



# **ACCESS MANAGEMENT SYSTEM**

## **Administrator Guide**

# Contents

<b>Preface</b> .....	2
About This Manual .....	3
Trademarks .....	7
Copyright .....	8
Disclaimers .....	9
<b>Introduction</b> .....	11
Main Functions .....	12
User Authentication Methods and Managed Users .....	17
Structure of Usage Restrictions .....	19
Regarding Base Roles and Custom Roles .....	20
Device Management Privileges .....	23
Device Function Restrictions .....	26
Access Management System Configurations .....	34
Administrators for the Access Management System .....	36
System Requirements .....	38
<b>Setting Up the Access Management System</b> .....	41
Flow of Settings for Operating with Local Device Authentication .....	42
Flow of Settings for Operating with Server Authentication .....	44
Preparing the Device and Network Environment .....	46
Logging in to User Authentication .....	49
Specifying the Preferences of the Devices .....	50
Specifying the Device Preferences Using User Authentication .....	51
Managing Roles .....	64
Managing Roles Using User Authentication .....	65
<b>Setting Up the Client Computers</b> .....	77
Installing the AMS Printer Driver Add-in .....	78
Setting User Information to the AMS Printer Driver Add-in .....	85
<b>Operation Example of Local Device Authentication</b> .....	90
Example of Operating with Local Device Authentication .....	91
Flow of Operations .....	93
Preparing the Device and Network Environment .....	95
Specifying the Preferences of the Devices .....	96
Creating Custom Roles .....	105
Exporting Custom Roles .....	109
Registering Local Users and Specifying Roles .....	110
Exporting User Information .....	114

Importing Roles and User Information .....	115
Starting the Department ID Management Function .....	118
Confirming the Login Method and Usage Restrictions on the Touch Panel Display .....	124
Setting Up the Client Computers .....	130
Confirming the Print Restrictions on Client Computers .....	138
<b>Canceling the Operation of the Access Management System .....</b>	<b>141</b>
Flow of Canceling the Operation of the Access Management System .....	142
Uninstalling the AMS Printer Driver Add-in .....	143
<b>Troubleshooting .....</b>	<b>146</b>
List of Error Messages .....	147
Troubleshooting .....	167
List of Error Codes .....	169
<b>Appendix .....</b>	<b>171</b>
Regarding Security when Operating the Access Management System .....	172
Updating the Key Pair for Access Control .....	173
Other Precautions .....	175

# Preface

<b>Preface</b> .....	2
<b>About This Manual</b> .....	3
<b>Trademarks</b> .....	7
<b>Copyright</b> .....	8
<b>Disclaimers</b> .....	9

## 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(P. 3)**
- ▶ **Symbols Used in This Manual(P. 3)**
- ▶ **Buttons Used in This Manual(P. 4)**
- ▶ **Displays Used in This Manual(P. 4)**
- ▶ **Abbreviations Used in This Manual(P. 5)**
- ▶ **Terms Used in This Manual(P. 5)**
- ▶ **Key/Button Names(P. 6)**

## 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.



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:

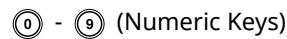
- Device Touch Panel Display Keys: [Key Name]

Examples: [Log In]

[OK]

- Control Panel Keys: Key Icon (Key Name)

Examples:



- 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.

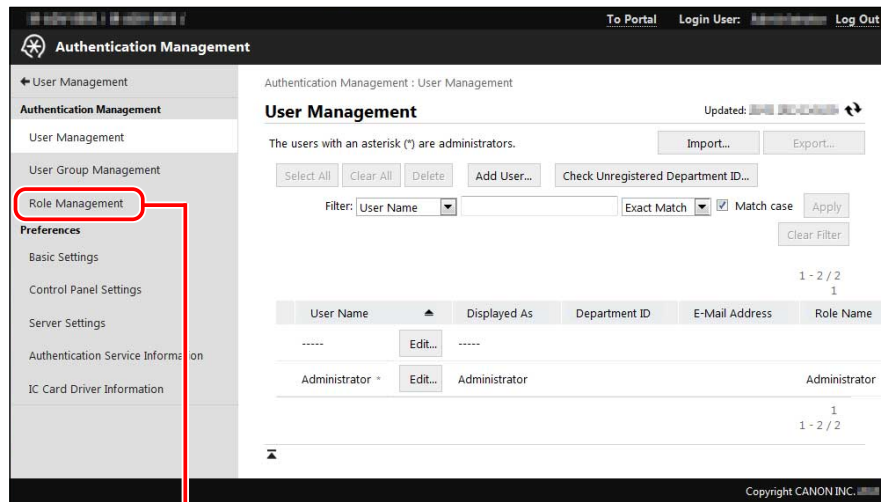
## Displays Used in This Manual

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/Button Names

The key/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. Replace the names as indicated below.

Key/Button Name in This Document	Key/Button Name in Your Machine
Main Menu	Home
Quick Menu	Home
Status Monitor/Cancel	Status Monitor
	<Settings/Registration> on the touch panel display
Numeric keys ([0] - [9])	Numeric keys ([0] - [9]) on the touch panel display
	<Energy Saver> on the touch panel display
[Counter/Device Information] key	<Counter/Device Information> on the touch panel display
Brightness Adjustment key	<Adjust Brightness> on the touch panel display
Volume Settings key	<Adjust Volume> on the touch panel display
	<Clear> on the touch panel display
	<Stop> on the touch panel display
	<Start> on the touch panel display
	<Reset> on the touch panel display
	<Log In>/<Log Out> on the touch panel display

## 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

---

© CANON INC. 2020

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written permission of Canon Inc.

## 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

<b>Introduction</b> .....	11
<b>Main Functions</b> .....	12
<b>User Authentication Methods and Managed Users</b> .....	17
<b>Structure of Usage Restrictions</b> .....	19
<b>Regarding Base Roles and Custom Roles</b> .....	20
<b>Device Management Privileges</b> .....	23
<b>Device Function Restrictions</b> .....	26
<b>Access Management System Configurations</b> .....	34
<b>Administrators for the Access Management System</b> .....	36
<b>System Requirements</b> .....	38

# 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.

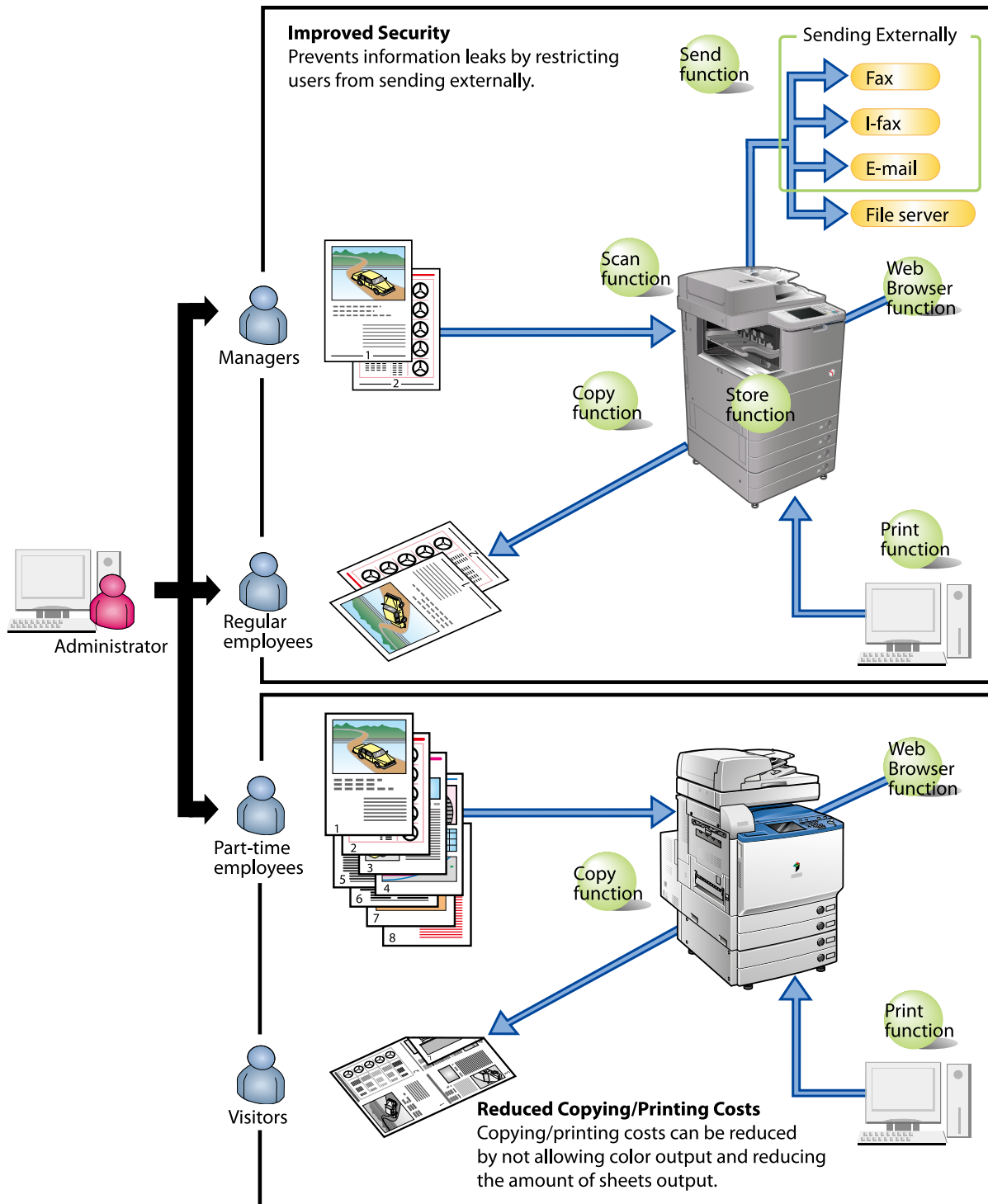
Function Name	Restrictions
Print function	Color printing, one-sided printing, page layout printing, saving to user inboxes
Store function	Color printing of user inbox documents, one-sided printing of user inbox documents, page layout printing of user inbox documents, saving to memory media, saving scanned 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.



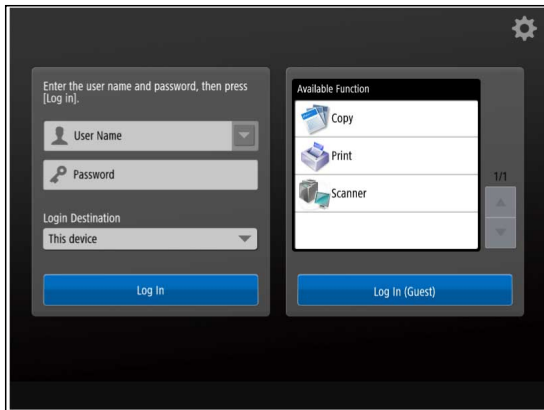
## Flow of User Authentication and Usage Restriction

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

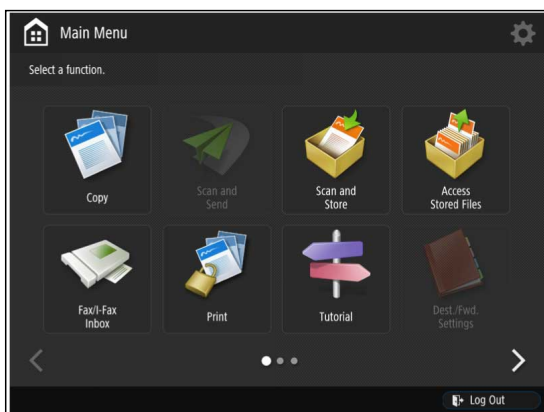
### If Using the Touch Panel Display <Device Level Log-in>:

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.

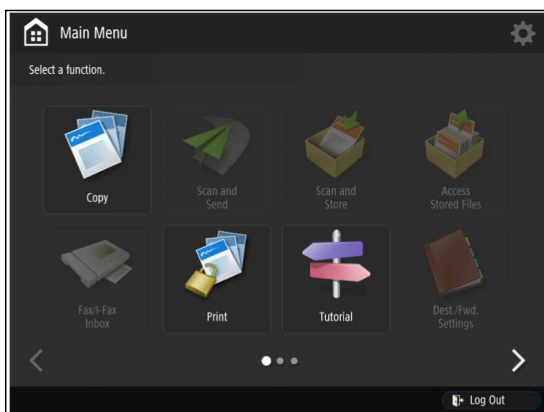




When [Log In] is pressed after entering a user name and password, user authentication is performed, and only the functions which that user can use become available on the touch panel display.



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.



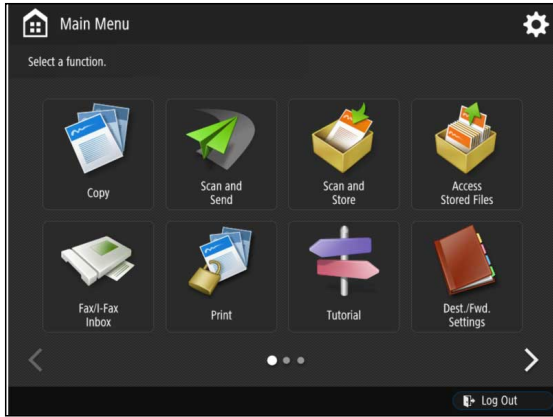
Since the [Settings/Registration] screen of the device can also be restricted, you can limit which users can change the settings of the device.

**IMPORTANT**

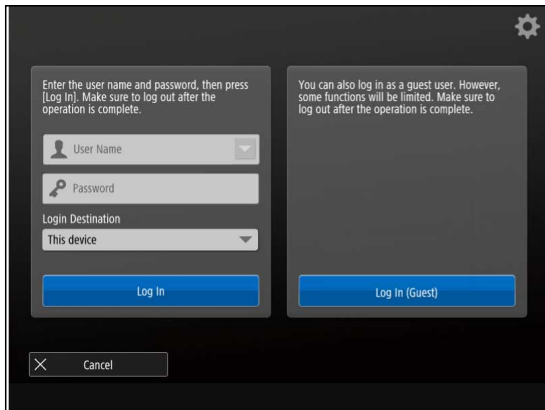
- To effectively use the Access Management System, make sure that users log out from the device when they finish using it by pressing (Log In/Out) or (Log Out) on the touch panel display.

**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.



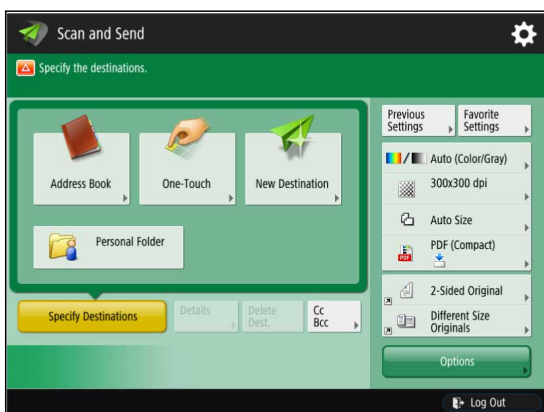
If you press the button for a function with authentication set, a login screen is displayed.



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.


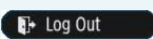
### NOTE

- 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  (Log In/Out) or  (Log Out) on the touch panel display.

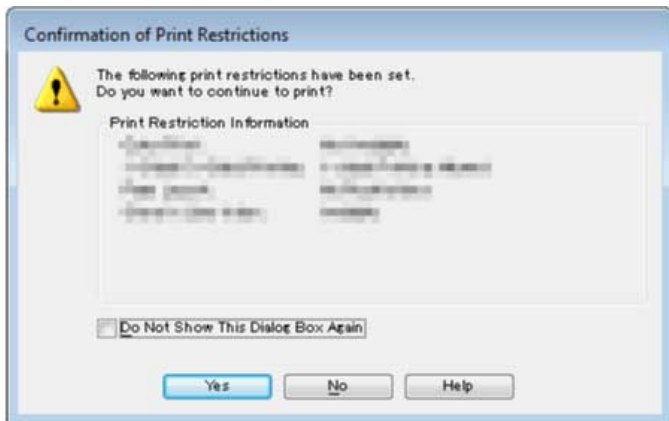
### If Printing from a Computer:

If you want to restrict printing from computers, it is necessary to set up (install the AMS Printer Driver Add-in and set user information for) all client computers that use the device after setting up the Access Management System.

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.

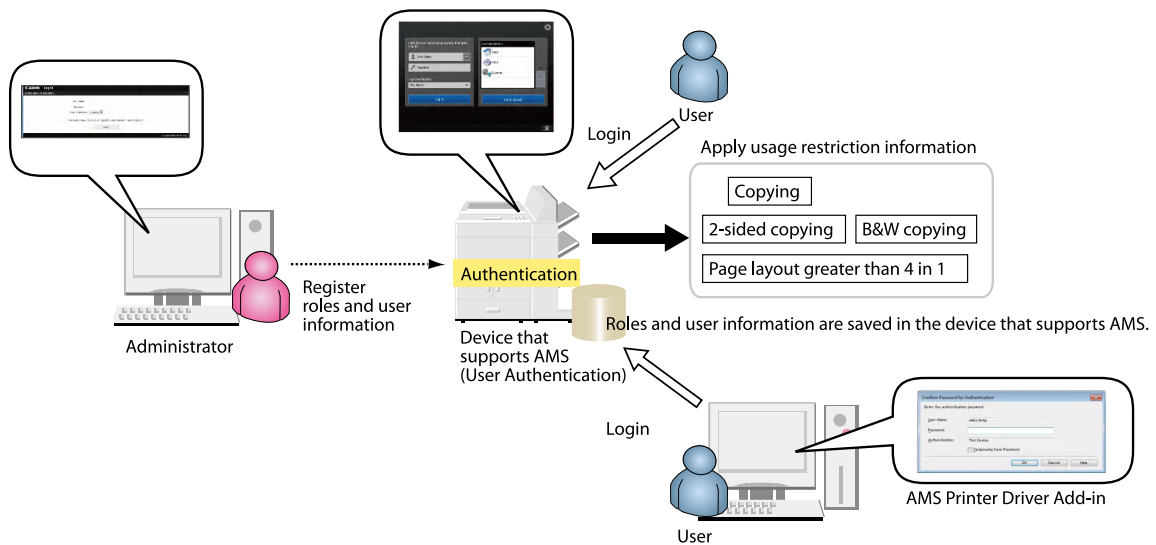


# User Authentication Methods and Managed Users

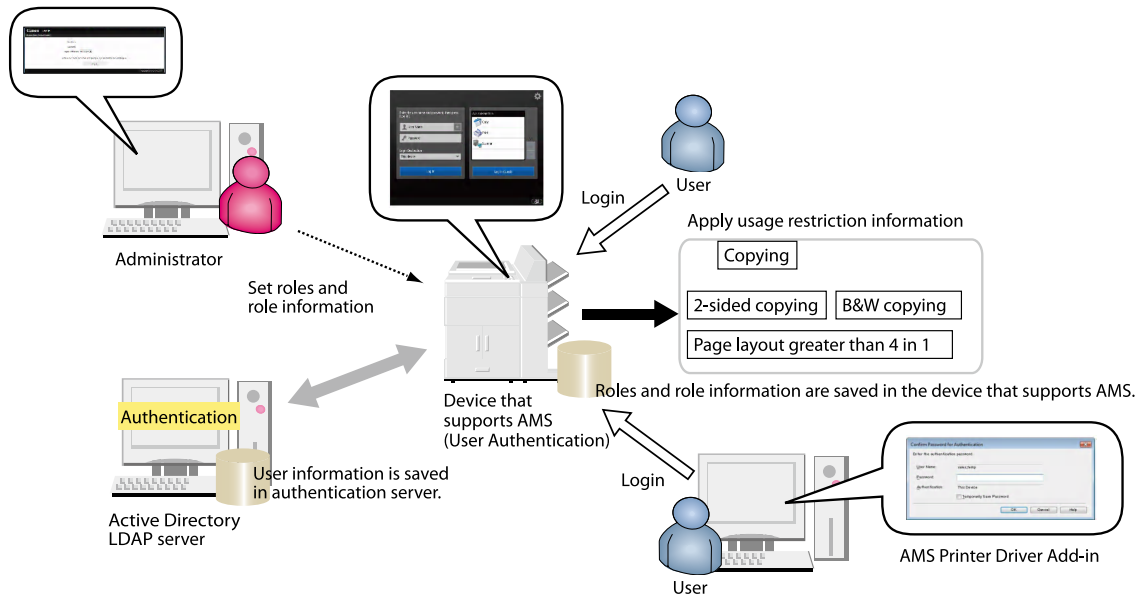
Devices to manage with the Access Management System have the following three user authentication methods, and each method manages different types of users.


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.	<p>The following keys cannot be used on the [Settings/Registration] screen:</p> <ul style="list-style-type: none"> <li>• Register Remote Device for Cascade Copy (Function Settings)</li> <li>• Limit New Destinations (Function Settings)</li> <li>• Always Add Device Signature to Send (Function Settings)</li> <li>• Address Book PIN (Set Destination)</li> </ul>
[PowerUser]	All functions are available.	<p>The following keys cannot be used on the [Settings/Registration] screen, in addition to the restrictions applied when the AMS is not used:</p> <ul style="list-style-type: none"> <li>• Register Remote Device for Cascade Copy (Function Settings)</li> <li>• Limit New Destinations (Function Settings)</li> <li>• Always Add Device Signature to Send (Function Settings)</li> </ul>

Introduction

Role Name	Device Function Restrictions	Device Management Privileges
		<ul style="list-style-type: none"> <li>• Address Book PIN (Set Destination)</li> <li>• Output Report (Function Settings)</li> <li>• Key and Certificate List for Certificate Settings (Management Settings)</li> </ul>
[GeneralUser]	All functions can be used except for address books and specifying destination domains.	<p>The following keys cannot be used on the [Settings/Registration] screen, in addition to the restrictions applied when the AMS is not used:</p> <ul style="list-style-type: none"> <li>• Register Remote Device for Cascade Copy (Function Settings)</li> <li>• Limit New Destinations (Function Settings)</li> <li>• Always Add Device Signature to Send (Function Settings)</li> <li>• Set Destination</li> <li>• Output Report (Function Settings)</li> <li>• Key and Certificate List for Certificate Settings (Management Settings)</li> </ul>
[LimitedUser]	<p>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.</p>	No keys can be used on the [Settings/Registration] screen.
[GuestUser] (guest role)	<p>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.</p>	No keys can be used on the [Settings/Registration] screen.
[NetworkAdmin] (custom role (administrator))	All functions are available.	<p>The following keys cannot be used on the [Settings/Registration] screen, in addition to the restrictions applied when the AMS is not used:</p> <ul style="list-style-type: none"> <li>• Register Remote Device for Cascade Copy (Function Settings)</li> <li>• Limit New Destinations (Function Settings)</li> <li>• Always Add Device Signature to Send (Function Settings)</li> <li>• Address Book PIN (Set Destination)</li> </ul>
[DeviceAdmin] (custom role (administrator))	All functions are available.	<p>The following keys cannot be used on the [Settings/Registration] screen, in addition to the restrictions applied when the AMS is not used:</p>



Role Name	Device Function Restrictions	Device Management Privileges
		<ul style="list-style-type: none"> <li>• Register Remote Device for Cascade Copy (Function Settings)</li> <li>• Limit New Destinations (Function Settings)</li> <li>• Always Add Device Signature to Send (Function Settings)</li> <li>• Address Book PIN (Set Destination)</li> </ul>

 **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**

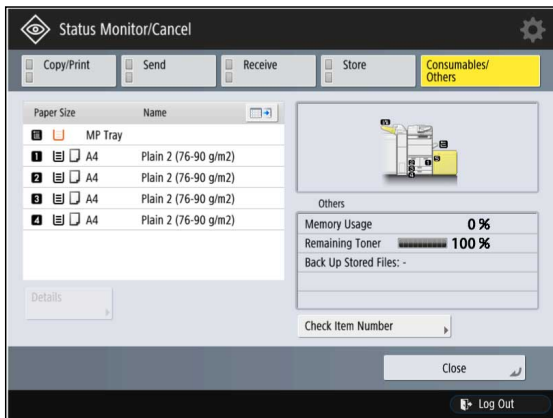
- For devices using the AMS, only users who have been assigned the [Administrator]/[DeviceAdmin]/[NetworkAdmin] role (or a custom role with the same settings as this role) have device management privileges to access the screen for managing the device from the remote UI. The operations possible when using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

[Status Monitor/Cancel] screen				Users with device management privileges	Users without device management privileges
			[Stop]	Displayed	Displayed as "****"
			[Secured Print]		
			Names of jobs		
		[Copy]	[Details]	Available	Unavailable
			[Stop]		
[Send]	[Job Status]	[Send]	[Details]	Available	Unavailable
			[Stop]		
			Destinations		
		[Fax]	[Details]	Available	Unavailable
			[Stop]		
			Destinations		
[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

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

\*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. 32)**
- ▶ **[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.
- It may not be necessary to install the AMS Printer Driver Add-in, depending on your environment. For more information, see "**Access Management System Configurations.**"(P. 34)

**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	✓	✓	✓		

Introduction

Function Restrictions		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
	Not Allowed				✓	✓
WebDAV TX	Allowed	✓	✓	✓		
	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

Button/Applet Name	Application Name
Access Stored Files	Access Stored Files
Fax/I-Fax Inbox	Access Stored Files
Secured Print	Secured Print
Web Access	Web Access
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. A supported printer driver must be installed in the computer before installing the AMS Printer Driver Add-in.

## IMPORTANT

- If any of the following conditions are met, you can set restrictions on color printing, one-sided printing, and storing to the inbox for users, even if you do not install 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 When server authentication is used, it is necessary to install the AMS Printer Driver Add-in to set restrictions for user 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.
- When server authentication is used, it is necessary to install the AMS Printer Driver Add-in to set restrictions for user printing.
- To set restrictions for page layouts when a user prints from a computer, it is necessary to install 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. 60)**."
- For more information on the printer drivers, see the instruction manuals for the printer drivers.

## Operating with Local Device Authentication Configuration

Software required	<ul style="list-style-type: none"> <li>• User Authentication</li> <li>• AMS Printer Driver Add-in*1</li> </ul>
Computer required	<ul style="list-style-type: none"> <li>• Client computer (AMS Printer Driver Add-in)*1</li> </ul>

\*1 Required for restricting printing from computers.

## Operating with LDAP Authentication in the Configuration

Software required	<ul style="list-style-type: none"> <li>• User Authentication</li> <li>• AMS Printer Driver Add-in*1</li> </ul>
Computer required	<ul style="list-style-type: none"> <li>• LDAP Server</li> <li>• Client computer (AMS Printer Driver Add-in)*1</li> </ul>

\*1 Required for restricting printing from computers.

## Operating with Active Directory Authentication Configuration

Software required	<ul style="list-style-type: none"> <li>• User Authentication</li> <li>• AMS Printer Driver Add-in*1</li> </ul>
Computer required	<ul style="list-style-type: none"> <li>• Domain server (Active Directory)</li> <li>• Client computer (AMS Printer Driver Add-in)*1</li> </ul>

\*1 Required for restricting printing from computers.

