KONICA MINOLTA

Authentication Unit AU-211P

User's Guide

Ver. 1.2

Contents

1 Introduction

Thank you for choosing this device.

This User's Guide provides descriptions of the 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, and then store it in a safe place.

- Before using this device, carefully read this information and follow it to operate the device correctly.
- After reading this information, store it in the designated holder with the warranty.

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 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.

2 Getting Started

2.1 Product Overview

This product is a PKI card authentication unit that scans a PKI card (CAC or PIV card) to perform personal authentication.

Connecting this unit enables you to run a PKI card authentication system (hereinafter referred to as "this system") that uses the PKI card authentication unit on the MFP.

Using this system will enable you to carry out operations without making a password public on the network, and to configure the system environment with a higher level of security. You can also implement the unique functions using this system on the MFP.

Use conditions

The following conditions are required to use this system.

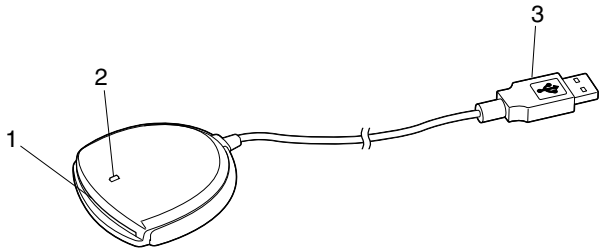
- PKI card authentication unit (This unit)
- MFP compatible with a PKI card authentication system
- PKI card available for PIV and CAC
- User management using Active Directory (Kerberos authentication + PKINIT)

...

Reminder

Do not disconnect the USB cable while using this unit. Doing so may cause this system to become unstable.

2.2 Part names and their functions



No.	Part name	Description
1	Card inlet	Used to insert the PKI card.
2	LED lamp	Turns green when you insert a PKI card into this unit. Blinks green while authentication.
3	USB cable	Used for connecting this device to the multifunctional product.

2.3 Pre-Setting

To use this system, pre-configure the following settings on the MFP.

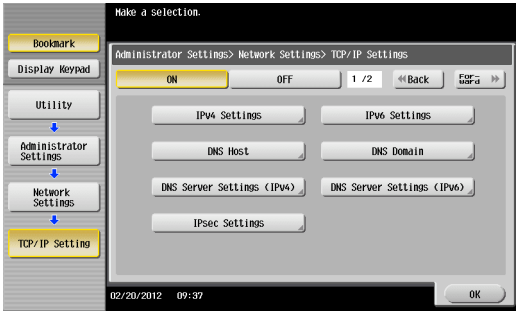
- Configuring network settings (page 10)
- Registering Active Directory for Authentication (page 12)
- Correcting the MFP time (page 13)
- Registering the DNS server associated with Active Directory (page 14)
- Specifying the PIV transitional mode (page 16)
- Configuring settings for verifying the Active Directory certificate (page 17)

2.3.1 Configuring Network Settings

Configure the basic settings required to use the MFP in a network environment.

TCP/IP Settings

On the MFP control panel, tap [Utility] - [Administrator Settings] - [Network Settings] - [TCP/IP Settings].



Item	Description
ON/OFF	Select [ON].

IPv4 Settings

Item	Description
IP Application Method	Select whether to automatically retrieve the IP address or directly specify it.
Auto Input	When automatically retrieving the IP address, select the automatic retrieval method.
IP Address	When directly specifying the IP address, enter the IP address of the MFP.

Item	Description
Subnet Mask	When directly entering the IP address, specify the subnet mask for the connected network.
Default Gateway	When directly entering the IP address, specify the default gateway for the connected network.

IPv6 Settings

...

Note

These settings are required when using the MFP in an IPv6 environment.

Item	Description
ON/OFF	Select [ON] when using the MFP in an IPv6 environment.
Auto IPv6 Settings	Select [ON] when automatically retrieving the IPv6 address.
DHCPv6 Setting	Select [ON] when retrieving the IPv6 address using DHCPv6.
Global Address	Specify the IPv6 global address when not automatically retrieving the IPv6 address.
Prefix Length	Specify the IPv6 global address prefix length when not automatically retrieving the IPv6 address.
Gateway Address	Specify the IPv6 gateway address when not automatically retrieving the IPv6 address.
Link-Local Address	Displays the link-local address generated from the MAC address.

DNS Host

Item	Description
DNS Host Name	Specify the host name of the MFP (up to 63 characters).
Dynamic DNS Settings	Select [Enable] when automatically registering the specified DNS host name in the DNS server that supports the Dynamic DNS function.

DNS Domain

Item	Description
Domain Name Auto Retrieval	Select whether to automatically retrieve the domain name. This item is available when using DHCP.

Item	Description
Search Domain Name Auto Retrieval	Select whether to automatically retrieve the search domain name. This item is available when using DHCPv6.
Default DNS Domain Name	Specify the domain name that the MFP is connected to (up to 253 bytes with the host name).
DNS Search Domain Name 1 to 3	Specify the DNS search domain name (up to 251 bytes).

2.3.2 Registering Active Directory for Authentication

Register Active Directory for authentication in the MFP. You can register up to 20 Active Directory services.

External Server Settings

On the MFP control panel, tap [Utility] - [Administrator Settings] - [User Authentication/Account Track] - [External Server Settings] - [New].

Item	Description
Server Name	Specify the name of the external server (up to 32 characters).
Server Type	Select Active Directory, and specify its default domain name (up to 64 characters).

Detail

When registering multiple Active Directory services, specify the default Active Directory previously. Select the desired Active Directory on the External Server Settings screen, and tap [Set as Default].

2.3.3 Correcting the MFP Time

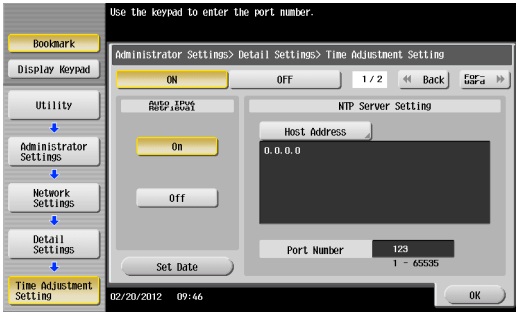
You cannot log into Active Directory if the MFP system time is extremely different between the MFP and Active Directory. Correct the MFP time so it matches the Active Directory time with the system time.

Time Adjustment Setting

On the MFP control panel, tap [Utility] - [Administrator Settings] - [Network Settings] - [Forward] - [Detail Settings] - [Time Adjustment Setting].

Note

Before correcting the MFP time, tap [Utility] - [Administrator Settings] - [System Settings] - [Date/Time Setting], and check that the time zone is specified correctly.



Page 1/2

Item	Description
ON/OFF	Select [ON].
Auto IPv6 Retrieval	To automatically obtain the IPv6 address of the NTP server, select [On]. This item is necessary when IPv6 is used while DHCPv6 is enabled.
Host Address	Specify the host address of the NTP server associated with Active Directory.
Port Number	Specify the port number.
Set Date	Correct the time.

Page 2/2

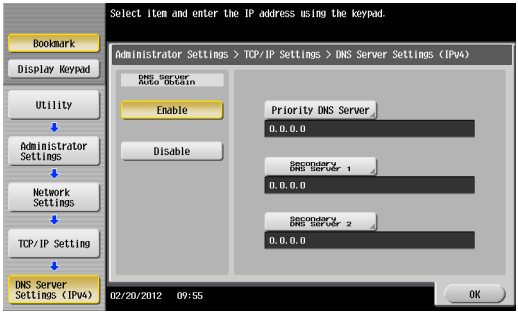
Item	Description
Auto Time Adjustment	When an automatic time correction is made, select [On].
Polling Interval	When [On] is selected for Auto Time Adjustment, set the polling interval.

2.3.4 Registering the DNS Server Associated with Active Directory

Register the DNS server associated with Active Directory in the MFP.

DNS Server Settings (IPv4)

On the MFP control panel, tap [Utility] - [Administrator Settings] - [Network Settings] - [TCP/IP Settings] - [DNS Server Settings (IPv4)].



