Guide [Network Administrator] supplied together with the MFP.

5.7.3 Scan to Me Related Settings

The following explains the settings required to use the Scan To Me function.

Obtaining the E-mail address

In your environment, configure the settings required to obtain the user's e-mail address using the LDAP protocol.

E-Mail TX (SMTP) setting

Configure the setting to send an e-mail from the MFP.

For details on settings, refer to the User's Guide [Network Administrator] supplied together with the MFP.

S/MIME Communication Setting

This function enables you to encrypt an e-mail using the CAC/PIV card or add a digital signature as required when sending an e-mail.

For details on how to handle e-mail TX using the CAC/PIV card and configure its settings, refer to "Scan to E-mail (S/MIME) " (page 79).

5.7.4 Performing Scan To Me

The following explains how to perform Scan To Me on the MFP.

Detail

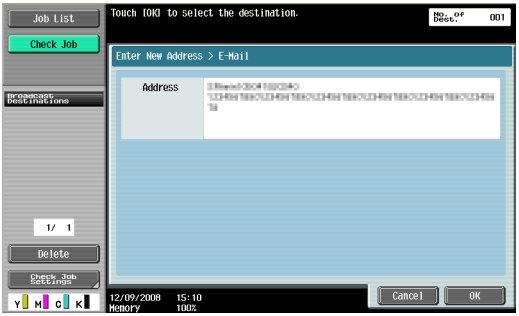
If the correct settings are configured to use Scan To Me, [E-Mail] appears on the Fax/Scan screen to send data to the user's e-mail address.

1 Press the [Fax/Scan] key on the control panel.

2 Press [Direct Input].

3 Press [E-mail].

4 Press [OK].



5 Specify scan conditions in [Scan Settings], [Original Settings], and [Communication Settings].

6 Load the original and press the [Start] key on the control panel.

This scans the original and sends data to the user's e-mail address.

Note

For details on scan conditions, refer to the User's Guide [Network Scan/ Fax/Network Fax Operations] supplied together with the MFP.

5.8 Scan To Home

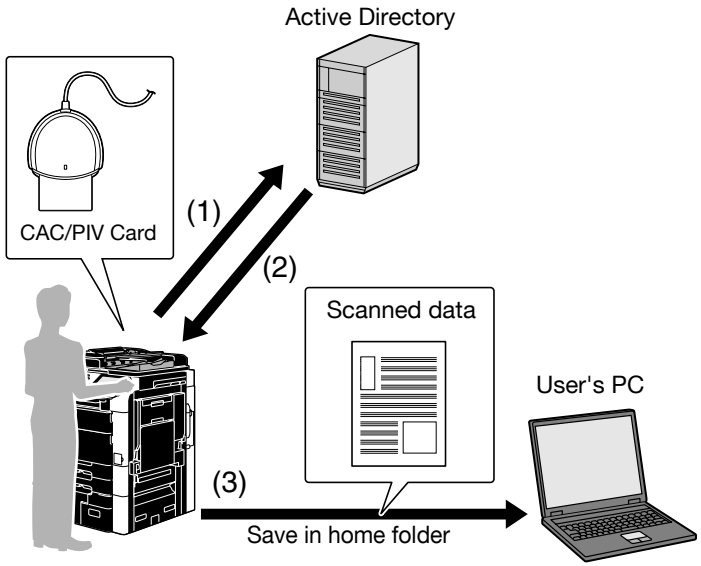
...

Note

To use this function, ask your service engineer to configure settings. For details, contact your service representative.

5.8.1 Overview

The Scan To Home function is similar to Scan to Me in that the Home folder information (UNC) is obtained automatically from Active Directory and automatically populated in the MFP after the user has successfully authenticated to the network via the MFP. This function is useful is securing the scaning process, the user can only scan from the MFP back to their own designated folder.



(1) Insert the CAC/PIV card into the MFP to perform Active Directory authentication.

(2) Obtain the Kerberos authentication ticket and the position of the user's Home folder.

(3) Use the Kerberos authentication ticket to log into the user's computer and save scanned data in the Home folder.

Note

This function is not available when you log in to the MFP as a public user or as a User Box administrator.

5.8.2 Before Using Scan To Home

Restrictions

Enabling Scan To Home provides the following restrictions to ensure higher level security.