## 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. 36)**
- ▶ **Operating with LDAP authentication(P. 36)**
- ▶ **Operating with central management configuration using Active Directory authentication(P. 37)**

### Operating with Local Device Authentication

Type of Administrator	Function	Required Privileges
Device administrator	<ul style="list-style-type: none"> <li>• Configuring of the Access Management System</li> <li>• Managing restricted devices               <ul style="list-style-type: none"> <li>- Date/time settings</li> <li>- Network settings</li> <li>- Registering the System Manager ID</li> <li>- Starting User Authentication</li> </ul> </li> <li>• Selecting the device restriction administrator</li> </ul>	<p>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.</p>
Device restriction administrator	<ul style="list-style-type: none"> <li>• Specifying the Preferences of the device</li> <li>• Security settings</li> <li>• User management</li> <li>• Role management</li> <li>• Associating roles and users</li> </ul>	<ul style="list-style-type: none"> <li>• Associated with the [Administrator] role</li> </ul>
Client computer administrator	<ul style="list-style-type: none"> <li>• Installing and updating printer drivers to client computers</li> <li>• Installing the AMS Printer Driver Add-in to client computers</li> </ul>	<p>Administrator privileges for Windows used in the client computers</p>

### Operating with LDAP authentication

Type of Administrator	Function	Required Privileges
Device administrator	<ul style="list-style-type: none"> <li>• Configuring of the Access Management System</li> <li>• Managing restricted devices               <ul style="list-style-type: none"> <li>- Date/time settings</li> <li>- Network settings</li> <li>- Registering the System Manager ID</li> <li>- Starting User Authentication</li> </ul> </li> <li>• Selecting the device restriction administrator</li> </ul>	<p>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.</p>
Device restriction administrator	<ul style="list-style-type: none"> <li>• Specifying the Preferences of the device (default role settings)</li> <li>• Security settings</li> <li>• User Management</li> <li>• Managing guest roles</li> </ul>	<p>Associated with the [Administrator] role</p>

## Introduction

Type of Administrator	Function	Required Privileges
Client computer administrator	<ul style="list-style-type: none"> <li>• Installing and updating printer drivers to client computers</li> <li>• Installing the AMS Printer Driver Add-in to client computers</li> </ul>	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	<ul style="list-style-type: none"> <li>• Configuring of the Access Management System</li> <li>• Managing restricted devices                             <ul style="list-style-type: none"> <li>- Date/time settings</li> <li>- Network settings</li> <li>- Registering the System Manager ID</li> <li>- Starting User Authentication</li> </ul> </li> <li>• Selecting the device restriction administrator</li> </ul>	<p>Able to log in to SMS (Service Management Service)</p> <p>However, the [Administrator] role must be associated with the administrator after starting to operate the Access Management System.</p>
Company network administrator	<ul style="list-style-type: none"> <li>• DNS server settings</li> <li>• Trusted domain settings</li> <li>• Creating a user group in Active Directory and adding users to the user group</li> </ul>	<ul style="list-style-type: none"> <li>• Administrator privileges for the DNS server (when using multiple domains)</li> <li>• Administrator privileges for Active Directory</li> </ul>
Device restriction administrator	<ul style="list-style-type: none"> <li>• Specifying the Preferences of the device</li> <li>• Security settings</li> <li>• User management</li> <li>• Role management</li> <li>• Associating roles and users</li> </ul>	<ul style="list-style-type: none"> <li>• Associated with the [Administrator] role</li> <li>• Administrator privileges for Active Directory</li> </ul>
Client computer administrator	<ul style="list-style-type: none"> <li>• Installing and updating printer drivers to client computers</li> <li>• Installing the AMS Printer Driver Add-in to client computers</li> </ul>	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. 38)**
- ▶ **Client Computer (AMS Printer Driver Add-in)(P. 38)**

## 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, the AMS Printer Driver Add-in must be installed to 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.

- Canon UFR II Printer Driver V2.90 or later, earlier than V20.00, V20.60 or later
- Canon PCL6 Printer Driver V6.90 or later, earlier than V20.00, V20.60 or later
- Canon PCL5e/5c Printer Driver V8.90 or later, earlier than V20.00, V20.60 or later
- Canon PS3 Printer Driver V4.90 or later, earlier than V20.00, V20.60 or later
- Canon Generic Plus PCL6 Printer Driver V1.00 or later

### Supported Operating Systems

32-bit Operating System (x86)	Microsoft Windows Server 2008 Microsoft Windows Server 2008 Service Pack 2 Edition: Enterprise/Standard  Microsoft Windows Vista Service Pack 2 Edition: Enterprise/Business/Ultimate/Home Premium/Home Basic  Microsoft Windows 7 Microsoft Windows 7 Service Pack 1 Edition: Enterprise/Professional/Ultimate/Home Premium  Microsoft Windows 8.1 Edition: Enterprise/Pro/(No edition name)  Microsoft Windows 10 Edition: Enterprise/Education/Pro/Home
64-bit Operating System (x64)	Microsoft Windows Server 2008 Microsoft Windows Server 2008 Service Pack 2 Edition: Enterprise/Standard  Microsoft Windows Server 2008 R2 Microsoft Windows Server 2008 R2 Service Pack 1 Edition: Enterprise/Standard  Microsoft Windows Vista Service Pack 1 Edition: Enterprise/Business/Ultimate/Home Premium/Home Basic  Microsoft Windows 7


	Microsoft Windows 7 Service Pack 1 Edition: Enterprise/Professional/Ultimate/Home Premium
	Microsoft Windows 8.1 Edition: Enterprise/Pro/(No edition name)
	Microsoft Windows Server 2012 Microsoft Windows Server 2012 R2 Edition: Datacenter/Standard/Essentials/Foundation
	Microsoft Windows 10 Edition: Enterprise/Education/Pro/Home
	Microsoft Windows Server 2016 Edition: Datacenter/Standard/Essentials

 **NOTE**

- An appropriate version of Internet Explorer needs to be installed on the above operating systems.
- Port number 8000 is used for HTTP communication and 8443 is used for HTTPS communication.
- Although print restrictions are also normally applied when you print from the Windows Store app in Windows 8.1/10/Server 2012/Server 2016, these print restrictions are not displayed in the print settings on the screen.

### Computer


- CPU:  
Pentium 4 processor, 1.8 GHz or faster (Recommended: Pentium D processor, 2.4 GHz or faster)
- Memory:  
1,024 MB or more (Recommended: 1,024 MB or more)
- Hard Disk:  
25 MB minimum (Space required for installation)
- Display Environment:  
SVGA 800 x 600 or higher resolution, 65,536 colors or higher color (Recommended: XGA 1,024 x 768 or higher resolution, 16,777,216 colors or higher color)

 **IMPORTANT**

- Operations may become slower when the AMS Printer Driver Add-in is installed, depending on the performance of the computer.

### 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

<b>Setting Up the Access Management System</b> .....	41
<b>Flow of Settings for Operating with Local Device Authentication</b> .....	42
<b>Flow of Settings for Operating with Server Authentication</b> .....	44
<b>Preparing the Device and Network Environment</b> .....	46
<b>Logging in to User Authentication</b> .....	49
<b>Specifying the Preferences of the Devices</b> .....	50
Specifying the Device Preferences Using User Authentication .....	51
<b>Managing Roles</b> .....	64
Managing Roles Using User Authentication .....	65

## 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. 44)

## 1. Preparing the Device and Network Environment(P. 46)

---

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. 50)

---

Specify the preferences of all devices that support AMS.

- ▶ **Setting the User Authentication Method(P. 51)**
- ▶ **Setting the Default Role for Registered Users(P. 51)**
- ▶ **Role Association(P. 53)**
- ▶ **Setting the Login Method(P. 53)**
- ▶ **Allowing Unregistered Users to Log In(P. 53)**
- ▶ **Setting the Number of Users to Cache on the Login Screen(P. 54)**
- ▶ **Retaining User Authentication Information with the Printer Driver(P. 55)**
- ▶ **Prohibiting the Printing from Drivers without AMS Printer Driver Add-in(P. 56)**

- ▶ **Setting Remote Job Restrictions(P. 59)**
- ▶ **Setting Usage Restrictions for Remote Scanning/Cascade Copy(P. 60)**
- ▶ **Adding a Device Signature When Forwarding Files(P. 61)**
- ▶ **Configuring IPP Printing(P. 62)**

## 6. Managing Roles(P. 64)

---

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. 65)**
- ▶ **Editing Custom Roles(P. 69)**
- ▶ **Editing the [GuestUser] Role (Guest Role)(P. 70)**
- ▶ **Deleting Custom Roles(P. 71)**
- ▶ **Importing Roles(P. 72)**
- ▶ **Exporting Roles(P. 74)**

## 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, it is necessary to add the AMS Printer Driver Add-in to the printer drivers installed in the computers, after the above operations are complete. For more information, see "**Setting Up the Client Computers.**"(P. 77)

# 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. 42)

## 1. Preparing the Device and Network Environment(P. 46)

---

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. 50)

---

Specify the preferences of all devices that support AMS.

- ▶ **Setting the User Authentication Method(P. 51)**
- ▶ **Setting the Default Role for Registered Users(P. 51)**
- ▶ **Role Association(P. 53)**
- ▶ **Setting the Login Method(P. 53)**
- ▶ **Allowing Unregistered Users to Log In(P. 53)**

- ▶ **Setting the Number of Users to Cache on the Login Screen(P. 54)**
- ▶ **Retaining User Authentication Information with the Printer Driver(P. 55)**
- ▶ **Prohibiting the Printing from Drivers without AMS Printer Driver Add-in(P. 56)**
- ▶ **Setting Remote Job Restrictions(P. 59)**
- ▶ **Setting Usage Restrictions for Remote Scanning/Cascade Copy(P. 60)**
- ▶ **Adding a Device Signature When Forwarding Files(P. 61)**
- ▶ **Configuring IPP Printing(P. 62)**

## 6. Managing Roles(P. 64)

---

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. 65)**
- ▶ **Editing Custom Roles(P. 69)**
- ▶ **Editing the [GuestUser] Role (Guest Role)(P. 70)**
- ▶ **Deleting Custom Roles(P. 71)**
- ▶ **Importing Roles(P. 72)**
- ▶ **Exporting Roles(P. 74)**

### 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. 42) and then perform step 6 in "**Flow of Settings for Operating with Server Authentication.**"(P. 44)

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, it is necessary to add the AMS Printer Driver Add-in to the printer drivers installed in the computers, after the above operations are complete. For more information, see "**Setting Up the Client Computers.**"(P. 77)



## 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(P. 46)**
- ▶ **Specifying the Network Settings(P. 46)**
- ▶ **Making Devices Accessible from Web Browsers(P. 47)**
- ▶ **Registering the System Manager ID(P. 47)**
- ▶ **Setting the LDAP Server(P. 47)**
- ▶ **Setting the DNS Server(P. 47)**
- ▶ **Setting the Domain Trust Relationships(P. 48)**

### 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

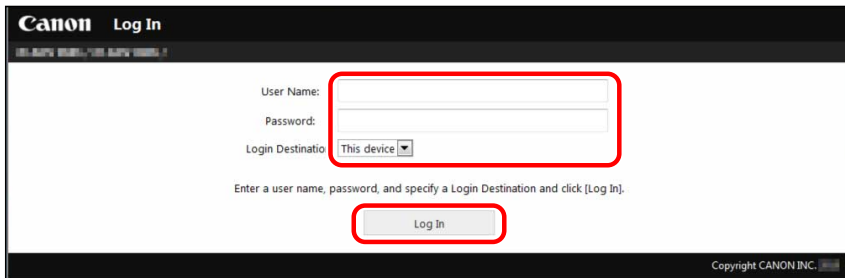
To manage roles and users and specify the preferences of the devices, log in to User Authentication.

**1 Open your Web browser → enter the following URL:**

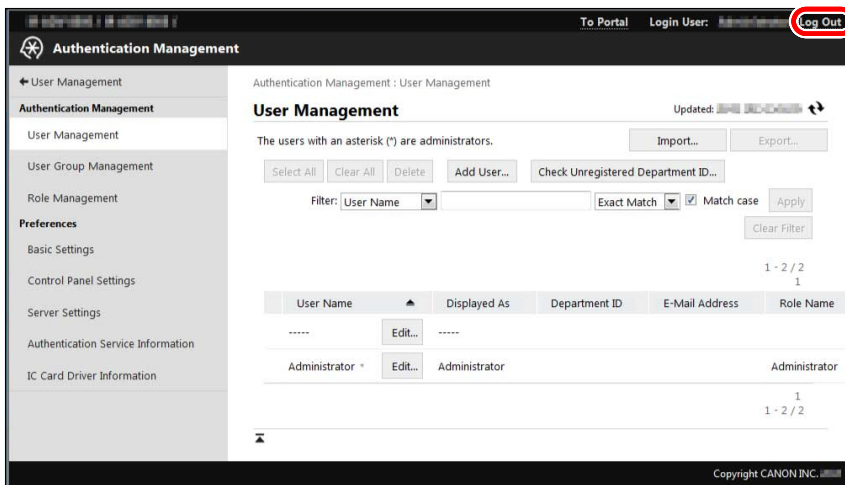
http://<IP address or host name of the device>

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].**



**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. 51)**

#### 📌 **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. 42) or "**Flow of Settings for Operating with Server Authentication.**"(P. 44)

# 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(P. 51)**
- ▶ **Setting the Default Role for Registered Users(P. 51)**
- ▶ **Role Association(P. 53)**
- ▶ **Setting the Login Method(P. 53)**
- ▶ **Allowing Unregistered Users to Log In(P. 53)**
- ▶ **Setting the Number of Users to Cache on the Login Screen(P. 54)**
- ▶ **Retaining User Authentication Information with the Printer Driver(P. 55)**
- ▶ **Prohibiting the Printing from Drivers without AMS Printer Driver Add-in(P. 56)**
- ▶ **Setting Remote Job Restrictions(P. 59)**
- ▶ **Setting Usage Restrictions for Remote Scanning/Cascade Copy(P. 60)**
- ▶ **Adding a Device Signature When Forwarding Files(P. 61)**
- ▶ **Configuring IPP Printing(P. 62)**

## 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. 49)

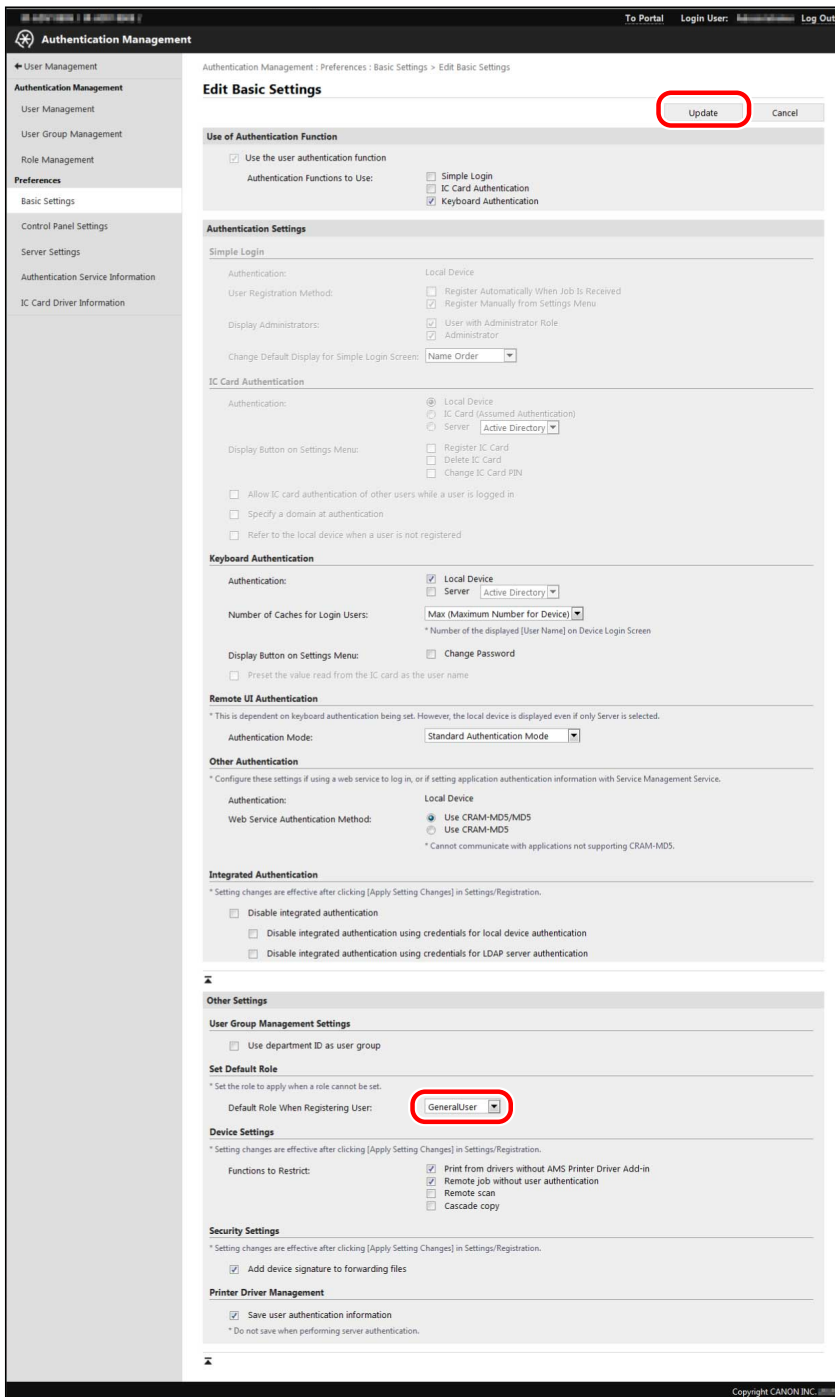
### 2 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Basic Settings].

### 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.

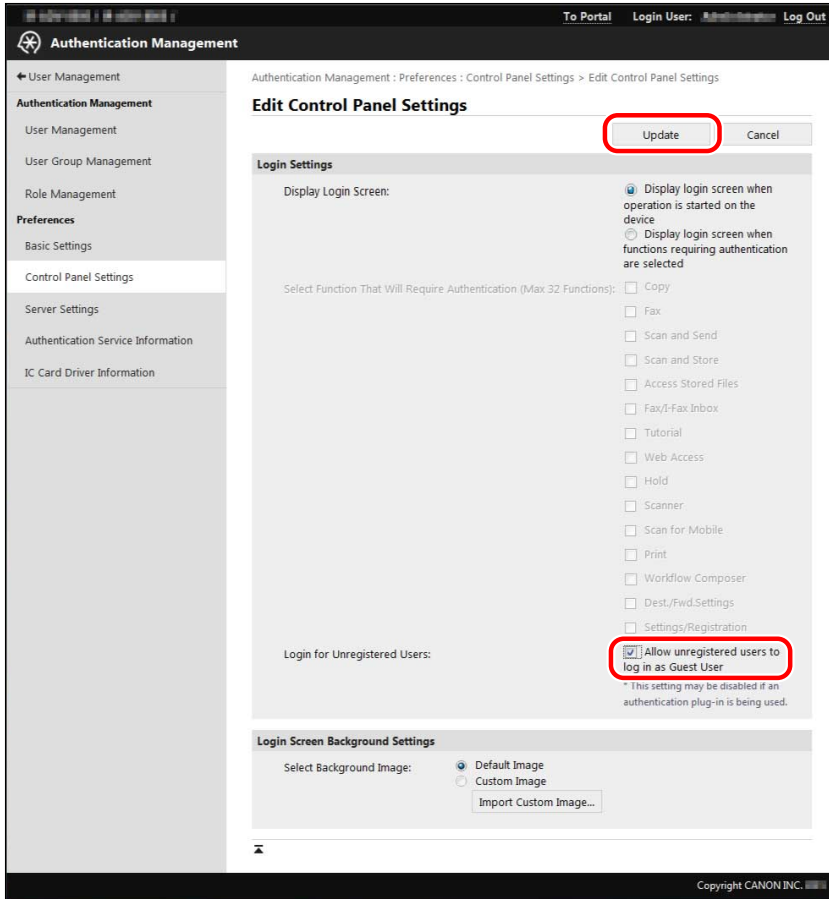
For more information, see "Logging in to User Authentication."(P. 49)

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

### **3** Click [Edit].

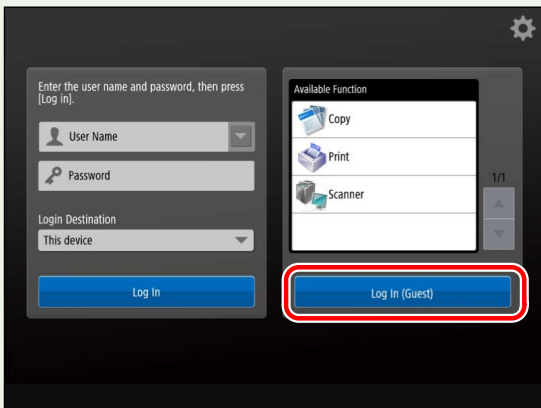
### **4** Select [Allow unregistered users to log in as Guest User] in [Login for Unregistered Users] → click [Update].






**NOTE**

- The [GuestUser] role (guest role) can be edited. For more information, see **"Editing the [GuestUser] Role (Guest Role)."**(P. 70)
- 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.

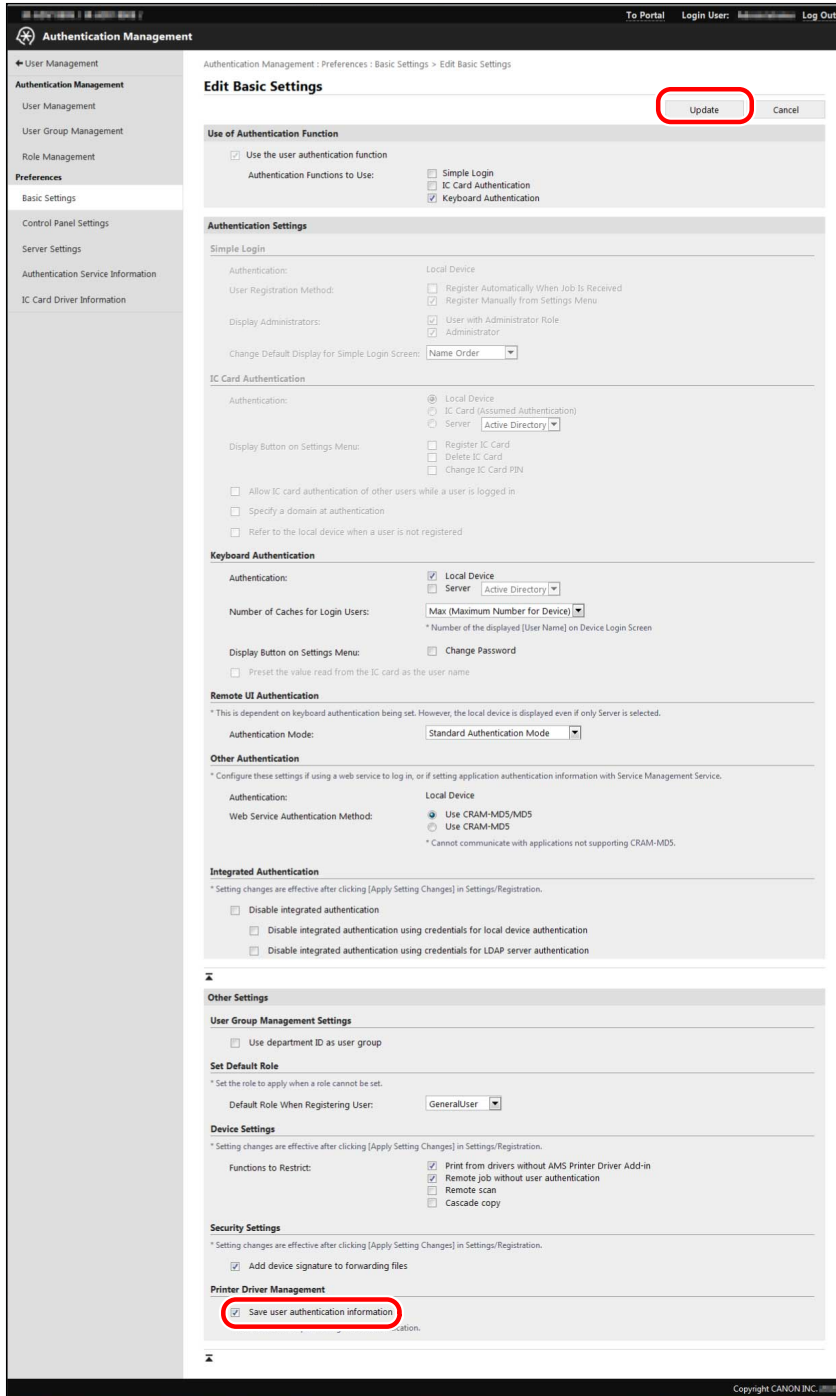
### 1 Log in to User Authentication.

For more information, see "Logging in to User Authentication."(P. 49)

### 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.
- If you do not restrict the printing of jobs that do not support print restrictions, you cannot prevent printing from computers in which the AMS Printer Driver Add-in is not installed or from computers in 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.

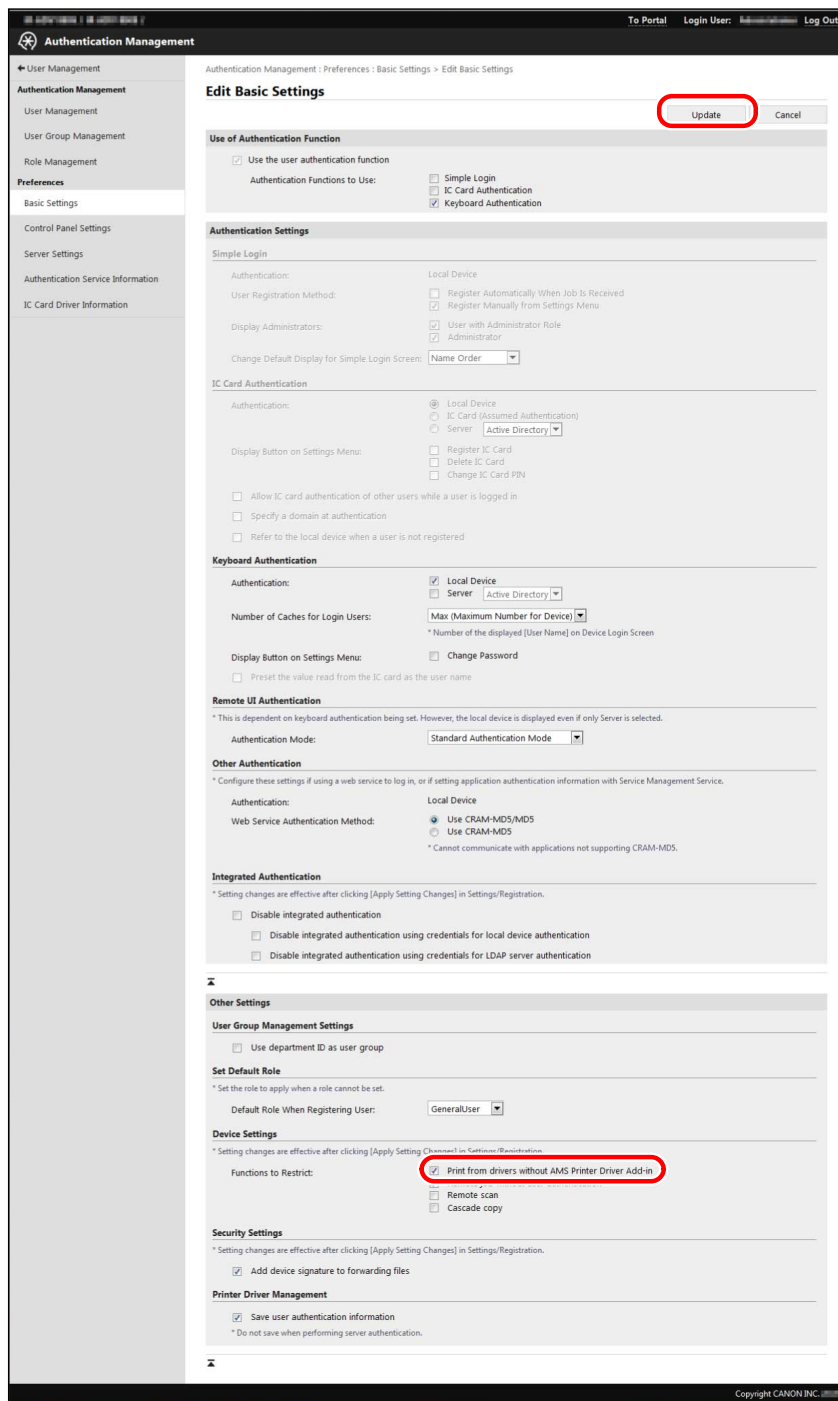
**1 Log in to User Authentication.**

For more information, see "**Logging in to User Authentication.**"(P. 49)

**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

- When [Print from drivers without AMS Printer Driver Add-in] is selected, a security check is automatically performed when printing from printer drivers in which the AMS Printer Driver Add-in is installed. If a problem is found, printing will be canceled.