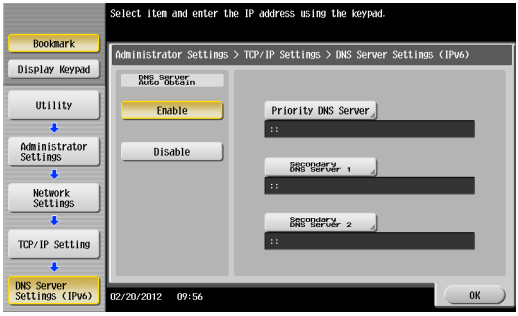
Item	Description
DNS Server Auto Obtain	Select whether to automatically obtain the DNS server address. This item is available when using DHCP.
Priority DNS Server	Specify the IPv4 address of the priority DNS server associated with Active Directory.
Secondary DNS Server 1 and 2	Specify the IPv4 address of the secondary DNS server associated with Active Directory.

DNS Server Settings (IPv6)

On the MFP control panel, tap [Utility] - [Administrator Settings] - [Network Settings] - [TCP/IP Settings] - [DNS Server Settings (IPv6)].

Note

These settings are required when using the MFP in the IPv6 environment.



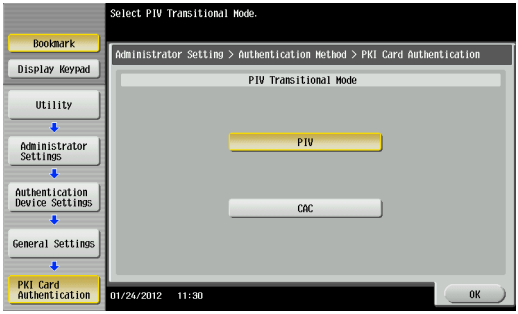
Item	Description
DNS Server Auto Obtain	Select whether to automatically obtain the DNS server address. This item is available when using DHCPv6.
Priority DNS Server	Specify the IPv6 address of the priority DNS server associated with Active Directory.
Secondary DNS Server 1 and 2	Specify the IPv6 address of the secondary DNS server associated with Active Directory.

2.3.5 Specifying the PIV Transitional Mode

Specify the PIV transitional mode in the PIV transitional specifications.

Authentication Device Settings

On the MFP control panel, tap [Utility] - [Administrator Settings] - [User Authentication/Account Track] - [Authentication Device Settings] - [General Settings] - [PKI Card Authentication].



Item	Description
PIV Transitional Mode	Select PIV or CAC as the PIV transitional mode.

2.3.6 Configuring Settings for Verifying the Active Directory Certificate

Configure the certificate verification settings to verify the Active Directory certificate when communicating with Active Directory.

Certificate Verification Setting

On the MFP control panel, tap [Utility] - [Administrator Settings] - [User Authentication/Account Track] - [Certificate Verification Setting].

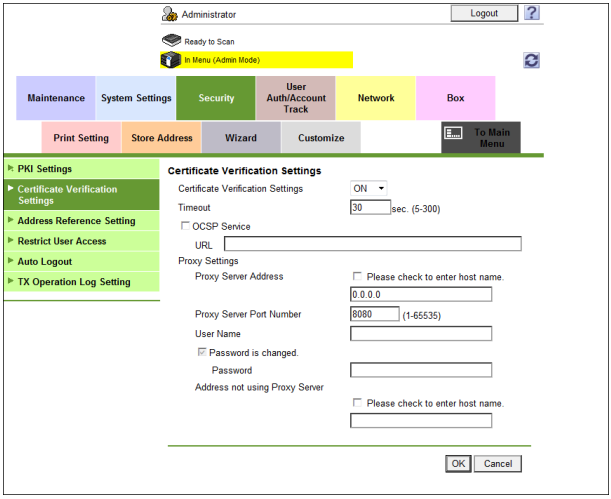
Item	Description
Verify Validity Period	Select whether to verify that the certificate is within the validity period.
Check Root Signature	Select whether to check the root signature. To check the root signature, view the external certificates managed on the MFP. For details on how to register an external certificate on the MFP, refer to "External Certificate Setting" (page 20).
Check CRL Expiration	Select whether to check that the certificate is not expired in the CRL (Certificate Revocation List).
Check OCSP Expiration	Select whether to check that the certificate is not expired in the OCSP service. For details on how to configure the OCSP service setting, refer to "Certificate Verification Settings" (page 18).

Certificate Verification Settings

In the PageScope Web Connection administrator mode, select [Security], and then [Certificate Verification Settings].

Note

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



Item	Description
Certificate Verification Settings	Select [ON] to enable certificate verification.
Timeout	Enter the timeout period to check the expiration date.
OCSP Service	Select this check box to use an OCSP service.
URL	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the system accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, it will result in an error.
Proxy Server Address	To check the expiration date via a proxy server, enter the proxy server address. If the DNS server is specified, you can enter the host name instead. If [IPv6] is set to [ON], you can also specify the IPv6 address.

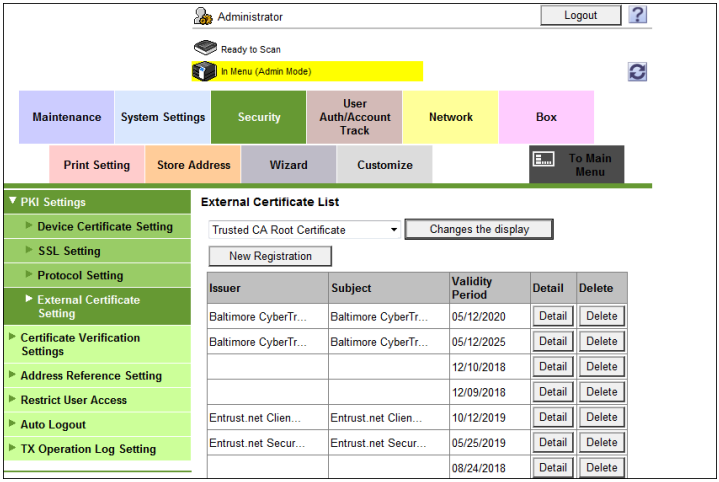
Item	Description
Proxy Server Port Number	Enter the port number for the proxy server.
User Name	Enter the user name to log in to the proxy server (up to 63 characters).
Password	Enter the password to log in to the proxy server (up to 63 characters). When changing the registered password, select [Password is changed.], and enter a new password.
Address not using Proxy Server	Specify an address with no proxy server used depending on your environment when checking the expiration date. If the DNS server is specified, you can enter the host name instead. If [IPv6] is set to [ON], you can also specify the IPv6 addresses.

External Certificate Setting

In the PageScope Web Connection administrator mode, select [Security] , and then [PKI Settings] - [External Certificate Setting].

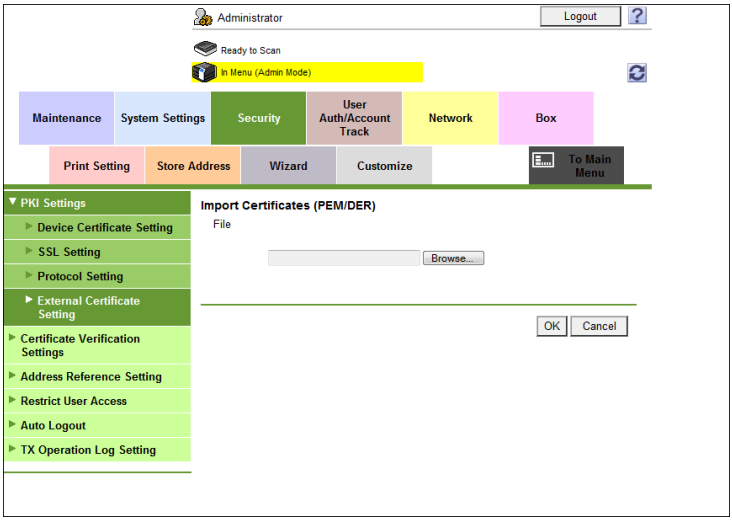
Detail

- *To check the root signature in Certificate Verification, register the external certificate you want to view when checking the root signature as necessary.*
- *For details on how to use PageScope Web Connection, refer to the User's Guide [Web Management Tool] supplied together with the MFP.*



Item	Description
Certificate type	Select the type of the external certificate you want to display, and click [Changes the display]. You will see a list of the selected types of external certificates.
[New Registration]	Click this button to register a new external certificate. Click [Browse] in the New Registration screen, and specify a new external certificate.
Issuer	Displays the issuer of the external certificate.
Subject	Displays the destination to issue the external certificate.
Validity Period	Displays the validity period of the external certificate.
Detail	View the detailed information about the external certificate.
Delete	Displays the deletion confirmation dialog box. If necessary, you can delete the external certificate.

