ACCESS MANAGEMENT SYSTEM

Administrator Guide

USRMA-1536-07 2023-03 en

Contents

Preface

Preface

Thank you for selecting this Canon product. Please read this manual thoroughly before operating the product to familiarize yourself with its capabilities, and to make the most of its many functions. After reading this manual, store it in a safe place for future reference.

About This Manual

System Requirements

The manual works with the following web browsers. Use the manual with the script functions and cookies activated in the web browser.

Windows

- Internet Explorer 9 and later
- Microsoft Edge
- Firefox 38 and later
- Firefox ESR 38 and later
- Chrome 45 and later *

macOS

- Safari 8 and later
- Firefox 38 and later
- Chrome 45 and later *

Linux

- Firefox 38 and later

iOS

- Safari (iOS 6.0 and later) *

Android

- Chrome 45 and later *

* Only when browsing the manual on the Internet.

Symbols Used in This Manual

The following symbols are used in this manual to explain procedures, restrictions, handling precautions, and instructions that should be observed for safety.

IMPORTANT

Indicates operational requirements and restrictions. Be sure to read these items carefully to operate the product correctly, and avoid damage to the product or property.

NOTE

Indicates a clarification of an operation, or contains additional explanations for a procedure. Reading these notes is highly recommended.

Buttons Used in This Manual

The following symbols and key/button names are a few examples of how keys on the device and buttons on computer operation screens to be clicked or pressed are expressed in this manual:

- Device Touch Panel Display Keys: [Key Name]

  Examples: [Log In]

  [OK]

- Control Panel Keys: Key Icon (Key Name)

  Examples: (Start)

  0 - 9 (Numeric Keys)

- Buttons/Menu Commands on Computer Operation Screens: [Button/Menu Command Name]

  Examples: [Log In]

  [OK]

NOTE

- The procedures in this manual assume that the [Settings]/[Start] menu and Control Panel display have not been customized after the Windows installation.

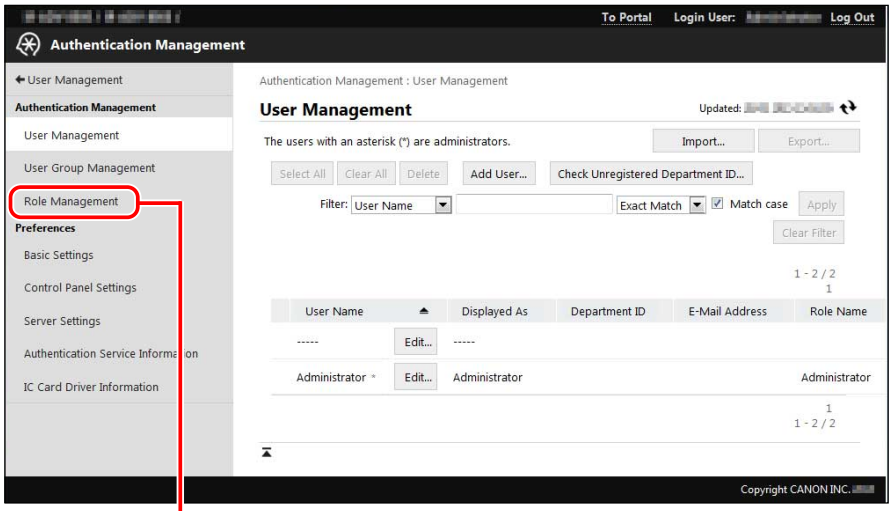
Displays Used in This Manual

Screen shots of computer operation screens used in this manual may differ from the ones you actually see, depending on the operating system and the model or options that come with your device.

The items which you should select/click are marked with a , as shown below.

When multiple items can be selected/clicked, they are circled, and mentioned in the order in which they should be selected or clicked.

3. Click [Role Management].



Click this button for operation.

Abbreviations Used in This Manual

In this manual, product and model names are abbreviated as follows:

Microsoft Windows Server 2008 operating system:	Windows Server 2008
Microsoft Windows Server 2008 R2 operating system:	Windows Server 2008 R2
Microsoft Windows Server 2012 operating system:	Windows Server 2012
Microsoft Windows Server 2012 R2 operating system:	Windows Server 2012 R2
Microsoft Windows Server 2016 operating system:	Windows Server 2016
Microsoft Windows Vista operating system:	Windows Vista
Microsoft Windows 7 operating system:	Windows 7
Microsoft Windows 8.1 operating system:	Windows 8.1
Microsoft Windows 10 operating system:	Windows 10
Microsoft Windows operating system:	Windows
Microsoft Windows Internet Explorer	Internet Explorer
Canon Access Management System:	AMS
Canon Access Management System Printer Driver Add-in:	AMS Printer Driver Add-in

Terms Used in This Manual

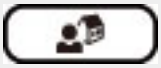
- The term "device" refers to multi functional peripherals (MFP) manufactured by Canon.
- This manual uses the term "Active Directory authentication" to refer to "Server Authentication (Active Directory)".
- This manual uses the term "Windows Server 2008" to refer to the both of Windows Server 2008 (x64) and Windows Server 2008 (x86).

- This manual uses the term "Windows Server 2012" to refer to both Windows Server 2012 and Windows Server 2012 R2.
- This manual uses the term "Windows server operating system" to refer to Windows Server 2008/Windows Server 2008 R2/Windows Server 2012.
- This manual uses the term "Windows client operating system" to refer to Windows Vista/Windows 7/Windows 8.1/Windows 10.
- Some products described in this manual may not be available, depending on the region.

Key and Button Names

The key and button names used in this document may differ from those used in the model of your machine, or keys on the control panel may be changed to buttons on the touch panel display.

The key and button names for the model of your machine are used in this manual as follows.

Key or Button Name in Your Machine	**Key or Button Name in This Document**
 , Main Menu, Home	Main Menu
 , Quick Menu	Quick Menu*
 , 	 (Status Monitor/Cancel)
 ,  , 	 (Settings/Registration)
	 (Log In/Out)

* Quick Menu buttons may be displayed on the Home screen, depending on the model of your machine.

Trademarks

"MEAP" is a trademark of CANON Inc., referring to an "application platform" for Canon multifunction and single function printers.

Windows and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Copyright

Disclaimers

The information in this document is subject to change without notice.

CANON INC. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, EITHER EXPRESS OR IMPLIED, EXCEPT AS PROVIDED HEREIN, INCLUDING WITHOUT LIMITATION, THEREOF, WARRANTIES AS TO MARKETABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OF USE OR NON-INFRINGEMENT. CANON INC. SHALL NOT BE LIABLE FOR ANY DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY NATURE, OR LOSSES OR EXPENSES RESULTING FROM THE USE OF THIS MATERIAL.

Introduction

Introduction

This section describes an overview of the Access Management System and its system requirements.

Main Functions

The Access Management System is a system for managing device restrictions. Restricting the functions that users can use with the Access Management System can have the following effects.

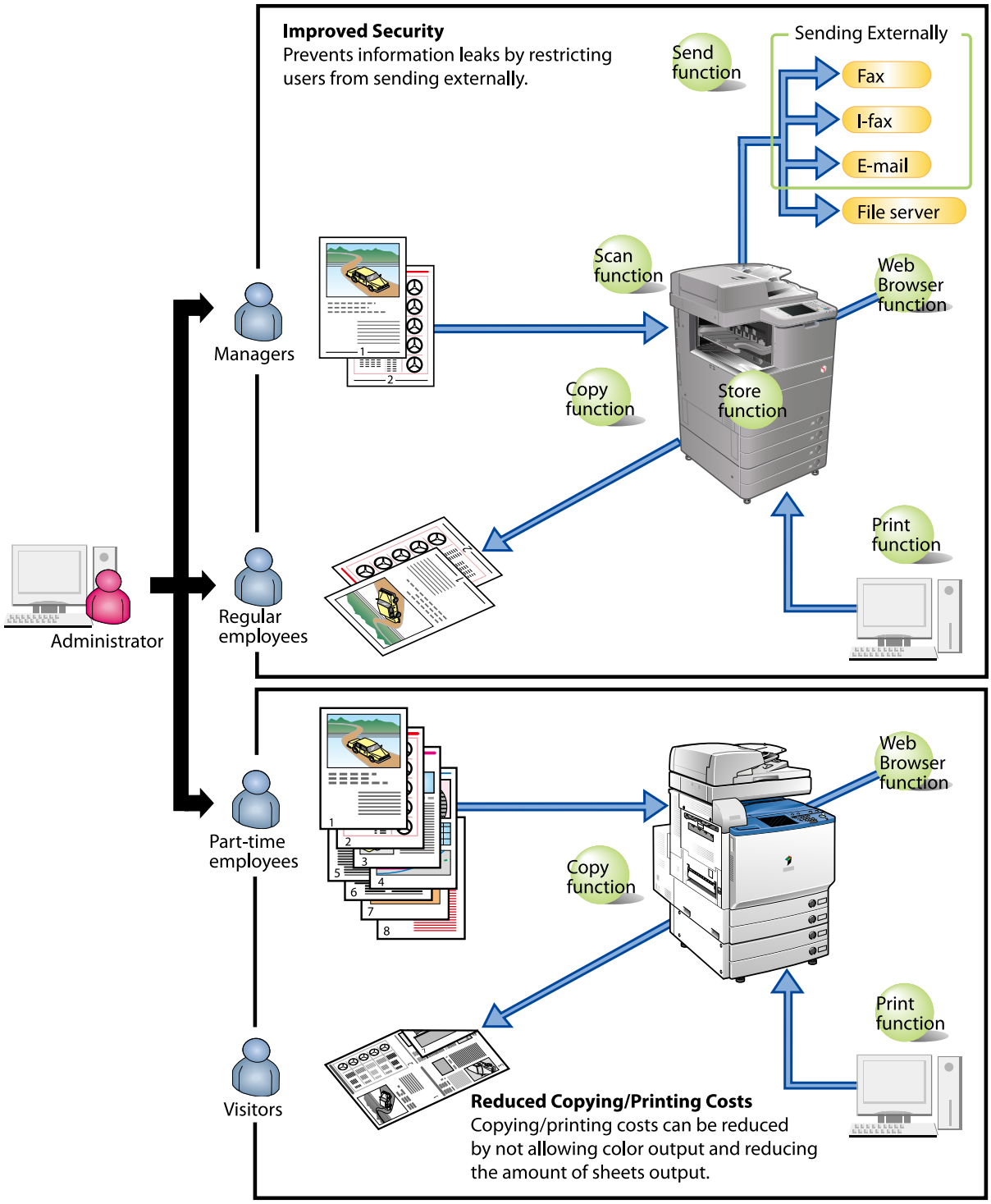
Function Name	Restrictions
Print function	Color printing, one-sided printing, page layout printing, saving to user inboxes
Store function	Color printing of user inbox documents, one-sided printing of user inbox documents, page layout printing of user inbox documents, saving to memory media, saving scanned documents to memory media, printing memory media documents
Copy function	Color copying, one-sided copying, page layout copying
Scan function	Color scanning
Send function/Store on Network	Sending e-mail, sending e-mail using Send to Myself, sending I-faxes, sending faxes, sending to file servers, using the Personal Folder send function, methods for specifying destinations, specifying the format for sending, registering network destinations

NOTE

- Depending on your device, some restrictions may not be supported.

Using the Access Management System can provide the following effects:

- Preventing external leakage of information
  By restricting functions such as the Copy, Send, and Store functions and restricting the keys that can be used on the [Settings/Registration] screen for each user, you can prevent the external leakage of information.
- Reducing costs
  By restricting functions related to copying/printing such as color output, one-sided output, and page layout for each user, you can reduce the cost of using devices.



Flow of User Authentication and Usage Restriction

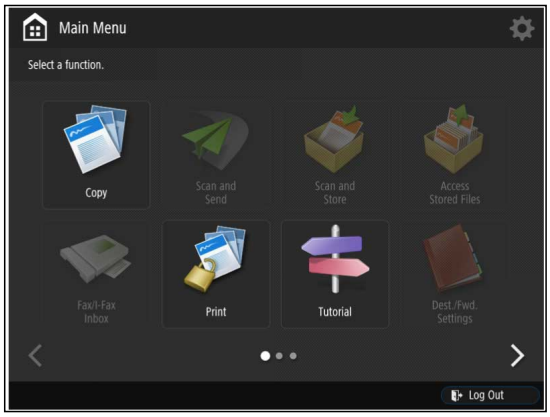
When the Access Management System setup is complete, user authentication is required when operating the touch panel display or printing from a computer.

If Using the Touch Panel Display <Device Level Log-in>:

When using the Access Management System with Device Level Log-in, if the Access Management System setup is complete, a Login screen is displayed on the touch panel display.

When [Log In] is pressed after entering a user name and password, user authentication is performed, and only the functions which that user can use become available on the touch panel display.

When an unregistered user is using the device and they press [Log In (Guest)] without entering a user name and password, only the functions that are not restricted become available on the touch panel display.



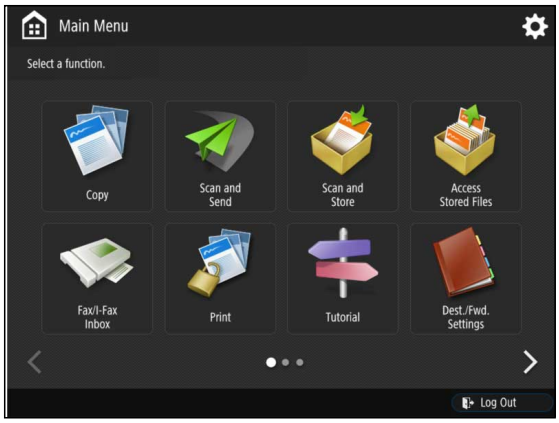
Since the [Settings/Registration] screen of the device can also be restricted, you can limit which users can change the settings of the device.

IMPORTANT

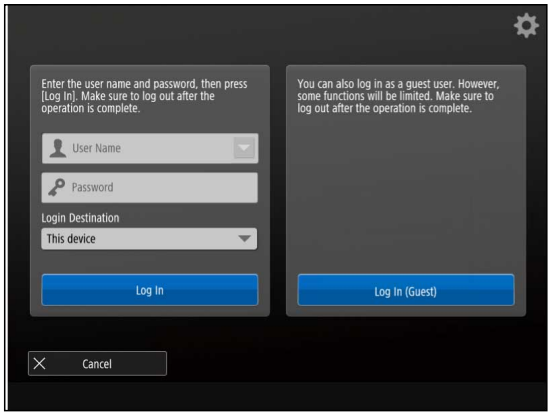
- To effectively use the Access Management System, make sure that users log out from the device when they finish using it by pressing (ID) (Log In/Out) or Log Out (Log Out) on the touch panel display.

If Using the Touch Panel Display<Function Level Log-in>:

When using the Access Management System with Function Level Log-in, if the Access Management System setup is complete, the [Main Menu] screen is displayed on the touch panel display.



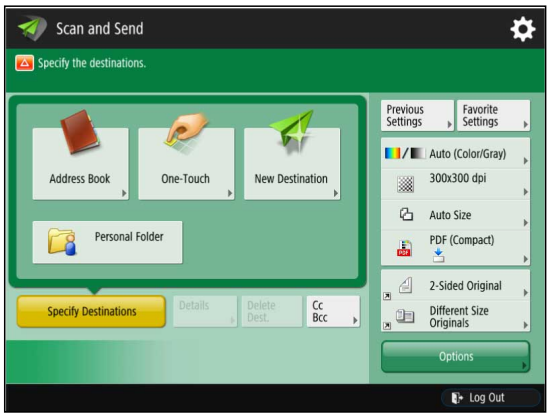
If you press the button for a function with authentication set, a login screen is displayed.



When [Log In] is pressed after entering a user name and password, user authentication is performed, and the screen for specifying detailed settings for the function is displayed on the touch panel display, only if the user is allowed to use that function.

NOTE

- If unregistered users have usage privileges, the [Log In (Guest)] button is displayed. The usage privileges for unregistered users depend on the settings of the guest role ([GuestUser]).



Since the [Settings/Registration] screen of the device can also be restricted, you can limit which users can change the settings of the device.

IMPORTANT

- To effectively use the Access Management System, make sure that users log out from the device when they finish using it by pressing (ID) (Log In/Out) or Log Out (Log Out) on the touch panel display.

If Printing from a Computer:

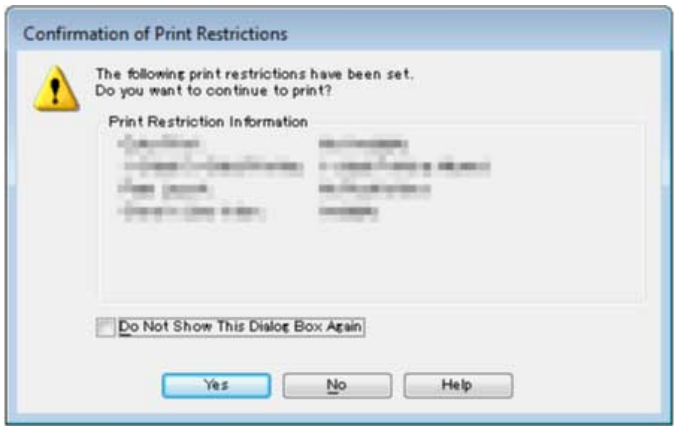
To restrict printing from computers, you must:

1. Set up the Access Management System.

2. Set up (enable the AMS function of the printer driver and set user information for) all client computers that use the device.

If the client computers have been set up, the [Confirm Password for Authentication] dialog box is displayed when users print from a computer.

When [OK] is pressed after entering a password, user authentication is performed, and the restricted printing functions are displayed.

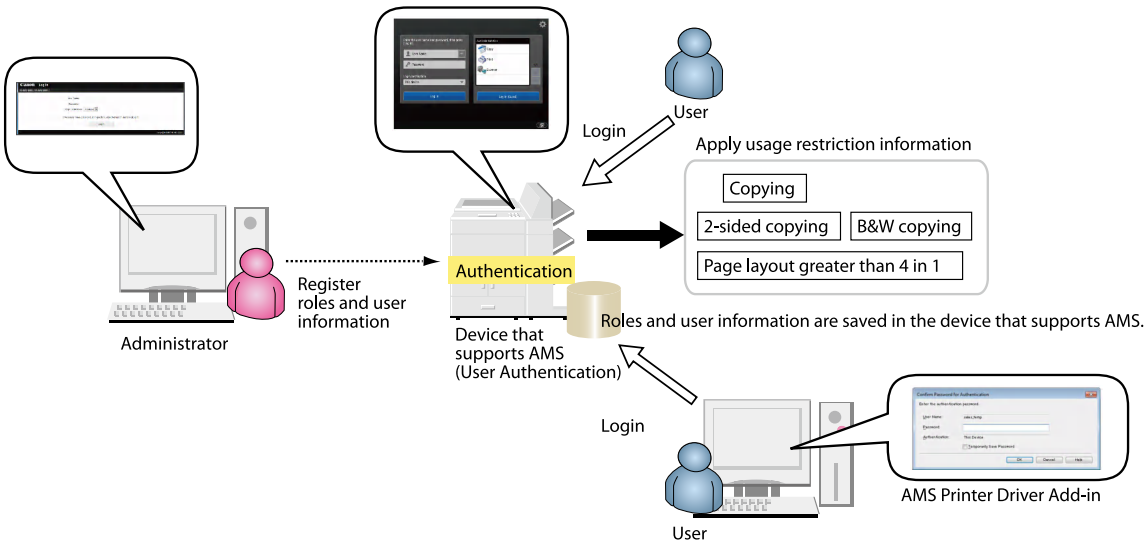


User Authentication Methods and Managed Users

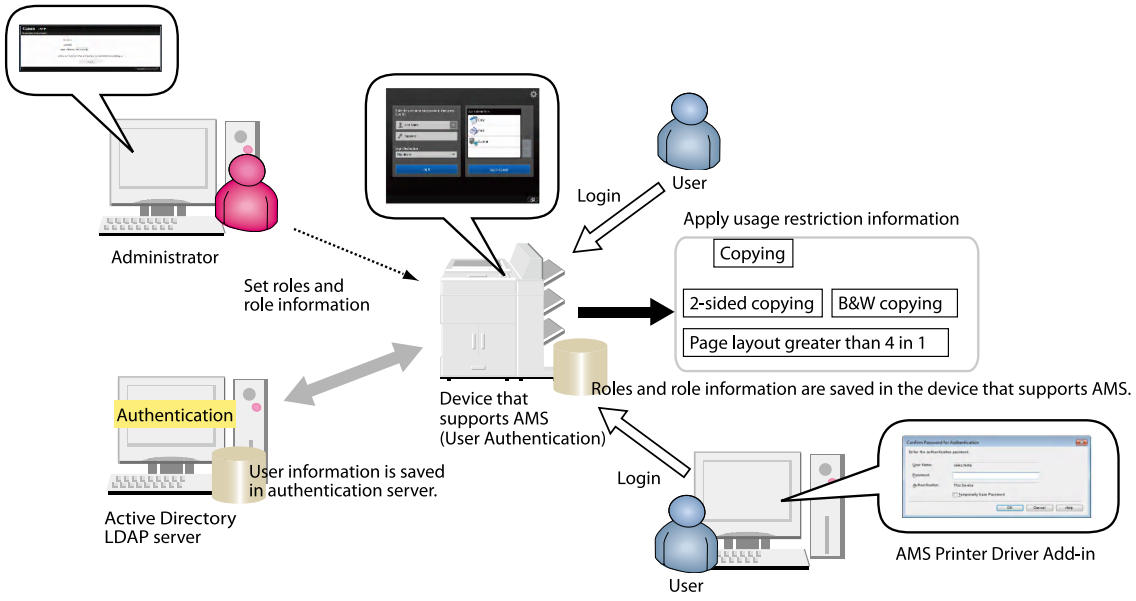
Devices to manage with the Access Management System have the following three user authentication methods, and each method manages different types of users.

User Authentication Method	Description
Local Device Authentication	Performs user information management and user authentication at the device. When a user enters a user name and password on a device, user authentication is performed based on local user information registered in the device.
Local Device Authentication + Active Directory Authentication, or Local Device Authentication + LDAP Authentication	These user authentication methods support both server authentication/local device authentication for Active Directory authentication and local device authentication or LDAP authentication and local device authentication. For example, this can enable you to manage users registered in the authentication server (such as regular employees) using Active Directory authentication/LDAP authentication, and temporary users (such as contract employees) using local device authentication. As this user authentication method also enables you to use devices with local device authentication when you cannot access the authentication server for a reason such as network trouble, it is recommended that you operate the Access Management System using these methods. LDAP authentication uses user information registered on an LDAP server to authenticate users.

Local Device Authentication Method



Active Directory Authentication/LDAP Authentication



NOTE

- When using Local Device Authentication + Active Directory Authentication, or Local Device Authentication + LDAP Authentication, the location for authentication differs according to the type of user that logs in.

Structure of Usage Restrictions

In the Access Management System, device usage restriction information is managed in units called "roles." Roles enable you to set which functions of a device are allowed to be used.

When operating with local device authentication, use User Authentication via a Web browser to set individual roles for each user of each device.

When operating with server authentication, create role and user association information.

Regarding Base Roles and Custom Roles

There are two types of roles for setting device restriction information: "Base Roles" and "Custom Roles."

"Base Roles" refer to roles provided by the Access Management System, which have usage restriction information (device management privileges and device function restriction) set by default.

"Custom Roles" refer to original roles created based on the above base roles. You can edit the device function usage restriction information according to your office environment. The device management privileges are determined by the [Base Role] setting, but the [Device Management Restriction] setting takes preference for Canon multifunction printers.

"Custom Role (Administrator)" is a custom role based on the [Administrator] role with [Device Management Restriction] already set, to enable easy management of Canon multifunction printers.

The following types of base roles and custom roles (administrator) are available. A summary of the device function restrictions and device management privileges they have are indicated below.

IMPORTANT

- The device can be managed with device management privileges from the remote UI, and from the control panel of the device. For devices using the AMS, only users who have been assigned the [Administrator]/[DeviceAdmin]/[NetworkAdmin] role (or a custom role with the same settings as this role) have device management privileges to access the screen for managing the device from the remote UI. The operations possible when using the control panel to manage the device are indicated below.
- For base roles and custom roles (administrator), you cannot edit the device function restrictions and device management privileges. You also cannot set application restrictions or button restrictions.
- For the [GuestUser] role, you can edit the device function restrictions and set application restrictions and button restrictions. However, you cannot edit the device management privileges.

NOTE

- "Device applications" refer to functions that are not included in the device, but are made available by installing them (such as MEAP applications).

Role Name	Device Function Restrictions	Device Management Privileges
[Administrator]	All functions are available.	The following keys cannot be used on the [Settings/Registration] screen: • Register Remote Device for Cascade Copy (Function Settings) • Limit New Destinations (Function Settings) • Always Add Device Signature to Send (Function Settings) • Address Book PIN (Set Destination)
[PowerUser]	All functions are available.	The following keys cannot be used on the [Settings/Registration] screen, in addition to the restrictions applied when the AMS is not used: • Register Remote Device for Cascade Copy (Function Settings) • Limit New Destinations (Function Settings) • Always Add Device Signature to Send (Function Settings)

Role Name	Device Function Restrictions	Device Management Privileges
		• Address Book PIN (Set Destination) • Output Report (Function Settings) • Key and Certificate List for Certificate Settings (Management Settings)
[GeneralUser]	All functions can be used except for address books and specifying destination domains.	The following keys cannot be used on the [Settings/Registration] screen, in addition to the restrictions applied when the AMS is not used: • Register Remote Device for Cascade Copy (Function Settings) • Limit New Destinations (Function Settings) • Always Add Device Signature to Send (Function Settings) • Set Destination • Output Report (Function Settings) • Key and Certificate List for Certificate Settings (Management Settings)
[LimitedUser]	Only the Copy function and Print function can be used. However, there are restrictions on color output, one-sided output, page layout, and saving to user inboxes. The Scan function, Store function (outputting user inbox documents), and Send function cannot be used.	No keys can be used on the [Settings/Registration] screen.
[GuestUser] (guest role)	The Copy function can be used. However, there are restrictions on color output, one-sided output, page layout, and saving to user inboxes. The Scan function, Store function (outputting user inbox documents), Send function, and Print function cannot be used. Application restrictions can be set. Depending on the model of the device, you can set usage restrictions for each button on the [Main Menu] screen.	No keys can be used on the [Settings/Registration] screen.
[NetworkAdmin] (custom role (administrator))	All functions are available.	The following keys cannot be used on the [Settings/Registration] screen, in addition to the restrictions applied when the AMS is not used: • Register Remote Device for Cascade Copy (Function Settings) • Limit New Destinations (Function Settings) • Always Add Device Signature to Send (Function Settings) • Address Book PIN (Set Destination)
[DeviceAdmin] (custom role (administrator))	All functions are available.	The following keys cannot be used on the [Settings/Registration] screen, in addition to the restrictions applied when the AMS is not used:

Role Name	Device Function Restrictions	Device Management Privileges
		• Register Remote Device for Cascade Copy (Function Settings) • Limit New Destinations (Function Settings) • Always Add Device Signature to Send (Function Settings) • Address Book PIN (Set Destination)

IMPORTANT

- If you use User Authentication as the login application when the AMS is not used, the [Settings/Registration] screen is restricted for general users (users set with a role other than [Administrator]/[DeviceAdmin]/[NetworkAdmin]). Even for administrator users, the [Settings/Registration] screen is restricted according to the device management privileges ([DeviceAdmin]/[NetworkAdmin]). When the AMS is used, the above restrictions are applied in addition to the restrictions applied when the AMS is not used.

NOTE

- Depending on your device, some restrictions may not be supported.

Device Management Privileges

For devices operating the Access Management System, the display and operation of the following screens related to device management are restricted according to the role associated with the user.

- [Status Monitor/Cancel] screen
- [Settings/Registration] screen

IMPORTANT

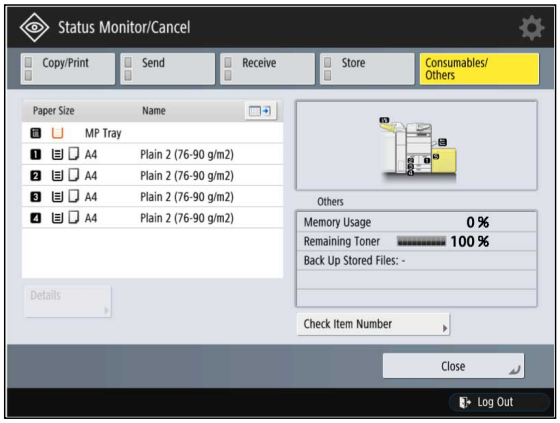
- For devices using the AMS, only users who have been assigned the [Administrator]/[DeviceAdmin]/[NetworkAdmin] role (or a custom role with the same settings as this role) have device management privileges to access the screen for managing the device from the remote UI. The operations possible when using the control panel to manage the device are indicated below.

Restrictions on the [Status Monitor/Cancel] Screen

The [Status Monitor/Cancel] screen is displayed when you press (Status Monitor/Cancel) on the touch panel display of the device. When operating the Access Management System, the device status can be checked on the [Status Monitor/Cancel] screen without logging in to the device, but the copy and send/receive status cannot be checked.

NOTE

- For more information on the [Status Monitor/Cancel] screen, see the instruction manuals of the device.



When a user with device management privileges (a user associated with the [Administrator] role or associated with a custom role based on the [Administrator] role, including the [DeviceAdmin] and [NetworkAdmin] roles) logs in, they can view/operate the job status and history.