## Setting Remote Job Restrictions

Set usage restrictions for remote jobs without user authentication.

### IMPORTANT

- When using local device authentication, to set restrictions on user printing without installing the AMS Printer Driver Add-in, enable the [Remote job without user authentication] restriction. For more information, see " **Access Management System Configurations(P. 34)** ."

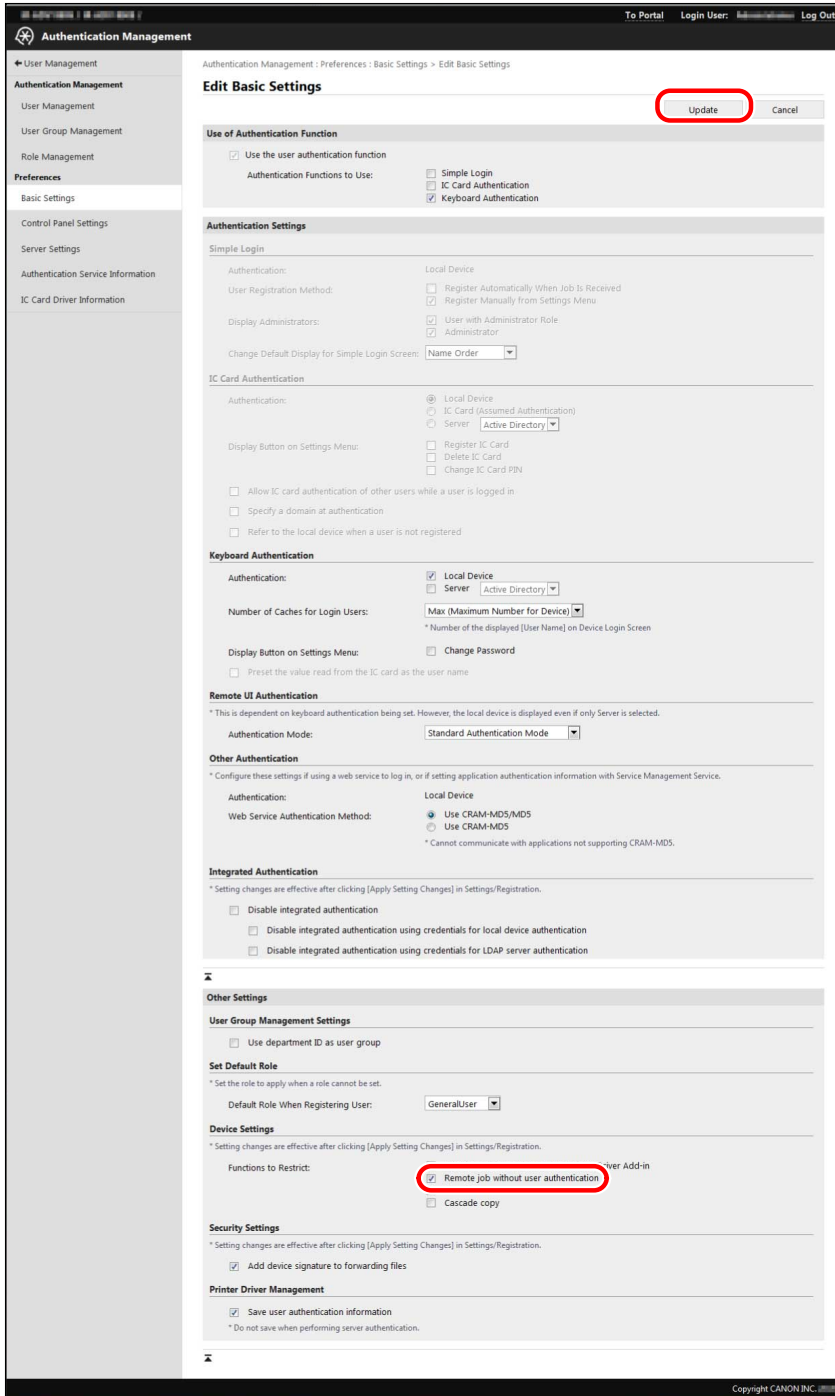
### **1** Log in to User Authentication.

For more information, see " **Logging in to User Authentication(P. 49)** ."

### **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.

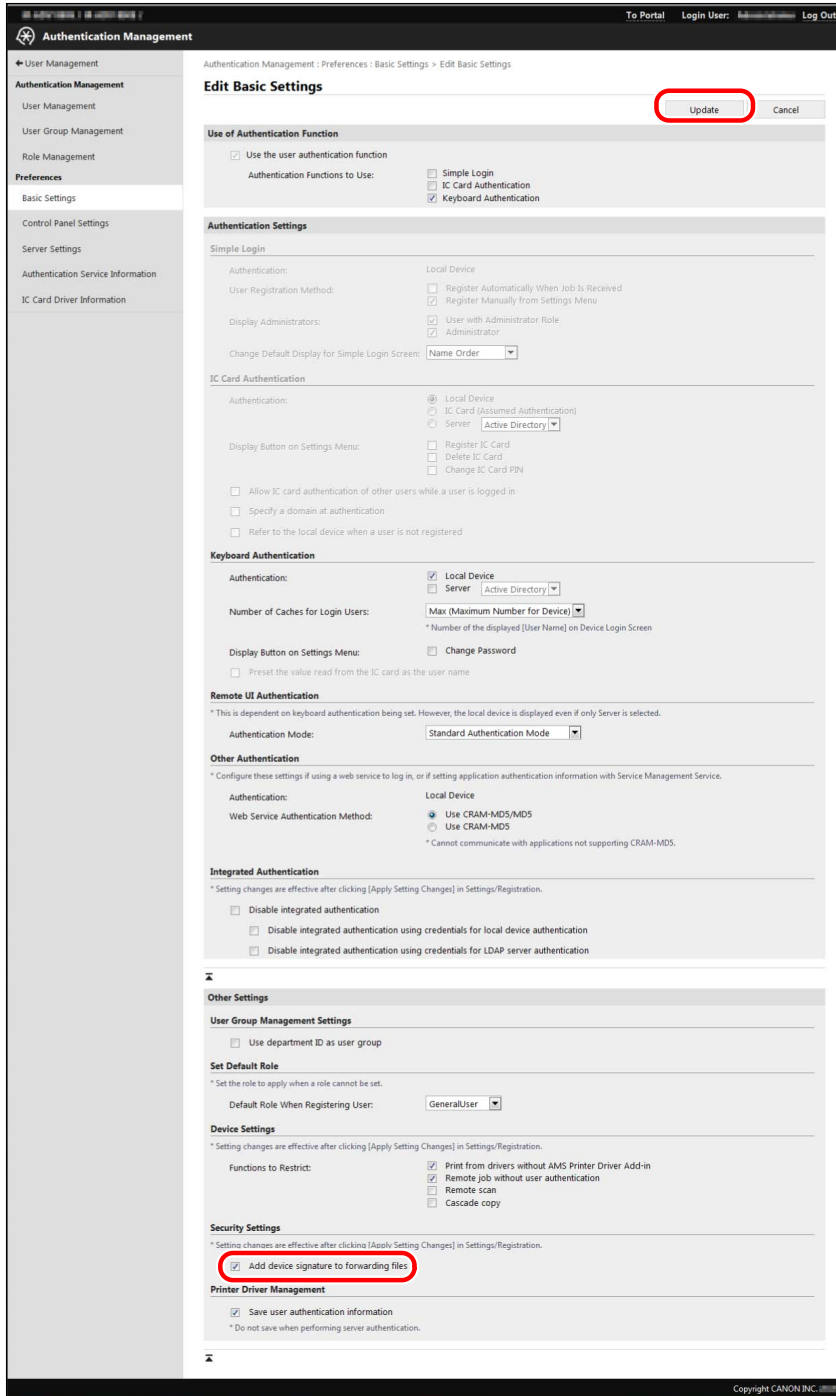
For more information, see "**Logging in to User Authentication.**"(P. 49)

### **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.

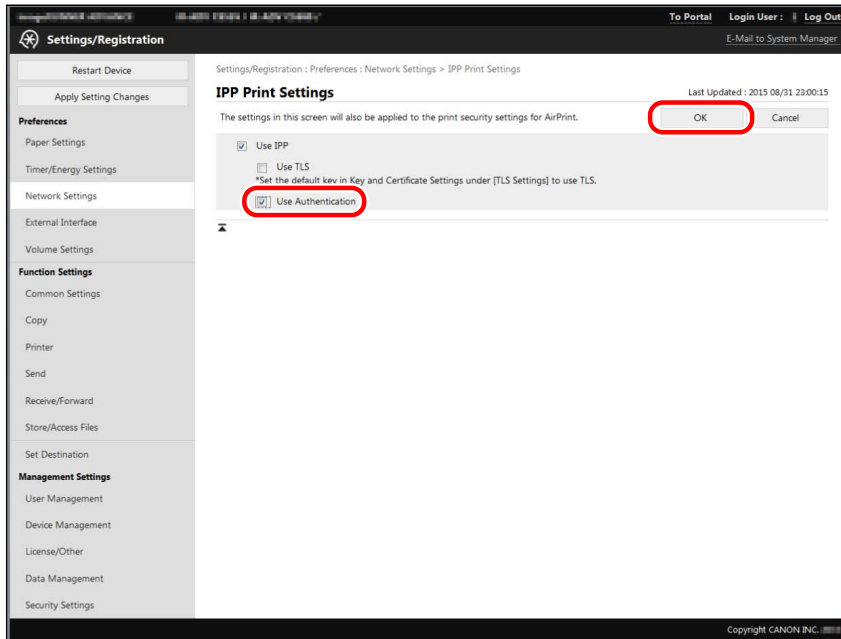
For more information, see " Logging in to User Authentication(P. 49) ."

**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. 65)

### 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. 42) or "**Flow of Settings for Operating with Server Authentication.**"(P. 44)

## Managing Roles Using User Authentication

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

- ▶ **Creating Custom Roles(P. 65)**
- ▶ **Editing Custom Roles(P. 69)**
- ▶ **Editing the [GuestUser] Role (Guest Role)(P. 70)**
- ▶ **Deleting Custom Roles(P. 71)**
- ▶ **Importing Roles(P. 72)**
- ▶ **Exporting Roles(P. 74)**

### 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. 69)

#### 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.

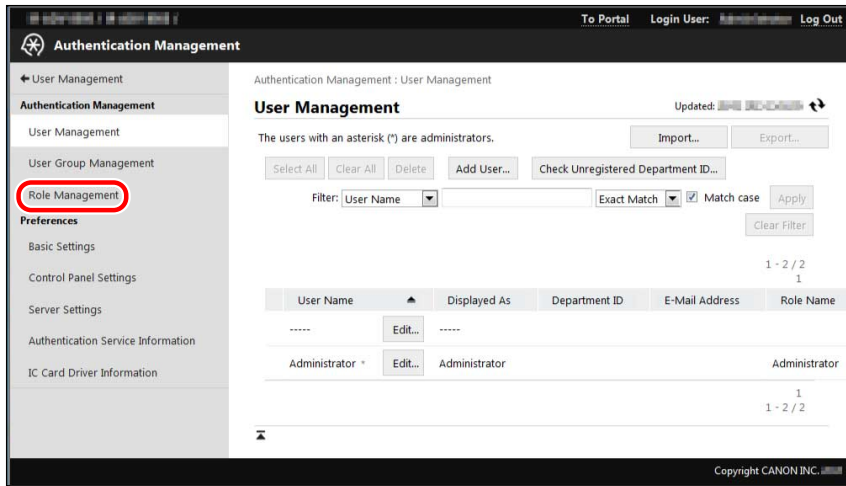
#### NOTE

- 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. 72) and see "**Exporting Roles.**"(P. 74)
- Associate roles to users on the [User Management] screen. For more information, see the instruction manuals of the device.

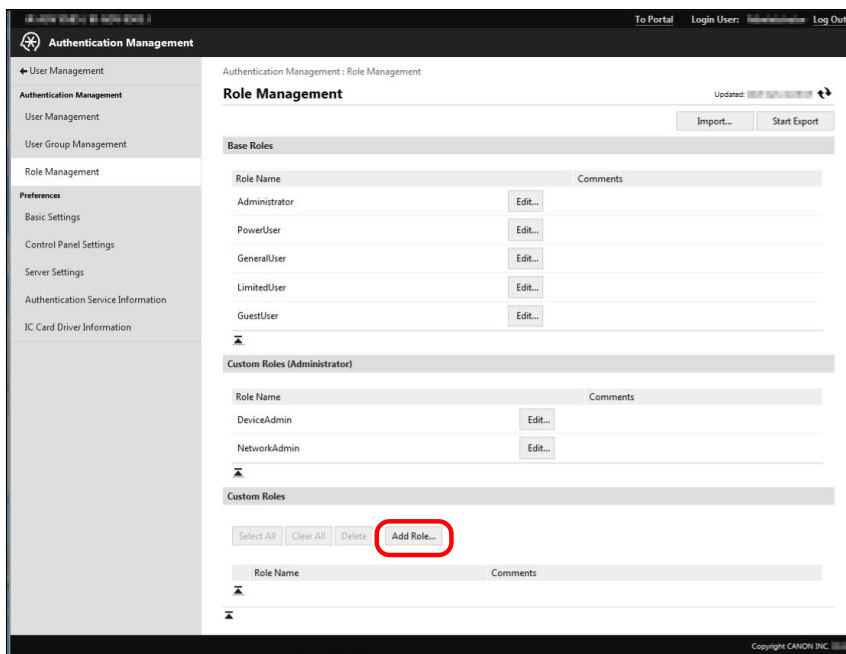
### 1 Log in to User Authentication.

For more information, see "**Logging in to User Authentication.**"(P. 49)

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



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



**4** Specify the required items → click [Add].

# Setting Up the Access Management System

**Add Custom Role**

Role Name: temp\_custom (Maximum 32 Characters)

Comments: For temporary employee (Maximum 50 Characters)

Base Role: GeneralUser

**Device Management Restriction**

All Settings: Restrictions

Network Settings: Not allowed

Device Settings: Not Allowed

**Function Category Restriction** \* Restrict device functions by category

Print Functions: Allowed

Save Functions (Mail Box/Memory Media): Allowed

Copy Functions: Allowed

Send Functions/Store on Network: Not Allowed

Web Access Function: Allowed

Utility Function: Allowed

Others Functions: Allowed

**Function Category Restriction Details**

**Print Functions**

Print: Allowed

1-Sided/2-Sided Printing: 2-Sided Printing Only

Page Layout: No Restrictions

Save to Mail Box: Allowed

**Save Functions (Mail Box/Memory Media)**

Print: Allowed

1-Sided/2-Sided Printing: No Restrictions

Page Layout: No Restrictions

**Save Function (Memory Media)**

Memory Media: Allowed

Scan: Allowed \* Can be set when [Scan] is allowed in [Scan Functions].

Print: Allowed \* Can be set when [Print] is allowed in [Save Functions (Mail Box/Memory Media)].

**Copy Functions**

1-Sided/2-Sided Copying: 2-Sided Copying Only

Page Layout: No Restrictions

**Scan Functions**

Scan: Allowed

Color Scan: Allowed

**Send Functions/Store on Network**

E-Mail TX: Allowed

E-Mail TX (Use [Send to Myself]): Allowed

Fax TX: Allowed

Fax TX: Allowed

FTP TX: Allowed

Windows (SMB) TX: Allowed

WebDAV TX: Allowed

Use (Personal Folder): Allowed

Mail Box TX: Allowed

Specify Address Domain: Not Allowed

Use Address Book/Register Storage Location for Network: Read-Only

Use Personal Address List: Allowed

Send to New Addresses: Allowed

Add Device Signature to Sending Files: Not Added

Sending Files Format: No Restrictions

**Application Restrictions**

\* Individually set device application restrictions

Application Name	Status	Application ID
Copy	Not Set	8c726860-29c2-46c5-a07a-86c4177a61e3
Scan and Send	Not Set	ae53008a-aab1-4aae-95c7-d746db532c88
Access Stored Files	Not Set	3d9b3c08-e4b5-4777-be55-fe0cd92f6d9
Web Access	Not Set	a2071ad7-7717-4817-9d2f-9dc71d91b7b
Hold	Not Set	18326034-010c-1000-a74e-00e0004ae6f
Scan for Mobile	Not Set	18d9822c-0140-1000-a701-00e0004ae6f
Print	Not Set	3c3527f-c0140-1000-9911-00e0004ae6f
IW Function Flow	Not Allowed	88a7d818-810c-4000-8000-000000000000

**Button Restrictions**

\* Set restrictions for the buttons in the device main menu and quick menu. Up to 32 buttons can be restricted.

Button/Applet Name	Status	Application Name
Copy	Not Set	Copy
Fax	Not Set	Scan and Send
Scan and Send	Not Set	Scan and Send
Scan and Store	Not Set	Access Stored Files
Access Stored Files	Not Set	Access Stored Files
Fax/F-Fax Inbox	Not Set	Access Stored Files
Tutorial	Not Set	Tutorial
Web Access	Not Set	Web Access
Hold	Not Set	Hold
Scanner	Not Set	Scan
Scan for Mobile	Not Set	Scan for Mobile
Print	Not Set	Print
IW Function Flow	Not Set	IW Function Flow
Desk./Fwd.Settings	Not Set	Scan and Send

The new role is registered.

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

## Setting Up the Access Management System

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]	<p>Set the device management restrictions.</p> <p><b>[All Settings]:</b> 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.)</p> <p><b>[Network Settings]:</b> Set [No Restrictions]/[Not Allowed] for the device management privileges that belong to each network setting category.</p> <p><b>[Device Settings]:</b> Set [No Restrictions]/[Not Allowed] for the device management privileges that belong to each device setting category.</p>	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. 70)
- 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. 74)
- Associate roles to users on the [User Management] screen. For more information, see the instruction manuals of the device.

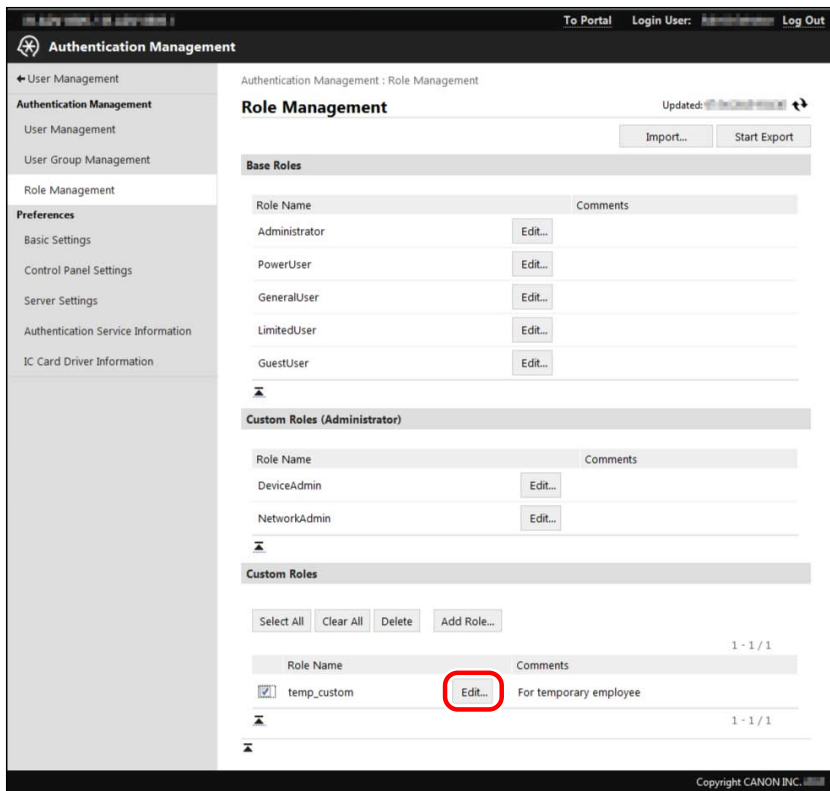
### 1 Log in to User Authentication.

For more information, see "**Logging in to User Authentication.**"(P. 49)

### 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

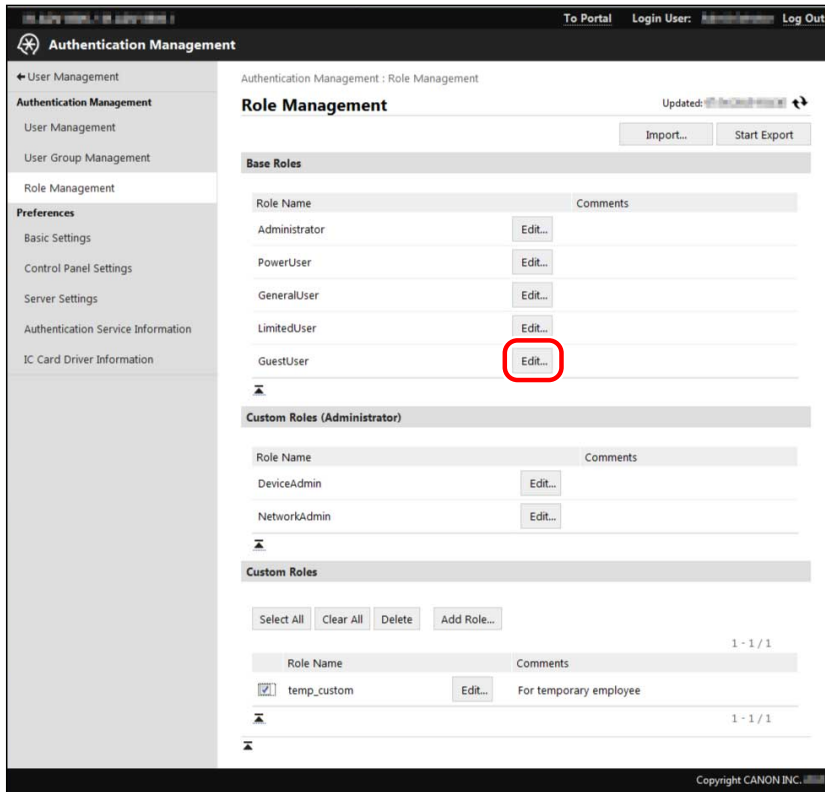
- It is recommended you export the role information after editing [GuestUser] role for backup purposes. For more information, see "**Exporting Roles.**"(P. 74)

#### 1 Log in to User Authentication.

For more information, see "Logging in to User Authentication."(P. 49)

**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

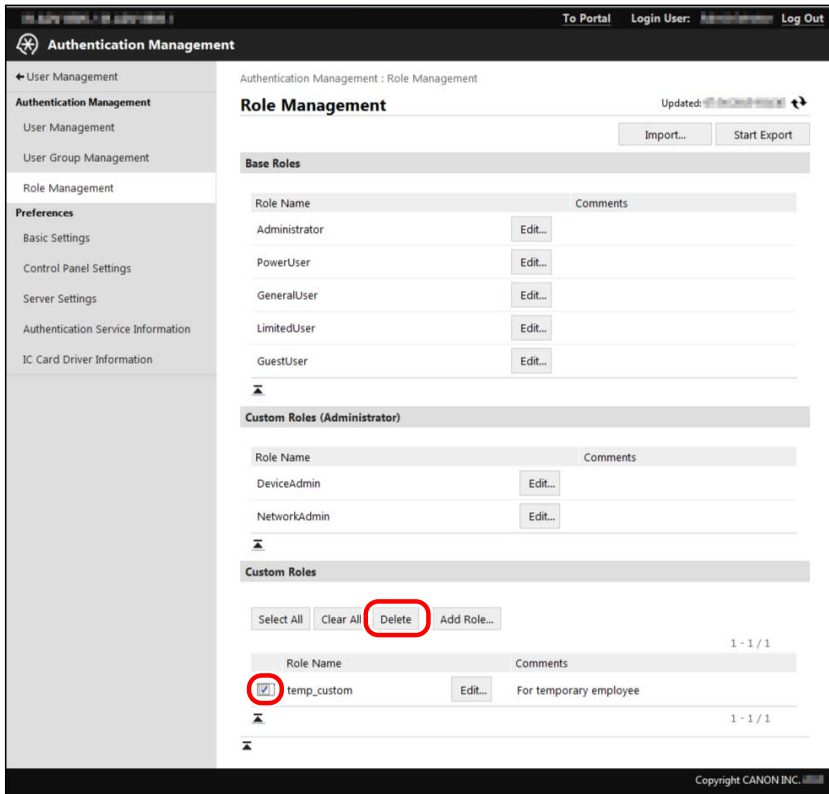
- Base roles and custom roles (administrator) cannot be deleted.

**1** Log in to User Authentication.


For more information, see "Logging in to User Authentication."(P. 49)

**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**

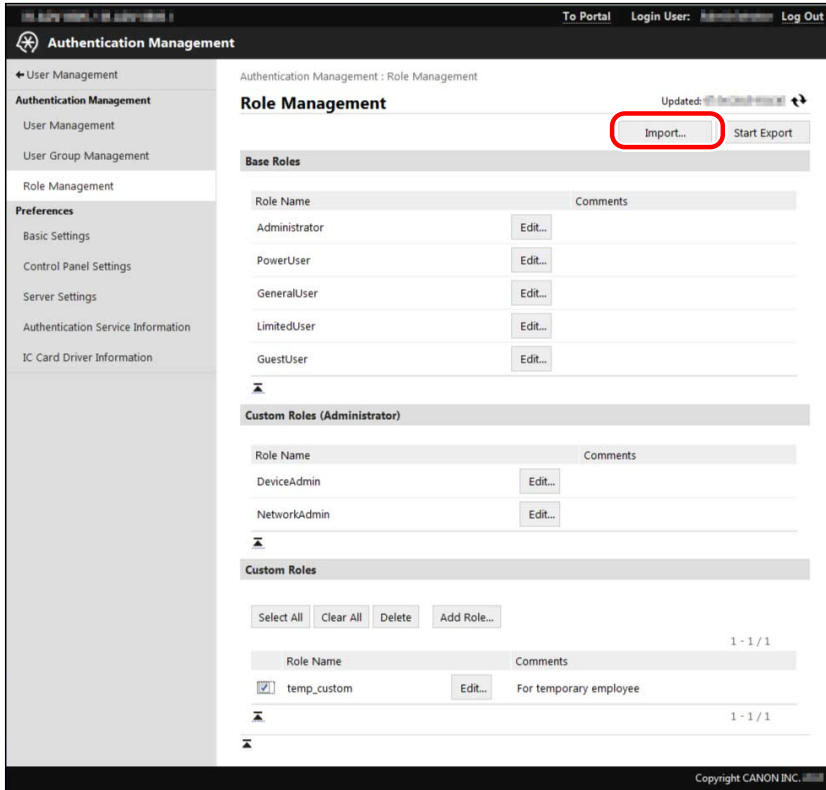
- If a role with the same name as a role to import already exists, that role is overwritten with the imported role information. However, only comments are overwritten for base roles other than the guest role and custom roles (administrator).
- If the [Device Management Restriction] setting is invalid (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.