<New Registration>



Item	Description
File	Click [Browse] in the Import Certificates (PEM/DER) screen, and specify a new external certificate to be registered. • If [Trusted CA Root Certificate] is selected, register the root certificate from the CA (Certificate Authority). • If [Trusted CA Intermediate Certificate] is selected, register the intermediate certificate from the CA (Certificate Authority). • If [Trusted EE (End Entity) Certificate] is selected, register the certificates individually. • If [Non-Trusted Certificate] is selected, register the non-trusted certificates individually.

2.3.7 Enabling TPM (Trusted Platform Module)

If TPM (Trusted Platform Module) is installed, enable TPM on this machine.

Note

An optional i-Option LK-115 is required to use TPM on this machine.

TPM Function Settings

On the control panel of the MFP, tap [Utility] - [Administrator Settings] - [Security Settings] - [TPM Setting], then set [TPM Function Settings] to [Enable].

SSL Setting

In the administrator mode of PageScope Web Connection, select [Security] - [PKI Settings] - [SSL Setting], then set SSL/TLS to Enable.

Note

For details on how to use PageScope Web Connection, refer to the User's Guide (Web Management Tool) supplied with the MFP.

2.4 Operation Settings

For security reasons, we recommend that you configure network settings as follows when this system is operated.

Item	Description
TCP Socket Settings	Set [TCP Socket] to [OFF] (default: [OFF]). However, you can also set this option to [ON] if TPM is installed.
WebDAV Settings	Set [WebDAV Server Settings] to [OFF] (default: [OFF]). However, you can also set this option to [ON] if TPM is installed.
FTP Settings	Set [FTP Server Settings] to [OFF] (default: [OFF]).
SNMP Settings	• Set [SNMP v1/v2c Settings] - [Write Setting] to [Invalid] (default: [Invalid]). • Set [SNMP v3 (IP)] to [OFF] (default: [OFF]).

We recommend that you set PageScope Web Connection and the OpenAPI server function (external application connection) to Disable after the default settings of this machine have been completed.

Item	Description
HTTP Server Settings	Set [PSWC Settings] to [OFF] (default: [ON]). However, you can also set this option to [ON] if TPM is installed.
OpenAPI Settings	Set [External Application Connection] to [No] (default: [Yes]). However, you can also set this option to [Yes] if TPM is installed.

3 How to Use the Authentication Unit

This chapter explains how to log in and log out using this unit and also describes the functions for use with this system.

Note

The following explains the procedures applicable in the normal display mode. This unit is also available in the Enlarge Display mode. For details on the Enlarge Display mode, refer to the User's Guide [Accessibility] supplied together with the MFP.

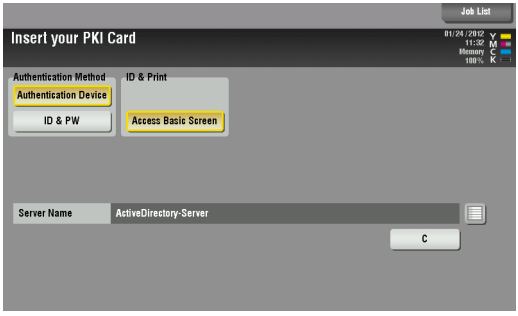
3.1 Login and Logout

3.1.1 Login

Use the following steps to insert a PKI card into this unit and log into the MFP.

1 Insert a PKI card in the unit.

- To change the server for authentication, tap the list icon of [Server Name] to select a desired server before inserting a PKI card into this unit, and tap [OK].
- 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, tap [ID & PW], and enter the password.

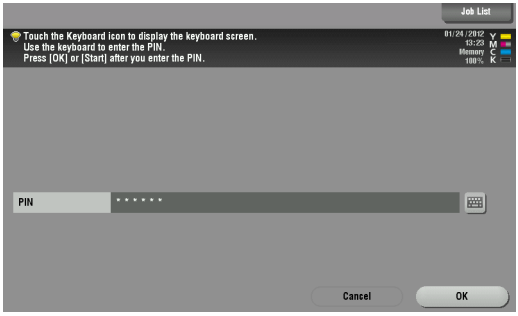


Detail

- *If you insert a PKI card into the unit while logged in as a public user, you will be logged out as a public user and the PIN code entry screen appears. However, even if logged in as a public user, you will not be logged out by inserting a PKI card during operations, when warnings occur, or when a screen that you cannot log out by pressing the [Access] key on the control panel is displayed.*
- *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.*

2 Enter the PIN code.

- You can use the keypad to enter the PIN code directly.
- When the [PIN] keyboard icon is tapped, the keyboard screen appears. If necessary, use this keyboard screen to enter characters as a PIN code.



Detail

If an incorrect PIN code is entered, "No. of Auth. Failure Allowed" appears on the screen. If the number of authentication failures reaches an upper limit, the PKI card will be locked to prevent the authentication. For details on the allowable number of PKI card authentication failures and how to unlock the PKI card, contact your PKI card administrator.

3 Tap [OK] or press the [Start] key.

This starts authentication and logs into the MFP.

Detail

When Account Track is enabled, use the PKI 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.

3.1.2 Logout

To log out the MFP, pull the PKI 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 [Access] 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.*
- *When the time for the system auto reset function is specified, the function will activate and you will be logged out automatically if the MFP is not operated for the specified time. If no operations are carried out for over 1 minute while you are logged in, you will be logged out automatically even when the system auto reset function is set to [OFF].*
- *In order to prevent the card from being left in the unit, the caution sound can be issued when you are logged out automatically.To issue the caution sound, select [Sound Setting] - [Sound Setting] and set [Warning Sound] to [On] in [Accessibility Setting], and also set [Simple Caution Sound (Level 1)] to [Yes] in [Sound Setting] - [Caution Sound] in advance.*

3.2 Functions Using the PKI Card Authentication System

This section explains the functions using the PKI card authentication system.

Function	Description	See
Address Search (LDAP) Using PKI Card	Logs into the LDAP server using the Kerberos authentication ticket that is obtained by Active Directory authentication with the PKI 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. 29
SMB TX Using PKI Card	Logs into the destination computer using the Kerberos authentication ticket that is obtained by Active Directory authentication with the PKI 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. 35
Scan to E-mail (S/MIME) Using PKI Card	Adds a digital signature using the PKI card when sending an e-mail. This function prevents fabrication or spoofing of an e-mail.	p. 40
PDF Encryption and Signature Addition Using PKI Card	Encrypts a PDF document and adds a signature using the digital certificate registered in the PKI card when distributing scanned data as a PDF document. This function prevents illegal access to or fabrication of a PDF document. The optional Upgrade Kit UK-204 and i-Option LK-102 v3 are required to encrypt a PDF document using the PKI card.	p. 44
PKI Card Print	The user can encrypt print data using the PKI card before sending the data to the MFP. Print data is stored on an MFP, and can be decrypted and printed if the same user performs authentication on a MFP using the PKI card. 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 PKI card is successful; therefore, you can ensure the confidentiality of documents.	p. 47

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.	p. 57
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.	p. 61

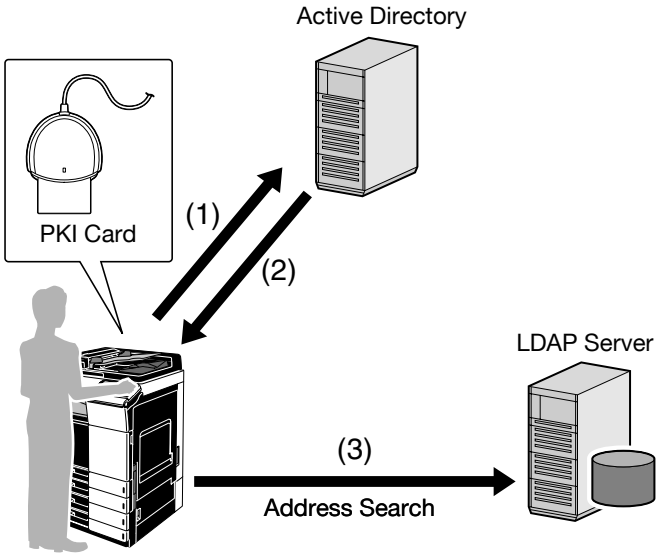
3.3 Address Search (LDAP) Using PKI Card

3.3.1 Overview

This function logs in to the LDAP server using the Kerberos authentication ticket that is obtained by Active Directory authentication with the PKI card when searching for the destination via the LDAP server.

