AU-211P CAC/PIV Solution

Network Configuration 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.

2 Getting Started

2.1 Introduction

This document is intented for authorized Konica Minolta service and networking representatives. This guide will outline the installation, network configuration and use of the Konica Minolta CAC/PIV PKI card solution with the designated bizhub Multifunction Printers (MFP).

CAC = Common Access Card (DoD)

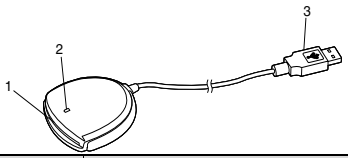
PIV = Personal Identity Verification Card (US Gov't)

The US Government CAC/PIV Card Directive

Following September 11th, 2001 the US Govenment created a directive, HSPD-12, to better secure all levels of government access; from building access to computer/network access. All levels of government are included Military personnel, government employees (civilian and like wise) as well as all governmental contractors. Anyone who is looking to gain access to a governmental building or network.

This solution will allow a bizhub MFP, that is connected to a DoD or other government agency network, to securely authenticate a CAC or PIV card carrying user to the network using the included CAC/PIV Card Reader and the Konica Minolta specialy designed Firmware/Middleware solution. This Firmware/Middleware can completely secure or lock down all access and functions of a specified MFP or secure only those MFP features that touch the government networks, featrures like; Scan to Email, Scan to Network Share, etc. The level of MFP security can be customized by an administrator and/or departmental requirements.

2.2 Included Parts and their functions



No.	Part name	Description
1	Card inlet	Used to insert the PKI card.
2	LED lamp	Turns green when you log in using the PKI card. A blinking light indicates activity between the card and reader.
3	USB cable	Used for connecting this device to the multifunctional product.

2.3 Before Installation Begins

This installation process must be completed by a trained Konica Minolta Service Technician and/or Network Engineer. Before beginning this installation procedure the individual performing this install must meet the technical requirements and complete the on-line training module. Please refer to the service training area of the Learning Place.

Before the installation process begins it is mandatory that the following Prerequisite Checklist is completed.

Prerequisite Checklist:

- ✔ CAC/PIV compatible bizhub MFP
- ✔ USB Host Kit for color bizhub MFPs (USB is preinstalled on B&W MFPs)
- ✔ Working Table for bizhub MFP
- ✔ AU-211P CAC/PIV USB Card Reader
- ✔ KM CAC/PIV Firmware (CF Card) for the compatible MFP.
- ✔ A USB Thumb Drive containing the AU-211P loadable driver files
- ✔ Completed CAC/PIV Solution Installation Survey & Checklist
- ✔ Access to a valid CAC or PIV card

Once the checklist is completed the installation proces can begin starting with the Firmware installation.

Detail

The AU-211P Loadable Drivers MUST be downloaded from MyKonica Minolta.com and loaded to a USB Thumb Driver before the installation process begins.

4 Network Configuration

It is recommended that a qualified Network Engineer perform the network configurations. Before beginning this portion of the installation procedure the individual performing these steps must meet the technical requirements for the CAC/PIV solution and complete the on-line training module. Please refer to the service training area of the Learning Place.

NOTE: The completed Installation Survey & Checklist will be required for this section!

This section will cover the following network settings;

- Configuring network settings IP address and DNS, (page 55)
- Registering Active Directory for authentication (page 57)
- Correcting the MFP time (page 58)
- Registering the DNS server associated with Active Directory (page 59)
- Specifying the CAC mode or PIV transitional mode (page 62)
- Configuring settings for verifying the Active Directory certificate (page 63)

Soft Switch Verification:

Please verify the mandatory and optional soft switch settings for the specific MFP you are now configuring for the network.

bizhub C353 series

MFP Generic Screen Settings

If during the reboot of the MFP you see the generic 'Globes' screen instead of the Blue Konica Minolta Logo you will need to make a soft switch setting change.

- Enter Service Mode
- Enter System 2-> Soft Switch Settings
- Switch No. 10
- HEX Assignment 00 (generic screen)
- HEX Assignment 02 (Konica Minolta Logo screen)
- Press Fix

Network Environment Settings

The following soft switch setting is manditory

- Enter Service Mode
- Enter System 2-> Soft Switch Settings
- Switch No. 41
- Bit Assignement 00011000 Enable PrincipleName '*user*@mil' & FQDN

- Press Fix

The folllowing settings are optional an will be determined by the customer environment, the Installation Survey & Checklist and the Ping Confirmation Test which is performed during the network configuration process.