- The user cannot directly enter the address using E-mail TX, FTP TX, SMB TX, WebDAV TX, or Save in User Box.
- The user cannot use Annotation User Box.
- The user cannot save documents using the User Box function.
- The user cannot send documents from User Boxes.
- The user cannot use the URL notification function.
- The user cannot use the TSI distribution function.

Operation settings

To ensure a higher level of security when using Scan To Home, apply the following settings.

- Disable Address Search (LDAP) (with **no** LDAP server registered).
- Disable saving a document in an external memory.
- When Public User Access is enabled, disable scanning in the public user mode.

Note

For details on settings, refer to the User's Guide [Network Administrator] supplied together with the MFP.

5.8.3 Scan to Home Related Settings

The following explains the settings required to use the Scan To Home function.

Obtaining the Home folder position

Configure the setting to enable the user to obtain the position of the user's Home folder from Active Directory.

Client Setting

Configure the setting to perform SMB TX.

For details on how to handle SMB TX using the PKI card and configure its settings, refer to "SMB TX Using the PKI Card" (page 76).

Note

Specify the WINS server or direct hosting service to fit your environment. For details, refer to the User's Guide [Network Administrator] supplied together with the MFP.

5.8.4 Using Scan To Home

The following explains how to use Scan To Home on the MFP.

Detail

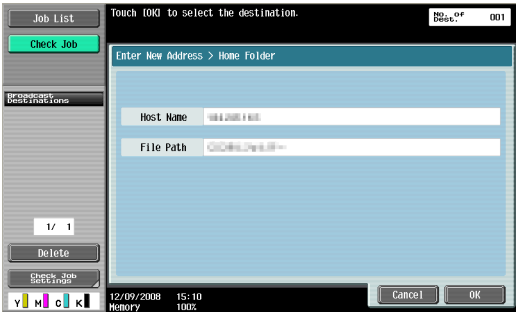
If the correct settings are configured to use Scan To Home, [Home Folder] appears on the Fax/Scan screen to send data to the user's Home folder.

1 Press the [Fax/Scan] key on the control panel.

2 Press [Direct Input].

3 Press [Home Folder].

4 Press [OK].



5 Specify scan conditions in [Scan Settings], [Original Settings], and [Communication Settings].

6 Load the original and press the [Start] key on the control panel.

This scans the original and sends data to the user's Home folder.

Note

For details on scan conditions, refer to the User's Guide [Network Scan/ Fax/Network Fax Operations] supplied together with the MFP.

6 Added or Changed Setting Information

The MFP that supports this system provides some settings added or changed from an ordinary MFP model. This chapter shows a list of the added or changed setting items for each category.

Note

For the settings of an ordinary MFP model, refer to the User's Guide supplied together with the MFP.

6.1 User Settings

6.1.1 System Settings

Item	Description
Language Selection	The available language is English only.

6.2 Administrator Settings

6.2.1 System Settings

User Box Settings

Item	Description
PKI Encrypted Document Delete Time Setting	Allows the user to specify the time required to delete a PKI encrypted document. For details, refer to "Specifying the Print Data Deletion Time" (page 39).

6.2.2 User Authentication/ Account Track

General Settings

Item	Description
User Authentication	Not displayed. User Authentication is automatically set to External Server Authentication.
Synchronize User Authentication & Account Track	Not displayed. Specified so that User Authentication is automatically associated with Account Track when enabling Account Track.

External Server Settings

Description
Active Directory is only available as an external server.

Authentication Device Settings

Item	Description
General Settings	"PKI Card Authentication" is the only available authentication method. In PIV Transitional Mode, select PIV or CAC.

Certificate Verification Settings

Description
Allows the user to configure the setting to verify a certificate. For details, refer to "Configuring Settings for Verifying the Active Directory Certificate" (page 16).

6.2.3 Network Settings

TCP/IP Settings

Item	Description
IPv4 Settings	This item has been renamed from "IP Settings". For details, refer to "IPv4 Settings" (page 10).
IPv6 Settings	"DHCPv6 Setting" has been added. For details, refer to "IPv6 Settings" (page 11).
DNS Domain	"Search Domain Name Auto Retrieval" has been added. For details, refer to "DNS Domain" (page 11).
DNS Server Settings (IPv4)	This item has been renamed from "DNS Server Settings". For details, refer to "DNS Server Settings (IPv4)" (page 14).
DNS Server Settings (IPv6)	This item has been renamed from "DNS Server Settings". For details, refer to "DNS Server Settings (IPv6)" (page 14).
LLMNR Setting	Select whether to enable the LLMNR function. To communicate with a computer that contains Windows Vista/Server 2008, you can perform name resolution using the LLMNR function even if the DNS server is not supported.