If a Kerberos authentication ticket is used to authenticate the LDAP server, the user can use the LDAP server securely without making the password public on the network.

The user can also perform the Active Directory authentication only once to obtain access privileges, and configure the single sign-on environment to be convenient.



(1) Insert the PKI 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.

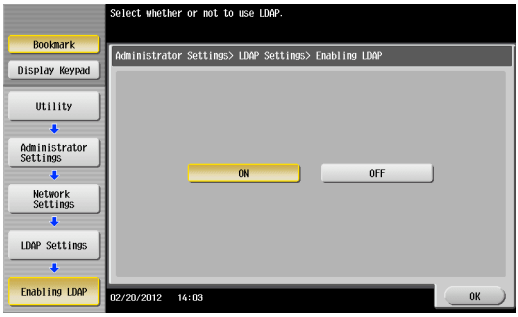
3.3.2 Related Settings

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, tap [Utility] - [Administrator Settings] - [Network Settings] - [LDAP Settings] - [Enabling LDAP].

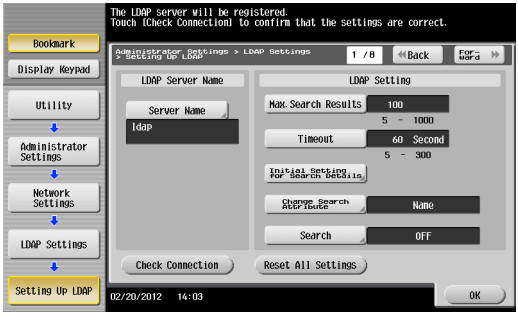


Item	Description
Enabling LDAP	Select [ON].

Setting Up LDAP

Register the desired LDAP server to search for the destination.

On the MFP control panel, tap [Utility] - [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.
Change Search Attribute	Select the attribute of the name used for LDAP searching. You can toggle this attribute between [Name] (cn) and [Nickname] (displayName).
Search	Select whether to display candidate destinations when entering part of a name.
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.

Item	Description
Certificate Verification Level Settings	To verify the certificate, configure settings to verify the certificate. • [Expiration Date]: Select whether to check that the certificate is within the validity period. • [Key Usage]: Select whether to check that the certificate is used according to the purpose approved by the issuer. • [Chain]: Select whether to check that the certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. • [Expiration Date Confirmation]: Select whether to check that the certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked. • [CN]: Select whether to check that the CN of the certificate matches the server address.
Authentication Type	Select the authentication method to connect to the LDAP server. • When connecting to the LDAP server using the Kerberos authentication method, select [GSS-SPNEGO]. Then specify the domain name of the Active Directory in [Domain Name]. • When specifying the LDAP server with an anonymous user enabled, you can select [Anonymous].
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).
Search Attributes Authentication	This setting is not available.
Search Attribute(s)	This setting is not available.

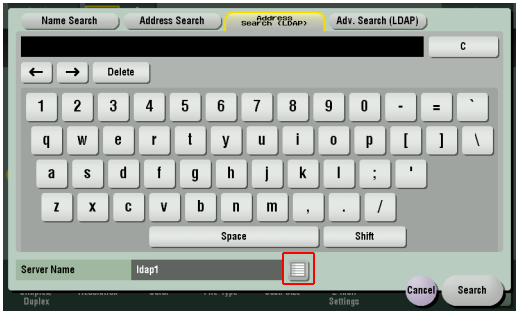
3.3.3 Handling Address Search (LDAP)

Use the Fax/Scan screen on the MFP control panel, and tap [Addr. Search]-[Search]-[Address Search (LDAP)] or [Adv. Search (LDAP)]. This section explains examples of procedures when [Address Search (LDAP)] is selected.

Note

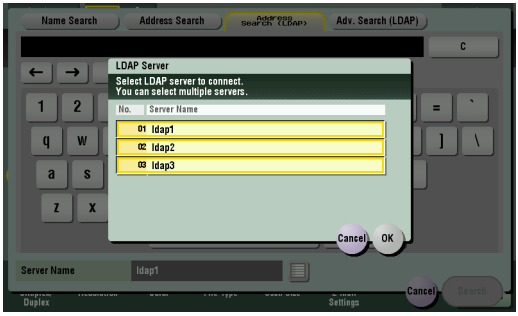
If address search (LDAP) setting incorrectly configured properly, [Address Search (LDAP)] and [Adv. Search (LDAP)] will not appear. Check that the address search (LDAP) setting is configured correctly.

1 When selecting an LDAP server to search for a target address, tap the list icon next to [Server Name].



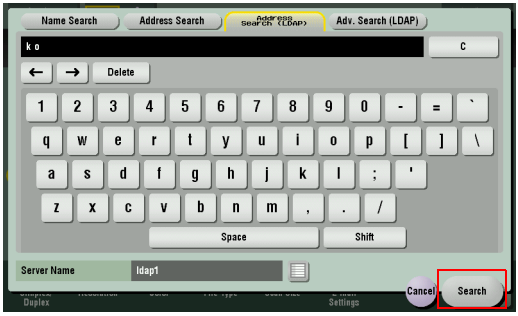
2 Select an LDAP server in which to search for a target address, and tap [OK].

– If necessary, you can select multiple LDAP servers.



3 Enter a search keyword, then tap [Search].

Authentication is performed for the selected LDAP server using the Kerberos authentication ticket before searching starts.



...

Note

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

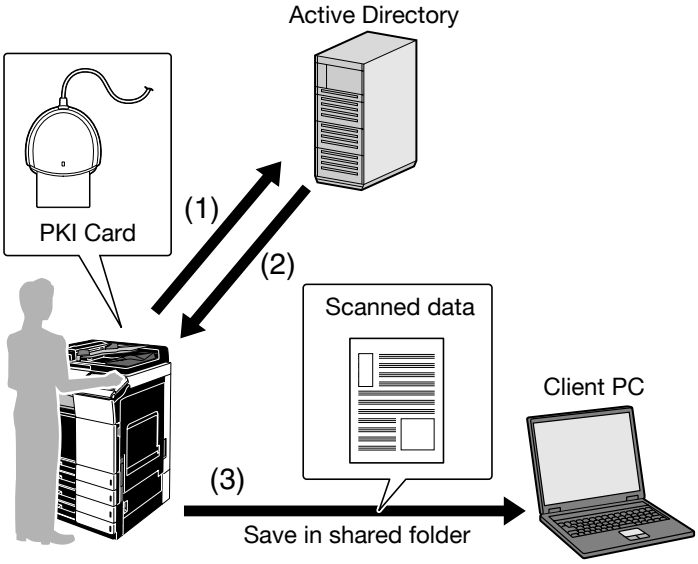
3.4 SMB TX Using PKI Card

3.4.1 Overview

This function logs into the destination computer using the Kerberos authentication ticket that is obtained by Active Directory authentication with the PKI card when sending scanned data via SMB.

If the Kerberos authentication ticket is used for authentication in the destination computer, the user can carry out SMB TX securely without making the password public on the network.

The user can also perform the Active Directory authentication only once to obtain access privileges, and configure the single sign-on environment to be convenient.



(1) Insert the PKI 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.