- Bit Assignement 00011100 Enable PrincipleName, FQDN & LDAP w/SSL
- Press Fix

Scan to Me/Scan to Home

If the customer requires Scan to Me/Scan to Home the following soft switch will have to be enbled. Please reference the Installation Survey & Checklist

- Enter Service Mode
- Enter System 2-> Soft Switch Settings
- Switch No. 26
- HEX Assignment 10 (to enable)
- HEX Assignment 00 (to disable) *Default
- Press Fix

bizhub 501 series

Network Environment Settings

The following soft switch setting is manditory

- Enter Service Mode
- Enter System 2-> Soft Switch Settings
- Switch No. 44
- Bit 2 = ON Enable PrincipleName '*user*@mil'
- Press Set
- Bit 3 = ON Enable FQDN
- Press Set

The folllowing settings are optional an will be determined by the customer environment, the Installation Survey & Checklist and the Ping Confirmation Test which is performed during the network configuration process.

- Bit 1 = Enable LDAP w/SSL
- Bit 5= Enable Scan to Me and Scan to Home
- Bit 6= Enable Scan to Me and SMB

4.0.1 Configuring Network Settings

TCP/IP Settings

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

The MFP is defaulted to DHCP ON this will automatically capture most of the

network settings. If the customer wants the MFP to utilize a static address the DHCP functions will need to be turned OFF.

➔ Select ON to activate TCP/IP settings.

➔ Select either IPv4 or IPv6 (deactivate the auto obtain function if necessary),

➔ Enter the IP Address, Subnet Mask and Default Gateway as they appear in the Installation Survey & Checklist.

➔ Close this window, you will be asked to restart the MFP.

IPv4 Settings

Item	Description
IP Application Method	Select whether to automatically retrieve the IP address or directly specify it.
IP Application Method Auto Setting	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.
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 enviroment.
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

The DNS Host Name can be modified to accomodate the customers requirements.

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

Again, if the customer is allowing DHCP the domain name will automatically be populated. If they are not you will have to disable auto retrieval and manually enter the domain name. Click OK to exit

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 255 bytes with the host name).
DNS Search Domain Name 1 to 3	Specify the DNS search domain name (up to 253 bytes).

4.0.2 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, press the [Utility/Counter] key, and then [Administrator Settings] - [User Authentication/Account Track] - [External Server Settings] - [select the next available number (i.e No. 1)] - [New]

➔ Select Server Name and enter the name of the server as the custromer would like it to appear on the MFP. For security purposes this name does not have to mimic the actual server name. A department, group or division name can be used.

➔ Select Server Type - Active Directory

➔ Enter the Fully Qualified Domain Name. Select Close

Item	Description
Server Name	Specify the name of the external server (up to 32 characters).

Item	Description
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 press [Set as Default].

Troubleshooting Tip:

Use the Ping Confirmation option to confirm the IP Address and the Host Name, refer to page 60

4.0.3 Syncronizing the MFP Time with an NTP Server

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

Time Adjustment Setting

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [Forward] - [Detail Settings] - [Time Adjustment Setting].

➔ Select ON to activate the Time Adjustment Feature.

➔ Select Host Address and enter the NTP server IP Address.

➔ Proceed to Date/Time Settings.

Item	Description
ON/OFF	Select [ON].
Host Address	Specify the host address of the NTP server associated with Active Directory.

Item	Description
Port Number	Specify the port number.

Daylight Saving Time

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [System Settings] - [Daylight Saving Time].

➔ Select Yes to activate Daylight Saving the minute field will automatically set 60 minutes in the field.

➔ Select No to deselect.

Date/Time Settings

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [System Settings] - [Date/Time Settings].

➔ Enter the Time Zone Adjustment (i.e. EST= -5:00, PST= -8:00)

➔ Next select Set Date to sync the MFP with the server clock.

– You will see the “Adjustment Completed Successfully” message, click close.

Item	Description
Set Date	Correct the time. Then press [OK] to start the clock.

4.0.4 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, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [TCP/IP Settings] - [DNS Server Settings (IPv4)].

➔ If the customer does not want to auto obtain this information disable the function by selecting the Disable button.

➔ Enter the Primary DNS Server IP Address. Enter the second and third IP addresses if necessary/available.

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, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [TCP/IP Settings] - [DNS Server Settings (IPv6)].

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.

4.0.5 Email Server Settings

To enable Scan to Email the folllowing settings will need to be entered. Verify all email settings and functions with the Installation Survey and Checklist and an IT admin.

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

➔ If using SMTP select Email TX (SMTP)

➔ Turn ON

➔ Scroll to page 2, select Host Address and enter the email server IP Address. Click OK.

➔ If using POP select Email TX (PoP)

➔ Turn ON

➔ Select Host Address and enter email server IP Address. Click OK.

➔ Select S/MIME Communication Settings

➔ Turn ON, Click OK and Close.