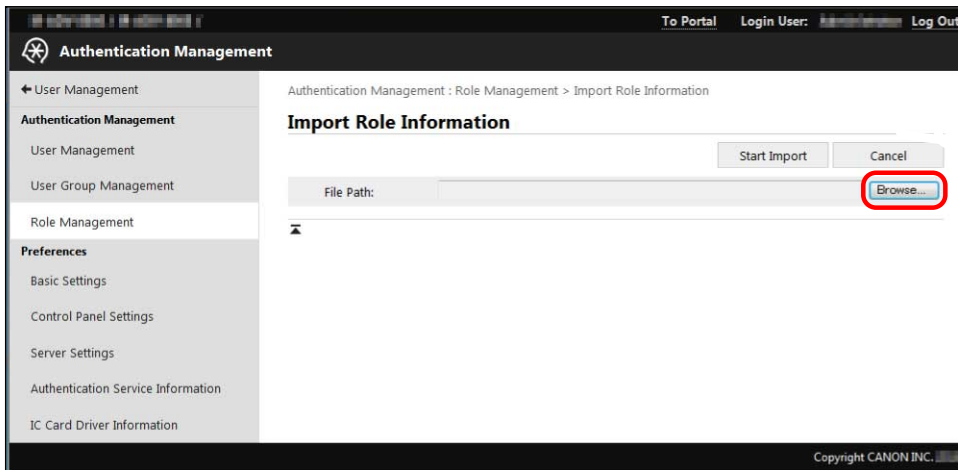
For more information, see "Logging in to User Authentication."(P. 49)

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

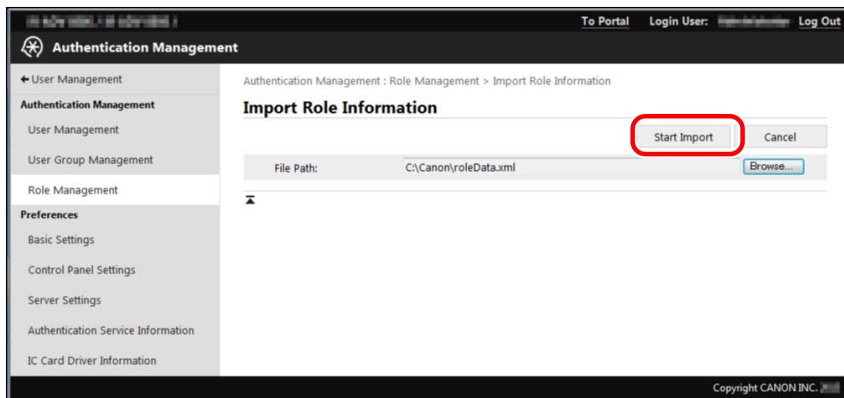
**3** Click [Import].



**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**

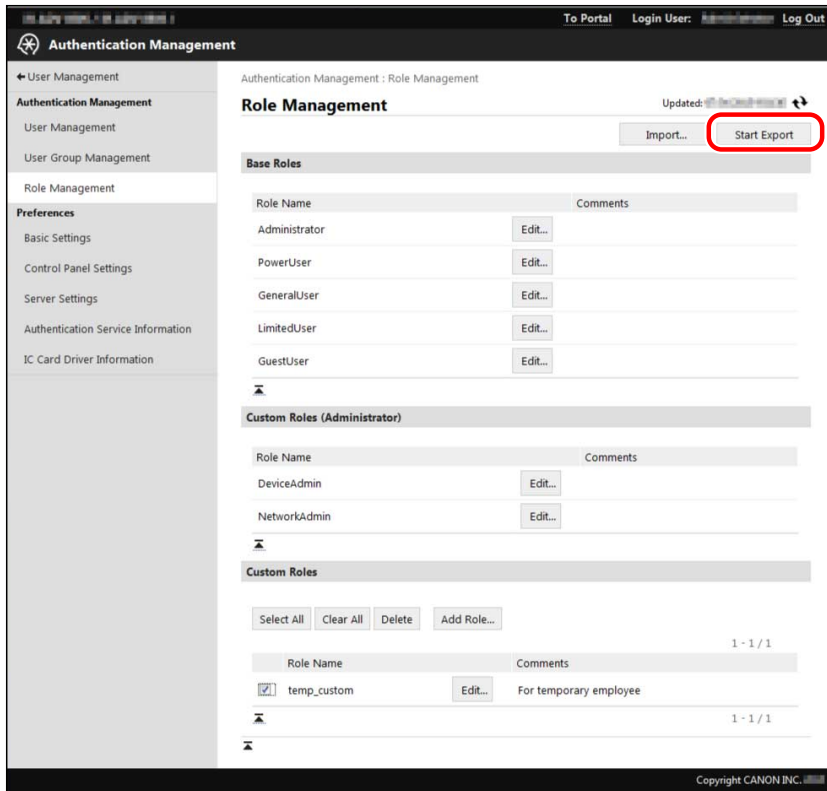
- The file extension is 'xml' and the default file name is 'roleData.xml'.
- It is also possible to export the role and edit it with a text editor. This is useful when you want to change the role names. However, take care not to edit the control characters in this case.

### 1 Log in to User Authentication.

For more information, see "**Logging in to User Authentication.**"(P. 49)

### 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

<b>Setting Up the Client Computers</b> .....	77
<b>Installing the AMS Printer Driver Add-in</b> .....	78
<b>Setting User Information to the AMS Printer Driver Add-in</b> .....	85

## Setting Up the Client Computers

---

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



## Installing the AMS Printer Driver Add-in

In the Access Management System, it is necessary to add the AMS Printer Driver Add-in to the printer driver installed in the computers to restrict printing from.

- ▶ **Preparing to Install the AMS Printer Driver Add-in(P. 78)**
- ▶ **Installing the AMS Printer Driver Add-in(P. 79)**

### IMPORTANT

- The AMS Printer Driver Add-in may already be included, depending on the printer driver. In this case, it is not necessary to install the AMS Printer Driver Add-in. Select [Use AMS Function] on the [AMS] page of the printer driver to enable the functions of the AMS Printer Driver Add-in.
- Confirm that the printer driver supports AMS before installing the AMS Printer Driver Add-in. The add-in will not be installed correctly unless the printer driver supports it. For more information, see "**Client Computer (AMS Printer Driver Add-in).**"(P. 38)
- Before installing the AMS Printer Driver Add-in, it is necessary to confirm that the Access Management System setup is complete. For more information, see "**Setting Up the Access Management System.**"(P. 41)
- If you want to restrict the printing of jobs from printer drivers in which the AMS Printer Driver Add-in is not installed, do so when specifying the preferences of the devices. For more information, see "**Prohibiting the Printing from Drivers without AMS Printer Driver Add-in**"(P. 56) .
- If you are using User Authentication with server authentication, it cannot be used in conjunction with the Department ID Management function. Disable the Department ID Management function of the printer driver.
- When using the AMS Printer Driver Add-in in a shared printer environment, install the AMS Printer Driver Add-in to the printer drivers on the print server. (Install the AMS Printer Driver Add-in to the printer driver on the print server. After installing the AMS Printer Driver Add-in to a printer driver on the print server, it may take some time until the [AMS] page is displayed in the printer properties dialog box on a client computer. If the [AMS] page is still not displayed, add the printer icon to the client computer.)
- 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.
- It may not be necessary to install the AMS Printer Driver Add-in, depending on your environment. For more information, see "**Access Management System Configurations**(P. 34) ."

### NOTE

- When installing to multiple computers, you can use the silent installation function. For more information, contact your local authorized Canon dealer.
- If you install the AMS Printer Driver Add-in to a printer driver, the [AMS] page is added to all printer icons associated with that printer driver.

## Preparing to Install the AMS Printer Driver Add-in

Before installing the AMS Printer Driver Add-in, update the printer driver to install it in.

 **IMPORTANT**

- If AMS Printer Driver Add-in V1.x is installed, uninstall it using the version 1.x uninstaller, and then update the printer driver. For more information, see "**Uninstalling the AMS Printer Driver Add-in.**"(P. 143) If AMS Printer Driver Add-in V2.0 or later is installed, you can update the printer driver without uninstalling the add-in.

 **NOTE**

- If the printer driver is not installed with [Standard TCP/IP Port], it is recommended you update it with [Standard TCP/IP Port].

- 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 Update the printer driver to install the AMS Printer Driver Add-in, and install the Canon Driver Information Assist Service.**

The Canon Driver Information Assist Service can be installed at the same time as updating the printer driver. Follow the instructions in the update wizard to install the Canon Driver Information Assist Service.

 **IMPORTANT**

- Update the printer driver using the latest installer (Setup.exe). The latest installer can be downloaded from the Canon Web site.

 **NOTE**

- For information on updating the printer driver, see the instruction manual for the printer driver.

## Installing the AMS Printer Driver Add-in

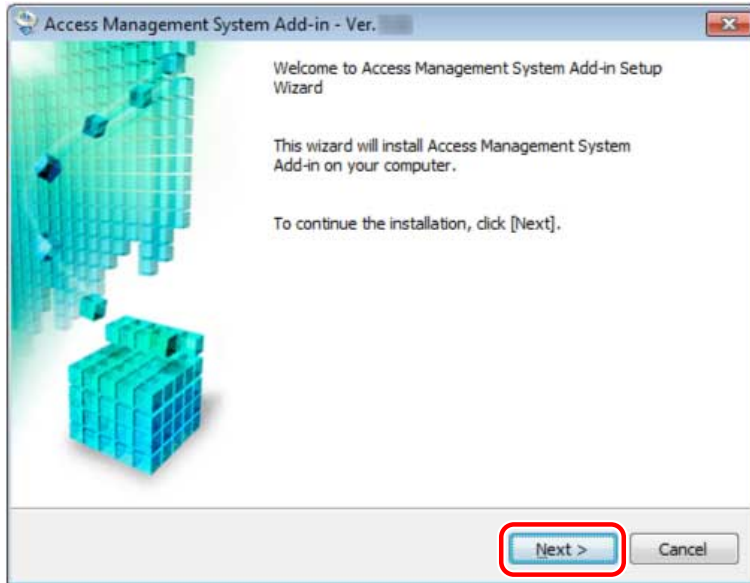
This section describes the procedure for installing the AMS Printer Driver Add-in individually in the computers to restrict printing for.

- 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.**

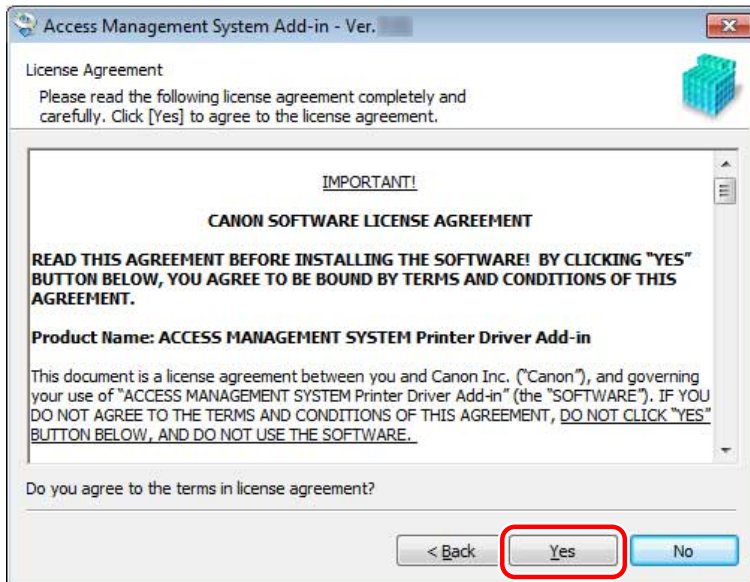
**4 Double-click the Setup.exe file for the AMS Printer Driver Add-in.**

The AMS Printer Driver Add-in setup wizard starts.

**5 Click [Next].**

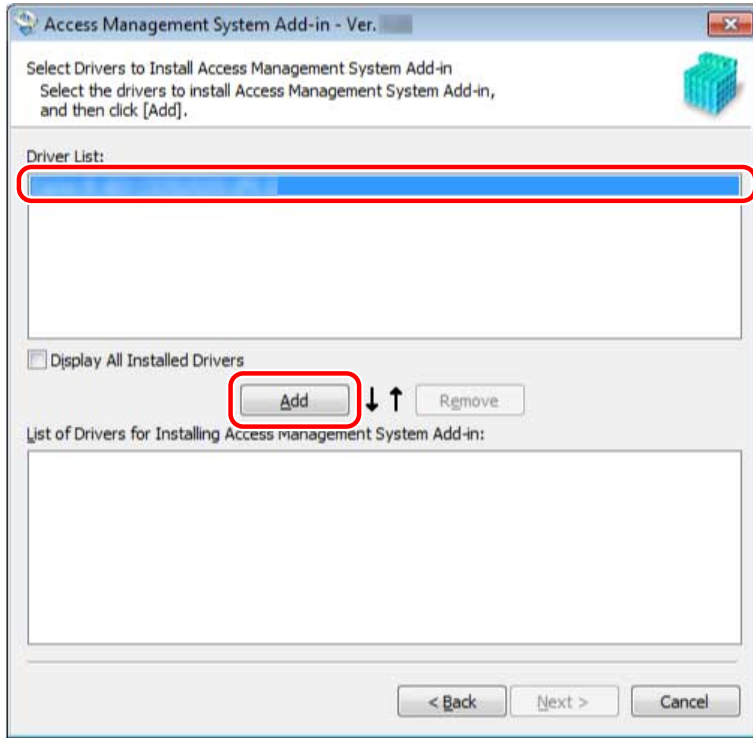


**6 Confirm the displayed information → click [Yes].**

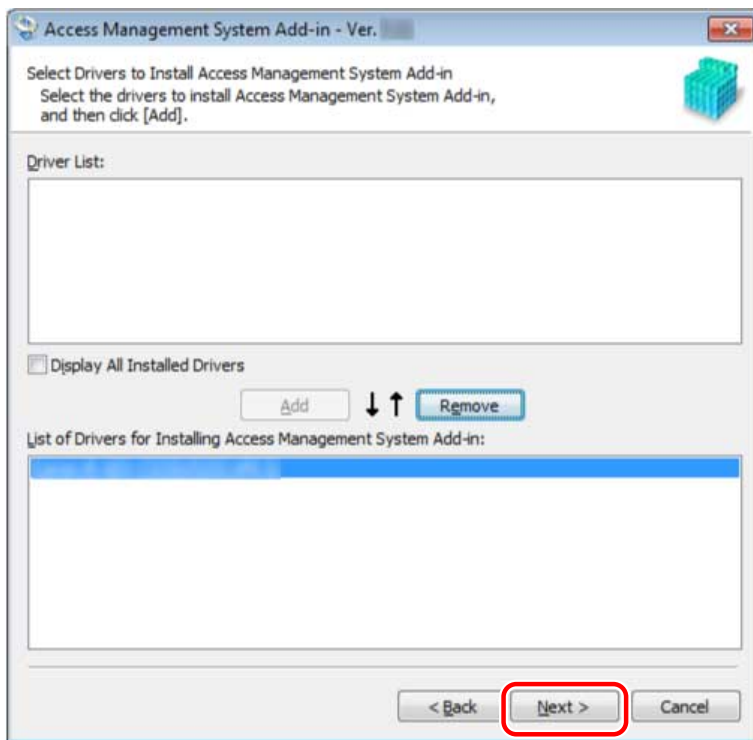


**7 Select the driver to install the AMS Printer Driver Add-in to from the [Driver List] → click [Add].**

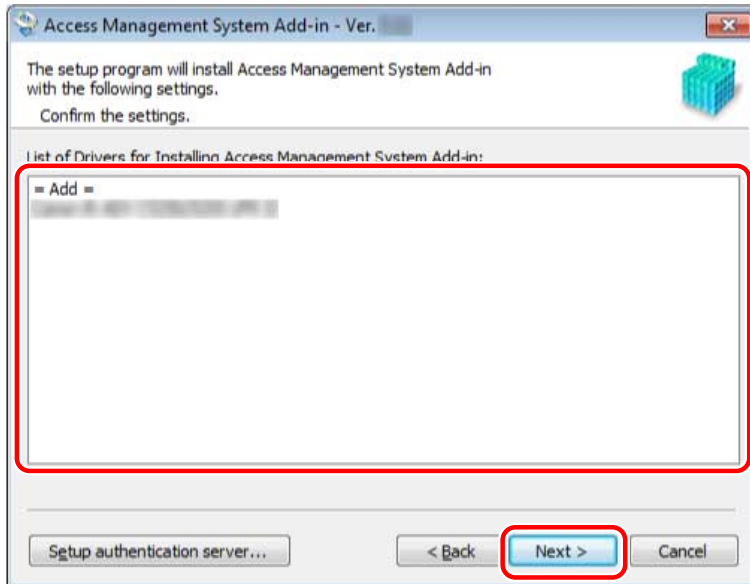
When a desired printer driver is not displayed or a printer driver exists but does not have a printer icon (for the server of a terminal service, etc.), select [Display All Installed Drivers].



**8** Click [Next].



**9** Confirm that the appropriate driver names are displayed in [List of Drivers for Installing Access Management System Add-in] → click [Next].



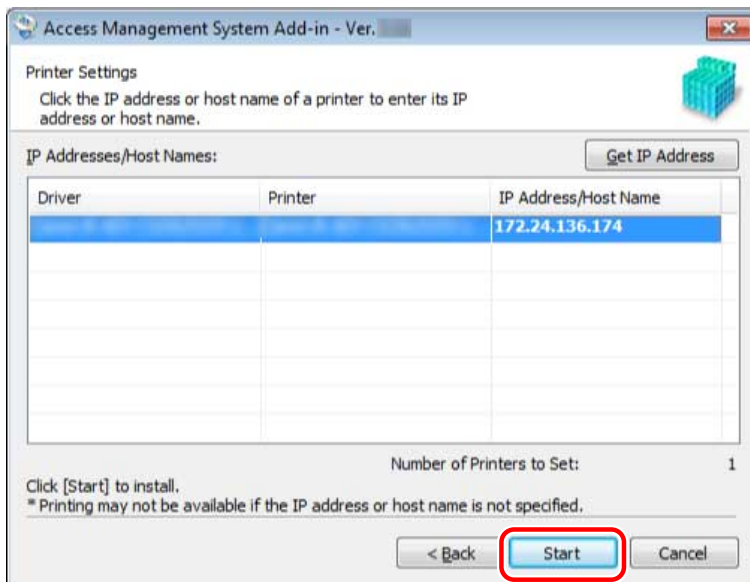
**10 Click [Yes] when the message confirming whether you want to retrieve the device (printer) information is displayed.**

If you click [No], the device information is not retrieved. Enter the IP address or host name of the printer on the next screen.

**11 Click [Start].**

If you clicked [No] in the previous page, click the [IP Address/Host Name] field for that driver → enter the IP address or host name of the device.

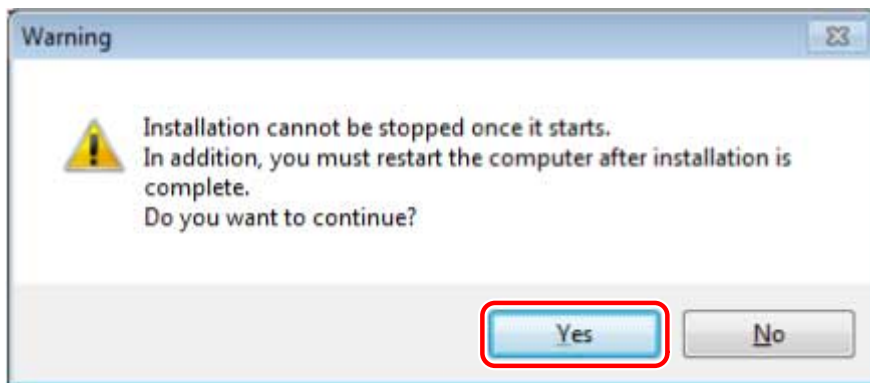
If [Enter IP Address/Host Name] is displayed in the [IP Address/Host Name] field, click [Get IP Address]. If the IP address cannot be retrieved, click the [IP Address/Host Name] field for that driver → enter the IP address or host name of the device.



**NOTE**

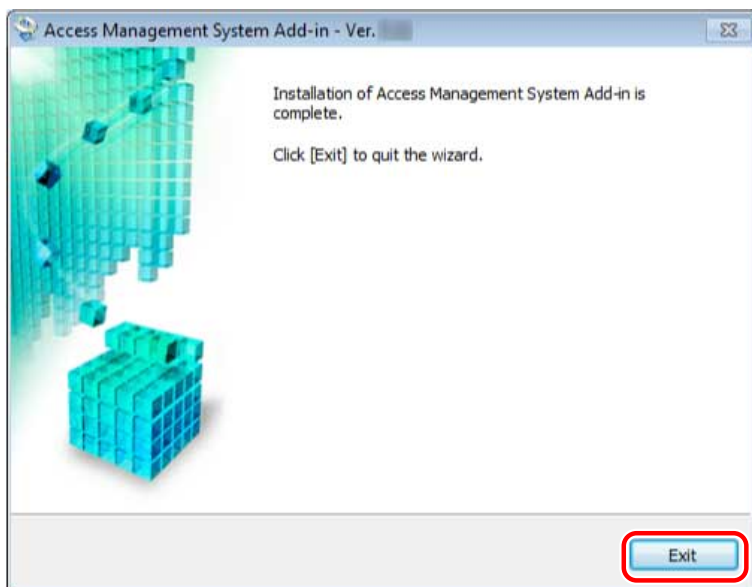
- If multiple printers that use the same printer driver are connected to the network, all of those printers are displayed in [IP Addresses/Host Names].

**12** Click [Yes] when the message confirming whether you want to start installing is displayed.

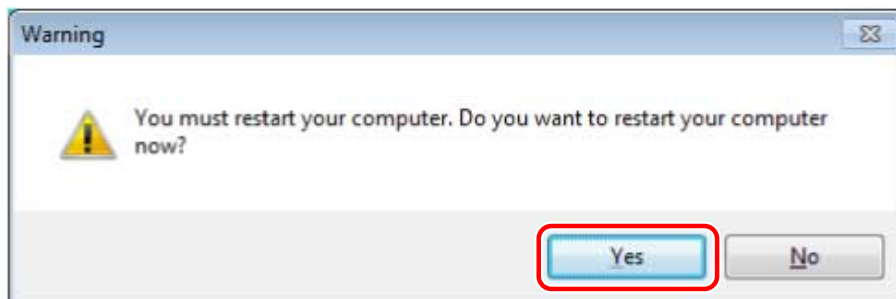


The AMS Printer Driver Add-in is installed.

**13** Click [Exit].



**14** Click [Yes] in the displayed dialog box.



The computer will be restarted and the installation completes.

**! IMPORTANT**

- It is necessary to set user information to the AMS Printer Driver Add-in installed in each computer. For more information, see "**Setting User Information to the AMS Printer Driver Add-in.**"(P. 85)

 **NOTE**

- If you want to restart the computer later, click [No].

# Setting User Information to the AMS Printer Driver Add-in

Set user information to the installed AMS Printer Driver Add-in, and retrieve print restriction information.

## NOTE

- For details on operating the AMS Printer Driver Add-in, see the Help for the AMS Printer Driver Add-in.
- If the currently logged in user sets user information in one [AMS] page, that information is applied to all the AMS Printer Driver Add-ins that the user uses on that computer.

## 1 Log on to the computer in which the AMS Printer Driver Add-in is installed.

### IMPORTANT

- When operating the Access Management System with Active Directory authentication, log on to the computer using the user name of a domain user.

## 2 Display the properties of the printer that use the printer driver in which the AMS Printer Driver Add-in is installed.

### For Windows Vista/Windows Server 2008:

- Select [Start] - [Control Panel] - [Hardware and Sound] - [Printers].
- Right-click the printer icon, and select [Properties].

### For Windows Server 2008 R2:

- Select [Start] - [Control Panel] - [Hardware] - [Devices and Printers].
- Right-click the printer icon, and select [Properties].

### For Windows 7:

- Select [Start] - [Control Panel] - [Hardware and Sound] - [Devices and Printers].
- Right-click the printer icon, and select [Printer properties].

### For Windows 8.1/Windows Server 2012:

- Move to the desktop and display the charm bar to the right of the screen.
- Select [Settings] - [Control Panel] - [View devices and printers].
- Right-click the printer icon, and select [Printer properties].

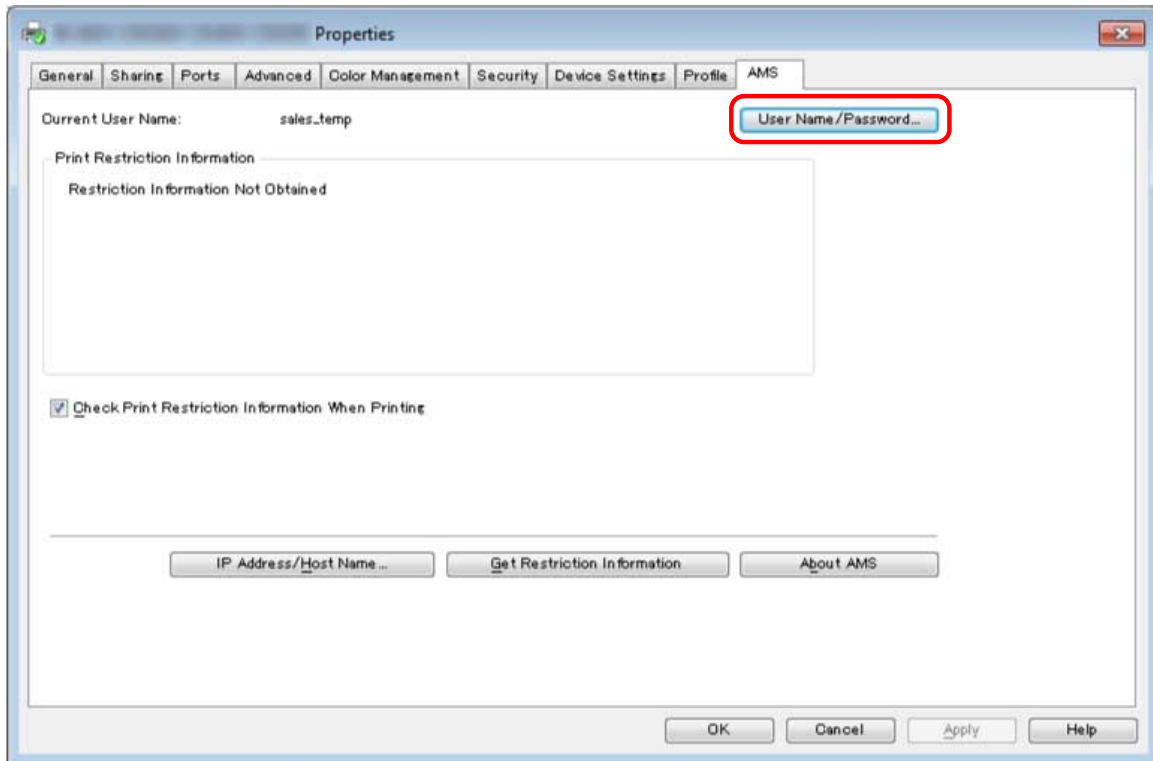


**For Windows 10/Windows Server 2016:**

- Right-click [Start], and select [Control Panel] - [Devices and Printers].
- Right-click the printer icon, and select [Printer properties].

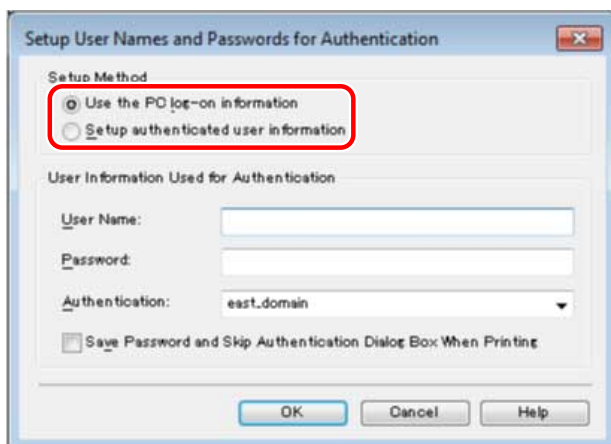
**3** Click the [AMS] tab.

**4** Click [User Name/Password].




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

**5** Select the method for setting the user information to use for authentication in [Setup Method].



**!** IMPORTANT

- [Use the PC log-on information] cannot be used when the AMS Printer Driver Add-in is used on an Active Directory server. Select [Setup authenticated user information].

 **NOTE**

- [Setup Method] is enabled when you are logged on to the computer as a domain user in an environment using Active Directory authentication. Otherwise, [Setup authenticated user information] is selected.

**6 Confirm that [This Device] is selected for [Authentication] → specify [User Name] and [Password].**


If you selected [Use the PC log-on information], proceed to step 7.

Contact the administrator in charge of usage restrictions for information on the user information to use for authentication.



 **IMPORTANT**

- If you are using local device authentication, select [This Device] for [Authentication]. If you are using Active Directory authentication, enter the domain name (NetBIOS name).

 **NOTE**

- If you select [Save password and skip authentication dialog box when printing], you can print without entering passwords. However, it is recommended you set to enter a password each time printing is performed, for increased security. [Save password and skip authentication dialog box when printing] is enabled if you select [Save user authentication information] in [Printer Driver Management] when specifying the preferences of the devices. For more information, "**Specifying the Preferences of the Devices.**"(P. 50)
- 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.