When a user without device management privileges logs in, they can view/operate the status and logs of their own jobs, but the following restrictions are applied to jobs of other users.

[Status Monitor/Cancel] screen				Users with device management privileges	Users without device management privileges
[Copy/Print]	[Job Status]	[Print]	[Print Next]	Available	Unavailable
			[Details]		

[Status Monitor/Cancel] screen				Users with device management privileges	Users without device management privileges
			[Stop]		
			[Secured Print]		
			Names of jobs	Displayed	Displayed as "***"
		[Copy]	[Details]	Available	Unavailable
			[Stop]		
[Send]	[Job Status]	[Send]	[Details]	Available	Unavailable
			[Stop]		
			Destinations	Displayed	Displayed as "***"
		[Fax]	[Details]	Available	Unavailable
			[Stop]		
			Destinations	Displayed	Displayed as "***"
[Receive]	[Job Status]	[Forward]	[Details]	Available	Unavailable
			[Check I-Fax RX]		
		[Fax]	[Details]		
			[Stop]		
[Store]	[Job Status]	-	[Details]	Available	Unavailable
			[Stop]		
			Destinations	Displayed	Displayed as "***"
Other keys				Available	Available
Other displayed items				Displayed	Displayed

Restrictions on [Settings/Registration]

If you enable the AMS, the following items in [Settings/Registration] become unavailable. These settings will not be displayed.

IMPORTANT

- If you enable the AMS, the settings for [Limit New Destinations] and [Address Book PIN] are disabled. Even if you disable the AMS, the settings in [Limit New Destinations] and [Address Book PIN] will not automatically return to the original configuration. It is necessary to configure the settings again.

[Settings/Registration] screen			
[Function Settings]	[Copy]	[Register Remote Device for Cascade Copy]	
	[Send]	[Common Settings]	[Limit New Destinations]*1

<table>
<tr><th colspan="4">[Settings/Registration] screen</th></tr>
<tr><td rowspan="5"></td><td rowspan="4"></td><td rowspan="4"></td><td>[Allow Sending with Expired Certificate]</td></tr>
<tr><td>[Always Add Device Signature to Send]*2</td></tr>
<tr><td>[Limit E-Mail to Send to Myself]*4</td></tr>
<tr><td>[Restrict File TX to Personal Folder]*4</td></tr>
<tr><td>[Store/Access Files]</td><td colspan="2">[Memory Media Settings]</td></tr>
<tr><td>[Set Destination]</td><td colspan="3">[Address Book PIN]*3</td></tr>
</table>

*1: Can be restricted for each user in the [Send to New Addresses] restricted item inside the role.
*2: Can be restricted for each user in the [Add Device Signature to Sending Files] restricted item inside the role.
*3: Address book usage can be restricted for each user in the [Use Address Book/Register Storage Location for Network] restricted item inside the role.
*4: Depending on the model of the device, this item may not be displayed.

IMPORTANT

- When functions on the [Settings/Registration] screen are restricted, shortcuts to those functions cannot be used.
- If the Scan function is restricted in the [Scan] restricted item inside a role, [Function Settings] → [Common] → [Print Settings] → [Register Form] cannot be used.
- If address book usage is set to [Not Allowed] in the [Use Address Book/Register Storage Location for Network] restricted item inside a role, [Set Destination] → [Address Lists]/[Register Destinations]/[Rename Address List]/[Register One-Touch]/[Change Default Display of Address Book] cannot be used.
  If address book usage is set to [Read-Only], [Set Destination] → [Register Destinations]/[Rename Address List]/[Register One-Touch]/[Change Default Display of Address Book] cannot be used.

Device Function Restrictions

The device function restrictions for base roles are set as indicated below. For custom roles, the settings for the following items can be changed.

- **[Function Category Restriction](P. 26)**
- **[Function Category Restriction Details](P. 27)**
- **[Application Restrictions](P. 31)**
- **[Button Restrictions](P. 32)**

IMPORTANT

- You can change the device restriction settings for the guest role ([GuestUser]). You cannot change device restriction settings for custom roles (administrator) ([DeviceAdmin] and [NetworkAdmin]).

[Function Category Restriction]

Sets device function restrictions by category.

IMPORTANT

- The settings in [Application Restrictions] take preference over the settings here.

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
Print Functions	Allowed	✓	✓	✓	✓	✓
	Not Allowed					
Save Functions (Mail Box/Hold/ Memory Media)	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Copy Functions	Allowed	✓	✓	✓	✓	✓
	Not Allowed					
Send Functions/Store on Network	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Web Access Function	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Utility Function	Allowed	✓	✓	✓		

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
	Not Allowed				✓	✓
Others Functions	Allowed	✓	✓	✓		
	Not Allowed				✓	✓

[Function Category Restriction Details]

Sets detailed restrictions for the device functions set to [Function Category Restriction] and [Application Restrictions] and the device functions that have not yet been set.

NOTE

- Depending on your device, some restrictions may not be supported.

Print Functions

Sets restrictions for outputting documents (printing or saving to user inboxes) from computers.

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
Print	Allowed	✓	✓	✓	✓	✓
	Not Allowed					
Color Print	Allowed	✓	✓	✓		
	Only Allowed with Black and White Printing				✓	✓
1-Sided/2-Sided Printing	No Restrictions	✓	✓	✓		
	2-Sided Printing Only				✓	✓
Page Layout	No Restrictions	✓	✓	✓		
	1 on 1 Not Available					
	1-2 on 1 Not Available				✓	✓
Save to Mail Box	Allowed	✓	✓	✓		
	Not Allowed				✓	✓

IMPORTANT

- Depending on the model of the device, the firmware may have to be upgraded in order to use the Save to Mail Box function. For information on whether the firmware of your device needs upgrading, contact your local authorized Canon dealer.

Save Functions (Mail Box/Memory Media)

Sets restrictions for printing user inbox documents.

IMPORTANT

- This item/settings can only restrict the output of the box documents by MEAP application. It cannot restrict the output of the box documents using the functions of anything other than MEAP application. For example, AMS cannot restrict printing documents in the USB memory that is connected to the device.

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
Print	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Color Print	No Restrictions	✓	✓	✓		
	Full-Color Printing Not Allowed					
	Full-Color/Two Colors Printing Not Allowed					
	Only Allowed with Black and White Printing				✓	✓
1-Sided/2-Sided Printing	No Restrictions	✓	✓	✓		
	2-Sided Printing Only				✓	✓
Page Layout	No Restrictions	✓	✓	✓		
	1 on 1 Not Available					
	1-2 on 1 Not Available				✓	✓

Save Function (Memory Media)

Sets input/output restrictions for documents to save to memory media.

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
Memory Media	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Scan	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Print	Allowed	✓	✓	✓		
	Not Allowed				✓	✓

Copy Functions

Sets restrictions for printing scanned documents.

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
Color Copy	No Restrictions	✓	✓	✓		
	Full-Color Copying Not Allowed					
	Full-Color/Two Colors Copying Not Allowed					
	Only Allowed with Black and White Copying				✓	✓
1-Sided/2-Sided Copying	No Restrictions	✓	✓	✓		
	2-Sided Copying Only				✓	✓
Page Layout	No Restrictions	✓	✓	✓		
	1 on 1 Not Available					
	1-2 on 1 Not Available				✓	✓

Scan Functions

Sets restrictions for the Scan function.

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
Scan	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Color Scan	Allowed	✓	✓	✓		
	Not Allowed				✓	✓

Send Functions/Store on Network

Sets restrictions for outputting (sending externally) scanned documents and user inbox documents. These restrictions also apply to saving documents to file servers and network storage.

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
E-Mail TX	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
E-Mail TX (Use [Send to Myself])	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
I-Fax TX	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Fax TX	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
FTP TX	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Windows (SMB) TX	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Use [Personal Folder]	Sets output restrictions (output destination :Personal Folder) for scanned documents and user inbox documents.					
	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
WebDAV TX	Allowed	✓	✓	✓		

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
	Not Allowed				✓	✓
Mail Box TX	Sets restrictions for saving scanned documents to user inboxes.					
	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Specify Address Domain	Allowed	✓	✓			
	Not Allowed			✓	✓	✓
Use Address Book/Register Storage Location for Network	These restrictions also apply to registering/editing/deleting network storage. For device models installed with User Authentication, this also applies to usage restrictions for the Address Book (Address List management function) provided on the Remote UI.					
	No Restrictions	✓	✓			
	Not Allowed				✓	✓
	Read-Only			✓		
Use Personal Address List	Sets restrictions for using Personal Address List.					
	Allowed	✓	✓			
	Not Allowed			✓	✓	✓
Send to New Addresses	Allowed	✓	✓	✓		
	Not Allowed				✓	✓
Add Device Signature to Sending Files	Allows or prohibits adding of a device signature when sending PDF files.					
	Added				✓	✓
	Not Added	✓	✓	✓		
Sending Files Format	Allows or prohibits sending file formats that a device signature cannot be added to.					
	No Restrictions	✓	✓	✓		
	Restrictions				✓	✓

[Application Restrictions]

With the Access Management System, you can set restrictions by application ([Application Restrictions]) in addition to setting restrictions by function ([Function Category Restriction] and [Function Category Restriction Details]).

When [Application Restrictions] is set, restrictions are applied according to those settings, but when it is not set, restrictions are applied according to the settings in [Function Category Restriction] and [Function Category Restriction Details] for the function category that the application belongs to. Applications that do not belong to any function categories are restricted according to the settings in [Others Functions] in [Function Category Restriction].

The basic applications belong to the function categories indicated below.

Basic Applications	Category
Web Access	[Web Access Function] category
Copy	[Copy Functions] category
Scan and Send/Fax	[Send Functions/Store on Network] category
Print/Secured Print	[Print Functions] category
Hold	[Save Functions (Mail Box/Hold/Memory Media)] category
Mobile Print	[Print Functions] category
Access Stored Files	[Save Functions (Mail Box/Hold/Memory Media)] category

IMPORTANT

- The settings in [Application Restrictions] take preference over the settings in [Function Category Restriction].
- Since application restrictions cannot be set for base roles and custom roles (administrator), all applications are restricted according to the settings in [Function Category Restriction] and [Function Category Restriction Details] for the function category the application belongs to.

[Button Restrictions]

You can set usage restrictions for buttons on the [Main Menu] screen and [Quick Menu] screen on models that have User Authentication.

However, since some functions provided by applications are registered in buttons, you cannot use functions set to [Not Allowed] in [Application Restrictions], regardless of whether they are not restricted in [Button Restrictions].

Usage restrictions can be set with the following basic application buttons.

Button/Applet Name	Application Name
Copy	Copy
Fax	Scan and Send
Scan and Send	Scan and Send
Scan and Store	Access Stored Files
Access Stored Files	Access Stored Files
Fax/I-Fax Inbox	Access Stored Files
Secured Print	Secured Print
Web Access	Web Access

Button/Applet Name	Application Name
Scanner	Scan

IMPORTANT

- Since button restrictions cannot be set for base roles and custom roles (administrator), all buttons are restricted according to the settings in [Function Category Restriction] and [Function Category Restriction Details] for the application that the button belongs to.

Access Management System Configurations

The Access Management System is comprised of the following software.

Software	Description
User Authentication	A login application that supports the AMS and operates on the device. It retains role information, and executes device restrictions according to the role information associated with each user. It also provides the login service selectable for the user authentication method. For the local device authentication method, it also retains user information and performs user authentication.
Access Management System Printer Driver Add-in (AMS Printer Driver Add-in)	This is add-in software for restricting printing from computers according to the role information retrieved from the User Authentication. To enable the AMS Printer Driver Add-in, you must install a supported printer driver to the computer in advance.

IMPORTANT

- If any of the following conditions apply, you can restrict the use of color printing, one-sided printing, and storing to the inbox without enabling the AMS Printer Driver Add-in.

Condition 1

- Local device authentication is used.*1
- Either of the following printer drivers is used on the client computer.

Canon UFR II Printer Driver V21.50 or later

Canon UFR II V4 Printer Driver V5.10 or later *2
Canon PCL6 Printer Driver V21.50 or later
Canon PCL5e/5c Printer Driver V21.50 or later
Canon PS3 Printer Driver V21.50 or later

- The [Remote job without user authentication] restriction is enabled on the device.
- [User Authentication Settings] is specified in the printer driver.

*1 If you are using server authentication, you must enable the AMS Printer Driver Add-in to restrict users from printing.

*2 Not available in some regions.

Condition 2

- Either device authentication or function-specific authentication is used, and user authentication is specified for [Print].
- [Settings/Registration] → [Function Settings] → [Print] → [Forced Hold] is set to ON.

- If you are using server authentication, you must enable the AMS Printer Driver Add-in to restrict users from printing.
- To set restrictions for page layouts when a user prints from a computer, you must enable the AMS Printer Driver Add-in.
- For information on the [Remote job without user authentication] restriction, see " **Setting Usage Restrictions for Remote Scanning/Cascade Copy(P. 58)** ."
- For more information on the printer drivers, see the instruction manuals for the printer drivers.

Administrators for the Access Management System

Administrators with the privileges indicated below are required for the operation of the Access Management System. You can also assign all of the required privileges to a single administrator.

Operating with Local Device Authentication(P. 35)
Operating with LDAP authentication(P. 35)
Operating with central management configuration using Active Directory authentication(P. 36)

Operating with Local Device Authentication

Type of Administrator	Function	Required Privileges
Device administrator	• Configuring of the Access Management System • Managing restricted devices - Date/time settings - Network settings - Registering the System Manager ID - Starting User Authentication • Selecting the device restriction administrator	Able to log in to SMS (Service Management Service) However, the [Administrator] role must be associated with the administrator after starting to operate the Access Management System.
Device restriction administrator	• Specifying the Preferences of the device • Security settings • User management • Role management • Associating roles and users	• Associated with the [Administrator] role
Client computer administrator	• Installing and updating printer drivers to client computers • Enabling the AMS function of the printer drivers installed to the client computers	Administrator privileges for Windows used in the client computers

Operating with LDAP authentication

Type of Administrator	Function	Required Privileges
Device administrator	• Configuring of the Access Management System • Managing restricted devices - Date/time settings - Network settings - Registering the System Manager ID - Starting User Authentication • Selecting the device restriction administrator	Able to log in to SMS (Service Management Service) However, [Administrator] role must be associated with the administrator after starting to operate the Access Management System.
Device restriction administrator	• Specifying the Preferences of the device (default role settings) • Security settings • User Management • Managing guest roles	Associated with the [Administrator] role

Type of Administrator	Function	Required Privileges
Client computer administrator	• Installing and updating printer drivers to client computers • Enabling the AMS function of the printer drivers installed to the client computers	Administrator privileges for Windows used in the client computers

Operating with central management configuration using Active Directory authentication

Type of Administrator	Function	Required Privileges
Device administrator	• Configuring of the Access Management System • Managing restricted devices - Date/time settings - Network settings - Registering the System Manager ID - Starting User Authentication • Selecting the device restriction administrator	Able to log in to SMS (Service Management Service) However, the [Administrator] role must be associated with the administrator after starting to operate the Access Management System.
Company network administrator	• DNS server settings • Trusted domain settings • Creating a user group in Active Directory and adding users to the user group	• Administrator privileges for the DNS server (when using multiple domains) • Administrator privileges for Active Directory
Device restriction administrator	• Specifying the Preferences of the device • Security settings • User management • Role management • Associating roles and users	• Associated with the [Administrator] role • Administrator privileges for Active Directory
Client computer administrator	• Installing and updating printer drivers to client computers • Enabling the AMS function of the printer drivers installed to the client computers	Administrator privileges for Windows used in the client computers

System Requirements

This section describes the system requirements for the Access Management System.

Supported Devices(P. 37)
Client Computer (AMS Printer Driver Add-in)(P. 37)

Supported Devices

The Access Management System supports devices (that support AMS) in which User Authentication is running, a license for the AMS has been registered, and AMS is enabled.

Client Computer (AMS Printer Driver Add-in)

To restrict users from printing from computers, you must enable the AMS Printer Driver Add-in in the printer driver of devices that support AMS. The system requirements for the client computer (computer to print from) are as follows.

Supported Printer Drivers

One of the following printer drivers must be installed in the computer in advance.

- Generic Plus UFR II Printer Driver V2.30 or later
- Generic Plus PS3 Printer Driver V2.30 or later
- Generic Plus PCL6 Printer Driver V2.30 or later

Supported Operating Systems

For information on the supported operating systems of the printer driver, see the instruction manuals of the printer driver.

Add-ins that can be Installed on the Same Computer

- Canon Encrypted Secured Print Driver Add-in for Client PC

IMPORTANT

- You cannot specify the user name in the dialog box that is displayed when printing by the Secured Print function of the printer driver or the Encrypted Secured Print Driver Add-in for Client PC. (If you are logged in as a user with Windows administrator privileges, you can specify the user name, but it is ignored.) Printing is executed using the user name displayed in [Current User Name] on the [AMS] page.

Setting Up the Access Management System

Setting Up the Access Management System

This section describes the procedure for setting up the Access Management System, including the procedures for preparing the devices to restrict and installing the various software.

Flow of Settings for Operating with Local Device Authentication

This section describes the flow of settings for operating the Access Management System with local device authentication.

IMPORTANT

- The steps that are required differ according to the system configuration. When operating with server authentication, see **"Flow of Settings for Operating with Server Authentication."(P. 42)**

1. Preparing the Device and Network Environment(P. 44)

Set the network environment and date/time settings, etc., of all devices to operate with the Access Management System, and register a System Manager ID in each device.

2. Enabling the AMS

Enable the AMS on all devices to operate with the Access Management System.

For more information, see the instruction manuals of the device.

3. Starting User Authentication

Start User Authentication in all devices that support AMS.

For more information, see the instruction manuals of the device.

4. Setting Security

Specify the security related settings, such as passwords and lockout policies.

For more information, see the instruction manuals of the device.

5. Specifying the Preferences of the Devices(P. 48)

Specify the preferences of all devices that support AMS.

- **Setting the User Authentication Method(P. 49)**
- **Setting the Default Role for Registered Users(P. 49)**
- **Role Association(P. 51)**
- **Setting the Login Method(P. 51)**
- **Allowing Unregistered Users to Log In(P. 51)**
- **Setting the Number of Users to Cache on the Login Screen(P. 52)**
- **Retaining User Authentication Information with the Printer Driver(P. 53)**
- **Prohibiting the Printing from Drivers without AMS Printer Driver Add-in(P. 54)**

Setting Remote Job Restrictions(P. 57)
Setting Usage Restrictions for Remote Scanning/Cascade Copy(P. 58)
Adding a Device Signature When Forwarding Files(P. 59)
Configuring IPP Printing(P. 60)

6. Managing Roles(P. 62)

Create/edit the custom roles and edit the guest roles, as necessary. Since roles can be imported/exported, they can be used in multiple devices.

Creating Custom Roles(P. 63)
Editing Custom Roles(P. 67)
Editing the [GuestUser] Role (Guest Role)(P. 68)
Deleting Custom Roles(P. 69)
Importing Roles(P. 70)
Exporting Roles(P. 72)

7.Managing Users

Register/edit the users that will use the device. Also register role names to apply to the user information. If a role name is not registered to a user, the role set in [Default Role] in the preferences of the devices is applied to that user. Since user information can be imported/exported, it can be used in multiple devices.

For more information, see the instruction manuals of the device.

Precautions When Operating with Local Device Authentication

This section describes precautions to take when operating the Access Management System with local device authentication.

Using the Access Management System in Conjunction with the Department ID Management Function

When using the Department ID Management function in conjunction with the Access Management System, start the Department ID Management function and register the Department IDs after the Access Management System setup (the above operations) is complete. For information on the Department ID Management function, see the instruction manuals of the device.

When using the Department ID Management function in conjunction with the Access Management System, the [Department ID] and [System PIN] registered in the user information must match the [Department ID] and [System PIN] registered in Department ID Management. If the information in Department ID Management changes due to device information delivery settings, etc., change the user information in accordance.

Restricting Printing from Computers

To restrict printing from computers, you must enable the AMS function of the printer drivers installed to the client computers, after you complete the above operations. For details, see the instruction manuals of the printer driver.

Flow of Settings for Operating with Server Authentication

This section describes the flow of settings for operating the Access Management System with server authentication.

IMPORTANT

- If you are using server Authentication, user information managed on the server is used, so managing users with the local device authentication method is unnecessary.
- The steps that are required differ according to the system configuration. When operating with local device authentication, see **"Flow of Settings for Operating with Local Device Authentication."(P. 40)**

1. Preparing the Device and Network Environment(P. 44)

Set the network environment and date/time settings, etc., of all devices to operate with the Access Management System, and register a System Manager ID in each device.

2. Enabling the AMS

Enable the AMS on all devices to operate with the Access Management System.

For more information, see the instruction manuals of the device.

3. Starting User Authentication

Start User Authentication in all devices that support AMS.

For more information, see the instruction manuals of the device.

4. Setting Security

Specify the security related settings, such as passwords and lockout policies.

For more information, see the instruction manuals of the device.

5. Specifying the Preferences of the Devices(P. 48)

Specify the preferences of all devices that support AMS.

- **Setting the User Authentication Method(P. 49)**
- **Setting the Default Role for Registered Users(P. 49)**
- **Role Association(P. 51)**
- **Setting the Login Method(P. 51)**
- **Allowing Unregistered Users to Log In(P. 51)**

Setting the Number of Users to Cache on the Login Screen(P. 52)
Retaining User Authentication Information with the Printer Driver(P. 53)
Prohibiting the Printing from Drivers without AMS Printer Driver Add-in(P. 54)
Setting Remote Job Restrictions(P. 57)
Setting Usage Restrictions for Remote Scanning/Cascade Copy(P. 58)
Adding a Device Signature When Forwarding Files(P. 59)
Configuring IPP Printing(P. 60)

6. Managing Roles(P. 62)

Create/edit the custom roles and edit the guest roles, as necessary. Since roles can be imported/exported, they can be used in multiple devices.

Creating Custom Roles(P. 63)
Editing Custom Roles(P. 67)
Editing the [GuestUser] Role (Guest Role)(P. 68)
Deleting Custom Roles(P. 69)
Importing Roles(P. 70)
Exporting Roles(P. 72)

Precautions When Operating with Server Authentication

This section describes precautions to take when operating the Access Management System with server authentication.

Setup Flow for Using Server Authentication in Conjunction with Local Device Authentication

It is recommended that you use the Access Management System in conjunction with local device authentication to prevent cases where you cannot access the server for a certain reason, such as network trouble.

To use local device authentication in conjunction with server authentication, perform steps 1 to 8 in **"Flow of Settings for Operating with Local Device Authentication"(P. 40)** and then perform step 6 in **"Flow of Settings for Operating with Server Authentication."(P. 42)**

If you have constructed an environment to use server authentication in conjunction with local device authentication, and if you use a device with the local device authentication method without creating local user information, all users will use the device as an unregistered user ([GuestUser]).

IMPORTANT

- If you are using User Authentication with server authentication, it cannot be used in conjunction with the Department ID Management function.

Restricting Printing from Computers

To restrict printing from computers, you must enable the AMS function of the printer drivers installed to the client computers, after you complete the above operations. For details, see the instruction manuals of the printer driver.

Preparing the Device and Network Environment

This section describes the procedure for specifying the settings for the devices to restrict and the network environment.

Setting the Date/Time

In the Access Management System, the date/time settings of all equipment that comprises the system (devices, client computers, server computers, etc.) need to match.

If you are using Canon multifunction printers, set the date and time correctly in [Date/Time Settings] in [Timer/Energy Settings] in [Preferences] on the [Settings/Registration] screen of the device.

For more information, see the instruction manuals of the device.

Specifying the Network Settings

To install the Access Management System, it is necessary to set the devices to be accessible from the network.

If you are using Canon multifunction printers, specify the various items in [Network] in [Preferences] on the [Settings/Registration] screen of the device.

For more information, see the instruction manuals of the device.

IMPORTANT

- If the device is already operating on the network (documents can already be printed or sent from a computer), this operation is not required.

Registering DNS Server

To use a device in a domain environment, it is necessary to register the DNS server to use on the device.

If you are using Canon multifunction printers, this can be set from [Network] in [Preferences] on the [Settings/Registration] screen of the device.

For more information, see the instruction manuals of the device.

IMPORTANT

- This operation is not required if the device is already being operated in a domain environment.

Making Devices Accessible from Web Browsers

To operate the Access Management System, it is necessary to set the devices to be accessible from Web browsers.

For more information, see the instruction manuals of the device.

IMPORTANT

- The devices cannot be connected to via a proxy server. If you are using a proxy server, add the IP address of the device to [Exceptions] (addresses to not use a proxy server for) in the proxy server settings of the Web browser (contact your company network administrator, as the required settings differ according to the network environment).
- This function cannot be used unless Cookies, JavaScript, and JavaApplet are enabled in the Web browser.
- When entering characters from a Web browser, only use characters that can be entered from the touch panel display of the device. If you use other characters, the device may not display/recognize them correctly.

Registering the System Manager ID

To restrict device usage properly in the Access Management System, it is necessary to register the System Manager ID in advance.

If you are using Canon multifunction printers, set the System Manager ID in [System Manager Information Settings] for [User Management] in [Management Settings] on the [Settings/Registration] screen of the device.

For more information, see the instruction manuals of the device.

IMPORTANT

- The user can use the system management functions allowed for the [Administrator]/[DeviceAdmin]/[NetworkAdmin] role without knowing the System Manager ID and System PIN.

Setting the LDAP Server

If you are using the LDAP authentication method, set the LDAP server information in User Authentication. For more information, see the instruction manuals of the device.

Setting the DNS Server

When operating the device in a multi-domain environment, set the DNS server to ensure the following. For details on setting the DNS server, see the documentation for the DNS server.

- Name resolution can be performed with the DNS domain name of the Active Directory used for authentication (IP address of the domain controller can be retrieved)
- The DNS server supports SRV records

If the port number for the LDAP port has been changed on the Active Directory side, the following settings are also required.

- The information for the LDAP service of Active Directory is registered as an SRV record as follows:
  - Service: '_ldap'

- Protocol: '_tcp'
- Port number: port number actually used by the LDAP service of the Active Directory domain (zone)
- Host provided by this service: host name of the domain controller actually provided by the LDAP service of the Active Directory domain (zone)

IMPORTANT

- This operation is not required if the device is already being operated in a multi-domain environment.

Setting the Domain Trust Relationships

With the Access Management System, you can restrict devices that belong to domains trusted by the domain in which the user belongs to.

When operating the Access Management System with the Active Directory authentication, if the domain that the user belongs to and the domain that a device belongs to differ, it is necessary to set a bilateral trusted relationship between the domains.

IMPORTANT

- This operation is not required if you are operating the Access Management System using authentication method other than Active Directory authentication.
- You cannot restrict devices that belong to a domain other than the domain the user belongs to with trusted relationships that occur due to the hierarchical structure of Active Directory. Set direct trusted relationships.

Logging in to User Authentication

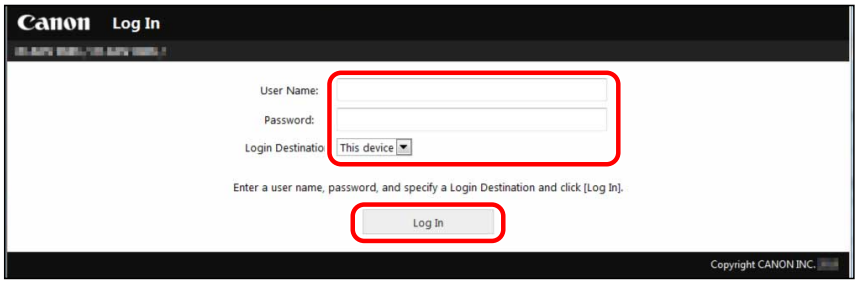
To manage roles and users and specify the preferences of the devices, log in to User Authentication.

1 Open your Web browser → enter the following URL:

http://<IP address or host name of the device>

The [Login] page is displayed.

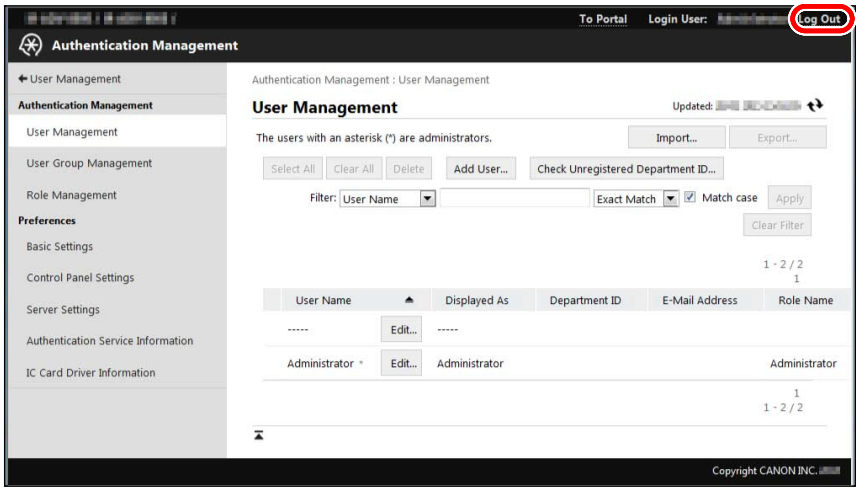
2 Enter the user name and password of a user associated with the [Administrator] role → select [This device] in [Login Destination] → click [Log In].



NOTE

- If your device has two-factor authentication enabled, click [Login] and enter the one-time password. For more information, see the instruction manuals of the device.