SMB Settings

Item	Description
Client Settings	"NTLM Settings" has been changed to "SMB Auth Setting". "DFS Setting" and "Password Authentication Restriction" have been added. For details, refer to "Client Settings" (page 31).

LDAP Settings

Item	Description
Setting Up LDAP	"Login Name", "Password", "Authentication Type" and "Select Server Authentication Method" are not displayed. On the MFP that supports this system, "Authentication Type" is automatically set to "GSS-SPNEGO". "Select Server Authentication Method" is automatically set so that User Authentication is enabled.

E-Mail Settings

Item	Description
S/MIME Communication Settings	"Digital Signature Type" has been added. For details, refer to "S/MIME Communication Settings" (page 34).

Web Service Settings

Item	Description
Web Service Common Settings	"Publication Service" has been added. Publication Service, which is one of the Web service functions, detects a connection destination using the multicast service. When using the MFP while NetBIOS is set to Disable in Windows Vista/Server 2008 or the IPv6-only communication is configured, the user cannot detect a connection destination using NetBIOS. In this case, set "Publication Service" to "Enable".

6.2.4 System Connection

OpenAPI Settings

Item	Description
SSL/Port Settings	This item has been renamed from "Port Number" or "SSL". The user can specify SSL and port for OpenAPI communication.

6.2.5 Security Settings

Security Details

Item	Description
Password Rules	Not displayed on the MFP that supports this system.
Prohibited Functions when Authentication Error	The setting value of [Release] has been changed from "Users & Accounts" to "Account".

Enhanced Security Mode

Description
Not displayed on the MFP that supports this system.

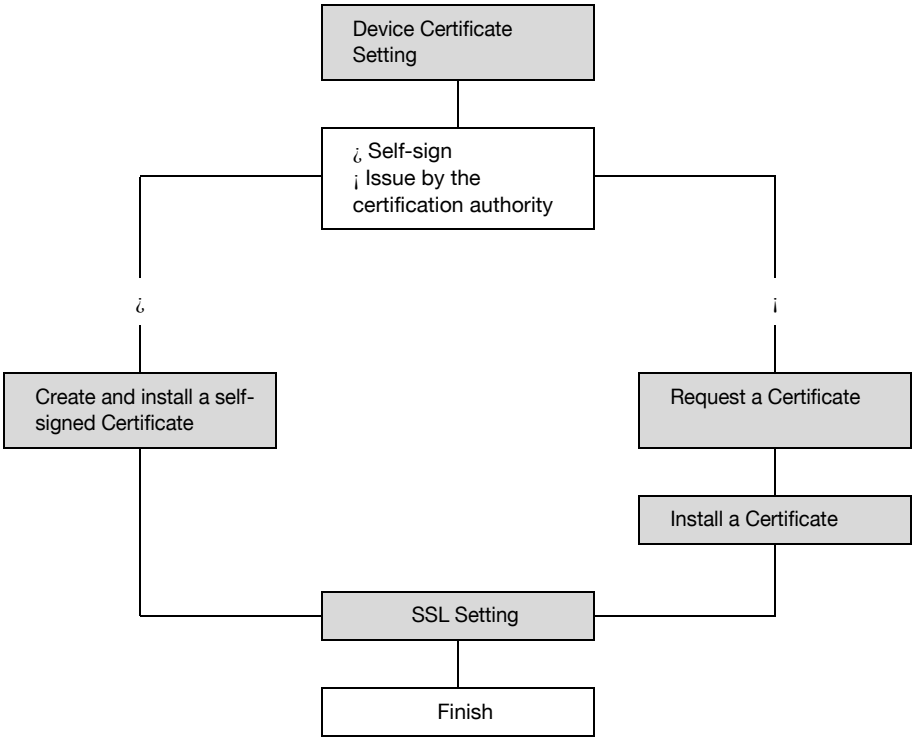
6.2.6 License Settings

Description
Not displayed on the MFP that supports this system.

6.3 Registering a Device Certificate

The user can register the MFP certificate (device certificate) using PageScope Web Connection. The method for registering a device certificate on an MFP with PKI card authentication is different from an ordinary MFP model.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.