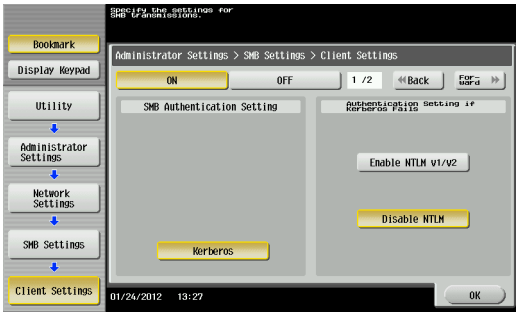
3.4.2 Related Settings

This section explains how to configure the SMB TX settings on the MFP that supports this system.

Client Settings

Configure the setting to perform SMB TX.

On the MFP control panel, tap [Utility] - [Administrator Settings] - [Network Settings] - [SMB Settings] - [Client Settings].



Item	Description
ON/OFF	Select [ON].
SMB Authentication Setting	The SMB authentication type is set to [Kerberos].
Authentication Setting if Kerberos Fails	Select whether to perform NTLM authentication when Kerberos authentication has failed.
User Authentication (NTLM)	Select whether or not the NTLM user authentication is performed.
DFS Setting	To perform SMB TX in a DFS (Distributed File System) environment, select [Enable].
Setting when NTLM is enabled	Select which operation is to be performed when authentication has failed using the Kerberos authentication ticket. • If [Yes] is selected while [Authentication Setting if Kerberos Fails] is set to [Enable NTLM v1/v2], the screen for entering the user ID and password appears when authentication has failed using the Kerberos authentication ticket. NTLM v1/v2 authentication can be performed by entering the user ID and password. • If [No] is selected, it results in an authentication failure.

Note

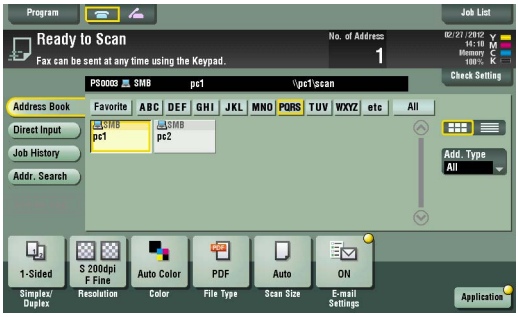
Specify the WINS server or direct hosting service to fit your environment. For details, refer to the User's Guide [Web Management Tool] supplied together with the MFP.

3.4.3 Using SMB TX

SMB TX

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

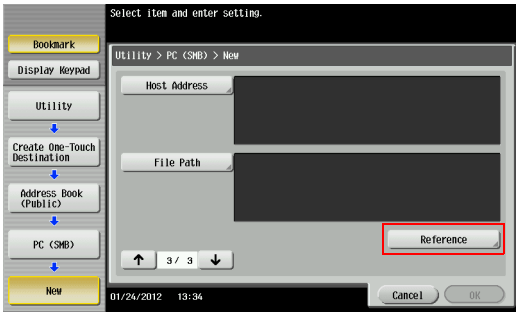
- *For details on how to register the SMB address or use SMB TX, refer to the User's Guide [Scan] supplied together with the MFP.*
- *In [Client Settings], you can specify the operation required when authentication has failed using the Kerberos authentication ticket. For details, refer to "Client Settings" (page 36).*

Searching for SMB address

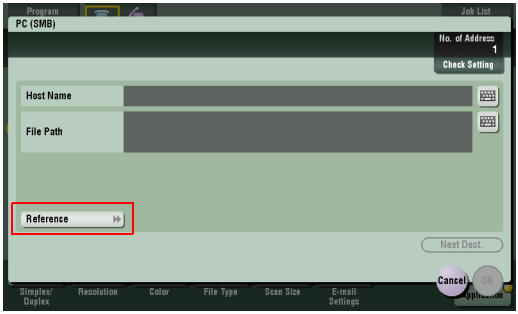
If [Reference] is tapped to register or specify the SMB address, the system searches for computers on the Windows network to enable you to register or specify the desired one as a destination.

If a PKI card is used to log in to the MFP, log in to the searched computer using the Kerberos authentication ticket to register or specify it as a destination.

<SMB address registration screen>



<SMB address specification screen (Direct Input)>



Detail

[Reference] is not displayed on the SMB address registration screen (Administrator Settings).

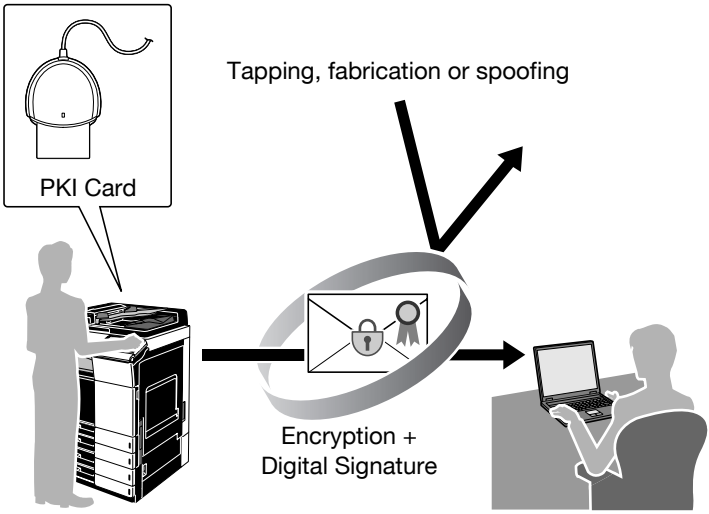
3.5 Scan to E-mail (S/MIME) Using PKI Card

3.5.1 Overview

This function uses the PKI card 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.

The certificate obtained from the PKI card is used to encrypt an e-mail to the user's address using the Scan to Me function. For details on the Scan to Me function, refer to "Scan to Me" (page 57).



Note

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

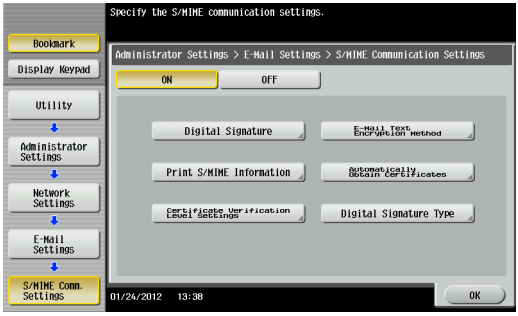
3.5.2 Related Settings

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

S/MIME Communication Settings

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

On the MFP control panel, tap [Utility] - [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 PKI card when sending an e-mail.
E-Mail Text Encryption Method	Select the e-mail text encryption method.
Print S/MIME Information	Select whether or not S/MIME information is printed when sending and receiving e-mail message.
Automatically Obtain Certificates	Select whether or not certificates are automatically obtained when sending and receiving e-mail messages.

Item	Description
Certificate Verification Level Settings	To verify the certificate, configure settings to verify the certificate. • [Expiration Date]: Select whether to check that the certificate is within the validity period. • [Key Usage]: Select whether to check that the certificate is used according to the purpose approved by the issuer. • [Chain]: Select whether to check that the certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. • [Expiration Date Confirmation]: Select whether to check that the certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.
Digital Signature Type	Select the digital signature type.

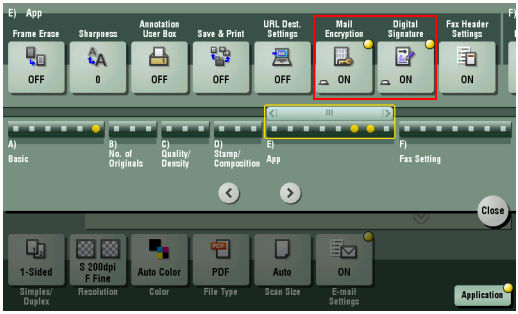
Note

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

3.5.3 Encrypting an E-Mail and Adding a Digital Signature

Display the Fax/Scan screen on the MFP control panel, and tap [Application].

- To encrypt an e-mail, set [E-Mail Encryption] to [ON].
- If [Select when sending] is selected to add a digital signature, set [Digital Signature] to [ON]. If [Always add signature] is selected, a digital signature will be automatically added.