3 When you have finished performing operations, click [Log Out].



Specifying the Preferences of the Devices

This section describes the procedure for specifying the preferences of the devices when operating the Access Management System.

Specifying the Device Preferences Using User Authentication(P. 49)

IMPORTANT

- Only users with the [Administrator] role can set the preferences of the device. (Users associated with a custom role based on the [Administrator] role (such as the [DeviceAdmin] or [NetworkAdmin] role) cannot specify the preferences of the devices.)
- Depending on the user authentication method you are using, the items that must be set will differ. For more information, see **"Flow of Settings for Operating with Local Device Authentication"(P. 40)** or **"Flow of Settings for Operating with Server Authentication."(P. 42)**

Specifying the Device Preferences Using User Authentication

This section describes the procedure for specifying the preferences of the device using User Authentication.

Setting the User Authentication Method

Specify the user authentication method. For more information, see the instruction manuals of the device.

Setting the Default Role for Registered Users

If you are using local device authentication, select the base role to apply to users that are not associated with a role (users that do not have a role name written in their user information) when they log in to a device.

For more information on the usage restrictions for each base role, see **"Regarding Base Roles and Custom Roles."(P. 20)**

IMPORTANT

- Since application restrictions and button restrictions cannot be set for base roles, application restrictions and button restrictions cannot be set for users that have the role specified in [Set Default Role] applied to them. It is necessary to create a suitable custom role and associate that role with users that you want to restrict applications and buttons for.

1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

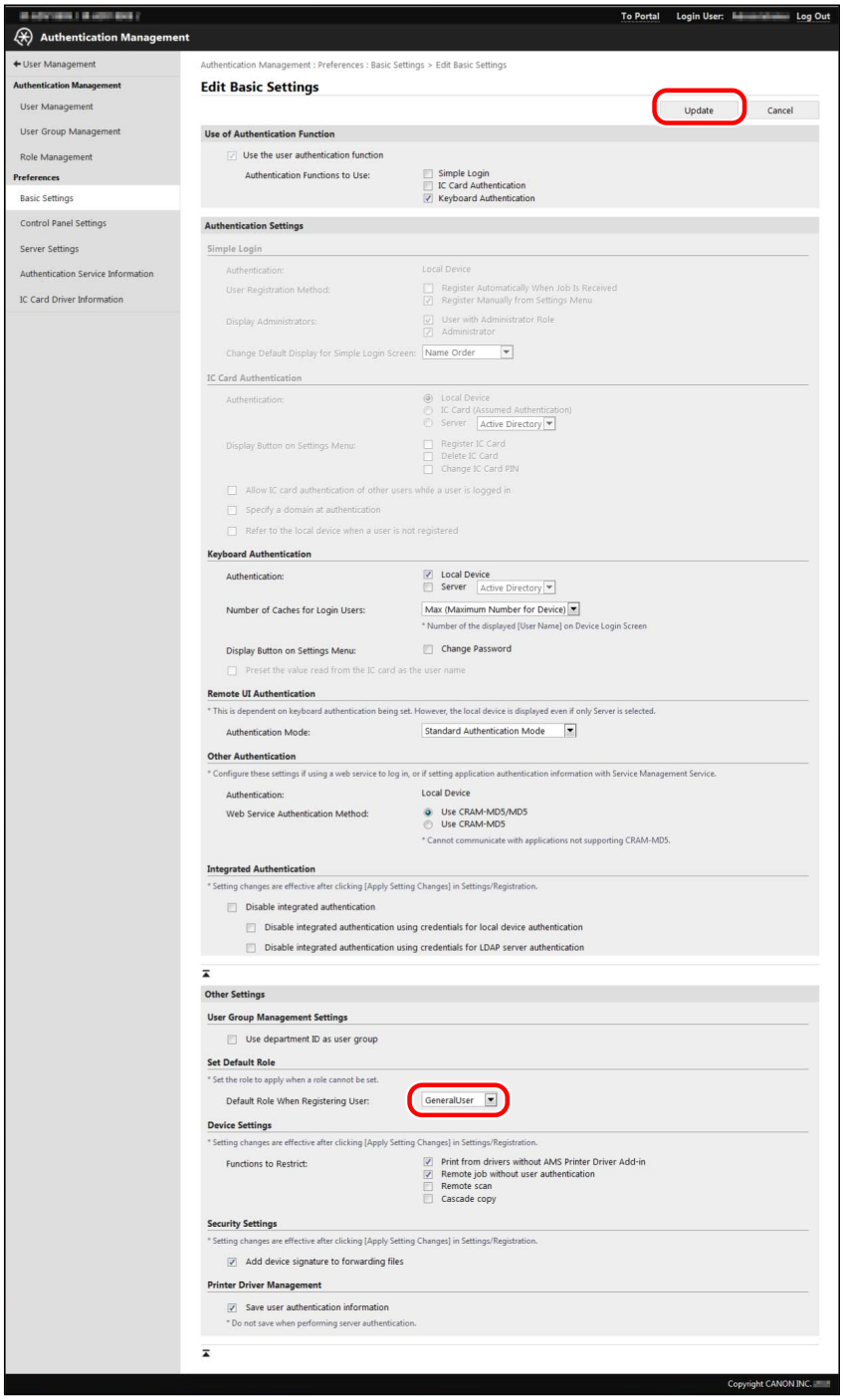
2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Basic Settings].

3 Click [Edit].

4 In [Default Role When Registering User] in [Set Default Role], select a role → click [Update].

If you are using the local device authentication method, roles selected here are assigned to users who do not have role names written in their user information.

When using server authentication method, the role selected here is applied to all users authenticated based on the user information registered in the server that do not match the role association conditions.



IMPORTANT

- The [Set Default Role] setting is enabled after the device is restarted. For information on restarting the device, see the instruction manuals of the device.

Role Association

When using server authentication, set the role to apply to server authentication users in [Role Association]. For more information, see the instruction manuals of the device.

Setting the Login Method

Specify the timing to display the login screen for user authentication. There are two types of login methods; "Device Level Log-in" and "Function Level Log-in." For more information, see the instruction manuals of the device.

IMPORTANT

- If you select Function Level Log-in, take particular care when creating/editing custom roles and editing the guest role so that the restrictions applied to registered users are not more strict than those applied to unregistered users. If the restrictions applied to registered users are stricter than those applied to unregistered users, the number of functions that can be used after logging in will be less than before logging in, which may lead to inappropriate user management.

Allowing Unregistered Users to Log In

You can set whether to allow unregistered users to log in to a device.

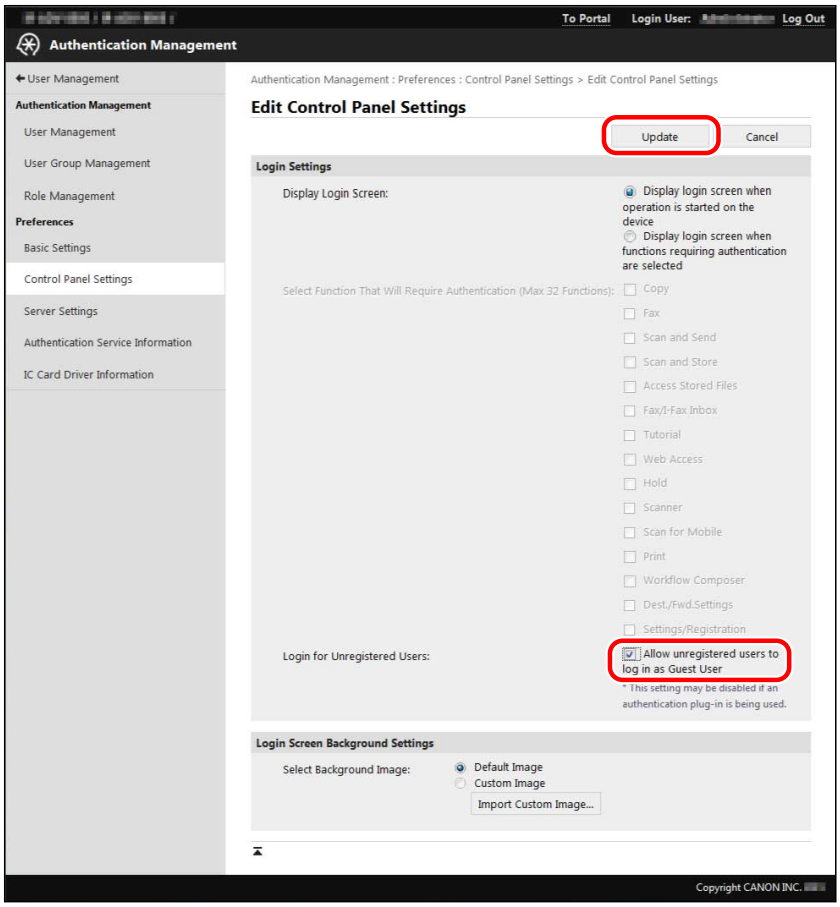
1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Control Panel Settings].

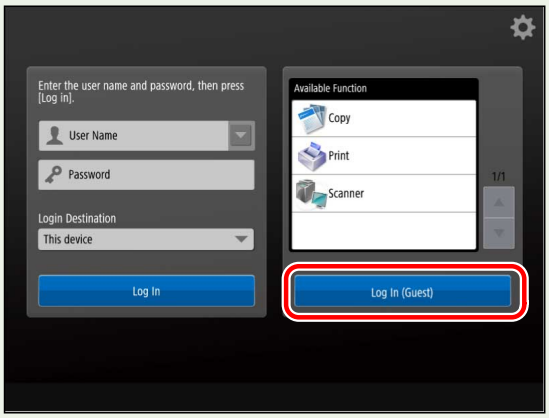
3 Click [Edit].

4 Select [Allow unregistered users to log in as Guest User] in [Login for Unregistered Users] → click [Update].



NOTE

- The [GuestUser] role (guest role) can be edited. For more information, see **"Editing the [GuestUser] Role (Guest Role)."(P. 68)**
- If you select [Allow unregistered users to log in as Guest User] when Device Level Log-in is selected as the login method, a login screen similar to the following is displayed on the touch panel display of the device. When unregistered users log in, they press [Log In (Guest)], without entering a user name and password. The functions that unregistered users can use are set in the usage restriction information of the [GuestUser] role.



Setting the Number of Users to Cache on the Login Screen

Set the number of users to cache on the login screen displayed on the touch panel display when logging in. This enables you to select a user name that has been previously used to log in, to save you having to enter it.

NOTE

- For more information, see the instruction manuals of the device.

Retaining User Authentication Information with the Printer Driver

You can set whether to allow users to retain the password entered in the AMS Printer Driver Add-in. If you retain the password, it becomes unnecessary to enter a password in the AMS Printer Driver Add-in after the first time.

IMPORTANT

- If you do not allow the user authentication information to be retained, [Save password and skip authentication dialog box when printing] in the [Setup User Names and Passwords for Authentication] dialog box of the AMS Printer Driver Add-in becomes disabled, and the password cannot be saved.

NOTE

- If you are not using the AMS Printer Driver Add-in, it is not necessary to set this item.

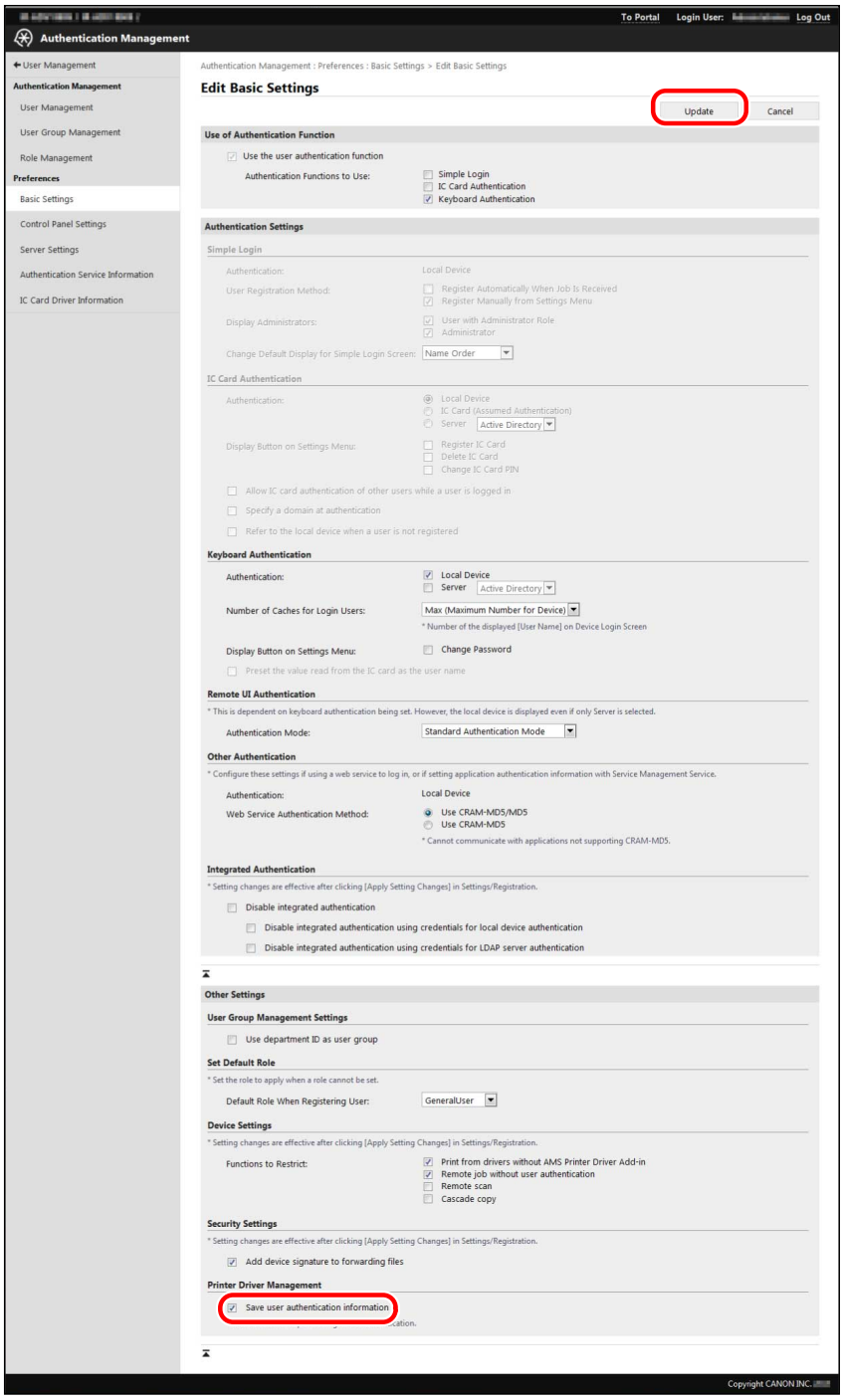
1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Basic Settings].

3 Click [Edit].

4 Select [Save user authentication information] in [Printer Driver Management] → click [Update].



IMPORTANT

- The [Printer Driver Management] setting is enabled after the device is restarted. For information on restarting the device, see the instruction manuals of the device.

Prohibiting the Printing from Drivers without AMS Printer Driver Add-in

You can set whether to restrict the printing of jobs that do not support print restrictions.

IMPORTANT

- Direct Printing from the Remote UI is also included in the jobs restricted by the settings in this item. If [Print from drivers without AMS Printer Driver Add-in] in [Functions to Restrict] is selected, you cannot use the Direct Printing from the Remote UI.
- Prohibit the printing of jobs that do not support print restrictions, if you want to restrict printing from the following computers:
  - Computers in which the AMS Printer Driver Add-in is not enabled
  - Computers to which an unknown user is logged on

NOTE

- If you are not using the AMS Printer Driver Add-in, it is not necessary to set this item.

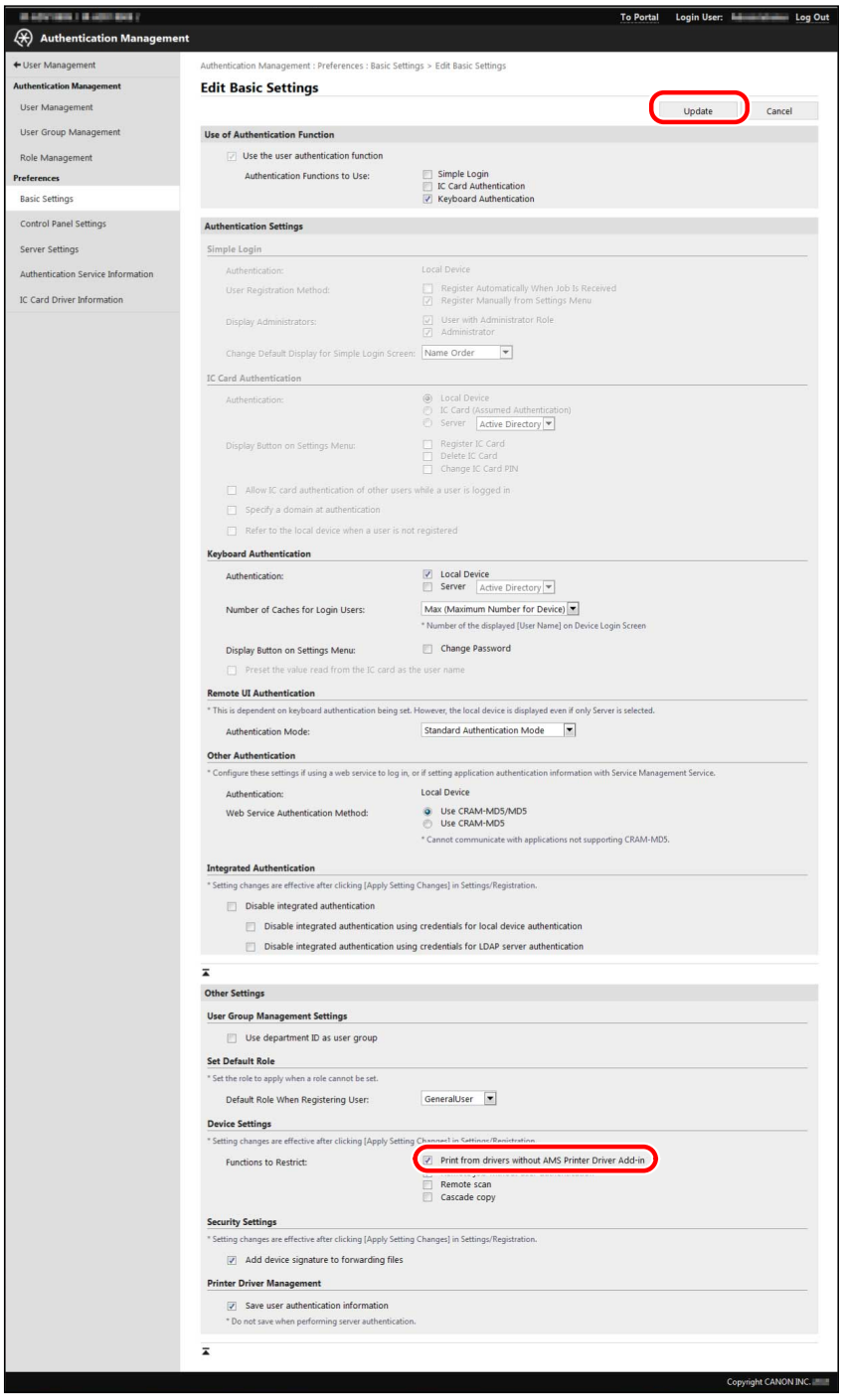
1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Basic Settings].

3 Click [Edit].

4 Select [Print from drivers without AMS Printer Driver Add-in] in [Functions to Restrict] → click [Update].



IMPORTANT

- The [Functions to Restrict] setting is enabled after the device is restarted. For information on restarting the device, see the instruction manuals of the device. (If an initialization completion screen is displayed on the touch panel display after the device is restarted, follow the instructions on the screen to restart the device.)

NOTE

- If you select [Print from drivers without AMS Printer Driver Add-in], a security check is automatically performed when printing from printer drivers in which theAMS Printer Driver Add-in is enabled. If a problem is found, printing is canceled.

Setting Remote Job Restrictions

Set usage restrictions for remote jobs without user authentication.

IMPORTANT

- If you are using local device authentication and you want to restrict printing without enabling the AMS Printer Driver Add-in, enable the [Remote job without user authentication] restriction. For more information, see " **Access Management System Configurations(P. 34)** ."

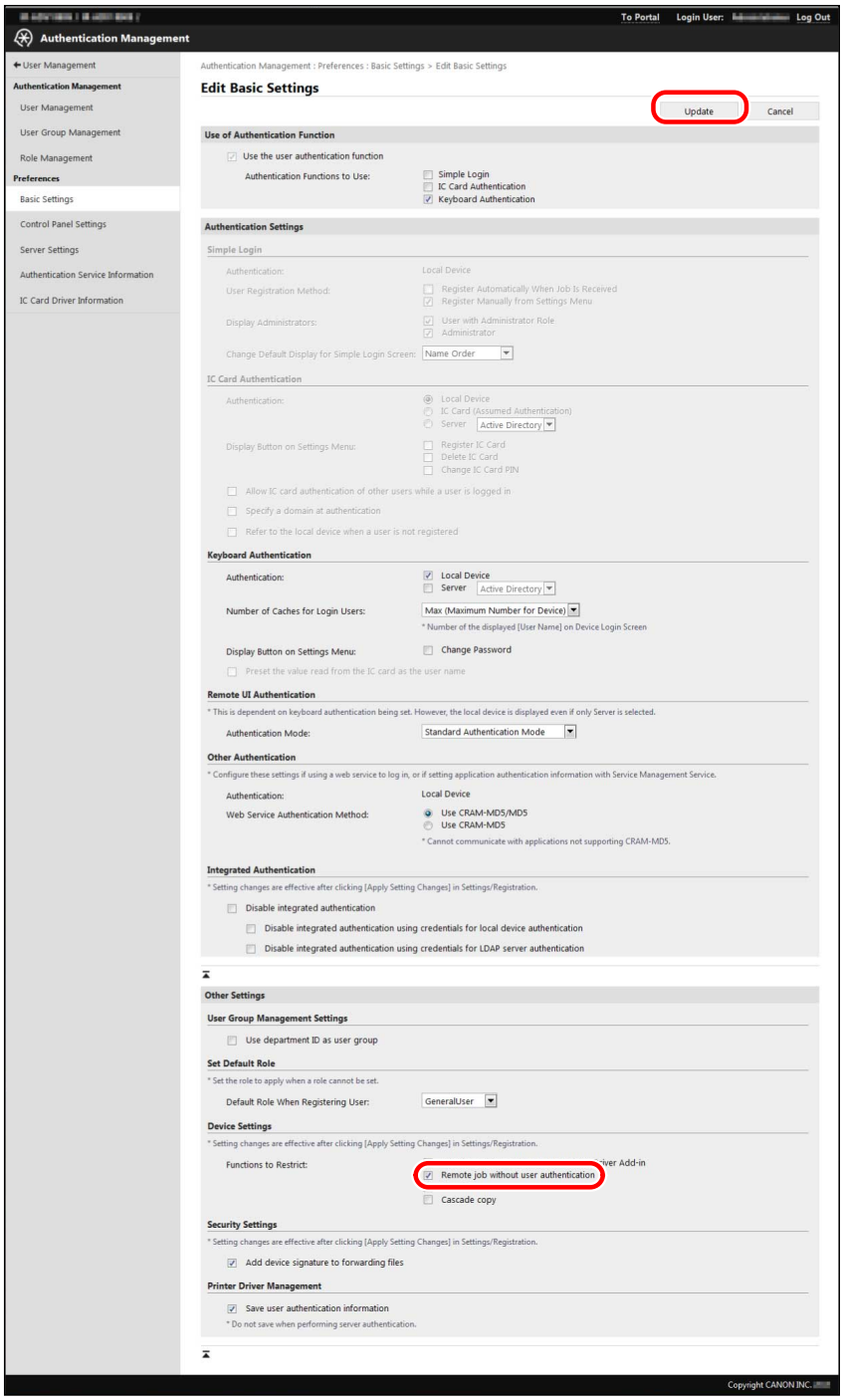
1 Log in to User Authentication.

For more information, see " **Logging in to User Authentication(P. 47)** ."

2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Basic Settings].

3 Click [Edit].

4 Select [Remote job without user authentication] in [Functions to Restrict] → click [Update].



IMPORTANT

- You need to restart the device to enable settings made in [Functions to Restrict]. For information on restarting the device, see the instruction manuals for the device. (If the initialization complete screen is displayed on the touch panel display after restarting the device, follow the instructions on the screen to turn the power of the device OFF and then ON again.)

Setting Usage Restrictions for Remote Scanning/Cascade Copy

Set usage restrictions for remote scanning/Cascade Copy.

IMPORTANT

- Restricted devices that support AMS cannot be used as the source device for Cascade Copy.

NOTE

- For more information, see the instruction manuals of the device.
- [Cascade copy] is not displayed on devices which do not support the Cascade Copy function.

Adding a Device Signature When Forwarding Files

You can set whether to add a device signature when forwarding files from a device.

NOTE

- This function is for adding a device signature to files forward with the optional Device Signature PDF Kit. For more information, see the instruction manuals of the device. (This function cannot be used unless the required options are installed.)

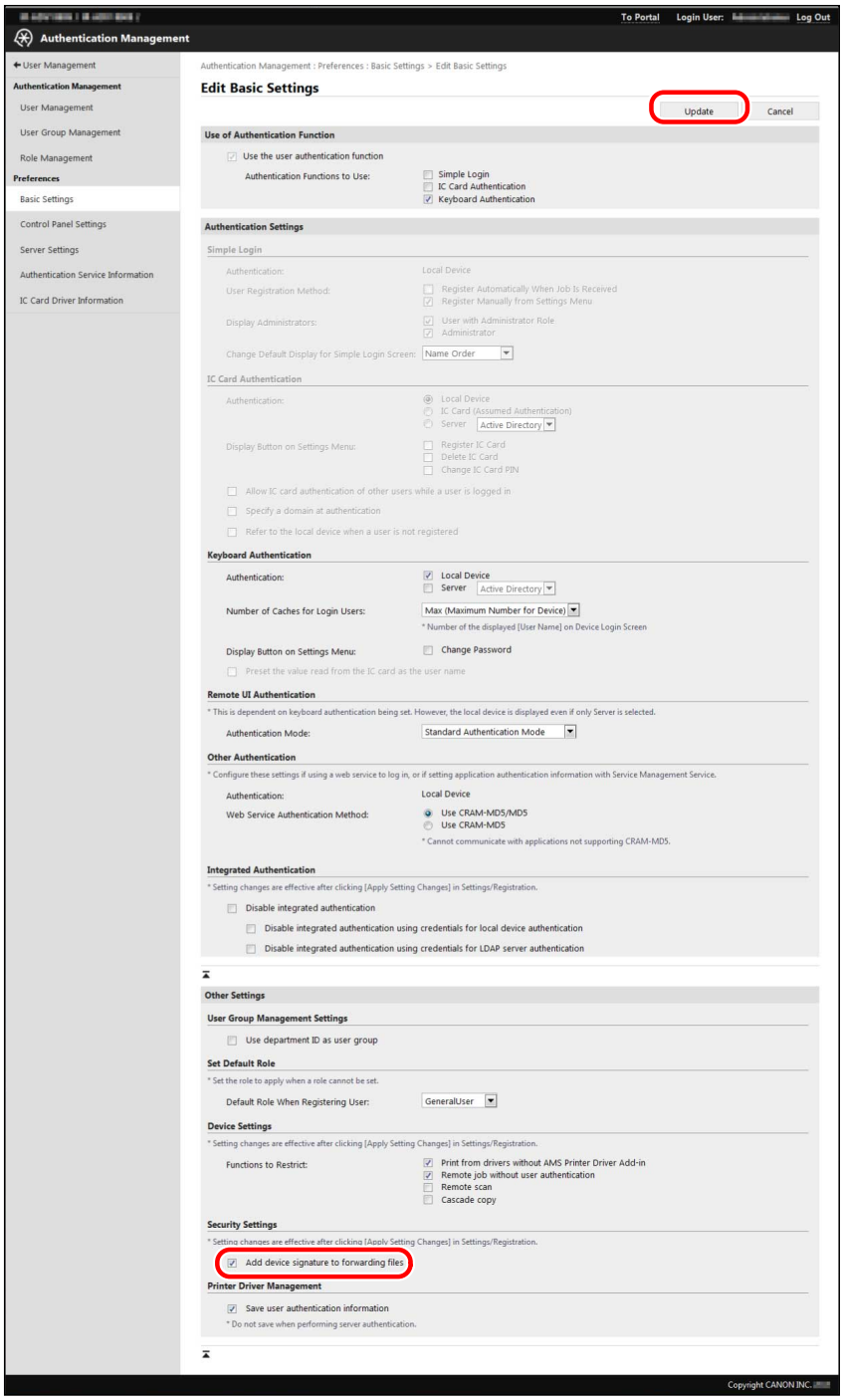
1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Basic Settings].

3 Click [Edit].

4 Select [Add device signature to forwarding files] in [Security Settings] → click [Update].



IMPORTANT

- The [Security Settings] setting is enabled after the device is restarted. For information on restarting the device, see the instruction manuals of the device.

Configuring IPP Printing

Set whether to use authentication when performing IPP printing. If you use authentication when performing IPP printing, you can set restrictions on user printing (including AirPrint) according to role.