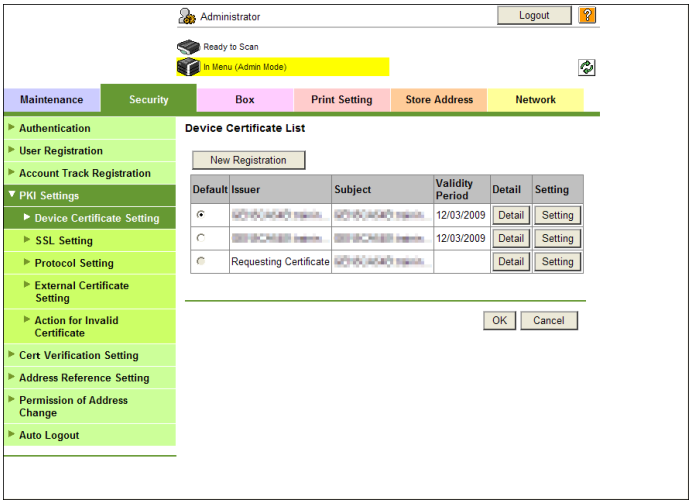
Note

For details on how to use PageScope Web Connection, refer to the User's Guide [Network Administrator] supplied together with the MFP.

6.3.1 Device Certificate Setting

The user can manage multiple device certificates on the MFP that supports this system.

In the PageScope Web Connection administrator mode, select the Security tab, and then "PKI Settings" - "Device Certificate Setting".



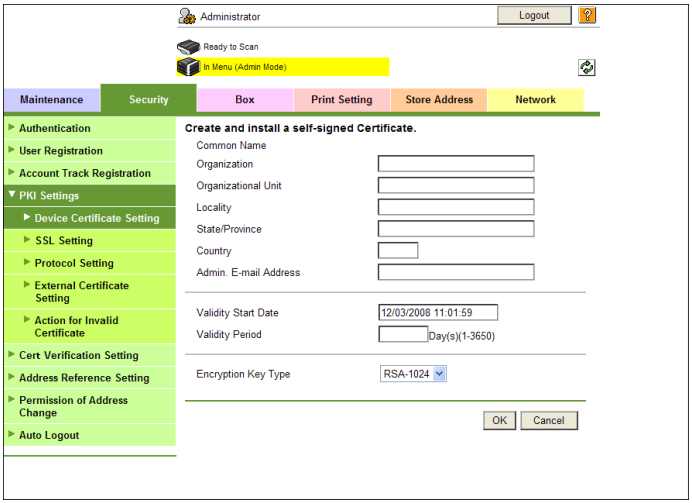
Item	Description
[New Registration]	Register a new device certificate.
Default	Specify a default device certificate for all protocols. Specify a default device certificate when not using protocol specific device certificates.
Issuer	Displays the device certificate issuer.
Subject	Displays a destination to issue a device certificate to.
Validity Period	Displays the validity period of a device certificate.
Detail	Enables you to view the detailed information about a device certificate.
Setting	Enables you to discard a device certificate if it is installed. If "Requesting Certificate" is displayed in "Issuer" of the device certificate, you can install a CA-issued certificate in the MFP.

Note

The user can use multiple registered device certificates depending on protocols. For details on the setting, refer to "Using Device Certificates per Protocol" (page 111).

6.3.2 Create and install a self-signed Certificate

In the PageScope Web Connection administrator mode, select the Security tab, and then "PKI Settings" - "Device Certificate Setting" - [New Registration] - "Create and install a self-signed Certificate".