**7 Click [OK].**

The print restriction information is retrieved.

### IMPORTANT

- To retrieve print restriction information (role information etc.), the information must be registered in the device. For more information, "**Setting Up the Access Management System**"(P. 41) or "**Operation Example of Local Device Authentication.**"(P. 90)
- To change the IP address/host name of the device specified when installing the AMS Printer Driver Add-in, click [IP Address/Host Name].

### NOTE

- If you select [Check Print Restriction Information When Printing] on the [AMS] page, the [Confirmation of Print Restrictions] dialog box is displayed each time printing is performed, enabling you to check the print restriction information.
- 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.

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

### IMPORTANT

- If the print restriction information registered in the device is changed, click [Get Restriction Information] on the [AMS] page to retrieve the latest print restriction information. If the print restriction information registered in the device and the print restriction information in the AMS Printer Driver Add-in differ, an error will occur. Take care, as documents for which printing is only allowed once will become unable to be printed.

### NOTE

- If the following conditions are met, the AMS Printer Driver Add-in will automatically retrieve print restriction information when printing, and will update the currently retained print restriction information.
  - 30 minutes or more have elapsed since printing was last performed
  - Print restriction information has been changed by the administrator

# Operation Example of Local Device Authentication

<b>Operation Example of Local Device Authentication</b> .....	90
<b>Example of Operating with Local Device Authentication</b> .....	91
<b>Flow of Operations</b> .....	93
<b>Preparing the Device and Network Environment</b> .....	95
<b>Specifying the Preferences of the Devices</b> .....	96
<b>Creating Custom Roles</b> .....	105
<b>Exporting Custom Roles</b> .....	109
<b>Registering Local Users and Specifying Roles</b> .....	110
<b>Exporting User Information</b> .....	114
<b>Importing Roles and User Information</b> .....	115
<b>Starting the Department ID Management Function</b> .....	118
<b>Confirming the Login Method and Usage Restrictions on the Touch Panel Display</b> .....	124
<b>Setting Up the Client Computers</b> .....	130
<b>Confirming the Print Restrictions on Client Computers</b> .....	138

## **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).

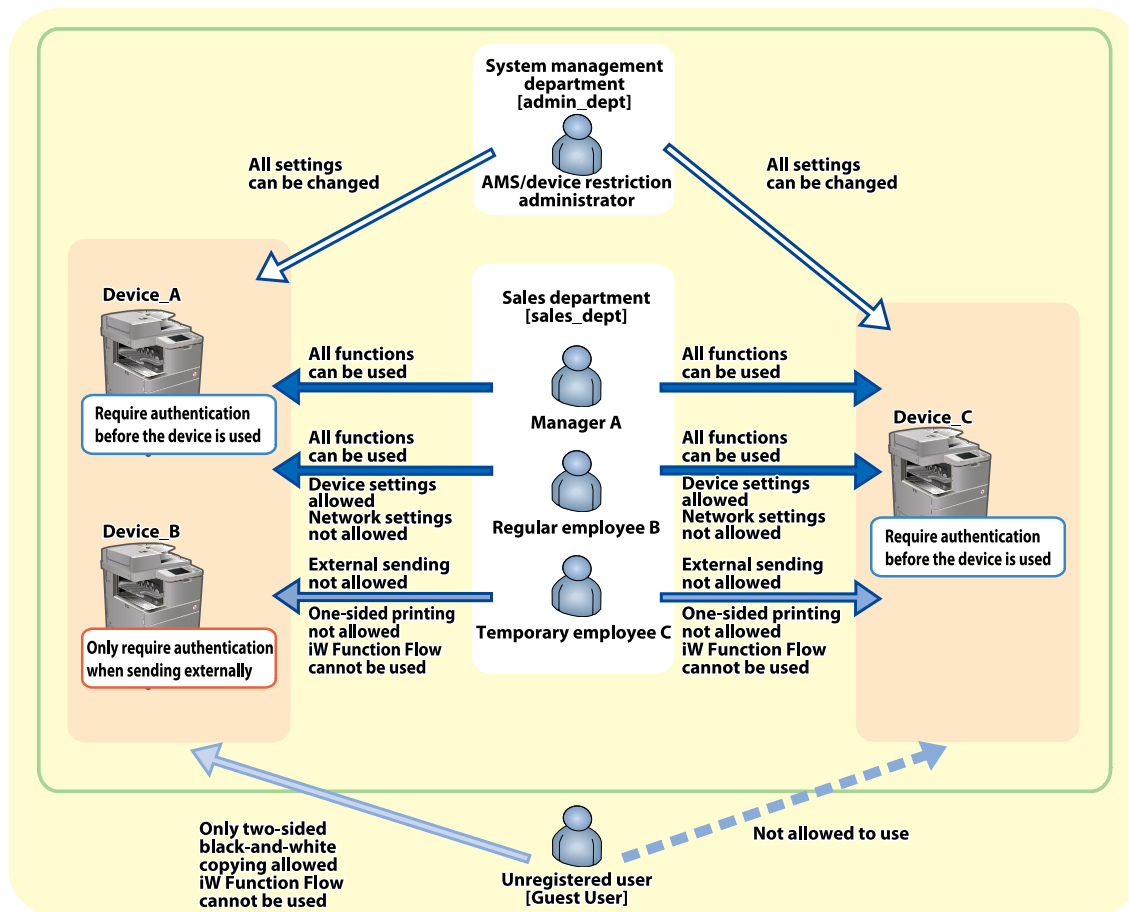
Three devices are used: Device\_A, Device\_B, and Device\_C. These three devices are the same model. These three devices all support using the Access Management System in conjunction with the Department ID Management function, and have the optional iW Function Flow added and started. These three devices 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)		

Operation Example of Local Device Authentication

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.
<b>System management department [admin_dept]</b> (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.
<b>Other Users</b>	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. 95)

---

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. 96)

---

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. 105)

---

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. 109)

---

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. 110)

---

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. 114)

---

Export the user information created on Device\_A.

## 9. Importing Roles and User Information(P. 115)

---

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. 118)

---

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. 124)

---

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. 130)

---

Install the AMS Printer Driver Add-in in all the client computers, and set the user information for each user.

## 13. Confirming the Print Restrictions on Client Computers(P. 138)

---

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. 95)**
- ▶ **Specifying the Network Settings(P. 95)**
- ▶ **Making Devices Accessible from Web Browsers(P. 95)**
- ▶ **Registering the System Manager ID(P. 95)**

### 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. 47)

### 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. 96)

## 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].

Canon Log In

User Name:

Password:

Login Destination:

Enter a user name, password, and specify a Login Destination and click [Log In].

Copyright CANON INC.

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

Authentication Management

Authentication Management : User Management

User Management Updated: 10/10/2010 10:10:10

The users with an asterisk (\*) are administrators.

Import... Export...

Select All Clear All Delete Add User... Check Unregistered Department ID...

Filter: User Name  Exact Match  Match case  Apply

Clear Filter

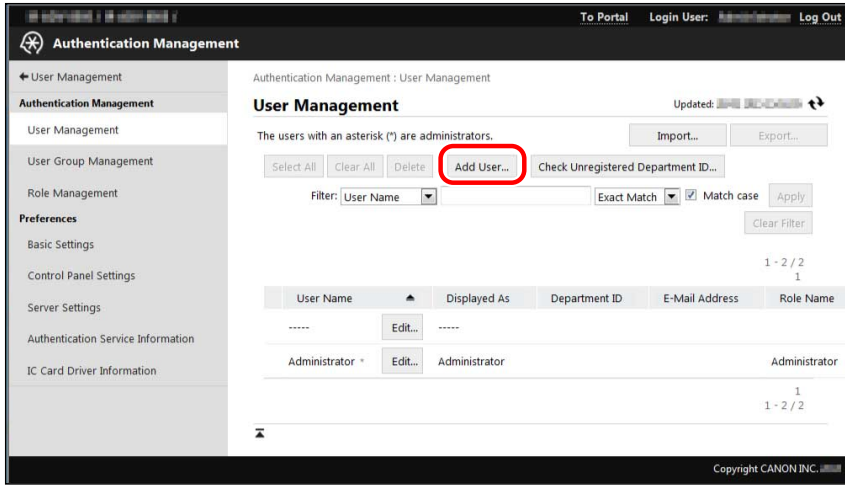
User Name	Displayed As	Department ID	E-Mail Address	Role Name
-----	Edit...	-----		
Administrator *	Edit...	Administrator		Administrator

1 - 2 / 2  
1

1 - 2 / 2  
1

Copyright CANON INC.


### 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. 95) 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].**

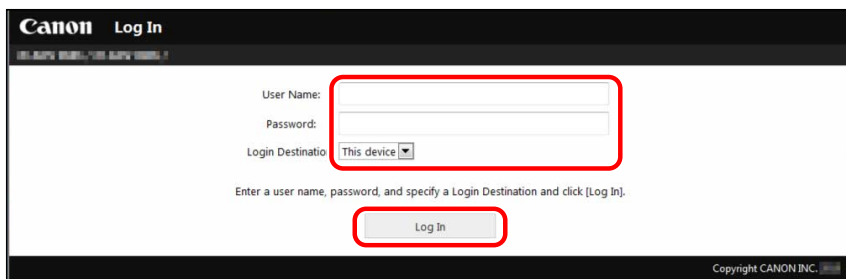
**7 Open your Web browser → enter the following URL:**

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].**

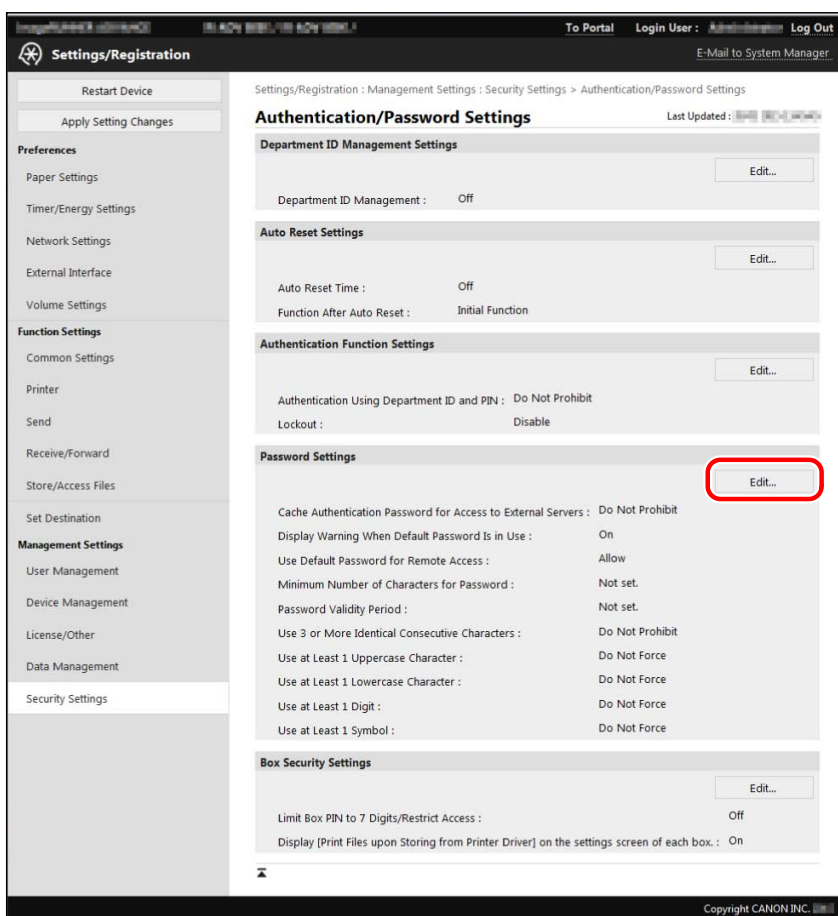
In this example, the following settings are specified:

[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].

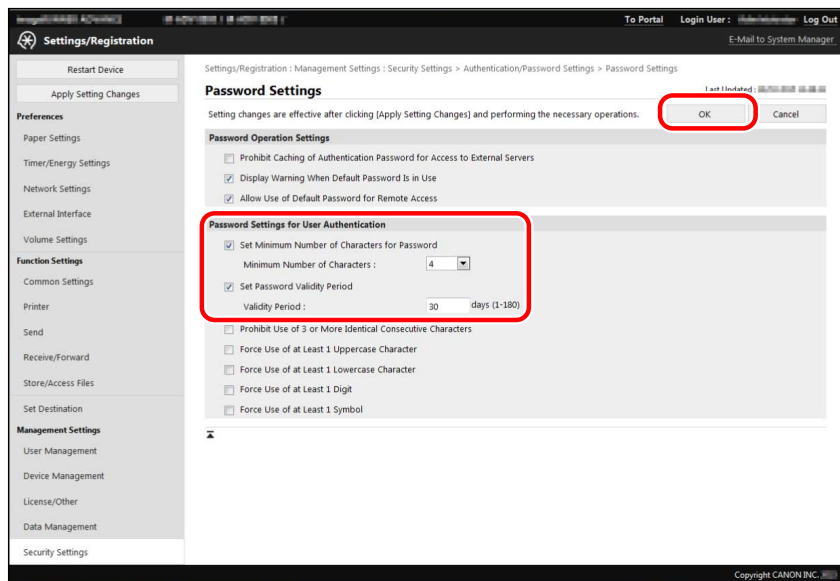


**11** Set the password policy in [Password Settings for User Authentication].

- 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].



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



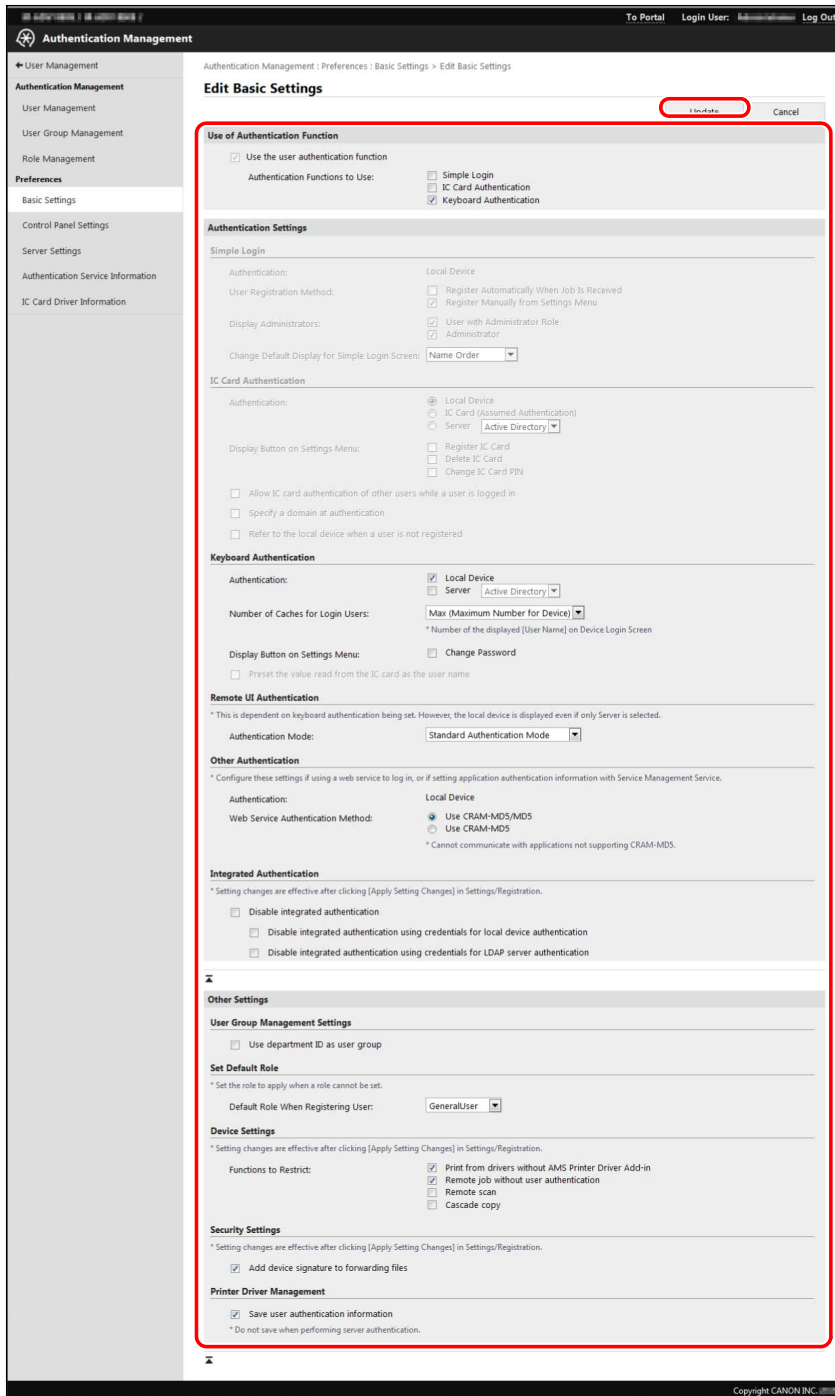
## 12 Specify [Preferences].

### NOTE

- For more information, see " **Specifying the Preferences of the Devices(P. 50)** " or instruction manuals of the device.

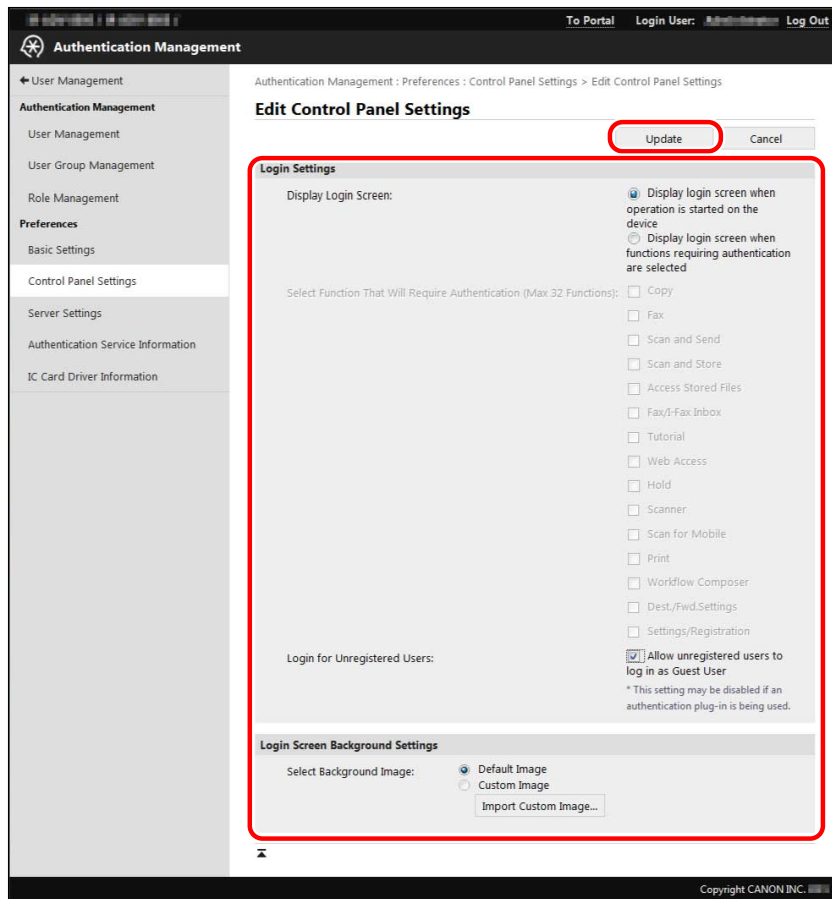
### [Basic Settings]

- ❑ Click [Settings/Registration] → [User Management] → [Authentication Management] → [Basic Settings].
- ❑ Click [Edit].
- ❑ Specify the required settings → click [Update].



### [Control Panel Settings]

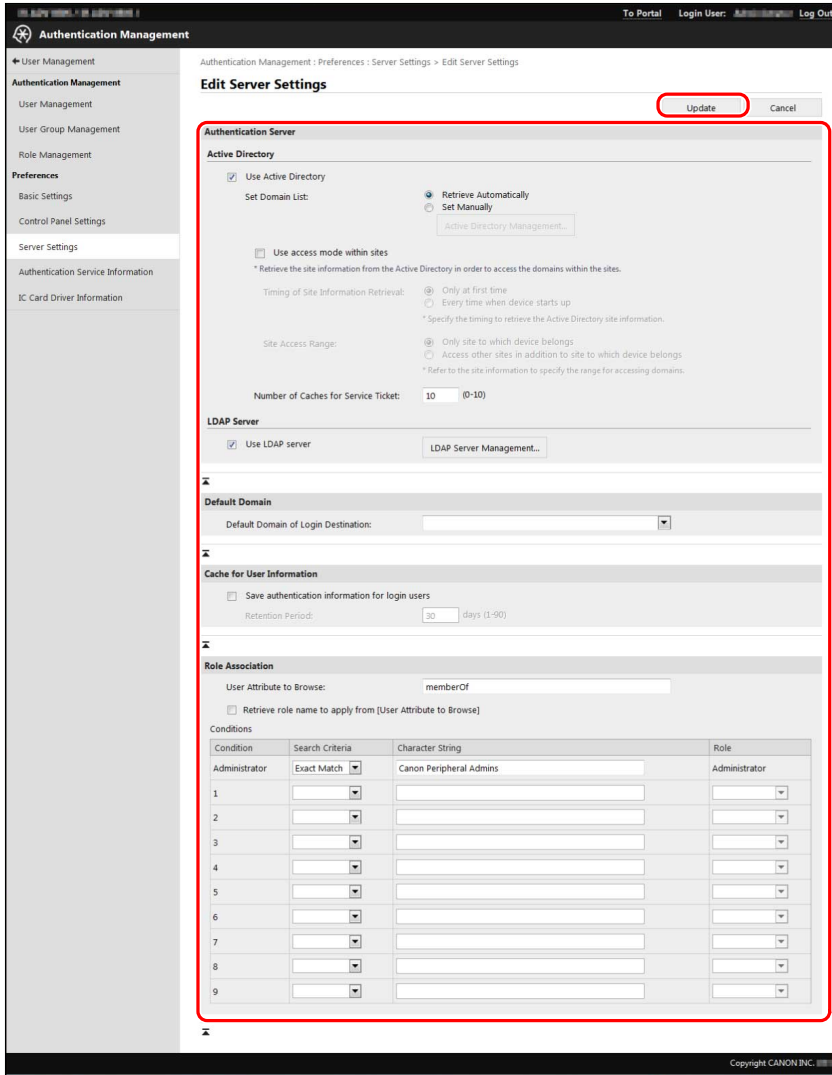
- ❑ Click [Settings/Registration] → [User Management] → [Authentication Management] → [Control Panel Settings].
- ❑ Click [Edit].
- ❑ Specify the required settings → click [Update].



### [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. 105)**
- ▶ **Editing [GuestUser] Role Registered(P. 108)**

### 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.

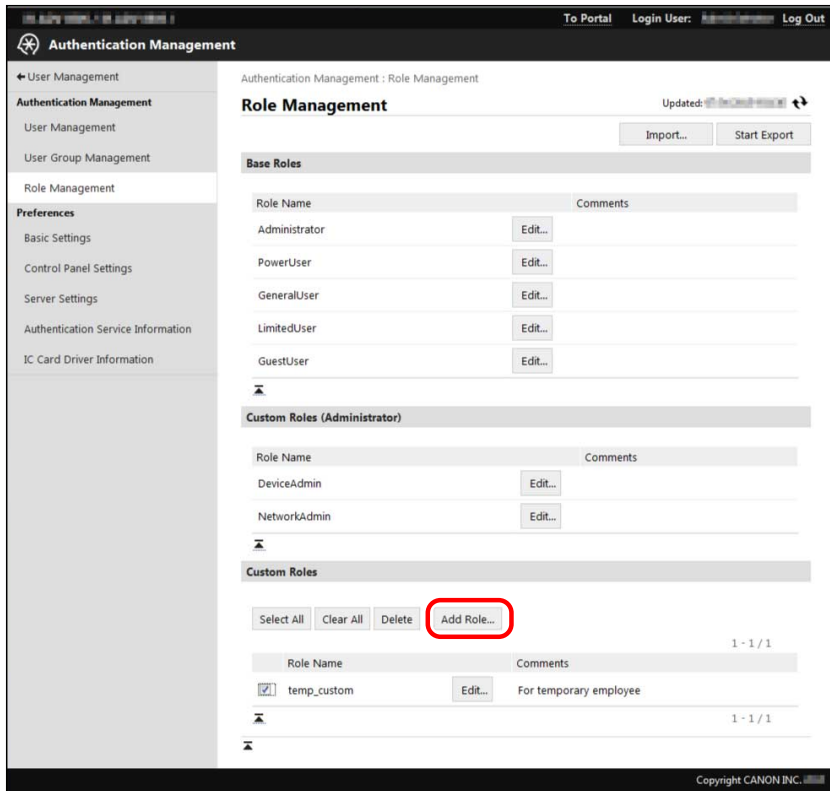
#### 2 Enter the user name and password of the device restriction administrator → select [This device] in [Login Destination] → click [Log In].

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. 64)**

# Operation Example of Local Device Authentication

The screenshot displays the 'Add Custom Role' configuration page in the Authentication Management system. The role name is 'temp\_custom' and it is intended for temporary employees. The configuration includes various restrictions for device management, function categories, and application-specific settings.

**Role Information:**

- Role Name: temp\_custom (Maximum 32 Characters)
- Comments: For temporary employee (Maximum 50 Characters)
- Base Role: GeneralUser

**Device Management Restriction:**

- All Settings: Restrictions
- Network Settings: Not allowed
- Device Settings: Not Allowed

**Function Category Restriction:**

- Print Functions: Allowed
- Save Functions (Mail Box/Memory Media): Allowed
- Copy Functions: Allowed
- Send Functions/Store on Network: Not Allowed
- Web Access Function: Allowed
- Utility Function: Allowed
- Others Functions: Allowed

**Function Category Restriction Details:**

- Print Functions:** Print (Allowed), 1-Sided/2-Sided Printing (2-Sided Printing Only), Page Layout (No Restrictions), Save to Mail Box (Allowed).
- Save Functions (Mail Box/Memory Media):** Print (Allowed), 1-Sided/2-Sided Printing (No Restrictions), Page Layout (No Restrictions).
- Save Function (Memory Media):** Memory Media (Allowed), Scan (Allowed), Print (Allowed).
- Copy Functions:** 1-Sided/2-Sided Copying (2-Sided Copying Only), Page Layout (No Restrictions).
- Scan Functions:** Scan (Allowed), Color Scan (Allowed).
- Send Functions/Store on Network:** E-Mail TX (Allowed), E-Mail TX (Use [Send to Myself]): (Allowed), F-Fax TX (Allowed), Fax TX (Allowed), FTP TX (Allowed), Windows (SMB) TX (Allowed), WebDAV TX (Allowed), Use (Personal Folder): (Allowed), Mail Box TX (Allowed), Specify Address Domain (Not Allowed), Use Address Book/Register Storage Location for Network: (Read-Only), Use Personal Address List (Allowed), Send to New Addresses (Allowed), Add Device Signature to Sending Files: (Not Added), Sending Files Format: (No Restrictions).

**Application Restrictions:**

Application Name	Status	Application ID
Copy	Not Set	8c72686d-29c2-46c5-a07a-86c4177a61e3
Scan and Send	Not Set	ae53008a-aab1-4aae-95c7-d746db532c88
Access Stored Files	Not Set	3d9b3c08-e4b5-4777-be55-fe0cd92f6d9
Web Access	Not Set	a2071ad7-7717-4817-9d2f-9dc71d91b7b
Hold	Not Set	18326034-010c-1000-a4e-00e0004ae6f
Scan for Mobile	Not Set	18d9822c-0140-1000-a701-00e0004ae6f
Print	Not Set	3c3527f-c0140-1000-9911-00e0004ae6f
IW Function Flow	Not Allowed	

**Button Restrictions:**

Button/Applet Name	Status	Application Name
Copy	Not Set	Copy
Fax	Not Set	Scan and Send
Scan and Send	Not Set	Scan and Send
Scan and Store	Not Set	Access Stored Files
Access Stored Files	Not Set	Access Stored Files
Fax/F-Fax Inbox	Not Set	Access Stored Files
Tutorial	Not Set	Tutorial
Web Access	Not Set	Web Access
Hold	Not Set	Hold
Scanner	Not Set	Scan
Scan for Mobile	Not Set	Scan for Mobile
Print	Not Set	Print
IW Function Flow	Not Set	IW Function Flow
Dest./Fwd.Settings	Not Set	Scan and Send

The [temp\_custom] role is registered.