1 Log in to User Authentication.

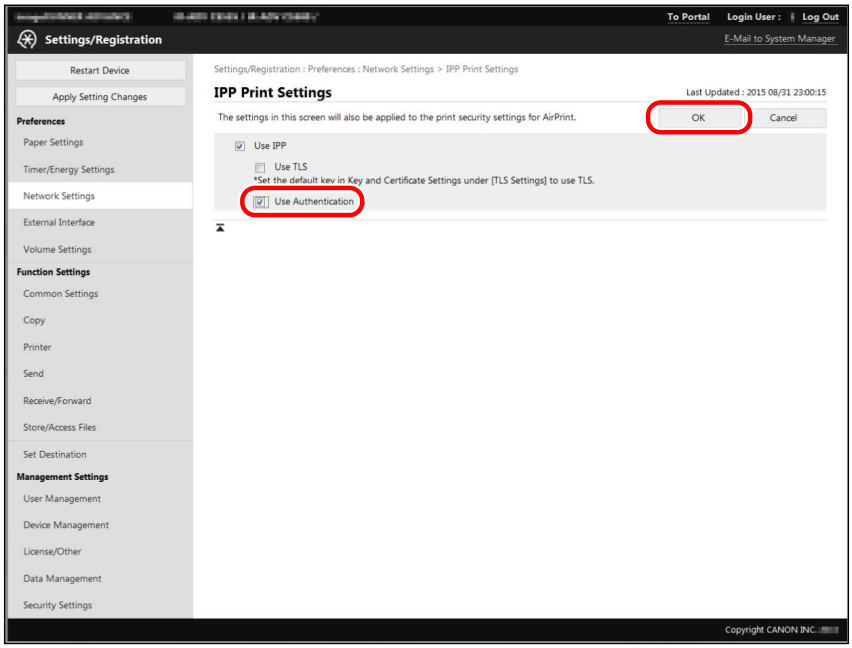
For more information, see " **Logging in to User Authentication(P. 47)** ."

2 Click [Settings/Registration] → [Network Settings] → [IPP Print Settings].

3 Select [Use Authentication] → click [OK].

NOTE

- If IPP printing settings are enabled, you can specify [Use Authentication].



Managing Roles

Register/edit the usage restrictions to associate to users as roles. Roles can also be imported/exported in batches.

There are two types of roles; base roles and custom roles. For more information, see **"Regarding Base Roles and Custom Roles."(P. 20)**

Managing Roles Using User Authentication(P. 63)

IMPORTANT

- Only users associated with the [Administrator] role can manage roles. (Users associated with a custom role based on the [Administrator] role (such as the [DeviceAdmin] or [NetworkAdmin] role) cannot manage roles.)
- Depending on the user authentication method you are using, required operations will differ. For more information, see **"Flow of Settings for Operating with Local Device Authentication"(P. 40)** or **"Flow of Settings for Operating with Server Authentication."(P. 42)**

Managing Roles Using User Authentication

This section describes the procedure for managing roles with User Authentication.

Creating Custom Roles

Custom roles are user-defined roles, and are created by adding/editing usage restriction information from a base role.

You can also edit the information for a created custom role. For more information, see **"Editing Custom Roles."(P. 67)**

IMPORTANT

- You can register a maximum of 100 roles, including base roles and custom roles (administrator).
- Custom roles registered in devices with an older version of the Access Management System can be used with this version.
- The restrictions for items not supported by a device cannot be set/checked from User Authentication, but are stored inside the device. (Therefore, when printing from a computer, [Available] may be displayed for [Color Print], even on a black-and-white device.)
- Do not set stricter restrictions for custom roles than those applied to unregistered users (the guest role). If the restrictions applied to registered users are stricter than those applied to unregistered users, the number of functions that can be used after logging in will be less than before logging in or than [Log In (Guest)], which may lead to inappropriate user management.

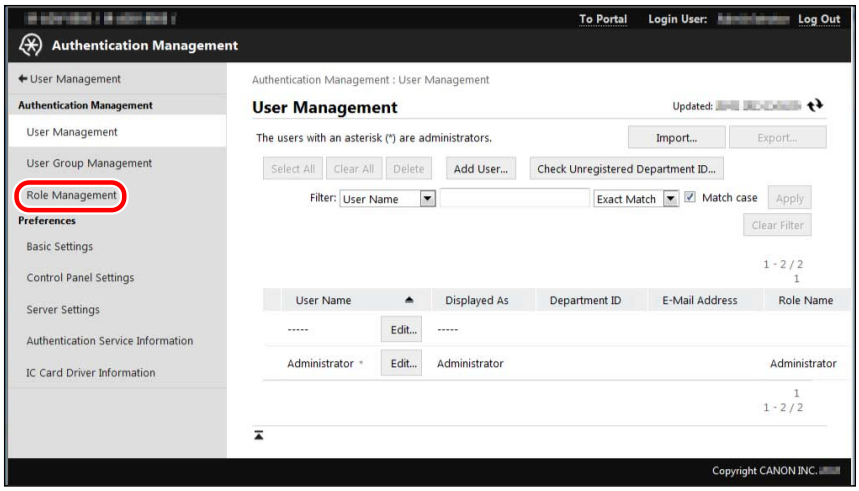
NOTE

- It is recommended you export role information after creating custom roles, for backup purposes. Since exported roles can be imported in other devices, the custom roles you create can also be registered in multiple devices. For more information, see **"Importing Roles"(P. 70)** and see **"Exporting Roles."(P. 72)**
- Associate roles to users on the [User Management] screen. For more information, see the instruction manuals of the device.

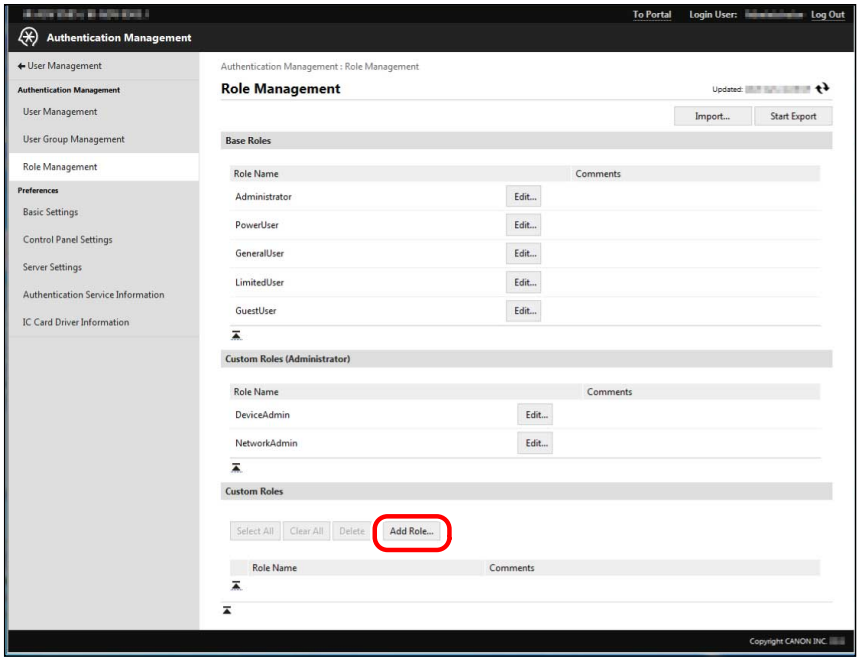
1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

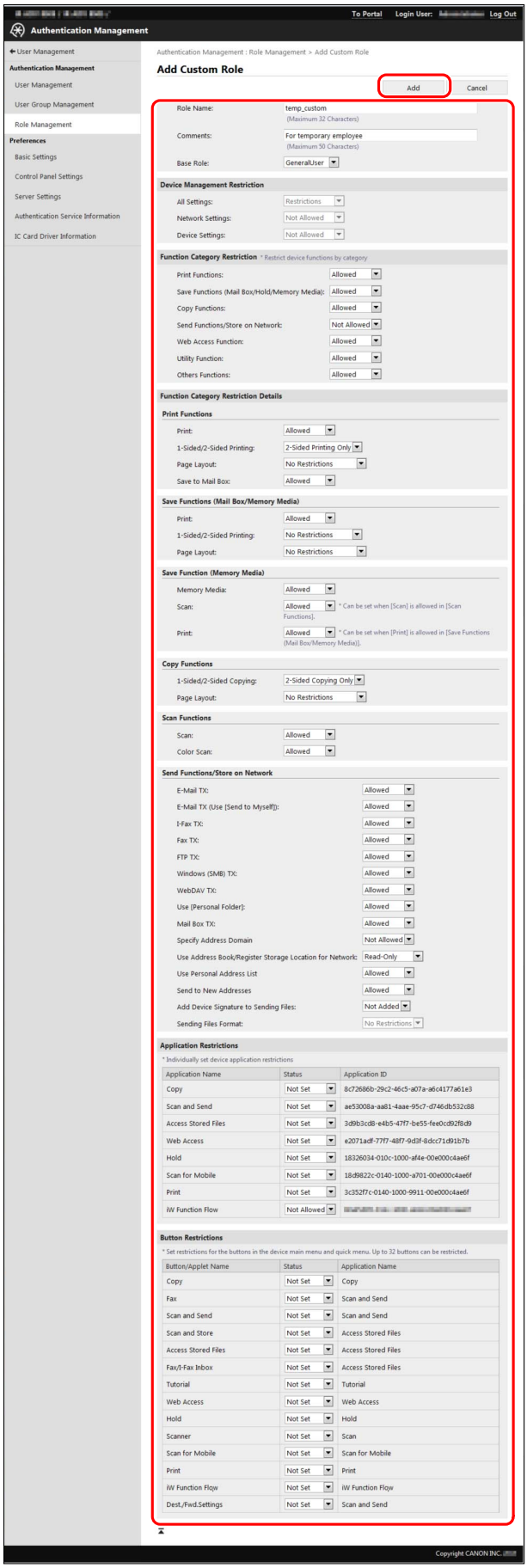
2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].



3 Click [Add Role] in [Custom Roles].



4 Specify the required items → click [Add].



The new role is registered.

The items required for entry and their scope are indicated below.

Item	Description	Scope
[Role Name]	Set the role name.	1 to 32 alphanumeric characters, hyphens (-), and underscores (_). You cannot register a role name that already exists. You cannot register a name that is the same or similar to the name of a base role or custom role (administrator).
[Comments]	Enter a description for the role.	User-defined string of 0 to 50 characters.
[Base Role]	Set the base role for the custom role.	You cannot set the [GuestUser] role. The base role set here determines the device management privileges. The role only has device management privileges if the [Administrator] role is set as the base role.
[Device Management Restriction]	Set the device management restrictions. **[All Settings]:** When set to [No Restrictions], no device management privileges are restricted, regardless of the settings in [Device Settings] and [Network Settings]. (Privileges equivalent to the [Administrator] role are available for the device management privileges.) When set to [Restrictions], the device management privileges are restricted according to the settings in [Device Settings] and [Network Settings]. (Even if both [Device Settings] and [Network Settings] are set to [No Restrictions], privileges equivalent to the [Administrator] role are not available for the device management privileges.) **[Network Settings]:** Set [No Restrictions]/[Not Allowed] for the device management privileges that belong to each network setting category. **[Device Settings]:** Set [No Restrictions]/[Not Allowed] for the device management privileges that belong to each device setting category.	You can set if [Administrator] is set for [Base Role].
[Function Category Restriction]	Set usage restrictions for each function category.	-
[Function Category Restriction Details]	Set usage restrictions for each detailed function.	-
[Application Restrictions]	Set usage restrictions for each device application.	Even if [Function Category Restriction] is set to [Not Allowed], functions with [Allowed] set for [Application Restrictions] can be used.
[Button Restrictions]	Set the usage restrictions for buttons displayed on the [Main Menu] screen or [Quick Menu] screen.	You cannot use functions set to [Not Allowed] in [Application Restrictions], regardless of whether they are not restricted in [Button Restrictions].

For information on device management privileges, see **"Device Management Privileges."(P. 23)** For information on device function restrictions, see **"Device Function Restrictions."(P. 26)**

NOTE

- The items displayed slightly differ for User Authentication version.
- "Device applications" refer to functions that are not included in the device, but are made available by installing them (such as MEAP applications).

Editing Custom Roles

You can edit the registered custom roles.

IMPORTANT

- Only [Comments] can be edited for base roles and custom roles (administrator). Restriction information can also be edited for the [GuestUser] role. For more information, see **"Editing the [GuestUser] Role (Guest Role)."(P. 68)**
- To change the role name of a custom role, it is necessary to delete the role and register it again as a new role.
- To change the [Base Role] setting (and therefore change the device management privileges), it is necessary to delete the role, and then register it again. (It is also possible to export the role and change the [Base Role] setting by editing it with a text editor. However, take care not to edit the control characters in this case.)
- The changed role information is enabled from the next time you log in. It is not applied to users currently logged in.
- Do not set stricter restrictions for custom roles than those applied to unregistered users (the guest role). If the restrictions applied to registered users are stricter than those applied to unregistered users, the number of functions that can be used after logging in will be less than before logging in or than [Log In (Guest)], which may lead to inappropriate user management.

NOTE

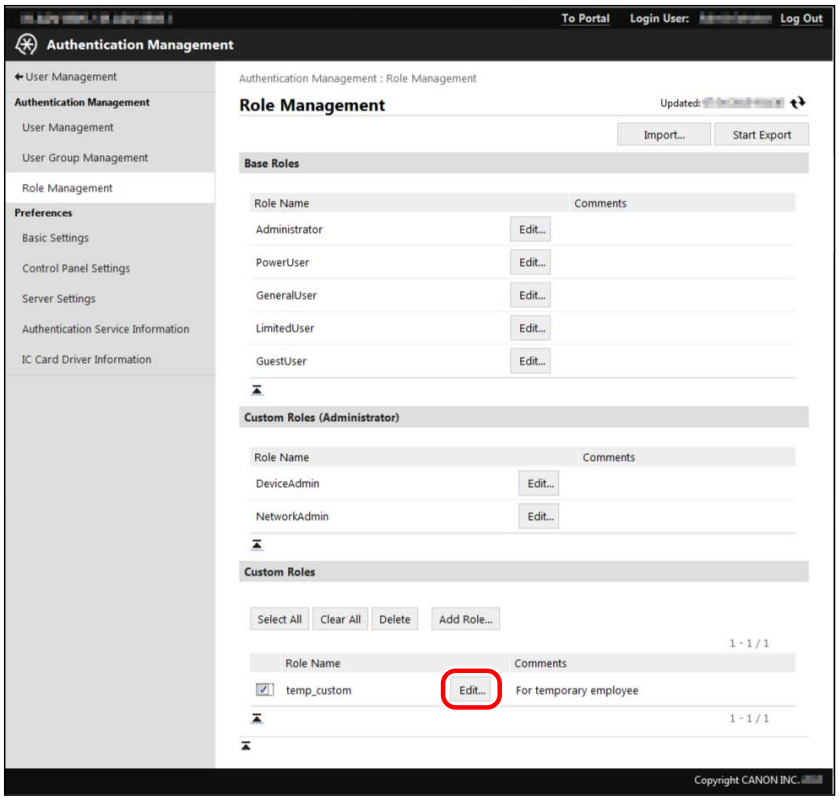
- It is recommended you export the role information after editing custom roles for backup purposes. For more information, see **"Exporting Roles."(P. 72)**
- Associate roles to users on the [User Management] screen. For more information, see the instruction manuals of the device.

1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].

3 Click [Edit] for the role you want to edit.



4 Edit the required items → click [Update].

The role information is changed.

IMPORTANT

- [Device Management Restriction] can only be set if [Administrator] is set for [Base Role].

Editing the [GuestUser] Role (Guest Role)

You can edit the roles for unregistered users.

IMPORTANT

- The changed role information is enabled from the next time you log in. It is not applied to users currently logged in.
- Set stricter restrictions for unregistered users (the guest role) than those applied to other base roles and custom roles. If the restrictions applied to registered users are stricter than those applied to unregistered users, the number of functions that can be used after logging in will be less than before logging in or than [Log In (Guest)], which may lead to inappropriate user management.

NOTE

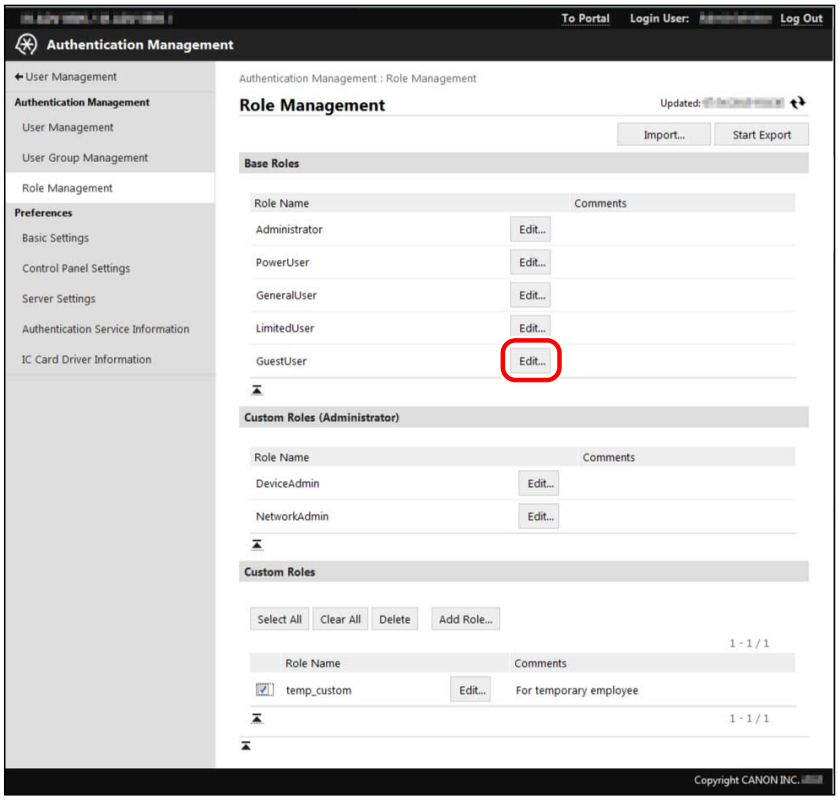
- It is recommended you export the role information after editing [GuestUser] role for backup purposes. For more information, see **"Exporting Roles."(P. 72)**

1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

2 **Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].**

3 **Click [Edit] for [GuestUser] in [Base Roles].**



4 **Edit the required items → click [Update].**

The role information is changed.

Deleting Custom Roles

You can delete registered custom roles.

IMPORTANT

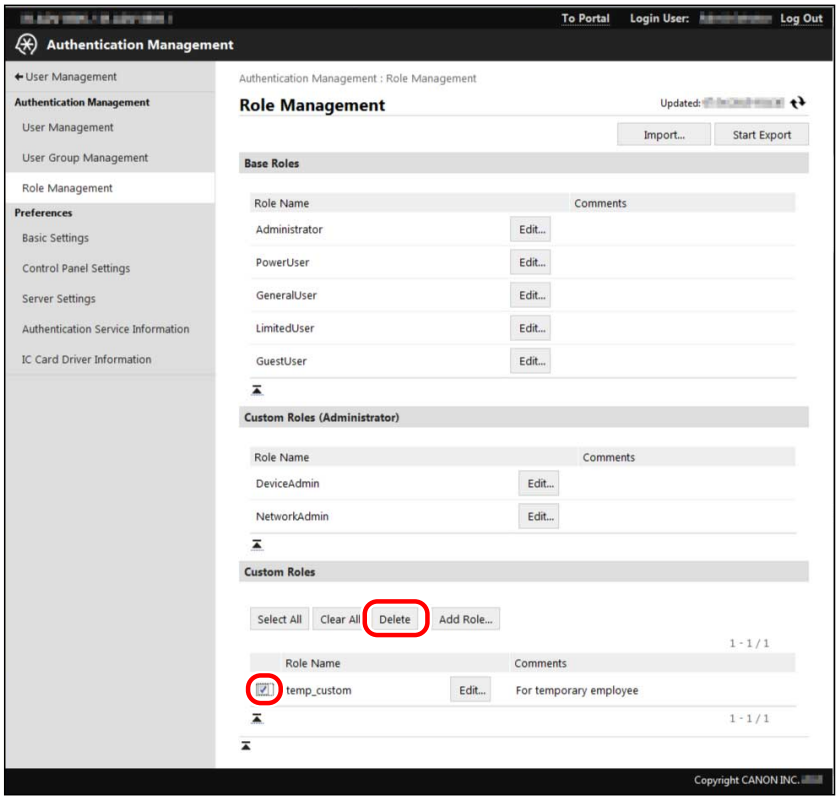
- Base roles and custom roles (administrator) cannot be deleted.

1 **Log in to User Authentication.**

For more information, see **"Logging in to User Authentication."(P. 47)**

2 **Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].**

3 Select the role you want to delete in [Custom Roles] → click [Delete].



The role is deleted.

NOTE

- If you want to select all the custom roles, select [Select All].

Importing Roles

You can import the roles registered in another device from a file.

IMPORTANT

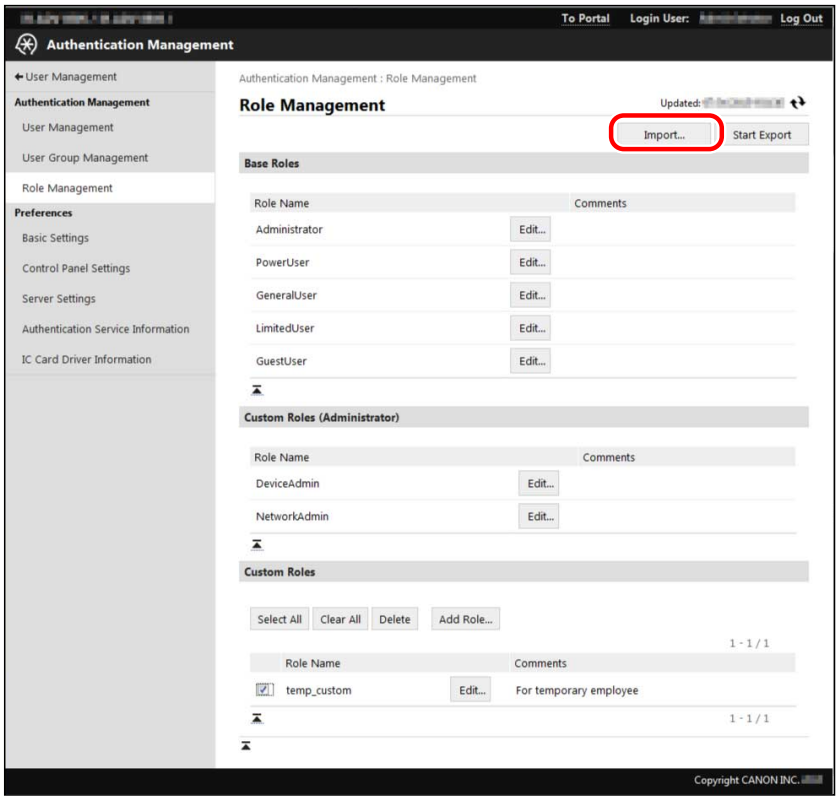
- If a role with the same name as a role to import already exists, that role is overwritten with the imported role information. However, only comments are overwritten for base roles other than the guest role and custom roles (administrator).
- If the [Device Management Restriction] setting is invalid (if [Device Settings] and [Network Settings] are set to [Not Allowed] despite [All Settings] being set to [No Restrictions]) the role information is deemed invalid and is not imported.
- If roles not included in the import file were registered in the device, those roles are not deleted, and the roles inside the import file are added to the device.

1 Log in to User Authentication.

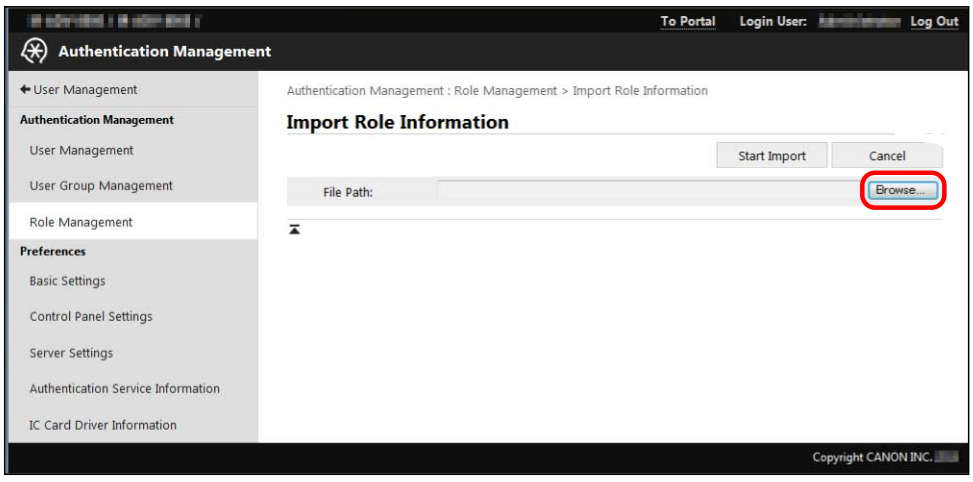
For more information, see **"Logging in to User Authentication."(P. 47)**

2 **Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].**

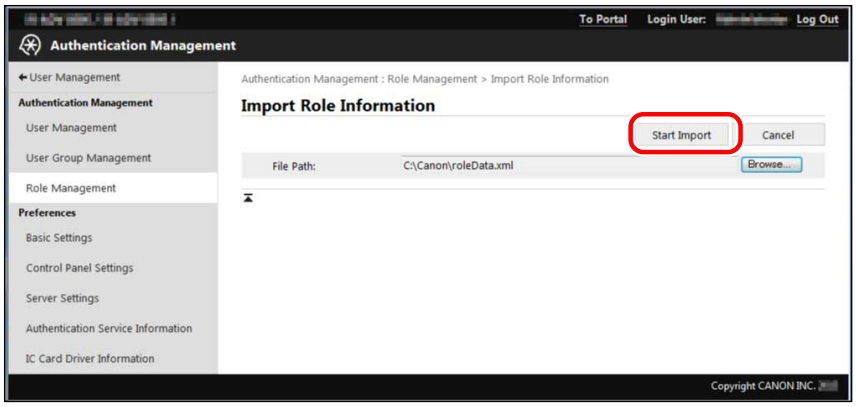
3 **Click [Import].**



4 **Click [Browse] to select the file to import.**



5 **Click [Start Import].**



The role information is imported.

NOTE

- If the role information fails to be imported, the data is rolled back, and returns to the state it was before the import.

Exporting Roles

You can save the role information registered in a device as a file. This is useful for backup purposes, or for using the registered role information in another device.

NOTE

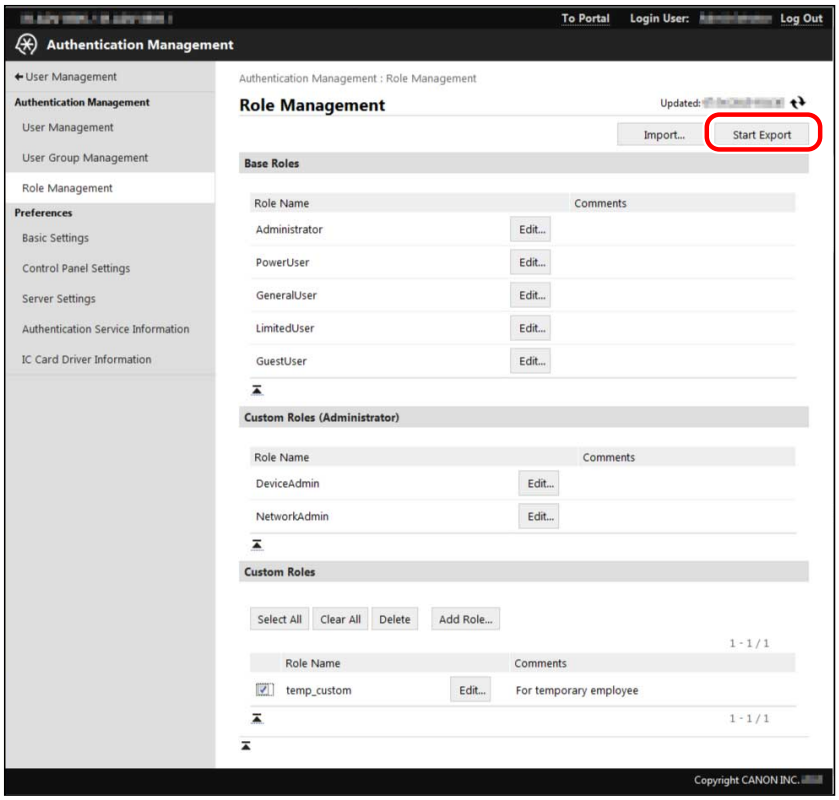
- The file extension is 'xml' and the default file name is 'roleData.xml'.
- It is also possible to export the role and edit it with a text editor. This is useful when you want to change the role names. However, take care not to edit the control characters in this case.

1 Log in to User Authentication.

For more information, see **"Logging in to User Authentication."(P. 47)**

2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].

3 Click [Start Export].



4 Follow the instructions on the screen to specify the location to save the file.

The file is downloaded.

Setting Up the Client Computers

Setting Up the Client Computers

This section describes the procedure for setting up client computers, such as enabling the AMS Printer Driver Add-in.

Flow of Setting Up Client Computers

This section describes the flow of setting up client computers, such as enabling the AMS Printer Driver Add-in.

1. Enabling the AMS Printer Driver Add-in

To restrict printing from computers using the Access Management System, you must enable the AMS Printer Driver Add-in of the printer driver installed to the client computers.

For details, see the instruction manuals of the printer driver.

2. Setting the User Information to Use for AMS Authentication

Set the information of users that use AMS to print from a computer.
For details, see the instruction manuals of the printer driver.