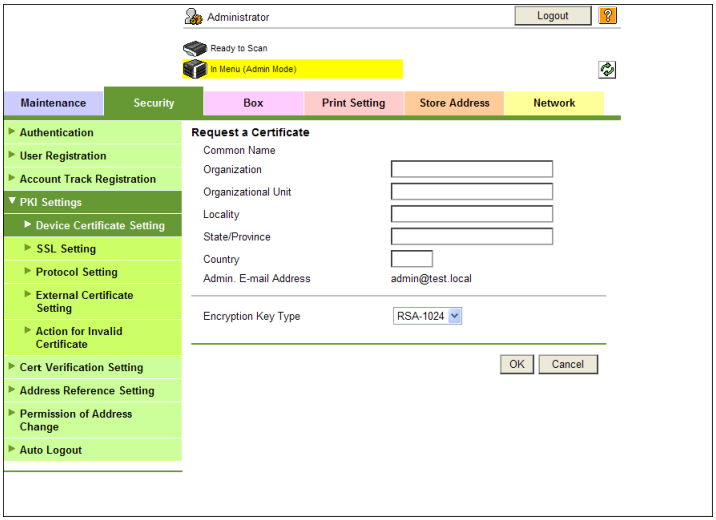


Item	Description
Common Name	Displays the IP address or domain name of the MFP. This item shows the setting value when accessing the MFP.
Organization	Enter the association name or organization name (up to 63 characters).
Organizational Unit	Enter the account name (up to 63 characters). This item may be left blank as required.
Locality	Enter the city, ward, town, or village name (up to 127 characters).
State/Province	Enter the state or province name (up to 127 characters).
Country	Enter the country code as defined in ISO03166 (2 characters). United States: US, Great Britain: GB, Italy: IT, Australia: AU, The Netherlands: NL, Canada: CA, Spain: ES, Czech Republic: CZ, China: CN, Denmark: DK, Germany: DE, Japan: JP, France: FR, Belgium: BE, Russia: RU
Admin. E-mail Address	Enter the e-mail address of the administrator (up to 127 characters). If the administrator's e-mail address is already registered, it appears.

Item	Description
Validity Start Date	Displays the validity period starting date. This item displays the date and time of the MFP when this screen appears.
Validity Period	Enter the certificate's the validity period (in days).
Encryption Key Type	Select the type of encryption key.
[OK]	Click this button to create a self-signed certificate. It may take several minutes to create the certificate.

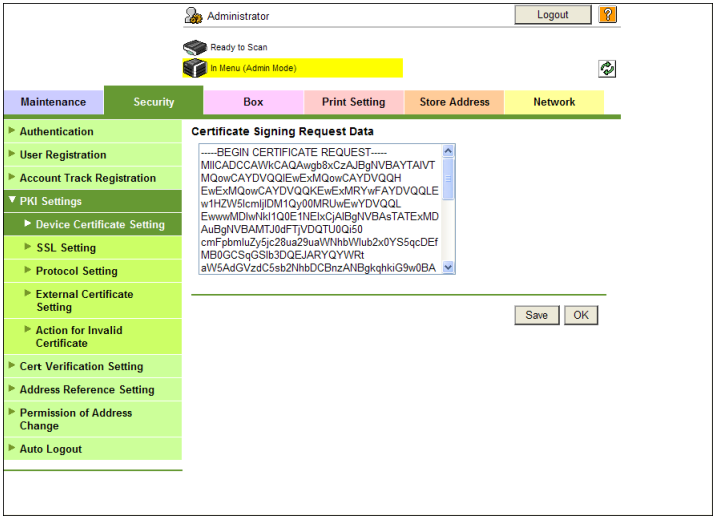
6.3.3 Request a Certificate

In the PageScope Web Connection administrator mode, select the Security tab, and then "PKI Settings" - "Device Certificate Setting" - [New Registration] - "Request a Certificate".



Item	Description
Common Name	Displays the IP address or domain name of the MFP. This item shows the setting value when accessing the MFP.
Organization	Enter the association name or organization name (up to 63 characters).
Organizational Unit	Enter the account name (up to 63 characters). This item may be left blank as required.
Locality	Enter the city, ward, town, or village name (up to 127 characters).

Item	Description
State/Province	Enter the state or province name (up to 127 characters).
Country	Enter the country name with the country code defined in ISO03166 (2 characters). United States: US, Great Britain: GB, Italy: IT, Australia: AU, The Netherlands: NL, Canada: CA, Spain: ES, Czech Republic: CZ, China: CN, Denmark: DK, Germany: DE, Japan: JP, France: FR, Belgium: BE, Russia: RU
Admin. E-mail Address	Enter the e-mail address of the administrator (up to 127 characters). If the administrator's e-mail address is already registered, it appears.
Encryption Key Type	Select the type of encryption key.
[OK]	Click this button to create a self-signed certificate. It may take several minutes to create a certificate.