Detail

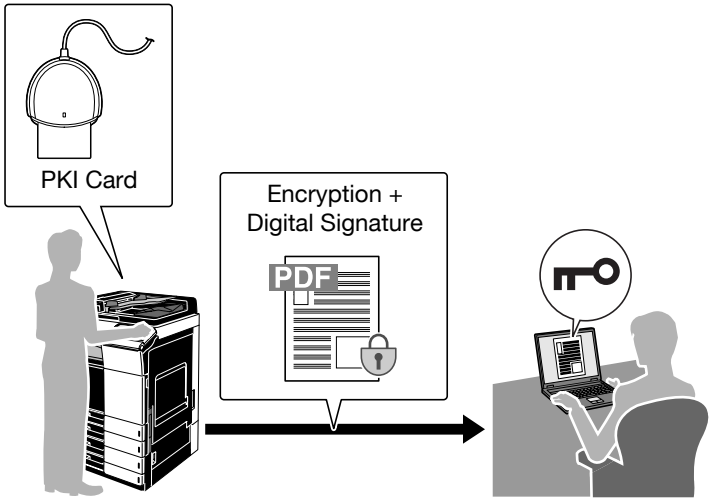
- *When setting to enable encryption or to add a digital signature, you can specify up to 10 E-mail addresses to be broadcasted.*
- *When setting to enable encryption or to add a digital signature after 11 or more E-mail addresses have already been specified, you need to cancel all the specified addresses once and reselect them.*
- *When the encryption is set after specifying the E-mail addresses (up to 10 E-mail addresses), specified E-mail addresses that do not have a registered certificate will be canceled.*
- *For details on how to send an e-mail, refer to the User's Guide [Scan] supplied together with the MFP.*
- *For details on how to register the certificate in the e-mail address, refer to the User's Guide [Web Management Tool] 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.*

3.6 PDF Encryption and Signature Addition Using PKI Card

3.6.1 Overview

This function encrypts a PDF document and adds a signature using the digital certificate registered in the PKI card when distributing scanned data as a PDF document.

Encrypting a PDF document prevents any third parties from illegally accessing it. Furthermore, adding a signature identifies the author of a PDF document and guarantees that the file has not been fabricated.



Note

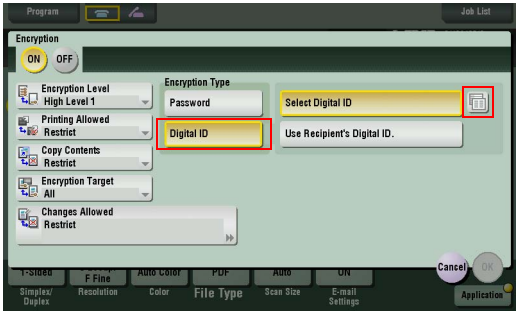
- *The optional Upgrade Kit UK-204 and i-Option LK-102 v3 are required to encrypt a PDF document using the PKI card.*
- *This function is not available when you log in to the MFP as a public user or User Box administrator.*

3.6.2 Encrypting a PDF Document

To encrypt a PDF document, use the digital certificate registered in the PKI card.

First, select [PDF] or [Compact PDF] as the file type, and set [PDF Detail Setting] - [Encryption] to [ON]. Then, execute the following settings.

1 Select [Digital ID] under [Encryption Type], then tap the detail icon next to [Select Digital ID].



2 To encrypt a PDF document using the digital ID of the PKI card, tap [PKI Card].

3.6.3 Adding a Signature to a PDF Document

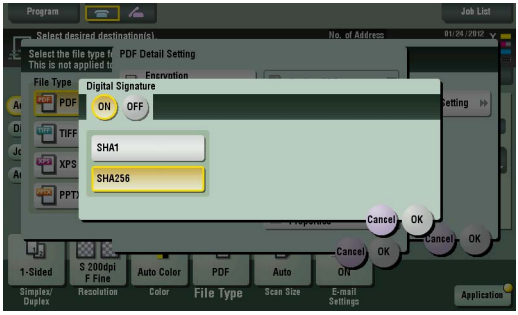
To add a signature to a PDF document, use the digital certificate registered in the PKI card.

...

Note

To use this function, you need to configure the setting for encrypting a PDF document in advance. For details, refer to "Encrypting a PDF Document" (page 45).

First, select [PDF] or [Compact PDF] as the file type, and set [PDF Detail Setting] - [Digital Signature] to [ON]. Then, select [SHA1] or [SHA256] as the signature encryption level.

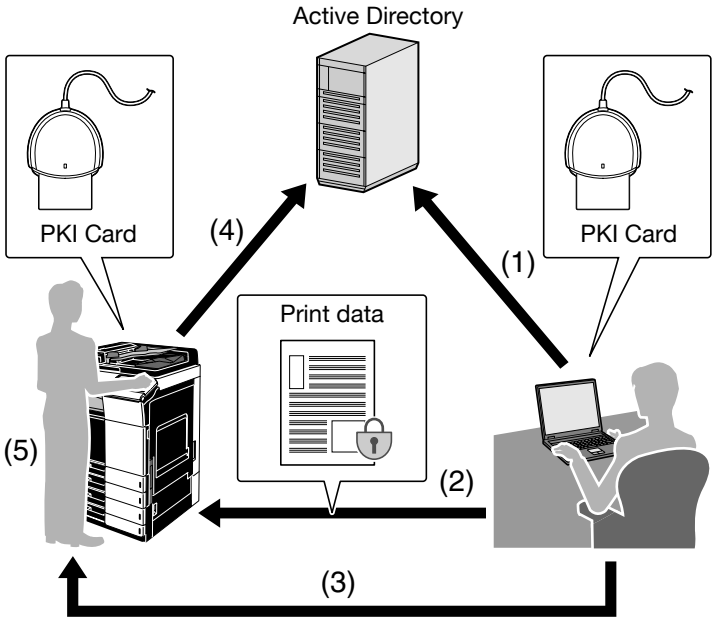


3.7 PKI Card Print

3.7.1 Overview

This function encrypts print data using the PKI 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, and the same user can perform authentication at the MFP with the PKI card to decrypt and print the data.

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 PKI card is successful; therefore, you can ensure the confidentiality of documents.



(1) Insert the PKI card into the computer to perform Active Directory authentication.

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

(3) Take the PKI card to the MFP.

(4) Insert the PKI card into the MFP to perform Active Directory authentication.

(5) Decrypt print data using the PKI card, and print it.

3.7.2 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	PCL6	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 7 Home Basic Windows 7 Home Premium * Windows 7 Professional * Windows 7 Enterprise * Windows 7 Ultimate * Windows 8 */Windows 8.1 * Windows 8 Pro */Windows 8.1 Pro * Windows 8 Enterprise */Windows 8.1 Enterprise * 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 Windows Server 2008 Standard * Windows Server 2008 Enterprise * Windows Server 2008 R2 Standard Windows Server 2008 R2 Enterprise Windows Server 2012 Datacenter Windows Server 2012 Standard Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Standard * Available in 32-bit (x86) or 64-bit (x64) environment.

Type	Page description language	Supported Operating System
PS driver	PostScript 3 Emulation	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 7 Home Basic Windows 7 Home Premium * Windows 7 Professional * Windows 7 Enterprise * Windows 7 Ultimate * Windows 8 */Windows 8.1 * Windows 8 Pro */Windows 8.1 Pro * Windows 8 Enterprise */Windows 8.1 Enterprise * 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 Windows Server 2008 Standard * Windows Server 2008 Enterprise * Windows Server 2008 R2 Standard Windows Server 2008 R2 Enterprise Windows Server 2012 Datacenter Windows Server 2012 Standard Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Standard * Available in 32-bit (x86) or 64-bit (x64) environment.

Installing the printer driver

The installer enables you to easily install the printer driver by following the instructions displayed on the pages.

Note

Administrator authority is required to install the printer driver on your computer.

1 Start the installer.

2 Check the contents of the license agreement, and click [AGREE].

– If you disagree, you will not be able to install the driver.

3 Install the printer driver by following the instructions displayed on the pages.

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 [Print] supplied together with the MFP.*
- *For details on how to uninstall the printer driver, refer to the User's Guide [Print] supplied together with the MFP.*

3.7.3 Specifying the Print Data Deletion Time

The data encrypted with the PKI 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.