Operation Example of Local Device Authentication

Operation Example of Local Device Authentication

This section describes the procedure for newly setting up the Access Management System with local device authentication, and describes an example configuration.

Example of Operating with Local Device Authentication

In the example described here, the system management department members act as both device administrators and device restriction administrators to set device usage restrictions for a group comprised of three sales department members (Manager A, Regular employee B, and Temporary employee C).

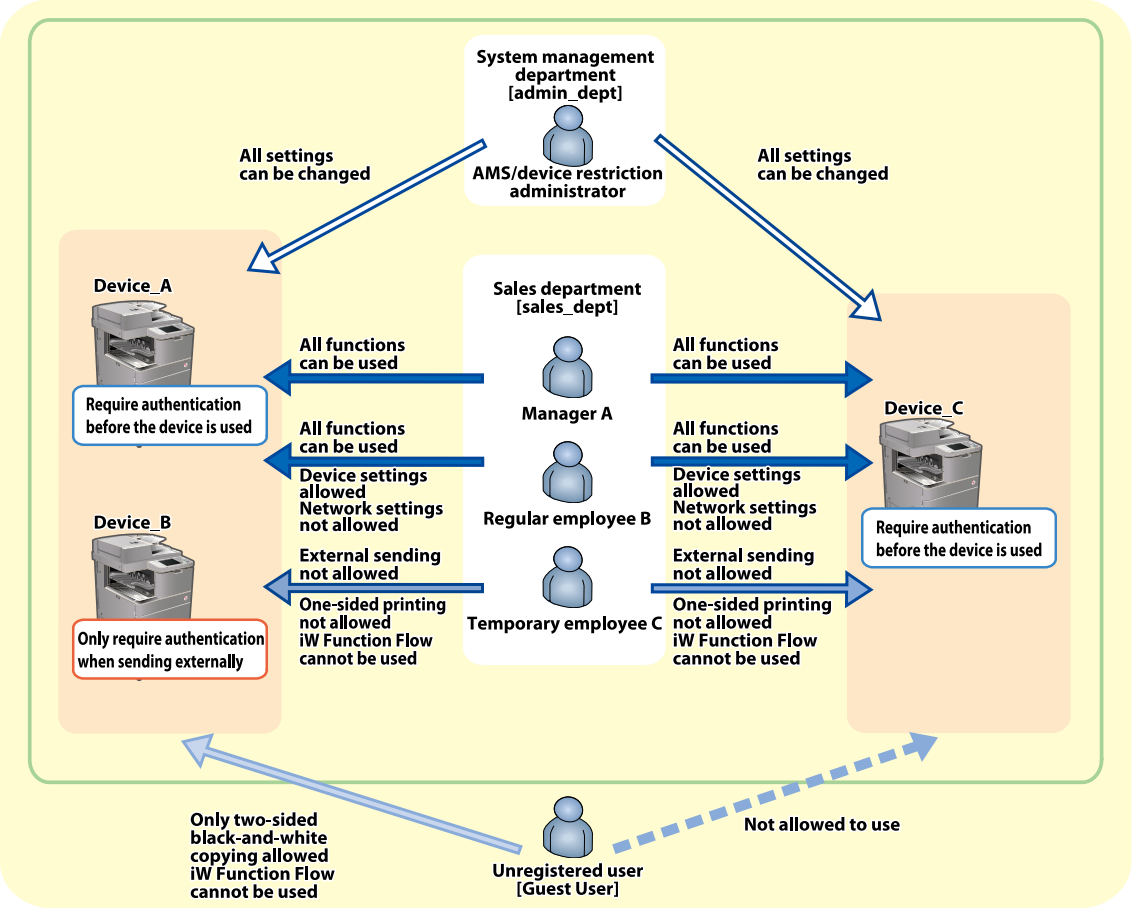
Three devices are used: Device_A, Device_B, and Device_C. These three devices are the same model. These three devices all support using the Access Management System in conjunction with the Department ID Management function, and have the optional iW Function Flow added and started. These three devices are managed by members of the system management department, who also act as device administrators.

Device_A and Device_C will be set to Device Level Log-in, and Device_B will be set to Function Level Log-in. Unregistered users will be allowed to use Device_A and Device_B but not allowed to use Device_C.

When registered users log in to the device, restrictions are applied according to their title in the organization.

When unregistered users use Device_A, they will be able to log in as guest users. When they use Device_B, they will not be required to log in. Unregistered users will not be allowed to use Device_C.

This example assumes that Department IDs are assigned by group (by department).



Users and Roles to Use in the Example

In this example, device restrictions are set for the following users.

Staff	User Name/Password	Role to Associate
Sales department ([sales_dept]) (Department ID: 3333333/ PIN: 0000003)		

Staff	User Name/Password	Role to Associate	
Manager A	[sales_manager]/ [m_password]	[PowerUser]	All device functions can be used. The [Settings/Registration] screen cannot be used, except for some functions.
Regular employee B	[sales_regular]/ [r_password]	[DeviceAdmin]	All device functions can be used. The network management functions on the [Settings/ Registration] screen cannot be used.
Temporary employee C	[sales_temp]/ [t_password]	[temp_custom] (custom role)	One-sided printing from a computer and the Send function cannot be used. The [Settings/Registration] screen cannot be used, except for some functions. iW Function Flow cannot be used.
System management department [admin_dept] (System Manager ID: 1111111/ System PIN: 0000001) (Department ID: 2222222/ PIN: 0000002)			
AMS/device restriction administrator	[IT_management]/ [admin_password]	[Administrator]	All device functions can be used. All functions can be used on the [Settings/Registration] screen.
Other Users	No User Name/Password	[GuestUser]	Only two-sided black-and-white copying are allowed. iW Function Flow cannot be used.

Flow of Operations

This section describes the flow of operations. For more information, see each page.

1. Preparing the Device and Network Environment(P. 83)

Set the network environment and date/time settings. and register a System Manager ID for all devices to operate with the Access Management System.

2. Enabling the AMS

Enable the AMS on all devices that support it.

For more information, see the instruction manuals of the device.

3. Starting User Authentication

Start User Authentication on all devices that support AMS.

For more information, see the instruction manuals of the device.

4. Specifying the Preferences of the Devices(P. 84)

For all devices that support AMS, set the user authentication method, login method, and whether to allow unregistered users to use the device, etc., and then restart the device. In this example, Device_A and Device_C will be set to Device Level Log-in, and Device_B will be set to Function Level Log-in. Unregistered users will be allowed to use Device_A and Device_B, but not allowed to use Device_C.

5. Creating Custom Roles(P. 93)

In this example, a [temp_custom] role will be created on Device_A for temporary employees, based on the [GeneralUser] role. The content of the [GuestUser] role will also be checked.

6. Exporting Custom Roles(P. 97)

In this example, the roles in Device_A will be exported (all roles including the base roles, not just the [temp_custom] role).

7. Registering Local Users and Specifying Roles(P. 98)

Create the user information on Device_A. In this example, local user accounts will be created for the staff in the sales department and system management department. The name of the role to apply to each local user will also be registered in the user information.

IMPORTANT

- When using the Department ID Management function, set the Department ID in the user information for each user.

8. Exporting User Information(P. 102)

Export the user information created on Device_A.

9. Importing Roles and User Information(P. 103)

Import the roles and user information in all devices that support AMS. In this example, the roles and user information will be imported in Device_B and Device_C.

10. Starting the Department ID Management Function(P. 106)

Start the Department ID Management function. In this example, the Department IDs for the sales department and system management department will be registered in Device_A, Device_B, and Device_C.

IMPORTANT

- Before using the Department ID Management function, check that a Department ID is set in the user information for each user. When you start using the Department ID Management function, users with no Department ID registered in their user information cannot log in.

11. Confirming the Login Method and Usage Restrictions on the Touch Panel Display(P. 112)

In this example, Device_A and Device_C will be checked to confirm that they are set to Device Level Log-in, and Device_B will be checked to confirm that it is set to Function Level Log-in. The devices will also be logged in to with each user to check that the specified restrictions are being applied.

12. Setting Up the Client Computers(P. 118)

Install a printer driver supporting the AMS function to all the user computers. Then, enable the AMS function and set the user information.

13. Confirming the Print Restrictions on Client Computers(P. 121)

Confirm that the specified printing restrictions are applied on each client computer.

Preparing the Device and Network Environment

In this example, the device and network environment will be prepared for three new devices. The System Manager ID will then be set, and the devices set to prevent users other than system management department members from changing the device settings.

Setting the Date/Time(P. 83)
Specifying the Network Settings(P. 83)
Making Devices Accessible from Web Browsers(P. 83)
Registering the System Manager ID(P. 83)

Setting the Date/Time

Set the correct date and time for all the devices. For more information, see the instruction manuals of the device.

Specifying the Network Settings

Specify the network settings for all the devices. For more information, see the instruction manuals of the device.

Making Devices Accessible from Web Browsers

Set all the devices to be accessible from Web browsers. For more information, see **"Making Devices Accessible from Web Browsers."(P. 45)**

Registering the System Manager ID

Register the System Manager ID in all the devices, and set the devices to prevent users other than system managers from changing the device settings.

In this example, members of the system management department are registered as system managers.

For more information, see the instruction manuals of the device.

[System Manager ID]	1111111
[System PIN]	0000001
[System Manager]	IT_management

Specifying the Preferences of the Devices

In this example, Device_A and Device_C will be set to Device Level Log-in, and Device_B will be set to Function Level Log-in. Unregistered users will be allowed to use Device_A and Device_B, but not allowed to use Device_C.

Specifying the preferences of the devices(P. 84)

Specifying the preferences of the devices

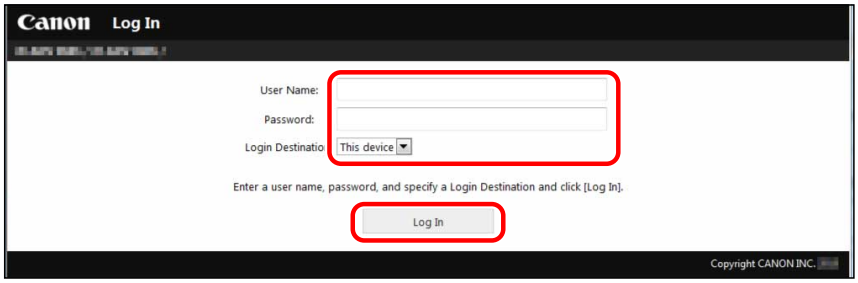
Specify the preferences of the devices for Device_A, Device_B, and Device_C. You can specify security settings. In this example, security settings are also specified for Device_A and Device_B.

1 Open your Web browser → enter the following URL:

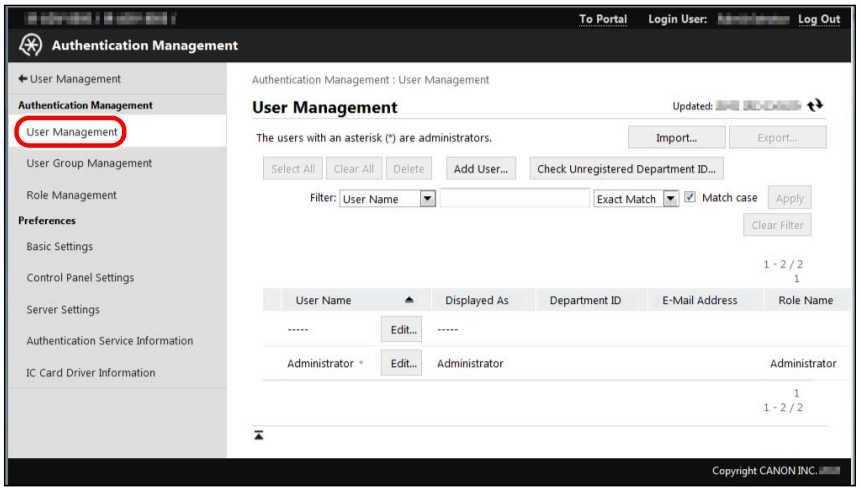
http://<IP address or host name of the device>

The [Login] page is displayed.

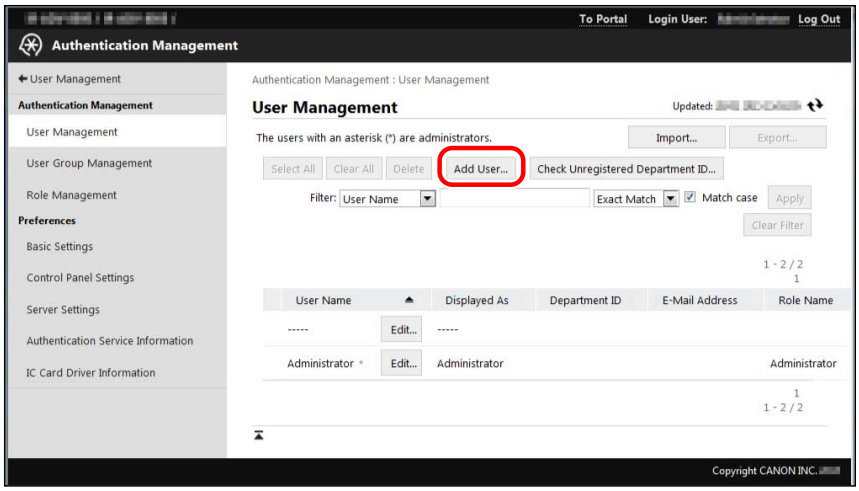
2 Enter the user name and password of a user assigned the [Administrator] role → select [This device] in [Login Destination] → click [Log In].



3 Click [Settings/Registration] → [User Management] → [Authentication Management] → [User Management].



4 Click [Add User].



5 Set the user name and password for the device restriction administrator → click [Update].

Since the system management department members act as both device administrators and device usage restriction administrators in this example, the account registered as the system administrator in **"Preparing the Device and Network Environment"(P. 83)** is registered as the device usage restriction administrator.

[User Name]	IT_management
[Password]	admin_password
[Select Role to Set]	[Administrator]
[Department ID]	[2222222]
[PIN]	[0000002]

NOTE

- Device restriction administrators (users associated with the [Administrator] role) do not need to also be system managers (users that know the System Manager ID) because all the device management privileges are assigned to device restriction administrators.

6 Click [Log Out].

7 Open your Web browser → enter the following URL:

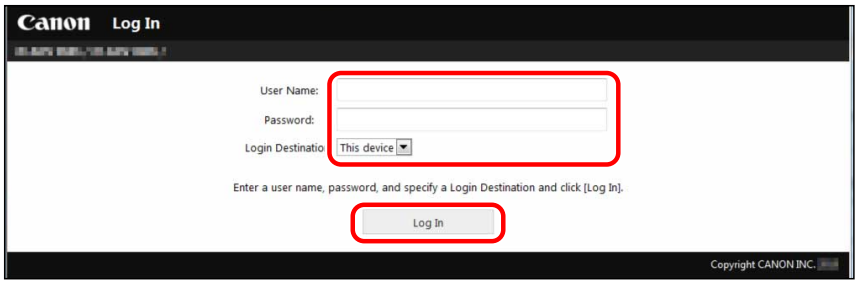
http://<IP address or host name of the device>

The [Login] page is displayed.

8 Enter the user name and password of a user assigned the [Administrator] role → select [This device] in [Login Destination] → click [Log In].

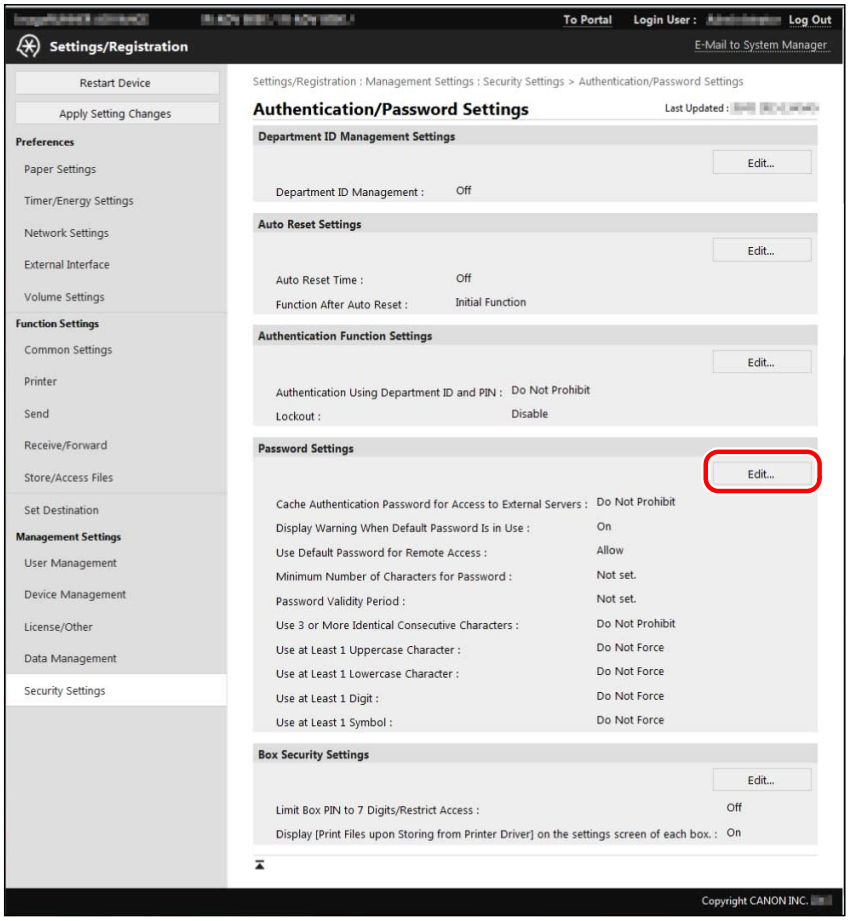
In this example, the following settings are specified:

[User Name]	IT_management
[Password]	admin_password
[Login Destination]	[This device]



9 Click [Settings/Registration] → [Security Settings] → [Authentication/Password Settings].

10 Click [Edit] in [Password Settings].

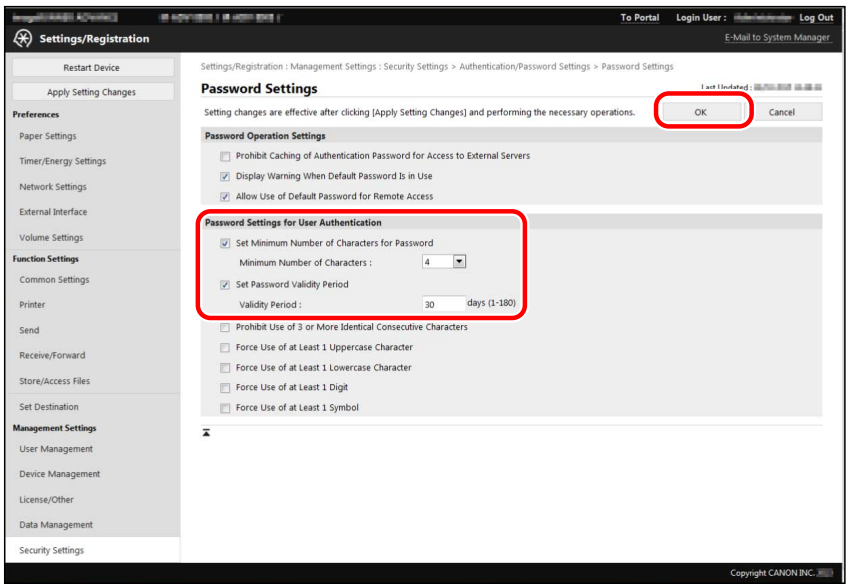


11 Set the password policy in [Password Settings for User Authentication].

- ❑ Select [Set Minimum Number of Characters for Password].
- ❑ Select [4] from the [Minimum Number of Characters] drop-down list.
- ❑ Select [Set Password Validity Period].
- ❑ Enter [30] for [Validity Period].
- ❑ Click [OK].

NOTE

- For more information, see the instruction manuals of the device.



12 Specify [Preferences].

NOTE

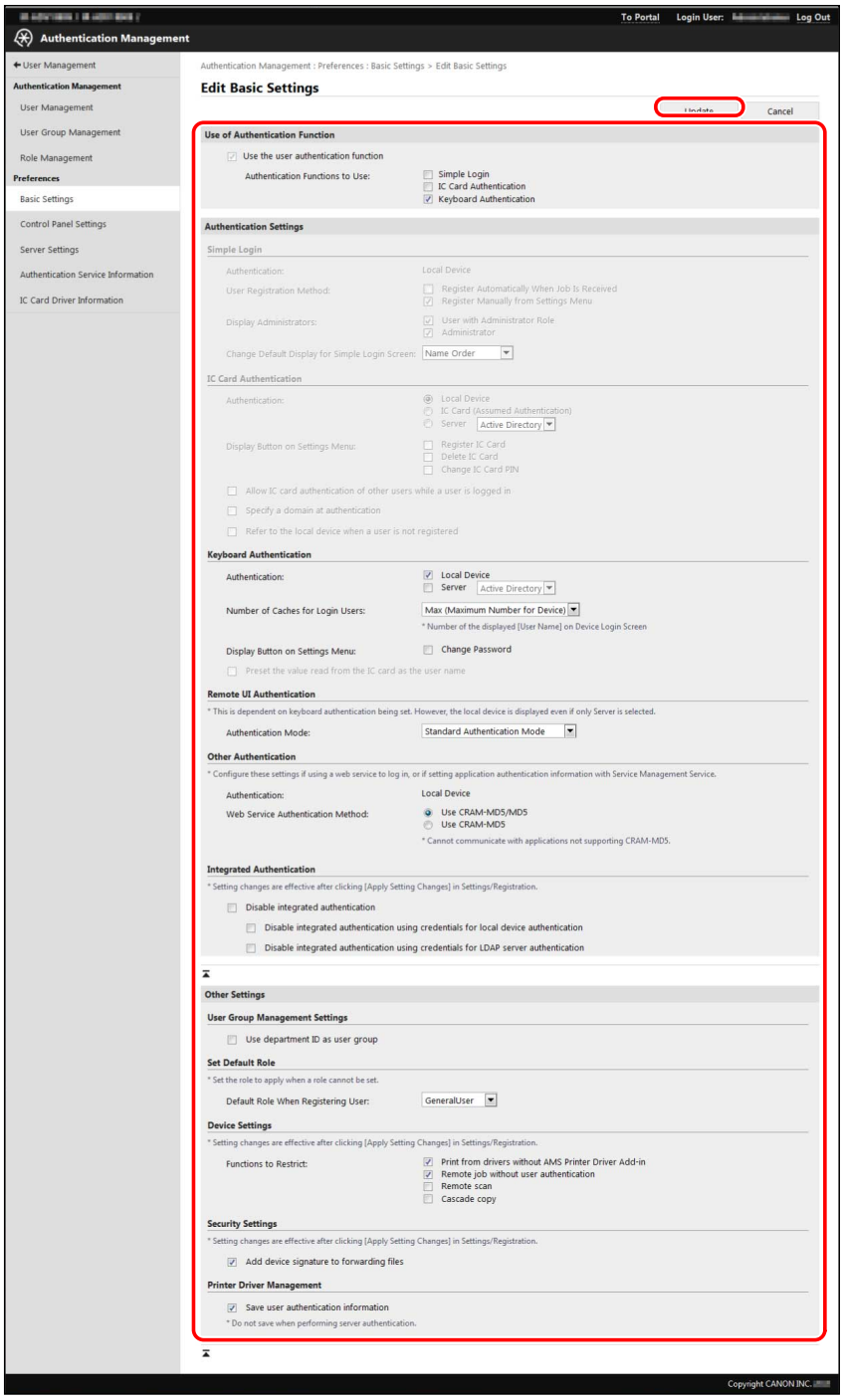
- For more information, see " **Specifying the Preferences of the Devices(P. 48)** " or instruction manuals of the device.

[Basic Settings]

❑ **Click [Settings/Registration] → [User Management] → [Authentication Management] → [Basic Settings].**

❑ **Click [Edit].**

❑ **Specify the required settings → click [Update].**

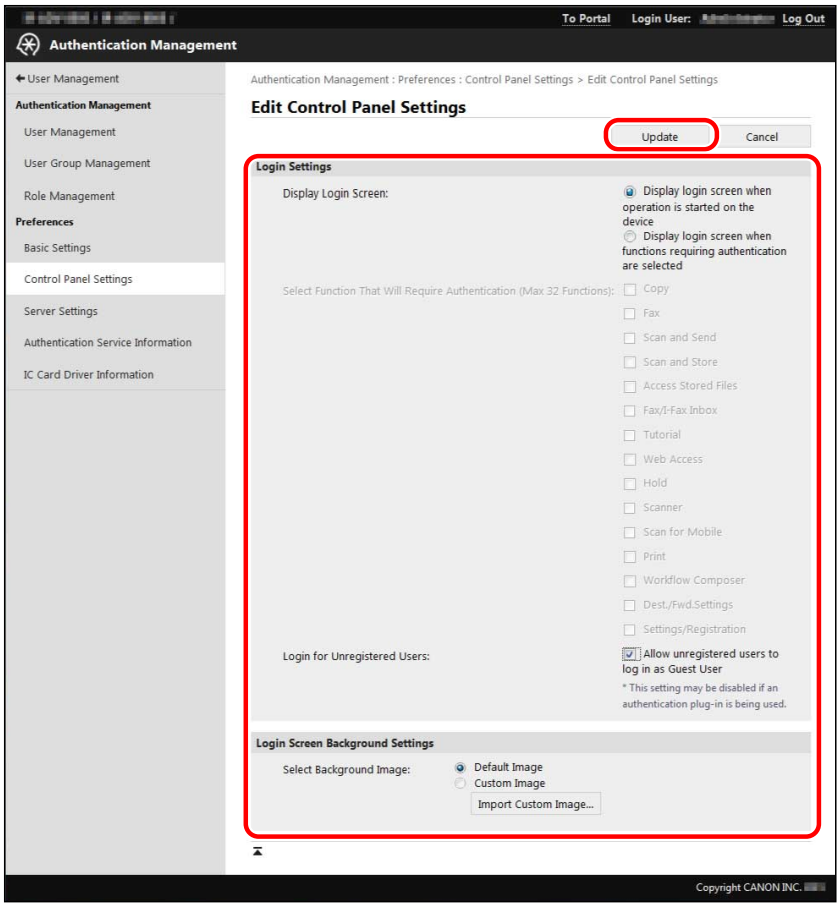


[Control Panel Settings]

❑ **Click [Settings/Registration] → [User Management] → [Authentication Management] → [Control Panel Settings].**

❑ **Click [Edit].**

❑ **Specify the required settings → click [Update].**

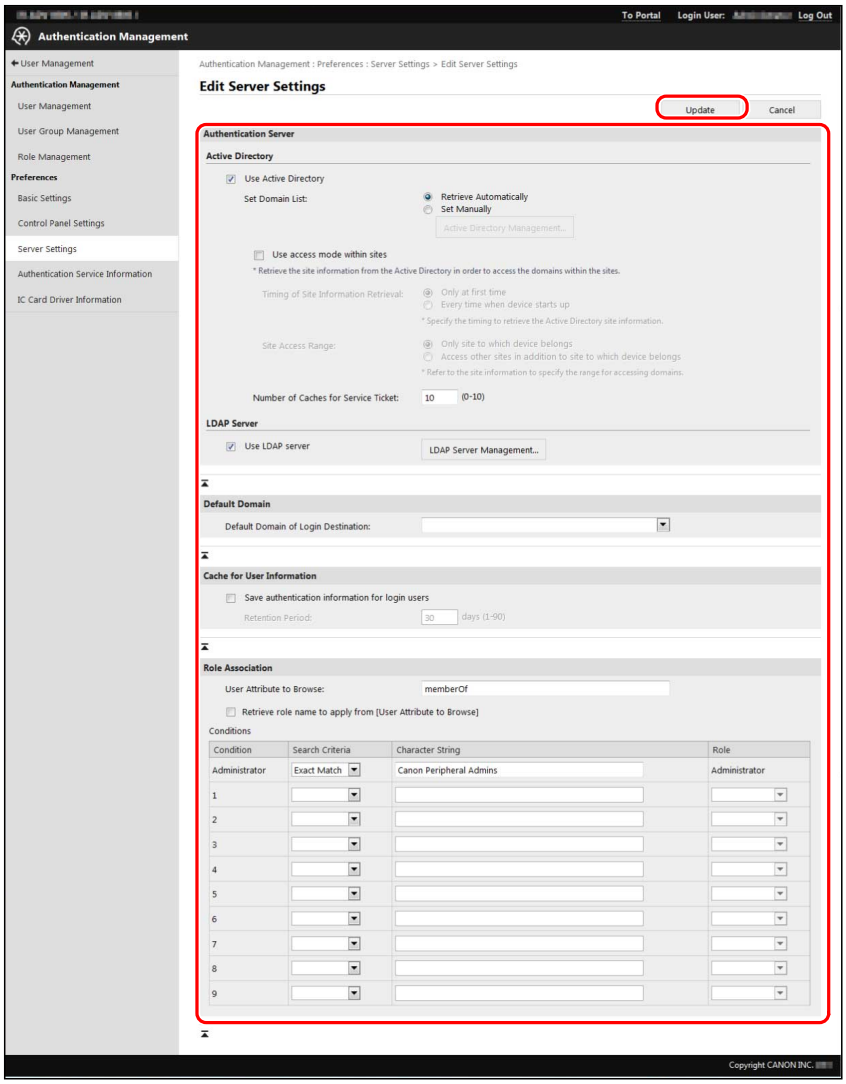


[Server Settings]

❑ **Click [Settings/Registration] → [User Management] → [Authentication Management] → [Server Settings].**

❑ **Click [Edit].**

❑ **Specify the required settings → click [Update].**



In this example, the following settings are specified:

Device_A

☞ [Basic Settings]

[Functions to Restrict]	[Keyboard Authentication]
[Default Role When Registering User]	[LimitedUser]
[Functions to Restrict]	[Print from drivers without AMS Printer Driver Add-in]
	[Remote job without user authentication]
[Printer Driver Management]	[Save user authentication information]

☞ [Control Panel Settings]

[Display Login Screen]	[Display login screen when operation is started on the device]
[Login for Unregistered Users]	[Allow unregistered users to log in as Guest User]

☞ [Server Settings]

[Use of Active Directory]	[Do not use]
[Use of LDAP Server]	[Do not use]

Device_B

☞ [Basic Settings]

[Authentication Functions to Use]	[Keyboard Authentication]
[Default Role When Registering User]	[LimitedUser]
[Functions to Restrict]	[Print from drivers without AMS Printer Driver Add-in]
	[Remote job without user authentication]
[Printer Driver Management]	[Save user authentication information]

☞ [Control Panel Settings]

[Display Login Screen]	[Display login screen when functions requiring authentication are selected]
[Select Function That Will Require Authentication]	[Scan and Send]
	[iW Function Flow]
	[Settings/Registration]

☞ [Server Settings]

[Use of Active Directory]	[Do not use]
[Use of LDAP Server]	[Do not use]

Device_C

☞ [Basic Settings]

[Authentication Functions to Use]	[Keyboard Authentication]
[Default Role When Registering User]	[LimitedUser]
[Functions to Restrict]	[Print from drivers without AMS Printer Driver Add-in]
	[Remote job without user authentication]
[Printer Driver Management]	[Save user authentication information]

☞ [Control Panel Settings]

[Display Login Screen]	[Display login screen when operation is started on the device]
[Login for Unregistered Users]	Deselected

☞ [Server Settings]

[Use of Active Directory]	[Do not use]
[Use of LDAP Server]	[Do not use]

13 Click [Log Out].

14 Restart the device.

IMPORTANT

- These settings are enabled only after the device is restarted. For instructions on restarting the device, see the manuals included with the device.