4.0.6 LDAP Settings

To enable LDAP the folllowing settings will need to be entered. Verify all settings and functions with the Installation Survey and Checklist and an IT admin.

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

➔ Select Enabling LDAP
➔ Turn ON and OK
➔ Select Setting Up LDAP
➔ Select a blank button
➔ Select Server Name and enter the LDAP server name. For security purposes a generic name can be entered.
➔ Scroll to page 2, Select Server Name and enter the server IP Address
➔ Select Search Base and enter the search base criteria. This information can be found in the Installation Survey & Checklist or provide by the IT admin. The generic criteria can be cn=users, dc=*domain name*, dc=*.com or .mil etc.*
➔ Scroll to page 3 for SSL settings if needed.
➔ Scroll to page 6, select domain name and enter the domain name. Click OK and close.

4.0.7 Ping Confirmation Test

To verify the current network settings, AD server IP Address, Fully Qualified Domain Name, DNS Server, Email Server, LDAP etc, perform the following Ping test from the MFP.

On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [Forward] - [Detail Settings] - [Ping Confirmation].

➔ Host Address enter the IP Address for the DNS server, LDAP server and Email server. Select Check Confirmation.

If successful move on to the next test below, if unsuccessful confirm addresses with IT Admin, confirm blocked/unblocked ports, firewalls, routers, etc.

➔ Host Address enter the Domain Name and Check Confirmation. Perform this test 5 or more times in a row. If the address fails one or more times a change to the soft switch settings will be needed.

4.0.8 Specifying CAC Mode or PIV Transitional Mode

Originally the DoD used a CAC card exclusively, recently the DoD has introduced a CAC card with PIV transition, so there may be CAC enivironments with just CAC or CAC and CAC with PIV Transition cards mixed together. The CAC/PIV PKI solution has the ability to be configured to handle both types of cards. You will see that the PIV mode is default. This setting will allow for both cards. Start with this setting and move to CAC only if any login issues persist. The CAC settings will allow for CAC card only.

Authentication Device Settings

On the MFP control panel, press the [Utility/Counter] key, and then [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.

4.0.9 Configuration of the Active Directory Certificate Verification Options

Configure the certificate verification settings that will be used to verify the Active Directory certificate when the MFP is communicating with Active Directory.

Certificate Verification Setting

On the MFP control panel, press the [Utility/Counter] key, and then [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 67).
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 "Cert Verification Setting" (page 65).

OCSP Responder Settings

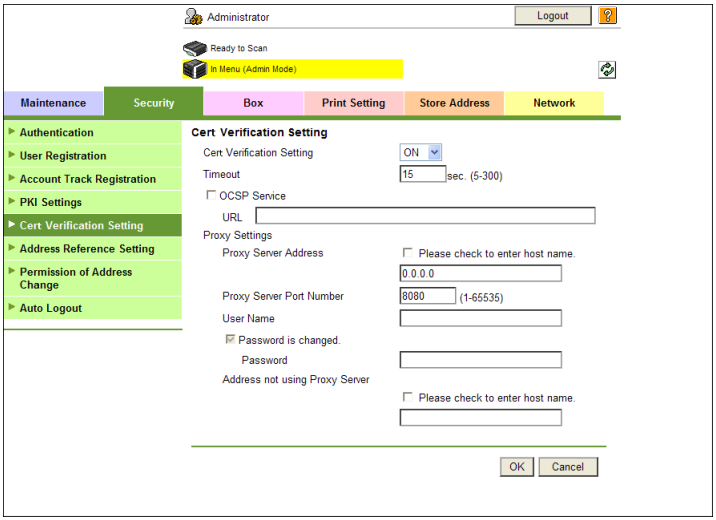
Cert Verification Setting

In the PageScope Web Connection administrator mode, select the Security tab, and then "Cert Verification Setting".

➔ In the Cert Verification Settings drop down select ON

➔ Check the OCSP Service box and enter the URL for the OCSP Server.

➔ Enter any proxy Service information only if a Proxy server is in use.



Item	Description
Cert 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.