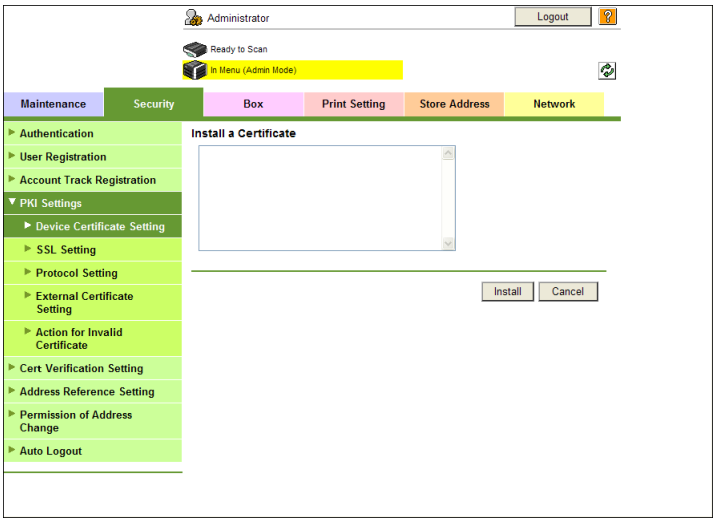


Item	Description
Certificate Signing Request Data	Displays request data to issue a certificate. Send the displayed character string to the CA.
[Save]	Click this button to save the certificate signing request data as a file in your computer.

6.3.4 Install a Certificate

In the PageScope Web Connection administrator mode, select the Security tab, and then- "PKI Settings" - "Device Certificate Setting" - [Setting] - "Install a Certificate".

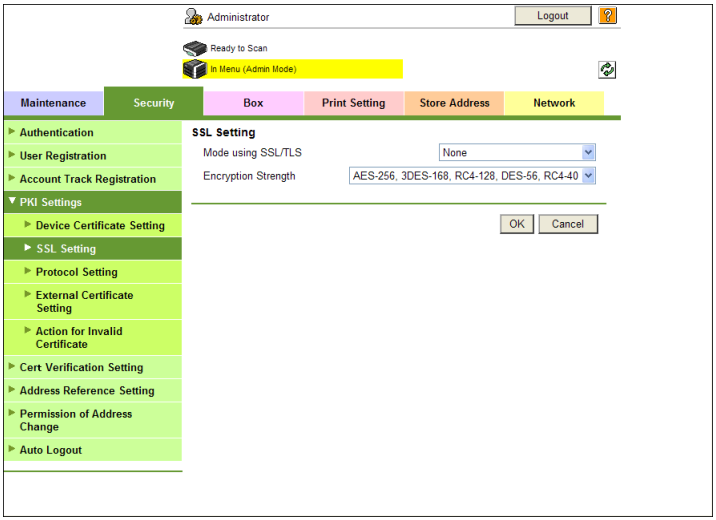
Ask the CA to issue a certificate, and install the certificate sent from the CA in the MFP.



Item	Description
Install Certificate	Pastes text data sent from the CA.
[Install]	Click this button to install the certificate.

6.3.5 SSL Setting

In the PageScope Web Connection administrator mode, select the Security tab, and then "PKI Settings" - "SSL Setting".



Item	Description
Mode using SSL/TLS	Select the PageScope Web Connection mode to apply SSL. Select "None" to disable SSL.
Encryption Strength	Specify the SSL encryption strength.

6.4 Using Device Certificates per Protocol

The MFP that supports this system enables you to use different device certificates per protocol. Configure settings according to fit your environment.

On the MFP, you can specify the device certificate to be used for each of the following protocols.

Protocol1	Protocol2	Description
SSL	http Server	When the MFP acts as an http server: • This protocol is used to encrypt communications from the client to the MFP when the client accesses PageScope Web Connection over HTTPS. • This protocol is used to encrypt communications from the client to the MFP when printing data from the client over IPPS.
SSL	E-Mail Transmission (SMTP)	When the MFP acts as an SMTP client: • This protocol is used to submit a device certificate when it is requested from the SMTP server.
SSL	E-mail RX(POP)	When the MFP acts as a POP client: • This protocol is used to submit a device certificate when it is requested from the POP server.
SSL	TCP Socket	When the MFP acts as a TCP Socket client: • This protocol is used to submit a device certificate when it is requested from the TCP Socket server.
SSL	LDAP	When the MFP acts as an LDAP client: • This protocol is used to submit a device certificate when it is requested from the LDAP server.
SSL	WebDAV Client	When the MFP acts as a WebDAV client: • This protocol is used to submit a device certificate when it is requested from the WebDAV server.
SSL	OpenAPI	When the MFP acts as an OpenAPI server: • This protocol is used to encrypt communications from the client to the MFP when the OpenAPI client accesses the MFP over SSL.