Creating Custom Roles

Create the custom roles for operating the Access Management System.

Also confirm/edit the content of the [GuestUser] role to ensure that user management is performed appropriately.

Creating Custom Roles(P. 93)
Editing [GuestUser] Role Registered(P. 96)

Creating Custom Roles

In this example, a [temp_custom] role will be created on Device_A for temporary employees, based on the [GeneralUser] role.

1 Open your Web browser → enter the following URL:

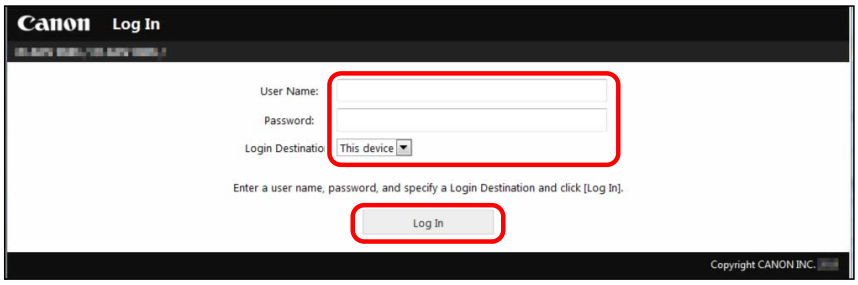
http://<IP address or host name of the device>

The [Login] page is displayed.

2 Enter the user name and password of the device restriction administrator → select [This device] in [Login Destination] → click [Log In].

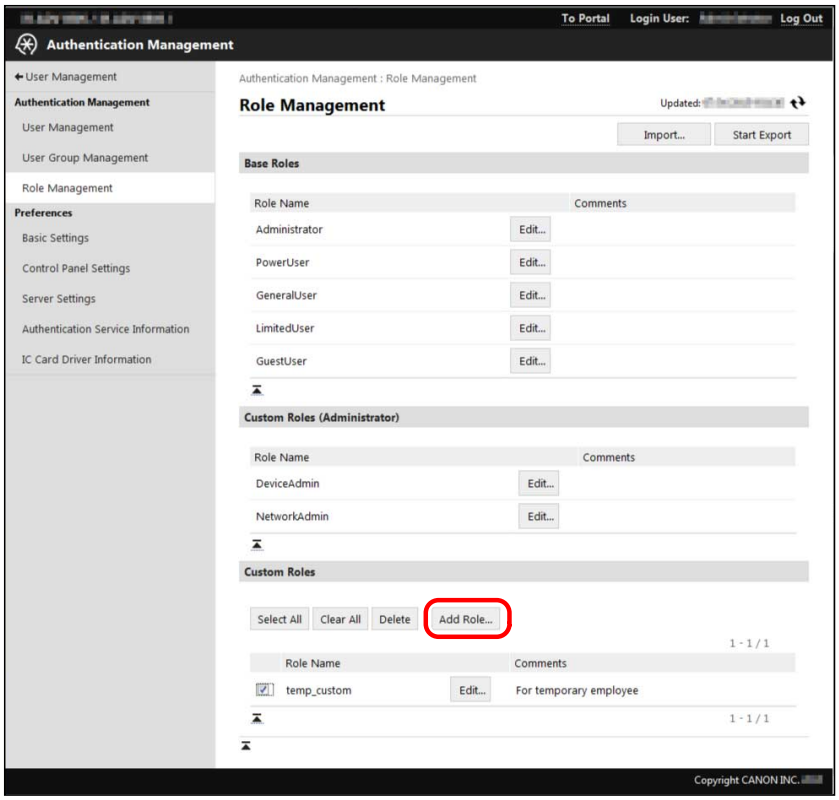
In this example, the following settings are specified:

[User Name]	IT_management
[Password]	admin_password
[Login Destination]	[This device]



3 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].

4 Click [Add Role].



5 Enter the required items → click [Add].

In this example, the following settings are specified:

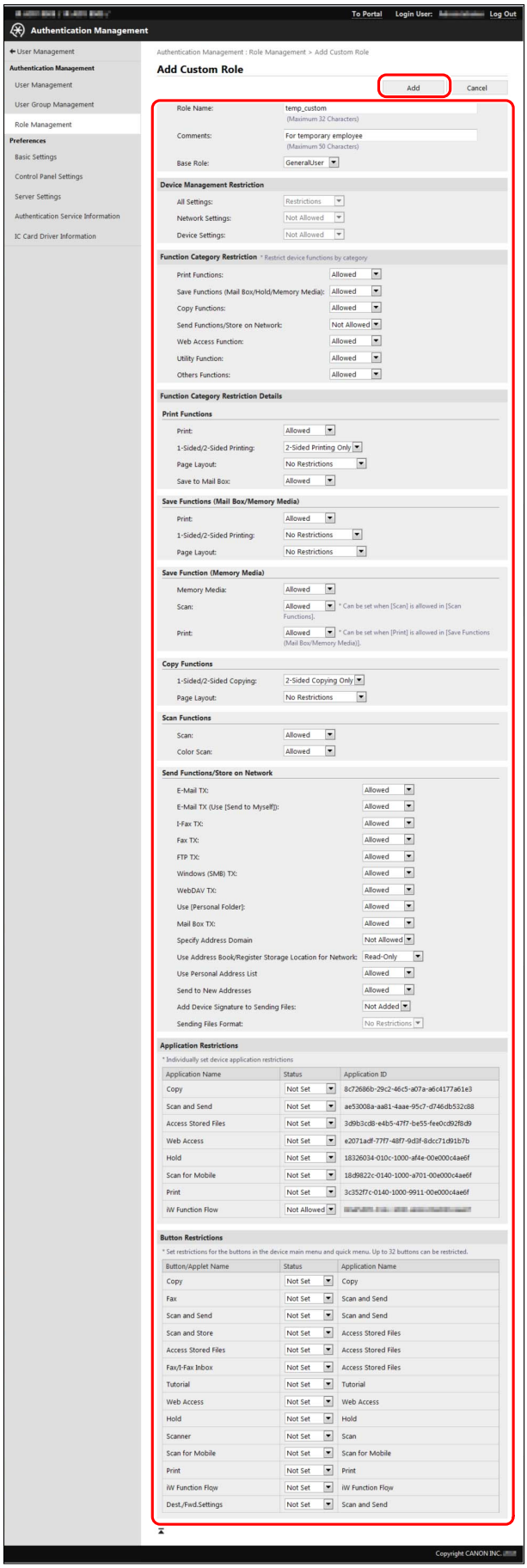
[Role Name]	temp_custom
[Comments]	For temporary employee
[Base Role]	[GeneralUser]
[Send Functions/Store on Network] in [Function Category Restriction]	[Not Allowed]
[1-Sided/2-Sided Printing] in [Print Functions] in [Function Category Restriction Details]	[2-Sided Printing Only]
[1-Sided/2-Sided Copying] in [Copy Functions] in [Function Category Restriction Details]	[2-Sided Copying Only]
[iW Function Flow] in [Application Restrictions]	[Not Allowed]

IMPORTANT

- In this example, since iW Function Flow is installed in Device_A, [iW Function Flow] is displayed in [Application Restrictions], and restrictions can be set.

NOTE

- For more information, see **"Managing Roles."(P. 62)**



The [temp_custom] role is registered.

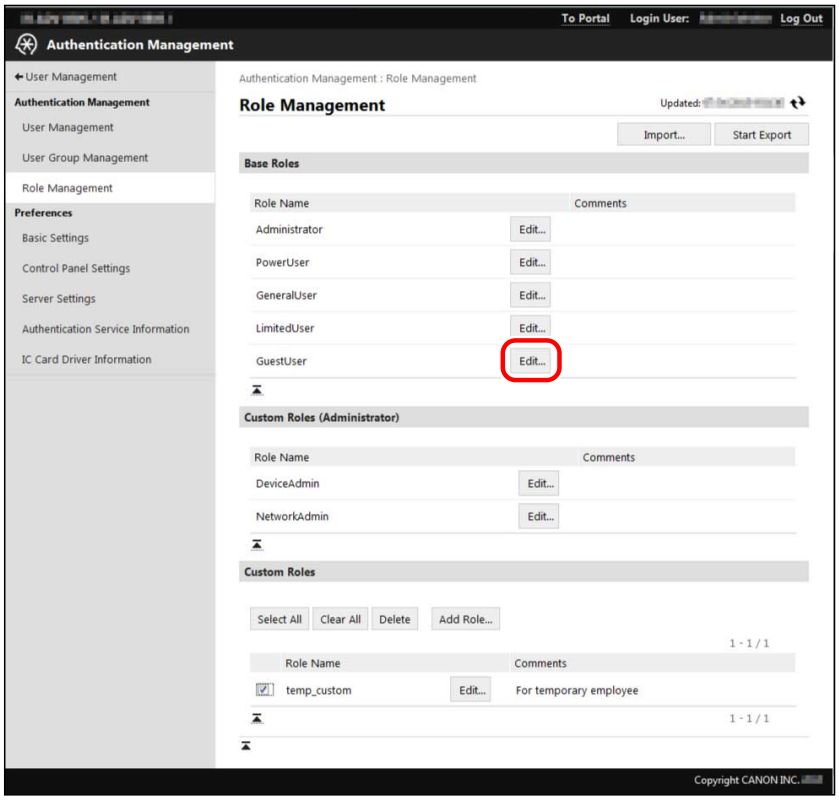
Editing [GuestUser] Role Registered

Confirm the content of the [GuestUser] role registered in Device_A, and set the application restrictions.

IMPORTANT

- If the restrictions applied to registered user ([GuestUser]) are stricter than those applied to unregistered users, the number of functions that can be used after logging in will be less than before logging in, which may lead to inappropriate user management.

1 Click [Edit] for [GuestUser] in [Base Roles].



2 Confirm the displayed information.

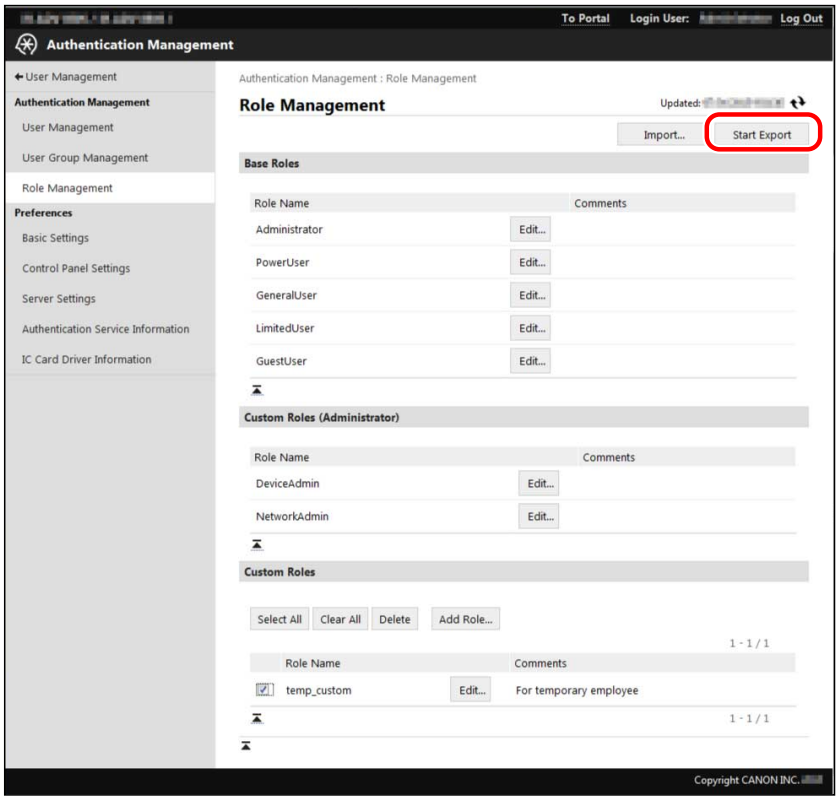
In this example, confirm that the content of the [GuestUser] role has not been changed. For information on each setting, see **"Device Function Restrictions."(P. 26)**

3 In [Application Restrictions], set [iW Function Flow] and [Scan and Send] to [Not Allowed] → click [Update].

Exporting Custom Roles

In this example, the roles in Device_A will be exported. All roles are exported to a file (not only the custom roles).

1 Click [Start Export] on the [Role Management] page.



2 Follow the instructions on the screen to specify the location to save the file.

The file is downloaded.

NOTE

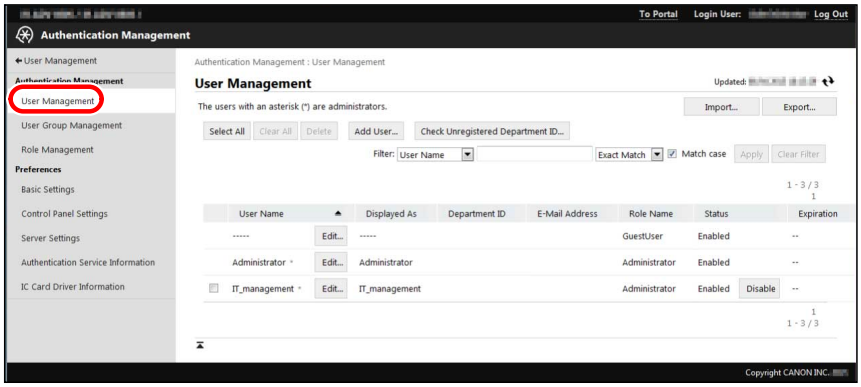
- The file extension is 'xml' and the default file name is 'roleData.xml'.

3 Click [Log Out].

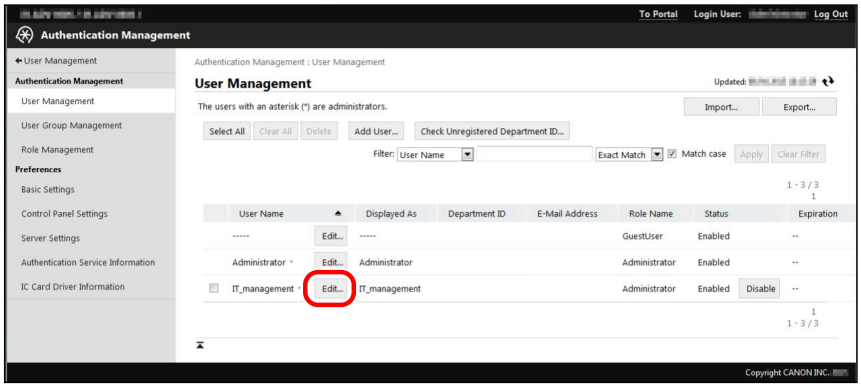
Registering Local Users and Specifying Roles

In this example, staff in the sales department (Manager A, Regular employee B, and Temporary employee C) will be registered in Device_A as local users, and assigned a role according to their title in the organization.

1 Click [Settings/Registration] → [User Management] → [Authentication Management] → [User Management].



2 Click [Edit] for the device restriction administrator.

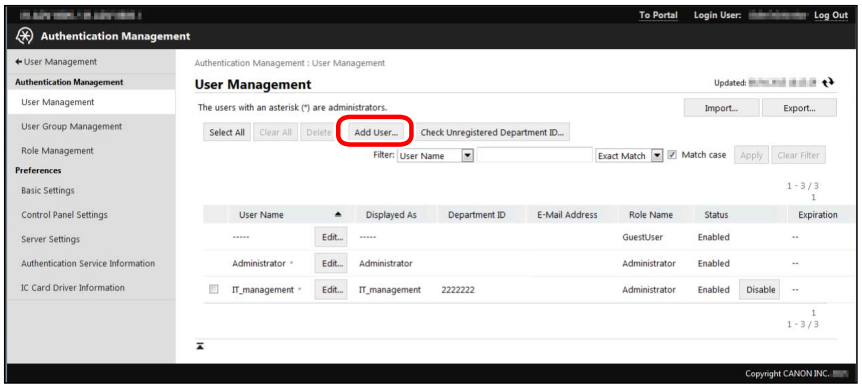


3 Specify the required settings → click [Update].

In this example, the following settings are specified:

[Department ID]	2222222
[PIN]	0000002

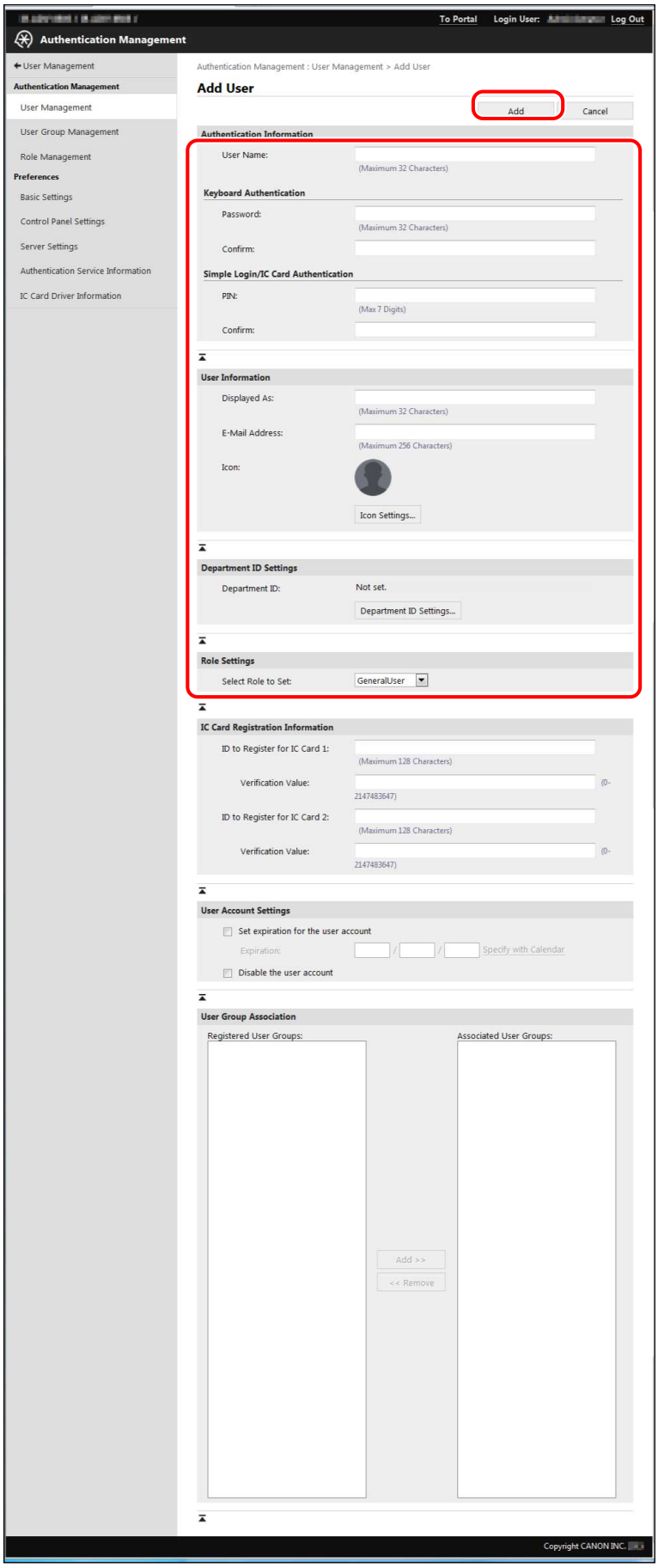
4 Click [Add User].



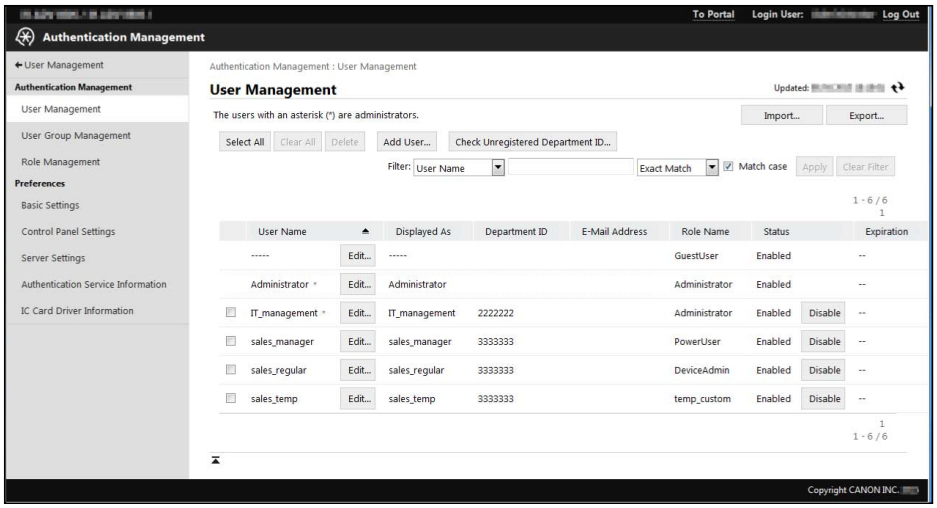
5 Enter the required settings → click [Add].

In this example, the following settings are specified:

Local User	Item	Description
Manager A	[User Name]	sales_manager
	[Password]	m_password
	[Department ID]	3333333
	[PIN]	0000003
	[Select Role to Set]	[PowerUser]
Regular employee B	[User Name]	sales_regular
	[Password]	r_password
	[Department ID]	3333333
	[PIN]	0000003
	[Select Role to Set]	[DeviceAdmin]
Temporary employee C	[User Name]	sales_temp
	[Password]	t_password
	[Department ID]	3333333
	[PIN]	0000003
	[Select Role to Set]	[temp_custom]



The user information is registered.



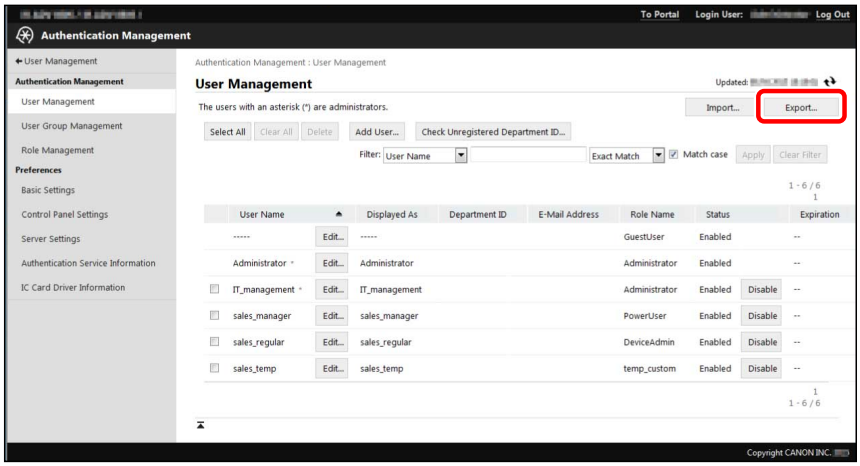
NOTE

- Users that are not device restriction administrators can change their own password. This enables increased security. The device restriction administrators should inform other users that they can change their own password. For more information changing the password, see the instruction manuals of the device.

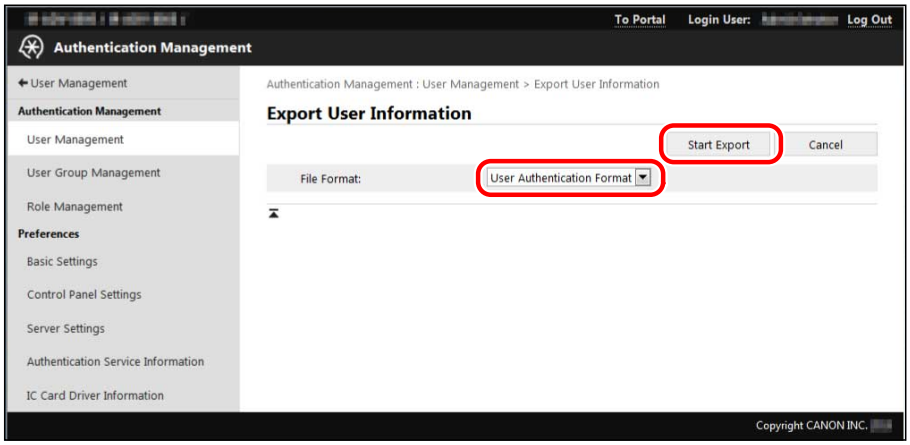
Exporting User Information

In this example, the user information in Device_A will be exported. The user information is exported with roles assigned to each user.

1 Click [Export] in [User Management] page.



2 Confirm that [User Authentication Format] is selected → click [Start Export].



3 Follow the instructions on the screen to specify the location to save the file.

The file is downloaded.

NOTE

- The file extension is 'csv' and the default file name is 'userData.csv'.

4 Click [Log Out].

Importing Roles and User Information

In this example, the role and user information exported from Device_A will be imported to Device_B and Device_C.

Importing Role and User Information(P. 103)

Importing Role and User Information

Import the role and user information to Device_B and Device_C.

Execute steps 1 to 12 for both Device_B and Device_C.

1 Open your Web browser → enter the following URL:

http://<IP address or host name of the device>

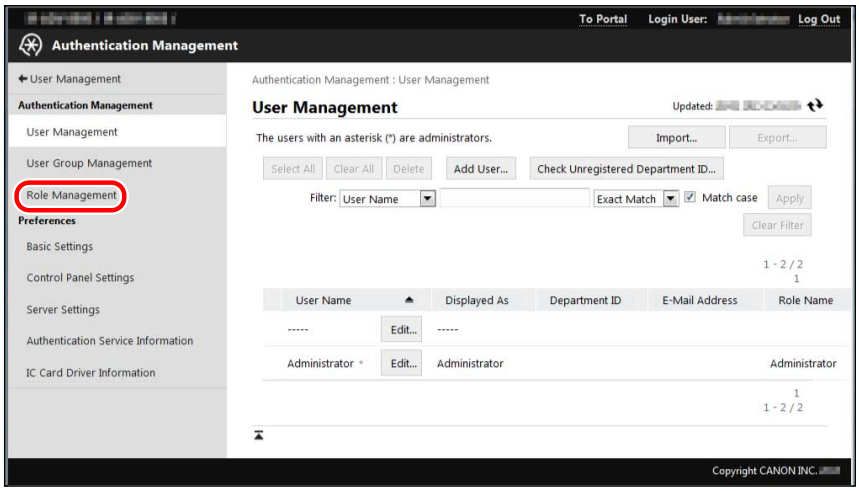
The [Login] page is displayed.

2 Enter the user name and password of the device restriction administrator → select [This device] in [Login Destination] → click [Log In].