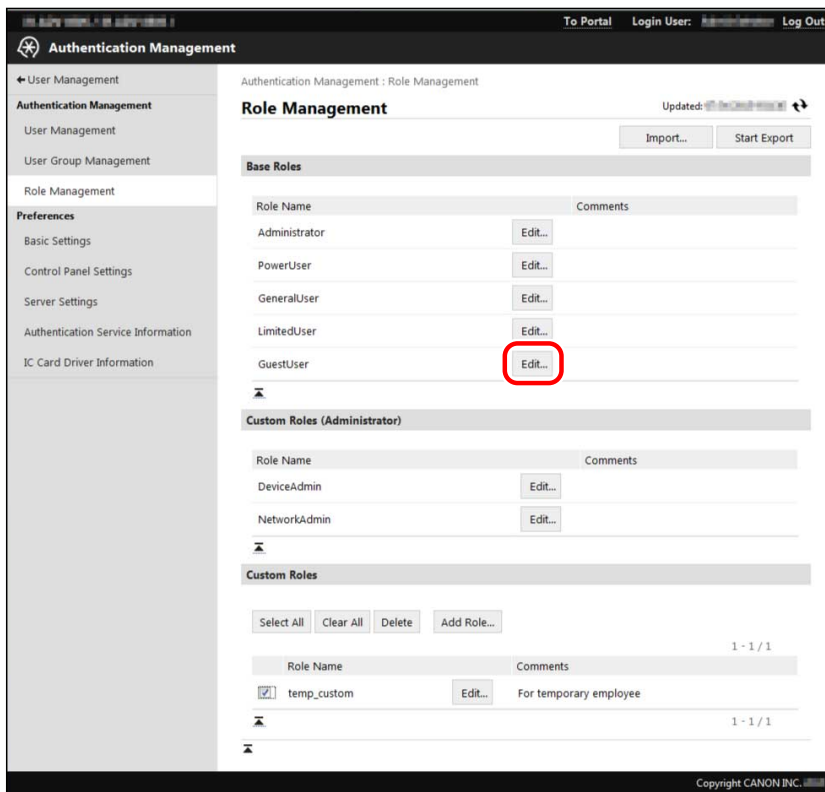
## Editing [GuestUser] Role Registered

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.

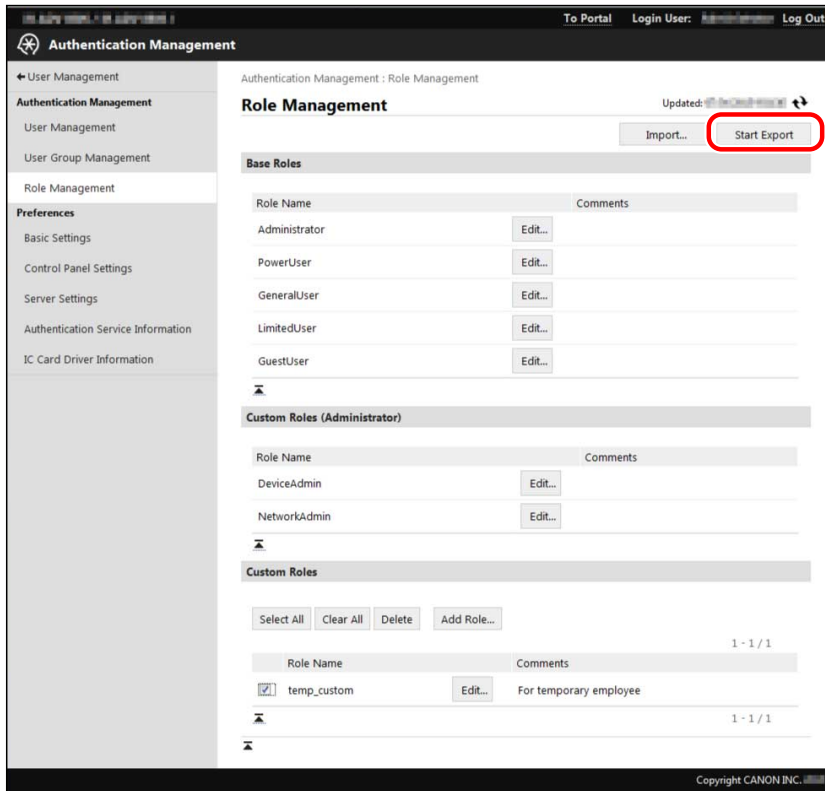
In this example, confirm that the content of the [GuestUser] role has not been changed. For information on each setting, see "Device Function Restrictions."(P. 26)

### 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'.

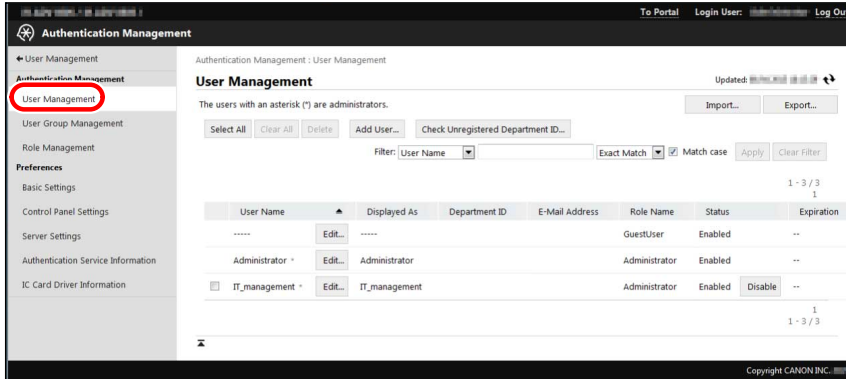
### 3 Click [Log Out].



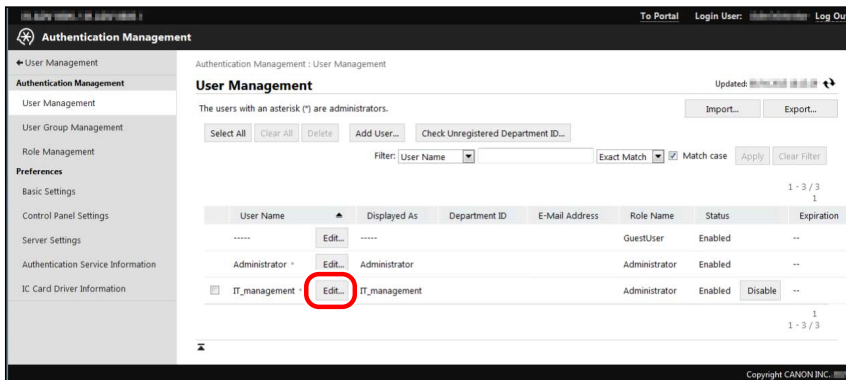
# Registering Local Users and Specifying Roles

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.

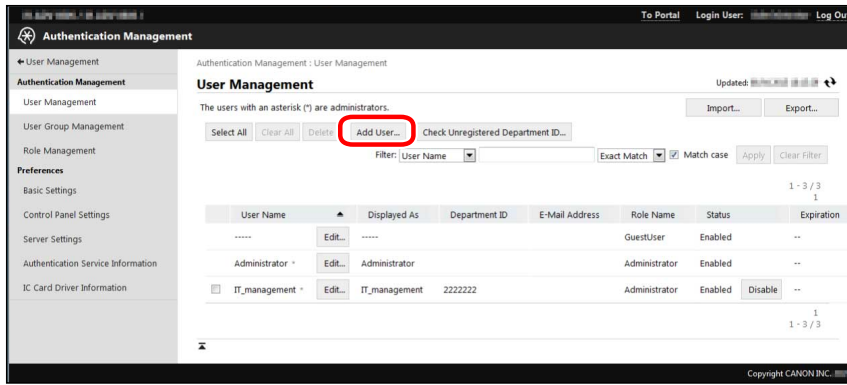


- 3 Specify the required settings → click [Update].

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]

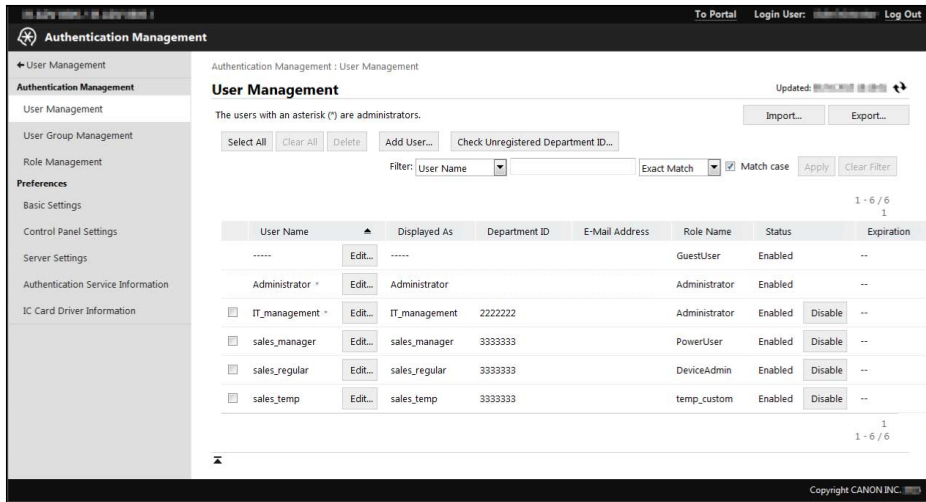
The screenshot shows the 'Add User' form in the Authentication Management interface. The form is divided into several sections:

- Authentication Information:** This section is highlighted with a red box. It contains fields for 'User Name' (Maximum 32 Characters), 'Password' (Maximum 32 Characters), 'Confirm' (Maximum 32 Characters), 'PIN' (Max 7 Digits), and 'Confirm' (Maximum 32 Characters).
- User Information:** This section contains fields for 'Displayed As' (Maximum 32 Characters), 'E-Mail Address' (Maximum 256 Characters), and 'Icon' (with an 'Icon Settings...' button).
- Department ID Settings:** This section contains a 'Department ID' field (Not set) and a 'Department ID Settings...' button.
- Role Settings:** This section contains a 'Select Role to Set' dropdown menu (GeneralUser).
- IC Card Registration Information:** This section contains fields for 'ID to Register for IC Card 1' (Maximum 128 Characters), 'Verification Value' (2147483647), 'ID to Register for IC Card 2' (Maximum 128 Characters), and 'Verification Value' (2147483647).
- User Account Settings:** This section contains checkboxes for 'Set expiration for the user account' and 'Disable the user account', along with an 'Expiration' field (Specify with Calendar).
- User Group Association:** This section contains two columns: 'Registered User Groups' and 'Associated User Groups', with 'Add >>' and '<< Remove' buttons.

The 'Add' button is highlighted with a red box. The 'Authentication Information' section is also highlighted with a red box.

The user information is registered.

## Operation Example of Local Device Authentication



The screenshot shows the 'Authentication Management' web interface. The main content area is titled 'User Management' and displays a table of users. The table has the following columns: User Name, Displayed As, Department ID, E-Mail Address, Role Name, Status, and Expiration. The users listed are: Administrator (marked with an asterisk), IT\_management (marked with an asterisk), sales\_manager, sales\_regular, and sales\_temp. The status for all users is 'Enabled'. The interface includes a sidebar with navigation options like 'User Management', 'Role Management', and 'Preferences'. At the top right, there are links for 'To Portal', 'Login User', and 'Log Out'.

User Name	Displayed As	Department ID	E-Mail Address	Role Name	Status	Expiration
-----	-----			GuestUser	Enabled	--
Administrator *	Administrator			Administrator	Enabled	--
<input type="checkbox"/> IT_management *	IT_management	2222222		Administrator	Enabled	Disable --
<input type="checkbox"/> sales_manager	sales_manager	3333333		PowerUser	Enabled	Disable --
<input type="checkbox"/> sales_regular	sales_regular	3333333		DeviceAdmin	Enabled	Disable --
<input type="checkbox"/> sales_temp	sales_temp	3333333		temp_custom	Enabled	Disable --

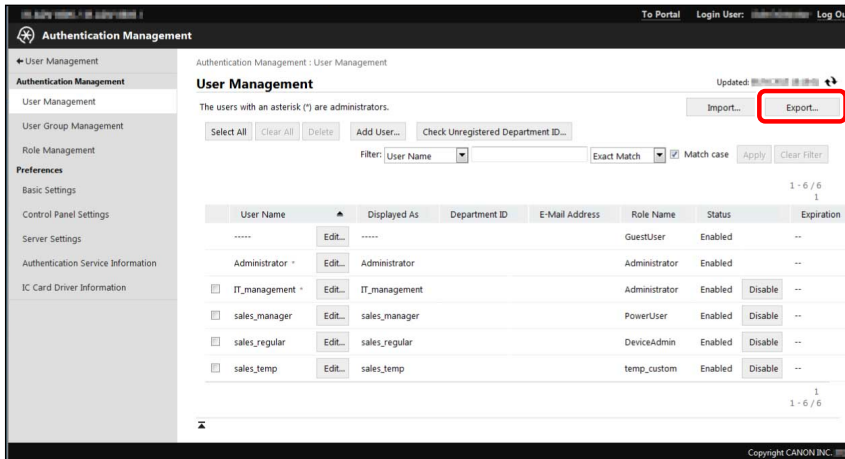
### NOTE

- 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.

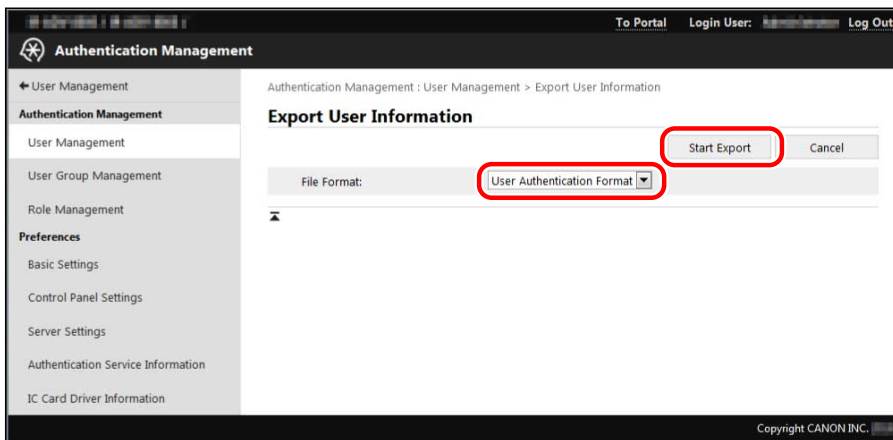
# Exporting User Information

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. 115)**

## 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>

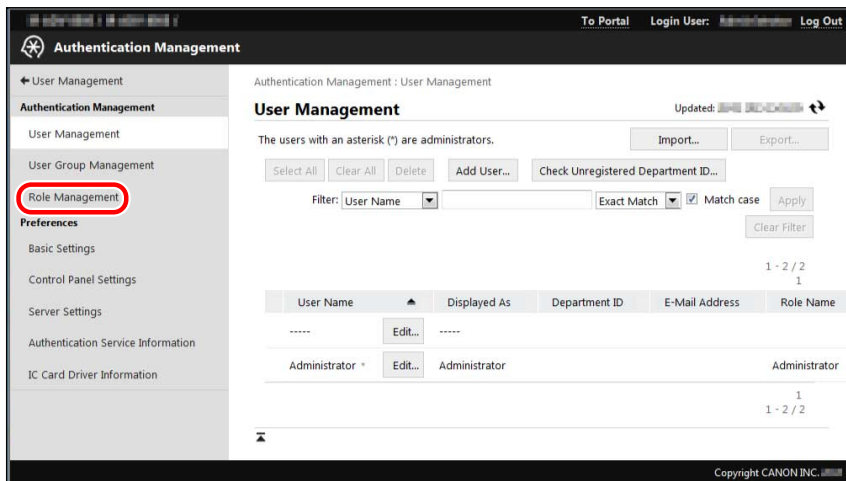
The [Login] page is displayed.

**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]

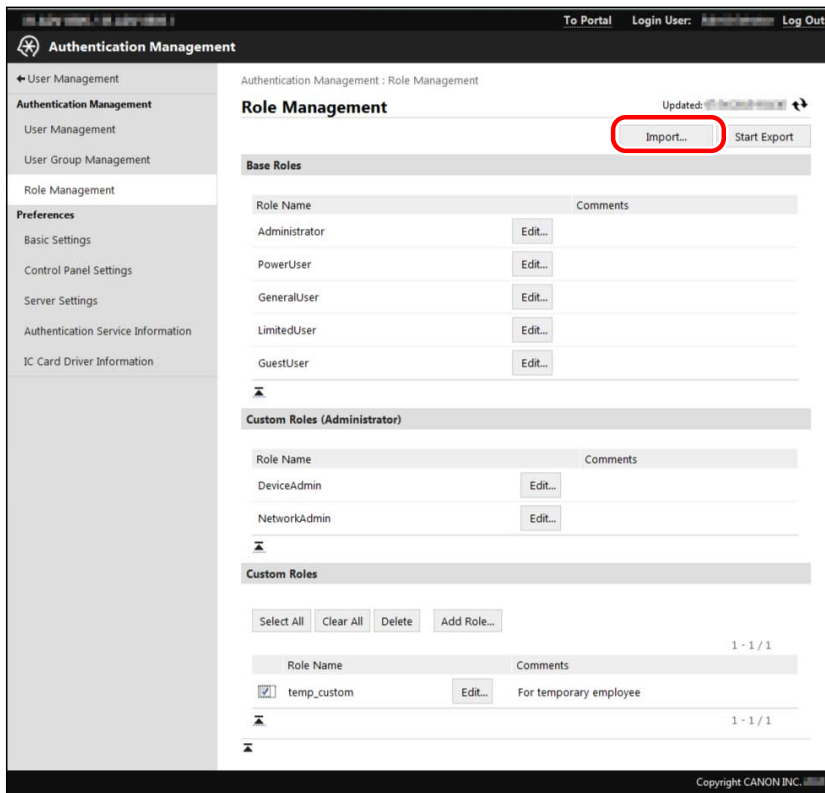
**3 Click [Settings/Registration] → [User Management] → [Authentication Management] → [Role Management].**



**IMPORTANT**

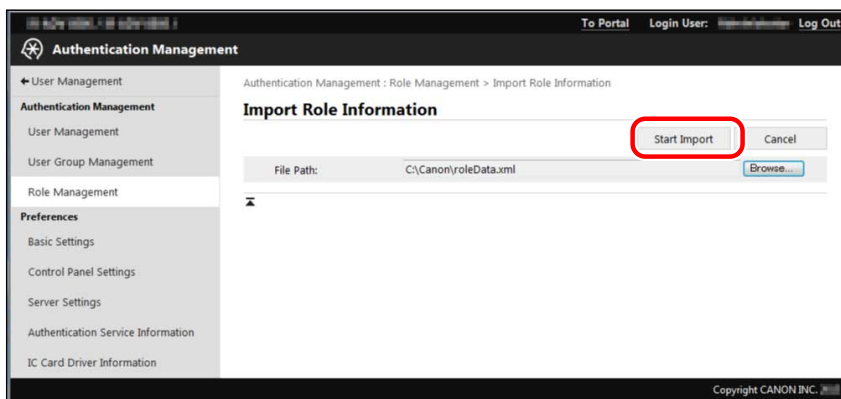
- If a role with the same name as a role to import already exists, that role is overwritten with the imported role information.

**4 Click [Import].**



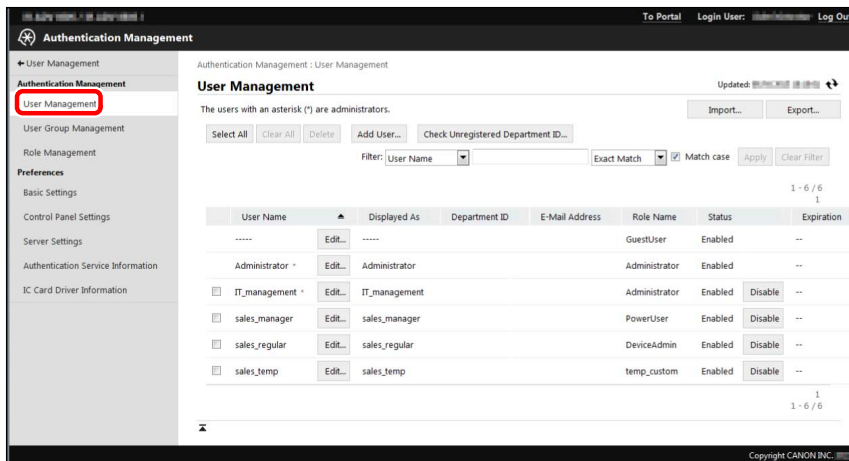
**5 Click [Browse] to select the file to import.**

**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].**

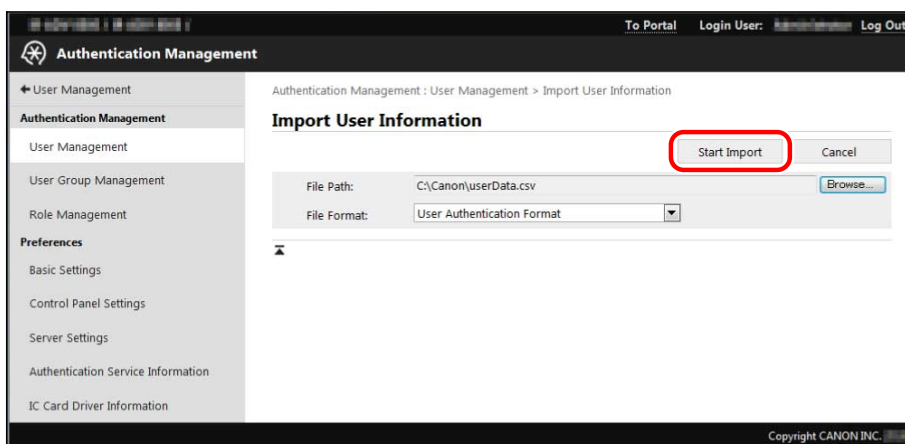
**9 Click [Browse] to select the file to import.**

**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. 118)

#### ! 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.

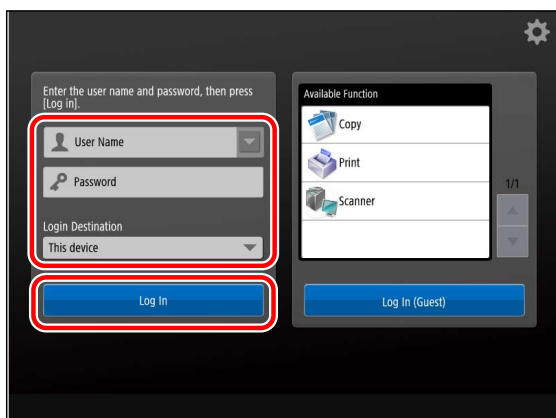
## Starting the Department ID Management Function on Device\_A and Device\_C

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]

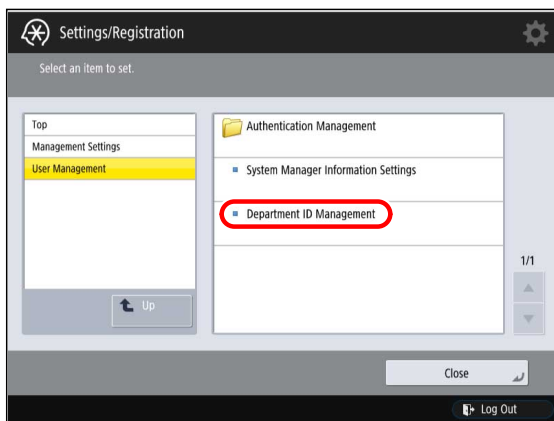
### Device\_A



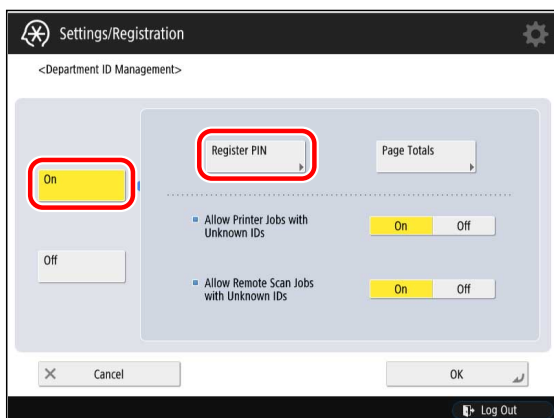
## Device\_C



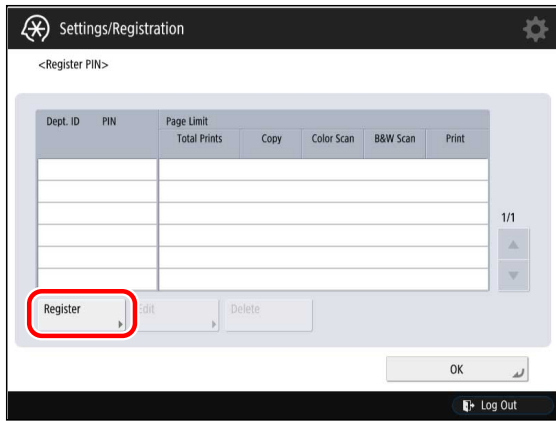
- 2** Press  (Settings/Registration) → [Management Settings] → [User Management] → [Department ID Management].



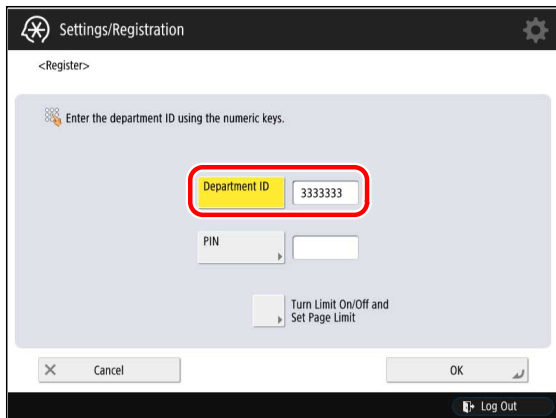
- 3** Press [On] → [Register PIN].



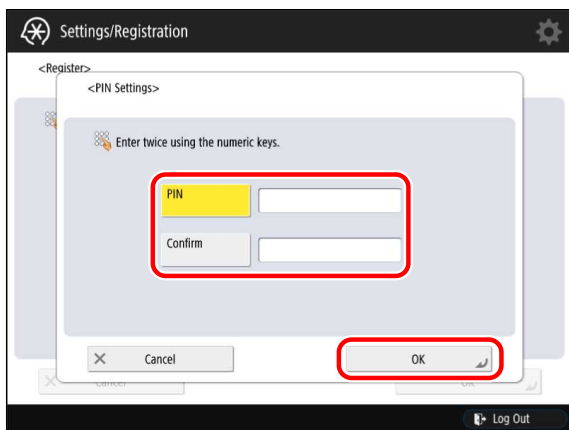
- 4** Press [Register].