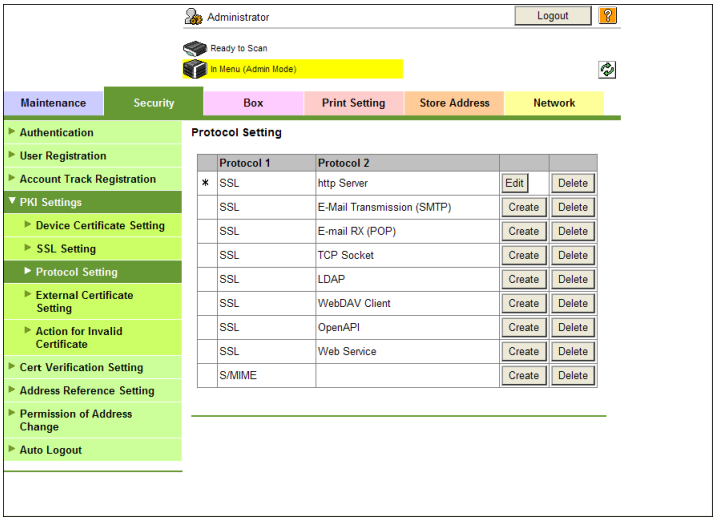
Protocol1	Protocol2	Description
SSL	Web Service	When the MFP acts as a Web service server: • This protocol is used to encrypt communications from Windows Vista to the MFP when Windows Vista accesses the MFP over HTTPS.
S/MIME		This protocol is used to attach a device certificate when sending an S/MIME e-mail.

Detail

- *When not using protocol specific device certificates, use the device certificate that is set to "Default" in "Device Certificate Setting". For details, refer to "Device Certificate Setting" (page 104).*
- *You cannot enable this function, which uses protocol specific device certificates, when a device certificate is not registered or it is only in the certificate signing request state.*

Protocol setting

In the PageScope Web Connection administrator mode, select the Security tab, and then "PKI Settings" - "Protocol Setting".



Item	Description
Protocol 1/2	Displays the classification for each protocol. If the device certificate is registered, the protocol is marked with *.

Item	Description
[Create]	Select the protocol and click [Create]. The device certificate registration page appears, and you can specify the target device certificate. If the device certificate is already registered, [Edit] appears. If [Edit] is clicked, the target device certificate details can be viewed or modified.
[Delete]	If the target device certificate is registered, click this button to delete the registered information.

7 Appendix

7.1 Product Specifications

Product name	Authentication unit (PKI-IC card type) AU-211P
Dimensions	70 mm (L) × 70 mm (W) × 10 mm (H)
Weight	60 g
Power supply	USB bus power
Range of operatingtemperature	0 to 50°C
Interface	Full speed USB (12 Mbps)
Connector shape	USB A type connector
Compatible card	PKI-IC card (PIV, CAC)

7.2 Cleaning the Authentication Unit

Wipe the surface using a soft, dry cloth. If the surface is still dirty, moisten a cloth with mild detergent and thoroughly wring it out before cleaning. Once the dirt has been removed, moisten a cloth with water, thoroughly wring it out, and wipe off the detergent.

...

Reminder

- *Remove this unit from the MFP before cleaning. Loading the USB port will result in a malfunction.*
- *Take care so that no water gets into this unit when cleaning. If water gets into this unit, it will result in a malfunction.*
- *Do not clean this unit using organic solvent such as benzene or alcohol. Doing so will result in a malfunction.*
- *Before disconnecting or connecting this unit, turn the MFP Main Power off. After 10 seconds or more have lapsed, turn the MFP Main Power on. Failing to do so may result in a malfunction.*
- *When connecting or disconnecting the USB cable, hold the plug. Failing to do so will result in a malfunction.*

7.3 Troubleshooting

If an error occurs during running, refer to the following.

Status	Point to be checked	Action
Failed to login.	Did you enter the correct PIN code?	Check the PIN code, and enter the correct one.
Cannot login.	Is the PKI card locked?	If the number of authentication failures reaches a specific limit, the PKI card will be locked to prevent the authentication. For details on how to unlock the PKI card, contact the PKI card administrator.
Scanning does not start.	Did you restart the MFP after connecting this unit to the MFP?	Turn the MFP Main Power off, disconnect the USB cable from either the MFP or this unit once, and connect it again. Wait at least 10 seconds, and turn the MFP Main Power on.

If any of the above errors recur after taking the specified action, or if other errors occur, contact your service engineer.