In this example, the following settings are specified:

[User Name]	IT_management
[Password]	admin_password
[Login Destination]	[This device]

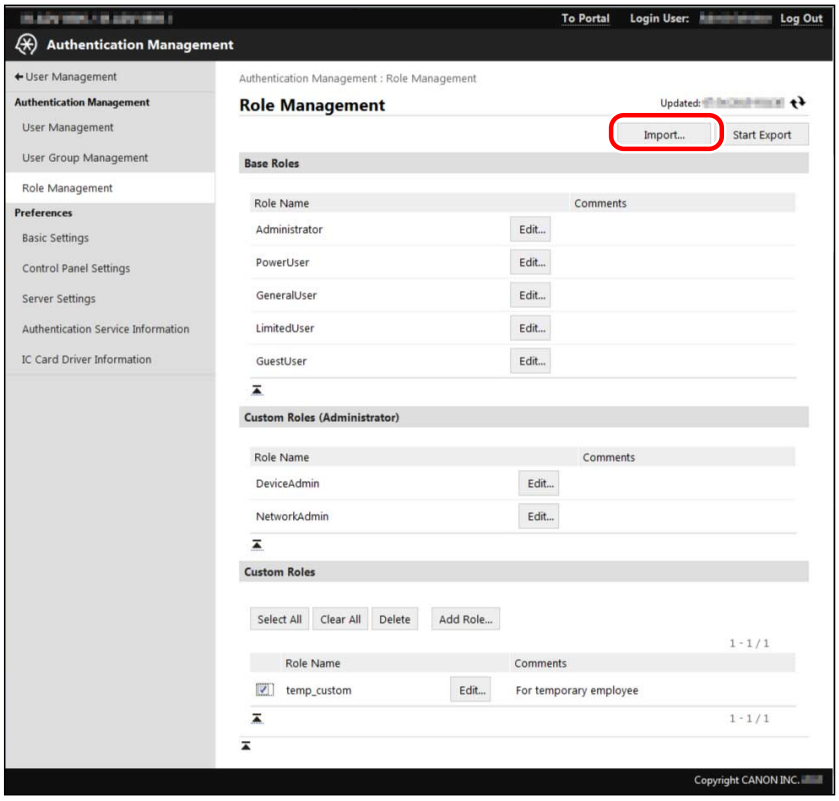
3 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].



IMPORTANT

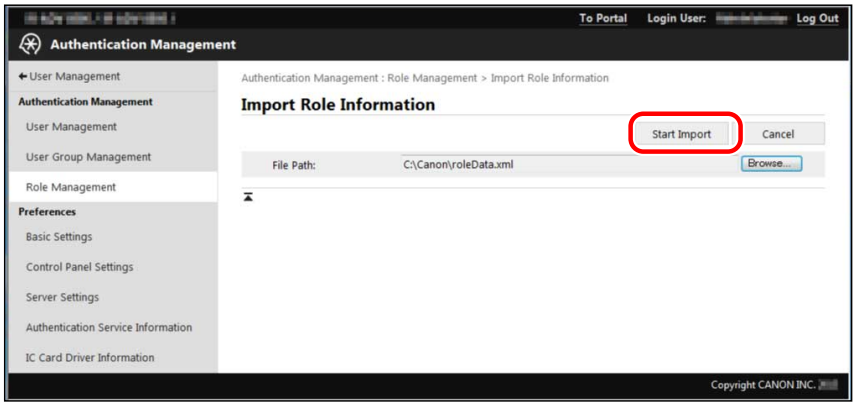
- If a role with the same name as a role to import already exists, that role is overwritten with the imported role information.

4 Click [Import].



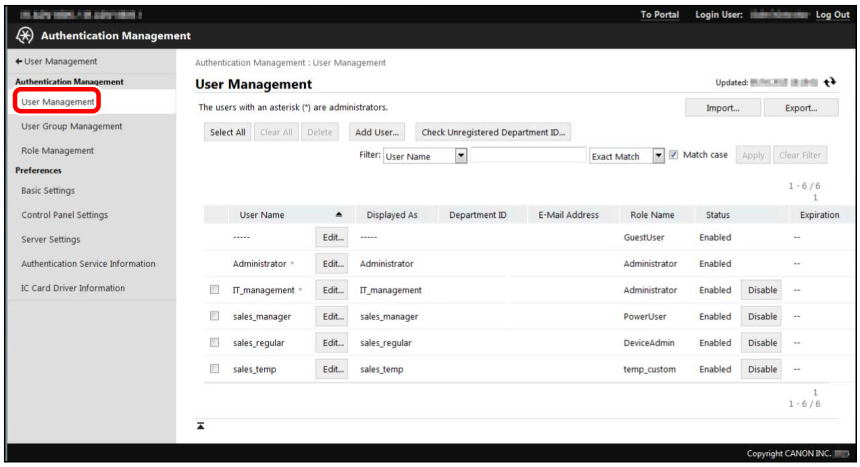
5 Click [Browse] to select the file to import.

6 Click [Start Import].



The role information is imported.

7 Click [User Management].



IMPORTANT

- If a user with the same name as a user to import already exists, that user information is overwritten with the imported user information.

8 Click [Import].

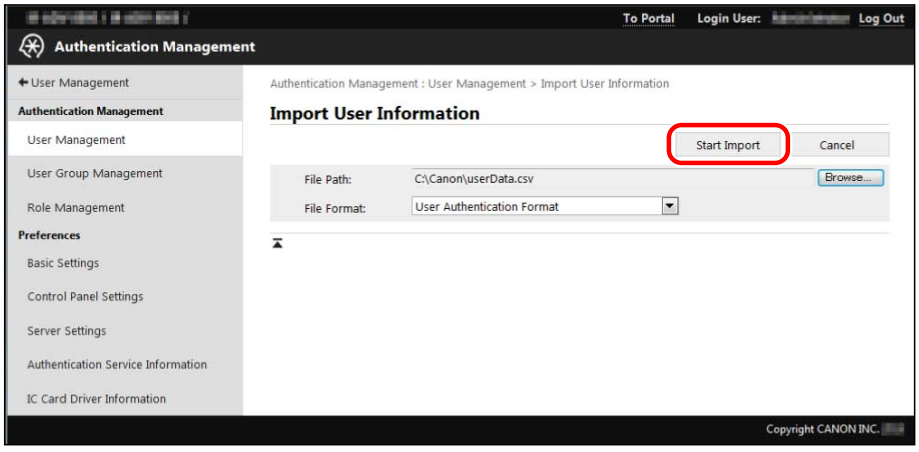
9 Click [Browse] to select the file to import.

10 Select [User Authentication Format] in [File Format].

NOTE

Files in a format other than [User Authentication Format] can also be imported. For more information, see the instruction manuals of the device.

11 Click [Start Import].



The user information is imported.

12 Click [Log Out].

Starting the Department ID Management Function

Start the Department ID Management function. In this example, the Department IDs for the sales department and system management department will be registered in the three devices.

Starting the Department ID Management Function(P. 106)

IMPORTANT

- Before starting the Department ID Management function, confirm that a Department ID is set in the user information for each user. If you start the Department ID Management function, users without a Department ID set in their user information will become unable to log in.

Starting the Department ID Management Function

In this example, the Department ID Management function will be started on devices.

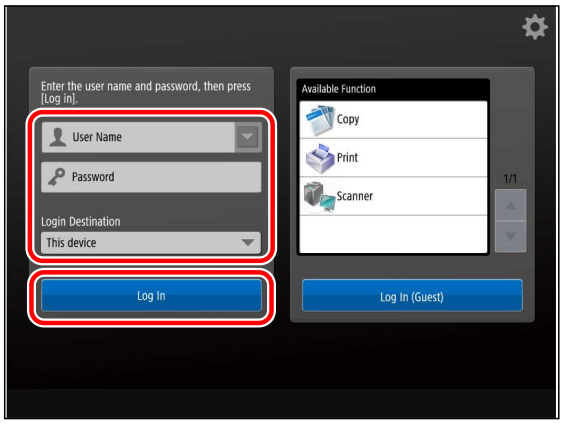
Starting the Department ID Management Function on Device_A and Device_C

Execute steps 1 to 9 for both Device_A and Device_C.

1 Enter the user name and password of the device restriction administrator → select [This device] in [Login Destination] → press [Log In].

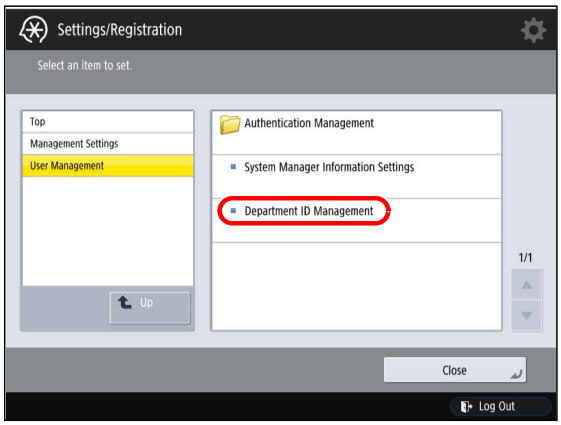
[User Name]	IT_management
[Password]	m_password
[Login Destination]	[This device]

Device_A

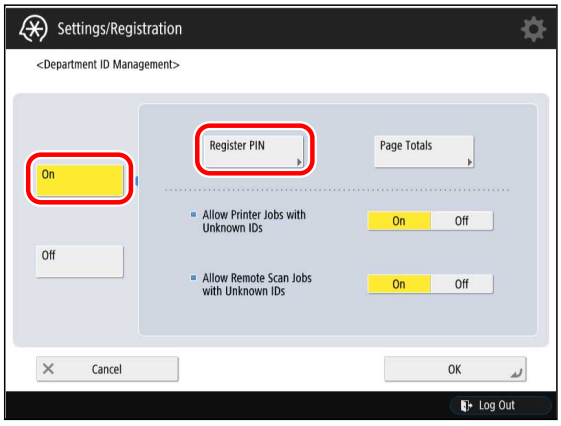


Device_C

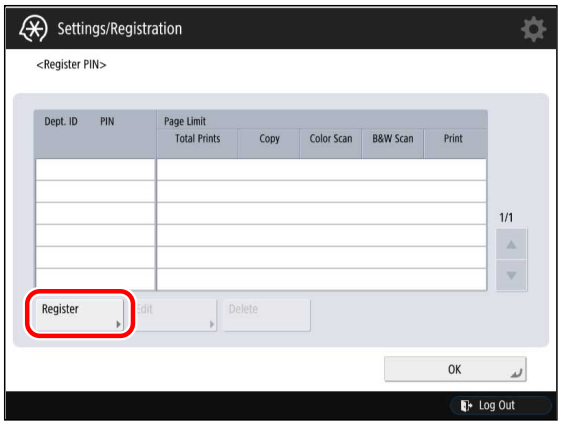
2 **Press (Settings/Registration) → [Management Settings] → [User Management] → [Department ID Management].**



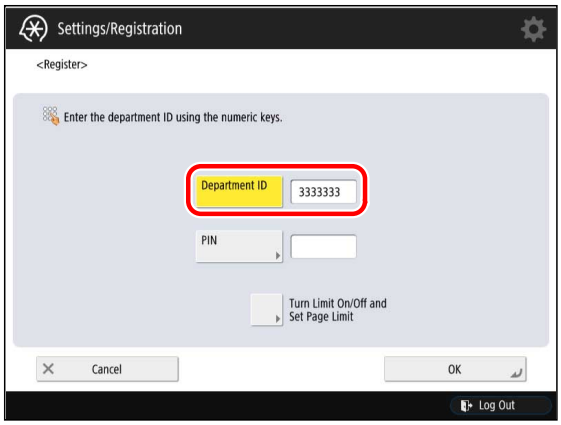
3 **Press [On] → [Register PIN].**



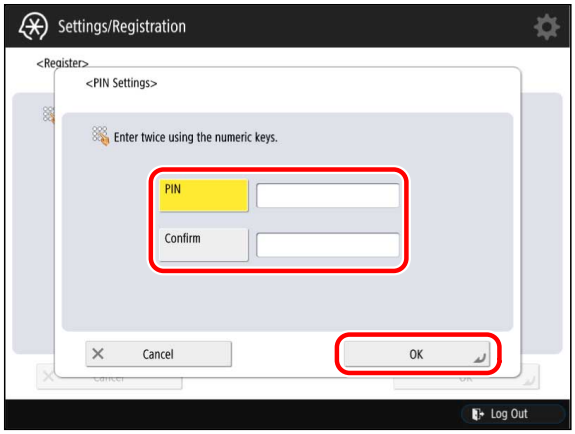
4 **Press [Register].**



5 Press [Department ID] → enter '3333333' (Department ID for the sales department).



6 Press [PIN] → enter '0000003' in [PIN] and [Confirm] → press [OK].



7 Press [OK].

8 Repeat steps 4 to 7 to register Department IDs of system management department.

[Department ID]	2222222
[PIN]	0000002

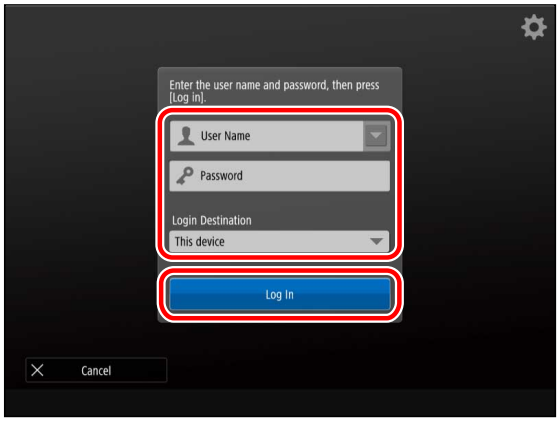
9 **Return to the [Main Menu] screen.**

Starting the Department ID Management Function on Device_B

1 **Press (Settings/Registration).**

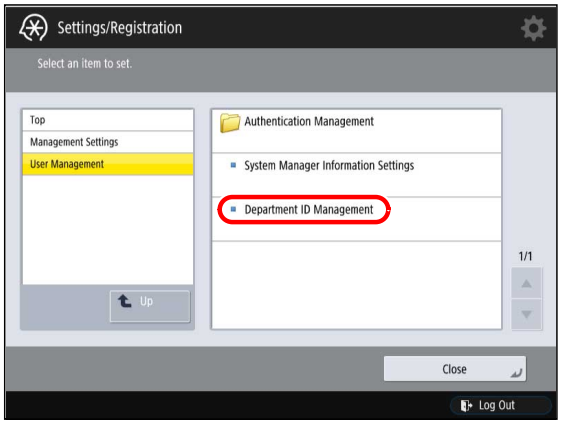
2 **Enter the user name and password of the device restriction administrator → select [This device] in [Login Destination] → press [Log In].**

[User Name]	IT_management
[Password]	m_password
[Login Destination]	[This device]

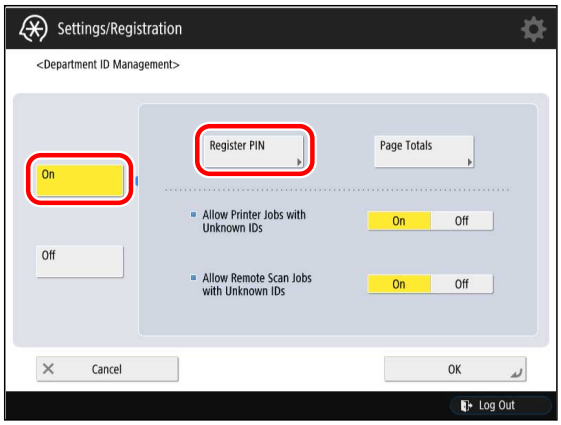


3 **Press [Device Settings].**

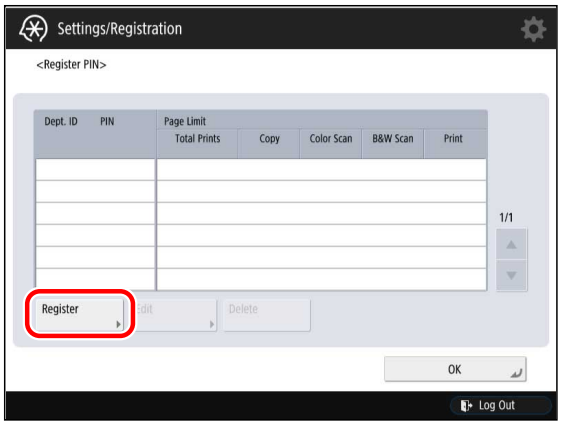
4 **Press [Management Settings] → [User Management] → [Department ID Management].**



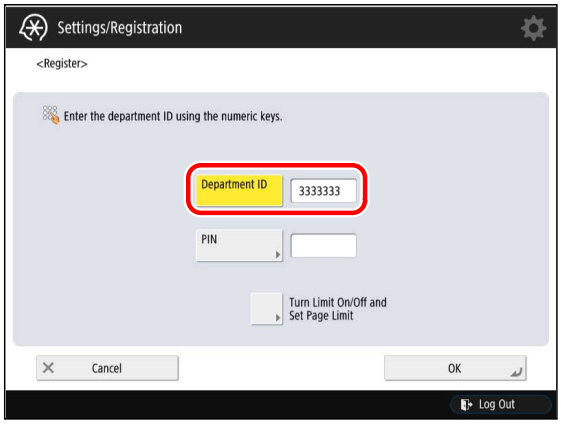
5 **Press [On] → [Register PIN].**



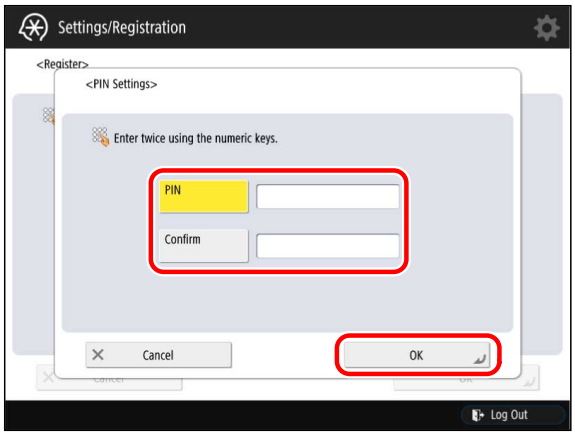
6 Press [Register].



7 Press [Department ID] → enter '3333333' (Department ID for the sales department).



8 Press [PIN] → enter '0000003' in [PIN] and [Confirm] → press [OK].



9 **Press [OK].**

10 **Repeat steps 6 to 9 to register Department IDs of system management department.**

[Department ID]	2222222
[PIN]	0000002

11 **Return to the [Main Menu] screen.**

Confirming the Login Method and Usage Restrictions on the Touch Panel Display

In this example, the devices will be checked to confirm that a Login screen with [Log In (Guest)] is displayed on Device_A, a screen with all the function buttons is displayed on Device_B, and a Login screen without [Log In (Guest)] is displayed on Device_C. The devices will also be logged in to with each user name to confirm that the device function restrictions and device management privileges are set correctly.

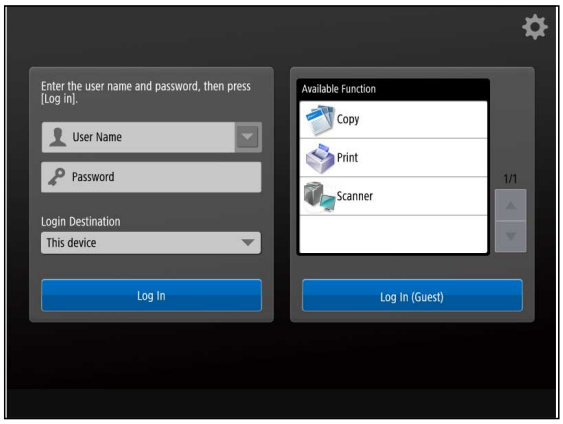
Confirming with Device_A and Device_C(P. 112)
Confirming with Device_B(P. 114)

Confirming with Device_A and Device_C

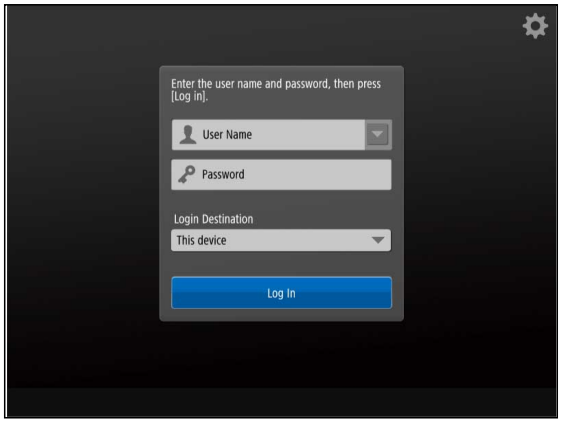
Execute steps 1 to 12 for both Device_A and Device_C.

1 Confirm that the following screen is displayed on the touch panel display.

Device_A



Device_C

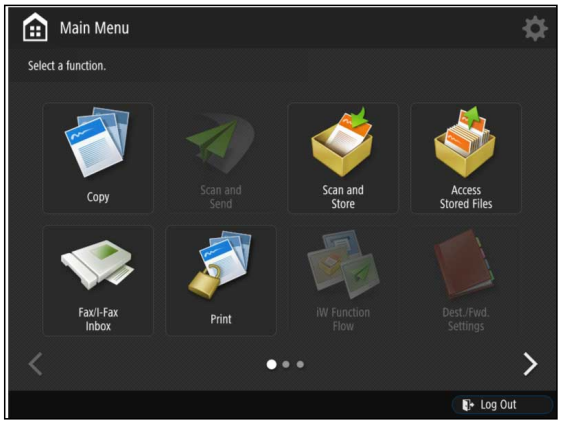


2 Enter the user name and password of a [sales_temp] user in [User Name] and [Password] → select [This device] in [Login Destination] → press [Log In].

[User Name]	sales_temp

[Password]	t_password
[Login Destination]	[This device]

3 Confirm [Scan and Send] and [iW Function Flow] cannot be used.



4 Press (Settings/Registration).

5 Confirm that [Function Settings] → [Send] → [Output Report] cannot be used.

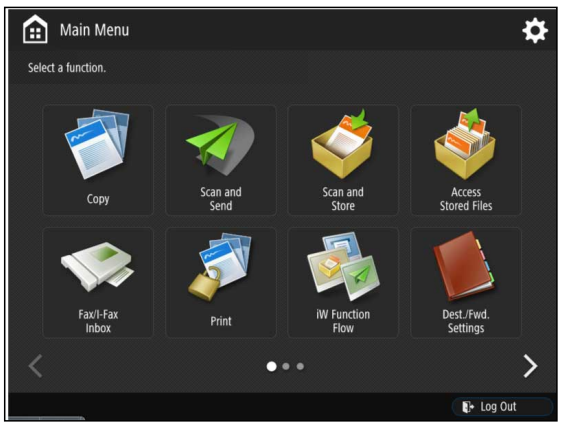
For information on the device screens, see the instruction manuals of the device.

6 Press (Log In/Out) to log out of the device that supports AMS.

7 Enter the user name and password of a [sales_regular] user in [User Name] and [Password] →select [This device] in [Login Destination] → press [Log In].

[User Name]	sales_regular
[Password]	r_password
[Login Destination]	[This device]

8 Confirm that [Scan and Send] and [iW Function Flow] can be used.



9 Press (Settings/Registration).

10 Confirm that [Function Settings] → [Send] → [Output Report] can be used.

For information on the device screens, see the instruction manuals of the device.

11 Press (Log In/Out) to log out of the device that supports AMS.

12 Log in with the other users and confirm that the device function restrictions and device management privileges are set correctly.

In this example, the following should be displayed for each user.

Device_A

User Name	Password	[Scan and Send] and [iW Function Flow]	[Output Report] in [Send] in [Function Settings]
sales_manager	m_password	Can be used.	Can be used.
sales_regular	r_password	Can be used.	Can be used.
sales_temp	t_password	Cannot be used.	Cannot be used.
IT_management	admin_password	Can be used.	Can be used.
Guest user	-	Cannot be used.	Cannot be used.

Device_C

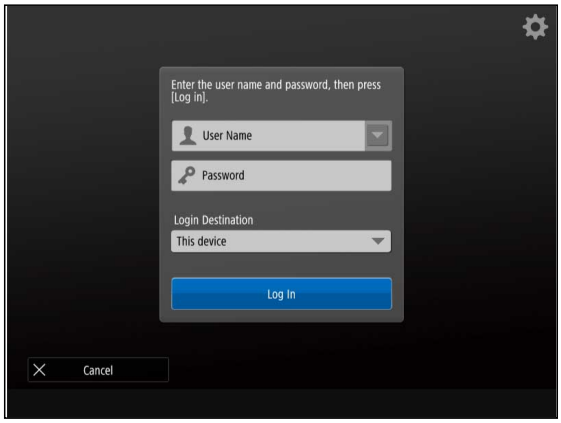
User Name	Password	[Scan and Send] and [iW Function Flow]	[Output Report] in [Send] in [Function Settings]
sales_manager	m_password	Can be used.	Can be used.
sales_regular	r_password	Can be used.	Can be used.
sales_temp	t_password	Cannot be used.	Cannot be used.
IT_management	admin_password	Can be used.	Can be used.

Confirming with Device_B

1 Confirm that the following screen is displayed on the touch panel display.

2 Press [Scan and Send].

3 Confirm that the Login screen is displayed.



4 Enter the user name and password of a [sales_temp] user in [User Name] and [Password] → select [This device] in [Login Destination] → press [Log In].

[User Name]	sales_temp
[Password]	t_password
[Login Destination]	[This device]

5 Confirm that [Scan and Send] cannot be used.

Also, confirm that [iW Function Flow] cannot be used.

6 Press (Settings/Registration) → [Log In].

The Login screen is displayed.

7 Enter the user name and password of a [sales_temp] user in [User Name] and [Password] → select [This device] in [Login Destination] → press [Log In].

[User Name]	sales_temp

[Password]	t_password
[Login Destination]	[This device]

8 Confirm that [Function Settings] → [Send] → [Output Report] cannot be used.

For information on the device screens, see the instruction manuals of the device.

9 Press (Log In/Out) to log out of the device that supports AMS.

10 Press [Scan and Send].

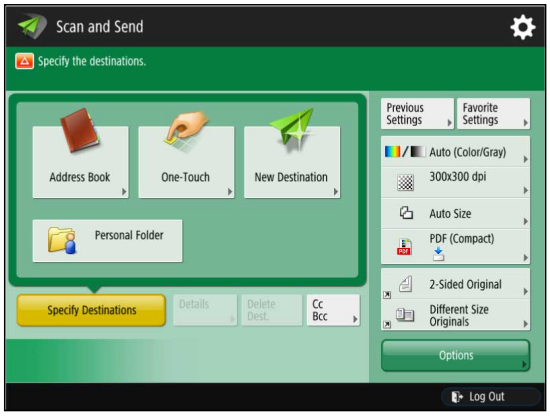
The Login screen is displayed.

11 Enter the user name and password of a [sales_regular] user in [User Name] and [Password] → select [This device] in [Login Destination] → press [Log In].

[User Name]	sales_regular
[Password]	r_password
[Login Destination]	[This device]

12 Confirm that [Scan and Send] screen is displayed.

Also, confirm that [iW Function Flow] screen is displayed.



13 Press (Settings/Registration).

14 Confirm that [Function Settings] → [Send] → [Output Report] can be used.

For information on the device screens, see the instruction manuals of the device.

15 Press (Log In/Out) to log out of the device that supports AMS.

16 Log in with the other users and confirm that the device function restrictions and device management privileges are set correctly.

In this example, the following should be displayed for each user.

User Name	Password	[Scan and Send] and [iW Function Flow]	[Output Report] in [Send] in [Function Settings]
sales_manager	m_password	Can be used.	Can be used.
sales_regular	r_password	Can be used.	Can be used.
sales_temp	t_password	Cannot be used.	Cannot be used.
IT_management	admin_password	Can be used.	Can be used.

Setting Up the Client Computers

To restrict printing from computers using the Access Management System, you must:

1. Enable the AMS function of the printer driver installed to the computers.

2. Set the user information.

Enabling the AMS Printer Driver Add-in(P. 118)
Setting User Information to the AMS Printer Driver Add-in(P. 119)
Setting Up Other Client Computers(P. 120)

In this example, three devices are used. Since all three are the same model, they use the same printer driver.

If you set user information on a single [AMS] page, that information is applied to all the AMS Printer Driver Add-in used from the computer that you are logged on to. This means you can complete the procedure for setting user information with a single operation.

IMPORTANT

- The AMS Printer Driver Add-in may not be included in some printer drivers. Use the latest version of the printer driver.
- If you are using a shared printer environment, enable the AMS function in the printer driver on the print server.
- If the date/time settings of all equipment that comprises the system (devices, client computers, server computers, etc.) do not match, printing may take longer, or you may be unable to print. For information on setting the date/time settings of the device, see the instruction manuals for the device.

Enabling the AMS Printer Driver Add-in

1 Log on to the computer as a user with Windows administrator privileges.

2 If you are using Windows 8.1/Windows Server 2012, move to the desktop.

3 Close all running applications.

4 Install the latest version of the printer driver that Device_A, Device_B, and Device_C use.

NOTE

- The latest installer of printer driver can be downloaded from the Canon Web site.
- If the printer driver is not installed with [Standard TCP/IP Port], it is recommended you update it with [Standard TCP/IP Port].

5 Add printer icons for Device_A, Device_B, and Device_C.

For more information, see the Windows instruction manuals.

6 Enable the AMS function of the printer driver that you added.

For details, see the instruction manuals of the printer driver.