**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).**

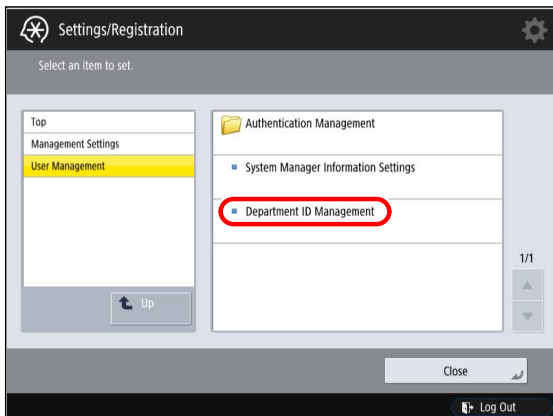
**2 Enter the user name and password of the device restriction administrator → select [This device] in [Login Destination] → press [Log In].**

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

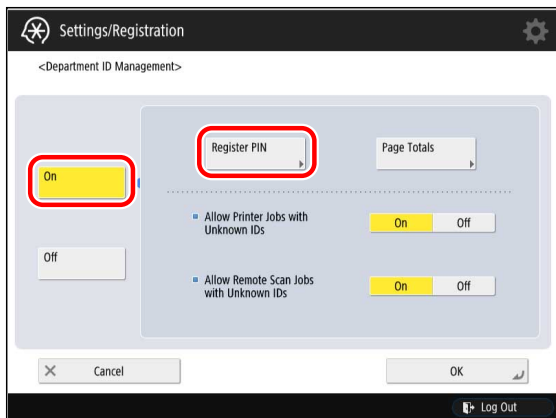


**3 Press [Device Settings].**

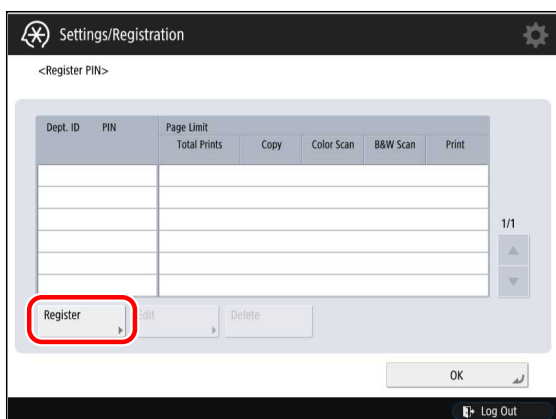
**4 Press [Management Settings] → [User Management] → [Department ID Management].**



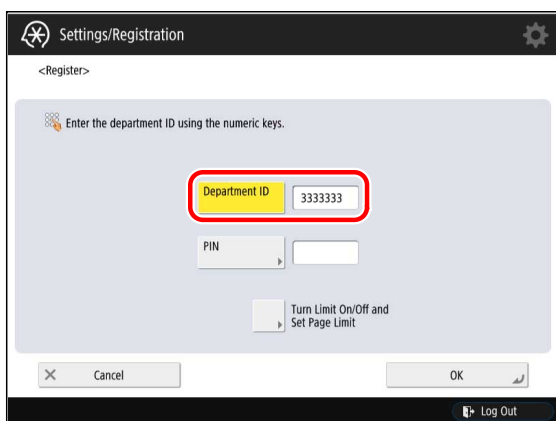
**5 Press [On] → [Register PIN].**



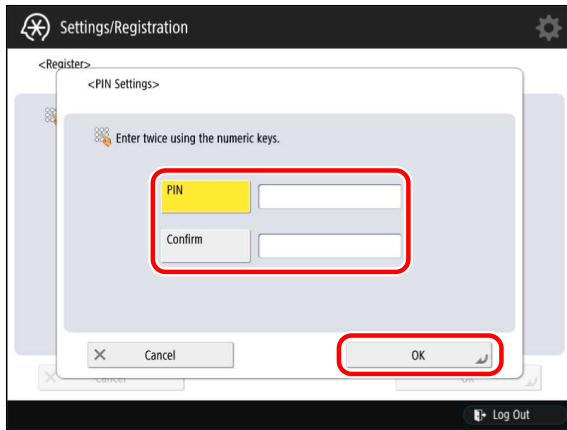
**6 Press [Register].**



**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.

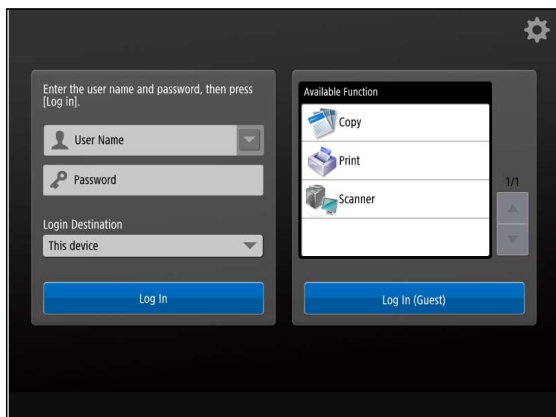
- ▶ **Confirming with Device\_A and Device\_C(P. 124)**
- ▶ **Confirming with Device\_B(P. 126)**

### Confirming with Device\_A and Device\_C

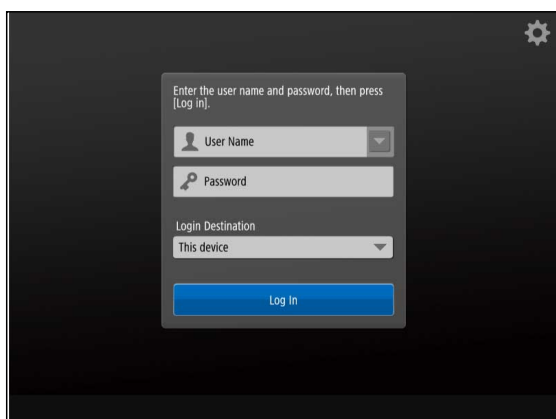
Execute steps 1 to 12 for both Device\_A and Device\_C.

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

#### Device\_A



#### Device\_C

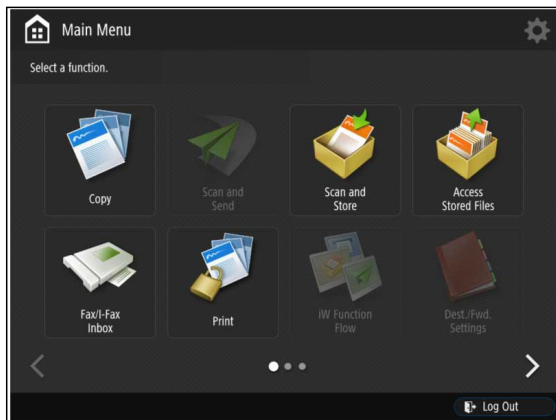


- 2 Enter the user name and password of a [sales\_temp] user in [User Name] and [Password] → select [This device] in [Login Destination] → press [Log In].**

[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.**

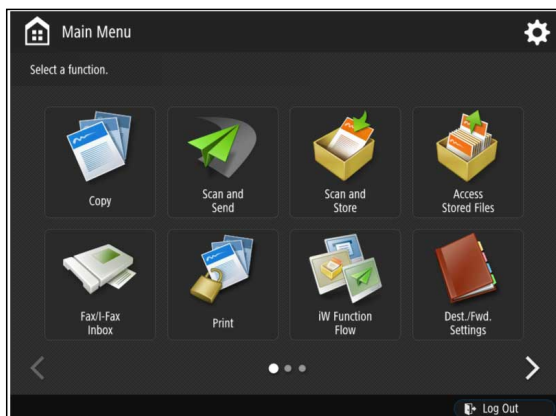
For information on the device screens, see the instruction manuals of the device.

**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.

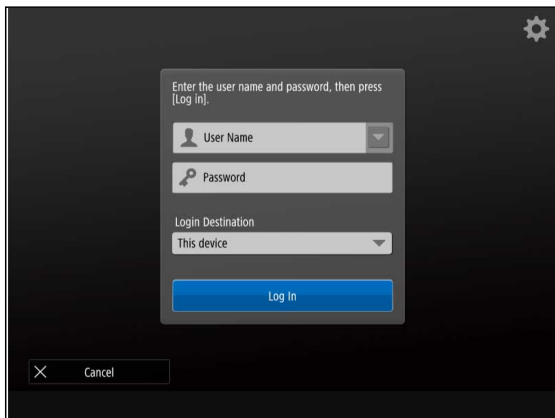
**Confirming with Device\_B**

**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].**

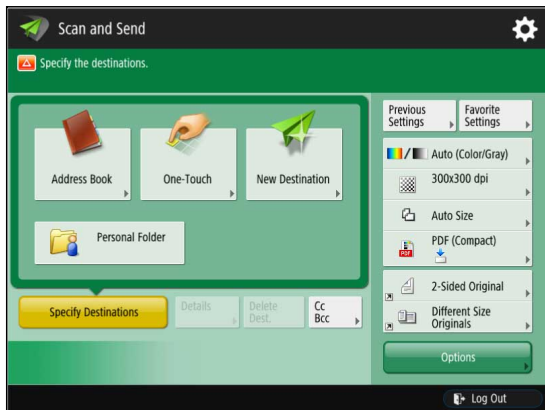
The Login screen is displayed.

**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 with the Access Management System, it is necessary to install the AMS Printer Driver Add-in to the printer drivers installed in the computers, and set the user information.

- ▶ **Installing the AMS Printer Driver Add-in(P. 130)**
- ▶ **Setting User Information to the AMS Printer Driver Add-in(P. 135)**
- ▶ **Setting Up Other Client Computers(P. 137)**

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

Even if multiple types of printer drivers exist on a single computer, the AMS Printer Driver Add-in can be installed to each printer driver with a single operation.

However, when the AMS Printer Driver Add-in is installed in a printer driver, the [AMS] page is added to all of the printer icons associated with that printer driver. Therefore, when a single [AMS] page is set, those settings are applied to all the AMS Printer Driver Add-ins used on computers that are logged on, and the installation of the AMS Printer Driver Add-in and setting of user information can be completed with a single operation.

### IMPORTANT

- The AMS Printer Driver Add-in may already be included, depending on the printer driver. In this case, it is not necessary to install the AMS Printer Driver Add-in. Select [Use AMS Function] on the [AMS] page of the printer driver to enable the functions of the AMS Printer Driver Add-in.
- Confirm that the printer driver supports AMS before installing the AMS Printer Driver Add-in. The add-in will not be installed correctly unless the printer driver supports it. For more information, see "**Client Computer (AMS Printer Driver Add-in)**."(P. 38)
- When using the AMS Printer Driver Add-in in a shared printer environment, install the AMS Printer Driver Add-in to the printer drivers on the print server. (Install the AMS Printer Driver Add-in to the printer driver on the print server. After installing the AMS Printer Driver Add-in to a printer driver on the print server, it may take some time until the [AMS] page is displayed in the printer properties dialog box on a client computer. If the [AMS] page is still not displayed, add the printer icon to the client computer.)
- 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.
- It may not be necessary to install the AMS Printer Driver Add-in, depending on your environment. For more information, see "**Access Management System Configurations(P. 34)**."

### Installing 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 printer driver and the Canon Driver Information Assist Service.

Canon Driver Information Assist Service can be installed at the same time as installing a printer driver. Perform the operations indicated by the wizard.

##### 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].

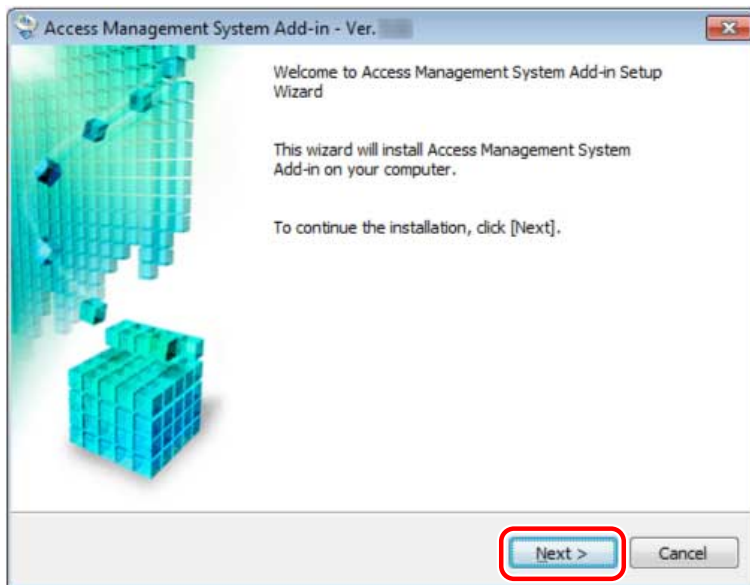
#### 5 Add printer icons for Device\_A, Device\_B, and Device\_C.

For more information, see the Windows instruction manuals.

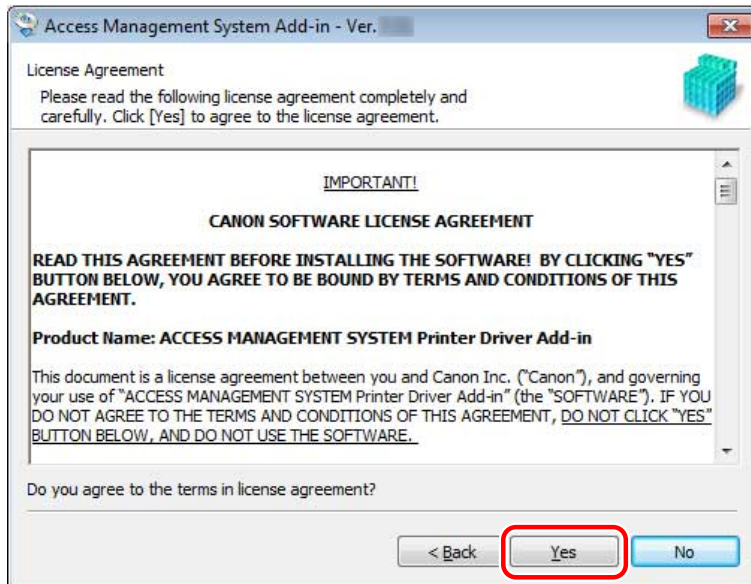
#### 6 Double-click the Setup.exe file for the AMS Printer Driver Add-in.

The AMS Printer Driver Add-in setup wizard starts.

#### 7 Click [Next].

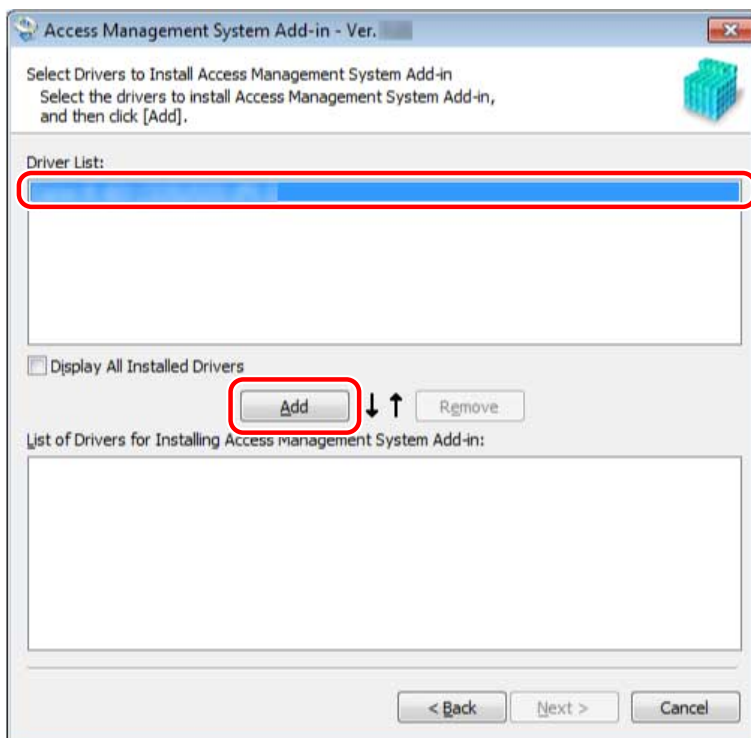


#### 8 Confirm the displayed information → click [Yes].

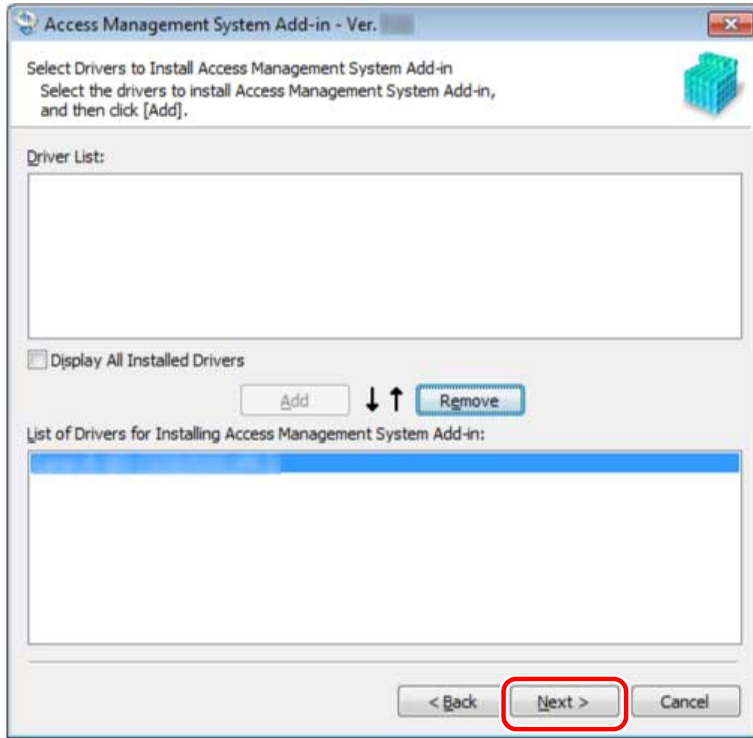


**9 Select the driver to install the AMS Printer Driver Add-in to from the [Driver List] → click [Add].**

In this example, select the printer driver used by Device\_A , Device\_B, and Device\_C → click [Add].

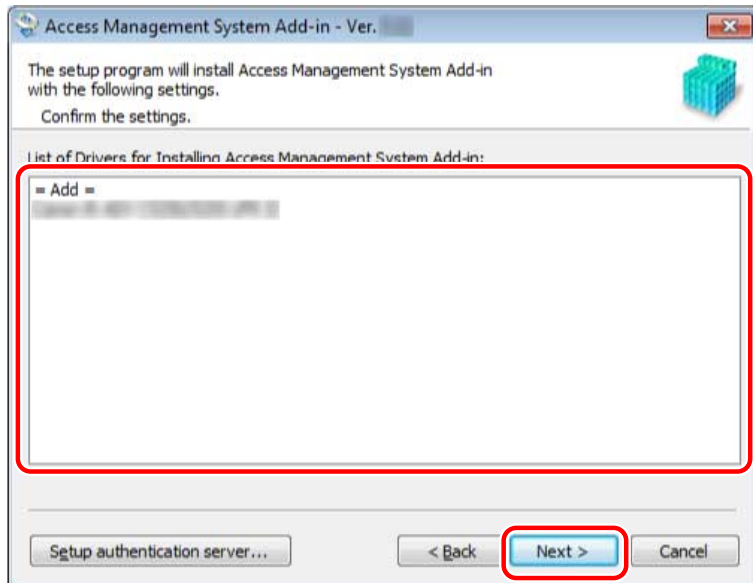


**10 Click [Next].**



**11 Confirm that the appropriate driver names are displayed in [List of Drivers for Installing Access Management System Add-in] → click [Next].**

In this example, confirm that the printer driver used by Device\_A and Device\_B, and Device\_C → click [Next].



**12 Click [Yes] when the message confirming whether you want to retrieve the device (printer) information is displayed.**

If you click [No], the device information is not retrieved. Enter the IP address or host name of the printer on the next screen.

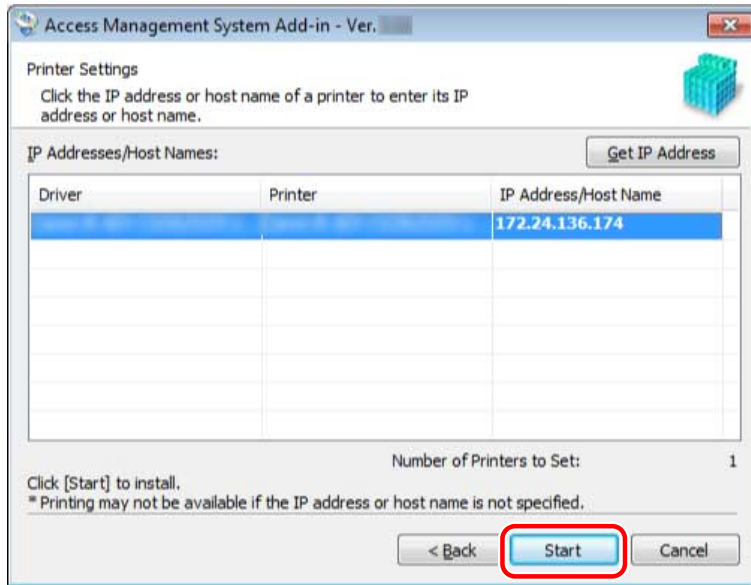
**13 Click [Start].**

If you clicked [No] in the previous screen, click the [IP Address/Host Name] field for that driver → enter the IP address or host name of the device.

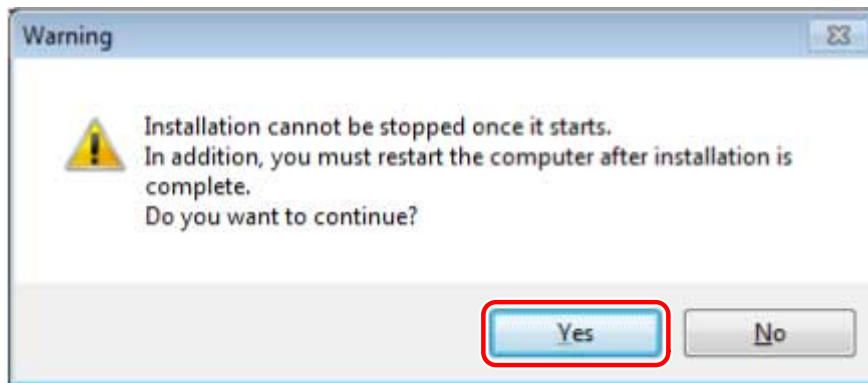


If [Enter IP Address/Host Name] is displayed in the [IP Address/Host Name] field, click [Get IP Address]. If the IP address cannot be retrieved, click the [IP Address/Host Name] field for that driver → enter the IP address or host name of the device.

In this example, confirm that the IP addresses of Device\_A, Device\_B, and Device\_C are displayed → click [Start].

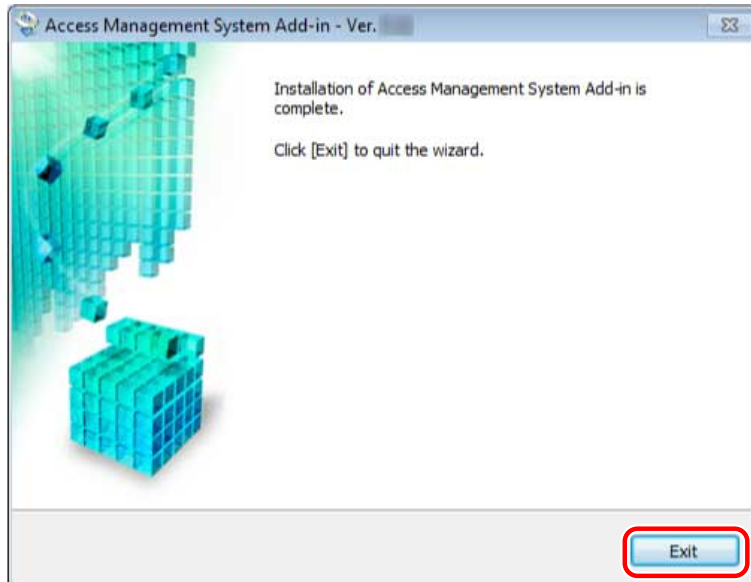


**14** Click [Yes] when the message confirming whether you want to start installing is displayed.

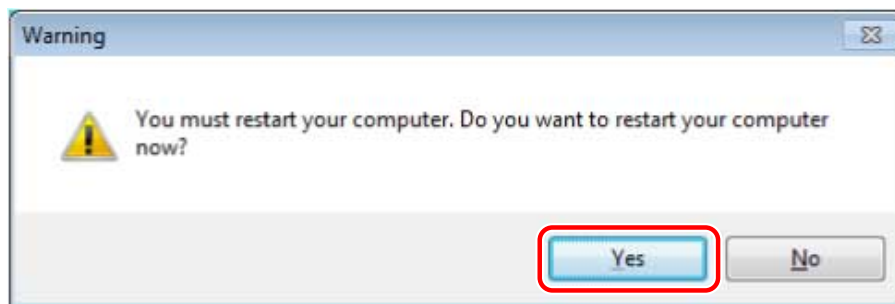


The AMS Printer Driver Add-in is installed.

**15** Click [Exit].



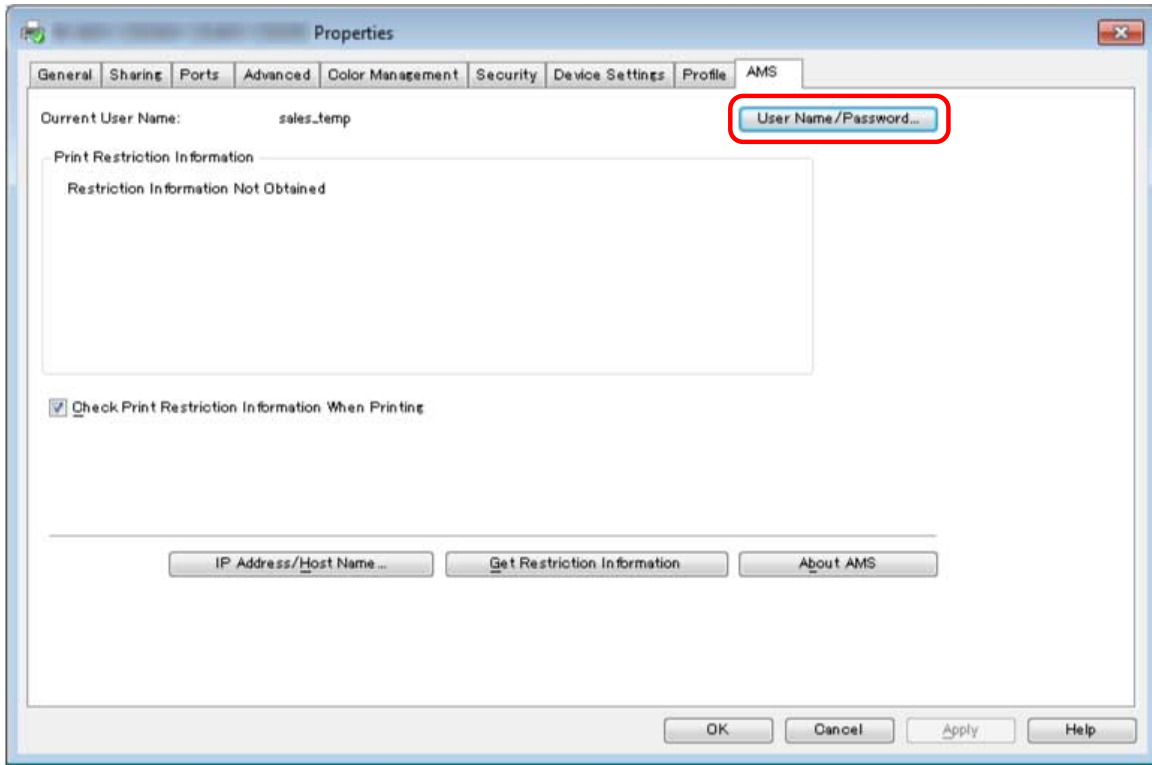
**16** Click [Yes] in the displayed dialog box.



The computer will be restarted and the installation completes.

## Setting User Information to the AMS Printer Driver Add-in

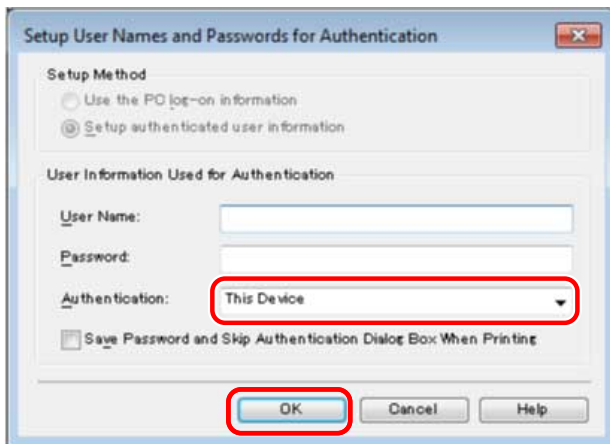
- 1** Log on to the computer in which the AMS Printer Driver Add-in is installed.
- 2** If you are using Windows 8.1/Windows Server 2012, move to the desktop.
- 3** Right-click the icon of Device\_A → select [Properties].
- 4** Click the [AMS] tab.
- 5** Click [User Name/Password].