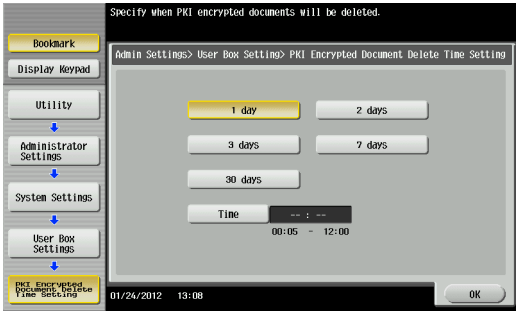
Note

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

PKI Encrypted Document Delete Time

On the MFP control panel, tap [Utility] - [Administrator Settings] - [System Settings] - [User Box Settings] - [PKI Encrypted Document Delete Time].

Specify the period from the document saving time to the automatic deletion time.



3.7.4 Handling 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 PKI card and sending it to the MFP.

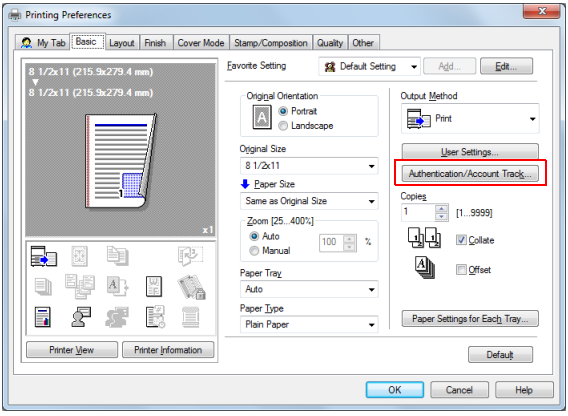
1 Click [Print] in the menu of the application software.

2 Select the desired printer .

3 Click [Properties] or [Preferences].

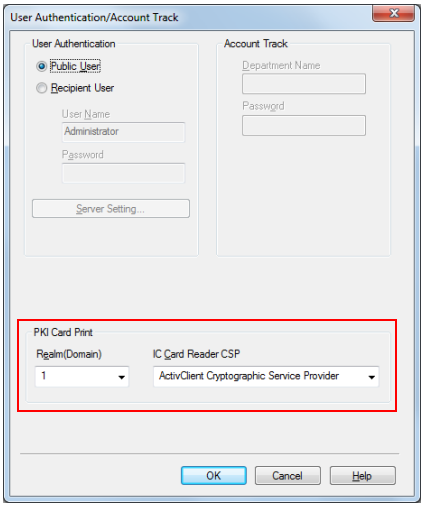
4 Click the [Basic] tab.

5 Click [Authentication/Account Track].

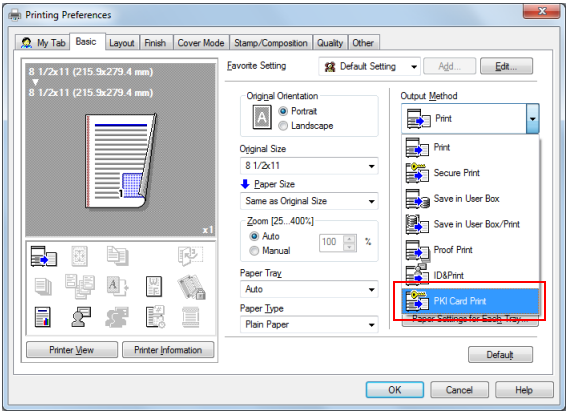


6 Select the [Realm(Domain)] and [IC Card Reader CSP], and click [OK].

- The value of [Realm(Domain)] corresponds to the registration number of the Active Directory. When using the Active Directory that was registered to No. 02 for authentication, set the value of [Realm(Domain)] to [2].
- PKI Card Print uses authentication information of the PKI card; therefore, it disables the authentication information specified in [User Authentication].



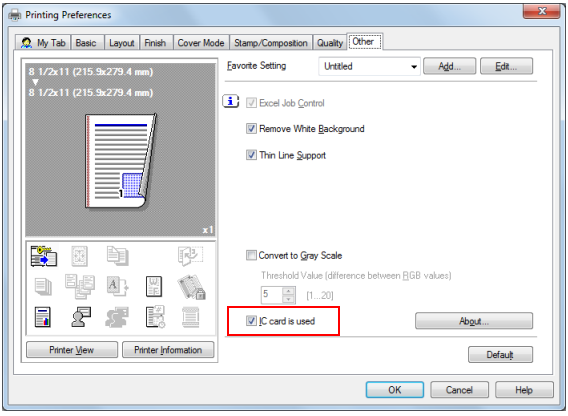
7 Under [Output Method], select [PKI Card Print], and click [OK].



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.*
- *To print without using a PKI card, select the [Other] tab, and then clear the [IC card is used] check box. In this case, perform authentication according to the [User Authentication] setting in step 6. The [IC card is used] check box is selected by default. If the check box is cleared, [PKI Card Print] cannot be selected in step 7.*



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 PKI 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.

...

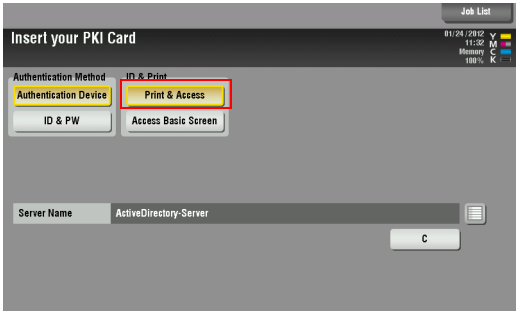
Note

- *Selecting method (1) prints all print documents stored in the user's PKI Encrypted Document User Box.*
- *The documents stored in the PKI Encrypted Document User Box are deleted automatically after the specified period has lapsed. For details on how to specify the deletion time, refer to "Specifying the Print Data Deletion Time" (page 51).*
- *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.

➔ Tap [Print & Access], and insert the PKI card into the authentication unit attached to the MFP.



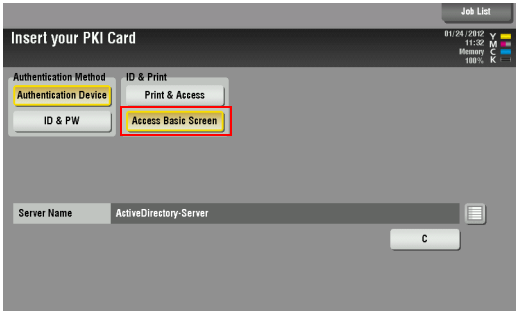
– If the PKI card is inserted, the PIN code entry screen appears. When authentication succeeds after entering the PIN code, the system prints all the relevant user's data and logs into the MFP.

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 [Print] supplied together with the MFP.

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

1 Tap [Access Basic Screen], and insert the PKI card into the authentication unit attached to the MFP.



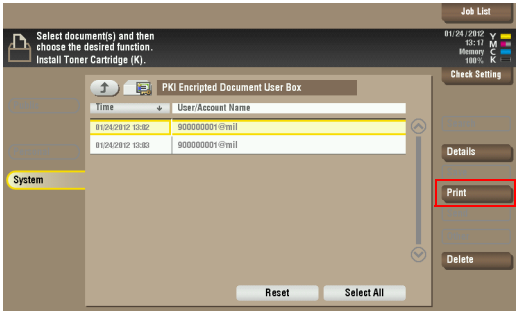
2 Enter the PIN code and to log into the MFP.

3 Tap [User Box] - [System] - [PKI Encrypted Document].

A login user's print data list is displayed.

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

- To delete data, select the data to be deleted, and tap [Delete].
- Tap [Details] to view detailed information on the selected document.