Setting User Information to the AMS Printer Driver Add-in

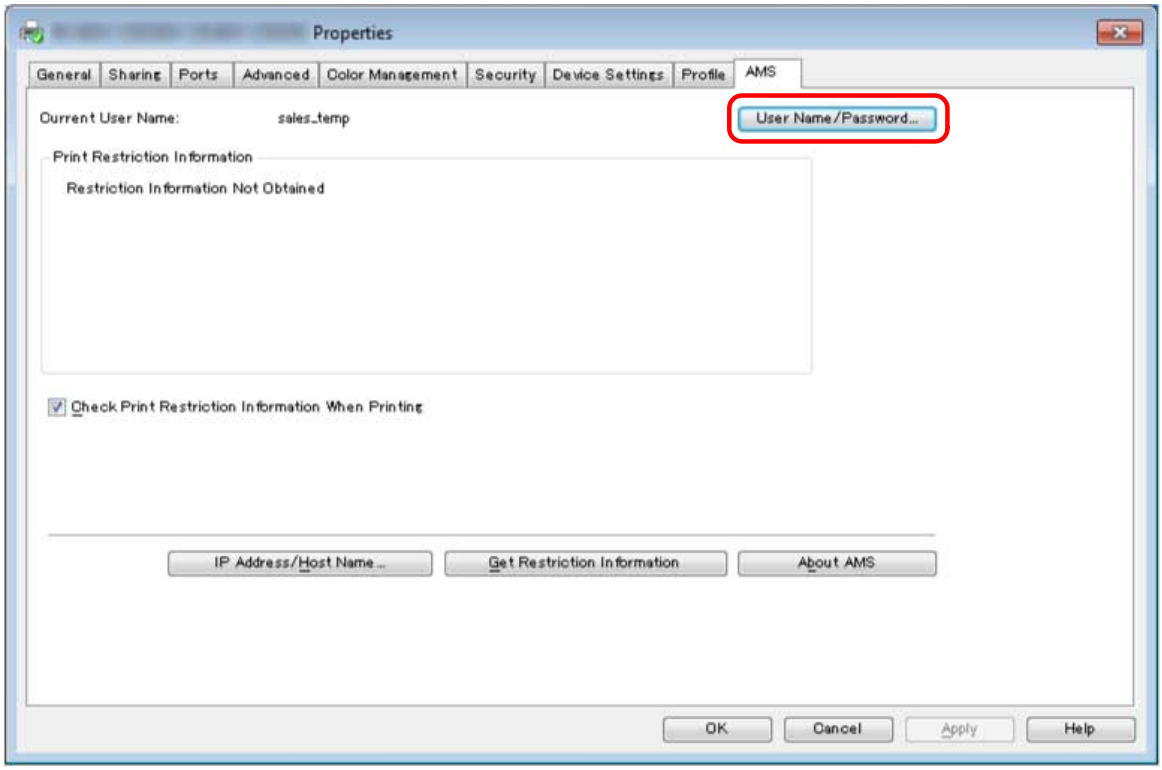
1 Log on to the computer where you enabled the AMS Printer Driver Add-in.

2 If you are using Windows 8.1/Windows Server 2012, move to the desktop.

3 Right-click the icon of Device_A → select [Properties].

4 Click the [AMS] tab.

5 Click [User Name/Password].



The [Setup User Names and Passwords for Authentication] dialog box is displayed.

6 Confirm that [This Device] is selected in [Authentication] → enter the user name and password of [sales_temp] in [User Name] and [Password] → click [OK].

[User Name]	sales_temp

[Password]	t_password

NOTE

- In this example, [Save password and skip authentication dialog box when printing] is enabled because [Save user authentication information] was selected in [Printer Driver Management] when specifying the preferences of the devices.

7 **Select [Check Print Restriction Information When Printing].**

8 **Click [OK] to close the dialog box.**

Setting Up Other Client Computers

Follow the procedures described in **"Enabling the AMS Printer Driver Add-in"(P. 118)** and **"Setting User Information to the AMS Printer Driver Add-in"(P. 119)** to set up the client computers for all users.

Confirming the Print Restrictions on Client Computers

Confirm that the specified print restriction information is being correctly applied on the client computers.

NOTE

- For details on the AMS Printer Driver Add-in, see the instruction manuals of the printer driver.

1 Log on to the computer of which the user name and password of [sales_temp] are set to the AMS Printer Driver Add-in.

2 Perform one-sided printing from an application of your choice.

The [Confirm Password for Authentication] dialog box is displayed.

NOTE

- In this example, [Confirm Password for Authentication] dialog box is because [Save password and skip authentication dialog box when printing] was not selected when setting the user information in the AMS Printer Driver Add-in.

3 Enter the password → click [OK].

[Password] : t_password

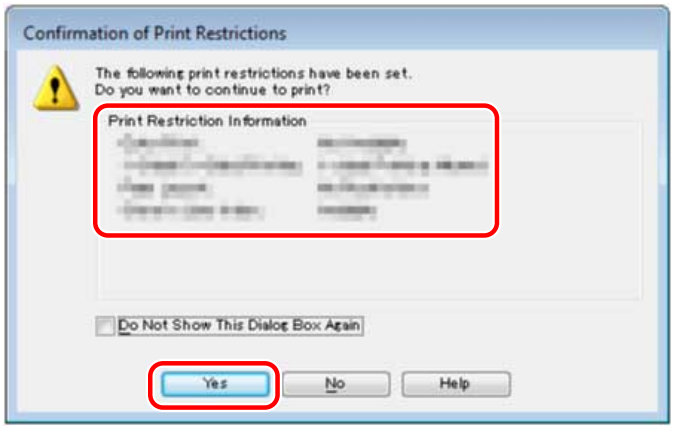
The [Confirmation of Print Restrictions] dialog box is displayed.

NOTE

- In this example, the [Confirmation of Print Restrictions] dialog box is displayed because [Check Print Restriction Information When Printing] was selected when setting the user information in the AMS Printer Driver Add-in.
- When you print from the Windows Store app in Windows 8.1/Server 2012, if you have configured the settings so that you are required to enter a password when printing, the message "The printer requires your attention. Go to the desktop to take care of it." is displayed. If this happens, move to the desktop and follow the instructions in the displayed dialog box.
  Note that the message will disappear after a while, but printing will not start until you have moved to the desktop and performed the operation displayed in the dialog box.

- If you select [Temporarily Save Password], you do not have to enter the password from the next time you print.

4 Confirm the displayed print restriction information → click [Yes].



Printing is executed.

NOTE

- When you print from the Windows Store app in Windows 8.1/Server 2012, if you have configured the settings so that you are required to confirm print restriction information when printing, the message "The printer requires your attention. Go to the desktop to take care of it." is displayed. If this happens, move to the desktop and follow the instructions in the displayed dialog box.
  Note that the message will disappear after a while, but printing will not start until you have moved to the desktop and performed the operation displayed in the dialog box.
- If you select [Do Not Show This Dialog Box Again], you can print without displaying this screen from the next time you print.

5 Confirm that the document is printed in two-sided.

6 Log in with the other users and confirm that the print restrictions are set correctly.

In this example, the following should be displayed for each user.

User Name	Password	[Color Print]	[1-Sided/2-Sided Printing]	[Page Layout]	[Store In User Inbox]
sales_manager	m_password	Available	1-sided Printing Allowed	No Restrictions	Available
sales_regular	r_password	Available	1-sided Printing Allowed	No Restrictions	Available
sales_temp	t_password	Not Available	2-sided Printing Only	No Restrictions	Available
IT_management	admin_password	Available	1-sided Printing Allowed	No Restrictions	Available
Guest user	Guest users cannot print from computers.				

NOTE

- Depending on your device, some restrictions may not be supported.

Canceling the Operation of the Access Management System

Canceling the Operation of the Access Management System

This section describes the procedure for canceling the operation of the Access Management System.

Flow of Canceling the Operation of the Access Management System

This section describes the flow of the procedure for canceling the operation of the Access Management System.

1. Disabling the AMS

Disable the AMS on all devices to cancel the operation of the Access Management System for.

For more information, see the instruction manuals of the device.

2. Disabling the AMS Printer Driver Add-in

Disable the AMS Printer Driver Add-in in the printer driver on the client computers.

For details, see the instruction manuals of the printer driver.

Troubleshooting

Troubleshooting

This section includes a list of error messages and troubleshooting.

List of Error Messages

This section describes the procedure for handling messages displayed when setting up or operating the Access Management System.

User Authentication(P. 128)
AMS Printer Driver Add-in(P. 128)

User Authentication

Before starting <application name>, pay attention to the following notes that concern the operations of other applications installed on the device.

Status 1	As this device application does not support AMS, detailed restrictions for each function cannot be set.
Remedy	Set the usage restrictions with [Application Restrictions] in the role information, as necessary.

Status 2	As a device application displayed in the application list does not support AMS, detailed restrictions for each function cannot be set.
Remedy	Set the usage restrictions with [Application Restrictions] in the role information, as necessary.

AMS Printer Driver Add-in

AMS Printer Driver Add-in Operations

The output may differ from the specified print settings, or the print job may be canceled because the following settings are in conflict with the print restrictions.
<Control Names>

Cause	A value specified by the user exceeds the value set for the print restrictions.
Remedy	Check the value set for the print restrictions. If the print job was canceled, specify the value again so that it does not exceed the value set for the print restrictions, and perform printing again. To check the values set for the print restrictions, click the [Get Restriction Information] button on the [AMS] page of the printer properties dialog box.

Could not obtain restriction information because the device is not responding.
Make sure that the device is turned on and try to obtain the information again later.
If the same error occurs, contact the administrator for details.

Status	Could not communicate with the device for an unspecified reason. There may be a problem with the communication environment, such as the network settings or network connection.

Remedy	Try retrieving the restriction information again after confirming that the power of the device is turned ON and the LAN cable, etc., is connected correctly. If you still cannot retrieve the information, contact the AMS administrator.

Could not obtain restriction information.

Status 1	There may be a problem with the communication environment, such as the network settings or connection status.
Remedy	After confirming the network settings, try retrieving the restriction information again. If the restriction information cannot be retrieved, contact your AMS administrator.

Status 2	AMS is disabled in the device.
Remedy	For information on enabling AMS in the devices, see the instruction manuals of the device.

The print restrictions have been updated. Try to print again.

Status	When print restriction information set in the AMS server has been updated.
Remedy	Check the value set for the print restrictions, and try printing again. To check the value set for the print restrictions, click the [Get Restriction Information] button on the [AMS] page of the printer properties dialog box.

Printing will be canceled because the following settings are in conflict with the print restrictions. <Control Names>

Status	In the print settings of the printer, settings that cannot be used in conjunction with the print restrictions set in the restriction information are set.
Remedy	Confirm the print restrictions, and try printing again. To check the value set for the print restrictions, click the [Get Restriction Information] button on the [AMS] page of the printer properties dialog box.

You do not have privileges to print using this device. Select a different printer.

Status	You do not have the privileges to print from the selected device.
Remedy	Get the device restriction administrator to assign privileges to print from the selected device to you, or select another device to print from.

Cannot set to [Store] because [Store In User Inbox] is set to [Not Available]. Printing will be canceled.

Status	[Store] is specified as the output method for printing. [Store In User Inbox] is not allowed in the print restrictions.
Remedy	Cancel the Store mode. Alternatively, contact the device restriction administrator.

The output may differ from the specified print settings because the following settings are in conflict with the print restrictions.
<Control Names>

Status	A value specified by the user exceeds the value set for the print restrictions. However, this message is displayed if a setting that cannot be used in conjunction with a compatible printer exceeds the print restriction.
Remedy	Check the value set for the print restrictions. To check the value set for the print restrictions, click the [Get Restriction Information] button on the [AMS] page of the printer properties dialog box.

Cannot print with booklet settings because [Page Layout] is set to [1-2 on 1 Not Available]. Change the settings and try again.

Status	Cannot perform booklet printing because of page layout restrictions.
Remedy	Cancel booklet printing. Alternatively, contact the device restriction administrator.

Cannot print in poster layout because [Page Layout] is set to [1 on 1 Not Available] or [1-2 on 1 Not Available].
Change the settings and try again.

Status	Cannot perform poster printing because of page layout restrictions.
Remedy	Cancel poster printing. Alternatively, contact the device restriction administrator.

Cannot print in poster layout because [1-Sided/2-Sided Printing] is set to [2-sided Printing Only].
Change the settings and try again.

Status	Cannot perform poster printing because of print restrictions.
Remedy	Cancel poster printing. Alternatively, contact the device restriction administrator.

Cannot set to [Store] because [Store In User Inbox] is set to [Not Available].
Change the settings and try again.

Status	[Store] is specified as the output method for printing. [Store In User Inbox] is not allowed in the print restrictions.
Remedy	Cancel the Store mode. Alternatively, contact the device restriction administrator.

Cannot print with booklet settings because [Page Layout] is set to [1-2 on 1 Not Available]. Printing will be canceled.

Status	Cannot perform booklet printing because of page layout restrictions.
Remedy	Cancel booklet printing. Alternatively, contact the device restriction administrator.

Cannot print in poster layout because [Page Layout] is set to [1 on 1 Not Available] or [1-2 on 1 Not Available].
Printing will be canceled.

Status	Cannot perform poster printing because of page layout restrictions.
Remedy	Cancel poster printing. Alternatively, contact the device restriction administrator.

Cannot print in poster layout because [1-Sided/2-Sided Printing] is set to [2-sided Printing Only].
Printing will be canceled.

Status	Cannot perform poster printing because of print restrictions.
Remedy	Cancel poster printing. Alternatively, contact the device restriction administrator.

Cannot create a form file or use overlay printing.
Printing will be canceled.

Status	Overlay printing or form file creation is specified in the print settings. Overlay printing or form file creation cannot be used.
Remedy	Cancel overlay printing or form file creation. Alternatively, contact the device restriction administrator.

Cannot obtain the device IP Address or host name.
Contact the administrator for details.

Status	Could not retrieve the IP address or host name of the device.
Remedy	If a user with Windows administrator privileges is logged in, specify the IP address/host name of the device in the [Set IP Address/Host Name] dialog box. If the setting cannot be specified, contact your AMS administrator.

Cannot obtain restriction information because network settings are incorrect.
Contact the administrator for details.

Status	The IP address or host name set in the AMS Printer Driver Add-in is incorrect, or there is a problem in the network settings.
Remedy	Check the IP address/host name settings in the [Set IP Address/Host Name] dialog box and the network settings, and retrieve the restriction information again. If you still cannot retrieve the information, contact the AMS administrator.

Cannot create a form file or use overlay printing.
Change the settings.

Status	Overlay printing or form file creation is specified in the print settings. Overlay printing or form file creation cannot be used.

Remedy	Cancel overlay printing or form file creation, or contact your device restriction administrator.

Cannot obtain restriction information because network settings are incorrect.
Contact the administrator for details.
Printing will be canceled.

Status	The IP address or host name set in the AMS Printer Driver Add-in is incorrect, or there is a problem in the network settings.
Remedy	Check the IP address/host name settings in the [Set IP Address/Host Name] dialog box and the network settings, and try printing again. If you still cannot print, contact the AMS administrator.

Could not obtain restriction information because the device is not responding.
Printing will be canceled.
Make sure that the device is turned on and try to print again later.
If the same error occurs, contact the administrator for details.

Status	Could not communicate with the device for an unspecified reason. There may be a problem with the communication environment, such as the network settings or network connection.
Remedy	Try printing again after confirming that the power of the device is turned ON and the LAN cable, etc., is connected correctly. If you still cannot print, contact the AMS administrator.

Cannot print with perfect binding settings because [Page Layout] is set to [1 on 1 Not Available] or [1-2 on 1 Not Available].
Change the settings and try again.

Status	Cannot print with the Perfect Binding mode because of page layout restrictions.
Remedy	Cancel the Perfect Binding mode. Alternatively, contact the device restriction administrator.

Cannot print with perfect binding settings because [Page Layout] is set to [1 on 1 Not Available] or [1-2 on 1 Not Available].
Printing will be canceled.

Status	Cannot print with the Perfect Binding mode because of page layout restrictions.
Remedy	Cancel the Perfect Binding mode. Alternatively, contact the device restriction administrator.

Could not set the user information.

Status	User information could not be retrieved, for an unspecified reason.
Remedy	Try retrieving the user information again after waiting a while. If you still cannot set the user information, contact the AMS administrator.

Could not obtain the device IP address or the host name.

Status	Could not retrieve the IP address or host name of the device.
Remedy	Enter the IP address or host name in the [Device IP Address/Host Name] text box.

Cannot set to [Hold] because [Store In User Inbox] is set to [Not Available]. Printing will be canceled.

Status	[Hold] is specified as the output method for printing. [Store In User Inbox] is not allowed in the print restrictions.
Remedy	Cancel the Hold mode. Alternatively, contact the device restriction administrator.

Cannot set the output method as selected because [Store In User Inbox] is set to [Not Available]. Printing will be canceled.

Status	[Store] or [Hold] is specified as the output method for printing. [Store In User Inbox] is not allowed in the print restrictions.
Remedy	Deselect the Store or Hold mode. Alternatively, contact the device restriction administrator.

Cannot set to [Hold] because [Store In User Inbox] is set to [Not Available]. Change the settings and try again.

Status	[Hold] is specified as the output method for printing. [Store In User Inbox] is not allowed in the print restrictions.
Remedy	Cancel the Hold mode. Alternatively, contact the device restriction administrator.

Cannot set the output method as selected because [Store In User Inbox] is set to [Not Available]. Change the settings and try again.

Status	[Store] or [Hold] is specified as the output method for printing. [Store In User Inbox] is not allowed in the print restrictions.
Remedy	Deselect the Store or Hold mode. Alternatively, contact the device restriction administrator.

The [Device IP Address/Host Name] has not been entered. Enter the [Device IP Address/Host Name].

Status	[OK] was clicked without specifying [Device IP Address/Host Name].
Remedy	Specify [Device IP Address/Host Name] before clicking [OK].

Could not set the user information because the network settings are incorrect. Contact the administrator for details.

Status	The IP address or host name set in the AMS Printer Driver Add-in is incorrect, or there is a problem in the network settings.
Remedy	Check the IP address/host name settings in the [Set IP Address/Host Name] dialog box and the network settings, and retrieve the user information again. If you still cannot retrieve the information, contact the AMS administrator.

Could not set the user information because the device is not responding. Make sure that the device is turned on and try to set the information again later. If the same error occurs, contact the administrator for details.

Status	Could not communicate with the device for an unspecified reason. There may be a problem with the communication environment, such as the network settings or network connection.
Remedy	Try setting the user information again after confirming that the power of the device is turned ON and the LAN cable, etc., is connected correctly. If you still cannot set the user information, contact the AMS administrator.

Characters that cannot be used have been entered for the Domain Name [Authentication]. Check the entered characters.

Status	If you are using local device authentication, an authentication server other than [This Device] is selected in [Authentication]. If you are using Active Directory authentication, invalid characters are used in the domain name entered in [Authentication].
Remedy	If you are using local device authentication, select [This Device] in [Authentication]. If you are using Active Directory authentication, confirm and enter the correct domain name.

The set user information and obtained restriction information do not match. Set the user information again. For Domain Authentication, enter the NetBIOS domain name in [Authentication].

Status	The user information set for the AMS Printer Driver Add-in and the user information set in the retrieved restriction information does not match.
Remedy	Check the user information specified in the [Setup User Names and Passwords for Authentication] dialog box. Select [This Device] in [Authentication] for local device authentication. Select the NetBIOS domain name for Active Directory authentication.

The set user information and obtained restriction information do not match. Set the user information again.

Status	The user information set for the AMS Printer Driver Add-in and the user information set in the retrieved restriction information does not match.

Remedy	Check the user information specified in the [Setup User Names and Passwords for Authentication] dialog box. Select [This Device] in [Authentication] for local device authentication. Select the NetBIOS domain name for Active Directory authentication.

The set user information and obtained restriction information do not match. Printing will be canceled.

Status	The user information set for the AMS Printer Driver Add-in and the user information set in the retrieved restriction information does not match.
Remedy	Check the user information specified in the [Setup User Names and Passwords for Authentication] dialog box. Select [This Device] in [Authentication] for local device authentication. Select the NetBIOS domain name for Active Directory authentication.

The account is locked out. Try to authenticate the account later, or contact the administrator for details.

Status	The user account that is used for authentication in the [Setup User Names and Passwords for Authentication] dialog box is locked out.
Remedy	Try to authenticate again after waiting a while. If you still cannot authenticate, contact the device restriction administrator.

Could not obtain restriction information because the account is locked out. Try to obtain it later, or contact the administrator for details.

Status	The user account that is used for authentication to obtain restriction information is locked out.
Remedy	Try to authenticate again after waiting a while. If you still cannot obtain restriction information, contact the device restriction administrator.

Could not obtain restriction information because the account is locked out. Printing will be canceled. Try to print later, or contact the administrator for details.

Status	The user account that is used for authentication for printing is locked out.
Remedy	Try to print again after waiting a while. If you still cannot print, contact the device restriction administrator.

Troubleshooting

This section explains how to handle any trouble you may have in operating the Access Management System.

Users set to [1-2 on 1 Not Available] cannot output inbox documents.

Cause	If you merge documents with different page layout settings (for example, a 2 On 1 document and a 4 On 1 document) and save them in an inbox, the page layout settings are reset and they are saved as a 1 On 1 document. Therefore, users set to [1-2 on 1 Not Available] cannot output the document.
Remedy	When saving documents that may be output by users with page layout restrictions applied, do not merge documents with different page layout settings.

List of Error Codes

When a job or operation ends in an error, confirm the error code, and perform the required operation according to the error code. Error codes can be checked on the detailed information screen for the job log, from the System Monitor screen or [Status Monitor/Cancel] screen.

NOTE

- "#817" is displayed on a device that sends a Cascade Copy job to a restricted device.
- "#866" is displayed on a device that is sent a job from a computer.

#817

Status	The job was canceled because the device that supports AMS set as the destination for Cascade Copy is set to not allow the reception of Cascade Copy jobs.
Remedy	Set to allow the reception of Cascade Copy jobs in the device that supports AMS set as the destination for Cascade Copy. For more information, see the instruction manuals of the device. If you do not want to allow the reception of Cascade Copy jobs in the device that supports AMS, on the source device, cancel the registration as the destination printer for Cascade Copy.

#866

Status	A job with a security violation error was detected.
Remedy	Check the content of the job.

Appendix

Appendix

This section includes security precautions and list of port numbers.

Regarding Security when Operating the Access Management System

The Access Management System is a system for restricting the use of device functions for the purpose of reducing costs and preventing information leaks.

To maintain security of the device usage environment after adopting the Access Management System, it is recommended you consider the following security policies when operating the system.

User Management

Even when not using Active Directory, make sure to manage user accounts. For example, avoid having multiple users logging in to devices with a single user account. Matching the login user name used for the device and the computer enables you to perform more strict user management.

Computer Administrator Privilege Management

Manage computer administrator privileges. For example, if a user with Windows administrator privileges logs on and disables the AMS Printer Driver Add-in, the Access Management System cannot restrict printing.

When operating the Access Management System with domain authentication, it is recommended you make the users log in to a domain when logging on to a computer.

Device Management

Manage devices that do not support AMS (devices that cannot be restricted) individually. For example, even if you restrict color output and sending externally for devices that support AMS, users can use these functions with devices that are not managed with the Access Management System.

It is recommended that you place devices not managed with the Access Management System close to administrators and perform security management.

Updating the Key Pair for Access Control

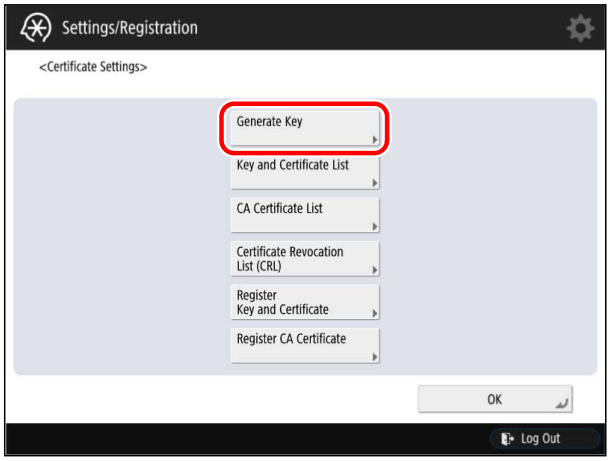
Periodically update the key pair as necessary, for improved security. This section describes the procedure for updating the key pair for access control.

If you want to print soon after updating the key pair, first click [Get Restriction Information] on the [AMS] page of the Printer Properties dialog box to retrieve print restriction information. An error will occur if the AMS Printer Driver Add-in tries to print using print restriction information retrieved before updating the key pair. Note that documents that are prohibited from being printed more than once can no longer be printed. (Print restriction information is automatically retrieved approximately 30 minutes after updating the key pair, enabling normal printing.)

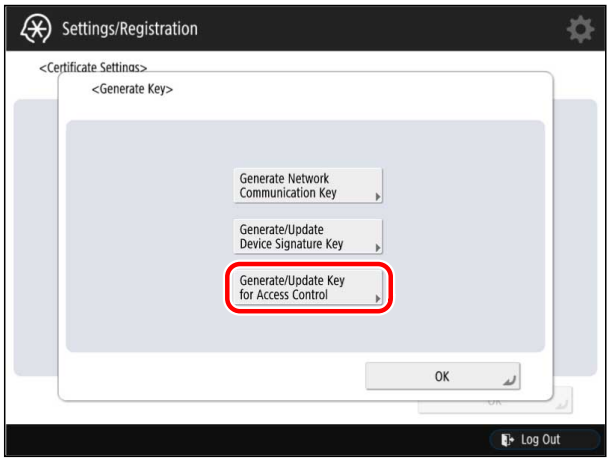
Updating the Key Pair for Access Control(P. 141)

Updating the Key Pair for Access Control

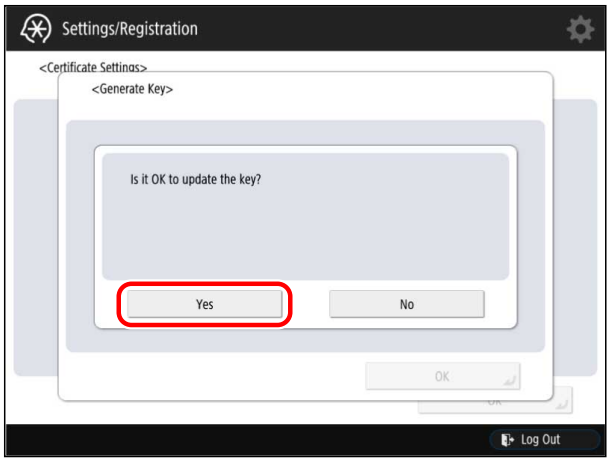
1 Press (Settings/Registration) → [Management Settings] → [Device Management] → [Certificate Settings] → [Generate Key].



2 Press [Generate/Update Key for Access Control].



3 Press [Yes].



4 After returning to the [Main Menu] screen, restart the device.

The key pair is updated.

IMPORTANT

- The key pair is updated after the device is restarted. For information on restarting the device, see the instruction manuals of the device.

Other Precautions

This section describes other precautions to take when operating the Access Management System.

Using the Access Management System in Conjunction with the Department ID Management Function

When operating the User Authentication with Active Directory authentication method or LDAP authentication method, the Department ID Management function cannot be used in conjunction with the Access Management System.

For more information on Department ID Management function, see the instruction manuals included with the device.

Canceling Jobs

If a user logs out from a restricted device that supports AMS during any of the following processes, jobs will be canceled, regardless of the role associated with the user.

- While scanning
- While confirming the progress of a job merge for copying
- While confirming the progress of a test copy
- While previewing the document to send

Remote UI Restrictions

An error screen is displayed if users other than the following log in to a restricted device that supports AMS and clicks a button other than [To Portal] and [Status Monitor/Cancel].

- A user associated with the [Administrator]/[DeviceAdmin]/[NetworkAdmin] role
- A user associated with a role set to have no items restricted

Remote UI Address Book

For models with User Authentication, you can set usage restrictions for the Address Book (Address List management function) provided on the Remote UI.
Set restrictions from [Use Address Book/Register Storage Location for Network] of a role.

Direct Printing from the Remote UI

For models with User Authentication, you can set restrictions for the Direct Print function (for printing without using a printer driver) provided on the Remote UI in the preferences of the devices.
If you select [Print from drivers without AMS Printer Driver Add-in] for [Functions to Restrict] in the preferences of the devices, you cannot use the Direct Print function.
If you do not select [Print from drivers without AMS Printer Driver Add-in] for [Functions to Restrict] in the preferences of the devices, you can use the Direct Print function. However, you cannot set detailed usage restrictions such as restricting color printing.

Cascade Copy Function Restrictions

A restricted device that supports AMS cannot be set as the device to send the data for Cascade Copy. The keys related to Cascade Copy are restricted as indicated below.

- [Options] → [Cascade Copy] is not displayed on the Copy Basic Features screen.
- [Register Remote Device for Cascade Copy] is disabled on the [Settings/Registration] screen.

Restrictions on [Settings/Registration]

Some settings for [Settings/Registration] of devices are restricted and will not be displayed when the AMS is running on those devices. For more information, see **"Restrictions on [Settings/Registration]."(P. 24)**

Restrictions on [Limit New Destinations] in [Settings/Registration]

[Limit New Destinations] in [Settings/Registration] is unavailable on devices in which the AMS is running. The settings become disabled and are not displayed. Even if you disable the AMS, the settings will not automatically return to the original configuration. It is necessary to configure the settings again.
On devices in which the AMS is running, similar restrictions can be configured for each user in the [Send to New Addresses] restricted item inside the role.

Restrictions on [Address Book PIN] in [Settings/Registration]

[Address Book PIN] in [Settings/Registration] is unavailable on devices in which the AMS is running. The PIN is cleared and will not be displayed. Even if you disable the AMS, the PIN will not automatically return to the original settings. It is necessary to configure the settings again.

On devices in which the AMS is running, similar restrictions on the address book can be configured for each user in the [Use Address Book/Register Storage Location for Network] restricted item inside the role.

Restrictions on Overlay Printing

Creating a Form File and Overlay Printing cannot be used from the printer driver for devices in which the AMS is running.

Restrictions on Faxing

The Direct Send and On-Hook fax features cannot be used on devices in which the AMS is running.

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at: http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are not met.

DISCLAIMER
THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.