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 "**Installing the AMS Printer Driver Add-in**"(P. 130) and "**Setting User Information to the AMS Printer Driver Add-in**"(P. 135) 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 operating the AMS Printer Driver Add-in, see the Online Help for the AMS Printer Driver Add-in.

- 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.**

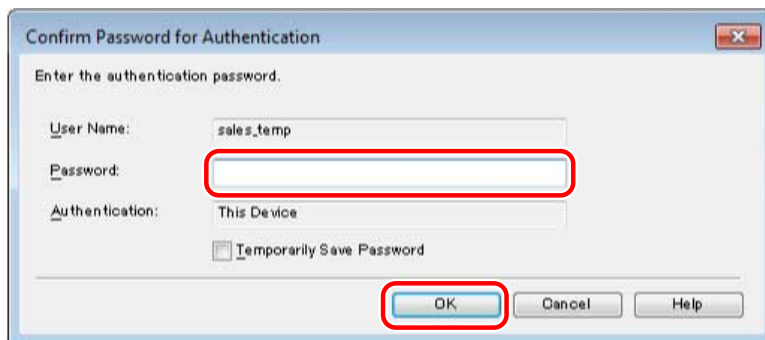
The [Confirm Password for Authentication] dialog box is displayed.

### 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



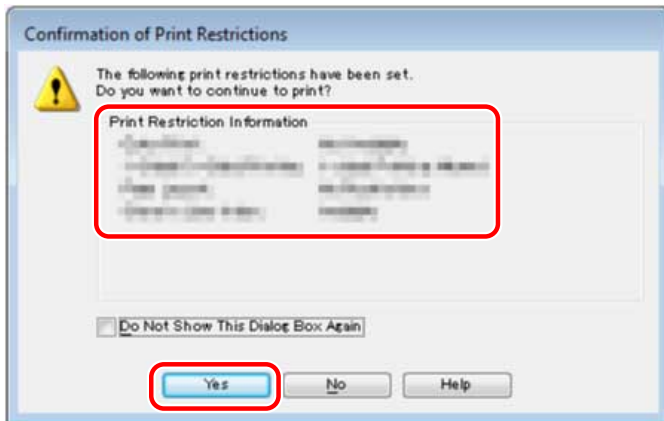
The [Confirmation of Print Restrictions] dialog box is displayed.

### 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

<b>Canceling the Operation of the Access Management System</b> .....	141
<b>Flow of Canceling the Operation of the Access Management System</b> .....	142
<b>Uninstalling the AMS Printer Driver Add-in</b> .....	143

# 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. Uninstalling the AMS Printer Driver Add-in(P. 143)

---

Uninstall the AMS Printer Driver Add-in from the client computers.

## Uninstalling the AMS Printer Driver Add-in

---

This section describes the procedure for uninstalling the AMS Printer Driver Add-in.

### IMPORTANT

- Use the previous version of the uninstaller to uninstall that previous version the AMS Printer Driver Add-in. The procedure for uninstallation is the same as for the previous version.
- When uninstalling the AMS Printer Driver Add-in from a printer driver in a shared printing environment, uninstall the AMS Printer Driver Add-in from the client computers after uninstalling it from the print server. If the driver name is not displayed in the uninstaller, it does not need to be uninstalled from the client computer. Close the uninstaller in this case.
- If you delete the printer driver from the print server, you will become unable to uninstall the AMS Printer Driver Add-in from the printer driver on each client computer. In this case, also delete the printer driver on each client computer.
- If you delete the AMS Printer Driver Add-in from the client computers but leave it on the server in a shared printing environment, the AMS Printer Driver Add-in on the client computers may be reinstalled by a function of the operating system.

- 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 Double-click the UNINSTAL.exe in the [Printer Driver Add-in] folder.**
- 5 Select the driver to uninstall the AMS Printer Driver Add-in from → click [Delete].**
- 6 When a message confirming whether you want to delete the AMS Printer Driver Add-in is displayed, click [Yes].**
- 7 Click [Exit].**
- 8 Click [Yes] in the displayed dialog box.**

The computer will be restarted and the uninstallation completes.

### IMPORTANT

- If you uninstall the AMS Printer Driver Add-in, some of the print settings specified in the printer driver may be changed. Specify the settings again, as necessary.

# Troubleshooting

<b>Troubleshooting</b> .....	146
<b>List of Error Messages</b> .....	147
<b>Troubleshooting</b> .....	167
<b>List of Error Codes</b> .....	169

# 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. 147)**
- ▶ **AMS Printer Driver Add-in(P. 147)**

### 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

## Installation

---

**Cannot install Access Management System Add-in in this operating system.**

Status	The operating system of the computer to install the AMS Printer Driver Add-in is not supported.
Remedy	Install the AMS Printer Driver Add-in in an operating system that is supported. For information on the operating systems that support the AMS Printer Driver Add-in, see " <b>Client Computer (AMS Printer Driver Add-in).</b> "(P. 38)

**The printer selected to install Access Management System Add-in does not exist.**

Status	A driver that supports the AMS Printer Driver Add-in is not installed.
Remedy	Install the AMS Printer Driver Add-in again after installing a printer driver that supports the AMS Printer Driver Add-in.

**Access Management System Add-in**

**The data of the software you want to install may have been modified.**

**If you continue to install, your computer may not operate properly.**

**Are you sure you want to continue to install?**

Status	The AMS Printer Driver Add-in installer is corrupt.
Remedy	Check the file for the AMS Printer Driver Add-in installer, and try executing it again.

**You do not have privileges to perform installation. Log on again with Administrator privileges.**

Status	Could not install the AMS Printer Driver Add-in because the computer is not logged on to as a user with Windows administrator privileges.
Remedy	Log on to the computer as a user with Windows administrator privileges, and try installing the AMS Printer Driver Add-in again.

**This program requires VGA or better resolution.**

Status	The resolution of the computer screen is less than 640 x 480 pixels.
Remedy	Install the AMS Printer Driver Add-in again after setting the resolution of the computer screen to 640 x 480 pixels or higher resolution.

**Cannot install Access Management System Add-in because of insufficient free disk space in drive.**

Status	The hard disk of the computer does not have enough space to install the AMS Printer Driver Add-in.
Remedy	Free enough space on the hard disk of the computer to install the AMS Printer Driver Add-in, and perform the installation again. For information on the required hard disk space, see " <b>Client Computer (AMS Printer Driver Add-in).</b> "(P. 38)

**Setup is not complete. If you quit now, the program will not be installed. Do you want to cancel the setup?**

Status	This message is displayed before canceling the AMS Printer Driver Add-in installation.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**Installation cannot be stopped once it starts. Do you want to continue?**

Status	This message is displayed before installing the AMS Printer Driver Add-in.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**Not authorized to perform printer administration for '<Printer Name>'. Authorize to perform printer administration before installation.**

Status	The AMS Printer Driver Add-in could not be installed because you do not have management privileges for the specified printer.
Remedy	Log on to the computer as a user with management privileges for the specified printer, and install the AMS Printer Driver Add-in again.

**NetSpot Job Monitor is running.  
Exit the NetSpot Job Monitor, and then try to install again.**

Status	Could not install the AMS Printer Driver Add-in because NetSpot Job Monitor is running.
Remedy	Close NetSpot Job Monitor, and try installing the AMS Printer Driver Add-in again.

**A later version of Access Management System Add-in is already installed. Use the installed later version.**

Status	Could not install the AMS Printer Driver Add-in because a version of the AMS Printer Driver Add-in later than the one in the install set is already installed.
Remedy	Check the version of the AMS Printer Driver Add-in.

**Some files related to the Access Management System Add-in program are in use.  
Restart your computer, and then try to install again.**

Status	Could not install the AMS Printer Driver Add-in because an AMS Printer Driver Add-in that is already installed is being used.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**The installer is currently being used.**

Status	Another user is using the AMS Printer Driver Add-in installer with the fast user switching function of Windows.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**The file path to the saved setup file is too long.  
Move the files required for setup to a folder with a shorter path.**

Status	The path to the folder in which the AMS Printer Driver Add-in installer is located is too long.
Remedy	Move the file for the AMS Printer Driver Add-in installer to another folder with a shorter file path, and try executing it again.



**This setup does not contain the files or folders that are required to execute installation on this operating system.**

Status	The files required for the AMS Printer Driver Add-in are insufficient.
Remedy	Check the file for the AMS Printer Driver Add-in installer, and try executing it again.

**Cannot correctly run this installer on this operating system. Use an installer compatible with your operating system.**

Status	The installer used is not compatible with your operating system.
Remedy	Use an installer compatible with your operating system. For information on the operating systems that support the AMS Printer Driver Add-in, see " <b>Client Computer (AMS Printer Driver Add-in)</b> ."(P. 38)

**One or more printer drivers are in use. Restart your computer, and then try to install again.**

Status	Could not install the AMS Printer Driver Add-in because the printer driver is being used on the computer.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again. (If the error is not resolved after restarting the computer, jobs may remain in the printer driver.)

**Print Spooler service is stopped. Restart your computer, and then try to install again.**

Status	Could not install the AMS Printer Driver Add-in because the Print Spooler service is stopped.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**Cannot install this add-in because the selected drivers have already been installed with a maximum number of add-ins.**

Status	Could not install the AMS Printer Driver Add-in because the maximum number of add-ins are installed in the specified printer driver.
Remedy	Install the AMS Printer Driver Add-in again after adding a printer driver that supports the AMS Printer Driver Add-in or uninstalling another add-in.

**Cannot install because Access Management System Add-in of a different language is already installed.**

Status	Could not install the AMS Printer Driver Add-in because the AMS Printer Driver Add-in of another language is installed.
Remedy	Install the AMS Printer Driver Add-in again after uninstalling the AMS Printer Driver Add-in of the other language.

**Could not confirm the specified server record name in DNS.**

**Do you want to set the server as an authentication server?**

Status	Could not confirm on DNS the record name of the specified substitute server.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**This setup will search for network printers then retrieve information, such as the IP address, from the printers.**

**This process may take a while.**

**Retrieve information from the printers?**

Status	It may take some time to retrieve printer information, depending on the status of the network.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**The printer IP address or host name is not entered correctly.**

**Installation cannot be stopped once it starts.**

**In addition, you must restart the computer after installation is complete.**

**Do you want to continue?**

Status	The IP address or host name of some printers are not yet set.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**The printer IP address or host name retrieval was interrupted.**

**Only part of the IP address or host name was retrieved.**

Status	Could not retrieve the IP address or host name of the printer.
Remedy	Click [Get IP Address], or enter the IP address or host name of the printer.

**Could not create the temporary folder.**

Status	Could not install the AMS Printer Driver Add-in because a temporary folder could not be created in the hard disk of the computer.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**Could not copy the setup file to the temporary folder.**

Status	Could not install the AMS Printer Driver Add-in because the AMS Printer Driver Add-in setup file could not be copied to the temporary folder in the hard disk.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**Could not register the setup file to the driver.**

Status	Could not install the AMS Printer Driver Add-in because the AMS Printer Driver Add-in could not be registered to the printer driver.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**Could not change the attribute of the setup file.**

Status	Could not install the AMS Printer Driver Add-in because the read attribute of the AMS Printer Driver Add-in setup file could not be canceled.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**Could not pause the spooler.  
Installation will be canceled.**

Status	Could not install the AMS Printer Driver Add-in because the Print Spooler service could not be stopped.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**Could not restart the spooler. Restart the computer.**

Status	Failed to start the Print Spooler service after installing the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**An error occurred when the registry was being modified or removed.**

Status	Could not install the AMS Printer Driver Add-in because an error occurred when editing or deleting the registry information created with the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**Could not get the starting path of the installer.**

Status	Could not install the AMS Printer Driver Add-in because the running path of the AMS Printer Driver Add-in installer failed to be retrieved.
Remedy	Move the file for the AMS Printer Driver Add-in installer to another folder, and try executing it again.

**Could not delete the already installed Access Management System Add-in.**

Status	Could not delete the already installed AMS Printer Driver Add-in.
Remedy	Restart the computer, and try installing the AMS Printer Driver Add-in again.

**Cannot install because the version of Internet Explorer is old.**

**Install Internet Explorer 6.0 SP2 or later and try again.**

Status	The version of Internet Explorer is not supported by the AMS Printer Driver Add-in.
Remedy	Use a version of Internet Explorer that is supported by the AMS Printer Driver Add-in.

**Cannot update Add-ins that are installed in unsupported versions of printer drivers. Update the printer drivers and try again.**

Status	The AMS Printer Driver Add-in you are trying to install over is installed in an unsupported version of the printer driver.
Remedy	Try installing the AMS Printer Driver Add-in again after updating the printer driver.

**[Record Name] is not entered correctly. Enter the [Record Name] again.**

Status	A record name composed entirely of spaces or an incorrect record name was entered.
Remedy	Click [OK], and enter the correct record name.

## Uninstallation

---

**The driver selected to delete Access Management System Add-in is in use. Restart your computer and then delete Access Management System Add-in.**

Status	Could not uninstall the AMS Printer Driver Add-in because the printer driver for the AMS Printer Driver Add-in to uninstall is being used.
Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.

**You do not have privileges to perform uninstallation. Log on again with Administrator privileges.**

Status	Could not uninstall the AMS Printer Driver Add-in because the computer is not logged on to as a user with Windows administrator privileges.
Remedy	Log on to the computer as a user with Windows administrator privileges, and try uninstalling the AMS Printer Driver Add-in again.

**You do not have privileges to delete one or more of the printers that use the driver '<Driver Name>'. The deletion of Access Management System Add-in in the driver '<Driver Name>' is canceled.**

Status	Could not uninstall the AMS Printer Driver Add-in because you do not have administrator privileges for the specified printer.
--------	---

Remedy	Uninstall the AMS Printer Driver Add-in again after logging on to the computer as a user with administrator privileges for the specified printer.
--------	---

**You do not have privileges to delete one or more of the printers that use the driver '<Driver Name>'.**

**The deletion of Access Management System Add-in in the driver '<Driver Name>' is canceled.**

**Do you want to continue to delete Access Management System Add-in in other drivers?**

Status	Uninstallation of the AMS Printer Driver Add-in was stopped because you do not have administrator privileges for a specified printer, but the operation can be continued.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**Could not delete Access Management System Add-in in the driver '<Driver Name>'.**

**The deletion of Access Management System Add-in in the driver '<Driver Name>' is canceled.**

Status	Could not uninstall the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.

**Could not delete Access Management System Add-in in the driver '<Driver Name>'.**

**The deletion of Access Management System Add-in in the driver '<Driver Name>' is canceled.**

**Do you want to continue to delete Access Management System Add-in in other drivers?**

Status	Could not uninstall the AMS Printer Driver Add-in, but the operation can be continued.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**Printing is incomplete or print jobs remain in one or more of the printers that use the driver '<Driver Name>'.**

**The deletion of Access Management System Add-in in the driver '<Driver Name>' is canceled.**

Status	Could not uninstall the AMS Printer Driver Add-in because print jobs remain in the printer driver.
Remedy	Uninstall the AMS Printer Driver Add-in again after the print jobs in the printer driver finish.

**Printing is incomplete or print jobs remain in one or more of the printers that use the driver '<Driver Name>'.**

**The deletion of Access Management System Add-in in the driver '<Driver Name>' is canceled.**

**Do you want to continue to delete Access Management System Add-in in other drivers?**

Status	Uninstallation of the AMS Printer Driver Add-in was stopped because print jobs remain in the printer driver, but the operation can be continued.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**Do you want to delete Access Management System Add-in in the driver '<Driver Name>'?**

Status	This message is displayed before deleting the AMS Printer Driver Add-in.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**One or more of the printers using the driver '<Driver Name>' are shared on the network. The driver may be in use.**

**Are you sure you want to delete Access Management System Add-in?**

Status	The message is displayed when the specified printer driver is shared on the network.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**NetSpot Job Monitor is running.**

**Exit the NetSpot Job Monitor, and then try to uninstall again.**

Status	Could not uninstall the AMS Printer Driver Add-in because NetSpot Job Monitor is running.
Remedy	Close NetSpot Job Monitor, and try uninstalling the AMS Printer Driver Add-in again.

**One or more of the printers using the driver '<Driver Name>' are network printers.**

**Are you sure you want to delete Access Management System Add-in?**

Status	The message is displayed when a network printer is included in the printers that use the specified printer driver.
Remedy	Confirm whether it is OK to proceed, and click [Yes] or [No].

**Could not delete registry.**

Status	Could not uninstall the AMS Printer Driver Add-in because an error occurred when deleting the registry information created with the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.

**The uninstaller is currently being used.**

Status	Another user is using the AMS Printer Driver Add-in uninstaller with the fast user switching function of Windows.
--------	---

Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.
--------	---

**The file path to the saved files for uninstallation is too long.  
Move the files required for uninstallation to a folder with a shorter path.**

Status	The file path to the folder in which the AMS Printer Driver Add-in uninstaller is stored is too long.
Remedy	Try uninstalling the AMS Printer Driver Add-in again after moving the AMS Printer Driver Add-in uninstaller to another folder with a shorter path.

**Cannot correctly run this uninstaller on this operating system.**

Status	The uninstaller used is not compatible with your operating system.
Remedy	Use an uninstaller compatible with your operating system.

**Cannot correctly run this uninstaller on this operating system.  
Use an uninstaller compatible with your operating system.**

Status	The uninstaller used is not compatible with your operating system.
Remedy	Use an uninstaller compatible with your operating system.

**One or more files or folders required for executing uninstallation are missing.**

Status	The files required for the AMS Printer Driver Add-in uninstallation are insufficient.
Remedy	Check the files for the AMS Printer Driver Add-in uninstaller, and try executing it again.

**Could not delete the file to uninstall.**

Status	Failed to delete files while uninstalling the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.

**Could not restart the spooler.  
Restart the computer.**

Status	Failed to start the Print Spooler service after uninstalling the AMS Printer Driver Add-in.
Remedy	Restart the computer.

**Could not start or pause the related service.  
Restart the computer.**

Status	Failed to start or stop related services while uninstalling the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.

**Could not pause the spooler.**

**Restart the computer.**

Status	Failed to stop the Print Spooler service when uninstalling the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.

**Print Spooler service is stopped. Restart your computer, and then try to uninstall again.**

Status	Could not uninstall the AMS Printer Driver Add-in because the Print Spooler service is stopped.
Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.

**Could not browse the user information.**

Status	Failed to access the user information in the registry while uninstalling the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try uninstalling the AMS Printer Driver Add-in again.

**Could not get the starting path of the uninstaller.**

Status	Could not uninstall the AMS Printer Driver Add-in because the running path of the AMS Printer Driver Add-in uninstaller failed to be retrieved.
Remedy	Move the file for the AMS Printer Driver Add-in uninstaller to another folder, and try executing it again.

## Common Messages

---

This section describes messages that are displayed both when installing and uninstalling the AMS Printer Driver Add-in.

**Cannot find the file '<File Name>' in the folder '<Folder Name>'.**

Status	The files required for the AMS Printer Driver Add-in installation are insufficient.
Remedy	Check the file for the AMS Printer Driver Add-in installer, and try executing it again.

**An error occurred in the initialization file.**

Status	Could not install/uninstall the AMS Printer Driver Add-in because an error occurred in the initialization file for the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try installing/uninstalling the AMS Printer Driver Add-in again.



**An invalid parameter has been specified.**

Status	Could not install/uninstall the AMS Printer Driver Add-in because an invalid parameter was specified for the AMS Printer Driver Add-in installer/uninstaller.
Remedy	Check the parameters specified for the AMS Printer Driver Add-in installer/uninstaller, and install/uninstall the AMS Printer Driver Add-in again.

**Another installation or uninstallation application is running.  
Please wait a moment, and then try to start this application again.**

Status	Another installation or uninstallation application is running.
Remedy	Close the installation or uninstallation program, and try installing/uninstalling the AMS Printer Driver Add-in again.

**Could not perform the process to control exclusion.**

Status	Failed the mutual exclusion process while installing/uninstalling the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try installing/uninstalling the AMS Printer Driver Add-in again.

**Could not get printer information.**

Status	Failed to retrieve printer information while installing/uninstalling the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try installing/uninstalling the AMS Printer Driver Add-in again.

**Could not allocate the memory required.  
Restart the computer and try again.**

Status	The memory required for the AMS Printer Driver Add-in installation/uninstallation is insufficient.
Remedy	Close any unnecessary applications and services that are running, and install/uninstall the AMS Printer Driver Add-in again.

**Could not access the service.  
Check the Print Spooler or Canon Output Manager Service.**

Status	Failed to access the service while installing/uninstalling the AMS Printer Driver Add-in.
Remedy	Restart the computer, and try installing/uninstalling the AMS Printer Driver Add-in again.

**Could not create the result file.**

Status	Could not install/uninstall the AMS Printer Driver Add-in because an invalid parameter was specified for the AMS Printer Driver Add-in installer/uninstaller.
--------	---

Remedy	Check the parameters specified for the AMS Printer Driver Add-in installer/uninstaller, and install/uninstall the AMS Printer Driver Add-in again.
--------	--

## 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 version of this add-in does not match the obtained restriction information.

Status	The restriction information retrieved from the installed add-in is not supported.
Remedy	Check the version of the add-in and the restriction information. To check the version of the add-in, click the [About AMS] button on the [AMS] page of the printer properties dialog box.

### 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.

**Cannot use Access Management System Add-in because the version of Internet Explorer is old.**

**Install Internet Explorer 6.0 SP2 or later and try again.**

Status	The version of Internet Explorer is not supported by the AMS Printer Driver Add-in.
Remedy	Use a version of Internet Explorer that is supported by the AMS Printer Driver Add-in.

**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.

## Nothing is displayed when the AMS Printer Driver Add-in installer is executed.

Cause	The path to the folder in which the AMS Printer Driver Add-in installer is located is too long.
Remedy	Move the file for the AMS Printer Driver Add-in installer to another folder with a shorter file path, and try executing it again.

## The AMS Printer Driver Add-in is installed, but the [AMS] tab is not displayed on the Printer Properties dialog box.

Cause 1	The AMS Printer Driver Add-in is not installed properly.
Remedy	Check that the printer driver supports AMS Printer Driver Add-in. For information on the printer drivers that support the AMS Printer Driver Add-in, see " <b>Client Computer (AMS Printer Driver Add-in).</b> "(P. 38)
Cause 2	You tried to install the AMS Printer Driver Add-in in a printer driver on a client computer when using a shared printer environment.
Remedy	Install the AMS Printer Driver Add-in to the printer driver on the print server. After installing the AMS Printer Driver Add-in to a printer driver on the print server, it may take some time until the [AMS] page is displayed in the printer properties dialog box on a client computer. If the [AMS] page is still not displayed, add the printer icon to the client computer.

## When installing the AMS Printer Driver Add-in, a driver name is not displayed in [Driver List] on the driver selection screen.

Cause 1	The printer driver installed in the computer does not support Access Management System.
Remedy	Download the latest printer driver from the Canon Web site, and install it.
Cause 2	The printer driver installed in the computer does not have an icon corresponding to it on the computer.
Remedy	If you are using the latest printer driver and its printer icon is not displayed, select [Display All Installed Drivers].


**Printing from a computer with the AMS Printer Driver Add-in installed takes a long time.**

Cause	When using TLS for communication between the client computer and the devices, the authentication process may take a long time if the root certificate is automatically updated during authentication. (For devices that can select whether to use TLS communication for each function, TLS communication is always used during authentication, regardless of the device settings.)
Remedy	<p>If you want to reduce the processing time, use the following procedure to disable the root certificate automatic updating function in the computer with the AMS Printer Driver Add-in installed.</p> <ul style="list-style-type: none"> <li>• If you disable this setting, the root certificate will also not be automatically updated when performing TLS communication other than with the AMS Printer Driver Add-in. Restore the setting after printing from the device, as necessary.</li> <li>• Some terms may differ depending on the operating system you are using.             <ol style="list-style-type: none"> <li>1. Select [Run] from the [Start] menu.</li> <li>2. Enter 'gpedit.msc' and press the [Enter] key. The [Local Group Policy Editor] dialog box is displayed.</li> <li>3. Click [Computer Configuration] → [Administrative Templates] → [SYSTEM] → [Internet Communication Management] → [Internet Communication Settings].</li> <li>4. Set [Turn off Automatic Root Certificates Update] to [Enabled].</li> </ol> </li> </ul>

## 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

<b>Appendix</b> .....	171
<b>Regarding Security when Operating the Access Management System</b> .....	172
Updating the Key Pair for Access Control .....	173
<b>Other Precautions</b> .....	175

## 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 uninstalls the AMS Printer Driver Add-in, the Access Management System will become unable to 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

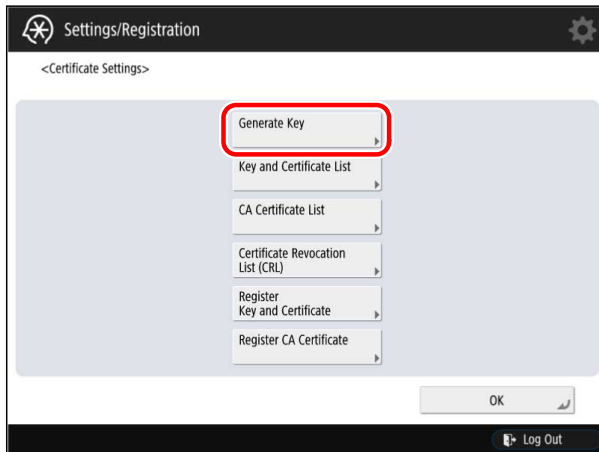
Periodically update the key pair as necessary, for improved security. This section describes the procedure for updating the key pair for access control.

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.)

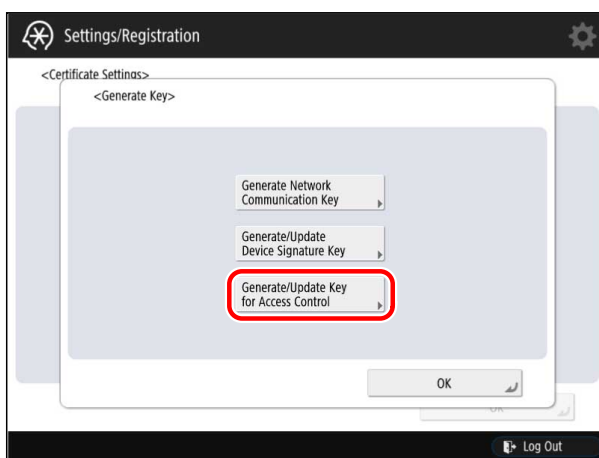
### Updating the Key Pair for Access Control(P. 173)

## Updating the Key Pair for Access Control

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

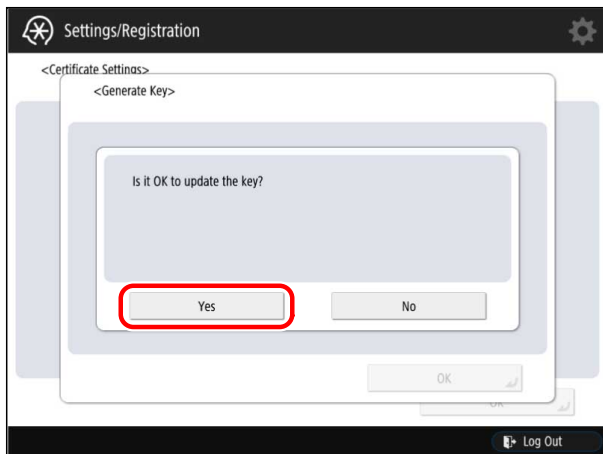


- 2 Press [Generate/Update Key for Access Control].



- 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.