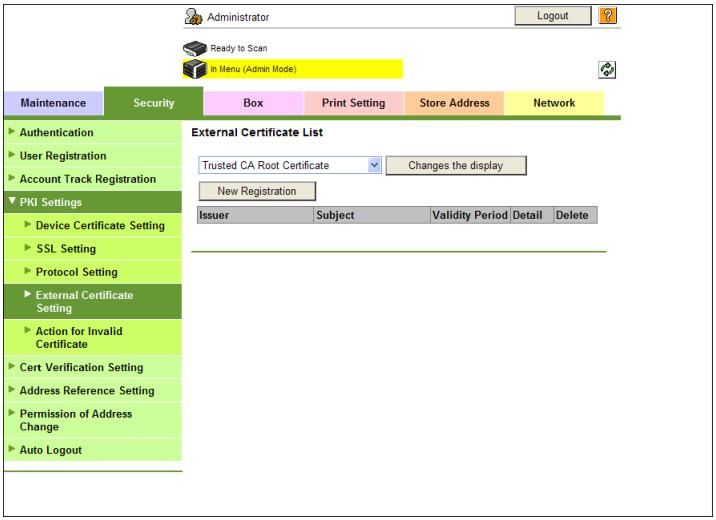
Item	Description
Proxy Server Port Number	Enter the port number for the proxy server.
User Name	Enter the user name to log in to the proxy server (up to 63 characters).
Password	Enter the password to log in to the proxy server (up to 63 characters). When changing the registered password, select "Password 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 the Security tab, and then "PKI Settings" - "External Certificate Setting".

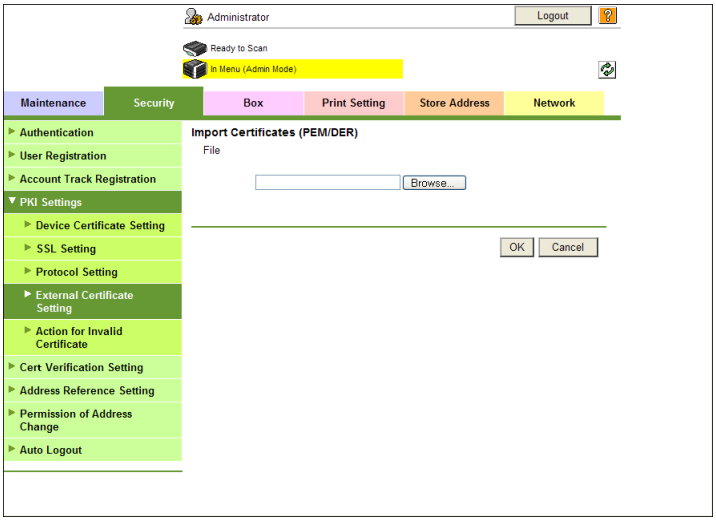
Detail

- *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 [Network Administrator] 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.

4.1 Configuring for Public User Access

The customer may require that some of the MFP functionality be accessible to a user without CAC/PIV card authentication. They may want any user to walk up and copy for example. This request can be accomplished via Public User Access.

➔ On the MFP control panel, press the [Utility/Counter] key, and then [Administrator Settings] - [User Authentication/Account Track] - [General Settings] - [Public User Access] - Allow. Click OK

➔ Select User Authentication Settings - User Registration.

➔ Scroll up (using the up arrow) to the Public button and select the Public button.

➔ Select the Edit button - Function Permission button -

- Copy = Allow
- Scan= Restrict
- Print = Restrict
- User Box = Restrict
- Print Scan/Fax TX = Restrict
- Manual Destination Input = Restrict

Note: Any of these options can be set to allow if the customer requires, but it is **highly recommended** that all functionality that requires network access (scan to email, scan to Me, scan to Home, scan to SMB,etc.) should be restricted from Public Access.

IMPORTANT: A user MUST select the Access hard key to log out of Public User.

4.2 Optional Operation Settings

When operating this system, the following settings can be disabled to ensure a higher level of security if an administrator and/or department/agency requires more security. These are optional settings.

Disabling PageScope Web Connection

Disabling PageScope Web Connection will restrict remote access to the MFP. If this restriction is desired follow the steps below;

Detail

To disable PageScope Web Connection, press the [Utility/Counter] key, and then [Administrator Settings] - [Network Settings] - [HTTP Server Settings] on the MFP control panel, and set "PSWC Settings" to "OFF".

Disabling the OpenAPI function

To associate the MFP with PageScope Authentication Manager, register the MFP in the initial setting of PageScope Authentication Manager, and disable the OpenAPI function of the MFP in the disable state. However, the initial setting results in the MFP administrator password being made public on the network. To ensure security, change the administrator password as required after the initial setting.

Detail

- *To disable the OpenAPI function, press the [Utility/Counter] key, and then [Administrator Settings] - [System Connection] - [OpenAPI Settings] on the MFP control panel, and set "Access Setting" to "Restrict".*
- *To change the MFP administrator password, press the [Utility/Counter] key, and then [Administrator Settings] - [Security Settings] - [Administrator Password] on the MFP control panel.*

Disabling TCP Socket, FTP server, and SNMPv3

To operate this system, disable the TCP Socket, FTP server, and SNMPv3 in the disable state.

Detail

On the MFP that supports this system, the TCP Socket, FTP server, and SNMPv3 functions are disable by default. For details on each setting, refer to the User's Guide [Network Administrator] supplied together with the MFP.