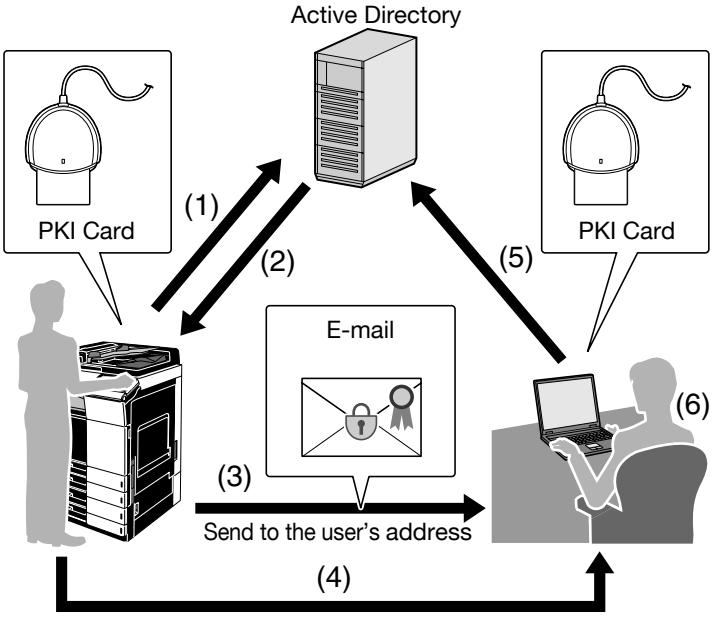
3.8 Scan To Me

3.8.1 Overview

Scan To Me is a function that sends scanned data to the user's e-mail address.

This function is useful when frequently sending scanned data to the user's address.

Using this function, the user can obtain the authenticated user's e-mail address using the LDAP protocol to easily send data to the obtained address. The user can also encrypt an e-mail using the PKI card or add a digital signature when sending an e-mail, ensuring a higher level of security.



(1) Insert the PKI 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 PKI card to encrypt an e-mail or add a digital signature.

(4) Take the PKI card to the computer.

(5) Insert the PKI card into the computer to perform Active Directory authentication.

(6) Receive the e-mail. After you have encrypted an E-mail or added a digital signature when sending the E-mail, decrypt the E-mail and check the signature using the PKI card.

Note

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

3.8.2 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 [Web Management Tool] supplied together with the MFP.

S/MIME Communication Setting

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

For details on how to handle e-mail TX using the PKI card and configure its settings, refer to "Scan to E-mail (S/MIME) Using the PKI Card" (page 40).

3.8.3 Handling Scan To Me

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

Detail

- *If the correct settings are configured to use Scan To Me, [Me] appears on the Fax/Scan screen to send data to the user's e-mail address.*
- *If the system fails to obtain the certificate in the PKI card when encrypting the e-mail to the user's address using the PKI card, [Me] will not appear. For details on the e-mail encryption setting, refer to "Scan to E-mail (S/MIME) Using the PKI Card" (page 40).*

1 Tap [Scan/Fax].

2 Configure Scan option settings as necessary.

3 Tap [Me].

4 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 [Scan] supplied together with the MFP.

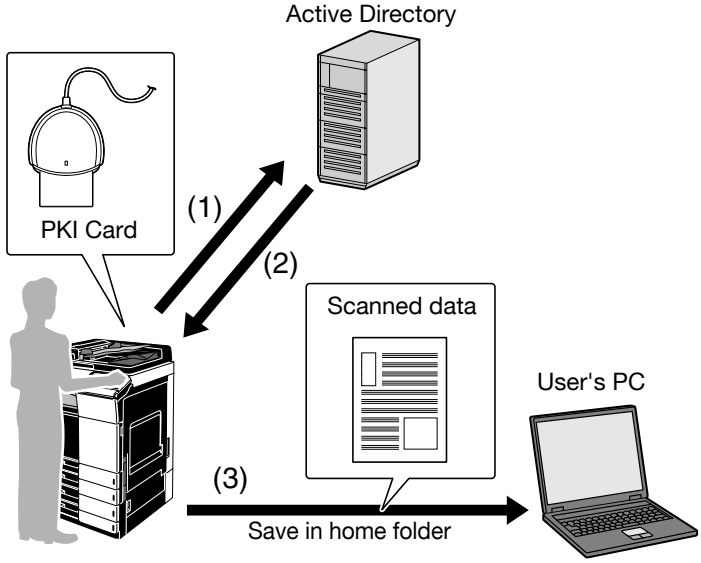
3.9 Scan To Home

3.9.1 Overview

Scan To Home is a function that sends scanned data to the user's computer.

This function is effective when frequently sending scanned data to the user's address.

The user can obtain the position of the user's Home folder from Active Directory, and easily send data to the user's Home folder. To perform authentication in the user's computer, this function uses the Kerberos authentication ticket obtained when logging into the MFP, preventing the password from being made public on the network.



(1) Insert the PKI 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.

3.9.2 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 35).

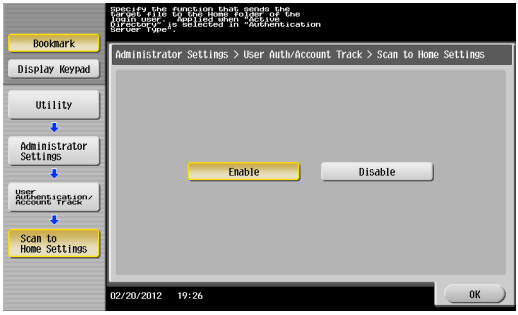
Note

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

Scan to Home Settings

Enable the Scan to Home function.

On the MFP control panel, tap [Utility] - [Administrator Settings] - [User Authentication/Account Track] - [Scan to Home Settings].



Item	Description
Scan to Home Settings	Select [Enable].

3.9.3 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] appears on the Fax/Scan screen to send data to the user's Home folder.

1 Tap [Scan/Fax].

2 Tap [Home].

3 Configure Scan option settings as necessary.

4 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 [Scan] supplied together with the MFP.

4 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.

4.1 User Settings

4.1.1 System Settings

Item	Description
Language Selection	The available language is English only.

4.2 Administrator Settings

4.2.1 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 51).

4.2.2 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 the PIV transitional specifications, select PIV or CAC as the PIV Transitional Mode.

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 17).

4.2.3 Network Settings

FTP Settings

Item	Description
FTP Server Settings	The default is [OFF].

Note

We recommend that this function is set to the disable state when this system is operated.

SMB Settings

Item	Description
Client Settings	• [SMB Authentication Setting] is available only for [kerberos]. • [Setting when NTLM is enabled] has been added. • [Single Sign-On Setting] is not displayed. • For details, refer to "Client Settings" (page 36).

LDAP Settings

Item	Description
Setting Up LDAP	• [Login Name], [Password] and [Select Server Authentication Method] are not displayed. • [Authentication Type] is available only for [GSS-SPNEGO] or [Anonymous]. • [Select Server Authentication Method] is automatically set so that User Authentication is enabled. • For details, refer to "Setting Up LDAP" (page 31).

E-Mail Settings

Item	Description
E-Mail TX (SMTP)	[Detail Settings] - [SMTP Authentication] - [Authentication Setting] is fixed to [Use Set Value]. When performing SMTP authentication, specify the user ID and password for SMTP authentication.
S/MIME Communication Settings	[Select when sending] is set as the default for [Digital Signature].

SNMP Settings

Item	Description
SNMP v1/v2c Settings	The default of [Write Setting] is [Invalid].
SNMP v3 (IP)	The default is [OFF].

Note

We recommend that this function is set to the disable state when this system is operated.

TCP Socket Settings

Item	Description
TCP Socket	The default is [OFF].

Note

When this setting is set to [ON], the i-Option LK-115 (TPM option) is recommended in order to use the machine more securely.

WebDAV Settings

Item	Description
WebDAV Server Settings	The default is [OFF].

Note

When this setting is set to [ON], the i-Option LK-115 (TPM option) is recommended in order to use the machine more securely.

4.2.4 Security Settings

Security Details

Item	Description
Prohibited Functions when Authentication Error	The default is [Mode 2].
Confidential Document Access Method	The default is [Mode 2].
Job Log Settings	The default of [Audit Log] is [OFF]. When this setting is set to [ON], the i-Option LK-115 (TPM option) is recommended in order to use the machine more securely.

5 Appendix

5.1 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 operating temperature	0 to 50°C
Interface	Full speed USB (12 Mbps)
Connector shape	USB A type connector
Compatible card	PKI-IC card (PIV, CAC)

5.2 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.*

5.3 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 representative.

KONICA MINOLTA

http://konicaminolta.com

A2X0-9608-02

2014. 2